Кибердзюцу. Кибербезопасность для современного ниндзя

Полный русский перевод книги Бена Маккарти о применении принципов и тактик синоби к современной кибербезопасности.

Больше крутых материалов в моём телеграм-канале @grogrigs

Глава 1. Картографирование сетей

> Имея эти карты, полководец может обдумать, как защищать и атаковать замок.
>
> При переносе лагеря следует соблюдать ряд правил, касающихся времени и дня выступления. Обязанность синоби - точно знать географию местности и расстояние до врага.
>
> - «Ёсимори хякусю», стихотворение 9

> Как только раздобудете подробные сведения о замке или лагере и его планировке, вам останется лишь как можно скорее вернуться с ними: именно так и должен поступать хороший синоби.
>
> - «Ёсимори хякусю», стихотворение 24

Самый первый совет из раздела «Наставление для командиров» в «Бансэнсюкай» - составлять скрупулёзно точные карты, по которым полководцы смогут планировать нападения на врага.[1] Избранные стихотворения из «Ёсимори хякусю»[2] также подчёркивают, насколько важно чертить и поддерживать в актуальном состоянии карты, достаточно подробные, чтобы они были полезны и целой армии, и отдельному синоби.

Командиры обычно поручали составление карт синоби. В свитках ясно сказано: умение точно зарисовать увиденное - горы, реки, поля - не равнозначно умению составлять целенаправленные, снабжённые контекстом карты разведывательных данных об угрозах, которые помогают вырабатывать военную стратегию или планировать проникновение синоби. Согласно свиткам, для тактики ведения войны и оперативного искусства синоби существенны, а потому должны наноситься на карты следующие сведения:[3]

- **Все входы и ворота дома, замка или крепости.** Какие там замки, засовы и механизмы открывания? Насколько трудно открыть ворота или двери и шумят ли они при открывании или закрывании?
- **Подходящие дороги.** Прямые они или извилистые? Широкие или узкие? Грунтовые или мощёные камнем? Ровные или идут под уклон?
- **Устройство, состав и планировка сооружения.** Каковы размер и назначение каждой комнаты? Что хранится в каждой комнате? Скрипят ли половицы?
- **Обитатели сооружения.** Как их зовут? Владеют ли они какими-либо заслуживающими внимания навыками или искусствами? Насколько каждый из них бдителен или подозрителен?
- **Топология замка и окружающей местности.** Видны ли сигнальные посты изнутри и снаружи? Где хранятся продовольствие, вода и дрова? Каковы ширина и глубина рвов? Какова высота стен?

Что представляют собой карты сетей

В кибербезопасности карты сетей - это графы сетевой топологии, описывающие физические и/или логические отношения и конфигурацию связей (соединений связи) и узлов (устройств) сети. Чтобы лучше понять это понятие, вспомните дорожную карту или карту в атласе. На них показаны физические места, географические объекты, политические границы и природный ландшафт. Сведения о дорогах (связях) - их названиях, направлении, протяжённости и пересечениях с другими дорогами - позволяют перемещаться между разными местами (узлами). Теперь рассмотрим следующий вымышленный сценарий.

Представьте, что вы живёте в мире, где дороги и здания самопроизвольно возникают и исчезают в мгновение ока. GPS существует, и вы знаете координаты своего местонахождения и пункта назначения, но добираться туда приходится по запутанной сети непрерывно меняющихся дорог.

К счастью, на каждом перекрёстке стоят служащие навигационной службы (маршрутизаторы), помогающие таким путешественникам, как вы, найти дорогу. Эти маршрутизаторы постоянно обзванивают соседние маршрутизаторы, выясняя, какие маршруты и места открыты, чтобы обновить таблицу маршрутизации, которую держат на планшете. На каждом перекрёстке вы должны остановиться и спросить у маршрутизатора, как добраться до следующего угла, предъявив дорожную карточку, где пункт назначения закодирован координатами GPS. Маршрутизатор сверяется со своим планшетом, на котором указаны открытые в данный момент пути, выполняет некоторые расчёты, быстро показывает направление, ставит на дорожной карточке штамп со своим адресом, пробивает в карточке отверстие, чтобы учитывать число маршрутизаторов, у которых вы отметились за время путешествия, и отправляет вас к следующему маршрутизатору. Этот процесс повторяется до тех пор, пока вы не достигнете пункта назначения. А теперь представьте картографов этого мира: скорее всего, они уже отказались бы от попыток составлять точные карты, поскольку не поспевали бы за вечно меняющейся сетью. Таким картографам пришлось бы довольствоваться тем, что они отмечают основные ориентиры и достопримечательности условными названиями и проводят между ними нечёткие линии, показывая, что между точками существуют какие-то пути.

Этот вымышленный мир в действительности существует в киберпространстве. Именно поэтому карты сетей недостаточно точны, а их актуализации уделяется меньше внимания, чем следовало бы. Отсутствие качественных, всеобъемлющих карт сетей считается общеизвестной проблемой организаций, занимающихся кибербезопасностью. Если карта у организации вообще есть, её обычно передают центру управления безопасностью (security operations center, SOC), чтобы показать расположение датчиков или защитных устройств в потоках данных и облегчить понимание перехватов пакетов, правил межсетевых экранов, предупреждений и системных журналов. Но, вероятнее всего, такая карта вдобавок абстрактна: на ней показаны лишь базовые элементы - границы Интернета, периметровой и внутренней сетей; примерное расположение пограничных маршрутизаторов или межсетевых экранов; а также неопределённые сетевые границы и умозрительные схемы, обозначенные облачными контурами. Пример слабо проработанной, но широко распространённой карты сети, доступной специалистам по кибербезопасности и ИТ, приведён на рисунке 1-1.

Чтобы объяснить, почему рисунок 1-1 представляет собой «плохую» карту, снова рассмотрим советы «Бансэнсюкай» по картографированию, но теперь применительно к соответствующим подробностям киберсреды.

- **Все точки доступа к узлу сети.** Какие интерфейсные точки доступа есть на устройстве: Ethernet (`e`), Fast Ethernet (`fe`), Gigabit Ethernet (`ge`), Universal Serial Bus (`USB`), Console (`con`), loopback (`lo`), Wi-Fi (`w`) и так далее? Применяется ли управление доступом к сети (network access control, NAC) или фильтрация адресов управления доступом к среде (media access control, MAC)? Разрешён ли удалённый или локальный консольный доступ и защищён ли он должным образом? Какая физическая защита предусмотрена? Есть ли замки на дверцах стоек или даже блокираторы USB-портов? Ведётся ли журналирование доступа через интерфейсы? Где находятся интерфейс и сеть управления? Каковы IP- и MAC-адреса каждой точки доступа?

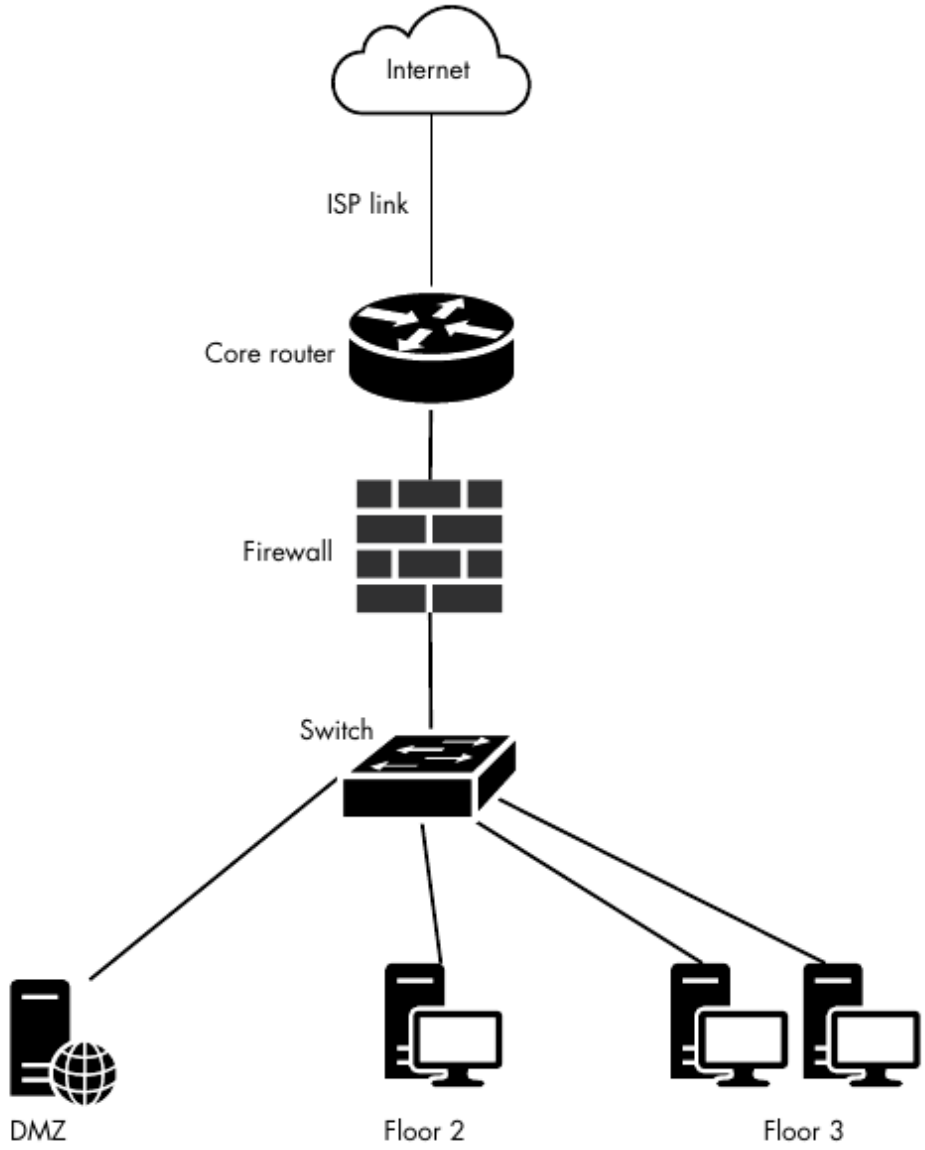

Рисунок 1-1. Упрощённая карта сети

• **Пограничные шлюзы, промежуточные узлы и точки выхода.** Использует ли организация более одного интернет-провайдера (internet service provider, ISP)? Относится ли подключение к типу Trusted Internet Connection (TIC) или Managed Internet Service (MIS)? Какова пропускная способность интернет-соединения? Из какой среды передачи состоит выходное соединение: оптоволокна, Ethernet, коаксиального кабеля или чего-то иного? Через какие промежуточные узлы подходят к сети? Предусмотрены ли спутниковые, микроволновые, лазерные или Wi-Fi-каналы выхода из сети или входа в неё?

- **Устройство, состав и структура сети.** Каковы название, назначение и размер каждой подсети (например, в терминах бесклассовой междоменной маршрутизации - Classless Inter-Domain Routing, CIDR)? Имеются ли виртуальные локальные сети (virtual local area network, VLAN)? Ограничен ли пул соединений? Является ли сеть плоской либо иерархической, разделена ли она по зданиям, уровням защиты и/или функциям?
- **Хосты и узлы сети.** Как они называются? Какая версия операционной системы (operating system, OS) на них установлена? Какие службы и порты на них работают и какие из них открыты? Какие средства защиты могут обнаружить атаку? Затрагивают ли их какие-либо известные уязвимости из перечня Common Vulnerabilities and Exposures (CVE)?
- **Физическая и логическая архитектура сети и здания.** Где расположен центр обработки данных? Есть ли розетки Ethernet в вестибюле? Распространяется ли сигнал Wi-Fi за пределы здания? Видны ли снаружи компьютерные экраны и терминалы? Используются ли в офисе защитные стёкла? Правильно ли сегментированы гостевые сети и сети переговорных комнат? Каковы основные списки контроля доступа (access control list, ACL) и правила межсетевых экранов сети? Где выполняется разрешение DNS-имён? Что доступно в периметровой сети или DMZ? Используются ли внешние поставщики электронной почты или другие облачные службы? Как устроены удалённый доступ и виртуальная частная сеть (virtual private network, VPN)?

Организации, у которых нет рабочей карты сети, иногда обращаются вместо неё к монтажным схемам, подготовленным ИТ-отделом. Эти упрощённые изображения документируют взаимное расположение систем, сетевого оборудования и соединений устройств и могут служить справочным материалом при устранении технических или эксплуатационных неполадок в сети. Однако слишком многие организации отказываются даже от таких грубых схем в пользу электронной таблицы, где для всего оборудования перечислены имена хостов, модели и серийные номера, почтовые и IP-адреса, а также ряды монтажных стоек в центре обработки данных. Если заинтересованные лица могут находить ресурсы по этой таблице, а в сети не происходит крупных неполадок или сбоев, наличие такой документации способно даже отбить желание составлять карту сети. Поразительно, но некоторые компании полагаются на архитектора или специалиста, который держит «карту» в голове, и формальная - или хотя бы неформальная - карта так никогда и не появляется.

Справедливости ради следует признать: для отсутствия полезных карт сетей существуют веские причины. На создание, распространение и поддержание карт в актуальном состоянии может уходить драгоценное время и другие ресурсы. Кроме того, карты подвержены изменениям. Добавление систем в сеть или их удаление, изменение IP-адресов, перекоммутация кабелей, внедрение новых правил маршрутизаторов или межсетевых экранов - всё это способно существенно снизить точность карты, даже если она была составлена всего несколько мгновений назад. К тому же современные компьютеры и сетевые устройства используют протоколы динамической маршрутизации и настройки хостов, которые автоматически передают сведения другим системам и сетям без всякой карты, то есть сети по сути способны настраиваться самостоятельно.

Разумеется, существует множество программных средств «картографирования», например Nmap,[4] которые сканируют сети в поисках хостов, визуализируют сеть по числу промежуточных узлов от сканера, обнаруживают и отображают топологию сети с помощью протокола Simple Network Management Protocol (SNMP) либо быстро строят сетевые схемы по файлам конфигурации маршрутизаторов и коммутаторов. Созданные программами сетевые схемы удобны, но редко охватывают все подробности и весь контекст, необходимые для той высококачественной карты, которую хотел бы иметь защитник или злоумышленник. Вероятно, идеальное решение - построить карту сети с программной поддержкой, сочетая средства картографирования, сетевое сканирование и человеческие знания. Но даже такой подход требует значительных затрат времени специалиста с особыми навыками, чтобы карта оставалась точной и, следовательно, полезной.

Несмотря на эти ограничения, защитникам жизненно важно сохранять бдительность в отношении картографирования. Пример на рисунке 1-2 показывает, насколько подробной должна быть карта защитника, чтобы с её помощью можно было защищать сеть.

Для обозначения сетевых устройств используются не пиктограммы, а легко различимые геометрические фигуры. Для однотипных устройств повторяется одна и та же форма. Например, кругами на рисунке 1-2 обозначены рабочие станции, квадратами - маршрутизаторы, а прямоугольниками - серверы; если бы на карте присутствовали ретрансляторы электронной почты или контроллеры домена, их обозначали бы треугольниками. Кроме того, фигуры не имеют текстуры или фона, благодаря чему вписанные в них сведения хорошо читаются.

Каждый интерфейс - и виртуальный, и физический - подписан с указанием типа и номера. Например, интерфейс типа Ethernet обозначен как `eth`, а его номер совпадает с физической маркировкой на устройстве: `eth 0/0`. Неиспользуемые интерфейсы также подписаны. Для каждого интерфейса указываются назначенные ему IP-адрес и подсеть, если они известны.

Известные сведения об устройстве - имя хоста, производитель и модель, версия ОС - записываются в его верхней части. Уязвимости, стандартные учётные данные, известные учётные данные и другие ключевые недостатки отмечаются в центре устройства. Там же документируются работающие службы, программное обеспечение и открытые порты. VLAN, сетевые границы, компоновка и структура должны быть отражены на карте сети и снабжены подписями наряду со всеми заслуживающими внимания сведениями.

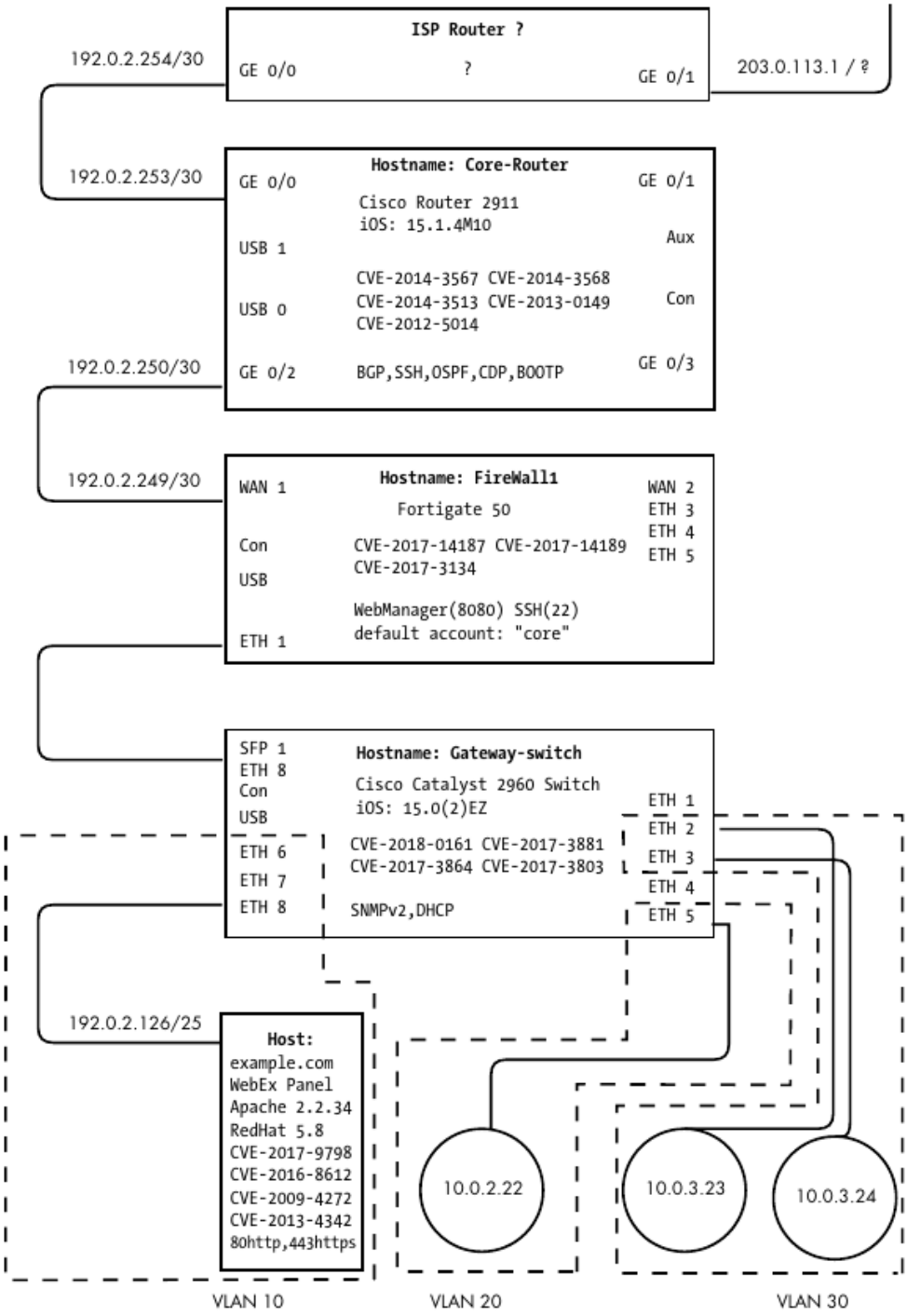

Рисунок 1-2. Подробная карта сети

Незаметный сбор разведывательных данных

Для синоби незаметный сбор разведывательных данных был искусством высшего уровня. Если бы кто-то слонялся возле замка и проводил подробные измерения плотницким угольником или иным приспособлением, обитатели заметили бы это и распознали в нём вражеского агента. Поэтому предусмотрительные синоби составляли карты в мирное время, когда жители укреплений теряли бдительность: тогда синоби могли свободнее путешествовать и вызывали меньше подозрений при сборе сведений.[5]

Однако синоби нередко приходилось изобретать способы скрытно снимать размеры, отмечать особенности рельефа и собирать другие разведывательные сведения. Показательно, что описание точного составления карт в «Бансэнсюкай» включено в раздел о приёмах открытой маскировки: это говорит о том, что синоби пользовались обманом, чтобы заниматься картографированием прямо на глазах у врага. В свитке упоминается приём под названием *урамитцу-но дзюцу*[6] - искусство оценки расстояния, при котором расстояние до знакомого предмета определяют, используя в качестве масштаба известный размер этого предмета. *Урамитцу-но дзюцу* включало и хитроумные тригонометрические уловки. Например, синоби мог лечь ногами к цели и снимать размеры, пользуясь известной длиной своих стоп, а со стороны казалось, будто он дремлет под деревом.

Сбор ориентиров в сети - одно из первых действий злоумышленников перед атакой на целевую сеть или хост. Карты, составляемые злоумышленниками, служат той же цели, что и карты исторических ниндзя: выявить и задокументировать сведения, необходимые для проникновения в цель. К таким сведениям относятся все точки входа в сеть и выхода из неё: подключения к ISP; точки беспроводного доступа; точки ультравысокочастотной, микроволновой, радио- или спутниковой связи; облачные, взаимосвязанные и внешние сети.

Злоумышленники также ищут шлюзы протокола Border Gateway Protocol (BGP), маршруты и промежуточные узлы на пути к сети. Их интересуют репрезентативная структура, компоновка и устройство сети; её инвентарные данные, включая имена хостов, модели устройств, операционные системы, открытые порты, работающие службы и уязвимости; а также сетевая топология - подсети, VLAN, ACL и правила межсетевых экранов.

Многие средства сетевого картографирования, которыми пользуются злоумышленники, работают «шумно»: они связываются с большим числом хостов, применяют нестандартные пакеты и могут быть обнаружены внутренними защитными устройствами. Однако злоумышленники способны ослабить эти недостатки, замедлив средство картографирования или ограничив его скорость, используя обычные, не вызывающие подозрений пакеты и даже ведя ручную разведку распространёнными средствами, уже имеющимися на компьютере жертвы, например `ping` или `net`. Можно также применять безобидные методы разведки: атакующий вообще не обращается к цели и не сканирует её, а собирает сведения через Shodan или из ранее проиндексированных данных, найденных интернет-поисковиками.

Более искушённые противники разрабатывают оперативные приёмы пассивного картографирования - тактику, при которой сведения о цели собираются без непосредственного взаимодействия с ней, то есть, например, без активного сканирования Nmap. Другой приём пассивного картографирования состоит в интерпретации пакетов, перехваченных через сетевой интерфейс в неразборчивом режиме. В этом режиме интерфейс настраивается на запись и исследование всего сетевого обмена, в отличие от обычного режима, где записывается и исследуется только обмен, адресованный самому интерфейсу. Неразборчивый режим позволяет разобраться в соседних хостах, потоках трафика, службах и протоколах сети, ни разу не вступая с ней в активное взаимодействие.

Ещё один способ картографировать сеть без непосредственного взаимодействия - собирать исходящую из сети электронную переписку сетевого администратора, искать карты целевой сети во

внешнем файловом хранилище с общим доступом или просматривать сторонние форумы технической поддержки, где администратор мог опубликовать журналы и сообщения об ошибках, конфигурации маршрутизаторов, результаты сетевой диагностики, `tracert` и `ping` либо другие технические подробности, раскрывающие структуру и конфигурацию сети. Подобно приёму синоби *урамитцу-но дзюцу*, использование наблюдаемых сведений из целевой сети позволяет составлять её карту, не привлекая внимания цели.

Пассивное картографирование может включать измерение задержек в сохранённых результатах `tracert` из сети для выявления спутниковых участков - например, присутствие спутника выдаёт внезапное увеличение задержки связи на 500 миллисекунд - или обнаружения углублённой обработки пакетов межсетевым экраном - например, препроцессор распознаёт возможную вредоносную атаку и вносит заметные задержки в специально сформированный обмен. К пассивному картографированию также можно отнести раскрытие сведений о внутренней сети через внешние зоны DNS и ответы с записями; открытые заказы на закупку и заявки на приобретение определённого программного или аппаратного обеспечения; и даже объявления о вакансиях сетевых или ИТ-администраторов, от которых требуется опыт работы с конкретной технологией, сетевым оборудованием, аппаратным или программным обеспечением.

Затратив столько времени на разработку своих карт, атакующий может получить более полную картину, чем сама цель: противник способен знать о целевой сети больше, чем её владелец. Чтобы лишить его такого преимущества, защитникам сети следует стремиться составлять и поддерживать карты более высокого качества и тщательно оберегать их.

Создание собственной карты

Общий процесс создания карты можно разделить на три этапа:

1. Вложите необходимые средства в создание исчерпывающей и точной карты, которую легко обновлять и можно безопасно хранить. Она должна содержать сведения, необходимые каждой команде для решения её задач, например ИТ-отделу, центру управления сетью (network operations center, NOC) и SOC. Рассмотрите возможность поручить составление и анализ карты специально выделенному сотруднику или коллективу либо внешнему подрядчику.
2. Составьте карту, включив в неё все разновидности точных сведений, перечисленные в начале этой главы.
3. Требуйте экспертной проверки карты в рамках заявок на управление изменениями, а также всякий раз, когда кто-либо замечает несоответствие внутри карты или расхождение с ней.

Рассмотрим подробнее второй этап - составление карты.

После того как вы определили всех ключевых заинтересованных лиц и убедили их в приоритетности проекта, первым делом соберите абсолютно всё, что имеется внутри организации и может помочь в картографировании. Сюда относятся монтажные схемы, старые планы проектов сетевой архитектуры, результаты сканирования уязвимостей, списки ресурсов, результаты инвентаризации центра обработки данных, аренды DHCP, записи DNS, данные сетевого управления SNMP, записи агентов на конечных устройствах, перехваты пакетов (packet capture, PCAP), журналы систем управления информацией и событиями безопасности (security information and event management, SIEM), конфигурации маршрутизаторов, правила межсетевых экранов и результаты сканирования сети. Главным источником для построения основной архитектуры и структуры карты сети должны стать конфигурации маршрутизаторов. В качестве отправной точки можно поместить основной или центральные маршрутизаторы в центр карты и от них выстраивать дальнейшие ветви. Перехваты PCAP способны выявить обменивающиеся данными конечные устройства, которые не отвечают на сетевое сканирование либо недоступны сканеру из-за сетевой фильтрации. Если разрешить избранным системам в течение продолжительного времени собирать PCAP в неразборчивом режиме, затем можно будет просмотреть список найденных в PCAP конечных устройств, как показано на рисунке 1-3.

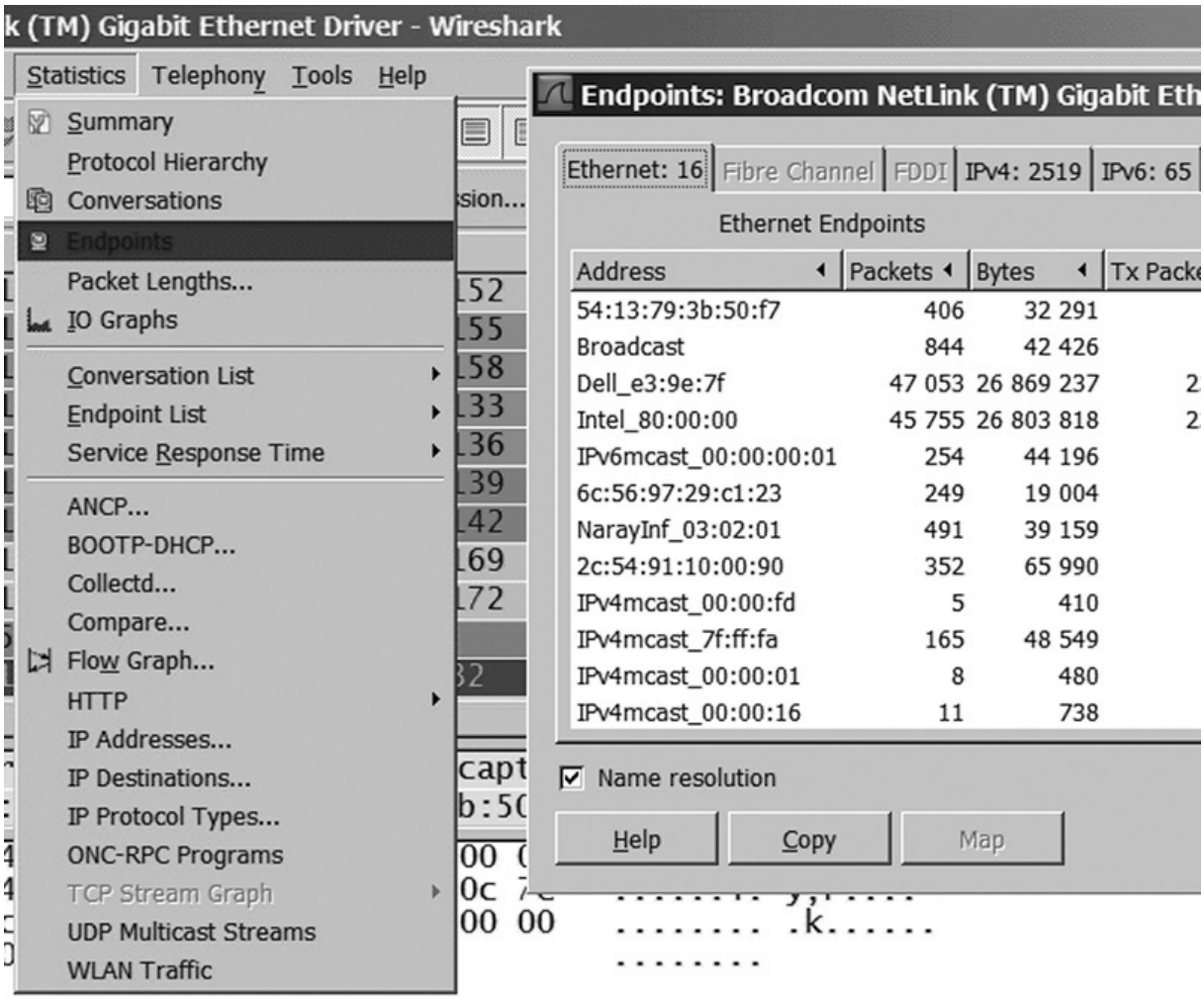

Рисунок 1-3. Снимок экрана Wireshark с конечными устройствами, обнаруженными при сборе PCAP

В идеале PCAP следует собирать во время сетевого сканирования, чтобы проверять охват сканера. Кроме того, нужно провести несколько сканирований сети, причём как минимум одно конечное устройство в каждой подсети должно просканировать свою подсеть. Результаты этих сканирований можно вручную соединить в единую топологическую карту сети, как показано на рисунке 1-4. Определите операции, которые можно автоматизировать, чтобы в будущем этот процесс было легче повторять.

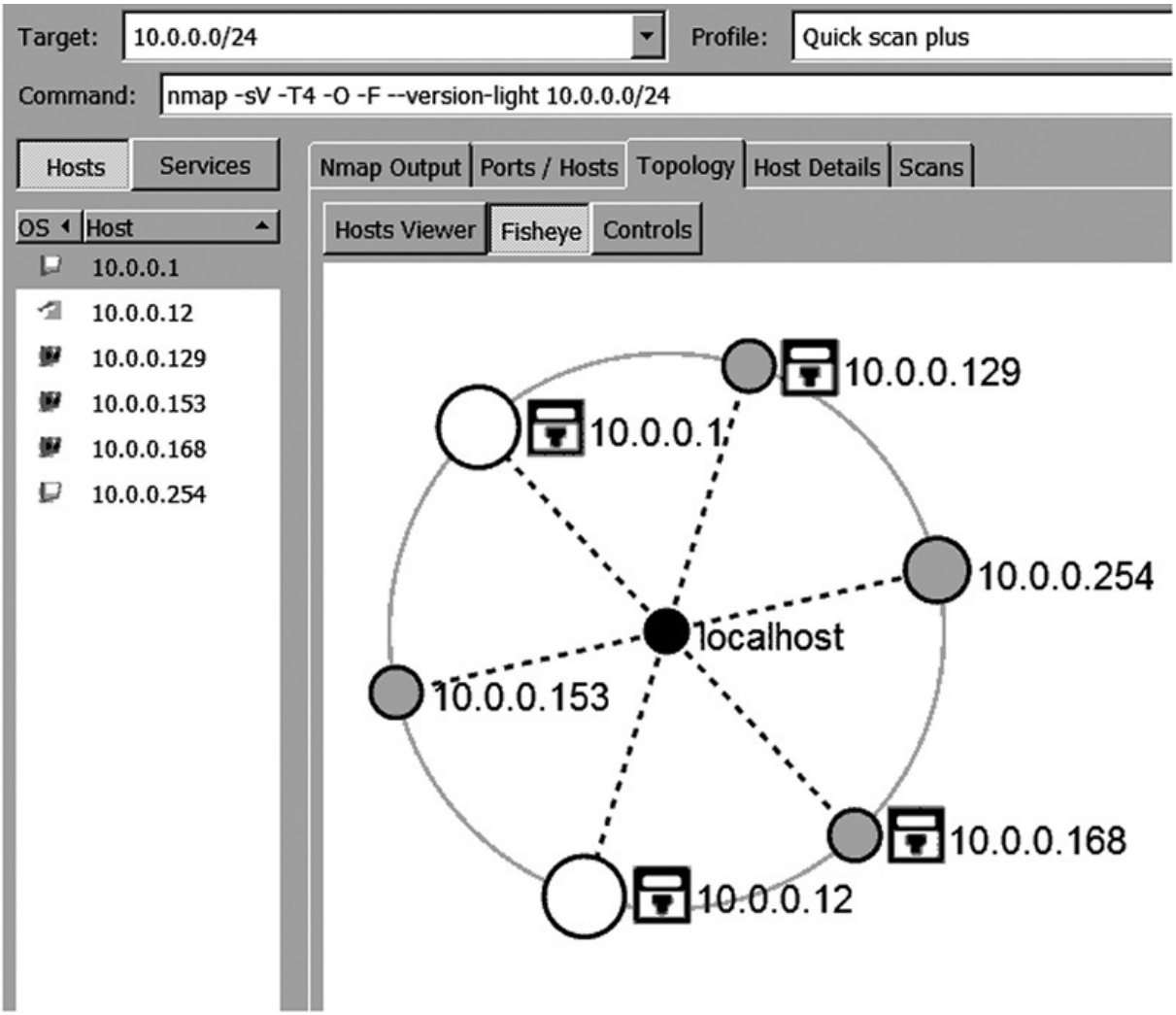

Рисунок 1-4. Представление топологии Zenmap по результатам сканирования подсети 10.0.0.0/24

После сбора все данные потребуется обработать, проанализировать и объединить. Перед сведением данных воедино полезно определить самый точный источник, а также выявить источники с уникальными и полезными сведениями, например временем, когда устройство наблюдалось в последний раз. Следует исследовать и любые несоответствия и расхождения. Среди них могут оказаться пропавшие из сети устройства, несанкционированные устройства в сети, а также странное поведение или соединения. Если выяснится, что сетевые сканеры не смогли проникнуть в некоторые анклавы или подсети из-за правил IP либо систем предотвращения вторжений (intrusion prevention system, IPS), подумайте о запросе изменений сети, которые позволят проводить более глубокое и всестороннее сканирование. Ключевым результатом этого этапа проекта становится выявление и определение местонахождения всех разрешённых и неразрешённых устройств, подключённых к сети, - это огромное достижение.

Оцените программные средства картографирования, способные автоматически принимать данные SNMP, результаты сканирования сети и уязвимостей, а также допускающие ручное редактирование для включения дополнительных данных. Выбранное средство должно создавать исчерпывающую, точную и подробную карту сети, отвечающую потребностям заинтересованных лиц. Выберите лучшее решение, которое справится с вашими данными и уложится в бюджет.

Создайте карту и испытайте её. Проверьте её полезность на совещаниях по управлению изменениями, при инцидентах безопасности, отказах сети и диагностике. Помогает ли она быстрее устранять неполадки и находить проблемы? Проверьте точность карты с помощью `traceroute` и `tcpdump` на интерфейсах. Для проверки посредством `traceroute` запустите трассировку внутренних и внешних маршрутов из разных точек сети и убедитесь, что промежуточные точки - маршрутизаторы - присутствуют на карте, а движение через них логически соответствует карте. Пример трассировки приведён на рисунке 1-5.

```
C:\Users\benm>tracert -4 example.com

Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  10.0.0.1
  2    18 ms    10 ms     9 ms  96.120.106.61
  3     9 ms    10 ms     9 ms  xe-5-2-0-sur01.newmexiconw.dc.bad.comcast.net [162.151.98.145]
  4    18 ms    10 ms    11 ms  ge-1-21-ur02.waldorf.md.bad.comcast.net [68.87.135.97]
  5    41 ms    11 ms    10 ms  ae-13-ar01.capitolhghts.md.bad.comcast.net [68.87.168.61]
  6    13 ms    14 ms    14 ms  be-33657-cr02.ashburn.va.ibone.comcast.net [68.86.90.57]
  7    11 ms    12 ms    12 ms  be-10142-pe01.ashburn.va.ibone.comcast.net [68.86.86.34]
  8    12 ms    12 ms    12 ms  as27471-2-c.350ecermak.il.ibone.comcast.net [173.167.57.50]
  9    11 ms    11 ms    13 ms  152.195.64.133
 10    11 ms    10 ms    11 ms  93.184.216.34

Trace complete.

C:\Users\benm>
```

Рисунок 1-5. Трассировка маршрута к example.com в Windows

Посмотрите, как вашей картой смогут воспользоваться красная и синяя команды. Соберите отзывы и повторите картографирование, поставив цель создать ещё более качественную карту за меньшее время.

> **Упражнение «Теория замка».** Представьте, что вы правитель средневекового замка, внутри которого находятся ценные сведения, сокровища и люди. Вы получаете достоверные разведывательные данные об угрозе: ниндзя тщательно картографировал ваш замок и окружающую местность, хотя неясно, было ли это частью активного выбора цели или всего лишь пассивной разведкой. Вы не знаете, как выглядит его карта и насколько она подробна. Единственная имеющаяся у вас карта замка - архитектурный проект, использованный при первоначальном строительстве; он предназначался строителям, а не другим пользователям, и с тех пор устарел.
>
> Что, вероятнее всего, есть на карте ниндзя, но отсутствует на вашей? Что ниндзя может знать о вашем замке такого, чего не знаете вы, и как эти сведения можно использовать для проникновения? Кому в ваших владениях пригодился бы доступ к карте ниндзя? Кому вы доверили бы нанести замок на карту так же, как это сделал ниндзя, чтобы увидеть замок его глазами?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, каждая рекомендация сопровождается применимой мерой безопасности из стандарта NIST 800-53; оценивать её следует с учётом карт.

1. Назначьте ответственных за документирование карты сети. Внедрите политики и процедуры, координирующие обновление карты между командами. [CM-1: Configuration Management Policy and Procedures; CM-3: Configuration Change Control | (4) Security Representative; CM-9: Configuration Management Plan]
2. Чтобы установить исходное состояние, задокументируйте конфигурацию топологии, архитектуры, логического размещения и информационных систем сети. [CM-2: Baseline Configuration]
3. Включите выявление недостатков, например неточностей карты, и их устранение, например исправление уязвимостей, присущих сетевой архитектуре, в процесс картографирования сети. [SI-2: Flaw Remediation]

Разбор

В этой главе вы познакомились с целями картографирования синоби, стандартами и приёмами составления карт, а также получили общее представление о современных методах и технологиях картографирования сетей. Размышления о важности карт сетей, о создании хороших карт и о том, как атакующие собирают разведывательные сведения о вашей системе, могли пробудить ваше воображение; возможно, вы придумали новые источники данных или приёмы для картографирования собственной и чужих сетей.

В следующей главе у вас появится возможность воспользоваться картой сети как разновидностью диаграммы потоков данных (data flow diagram, DFD), чтобы выполнить моделирование угроз. Иными словами, вы определите участки сети, которые субъект угрозы, вероятнее всего, атакует либо использует для обхода защиты и проникновения. Я расскажу о новом приёме защиты ниндзя - «охране», с помощью которого можно защищать эти слабые места сети.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), p. 55.
[2] [назад] Стихотворения 6-10 и 24.
[3] [назад] Cummins and Minami, «Shochi I - A Guideline for Commanders I», in *The Book of Ninja*, pp. 55-65.
[4] [назад] Gordon Lyon, «Nmap: The Network Mapper», Insecure.org, обновлено 18 марта 2018 г., https://nmap.org.
[5] [назад] Cummins and Minami, *The Book of Ninja*, p. 168.
[6] [назад] Cummins and Minami, *The Book of Ninja*, p. 148.

Глава 2. Особая охрана

> Даже замки с мощными укреплениями следует охранять, уделяя особое внимание углублённым углам.

> Проникая в замок или лагерь, синоби должен помнить о направлениях, которые защищены естественными преградами и труднодоступны, о лесах и слепых зонах.
>
> - «Ёсимори хякусю», стихотворение 10

Исторически синоби были искусными мастерами проникновения. В древних свитках рассказывается, как быстро находить слабые места во вражеских укреплениях и безжалостно ими пользоваться. Свитки также подчёркивают: при сооружении собственной обороны синоби должны мыслить на более высоком уровне и творчески применять свои знания. «Бансэнсюкай» советует командирам, которым поручено защищать лагерь или замок, выявлять, осматривать и особенно тщательно охранять те места, через которые синоби, вероятнее всего, попытаются проникнуть: углублённые углы каменных замковых стен, места сброса отходов, водопроводные трубы, расположенные поблизости леса или кустарник.[1]

Что представляют собой векторы атаки

Будем считать стену замка поверхностью атаки, а слабые места в этой стене - например, водопроводную трубу или неудачно уложенные камни, за которые можно цепляться ногами, - векторами атаки. Термином *поверхность атаки* обозначают всё программное обеспечение, сети и системы, на которые противник получает возможность напасть. Любая точка поверхности атаки может стать вектором атаки, то есть средством, с помощью которого атакующий получает доступ. В кибербезопасности всегда рекомендуется сокращать поверхность атаки. Однако, хотя уменьшение площади замка сократило бы поверхность атаки, которую требуется защищать, оно не снизило бы ущерб, который способен причинить противник, и не помешало бы ему воспользоваться конкретным вектором атаки. И всё же сокращение поверхности атаки может облегчить охрану цели.

В томе «Бансэнсюкай», посвящённом скрытому проникновению, перечислены благонамеренные оборонительные приёмы, оружие и подходы к мышлению, которые на деле способны подвергнуть лагерь опасности. Свиток настоятельно призывает командиров задумываться, как всё, что есть в их окружении, может быть использовано против них. Например, лазутчикам предписывается искать *синоби-гаэси* - шипы, расставленные вокруг вражеского лагеря, чтобы отпугивать возможных нападающих.[2] Поскольку защитники размещали эти шипы там, где сами видели уязвимость, их присутствие сообщало вражеским синоби, в каких местах оборона недостаточна: защитники буквально объявляли о собственной незащищённости. Синоби знали, что могут убрать шипы - это было сравнительно легко, поскольку их почти всегда устанавливали позднее, как дополнительную меру, - и пройти через самое слабое место в периметре цели.[3]

Наглядный пример подобной защиты, «прикрученной» задним числом, можно найти в PowerShell для Microsoft Windows. Множество средств безопасности, которые с каждой новой версией PowerShell надстраиваются над платформой .NET, не устраняют коренные недостатки продукта и фактически позволили субъектам угроз создать целый арсенал инструментов и оружия для проникновения в системы с поддержкой PowerShell. Это превосходный пример для любого исследователя безопасности, желающего подробнее изучить *синоби-гаэси*.

Сохранившиеся до наших дней старинные японские замки обычно не усеяны шипами, зато водопроводные трубы в них слишком узки, чтобы по ним мог пролезть человек, пространство вдоль периметра расчищено от растительности, а во внешних стенах нет углублённых углов. Всё это позволяет предположить, что императоры, следуя подсказкам синоби, со временем старались устранять подобные уязвимости. Однако, хотя в идеале слабые места следует устранять, чтобы их не приходилось охранять, это возможно не всегда.

В этой главе мы обсудим понятие охраны и предлагаемое для неё место среди пяти функций кибербезопасности. Затем с помощью моделирования угроз разберём, как выявлять уязвимые участки, которые, возможно, потребуется охранять.

Понятие охраны

Охрана - это осуществление защитного контроля над ресурсами посредством наблюдения за средой, обнаружения угроз и принятия предупредительных мер. Например, владелец замка выявляет слабое место - довольно широкую водосточную трубу в замковой стене. Он сохраняет трубу, выполняющую важную функцию отвода воды, но требует, чтобы рядом стоял стражник и не позволял нападающим воспользоваться трубой как путём для проникновения.

Как правило, организации не посвящают сотрудников службы кибербезопасности в сведения о слабых системах, слепых зонах сети или уязвимых векторах атаки, которые следует охранять особенно тщательно. Некоторые организации считают, что обнаружение недостатков защиты в сети целиком лежит на сотрудниках кибербезопасности. Многие заинтересованные лица изначально не выявляют эти векторы атаки; а если готового коммерческого решения нет или общепринятую контрмеру невозможно легко применить, они попросту игнорируют слабые места и надеются, что ими никто не воспользуется.

В отдельных случаях руководство запрещает специалистам по безопасности даже базовое журналирование, сканирование или установку исправлений в устаревших системах, опасаясь, что любое воздействие нарушит работу организации. В организациях с более развитой внутренней политикой угрозу нередко отказываются признавать обоснованной, пока она не выявлена в ходе формального документированного процесса. Представьте, что вы заметили отсутствие западной стены замка, доложили королю об этой очевидной уязвимости, а тот отверг ваши опасения, поскольку его стражники не упомянули её в официальных отчётах.

Охрана в составе системы кибербезопасности

Система кибербезопасности Национального института стандартов и технологий США (National Institute of Standards and Technology, NIST)[4] призвана предотвращать эти распространённые ошибки и повышать устойчивость организаций к киберугрозам посредством пяти основных функций кибербезопасности: выявления, защиты, обнаружения, реагирования и восстановления. Эти функции помогают выявлять уязвимости в сетях и системах с помощью распространённых инструментов и процессов информационной безопасности.

Например, большинство организаций начинает выявлять слабые места со сканирования систем в своей сети на уязвимости либо сканирования приложений - это функция выявления. Подобное сканирование эффективно и надёжно обнаруживает очевидные проблемы безопасности: программное обеспечение без исправлений, действующие учётные записи с пустыми паролями, стандартные заводские учётные данные, непараметризованный ввод и открытые в Интернет порты

SSH. Далее следует функция защиты. Обнаружив незащищённую систему, сканер документирует проблему, после чего сотрудники службы безопасности исправляют или смягчают уязвимость с помощью программных исправлений, изменений конфигурации либо долгосрочных преобразований архитектуры, системы безопасности или программного обеспечения.

Если сотрудники службы безопасности не могут защитить систему, которая была выявлена как вектор атаки, я считаю, что её следует охранять с помощью мер человеческого контроля. Однако функция охраны в системе NIST отсутствует. Вместо неё мы сразу переходим к функции обнаружения: сотрудники службы безопасности пытаются выявить противника, наблюдая за аномальными событиями и исследуя их. И только обнаружив проникновение, они приступают к функции реагирования: локализуют угрозу, нейтрализуют её и составляют отчёт.

Последней идёт функция восстановления: системы и данные возвращают в рабочее состояние и одновременно повышают их способность противостоять будущим атакам.

Хотя эти защитные меры необходимы для надёжной системы безопасности, они представляют собой функции предупреждения, защиты или реагирования. В индустрии кибербезопасности понятие охраны - использование человеческого контроля и защиты - редко применяется к информационным системам, поскольку человек физически не способен вручную исследовать и одобрять каждое письмо, веб-страницу, файл или пакет, покидающие среду либо поступающие в неё, как привратник мог бы проверять людей и посылки при входе в здание.

Например, компьютеры с сетевыми соединениями пропускной способностью 1 Гбит способны обрабатывать более 100 000 пакетов в секунду - намного больше, чем может проверить любой человек. Вместо людей-охранников защитники либо в значительной степени полагаются на автоматизированные средства безопасности, либо просто принимают или игнорируют риск как неизбежную часть ведения дел. Тем не менее охрана может быть осуществима и в современной цифровой сети, если размещать стражей лишь там, где требуются особая забота и внимание, например возле наиболее вероятных векторов атаки. Именно поэтому будет полезно выявить такие участки организации с помощью моделирования угроз.

Моделирование угроз

Ближе всего к охране в кибербезопасности находится охота за угрозами, заключающаяся в энергичном поиске признаков проникновения в журналах, криминалистических данных и других наблюдаемых свидетельствах. Охотой за угрозами занимаются немногие организации, но даже в тех, где она ведётся, задача охотника - обнаруживать, а не охранять.

Тем не менее защитникам киберсреды важно выходить за рамки традиционной системы, постоянно представлять новые способы нападения на сети и информационные системы и внедрять необходимую защиту. Для этого они могут применять моделирование угроз, чтобы устанавливать средства управления потоками информации и проектировать защитные меры против угроз, а не просто реагировать на них.

Моделирование угроз, которым обычно занимаются лишь организации с высоким уровнем зрелости в кибербезопасности, включает документирование диаграммы потоков данных (data flow diagram, DFD), описывающей потоки данных и процессы внутри систем. DFD обычно оформляют как разновидность блок-схемы, но приблизительно представить её способна и подробная карта сети. DFD служит инструментом структурированного анализа поверхности атаки и позволяет продумывать сценарии нападения в пределах документированных информационных систем. Для этого не нужны ни сканирование уязвимостей, ни доказательство реалистичности сценария красной командой, ни подтверждение со стороны системы обеспечения соответствия; организации также не

обязаны ждать инцидента безопасности, который докажет обоснованность модели угрозы, прежде чем приступить к охране от уязвимости.

Понимание того, что в современной киберсреде соответствует «углублённым углам каменных замковых стен, местам сброса отходов, водопроводным трубам, расположенным поблизости лесам или кустарнику», поможет выявить векторы атаки, нуждающиеся в особой охране.

Рассмотрим пример. В рамках ночных обязанностей охранник дёргает ручку каждой двери в офисе, проверяя, заперта ли она. Обнаружив незапертую дверь, он запирает её, убирает ключи в безопасное место и оформляет заявку об инциденте безопасности.

Позднее выясняется, что инцидент безопасности произошёл из-за копирования или кражи ключей. Поэтому организация добавляет к дверям средство аутентификации второго уровня, например цифровую клавиатуру или считыватель пропусков, меняет замки и выдаёт новые ключи. Новые предупредительные меры удовлетворяют аудиторов по соответствию требованиям, и заявку о незапертых дверях закрывают. Директор по информационной безопасности (chief information security officer, CISO) даже нанимает красную команду для узконаправленного физического испытания новых дверных запоров на проникновение, и команда подтверждает, что усиленные меры безопасности не позволили ей получить доступ.

Однако при моделировании угроз мы обнаруживаем, что подвижные потолочные плиты можно отодвинуть и перебраться через офисную стену, полностью обойдя новые меры безопасности. В противодействие этому можно установить средства контроля - камеры наблюдения или датчики движения в пространстве над подвесным потолком - либо смонтировать сплошные полы и потолки, устойчивые к прокладыванию лазов. Можно даже нанять и обучить охранников искать следы сдвинутых потолочных плит, осыпавшиеся на пол частицы потолочного материала или отпечатки ног на стенах. Для охраны от этой угрозы стражей пришлось бы разместить внутри комнаты или в пространстве над потолком, наделив их полномочиями и средствами защиты помещения от нарушителей.

Реализовать такие контрмеры едва ли возможно: за одно только предложение вас могут со смехом выставить из кабинета руководителя. Нетрудно понять, почему организации скорее готовы принять или проигнорировать некоторые угрозы, чем пытаться их отразить, и, вероятно, именно поэтому в системе кибербезопасности NIST нет функции охраны. Однако такой образ мыслей, сосредоточенный на охране, способен укрепить безопасность информационных систем и сетей, если он вдумчиво опирается на подробное моделирование угроз и тщательно, творчески и целенаправленно претворяется в жизнь.

Пример сценария, подходящего для внедрения функции охраны, связан с промежуточными узлами доступа. Такие узлы соединяют две или более сетевые области, позволяя администраторам удалённо войти в промежуточный узел из одной сети, а затем «перепрыгнуть» в другую и получить к ней доступ. Традиционная система кибербезопасности рекомендует усиливать защиту промежуточных узлов: исправлять все известные уязвимости, ограничивать доступ различными правилами межсетевых экранов и отслеживать в журналах аудита аномальные события, например несанкционированный доступ. Однако такие технические средства нередко атакуют или обходят. Страж, напротив, мог бы физически отсоединять кабель внутренней сети от другой сети и подключать его напрямую лишь после того, как удостоверится у администратора, что тому разрешено удалённо выполнять команды в этих системах. Страж мог бы также в реальном времени активно следить за действиями на компьютере и принудительно завершать сеанс всякий раз, когда заметит вредоносные или несанкционированные действия. Подобная реализация функции охраны может потребовать нанять человека, который будет сидеть в центре обработки данных и защищать как физический, так и удалённый доступ к этим критически важным системам.

Поиск возможных векторов атаки с помощью моделирования угроз

Основные шаги выявления векторов атаки состоят в соблюдении правил моделирования угроз, начиная с создания DFD. После того как по DFD выявлены возможные векторы атаки, свитки синоби рекомендуют исследовать их и определить, какие технические средства безопасности можно внедрить для защиты. Затем в качестве последнего средства эти участки следует дополнительно защищать стражами. Для создания DFD можно воспользоваться картой сети из предыдущей главы или применить её как приблизительную замену.

1. **Смоделируйте информационные системы.** Создайте точную DFD с помощью владельцев и специалистов по сетевым, защитным, программным, деловым и другим ИТ-системам организации. Необязательно применять унифицированный язык моделирования (Unified Modeling Language, UML) или другие сложные понятия: диаграмма должна всего лишь точно представлять ваши системы и находящиеся в них сведения. Учтите, что на построение схемы больших и сложных систем у целой команды легко может уйти более шести месяцев.
2. **Примените STRIDE и охрану.** STRIDE - разработанная Microsoft[5] методика моделирования угроз, описывающая возможные нарушения в информационной системе. Эта аббревиатура образована названиями способов, которыми атакующий способен нарушить шесть свойств системы:

   • Spoofing Identity (подмена личности) = Authentication (аутентификация);
   • Tampering with Data (искажение данных) = Integrity (целостность);
   • Repudiation/Deniability (отказ от совершённых действий) = Nonrepudiation (неотказуемость);
   • Information Disclosure (раскрытие информации) = Confidentiality (конфиденциальность);
   • Denial of Service (отказ в обслуживании) = Availability (доступность);
   • Elevation of Privilege (повышение привилегий) = Authorization (авторизация).

   Для применения STRIDE просмотрите DFD и в каждой точке ввода, обработки, вывода данных или иных потоков и правил выдвиньте предположение о том, как противник способен ей угрожать. Например, если система требует отпечаток большого пальца для проверки личности пользователя перед предоставлением доступа, подумайте, как злоумышленник мог бы подделать отпечаток и выдать себя за другого пользователя. Аналогичным образом можно рассмотреть способы изменения базы отпечатков с добавлением собственного либо сценарий, в котором атакующий выводит сканер отпечатков из строя и тем самым добивается несанкционированного доступа через более слабый процесс аутентификации.

   Освоив эту систему, вы сможете с её помощью оспаривать любые воображаемые модели угроз, которые неточно представляют ваши системы, и сценарии, не объясняющие, как правдоподобная угроза воздействует на конкретный компонент, поверхность или вектор. Для этого, возможно, понадобится приглашать на сеансы моделирования угроз технических специалистов в соответствующей предметной области.

   Предположим, например, что на сеансе моделирования угроз организации сформулирован следующий сценарий: «Угроза вредоносного ПО нарушает целостность внутренних баз данных».

Эта угроза смоделирована неправильно. Помимо прочих важнейших сведений, сценарий не объясняет, как вредоносное ПО может быть доставлено и установлено. Не описано и то, каким образом оно нарушит целостность базы данных: зашифрует, удалит или испортит данные? Сценарий не указывает, какие векторы позволяют угрозе воздействовать на систему, не учитывает существующие потоки информации и средства контроля и не предлагает реалистичных контрмер. Если, например, мы определили, что наиболее правдоподобный способ заразить внутреннюю деловую базу данных вредоносным ПО - подключить вредоносный USB-накопитель, службе безопасности, возможно, потребуется разработать правила использования USB-накопителей сотрудниками или установить камеры для наблюдения за доступом к USB-портам. Организация может решить предоставить службе безопасности возможность включать и отключать USB, предписывать, какие накопители разрешено подключать через USB, управлять потоком и направлением передачи информации через USB-порты, исследовать файлы на USB-накопителях перед предоставлением доступа запросившему его лицу, ограничивать доступ аппаратными или программными замками или даже залить USB-порты термоклеем. Подобные меры, выработанные в результате тщательного моделирования угроз, позволяют специалистам по безопасности особенно внимательно охранять от конкретных угроз, вместо того чтобы принимать риск или ограничиваться функциями защиты и обнаружения.

3. **Не выставляйте напоказ защиту, добавленную задним числом.** Моделирование угроз - итеративный, бесконечный процесс оценки новых угроз и разработки защитных контрмер. Торопясь защитить системы, избегайте средств безопасности типа *синоби-гаэси* - оборонительных мер, способных дать обратный результат, привлекая внимание к уязвимым участкам. Зачастую из-за ограничений по времени, ресурсам или эксплуатации удаётся принять лишь половинчатые меры, которые целеустремлённый и искушённый субъект угроз способен преодолеть. Например, термоклей из USB-порта можно удалить изопропиловым спиртом. По возможности оценивайте жизнеспособность подхода, при котором защита изначально ставится во главу угла.

   В примере с угрозой USB устройство взаимодействует с уровнем аппаратных абстракций (hardware abstraction layer, HAL), расположенным ниже ядра ОС. Его невозможно полностью защитить или смягчить угрозу средствами программного обеспечения и политик, поскольку те существуют выше ядра и могут быть обойдены. Поэтому более полным решением может стать такая конфигурация системной платы и корпуса, где USB-портов вообще нет. Напротив, термоклей в USB-порте сообщает целеустремлённым субъектам угроз, что безопасность USB не была обеспечена надлежащим образом, и, если им удастся вытащить клей, этот порт, вероятно, станет успешным вектором атаки - подобно тому как в древности синоби вытаскивали шипы, приделанные к трубам и стенам.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка, внутри которого находятся ценные ресурсы. Вы получаете достоверные разведывательные сведения о том, что ниндзя намерен проникнуть в замок и поджечь запасы продовольствия в подземелье. У подземелья несколько точек входа и выхода, через которые служащие переносят еду, свободно перемещаясь без наблюдения.

Подумайте, какие меры могли бы принять стражники, чтобы защитить продовольствие от пожара в подвале. Как можно изменить расстановку людей, чтобы контролировать взаимодействие с продовольствием и уберечь его от повреждения? Какие меры позволили бы стражникам быстро заметить пожар в подвале, сообщить о нём и отреагировать? Как стражники могли бы обнаружить ниндзя, проникающего в подвал, и какие архитектурные изменения позволили бы устранить слепые зоны, через которые можно добраться до продовольствия?

Учтите: хотя разумно иметь запас продовольствия в другом месте либо хранить еду в огнестойком материале, в этом упражнении следует подумать, как стражники могут контролировать и защищать продовольствие, а не устранять непосредственно угрозу пожара.

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, каждая рекомендация сопровождается применимой мерой безопасности из стандарта NIST 800-53; оценивать её следует с точки зрения особой охраны.

1. Изучите результаты работы аудиторов, оценок красной команды, сканирования уязвимостей и отчётов об инцидентах, чтобы найти уязвимости среды, которые нельзя легко исправить или смягчить средствами контроля, то есть требующие особой охраны. [CA-2: Security Assessments; CA-8: Penetration Testing; IR-6: Incident Reporting | (2) Vulnerabilities Related to Incidents; RA-5: Vulnerability Scanning]
2. Проведите моделирование угроз для своей среды, чтобы выявить уязвимости. Затем определите, какие из них можно устранить при проектировании среды. Исследуйте понятие функций охраны и примените эти средства контроля к угрозам, которые невозможно легко удалить. [SA-8: Security Engineering Principles; SA-14: Criticality Analysis; SA-15: Development Process, Standards, and Tools | (4) Threat Modeling/Vulnerability Analysis; SA-17: Developer Security Architecture and Design]
3. Чтобы сдерживать угрозы, защищаться от них и обеспечивать быстрое реагирование, наймите специалистов по безопасности, которые будут в реальном времени выполнять роль стражей, и включите их в уязвимые участки деловых операций. [IR-10: Integrated Information Security Analysis Team]

Разбор

Эта глава помогла вам задуматься о тех местах сетевой среды, которые противник, вероятнее всего, выберет для проникновения. Вы также познакомились с понятием охраны, предусматривающей непосредственное взаимодействие людей с информационными системами и процессами. Возможно, вы воспользовались картой сети из предыдущей главы или создали собственную диаграмму потоков данных (DFD), представляющую вашу среду, чтобы выявить вероятные векторы атаки и возможные угрозы STRIDE, которые можно смягчить с помощью стражей.

В следующей главе мы исследуем применявшуюся древними ниндзя «ксенофобную» концепцию безопасности, которая способна помешать противникам найти в вашей среде хоть какую-либо общую основу или точку опоры, чтобы даже приступить к реализации своих векторов атаки.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), p. 93.
[2] [назад] Cummins and Minami, *The Book of Ninja*, p. 183.
[3] [назад] Cummins and Minami, *The Book of Ninja*, p. 146.
[4] [назад] *Cybersecurity Framework*, National Institute of Standards and Technology, обновлено в сентябре 2018 г., https://www.nist.gov/cyberframework/.
[5] [назад] Adam Shostack, «STRIDE chart», Microsoft Secure (блог), Microsoft Corporation, 11 сентября 2007 г., https://bit.ly/39aeOWy.

Глава 3. Ксенофобная безопасность

> Если без особых раздумий принимать чужаков, вражеский синоби может явиться под видом незнакомца и начать собирать сведения изнутри.

> Если к караульному помещению приблизятся нищие или отверженные, обойдитесь с ними сурово и прогоните.
>
> - «Ёсимори хякусю», стихотворение 91

В этой главе мы исследуем понятие ксенофобной безопасности - защиты, основанной на недоверии к посторонним, - и узнаем, как её можно применять в виде области защиты с антиполномочиями. Чтобы пояснить эту идею, рассмотрим враждебную среду, в которой приходилось действовать синоби.

Синоби, пытавшиеся проникнуть в деревни и открыто собирать сведения, сталкивались с повсеместной проблемой - всепроникающей ксенофобией средневековых японцев. Изоляция деревень породила уникальные диалекты, причёски, одежду и другие обычаи, превратив каждую общину в самостоятельную социальную экосистему.[1] Из-за малочисленности населения в таких отдалённых местах обычно все знали друг друга, и посторонний явно не вписывался в окружение.[2]

К синоби как к чужакам неизменно относились с подозрением и следили за ними. Они не могли свободно передвигаться по городу, им часто не позволяли снимать комнаты и покупать еду. Разумеется, жители не стали бы делиться с ними сведениями. Ксенофобия общины придавала синоби статус субъекта с антиполномочиями.

Что представляют собой антиполномочия

Чтобы понять значение антиполномочий, сначала рассмотрим понятие полномочий, под которыми в кибербезопасности понимают разрешения пользователя на выполнение действий, например на чтение или удаление файла. Современные компьютерные системы имеют кольцевую архитектуру с разными уровнями полномочий:

• `ring4` - уровень по умолчанию (без полномочий);
• `ring3` - обычный пользователь (минимальные полномочия);
• `ring2` - суперпользователь (администратор);
• `ring1` - root (повышенные полномочия);
• `ring0` - ядро (система).

Например, простой житель деревни с минимальными полномочиями или кошка без полномочий могут покинуть деревню когда пожелают. Деревенский староста с повышенными полномочиями обладает дополнительным разрешением запирать ворота по своему усмотрению. Однако иностранцу, заподозренному в недобрых намерениях и наделённому антиполномочиями, может быть разрешено меньше, чем бродячей кошке без полномочий, поэтому ему не позволят покинуть деревню.

Различие между статусом субъекта с антиполномочиями и субъекта без полномочий существенно. В некоторых компьютерных системах такие действия, как выход из системы, считаются не требующими полномочий и по умолчанию доступны субъектам на всех кольцах. Не заслуживающие доверия процессы и пользователи способны применять эти стандартные возможности без полномочий, чтобы совершать более вредоносные действия или достаточно свободно действовать

ради достижения более сложных целей. Если, напротив, запретить процессу с антиполномочиями выходить из системы, он не сможет удалить историю своего сеанса или следы собственного существования. Представьте, что компьютерные системы могли бы внедрить средство безопасности `ring5` - кольцо антиполномочий. В примере с деревней подозреваемого синоби можно было бы принудительно обыскивать и допрашивать, прежде чем разрешить ему уйти. Так деревня могла бы ловить воров и шпионов. Более того, делая работу лазутчиков гораздо опаснее и дороже, деревни, несомненно, сдерживали враждебную деятельность.

Чтобы проникнуть в такую ксенофобную деревню, синоби прежде всего должен был запомнить и отрепетировать целый ряд характерных для данной культуры маскировок, в совершенстве освоив местную манеру одеваться, диалект, способы ухода за внешностью, денежные обычаи и общественные нравы.

Но даже овладев культурной маскировкой, синоби нуждался в убедительной причине находиться в деревне; обычно она была связана с работой. В «Нинпидэн» рассказывается, как синоби мог присвоить себе типичную легенду прикрытия, представившись монахом в духовном странствии, торговцем, нищим или даже самураем, путешествующим по приказу своего господина. Хотя жители тоже распознавали в самурае чужака, он не вызывал такого же недоверия, как возможный беглец или разбойник.

Находясь под прикрытием среди людей той же профессии, общественного слоя или касты, синоби советовали показывать достаточно знаний, чтобы выглядеть убедительным представителем профессии, но при этом притворяться глупым и нуждающимся в помощи при выполнении обычных дел. Притворное невежество вводило цель в заблуждение относительно истинного ума синоби и одновременно льстило её собственному интеллекту, заставляя её потерять бдительность и охотно делиться сведениями. В «Нинпидэн» перечислены конкретные цели, расположение которых синоби следовало завоёвывать подобными приёмами: местные помощники чиновников, магистраты, врачи, монахи и другие люди, которые могли служить в присутствии местного господина или представителя власти. Обычно эти цели располагали ценными для задания сведениями.[3]

Обратите внимание: общественная иерархия средневековой японской деревни напоминает структуру колец полномочий в современных компьютерных системах или даже многоуровневую сегментацию компьютерных сетей, где внешним уровням, например DMZ, доверяют меньше всего. Аналогичным образом обычные жители деревни с минимальными полномочиями не могли бы взаимодействовать с господином, находящимся в центре - на уровне `ring0`.

Способ, которым синоби определяли вероятные цели, можно перенести в контекст кибербезопасности. Подобно тому как синоби выбирали тех, кто метафорически находился ближе к `ring0` или имел к нему доступ, современные субъекты угроз выбирают привилегированные классы систем и пользователей. Поэтому защитникам следует задуматься, что в их системах соответствует таким высокопоставленным людям, как монахи и магистраты. Кроме того, нужно представить, какими маскировками современный субъект угроз может воспользоваться, чтобы приблизиться к более привилегированным системам и пользователям.

Проблема совместимости и универсальных стандартов

Осознают они это или нет, совместимость для потребителей технологий имеет первостепенное значение: люди ожидают, что их устройства, приложения, системы и программы будут безупречно работать с новыми и старыми версиями, на разных платформах, а также взаимозаменяемо с изделиями других производителей и моделей. Международная организация по стандартизации (International Organization for Standardization, ISO), Международная электротехническая комиссия (International Electrotechnical Commission, IEC), Инженерный совет Интернета (Internet Engineering Task Force, IETF), Общество Интернета (Internet Society, ISOC) и другие руководящие организации установили широко признанные стандарты проектирования, работы и интеграции технологий.

Благодаря этим усилиям появилось множество стандартов ISO, документов Request for Comments (RFC) и других протоколов совместимости, которые сделали компьютеры доступнее, не говоря уже о том, что их стало легче создавать, администрировать, диагностировать, ремонтировать, программировать, объединять в сети и эксплуатировать. Яркий пример - представленный в 1995 году стандарт Plug and Play (PnP), предписывающий основной системе обнаруживать и принимать любое постороннее устройство, подключённое через USB, PCI, PCMCIA, PCIe, FireWire, Thunderbolt или иным способом, после чего автоматически его настраивать, загружать, устанавливать и подключать.

К сожалению, когда целями становятся обеспечение функциональности и поддержание работоспособности, безопасность почти никогда не бывает приоритетом. Более того, стандарт PnP, способствующий доверию к незнакомым сущностям и их принятию, был построен прямо противоположно стандарту ксенофобной безопасности средневековых японцев. Например, незнакомая система может подключиться к сети как посторонняя и запросить IP-адрес у протокола динамической настройки узлов (Dynamic Host Configuration Protocol, DHCP), спросить дорогу у локального маршрутизатора, запросить у авторитетного DNS-сервера имена других устройств и получить локальные сведения от протокола разрешения адресов (Address Resolution Protocol, ARP), протокола Server Message Block (SMB), протокола автоматического обнаружения веб-прокси (Web Proxy Auto Discovery, WPAD) и других протоколов, призванных облегчить обеспечение совместимости. Вы подключаете систему к сети, и та работает, демонстрируя именно то поведение, которого пользователи ожидают и желают. Однако сетевым протоколам индустрии кибербезопасности пошла бы на пользу большая «ксенофобия».

Для смягчения слабостей, возникающих из-за доступности типа PnP, были внедрены такие средства безопасности, как управление доступом к сети (Network Access Control, NAC) и объекты групповой политики (Group Policy Objects, GPO). На основных системах эти технологии защищают от потенциально вредоносных посторонних устройств, которые физически подключаются к внутренним сетям или системам.

NAC обычно жёстко ограничивает DHCP, назначая нераспознанным компьютерам гостевые IP-подсети или VLAN без полномочий. Это позволяет посторонним системам подключаться к Интернету для обычного доступа, но отделяет их от остальной доверенной сети. Такое поведение особенно желательно в конференц-залах и вестибюлях, чтобы внешние деловые партнёры и подрядчики могли работать, не подвергая сеть угрозам.

GPO на локальных узлах определяет, какие типы устройств - внешние жёсткие диски, USB-накопители, считыватели носителей и тому подобное - разрешено настраивать и устанавливать в системе. GPO даже способен вносить известные приложения организации в белый список и одновременно блокировать загрузку или установку всего незнакомого программного обеспечения на основной системе.

Однако эти средства безопасности представляют собой заметные исключения. От разъёмов Ethernet RJ45, использующих стандарты EIA/TIA-561 и Yost, до пакетных сетей на основе

стандартов IEEE 802 - и всего, что находится между ними, - большинство технологий строится на прозрачных, широко известных стандартных правилах, обеспечивающих быстрое и лёгкое применение в посторонних системах и сетях. Это делает технологии уязвимыми перед несанкционированными чужими системами, которые способны заниматься обнаружением сети, разведкой, перехватом и обменом данными.

Разработка уникальных особенностей среды

Уникальные свойства и особенности ресурсов ИТ помогут отличить принадлежащие вам ресурсы от чужих, которые могут проникнуть в среду, и даже защитят сеть от компрометации. Эти особенности можно заметить при осмотре или анализе, но сведения об их использовании не следует раскрывать публично, иначе контрмеры потеряют смысл. Большинство элементов современных ИТ-систем и программ допускают настройку, а изменения конфигурации фактически создают в ваших системах ксенофобную модель ИТ.

Недавно появившиеся коммерческие продукты, основанные на модели нулевого доверия, могут с помощью сочетания технических протоколов и недоверия сделать сеть или системы «ксенофобными» по отношению к незнакомым системам, программам и устройствам. Строгие белые списки и процедуры аутентификации и авторизации способны обеспечить похожий результат, но правильное решение должно ввести компьютерный аналог «диалектов» - настройки, обычаи и другие уникальные особенности, отклоняющиеся от универсальных компьютерных стандартов. Системам или устройствам, подключающимся к внутренней сети, пришлось бы пройти «идеологическую подготовку» в уникальной культуре организации, тогда как не прошедшие её серверы, компоненты, сетевые устройства и протоколы не доверяли бы незнакомому чужому агенту или отвергали его и предупреждали службу безопасности о его присутствии.

Проявив творческий и инженерный подход, подобные культурные компьютерные идентификаторы можно реализовать на любом уровне модели взаимодействия открытых систем (Open Systems Interconnection, OSI) - прикладном, представительском, сеансовом, транспортном, сетевом, канальном или физическом, - чтобы выявлять посторонних в сети и создавать дополнительный уровень защиты от противников. Будь то перестановка отдельных проводов в скрытых переходниках разъёмов RJ45, ожидание тайных рукопожатий (`SYN`, `SYN ACK`, `ACK-PUSH`) на уровне TCP/IP или применение зарезервированных битов в заголовке Ethernet, ксенофобное решение должно быть модульным, настраиваемым и уникальным для каждого экземпляра.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка, внутри которого находятся ценные ресурсы. Вы замечаете, что один местный рыбак, продающий рыбу вашим поварам, сохраняет её незнакомым способом и говорит со странным акцентом. На вопрос о необычном способе хранения он отвечает, что так рыба становится вкуснее. Его фамилия вам неизвестна.

По каким уникальным культурным признакам можно определить, является ли рыбак чужаком, и как провести такую проверку? Если рыбак утверждает, что родился в вашей деревне, но на время уезжал, как проверить его рассказ? Если проверить рассказ невозможно и вы подозреваете рыбака в шпионаже, как справиться с угрозой, не изгоняя и не казня, возможно, невиновного человека? Чтобы ответить на эти вопросы, нужно рассмотреть три сценария: рыбак действительно шпион; рыбак не шпион; намерения рыбака невозможно установить. Можно попросить партнёра сыграть странного рыбака, заранее и втайне выбрав одну из ролей, либо мысленно сыграть обе роли - и допрашивающего, и рыбака.

Это упражнение помогает глубоко задуматься об идентификации ресурсов с помощью ксенофобных моделей мышления, не погружаясь в техническое обсуждение компьютерных стандартов и инвентарного контроля. Хотя сценарий вымышлен, синоби, вероятно, иногда выдавали себя за рыбаков: такое прикрытие давало им повод часами слоняться поблизости, беседовать с местными жителями и вести разведку целей.

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, следующие рекомендации сопровождаются применимой мерой безопасности из стандарта NIST 800-53. Каждую из них следует оценивать с учётом понятия ксенофобной безопасности.

1. Исследуйте системы и определяйте, не отклоняются ли их характеристики или требования от ранее согласованной исходной конфигурации. [CM-2: Baseline Configuration]
2. Поддерживайте документацию обо всех информационных системах организации, чтобы легче выявлять посторонние системы в своей среде. [CM-8: Information System Inventory]
3. Используйте зашифрованные сведения, встроенные данные, особые типы данных или метаданные, например дополнение всех пакетов до определённого размера, как специальные идентификаторы при обмене данными, чтобы фильтры могли выявлять и ограничивать незнакомый трафик. [AC-4: Information Flow Enforcement; SA-4: Acquisition Process]
4. Ограничивайте внедрение ксенофобных идентификаторов и сведения о них вновь приобретёнными системами и устройствами. [SA-4: Acquisition Process]
5. Встройте ксенофобную проверку в качестве средства безопасности для идентификации и аутентификации систем и устройств организации. [IA-3: Device Identification and Authentication]

Разбор

В этой главе была описана исторически ксенофобная среда, в которой синоби приходилось вкладывать время и силы и применять сложные приёмы, чтобы под открытой маскировкой провести подготовительную разведку, прежде чем приступить к разведке самой цели. Вы узнали о понятии антиполномочий и о создании уникальных внутренних особенностей для выявления чужих ресурсов или пользователей в своей среде. Теперь вы, возможно, сумеете обнаружить ключевые ресурсы или людей, которые, вероятно, станут целями в вашей среде, хотя при прежнем моделировании угроз вы не рассматривали их как векторы атаки; после этого можно будет обратить внимание на системы и учётные записи, тесно взаимодействующие с такими возможными целями.

Однако, пользуясь правильными знаками отличия, одеждой, причёской, акцентом и другими особенностями, синоби могли пройти ксенофобные проверки, описанные в этой главе. Поэтому в следующей главе мы исследуем парный защитный приём, которым японские господа исторически выявляли синоби, способных иначе проникнуть в укрепление под чужим обликом.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), p. 41.
[2] [назад] Cummins and Minami, *Secret Traditions*, p. 48.
[3] [назад] Cummins and Minami, *Secret Traditions*, pp. 41-43, 47.

Глава 4. Проверка подлинности

> Хотя существуют древние способы опознавания по знакам, паролям и удостоверениям, враг сумеет проникнуть с похожими подделками, если не изобретать новые способы и не менять их.

> Во время ночной атаки враг может последовать за вами и затесаться в ряды союзников. Чтобы предотвратить это, заранее установите правило - способ опознавания своих.
>
> - «Ёсимори хякусю», стихотворение 27

Представьте следующий исторический сценарий. Отправив большой отряд в ночной набег, военачальник должен открыть ворота и впустить воинов обратно в укрепление. Ночные набеги помогали выигрывать сражения, но вместе с тем создавали возможность для контратаки. Вражеский синоби мог подделать или украсть форму нападавших, смешаться с их строем и вместе с ними вернуться на базу.

Для борьбы с этой угрозой командиры ввели одноразовый пароль, который участники набега должны были назвать, прежде чем пройти через ворота. Но эту защиту было легко преодолеть: переодетый синоби слышал пароль от стоящего перед ним в очереди солдата. Тогда командиры пробовали другие способы опознавания. Некоторые требовали, чтобы все участники набега носили нижнее бельё определённого тайного цвета, которое проверяли по возвращении, но находчивые синоби брали с собой или надевали бельё нескольких цветов, а во время осмотра выборочно отгибали его слои, показывая только нужный цвет. К другим контрмерам относились смена паролей по нескольку раз в день, которая всё равно не мешала синоби подслушать действующий пароль, и уникальные знаки различия или жетоны, которые синоби мог снять с тела погибшего после набега солдата.

Синоби относили эти приёмы либо к искусству открытой маскировки (*ё-нин*, буквально «светлый синоби»), либо к искусству скрытого проникновения (*ин-нин*, буквально «тёмный синоби»). В данном случае *открытая* означает, что человек находится на виду: например, атакующий мог надеть форму солдата-защитника, прекрасно понимая, что его увидят. *Скрытая*, напротив, подразумевает попытку остаться незамеченным, например с помощью камуфляжа или растворения в тенях. Многие из разнообразных приёмов открытой маскировки, описанных в «Бансэнсюкай», можно было применять и в нападении, и в защите. Синоби умели не только пользоваться ими для собственных атак, но и распознавать вражеских лазутчиков. Шпионы часто воспроизводили форму и гербы или подслушивали пароли, поэтому синоби разработали контрмеры опознавания, позволявшие отличать союзников от врагов.

Одним из таких приёмов были парные соответствия - проверочные сочетания слов для аутентификации союзников.[1] Этот приём также известен как отзыв и пароль или аутентификация «запрос-ответ». Парные соответствия применялись следующим образом. Неизвестный человек подходил к стражнику у замковых ворот и просил впустить его. Сначала стражник проверял, правильная ли на незнакомце форма и надлежащий ли герб он несёт. Если всё было верно, стражник произносил слово - например, «дерево». Если незнакомец не отвечал заранее условленным соответствием - «лес», - стражник понимал, что перед ним враг. Хотя «Бансэнсюкай» утверждает, что парные выражения должны быть достаточно простыми, чтобы их запомнили люди «низшего ранга», свиток не советует использовать очевидные ассоциации, которые может угадать противник. Поэтому вместо пары «снег» и «гора» лучше выбрать «снег» и «гора Фудзи». В свитке рекомендуется, чтобы синоби вместе с командирами каждые сто дней составляли сто новых пар соответствующих слов и каждый день применяли новую пару.[2] Столь большой набор позволял

часовому при необходимости случайным образом переходить от одной пары к другой при приближении каждого солдата, поэтому переодетый враг едва ли мог подслушать ответ именно на то проверочное слово, которое достанется ему.

Парные соответствия использовали для выявления возможных лазутчиков. Если незнакомец отвечал неправильно, его быстро задерживали, допрашивали и, возможно, убивали. Понимая последствия, «Бансэнсюкай» советует синоби, пытающемуся проникнуть во вражеский лагерь, принять внешность, манеры и речь неряшливого солдата низкого сословия. Тогда, если его попросят ответить на неизвестную парную проверку, он сможет убедительно сослаться на невежество.[3] Некоторые читатели могли заметить, что их финансовые учреждения начали внедрять соответствующие пары слов или изображений для сетевой аутентификации, но следует учитывать: такие сайты не требуют ста разных пар и обновляют их редко, если вообще обновляют. Небольшой набор неизменных пар позволяет противнику подсмотреть их все, а затем совершать несанкционированные действия с помощью украденных ответов аутентификации.

Эти исторические примеры подчёркивают, как трудно защищать аутентификацию от развитого и динамичного противника. В этой главе мы вкратце поговорим о сложности доказательства личности и о различных факторах, с помощью которых обеспечение информации (information assurance, IA) аутентифицирует человека. Я упомяну некоторые приёмы, которыми современные субъекты киберугроз расстраивают самые старательные попытки допустить только нужных людей, и укажу сходные приёмы синоби, показывающие, почему аутентификация останется сложной задачей в обозримом будущем. Я также расскажу читателям, как применять приёмы аутентификации синоби в современных приложениях. Общая цель главы - помочь понять основные вопросы, связанные с этой проблемой опознавания, и не заблудиться в огромной области знаний, в которую превратились аутентификация и криптография.

Что представляет собой аутентификация

Аутентификация - это процесс подтверждения личности пользователя перед предоставлением доступа к информационным системам, данным, сетям, физическим территориям и другим ресурсам. В процессе аутентификации личность подтверждается запросом чего-либо, что пользователь знает, имеет или чем является. Например, аутентификатор может запросить пароль - то, что пользователь знает; жетон - то, что у него есть; или биометрический признак - то, чем он является. В зависимости от необходимого уровня защиты организации требуют однофакторную, двухфакторную или многофакторную аутентификацию.

Зрелые организации могут также применять строгую аутентификацию, использующую несколько уровней многофакторных учётных данных. Например, на первом этапе строгой аутентификации могут потребоваться имя пользователя, пароль и отпечаток пальца, а на втором - жетон и одноразовый код, отправленный по SMS. Специалисты отрасли всё чаще задумываются о возможности четвёртого фактора, например доверенного сотрудника организации, который подтверждал бы личность пользователя. Любопытно, что сценарий синоби с парными соответствиями начинается именно с этой проверки: к проверочному слову переходят лишь тогда, когда никто из присутствующих не может подтвердить личность незнакомца.

Отказ аутентификации - критический недостаток безопасности. С аутентифицированной личностью пользователя связаны разрешения, позволяющие выполнять определённые, нередко привилегированные действия. Противник, успешно присоединившийся к аутентифицированному соединению законного пользователя, получает свободный доступ к его ресурсам и может вести вредоносную деятельность в информационных системах, данных и сетях.

К сожалению, процесс аутентификации несовершенен. Несмотря на множество мер кибераутентификации, сейчас невозможно с полной уверенностью проверить личность пользователя или процесса, поскольку почти любую существующую проверку можно подделать - то есть воспользоваться ложными данными, чтобы выдать себя за другую сущность, - или скомпрометировать. Противники применяют многочисленные приёмы для кражи паролей, перехвата жетонов, копирования хешей или билетов аутентификации и подделки биометрических признаков. Получив несанкционированный доступ к системам управления идентификационными данными, например контроллерам домена, атакующие могут создавать поддельные учётные записи и проходить под ними аутентификацию. После аутентификации личность пользователя редко проверяют повторно в течение сеанса, если только для привилегированных задач не требуется заново ввести пароль. Точно так же переодетые синоби могли беспрепятственно бродить внутри замка: в обоих случаях предполагается, что все находящиеся внутри уже прошли проверку.

Для борьбы с угрозами аутентификации развиваются защитные технологии. Одно из новых решений, называемое непрерывной или активной аутентификацией, постоянно проверяет личность пользователя после первоначального входа. Но поскольку диалоги непрерывной аутентификации способны мешать работе, разрабатываются и методы контроля по манере печати, движениям мыши и другим особенностям поведения, связанным с личностью пользователя. Такие методы выявляли бы противников, получивших физический доступ к оставленной без присмотра системе с открытым сеансом, и блокировали бы их. Это работало бы и при несанкционированном удалённом доступе, например в сеансах протокола удалённого рабочего стола (Remote Desktop Protocol, RDP). Подобные методы могли бы выявлять атакующих, даже если те вошли с действительными учётными данными и аутентификаторами. Разумеется, поведение человека способно меняться. Более того, искушённый противник может воспроизвести или имитировать даже конкретные особенности поведения, включив разведку пользовательских привычек в свою атаку.

Один из возможных вариантов модели парных соответствий предусматривает человеко-машинный интерфейс с пассивными датчиками мозговых волн, подключёнными к системе, которая проверяет личность по образу мышления пользователя. Исследования показывают, что люди создают уникальные мозговые рисунки, когда видят предмет, с которым раньше взаимодействовали, или имеют определённую мысленную ассоциацию. Поэтому предъявление пользователю контролируемых стимулов, например парных сочетаний слов или изображений, наблюдение за электрическими откликами мозга и их сопоставление с пользовательским профилем могли бы точно аутентифицировать пользователя. При достаточно большом числе уникальных проверочных пар, динамически создаваемых в стилистически разных вариантах, противники едва ли сумеют воспроизвести или сымитировать мозговую активность пользователя в ответ на запрос.

В следующем разделе мы обсудим некоторые способы применения аутентификации по парным соответствиям.

Разработка парных аутентификаторов

Ниже приведено несколько предложений по разработке парных аутентификаторов и идей по их применению.

- **Работайте с подходящими коммерческими поставщиками средств аутентификации.** Ищите поставщиков, которые используют аутентификацию по проверочному выражению, не совпадающему с паролем, именем учётной записи и другими идентифицирующими сведениями, которые может скомпрометировать противник. Некоторые финансовые организации применяют проверочные парные выражения перед разрешением изменений учётной записи, но, к сожалению, этот способ обычно используется лишь после сообщения пользователя об утраченном или забытом пароле; при этом проверочные выражения остаются неизменными.
- **Разрабатывайте новые системы аутентификации.** Продукт аутентификации можно интегрировать со средствами управления идентификационными данными, чтобы предъявлять аутентифицированному пользователю парную проверку всякий раз, когда тот пытается выполнить привилегированное действие, например команду администратора, `root` или системы. При таком протоколе, даже если противник подсмотрит одну или несколько проверочных пар, его запрос на привилегированное действие будет отклонён.

  Идеальный продукт применяет два вида парных проверок: ежедневные и заранее заданные пользователем. Ежедневная проверка распространяется не в цифровом виде и только там, где её могут увидеть уполномоченные сотрудники; при запросе аутентификации внутри помещений она предъявляет слово или изображение и просит пользователя назвать пару. Все остальные сотрудники, в том числе удалённые и работающие через VPN, составляют большой набор пар соответствующих слов, которые едва ли забудутся или будут поняты неправильно. Организация случайным образом выбирает или меняет пары, чтобы быстро выявлять неуполномоченных пользователей, прошедших аутентификацию в сети. Чтобы противник не мог вставить собственные пары для скомпрометированных или поддельных учётных данных, передача, хранение и аудит новых пар в действующей системе проверок должны быть защищены. Рассмотрите возможность одностороннего интерфейса для ввода парных соответствий в защищённом помещении обработки секретной информации (secure controlled information facility, SCIF) или в изолированной комнате, куда можно войти и где можно работать только после ручной аутентификации и авторизации. Другие механизмы могли бы позволять организациям устраивать засаду на неопознанного пользователя, требуя доступа к микрофону, камере, данным о местоположении, работающим процессам, рабочей памяти или кешу, снимку рабочего стола и другим сведениям на подключающейся системе, чтобы точнее определить происхождение и личность угрозы.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка, внутри которого находятся ценные ресурсы. Вы успешно завершаете набег на вражеское войско и возвращаетесь в замок. Один солдат вашей армии желает приблизиться к вам и, согласно обычаю, вручить отсечённую голову вражеского командира, которого вы победили в бою. На воине ваша форма и правильный герб; он знает пароль на сегодняшний день, по-видимому, ориентируется внутри замка и ожидает разрешения войти во внутреннее укрепление, чтобы выразить почтение.

Подумайте, как поступить с подозрительными людьми, которые прошли обычные проверки подлинности и запрашивают привилегированный доступ. Какие существующие протоколы безопасности или процессы аутентификации помогли бы определить, не является ли этот воин переодетым вражеским синоби, намеренным причинить вам вред? Если проверить его личность невозможно, как снизить риск, не отвергая просьбу воина безоговорочно?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимой мерой безопасности из стандарта NIST 800-53. Каждую из них следует оценивать в контексте парного опознавания и ответов на запросы аутентификации.

1. Внедрите блокировку сеансов привилегированных учётных записей по истечении заданного времени, по запросу привилегированного пользователя или в ответ на подозрительное поведение. Восстанавливайте доступ только после того, как пользователь даст ответ на парную проверку. Блокировка сеанса может быть предпочтительнее обычной блокировки паролем, поскольку выбор парного соответствия требует одного щелчка или ввода более простого слова, чем пароль учётной записи. [AC-11: Session Lock; IA-2: Identification and Authentication (Organizational Users) | (1) Network Access to Privileged Accounts | (3) Local Access to Privileged Accounts; IA-10: Adaptive Identification and Authentication; IA-11: Re-Authentication]
2. Определите и задокументируйте действия, которые пользователь может выполнять в системе, не отвечая на парную проверку, например обращение в техническую поддержку или экстренный вызов, и обеспечьте соблюдение соответствующих мер безопасности. [AC-14: Permitted Actions Without Identification or Authentication]
3. Разработайте процессы аутентификации по парным соответствиям, устойчивые к атакам повторного воспроизведения, создав большие наборы одноразовых аутентификаторов типа «запрос-ответ». [IA-2: Identification and Authentication (Organizational Users) | (8) Network Access to Privileged Accounts - Replay Resistant]
4. Собирайте сведения, которые однозначно идентифицируют устройства пользователей, запрашивающих аутентификацию, чтобы получать разведывательные данные о неопознанных противниках, не сумевших ответить на парную проверку. [IA-3: Device Identification and Authentication | (4) Device Attestation]
5. Требуйте вводить парные соответствия лично, чтобы снизить риск компрометации системы опознавания по запросу и ответу. [IA-4: Identifier Management | (7) In-Person Registration]
6. Физически и логически отделите систему парных запросов и ответов и введите строгий контроль доступа, чтобы защитить её от компрометации. [IA-5: Authenticator Management | (6) Protection of Authenticators]

Разбор

В этой главе были показаны трудности командиров, которым требовалось проверять личности своих солдат, чтобы переодетые синоби не проникли в укрепления. Вы узнали о приёме опознавания по парным соответствиям: и о том, как синоби пользовались им для обнаружения врагов, и о мерах, которыми синоби защищались от этого приёма во время нападения. Вы также увидели современные аналоги такого приёма в аутентификации и идентификации средств компьютерной безопасности.

В следующей главе вы воспользуетесь знаниями о факторах аутентификации и исторических запросах и ответах, чтобы понять, чем двухэтапная аутентификация отличается от парных соответствий и как она их дополняет. Я расскажу о скрытом приёме аутентификации синоби - пароле с двойной печатью, позволяющем выявлять искушённых лазутчиков.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), p. 91.
[2] [назад] Cummins and Minami, *The Book of Ninja*, p. 92.
[3] [назад] Cummins and Minami, *The Book of Ninja*, p. 126.

Глава 5. Пароль с двойной печатью

> Иногда вместе с такими паролями следует подавать условные знаки - например, зажимать нос или держаться за ухо.

> К опознавательным знакам *айкэй* относятся приёмы *татисугури исугури* - произнесение паролей стоя или сидя.
>
> - «Бансэнсюкай», «Ё-нин II»

И в «Бансэнсюкай», и в свитках «Гунпо дзийосю» описан протокол обнаружения открытой маскировки, который якобы разработал самурай XIV века Кусуноки Масасигэ.[1] В сигнальных приёмах *татисугури исугури* жесты, поза или положение тела служат тайным фактором аутентификации, добавляя к проверке пароля ещё один уровень защиты. Эти приёмы образуют так называемую систему паролей с двойной печатью,[2] предназначенную для поимки переодетых вражеских синоби, даже если те способны пройти остальные проверки с помощью украденных паролей, опознавательных знаков и правильных ответов на проверочные слова.

В самом распространённом примере *татисугури исугури* человек в правильной форме и с правильным гербом подходит к воротам и просит впустить его. Не узнав незнакомца, стражник либо садится, либо встаёт, а затем шёпотом произносит проверочное слово. Если посетитель - союзник, которого ознакомили с протоколом опознавания *татисугури исугури*, то в ответ он совершает заранее оговорённое действие - неочевидный знак, например касается носа или уха, - и шепчет соответствующее кодовое слово. Стражник впускает незнакомца, только если тот правильно назвал кодовое слово и выполнил правильное движение. Помимо вставания или усаживания стражника, могли существовать и другие способы применения *татисугури исугури*, но, к сожалению, считается, что они были записаны в утраченном дополнительном разделе «Бансэнсюкай» - свитке «Тэйкайрон».[3]

Простая гениальность этого приёма заключается в том, что вставанию и усаживанию обычно не придают ни малейшего значения. Даже злоумышленник, пытающийся выдать себя за уполномоченного человека, скорее всего, не заметит этот второй, безмолвный запрос и ответ. Он может увидеть, как сто человек входят в ворота по одной и той же парольной фразе, пока стражник сидит, потому что знает каждого из них, и потому не поймёт, чем отличается взаимодействие, когда стражник встаёт. *Татисугури исугури* оказался настолько успешным, что даже другие синоби не располагали достаточными контрмерами. Тем не менее «Бансэнсюкай» велит синоби на всех контрольных пунктах повторять за стражниками всё, что те делают и говорят, даже если кажется, будто стражники действуют неосознанно;[4] по крайней мере, это могло сбить стражника с толку и заставить его решить, что синоби просто несобран или глуп. В свитках есть и такой полезный совет синоби, провалившему неизвестную проверку *татисугури исугури*: быстро думай и быстро говори - или спасайся бегством.[5]

В свитках синоби нет точного определения двойной печати, и у меня нет доказательств, что следующий вымышленный пример действительно имел место, однако он кажется мне правдоподобным пояснением понятия. С древних времён печати, часто оттиснутые на воске, защищали содержимое писем и свитков. В идеале у каждого отправителя был уникальный металлический штамп, и только он мог оставить определённый оттиск, тем самым подтверждая подлинность документа. Кроме того, если письмо или свиток открывал кто-либо, кроме предполагаемого получателя, печать ломалась, показывая, что документ вскрывали.

Однако шпионы научились особыми способами нагревать воск, размягчать его, снимать печать целиком, не повреждая бумагу, читать послание, а затем снова запечатывать исходный документ либо переносить печать на новую подделку с ложными сведениями. Возможной контрмерой против

нагревания восковой печати со стороны бумаги была «двойная печать» воска. Представьте, что вместо одного металлического штампа автор применял зажим или приспособление наподобие тисков со штампами спереди и сзади. Нижняя сторона восковой пластинки получала скрытый оттиск с обратной стороны бумаги, который можно было проверить, лишь разорвав документ. При попытке расплавить печать и отделить её от бумаги верхний оттиск мог сохраниться, но второй, скрытый, разрушался, благодаря чему послание оказывалось запечатано дважды.

Теперь понятно, почему двойная печать стала действенной контрмерой против преодоления одинарной и как она помогала обнаруживать действия вражеских синоби. В этой главе я отмечу различие между двухфакторной и вторым этапом аутентификации. Я также расскажу, как современный аутентификатор второго этапа можно снабдить двойной печатью, повысив его эффективность. Затем я опишу предлагаемые мною требования и критерии для внедрения паролей с двойной печатью, а также варианты, использующие существующие аутентификаторы и технологии. Надеюсь, что, выполнив мысленные упражнения и увидев мои примеры внедрения паролей с двойной печатью, вы оцените гениальность Кусуноки Масасигэ и сами испытаете эту чрезвычайно понятную идею.

Скрытая двухэтапная аутентификация

Всё больше протоколов кибераутентификации и идентификации требуют дополнительного уровня защиты поверх пароля. Это называется *двухэтапной аутентификацией*: на втором этапе пользователь должен выполнить дополнительное действие аутентификации, например сообщить секретный код или нажать кнопку на устройстве вне основного канала, то есть не участвующем в остальной части процесса аутентификации. Обратите внимание на небольшое отличие от двухфакторной аутентификации из предыдущей главы, которая не позволяет противнику получить доступ к учётной записи с украденными данными для входа.

Хотя секретный код второго этапа может случайным образом создаваться программным приложением, обычно каждый раз применяется одна и та же процедура. К сожалению, эта процедурная жёсткость даёт противнику множество возможностей скомпрометировать методы двухэтапной аутентификации. Например, код двухэтапной аутентификации обычно отправляется открытым текстом в незащищённом сообщении, которое можно перехватить клонированием телефона. В этом случае пользователь, получивший код `12345` и введший эту последовательность в поле пароля, невольно сообщает код и противнику. Устройство аутентификации, часто телефон, можно украсть, перехватить посредством переадресации вызовов или клонировать, после чего противник завершит аутентификацию с его помощью. Аналогично можно потерять или лишиться устройства вне основного канала, настроенного для доставки кодов второго этапа; тогда оно позволит обойти процесс аутентификации и похитить предоставленные пользователю резервные коды.

Код второго этапа с двойной печатью, созданной приёмом *татисугури исугури*, мог бы смягчить некоторые слабости, присущие процедурам аутентификации. Каждый пользователь должен иметь возможность установить заранее согласованный идентификатор *татисугури исугури*, уникальный и значимый лично для него. Предположим, например, что пользователю устно или иным защищённым способом велели переставлять цифры кода второго этапа симметрично относительно цифры 5 на клавиатуре: 1 превращается в 9, 2 - в 8 и так далее,[6] но лишь тогда, когда код показан красным, а не обычным зелёным шрифтом. Изменение цвета - безмолвный фактор *татисугури исугури*, который срабатывает, если система считает запрос аутентификации подозрительным из-за необычного времени, незнакомого устройства, другого IP-адреса или иных признаков. Чтобы скрыть протокол от противников, наблюдающих за входом, его не следует применять слишком часто. Теперь, получив красный код `12345`, законный пользователь знает, что

нужно ответить 98765, тогда как противник, похитивший его учётные данные, но не знающий скрытого правила, вводит 12345. Процесс аутентификации останавливается, учётная запись отмечается для расследования, а в сеанс добавляется событие неудачной двухэтапной аутентификации. Затем аутентификатор второго этапа отправляет подсказку - например, «Используйте протокол аутентификатора 5» - и, возможно, ещё один красный код, такой как 64831, на который пользователь должен ответить 46279. Ещё один неправильный ответ вызывает дополнительные предупреждения или блокировку учётной записи.

Разработка паролей с двойной печатью

Защитное решение с двойной печатью, интегрированное со стандартными отраслевыми средствами авторизации, должно отвечать следующим требованиям:

1. Применяться только тогда, когда личность пользователя вызывает подозрения, например если пользователь:
    - входит с нового устройства, из нового места, с нового IP-адреса или в новое время;
    - сообщает о краже или компрометации мобильного устройства;
    - потерял резервный жетон, код или пароль и нуждается в сбросе пароля.
2. Использовать способ связи вне основного или по боковому каналу.
3. Использовать тайный, основанный на правилах фактор знания. Каждый пользователь должен иметь возможность настраивать протокол, создавая уникальный набор скрытых правил.
4. Применять факторы аутентификации, которые легко понять и запомнить, но которые неочевидны.
5. Позволять накладывать правила друг на друга после нескольких последовательных ошибочных ответов или при достаточном промежутке времени между попытками аутентификации.
6. Позволять ограничивать, замораживать или блокировать учётную запись после слишком большого числа неудачных попыток аутентификации. Большинство приложений блокируют учётную запись после нескольких последовательных неправильных паролей, но не после нескольких неправильных ответов второго этапа.
7. Не описываться ни в стандартных рабочих процедурах службы поддержки, ни в другой документации. Сотрудникам также не следует открыто обсуждать защитный уровень с двойной печатью.

Для распространения защиты с двойной печатью проектировщикам, инженерам и пользователям необходимо исследовать технически осуществимые варианты и мыслить творчески. Например, рассмотрим различные варианты ввода, которые доступны на существующих мобильных устройствах с приложением двухэтапной аутентификации и требуют от пользователя только нажать кнопку Yes или No, чтобы подтвердить личность. Следующие примеры показывают разнообразие возможных ответов, когда пользователь получает сигнал *татисугури исугури* в приложении двухэтапной аутентификации:

1. Перед нажатием Yes пользователь переворачивает экран вверх ногами, а приложение незаметно проверяет, равно ли состояние `DeviceOrientation` значению `portraitUpsideDown`.
2. Перед нажатием Yes пользователь физическими кнопками громкости мобильного устройства устанавливает `OutputVolume` в `0.0` (без звука) или `1.0` (максимум), а приложение незаметно получает значение громкости с плавающей точкой и проверяет его совпадение с требуемым.
3. Пользователь ждёт, пока часы мобильного устройства перейдут на следующую минуту, и немедленно нажимает Yes. Приложение незаметно запрашивает отметку времени и сравнивает момент выбора с `HH:MM:0X`, где `X` меньше 3 секунд.
4. Нажимая Yes на мобильном устройстве, пользователь прикладывает чрезмерное усилие, а приложение незаметно получает значение `UITouch.force` события и проверяет, превышает ли оно заданный порог.
5. Пользователь несколько раз быстро нажимает Yes на мобильном устройстве, а приложение незаметно получает `tapCount` события `UIEvent` и проверяет, меньше ли это значение 2.
6. Нажимая Yes на мобильном устройстве, пользователь выполняет жест, а приложение незаметно получает `UIGestureRecognizer` и определяет его тип: `Pinch`, `LongPress`, `Swipe` (вверх, вниз, влево, вправо) или `Rotation`.

> **Упражнение «Теория замка».** Представьте, что вы правитель средневекового замка, внутри которого находятся ценные ресурсы. Вам сообщили, что ваши опознавательные знаки, гербы, тайные сигналы и другие способы опознавания раскрыты вражеским синоби, которые способны их воспроизвести и проникнуть в замок. Вы и без того меняете эти пароли и знаки трижды в день, но, по полученным сведениям, синоби успевают следить за изменениями, хотя вы не знаете, каким образом.
>
> Подумайте, как применить *тамисугури исугури* для поимки вражеских синоби. Можно ли создать небинарный вариант *тамисугури исугури* - иначе говоря, скрытые правила, более сложные, чем сидение или стояние? Как защитить процесс аутентификации *тамисугури исугури*, чтобы вражеские синоби о нём не узнали? Как наложить несколько уровней *тамисугури исугури* и провести проверку на утечки сведений об оперативной безопасности среди своих людей?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимой мерой безопасности из стандарта NIST 800-53. Каждую из них следует оценивать применительно к двухэтапной аутентификации с двойной печатью.

1. Используйте внеполосную аутентификацию (Out-of-Band Authentication, OOBA) по отдельному каналу связи, чтобы проверять, действительно ли запрос аутентификации исходит от подтверждённого пользователя. [IA-2: Identification and Authentication | (13) Out-Of-Band Authentication]

2. Следите, чтобы сотрудники не раскрывали существование скрытых правил двухэтапной аутентификации. [IA-5: Authenticator Management | (6) Protection of Authenticators]
3. Установите несколько правил двойной печати, чтобы *татисугури исугури* не оставался неизменным. [IA-5: Authenticator Management | (7) No Embedded Unencrypted Static Authenticators]
4. Внедрите внеполосную связь и установите правила двойной печати для сохранения конфиденциальности. [SC-37: Out-Of-Band Channels]
5. Тщательно проектируйте сообщения об ошибках при неудачной аутентификации, чтобы они не раскрывали противнику сведения о пароле с двойной печатью, которыми тот мог бы воспользоваться. [SI-11: Error Handling]

Разбор

В этой главе вы узнали о приёме аутентификации против синоби, называемом паролем с двойной печатью, или *татисугури исугури*. Мы разобрали различие между факторами и этапами процесса проверки личности. Затем провели краткий анализ критериев хорошего аутентификатора *татисугури исугури* и рассмотрели несколько примеров.

В следующей главе мы обсудим понятие синоби, называемое часами проникновения. Вы узнаете, в какие часы суток возникают благоприятные возможности для проникновения. Понимание подобных зависящих от времени возможностей поможет выбрать момент для внедрения или срабатывания аутентификаторов *татисугури исугури* в организации - например, только в определённые часы или даты, - чтобы применять этот приём как можно реже и сохранять его в тайне.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), p. 100.
[2] [назад] Cummins and Minami, *Secret Traditions*, p. 192.
[3] [назад] Cummins and Minami, *The Book of Ninja*, p. 127.
[4] [назад] Cummins and Minami, *The Book of Ninja*, p. 127.
[5] [назад] Antony Cummins and Yoshie Minami, *True Path of the Ninja* (North Clarendon, VT: Tuttle Publishing, 2017), p. 80.
[6] [назад] Поклонники сериала HBO *The Wire* могут помнить этот приём как код «переход через пятёрку», взломанный в 5-й серии 1-го сезона («The Pager»).

Глава 6. Часы проникновения

> Дождавшись часа Быка, ниндзя понял, что стражник уснул; всё вокруг замерло в тишине, огонь погас, и всё погрузилось во мрак.

> Для синоби крайне важно знать подходящее время. Следует всегда выбирать момент, когда враг устал или потерял бдительность.
>
> - «Ёсимори хякусю», стихотворение 5

Планируя кражу, шпионаж, диверсию, убийство или другое нападение, синоби не обременяли себя духом спортивного благородства или честной игры. Напротив, они тщательно выбирали наиболее «подходящее время и выгодное положение»[1] для удара. «Сёнинки» подчёркивает, как важно дождаться для проникновения момента, когда цель отвлечена, вяла, склонна к поспешным суждениям, пьёт и веселится или просто выбилась из сил; в стихотворении 63 из «Ёсимори хякусю» сказано, что усталость «может стать причиной серьёзной ошибки».[2] Синоби внимательно наблюдали за подобным поведением и часто проникали, когда враг рубил деревья, был занят обустройством собственной позиции, утомился после боя или менял караул.[3]

Изучая поведение врагов, синоби заметили, что предсказуемый распорядок жизни людей создаёт окна возможностей для нападения. В свитках день разделён на двухчасовые отрезки, а проникновение рекомендуется планировать на те из них, которые обычно совпадают с пробуждением, приёмом пищи и сном. Подходящий час зависит от вида нападения. Например, ночные атаки лучше всего проводить в часы Кабана (21:00-23:00), Крысы (23:00-1:00) и Кролика (5:00-7:00) - животных китайского зодиака.[4]

Кроме того, в «Бансэнсюкай» отмечается, что некоторые полководцы верили в «счастливые дни»,[5] определяемые по китайской астрологии. Считалось, что в такие даты нападению предначертана победа. Если синоби удавалось выявить вражеских командиров, веривших в эти суеверия, он мог воспользоваться сведениями - например, предсказать перемещение войск по тому, какой день командир считал счастливым или несчастливым для выхода из лагеря. Что касается предсказуемых моделей поведения, мало что изменилось. В этой главе мы обсудим, как субъекты угроз могут выбирать целью кибернетические аналоги событий, происходящих по расписанию.

Время и возможности

Люди по-прежнему встают, работают, едят, отдыхают и спят примерно по тому же расписанию, что и жители феодальной Японии. Поэтому предложенные в свитках часы проникновения почти точно совпадают с периодами, когда сотрудники отвлечены, истощены или стали невнимательны из-за трудностей современного рабочего дня, - иначе говоря, когда они наиболее уязвимы для нападения. Рассмотрим временные отрезки из свитков в контексте активности и характера использования сетей и информационных систем:

- **Час Кролика (5:00-7:00).** Пользователи просыпаются и впервые за день входят в систему. Запускаются автоматизированные и ручные системы, вызывая всплески в журналах событий и `syslog`.
- **Час Лошади (11:00-13:00).** Многие пользователи уходят на обед, то есть выходят из систем или их сеансы завершаются по тайм-ауту бездействия. Кроме того, они могут посещать веб-сайты по личным делам: читать новости, делать покупки, проверять личную почту, публиковать сообщения в социальных сетях или заниматься чем-то иным, что способно вызвать срабатывание систем обнаружения аномалий.
- **Час Петуха (17:00-19:00).** Пользователи ищут место, на котором можно прервать работу. Они сохраняют файлы и, возможно, торопятся закончить дела, что значительно повышает риск ошибок и в самой работе, и в соблюдении правил кибербезопасности. Например, сотрудник может не задумываясь открыть вложение из письма, которое кажется срочным. Пользователи массово выходят из учётных записей и систем, но некоторые сеансы просто бросают, оставляя их до тайм-аута и отключения.
- **Час Кабана (21:00-23:00).** Большинство пользователей находится вне работы. Дома ли они, проводят ли время в обществе или готовятся ко сну, безопасность рабочих учётных записей и систем едва ли занимает их мысли. В организациях, где SOC укомплектован на всю ночь, в это время обычно меняется смена, что создаёт для атакующих окно между входами пользователей или пока сотрудники SOC осваиваются с вечерней обстановкой. Чем позднее час, тем выше вероятность, что пользователи - даже привыкшие работать допоздна - станут сонными или потеряют бдительность, поскольку всё кажется спокойным.
- **Час Крысы (23:00-1:00).** Сети и системы выполняют резервное копирование или другое плановое обслуживание, создавая шум в сетевых датчиках и SIEM. Сотрудники SOC могли уже завершить ежедневные задачи по безопасности и обслуживанию и погрузиться в проектную работу.
- **Час Тигра (3:00-5:00).** В это время обычно выполняются пакетные задания, в том числе обработка файлов журналов, диагностика и запуск сборки программ. За исключением персонала SOC, большинство пользователей погружается в самую глубокую часть цикла сна и не проявляет активности в своих учётных записях.
- **Счастливые дни.** Существуют также конкретные дни, недели и месяцы, когда противники, вероятнее всего, выбирают целью системы и пользователей. Хотя большинство руководителей организаций не строит деятельность вокруг «счастливых дней», субъекты угроз, несомненно, знают о регулярных обновлениях и обслуживании, во время которых организации отключают защиту, а также о трёхдневных выходных и корпоративных праздниках, когда системы и учётные записи остаются почти без проверки. Если возможные угрозы не были учтены, отклонения в сетевом трафике и системных журналах могут остаться незамеченными в такие окна возможностей, позволяя противникам проводить атаки и разведку, обмениваться данными с командной инфраструктурой (command and control, C2), распространять вредоносное ПО или выводить данные.

Разработка средств безопасности и обнаружения аномалий с учётом времени

Систему часов проникновения синоби можно использовать для разработки зависящей от времени защиты, которая учитывает исходные состояния сети в разное время, отклонения от исходного уровня и деловые требования. В общем виде такая защита внедряется в три этапа:

1. Определите исходный уровень активности для каждого часа.
2. Обучите сотрудников отслеживать активность и досконально знать её обычный характер в назначенные им часы.
3. Оцените деловые потребности каждого часа. На основе этой оценки создайте деловую логику и аксиомы безопасности, чтобы лучше смягчать угрозы и обнаруживать аномалии.

Сначала попробуйте разделить журналы сети и систем на отрезки продолжительностью один-два часа. Изучите исторические тенденции и уровни активности сетей и систем, чтобы установить исходный уровень - важнейший показатель для охоты за угрозами и выявления проблем кибергигиены. Особое внимание уделите времени, когда уже происходили атаки, а также периодам, которые в силу обстоятельств организации, моделирования угроз и опыта могут регулярно быть уязвимы для нападения.

После сегментации всех данных и определения исходных уровней обучите аналитиков, системных администраторов и специалистов по безопасности досконально знать характер активности вашей сети. Они также должны понимать, какие пробелы в безопасности создаёт распорядок организации. Свитки синоби велят стражникам пристально исследовать каждое отклонение и несоответствие во время своей смены. Например, они должны замечать, что рыбак пришёл позже обычного или незнакомая птица подала голос в необычный час. Если специалисты по безопасности будут столь же чутко воспринимать несоответствия, они смогут повторно проверить необычное событие и тем самым выявить инцидент безопасности. Для развития столь глубоких знаний может понадобиться поручить сотруднику службы безопасности наблюдать за одним сектором - например, единственной системой, считающейся вероятной целью, - изучить её в мельчайших подробностях, а затем в течение двух часов из восьмичасовой смены просматривать каждый журнал и событие этой системы. Такая стратегия резко отличается от свойственного большинству SOC подхода «следить всегда и за всем», который вызывает усталость от предупреждений, перегрузку и выгорание. Она должна также смягчить проблемы многих автоматизированных систем обнаружения аномалий, где человек обязан изучать каждую аномалию, проводить расследование и предоставлять обратную связь. Эти системы быстро становятся непосильными, а данные - непонятными специалистам, просматривающим аномалии ежедневно или еженедельно.

Обратите внимание: журналы безопасности не исчезают, как ночные звуки, и доступны для будущего анализа. Искушённый противник, вероятно, способен изменить или удалить журналы безопасности, отфильтровать трафик от сетевых ответвителей и датчиков либо иным образом скомпрометировать системы, призванные регистрировать его проникновение и предупреждать службу безопасности. Однако такие действия должны нарушить нормальное поведение системы достаточно сильно, чтобы проницательный аналитик безопасности это заметил.

Далее задайте себе два вопроса:

• Когда активны ваши пользователи и системы?
• Когда может быть активен противник?

Понимание того, как и когда пользователи входят в системы и работают с ними, помогает стратегически ограничивать доступ, затрудняя внешней или внутренней угрозе проникновение в наиболее уязвимое время. Например, если система не используется с 20:00 до 8:00, выключайте её в эти часы. Если пользователям не нужно по делам обращаться к системам по субботам, отключите доступ для всех пользователей в субботу. Плановое отключение систем также помогает обучить сотрудников SOC выявлять аномалии в определённые часы, поскольку им придётся рассматривать меньше предупреждений и систем. Стандарты NIST предлагают внедрять подобный контроль доступа, но многие организации вместо этого ставят во главу угла удобство работы в чрезвычайных сценариях, сколь бы маловероятны ни были такие события.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка, внутри которого находятся ценные сведения, сокровища и люди. Вы получаете достоверные разведывательные сведения о том, что синоби намерен проникнуть в замок. Вообразите, что ваши стражники безупречно знают время, но могут обеспечивать соблюдение лишь двух правил:

- когда можно запирать и отпирать любые ворота и двери, внутренние и внешние;
- комендантский час, после которого любого встреченного в коридорах задерживают.

Подумайте, какого уровня целостности, уверенности и безопасности можно добиться строгим применением только этих двух средств, основанных на времени. Как научить жителей замка жить с такими ограничениями: как они будут посещать уборные ночью, убирать помещения, пока остальные спят, принимать ночные поставки и так далее? На какие компромиссы придётся пойти, чтобы средства безопасности оставались работоспособными?

Для этого упражнения полезно нарисовать план воображаемого замка или своего офисного здания. Можно также использовать абстрактную схему карты сети или диаграммы потоков данных (DFD) как «здание», где коммутаторы - коридоры, маршрутизаторы и межсетевые экраны - двери, системы - комнаты, а VPN и точки выхода - ворота.

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимой мерой безопасности из стандарта NIST 800-53. Каждую из них следует оценивать с учётом часов проникновения. Обратите внимание: для применения этих приёмов журналы и предупреждения должны содержать отметки времени, а часы всех систем должны быть синхронизированы. См. AU-8: Time Stamps.

1. Оцените свои часы работы и выполните моделирование угроз. В какое время вы наиболее уязвимы для нападения? Как подготовить сотрудников? [NIST SP 800-154: Guide to Data-Centric System Threat Modeling][6]
2. Внедрите для учётных записей зависящий от времени контроль полномочий на основе деловых и эксплуатационных потребностей пользователей. Например, запретите определённым пользователям отправлять и получать рабочую почту после 19:00. [AC-2: Account Management | (6) Dynamic Privilege Management]
3. Ограничьте возможность входа в конкретные учётные записи и их использования в определённые часы. Например, если с 21:00 до 23:00 кто-либо пытается выполнить несанкционированное действие в неактивной учётной записи, немедленно предупредите пользователя и попросите подтвердить личность. Если он не отвечает или не проходит аутентификацию, предупредите SOC. [AC-2: Account Management | (11) Usage Conditions]

4. Используйте системы эвристического анализа для выявления необычных моделей доступа к системе или её использования в установленное время. Пользователям следует добровольно документировать свои «обычные» модели работы и рассказывать о них, чтобы помочь смоделировать ожидаемое поведение в течение рабочего дня. [AC-2: Account Management | (12) Account Monitoring for A-Typical Usage]
5. Требуйте, чтобы владельцы и пользователи систем документировали ожидаемые периоды их использования и время, когда системы можно выключать. [AC-3: Access Enforcement | (5) Security Relevant Information]
6. Сократите период, в течение которого может действовать противник. Определите стратегическую корпоративную политику, согласно которой конфиденциальные или закрытые сведения разрешено получать только в установленное время - например, с 11:00 до 15:00 по рабочим дням. [AC-17: Remote Access | (9) Disconnect/Disable Access]
7. Сообщайте владельцу учётной записи об успешном и неудачном входе, включая дату и время последнего входа. Отслеживание этих сведений помогает пользователю предупредить SOC о компрометации учётной записи и сообщить, когда произошёл несанкционированный доступ. [AC-9: Previous Login (Access) Notification | (4) Additional Logon Information]
8. Установив часы работы, настройте пользовательские устройства и системы на автоматическую блокировку и завершение всех сеансов в заданное время. [AC-11: Session Lock]
9. Задокументируйте политику, сообщающую разрешённые даты и время внесения изменений в инфраструктуру и системы. Она поможет SOC ежечасно оценивать изменения сети и конфигурации. [AU-12: Audit Generation | (1) System Wide and Time Audit Correlation Trail; CM-5: Access Restrictions for Change]

Разбор

В этой главе вы узнали о традиционном японском исчислении времени по животным китайского зодиака, о влиянии китайской астрологии на предсказания и о том, как синоби, вероятно, пользовались ими, чтобы находить возможности для проникновения или переигрывать цель. Вы рассмотрели, как сетевая активность меняется в зависимости от времени суток и как уменьшить возможность нападения с помощью зависящих от времени средств. Вы познакомились со стандартом безопасности синоби. В частности, узнали, что стражник должен был замечать малейшее несоответствие в своём секторе наблюдения - всё, что могло указывать на присутствие противника. Кроме того, вы изучили рекомендации по применению некоторых из этих понятий в охоте за угрозами, процессах работы службы безопасности и системах обнаружения аномалий.

В следующей главе мы рассмотрим применение конфиденциальности времени: сокрытие времени от вредоносного ПО, которое может дать защитникам особые возможности обнаружения и защиты.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *True Path of the Ninja* (North Clarendon, VT: Tuttle Publishing, 2017), p. 78.
[2] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), p. 158.
[3] [назад] Cummins and Minami, *True Path*, p. 79.
[4] [назад] Cummins and Minami, *True Path*, p. 79.
[5] [назад] Antony Cummins and Yoshie Minami, «Tenji I - Opportunities Bestowed by Heaven I», in *The Book of Ninja* (London: Watkins Publishing, 2013), pp. 268-293.
[6] [назад] «SP 800-154 (DRAFT): Guide to Data-Centric System Threat Modeling», Computer Security Resource Center, National Institute of Standards and Technology, март 2016 г., https://bit.ly/3bjQofW.

Глава 7. Доступ ко времени

> Начинать атаку следует без промедления, но и не преждевременно, а точно в срок.
>
> Если вы собираетесь поджечь вражеский замок или лагерь, заранее согласуйте с союзниками время поджога.
>
> - «Ёсимори хякусю», стихотворение 83

Во время задания, особенно ночью, одной из важнейших и сложнейших обязанностей синоби было следить за временем. Если эта задача кажется простой, вспомните: у синоби не было ни наручных, ни иных часов. Даже песочные часы появились у них лишь в начале XVII века.[1] Чтобы вовремя отправлять и получать сигналы, координировать нападения, знать, когда враг будет уязвим, и решать другие задачи, синоби пришлось разработать надёжные способы определения времени.

Исторически один из способов отмечать часы заключался в зажигании благовоний или свечей, которые, как было известно, горели с постоянной скоростью, и звоне колокола через определённые промежутки. «Бансэнсюкай» рекомендует определять время по природным признакам, например движению звёзд, либо с помощью приборов, основанных на весе.[2] Вероятно, такими приборами были водяные часы, иногда называемые клепсидрами, где для точной подачи сигналов через заданные промежутки применялись равновесие, поток и вес воды. В других свитках приведены более загадочные способы, например отслеживание изменения размера кошачьего зрачка в течение дня или едва заметного теплового расширения жилища ночью, поскольку эти явления соответствуют определённым часам.[3] Синоби учили определять час даже по тому, через какую ноздрю он дышит активнее. В свитках объясняется, что воздух в основном входит и выходит через одну ноздрю, а затем через регулярные промежутки дыхание переключается на другую, благодаря чему можно следить за временем. Эта идея может показаться лженаучной, однако в 1895 году немецкий учёный Рихард Кайзер наблюдал и документировал, как в течение дня кровь приливает то к одной, то к другой стороне носа, заметно уменьшая поток воздуха через одну ноздрю, а затем через другую.[4] Острая наблюдательность синоби позволила не только обнаружить это явление более чем за триста лет до его научной публикации на Западе, но и найти ему практическое применение. Например, синоби мог быть вынужден лежать в подполье под целью, где нельзя было зажечь свечу или благовоние, воспользоваться прибором для отсчёта времени или даже осмелиться открыть глаза: блеск глаза через щели в полу мог привлечь внимание цели. В таких неудобных обстоятельствах он неподвижно лежал, следя за дыханием через нос, пока не наступало время нападения, - блестящий пример дисциплины, изобретательности и творческого подхода синоби.

Множество упоминаний времени в свитках синоби в сочетании с трудоёмкими способами его отслеживания позволяет предположить: эти приёмы не стали бы разрабатывать, если бы учёт времени не был важнейшим условием эффективных действий субъекта угроз. Повсеместное распространение в современном обществе дешёвых, простых и надёжных способов узнавать время почти наверняка приучило нас воспринимать само время и его измерение как нечто само собой разумеющееся.

В этой главе мы заново оценим значение и важность времени в цифровых системах и вкратце рассмотрим, как оно формируется, используется и защищается существующими передовыми методами. Затем зададимся вопросами: если точное время столь важно для противника, что произойдёт, если мы сможем скрыть от него время? Или лишить его доступа ко времени? Или даже обмануть, сообщив неверное время?

Важность времени

Время необходимо для работы почти каждой современной компьютерной системы. Синхронизируя последовательную логику и формируя тактовый сигнал, который задаёт интервалы работы, компьютеры создают конечные импульсы времени. Эти импульсы подобны тиканью часов: в них системы выполняют операции над данными в устойчивой и надёжной среде ввода и вывода. Огромные и сложные сети и системы, от которых зависят наши государства, экономика, предприятия и личная жизнь, работают по этим импульсам и непрерывно запрашивают время. Без часов они не могли бы действовать.

Для защиты данных времени существует множество средств безопасности. Аутентификация идентичности серверов сетевого протокола времени (Network Time Protocol, NTP) подтверждает, что атакующий не подменяет доверенный источник времени системы. Шифрование и контрольные суммы данных времени сервера NTP - шифрование кодирует обмен, а контрольные суммы выявляют ошибки передачи - подтверждают их целостность и защищают от изменения. К обмену временем добавляется *nonce* - произвольное случайное число, предотвращающее ошибки повторной передачи. Отметки времени и журналирование синхронизации сравнивают системное время со временем, сообщённым авторитетным источником. NTP сохраняет доступность и отказоустойчивость благодаря нескольким источникам времени и альтернативным способам распространения, а если доступ к NTP запрещён или отсутствует, резервные методы точно оценивают время по последней синхронизации. Дополнительные передовые методы безопасности предписывают ставить отметки времени в записях аудита, блокировать сеансы после бездействия, ограничивать доступ к учётным записям по времени суток, оценивать действительность сертификатов и ключей безопасности по сведениям о дате и времени, определять момент резервного копирования и срок хранения кешированных записей.

Эти средства защищают целостность и доступность данных времени, однако защите их конфиденциальности редко уделяется достаточно внимания. Почти любое современное приложение может в любой момент запросить время, и обычно ему разрешён доступ не только к дате и времени, но и к библиотекам и функциям часов. Хотя NTP способен шифровать данные времени при передаче системе, средства ограничения доступа к текущему системному времени явно отсутствуют. Этот пробел важно выявить, поскольку время - важнейшее сведение, с помощью которого противники распространяют вредоносное ПО. Например, разрушительное вредоносное ПО Shamoon[5] было настроено на запуск в начале выходных в Саудовской Аравии, чтобы причинить максимальный ущерб: оно должно было стереть все заражённые системы до того, как кто-либо это заметит.

К другим распространённым атакам относятся раскрытие конфиденциальных сведений, создание состояний гонки, принудительные взаимные блокировки, манипуляции состояниями информации и временные атаки для раскрытия криптографических секретов. Более сложное вредоносное ПО может пользоваться доступом ко времени, чтобы:

• приостанавливать работу на установленный период во избежание обнаружения;
• вычислять число пи до десяти миллионов знаков и по продолжительности вычисления определять, не находится ли заражённая система в песочнице или среде детонации, предназначенной для поимки вредоносного ПО;
• пытаться связаться с командной инфраструктурой (C2) по определённым временным указаниям;
• выявлять метаданные и другие сведения посредством временных атак, раскрывающих состояние, положение и возможности целевой системы.

Если бы администраторы могли запретить доступ к локальному, реальному и линейному времени, противнику было бы намного труднее - а возможно, и вовсе невозможно - действовать внутри целевых информационных систем. Однако важно учитывать, что бессистемное ограничение запросов времени, вероятнее всего, вызовет каскадные отказы и ошибки. Для запрета доступа ко времени нужен точный подход.

Сохранение конфиденциальности времени

Помните: поскольку конфиденциальность ещё не укоренилась так глубоко, как другие формы защиты времени, применение подобных средств потребует особых усилий от вашей организации и всего сообщества безопасности.

Определите исходный уровень

Выявите программы, приложения, системы и административные команды среды, которым необходим доступ ко времени. Внедрите перехват функций - перехват вызовов функций - и журналирование, чтобы определить, кто и что запрашивает время. Установив исходный уровень, используйте его для выявления необычных запросов времени и оценки временных потребностей, на основе которой будут настроены дополнительные средства безопасности, например Just in Time (JIT).

Оцените технические возможности

Свяжитесь с производителями оборудования и поставщиками программного обеспечения и выясните, какие технические средства можно включить для ограничения доступа к функциям времени. Если таких средств нет, запросите внедрение новых возможностей, побуждая отрасль разрабатывать решения для конфиденциальности времени.

Установите политику

Запрет доступа ко времени - нетрадиционная мера безопасности, но, как и в случае более привычных мер, для её соблюдения нужна стратегическая политика с подробными требованиями: в данном случае ограничивать доступ ко времени и следить за попытками его получить. По возможности включайте понятие конфиденциальности времени во все решения по управлению изменениями, закупки нового оборудования и программ и приоритеты SOC. Формально задокументируйте новые политики и заручитесь их одобрением со стороны CISO организации.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка, внутри которого находятся ценные ресурсы. Вы получаете достоверные разведывательные сведения о том, что синоби проник в замок с приказом поджечь его ровно в 3:00 ночи. По ночам стражник на башне жжёт свечу-часы и каждые 120 минут ударяет в колокол, чтобы остальные ночные стражи соблюдали распорядок; вы считаете, что синоби тоже слышит колокол.

Как управлять доступом ко времени, чтобы смягчить эту угрозу? Кому из доверенных людей в замке необходимо знать время, а кому можно полностью закрыть доступ? Какие действия позволят сорвать нападение или обнаружить синоби, если управлять только сведениями о времени?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую из них следует оценивать с учётом понятия конфиденциальности времени.

1. Внедрите защиту, блокирующую доступ к данным времени в журналах отметок времени и других журналах наблюдения за сведениями. Для предотвращения утечки времени или отметок времени могут потребоваться физические, средовые, технические средства и средства защиты носителей. [AU-9: Protection of Audit Information]
2. Изучите существующую информационную архитектуру в отношении времени, включая философию, требования и тактику, необходимые для внедрения контроля доступа к данным времени и их конфиденциальности в своей среде. Если заинтересованные лица согласны на временные ограничения, задокументируйте их в плане безопасности с утверждённым бюджетом, ресурсами и временем на внедрение. [PL-8: Information Security Architecture]
3. Проведите проверку журналов и внутреннюю охоту, чтобы выявить обмен через порт 123 с любыми неофициальными серверами NTP в своей среде. Ищите обмен NTP с внешними серверами и подумайте о блокировке доступа к серверам NTP, которые вы не контролируете. [SC-7: Boundary Protection]

Разбор

В этой главе вы узнали о некоторых средствах, которыми синоби определяли время, и о том, как они пользовались этим знанием. Мы обсудили значение времени для кибероперациий и безопасности и отметили, что современные методы защиты в первую очередь сосредоточены на доступности и целостности времени в системах. Вы также познакомились с мысленным упражнением, в котором нападение синоби смягчалось посредством манипуляции временем.

В следующей главе мы обсудим, как синоби превращали самые разные предметы в инструменты для решения задач. Понимание того, что представляет собой цифровой аналог таких «инструментов», может помочь обнаруживать новые способы их превращения в оружие и защищаться от них или по крайней мере затруднять их применение.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), p. 313.
[2] [назад] Cummins and Minami, *The Book of Ninja*, p. 169.
[3] [назад] Antony Cummins and Yoshie Minami, *True Path of the Ninja* (North Clarendon, VT: Tuttle Publishing, 2017), p. 85.
[4] [назад] Richard Kayser, «Die exakte Messung der Luftdurchgängigkeit der Nase», *Arch. Laryng. Rhinol.* 8 (1895), p. 101.
[5] [назад] Symantec Security Response, «The Shamoon Attacks», Symantec Official Blog, Symantec Corporation, 16 августа 2012 г., https://bit.ly/2L2Az2z.

Глава 8. Инструменты

> Помните: если пользуетесь инструментом ниндзя, делайте это при свистящем ветре, который скроет звук, и всегда забирайте инструмент с собой.

> Сколько бы инструментов вы ни носили как синоби, прежде всего помните, что еда всегда должна быть у вас на поясе.
>
> - «Ёсимори хякусю», стихотворение 21

Хотя в голливудских фильмах ниндзя обычно размахивают метательными звёздами или катанами, настоящие синоби разработали огромный и разнообразный набор инструментов и оружия; им предписывалось особенно тщательно выбирать правильный инструмент для работы.[1] Во всех трёх свитках синоби тайным инструментам отведено много места, и многие из них были передовой технологией своего времени. В одном только «Бансэнсюкай» инструментам посвящено пять объёмных томов. Среди прочих указаний там сказано, что лучшие инструменты пригодны для нескольких целей, не шумят и не громоздки.[2] «Сёнинки» советует синоби ограничивать количество переносимых инструментов, поскольку любой предмет снаряжения способен вызвать подозрения, если выглядит неуместно.[3] Свиток также рекомендует искать и выводить из строя инструменты и оружие целей: подобные средства имели центральное значение для возможностей синоби.[4]

Разумеется, синоби не приобретали инструменты в каком-нибудь огромном магазине товаров для синоби. Следуя наставлениям свитков, они создавали действенные инструменты из предметов, которые легко купить, найти или изготовить. У такого подхода было несколько преимуществ. Повседневные вещи можно было носить, почти не вызывая подозрений,[5] и даже применять как убедительный реквизит для маскировки синоби. Например, несколько правителей, в том числе Тоётоми Хидэёси и Ода Нобунага, объявляли «охоту за мечами» - массовое изъятие у мирных жителей всех мечей и другого оружия, чтобы ослабить способность мятежников нападать на правительственное войско.[6] В таких условиях любой человек, не принадлежавший к самураям и открыто носивший меч или иное вооружение, мог ожидать его конфискации. Чтобы обойти эту меру, синоби незаметно переделывали обычные сельскохозяйственные орудия в оружие: указа, запрещающего носить на людях острые инструменты для земледелия, не существовало. В руках обученного синоби повседневные сельскохозяйственные орудия становились смертоносными.

При всей их практичности «Бансэнсюкай» утверждает: главный принцип использования инструментов состоит не просто во владении ими, а в просветлённом, подобном дзену понимании их назначения.[7] Синоби глубоко и часто размышляли о полезности инструментов, постоянно упражнялись с ними и заново представляли способы применения в деле. В результате синоби регулярно совершенствовали существующие инструменты, изобретали новые и передавали знания другим, союзным синоби.[8]

В этой главе мы поразмышляем об инструментах. Мы затронем их двойственную природу: один и тот же инструмент способен приносить пользу или вред в зависимости от оператора. Эта бинарная концепция *ин-ё*, или инь-ян, представляет собой полезную модель для понимания подхода хакера к цифровым инструментам. Например, подумайте, как средство, предназначенное помогать пользователю, можно применить во вред.

Помимо способности приносить пользу и вред, любой инструмент можно приспособить для другой цели или применять разными способами. Задумайтесь на мгновение и назовите около дюжины способов использования молотка. Такие простые мысленные упражнения помогают глубже понять, что именно представляет собой молоток, как его можно улучшить и как изобрести новый его вид для решения новой задачи. Те же творческие навыки применимы к перепрограммированию цифровых и программных инструментов. На высшем уровне мастерства подобное творческое

переосмысление сравнимо с работой мастера-кузнеца. Кузнец способен выковать новые инструменты, машины и системы, которые кардинально изменят его представление о собственном ремесле, откроют новые возможности для создания вещей и расширят способность разрабатывать новое оружие, защиту и инструменты.

Следует ясно понимать: враждебное применение инструментов, вероятно, остаётся угрозой, от которой мы никогда не избавимся полностью. И всё же в этой главе я опишу передовые методы защиты, связанные с инструментами, а также некоторые усиленные средства контроля, способные смягчить нападения.

Жизнь за счёт окружения

В кибербезопасности инструментами называют любые средства, помогающие вручную или автоматически выполнять задачу. Если это определение кажется чрезвычайно широким, то лишь потому, что оно действительно таково. Существуют физические инструменты - BadUSB, перехватчики Wi-Fi и отмычки - и программные: платформы, эксплойты, код, сценарии и исполняемые файлы. Целая компьютерная система сама по себе представляет собой инструмент. Инструмент может иметь законное применение, но в руках хакера превратиться в оружие. Вспомните, например, клиент SSH, которым администратор удалённо обслуживает системы, а атакующий способен воспользоваться для обратного туннелирования SSH, чтобы нападать на системы и обходить межсетевые экраны.

Подобно синоби, киберпротивники в значительной степени полагаются на инструменты при достижении целей и непрерывно разрабатывают, настраивают, оттачивают и испытывают их на существующих технологиях в реальной среде. Сложные группы угроз держат штатных разработчиков инструментов и возможностей, занятых поддержкой и совершенствованием набора средств. В ответ предприимчивые защитники киберсреды проводят обратную разработку этих специализированных инструментов, чтобы создавать контрмеры, внедрять полезные политики безопасности и сигнатуры обнаружения, испытывать возможности вредоносных средств в песочницах и составлять белые списки приложений, выявляющие и блокирующие опасные инструменты. Иногда новая защита применяется настолько успешно, что противник не может загрузить или установить свои средства в целевой системе: узловая защита немедленно помещает их в карантин, закрывает доступ и предупреждает сотрудников службы безопасности.

Поскольку узловые системы безопасности способны выявлять и блокировать специализированные инструменты и вредоносное ПО, многие противники теперь применяют тактику проникновения под названием «жизнь за счёт окружения». Сначала атакующие собирают разведывательные сведения о программах и средствах, уже используемых в целевой системе. Затем строят атаку исключительно на этих приложениях, поскольку защита основной системы не считает их вредоносными. При нападении за счёт окружения можно применять любой файл на диске компьютера жертвы, включая планировщик задач, веб-браузер и программу командной строки Windows Management Instrumentation (WMI), а также механизмы сценариев `cmd` и `bat`, JavaScript, Lua, Python и VBScript. Синоби присваивали обычные предметы в среде цели, например сельскохозяйственные орудия, которые наверняка были под рукой и не выделялись; так и хакеры, приспосабливая уже существующее на целевом компьютере, превращают повседневные пользовательские и административные средства, приложения и файлы операционной системы в инструменты для своих целей.

Один из распространённых инструментов компьютеров Windows, подверженный эксплуатации, - мощная платформа PowerShell от Microsoft. Даже Microsoft признаёт, что субъекты угроз регулярно выбирают PowerShell для проникновения в системы, несанкционированных действий и иной

компрометации систем организации. В свою очередь Microsoft предлагает возможности защиты и смягчения, например Privilege Access Management (PAM), чтобы обеспечивать Just Enough Administration (JEA) в сочетании с администрированием Just in Time (JIT). К сожалению, JEA/JIT превращает повсеместность PowerShell в кошмар управления доступом для ИТ-администраторов. Каким образом? Я избавлю вас от технических подробностей. Просто представьте техника, которого вызвали для устранения неисправности, но разрешили принести только отвёртку и пользоваться ею лишь с 13:00 до 14:00.

Ограничение инструментов средствами управления доступом работает лишь тогда, когда ИТ-команда готова серьёзно снизить собственную эффективность. Но даже в этом случае само существование повседневных инструментов в целевой системе несёт неизбежную опасность: специалисты по кибербезопасности видели, как субъекты угроз без труда освобождают инструменты из локальных ограничений. Кибербезопасности присущ следующий факт: пока существуют подобные мощные средства, сохраняется и возможность злоупотребления ими.

Защита инструментов

Парадокс владения инструментами заключается в том, что они нужны для работы и вам, и противнику. Один из подходов к этой проблеме - сократить количество, функции, доступность и возможность доступа к инструментам до абсолютного минимума. Такая стратегия несколько осложнит работу в собственной среде, но при достаточных средствах безопасности должна ещё сильнее затруднить действия возможного противника. Один недостаток подхода состоит в ослаблении устойчивости и надёжности возможностей удалённо управлять средой. Поэтому, если противник скомпрометирует важнейшие инструменты, удалив или сломав их, ваша собственная защита может помешать управлять системой и восстанавливать её. Следующие шаги послужат хорошим началом защиты инструментов:

1. **Определите исходный уровень.** Проведите опрос сотрудников по ролям и аудит инвентарного списка программ во всех системах организации. Задокументируйте исчерпывающий перечень пользователей, номеров версий и местонахождения в системах для каждого инструмента среды, включая все программы и приложения, сценарии, библиотеки, системы и роли. Сюда относятся файлы ОС и системы, например:

```
sc.exe           find.exe        sdelete.exe      runasuser.exe
net.exe          curl.exe        psexec.exe       rdpclip.exe
powershell.exe   netstat.exe     wce.exe          vnc.exe
ipconfig.exe     systeminfo.exe  winscanx.exe     teamviewer.exe
netsh.exe        wget.exe        wscript.exe      nc.exe
tasklist.exe     gpresult.exe    cscript.exe      ammyy.exe
rar.exe          whoami.exe      robocopy.exe     csvde.exe
wmic.exe         query.exe       certutil.exe     lazagne.exe
```

2. **Изучите результаты и оцените потребности.** Оцените каждый инструмент и определите, каким пользователям, как, где и когда он нужен. Для каждого средства проведите оценку риска и определите возможные последствия его получения противником. Задокументируйте, как ограничить возможности инструмента ради повышения безопасности, предусмотрев обоснованные компромиссы для деловой деятельности, например отключение макросов в Microsoft Word и Excel.
3. **Внедрите ограничения.** Ограничьте доступность, доступ и авторизацию для неоправданно рискованных инструментов. Задокументируйте все исключения и запланируйте их ежеквартальный пересмотр, заставляя пользователей заново запрашивать разрешение. Можно даже предоставлять временный доступ, который по истечении срока автоматически отзывается, либо удалять инструменты. Составьте белый список разрешённых средств, чтобы доставка любых нераспознанных или несанкционированных инструментов в системы блокировалась автоматически. Подумайте о физической блокировке всех портов USB, носителей, Thunderbolt, FireWire, консольных и внешних портов во всех системах, требуя письменного разрешения на их разблокировку и использование.

> **Упражнение «Теория замка».** Представьте, что вы правитель средневекового замка, внутри которого находятся ценные ресурсы. В вашем поместье производятся редкие закрытые нити, необходимые для изготовления и ремонта тканей на месте. Их также продают за значительные суммы, и этот доход сохраняет прибыльность владений. Вы получаете достоверные разведывательные сведения о том, что синоби намерен проникнуть в замок и отравить иглу веретена прялки, но неизвестно, кого он выбрал целью и чего желает добиться.
>
> Смоделируйте сценарии угроз, при которых кто-либо может уколоться иглой веретена. Затем разработайте меры, снижающие вероятность и последствия укола. Например, можно затупить иглы или заставить людей в прядильной комнате носить защитные перчатки. Можно ли переставить прялку так, чтобы работникам было труднее случайно наткнуться на иглу или задеть её? Как ограничить перенос игл для веретена внутри замка и какую защиту цепочки поставок внедрить для поступающих новых игл? Сколько способов не допустить вредоносного применения отравленной иглы вы сможете придумать? Какими другими острыми инструментами работники могут заменить иглы и следует ли закрыть к ним доступ? Можно ли вообще переделать прялку так, чтобы она работала без иглы?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую из них следует оценивать с учётом понятия инструментов.

1. Оцените техническую возможность обеспечить «принцип минимальной функциональности», отключая и удаляя ненужные программы и системные функции среды и ограничивая доступ к ним. [CM-7: Least Functionality]
2. Периодически проверяйте функции, инструменты и программы каждой роли и системы, определяя, необходимы ли они или их можно удалить либо отключить. Создайте систему регистрации, отслеживания и управления этими средствами. [CM-7: Least Functionality | (1) Periodic Review | (3) Registration Compliance]
3. Задокументировав каждый инструмент, которым может воспользоваться пользователь или система, запретите пользователям применять их для функций, выходящих за пределы их роли в организации. [CM-7: Least Functionality | (2) Prevent Program Execution]
4. Внедрите белый или чёрный список программ, приложений и других инструментов либо оба списка. [CM-7: Least Functionality | (4) Unauthorized Software/Blacklisting | (5) Authorized Software/Whitelisting]
5. Введите физические и сетевые граничные ограничения для аппаратных и программных инструментов. Например, храните критически важные средства на файловом сервере отделённой сети управления или на переносных запираемых носителях и предоставляйте доступ лишь по необходимости в сочетании со средствами JEA/JIT. [MA-3: Maintenance Tools | (1) Inspect Tools | (3) Prevent Unauthorized Removal | (4) Restricted Tool Use; SC-7: Boundary Protection | (13) Isolation of Security Tools/Mechanisms/Support Components]
6. Оцените всё установленное программное обеспечение и определите импорты, API, вызовы функций и перехваты, которыми пользуются приложения, признанные безопасными. Рассмотрите применение защиты от вредоносного кода для блокировки любых инструментов, использующих эти реализации или другие механизмы, не применяемые обычными программами. Рассмотрите способы ограничить, отключить и удалить функции, модули, компоненты и библиотеки ОС, не используемые в деловой деятельности. [SA-15: Development Process, Standards, and Tools | (5) Attack Surface; SI-3: Malicious Code Protection | (10) Malicious Code Analysis]

Разбор

В этой главе вы узнали об инструментах - насколько они могущественны и почему их важно оберегать. Вы познакомились с «жизнью за счёт окружения» и сложностью создания одновременно защищаемых и работоспособных систем. Возможно, вы также начали размышлять о различиях между инструментами и вредоносным ПО и о том, как запрограммировать средство на их распознавание. Мысленное упражнение с отравленной иглой веретена заставило вас перехитрить врага, вторгающегося в подконтрольную вам среду.

В следующей главе мы обсудим различные приёмы разведчиков-синоби - обоняние, зрение и слух - и то, чему они могут нас научить, особенно при применении разных видов цифровых датчиков в киберсреде.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), p. 17.
[2] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), pp. 188, 342.
[3] [назад] Antony Cummins and Yoshie Minami, *True Path of the Ninja* (North Clarendon, VT: Tuttle Publishing, 2017), p. 101.
[4] [назад] Cummins and Minami, *True Path*, p. 112.
[5] [назад] Cummins and Minami, *The Book of Ninja*, p. 317.
[6] [назад] «Sword hunt», Wikipedia, Wikimedia Foundation, последнее изменение 26 ноября 2018 г., https://en.wikipedia.org/wiki/Sword_hunt.
[7] [назад] Cummins and Minami, *The Book of Ninja*, p. 189.
[8] [назад] Cummins and Minami, *The Book of Ninja*, p. 342.

Глава 9. Датчики

> Днём и ночью следует высылать разведчиков для дальнего наблюдения.

> Даже если синоби не обладает впечатляющими физическими способностями, помните: важнее всего иметь острую наблюдательность.
>
> - «Ёсимори хякусю», стихотворение 11

Помимо размещения стражников у ворот и солдат на наблюдательных постах, «Бансэнсюкай» рекомендует защищать замок, скрытно расставляя разведчиков вдоль дорог, троп и других подходов. Обороняющийся командир должен размещать разведчиков через неодинаковые промежутки по периметру замка.[1] Эти разведчики исполняли одну из трёх ролей:

• разведчики по запаху (*каги*);
• разведчики по слуху (*моногики*);
• внешние пешие разведчики (*тогики*).

Разведчики по запаху и слуху, пользовавшиеся обученными собаками и услугами собаководов, располагались на укрытых наблюдательных постах: они не могли видеть наружу, но и враг не мог заглянуть внутрь. Разведчик напряжённо вслушивался или принюхивался в поисках признаков проникновения. Эти приёмы особенно хорошо действовали ночью, поскольку разведчикам по запаху и слуху для работы не требовался свет.[2]

Внешние пешие разведчики пытались ловить лазутчиков, прочёсывая границу вражеской территории; скрываясь на вражеской земле и наблюдая за движением к собственному лагерю; либо выявляя нарушителей растяжками, шумом и даже физическим контактом. Согласно «Бансэнсюкай», разведчики *тогики* сами должны быть синоби, поскольку им требуются мастерство скрытности и наблюдения, сверхъестественное понимание направления, с которого нападёт враг, и способность успешно обнаружить вражеского ниндзя и вступить с ним в бой.[3]

Помимо разведчиков-людей и животных «Бансэнсюкай» рекомендует активные и пассивные приёмы обнаружения вражеских лазутчиков. При активном обнаружении синоби мог опустить или раскачать *саруби* - «обезьяний огонь», или «огонь на верёвке»[4] - внутри тёмного места либо поперёк него, например над рвом, траншеей или у подножия замковой стены. Так он быстро и динамично освещал место издалека, что было невозможно с неподвижным фонарём. Для пассивного обнаружения синоби строили системы: например, засыпали широкую, но мелкую траншею мелким песком, а затем разравнивали его сложным рисунком. Враг, обошедший внешнюю оборону, оставил бы следы и тем самым предупредил стражу о проникновении в замок. Следы на песке могли также сообщить наблюдательному синоби, откуда пришёл враг и ушёл ли он тем же путём, - ценные разведывательные сведения, помогающие нейтрализовать непосредственную угрозу и укрепить будущую защиту.[5]

В этой главе мы рассмотрим разные виды защитных датчиков, которые обычно применяются в сетях, и сопоставим современное развёртывание с историческими способами использования датчиков синоби. Мы уделим внимание размещению датчиков и приёмам противодействия им, учась у синоби совершенствовать собственную защиту киберсреды. Мы также предложим датчики, основанные на разведчиках древности, пользовавшихся органами чувств.

Выявление и обнаружение угроз с помощью датчиков

На языке кибербезопасности термин *датчик* охватывает разнообразные системы и приборы обнаружения. Чаще всего датчик представляет собой устройство наблюдения на ответвителе, Т-разветвителе, порте SPAN или зеркальном порте, которое копирует активность для наблюдения, записи и анализа. В одной из таких конфигураций датчики перехватывают и сохраняют необработанные пакеты (PCAP), проходящие по линии, а затем обрабатывают и анализируют их, предупреждая службу безопасности о подозрительных событиях. Датчики можно также располагать «в разрыв»: тогда пакет проходит через устройство, способное задержать, заблокировать или изменить содержащиеся в нём сведения, что позволяет действительно сорвать нападение, а не просто поднять тревогу. Вторичные датчики, например датчики Wi-Fi, обнаруживают внешние или иные несанкционированные сигналы и соединения, а датчики физической защиты, например камеры, наблюдают за доступом к критически важным центрам обработки данных, серверным стойкам и коммутационным шкафам. В более широком смысле некоторые программные агенты конечных устройств тоже действуют как датчики: они собирают события, действия и активность основной системы и сообщают их системе командного управления (C2), которая при необходимости анализирует данные и поднимает тревогу.

Организации часто выделяют датчики для определённых видов трафика: например, настраивают защитные устройства почтового шлюза на выявление фишинга и спама, системы предотвращения и обнаружения вторжений - на сетевые атаки, межсетевые экраны - на несанкционированные IP-адреса и порты, прокси - на подозрительные сайты, а системы предотвращения утечки данных - на потерю данных. Устройства кибербезопасности на основе датчиков обычно устанавливают в главной точке выхода из сети, как правило, в демилитаризованной зоне (DMZ). Поскольку датчики принято размещать как можно выше в сети, чтобы увеличить объём наблюдаемого трафика, противник, который скроется от датчиков на шлюзе или обойдёт главный выход посредством моста в сеть, сможет действовать внутри неё без проверки защитными датчиками.

Несмотря на такую слабость защиты, большинство организаций едва ли резко увеличит число датчиков в системах: покупка множества дополнительных устройств вместе с работой по их лицензированию, установке, обновлению, обслуживанию и наблюдению финансово непрактична. К сожалению, многие организации попросту полагают: если главный датчик на выходе не поймал угрозу, большее число таких же датчиков не будет эффективнее. Это ошибочное суждение подвергает их системы риску.

Более совершенные датчики

Главная проблема датчиков заключается в том, что почти всегда нужен человек, который будет за ними следить и действовать по переданным сведениям. Проблема усугубляется ограничениями защитных датчиков и доступных аналитических платформ. Представьте современные защитные датчики следующим образом. По зданию разбросано множество крошечных микрофонов и камер, но все они заключены в маленькие соломинки, сужающие область захвата. А теперь вообразите, что пытаетесь сложить картину продолжающегося взлома, имея возможность смотреть лишь через одну соломинку за раз. Кроме того, в каждой соломинке накапливаются тысячи часов данных, которые нужно хранить, обрабатывать и анализировать. Эту удручающую ситуацию часто облегчают сигнатуры, алгоритмы или машинное обучение - средства, помогающие выявлять аномалии и вредоносную активность. Но автоматизированные системы несовершенны. Они часто создают ложные срабатывания или настолько огромный поток обоснованных предупреждений, что это почти не отличается от полного отсутствия датчиков. Для устранения этих проблем можно позаимствовать приём у синоби: определить вероятные пути врага и скрыть вдоль них датчики разных типов, обеспечив раннее предупреждение об атаках. При совершенствовании датчиков организации примите во внимание следующие рекомендации:

1. **Смоделируйте сеть и выявите слабые места.** Создайте карту сети и модель потоков информации среды, описывающую каждую систему и её назначение, соединения систем, точки входа и выхода информации из сети, вид получаемых сведений, датчики, если они есть, которые их проверяют, и точки выхода. Выявите участки без датчиков и места, которые, по вашему мнению, контролируются правильно. Предскажите, где субъекты угроз попытаются проникнуть в сеть. Помните, что на создание исчерпывающей карты могут уйти месяцы и потребуется помощь всего предприятия. Полученная карта может оказаться несовершенной, но даже карта с изъянами лучше её полного отсутствия.
2. **Проведите испытания красной команды и испытания на проникновение.** Наймите красную команду для попытки проникнуть в сеть. Подумайте о проведении упражнения «фиолетовой команды», при котором защитники сети - синяя команда - наблюдают за красной командой в реальном времени в той же комнате и могут приостановить упражнение, чтобы задать вопросы. Опросите защитные датчики до, во время и после нападения и выясните, что они обнаружили или сообщили, если сообщили вообще. Эти сведения должны оказаться чрезвычайно поучительными. Позвольте синей команде подумать, как иное размещение датчиков помогло бы быстрее и точнее обнаружить красную. Обсудите предлагаемые испытанием изменения архитектуры защиты, настройку датчиков и другие решения.
3. **Обнаруживайте и блокируйте зашифрованный трафик.** Блокируйте весь зашифрованный трафик, который невозможно перехватить и исследовать датчиками. Примите также необходимые меры, чтобы лишить компьютеры возможности использовать несанкционированное шифрование. Попросите красную команду проверить вашу способность обнаруживать атаки по зашифрованному трафику. Большинство датчиков не может исследовать зашифрованный трафик, поэтому многие организации разрешают асимметричное шифрование, например эллиптический протокол Диффи-Хеллмана (elliptic-curve Diffie-Hellman, ECDH), который нельзя раскрыть корневыми сертификатами. Разрешение нераскрытого зашифрованного трафика на выход из организации без прохождения DLP создаёт пробел в безопасности, подобный ситуации, когда замковая стража тщательно проверяет каждого человека с открытым лицом, входящего или выходящего через ворота, но беспрепятственно пропускает любого в маске.

4. **Разрабатывайте датчики по запаху и слуху.** Исследуйте возможности создания датчиков, которые могут тайно обнаруживать определённые виды активности угроз. Например, настройте внешний физический датчик, наблюдающий за активностью процессора или энергопотреблением системы и способный выявлять несанкционированный доступ или использование - например, майнером криптовалюты - по тому, соответствует ли производительность известным командам или активности вошедшего пользователя.
5. **Внедрите пассивные датчики.** Создайте пассивные интерфейсы на коммутаторах и серверах, которые никогда не должны использоваться. Настройте также датчики на локальное обнаружение и предупреждение при активации интерфейса, указывающей на вероятное присутствие противника в сети. Подобно мелкой траншее с песком, такие системы способны выявлять боковое перемещение между сетевыми устройствами там, где его быть не должно.
6. **Установите датчики тогики.** Разместите за пределами сети обращённые внутрь датчики для выявления проникновения. Например, при содействии ISP настройте датчики за сетевой границей, чтобы наблюдать за входящим и исходящим трафиком, который могут не заметить остальные датчики. Разместите датчик на Т-разветвителе непосредственно у устройства, где он будет работать совместно с узловым датчиком, а затем сравнивайте различия между ними и определяйте, сообщают ли оба об одной активности. Такой подход помогает выявлять скомпрометированные датчики конечных устройств и драйверы сетевых интерфейсов.

> **Упражнение «Теория замка».** Представьте, что вы правитель средневекового замка, внутри которого находятся ценные ресурсы. За последнюю неделю в замке произошло три поджога, хотя пожарный дозор был наготове и успевал потушить пламя до распространения. Вы считаете поджигателя синоби, который изучил реакцию вашей команды и совершит новое нападение, возможно даже не связанное с огнём. Ресурсов мало, но пожарный дозор просит больше людей и оборудования для лучшего реагирования; архитектор желает усилить и защитить от огня части замка; а начальник службы безопасности требует больше стражников у ворот, чтобы поймать лазутчика.
>
> Как спрятать датчики для обнаружения поджигателя или других подозрительных лиц внутри замка? Можно ли ускорить и усилить реакцию пожарного дозора, сократив его численность, например используя людей как датчики, а не как участников реагирования? Где и как разместить людей-датчиков, чтобы они как можно эффективнее обнаруживали подозрительную деятельность и предупреждали остальных? Как перемещать стражников периметра между прочёсыванием внутренней и внешней территории замка и как расширить их возможности, чтобы противник не смог определить время и место патрулирования? Какие пассивные датчики помогут поймать поджигателя?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую из них следует оценивать с учётом понятия датчиков.

1. Внедрите анализаторы пакетов, полный сбор сетевых PCAP и другие автоматизированные датчики для поддержки обработки инцидентов, обслуживания и обеспечения соблюдения правил потоков информации. [AC-4: Information Flow Enforcement | (14) Security Policy Filter Constraints; IR-4: Incident Handling; MA-3: Maintenance Tools]
2. Для защиты физического доступа и обнаружения вмешательства установите датчики на замках коммутационных шкафов, камеры для наблюдения за доступом к центру обработки данных и серверам, датчики воды для обнаружения протечек, угрожающих электрическим устройствам, и датчики прослушивания на линиях связи. [PE-4: Access Control for Transmission; PE-6: Monitoring Physical Access; PE-15: Water Damage Protection]
3. Проводите для сотрудников, включая персонал вне ИТ, программы повышения осведомлённости, чтобы они могли действовать как люди-датчики и выявлять активность угроз. Предоставьте сотрудникам ясный, простой и доступный способ сообщать о подозрительной деятельности. [PM-16: Threat Awareness Program]
4. Перехватывайте зашифрованный обмен и позволяйте датчикам проводить глубокое исследование расшифрованных пакетов. [AC-4: Information Flow Enforcement | (4) Content Check Encrypted Information; SC-8: Transmission Confidentiality and Integrity]
5. Внедрите датчики, способные анализировать пакеты и принимать предупредительные меры, например блокировать или фильтровать. [SC-5: Denial of Service Protection; SC-7: Boundary Protection | (10) Prevent Exfiltration | (17) Automated Enforcement of Protocol Formats]
6. Запретите включать неразборчивый режим датчика в системах, не предназначенных для наблюдения, чтобы не допустить раскрытия критически важных сведений противнику, получившему несанкционированный доступ. [SC-42: Sensor Capability and Data]
7. Совместно с ISP разместите датчики Trusted Internet Connection (TIC) за границей сети. [AC-17: Remote Access | (3) Managed Access Control Points]
8. Задокументируйте все внутренние соединения систем, их интерфейсы, обрабатываемые, хранимые и передаваемые ими сведения и размещение датчиков между системами. [CA-9: Internal System Connections]
9. Проводите испытания на проникновение и упражнения красной команды, чтобы испытывать и подтверждать размещение и возможности датчиков. [CA-8: Penetration Testing; RA-6: Technical Surveillance Countermeasures Survey]

Разбор

В этой главе мы поговорили о разведчиках по запаху, слуху и внешнему наблюдению, которых в древней Японии использовали для обнаружения вражеских синоби. Мы также рассмотрели активные и пассивные датчики, которые замковая стража развёртывала для поимки нарушителей. Затем обсудили разнообразные виды современных защитных датчиков, помогающих защитникам видеть происходящее на окружающих линиях. Мы разобрали несколько организационно-технических проблем датчиков, в том числе их размещение, ложные срабатывания и управление. Наконец, мы поговорили о применении древних приёмов синоби для выявления нарушителей в сетевых системах.

Далее мы обсудим различные мосты и лестницы, которыми синоби обходили замковую оборону, - понятие, имеющее определённое значение и для датчиков. Представьте, например, что замок защищён рвом, а все датчики размещены у подъёмного моста. Вражеский синоби, способный тайно установить собственный мост и не пользоваться подъёмным, заодно обходит датчики, делая их бесполезными. Мы исследуем, насколько точно это понятие моста переносится в кибербезопасность и как трудно бывает справиться с проблемой.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), p. 96.
[2] [назад] Cummins and Minami, *The Book of Ninja*, p. 96.
[3] [назад] Cummins and Minami, *The Book of Ninja*, p. 97.
[4] [назад] Cummins and Minami, *The Book of Ninja*, p. 90.
[5] [назад] Cummins and Minami, *The Book of Ninja*, p. 91.

Глава 10. Мосты и лестницы

> Не останется ни стены, ни рва, через которые вы не сумеете перебраться, сколь бы высоки или круты они ни были, особенно если воспользоваться лестницей ниндзя.

> Караульное помещение у замковых ворот обычно охраняется строже всего, но его крыша - самое удобное место, чтобы закрепить крючковую лестницу.
>
> - «Бансэнсюкай», «Ин-нин II»[1]

Синоби могли тихо и незаметно перемещаться над вражескими стенами и воротами, используя инструменты проникновения *нинки*, описанные и в «Бансэнсюкай»,[2] и в «Гунпо дзийосю».[3] Многофункциональные лестницы и переносные мосты, такие как шипованная лестница, облачная лестница или проволока для перемещения инструментов,[4] позволяли синоби пересекать рвы, взбираться на стены и безопасно и скрытно передавать инструменты другим синоби. Иногда эти лестницы были «настоящими», то есть заранее изготовленными синоби перед заданием, а иногда «временными», сооружёнными на месте.[5] Это были ценные инструменты, поскольку открывали доступ к критически важным местам, которые часто оставляли без охраны из-за чрезмерной уверенности в их недоступности.

В свитках также объясняется, как проникнуть во вражеский лагерь, манипулируя защитными мерами самого врага. «Сёнинки» предлагает синоби представить, как птица или рыба могла бы попасть в замок,[6] - иными словами, осознать особые преимущества, которые дают большая высота или глубина. Например, взобравшись на стену, можно с огромной скоростью переходить по мостам через другие стены и крыши и получить лучший доступ во внутреннюю часть замка, чем через ворота. Переплыв ров, можно под водой попасть в общий водный путь, ведущий внутрь замка. «Бансэнсюкай» даже рекомендует намеренно пытаться проложить мост над воротами караульного помещения, где логично ожидать больше всего стражников, поскольку защитники могут предположить, что атакующие не станут пытаться проникнуть именно здесь.[7]

В этой главе мы обсудим сходство мостов между сетевыми областями и мостов через периметры замковых стен. Как и стены замка, сети проектируются с преградами и сегментацией в предположении, что всякий обязан проходить через контролируемый шлюз. Мосты позволяют угрозам обойти шлюзы, а вместе с ними и средства безопасности, установленные в точках выхода. На первый взгляд очевидная мера - например, велеть страже задерживать каждого, кто строит мост через замковый ров, - может оказаться бесполезной, если архитектор замка соединил концентрические кольца рвов ради управления водой. Три соединённых рва уже не являются тремя отдельными границами, которые должен пересечь противник. Они превращаются в водный мост, по которому можно вплавь добраться прямо до сердца замка. Умение мыслить как синоби и видеть в преградах возможные точки крепления лестниц поможет заново оценить собственную сеть и заранее устранить возможности для мостов.

Мосты через границы сети

Для специалистов по кибербезопасности мост - это виртуальное или физическое сетевое устройство, работающее одновременно на физическом и канальном уровнях - уровнях 1 и 2 модели OSI - и соединяющее два сегмента сети в одну совокупную сеть. Термин также обозначает любое устройство, инструмент или способ, позволяющий сведениям пересечь «разрыв», например воздушный зазор сети или границу сегментации. Мосты обычно обходят средства безопасности и защиты, позволяя выводить данные из сети или доставлять в неё несанкционированные либо вредоносные данные. Эти потенциально тяжёлые последствия побудили специалистов по кибербезопасности разработать способы обнаружения и смягчения для предотвращения мостов, в том числе:

- отключение сетевых мостов на беспроводных платах Ethernet;
- отключение систем с двумя или более активными сетевыми интерфейсами;
- внедрение средств управления доступом к сети (NAC) и наблюдение для выявления новых устройств в сети;
- установка датчиков для обнаружения несанкционированных точек доступа Wi-Fi;
- ограничение определённых сетей с помощью VLAN или других технологий маршрутизаторов;
- применение аутентификации в протоколе обнаружения канального уровня (Link Layer Discovery Protocol, LLDP).

Несмотря на развитие средств безопасности, несанкционированные мосты по-прежнему возникают, а некоторые передовые приёмы проникновения, пока доказанные только в научных или лабораторных условиях, демонстрируют огромный вредоносный потенциал. Среди последних примеров - захват управления системными светодиодами для передачи битов миганием оптическому приёмнику в другой комнате или здании; применение сигналов FM-диапазона для связи с ближайшими телефонами, как в эксплойтах AirHopper и GSMem; управление вентиляторами и их пульсация для акустической передачи битов; искусственный нагрев и охлаждение процессоров для медленной отправки данных, как в эксплойте BitWhisper. Субъекты угроз способны даже прокладывать мосты между сетями через кабели питания системы посредством Ethernet по электропроводке (Ethernet over power, EOP; не путать с питанием по Ethernet - power over Ethernet, POE). В других случаях микрофоны и динамики телефонов VoIP организации можно включить удалённо, что позволит противнику передавать звуковые данные или подслушивать разговоры.

Разумеется, некоторые мосты не столь передовые. Противник может забраться на крышу офисного здания, врезаться в доступные сетевые провода и установить небольшую наземную спутниковую станцию, обеспечивающую надёжный мост в сеть. Смартфоны постоянно подключают к системным USB-портам для зарядки, но заряжающийся телефон одновременно соединяет компьютер с внешней сотовой сетью, которая не проверяется межсетевыми экранами, DLP и другими средствами безопасности; так он полностью обходит защиту организации и упрощает кражу данных или внедрение кода в основную сеть. При переносе данных «на кроссовках» пользователь загружает сведения на переносной носитель и относит его к другому компьютеру или в другое сетевое место, вручную обходя средства безопасности. Существуют также опасения, что угрозы могут пользоваться скрытой сетью управления, обычно расположенной в сети `10.0.0.0/8` и напрямую соединённой с консолями маршрутизаторов, межсетевых экранов и других защитных систем. Они способны превратить эти устройства в промежуточные точки для мостов между разными VLAN и сегментами, фактически заставив сеть обходить собственную защиту. Кроме того, риск создаёт раздельное туннелирование: сведения могут утекать в разные сети и из них через устройство, одновременно подключённое к обеим.

Зрелые организации исходят из предположения, что противники непрерывно разрабатывают разные технологии мостов для обхода защиты новыми, непредвиденными способами. По всей видимости, жизнеспособным средством наведения мостов через сети и воздушные зазоры может стать всё в электромагнитном спектре, включая акустические, световые, сейсмические, магнитные, тепловые и радиочастотные явления.

Противодействие мостам

Предотвратить мосты между системами, изначально предназначенными для соединения с другими системами, - сложная задача. Совершенного решения нет, но можно сократить возможности для мостов и сосредоточить изоляцию на важнейших ресурсах. Кроме того, контрмеры, лишающие приёмы наведения мостов работоспособности, можно накладывать друг на друга, повышая эффективность защиты.

1. **Выявите слабые места.** Определите сети и информационные системы, где хранятся конфиденциальные, критически важные или особо ценные данные организации. Создайте диаграмму потоков данных (DFD), моделирующую хранение и движение сведений в системе. Затем выявите участки, где возможна скрытая атака посредством моста вне основного канала.
2. **Внедрите контрмеры против мостов.** Рассмотрите внедрение средств TEMPEST,[8] таких как клетки Фарадея или экранированное стекло, чтобы блокировать наведение мостов через воздушные зазоры посредством излучения или других сигналов. Чтобы блокировать чужие мосты, обязательно идентифицируйте и аутентифицируйте устройства, прежде чем разрешать им подключаться к сети или другому устройству. Разработайте надлежащие защитные меры для смягчения возможных угроз мостов, выявленных в модели угроз.

> **Упражнение «Теория замка».** Представьте, что вы правитель средневекового замка, внутри которого находятся ценные сведения, сокровища и люди. Вы получаете достоверные разведывательные сведения о том, что синоби применял специальные крючковые лестницы и облачные мосты, чтобы незаметно для стражи у ворот переносить людей или предметы через замковые стены.
>
> Подумайте, как перестроить стены замка для обнаружения лестниц и мостов и/или предотвращения их применения в обход стен. Можно ли предсказать, где синоби попытается проложить мост через защиту? Как изменить протоколы осмотра стражников и приказать им искать временные мосты? Как вы отреагируете, узнав о преодолении периметра, и как приспособитесь к работе в предположении, что внутренняя среда была изменена и, возможно, не заслуживает доверия?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую из них следует оценивать с учётом понятия мостов.

1. Внедрите защиту границ и управление потоками информации, чтобы внешние устройства, системы и сети не могли выводить данные или переносить вредоносный код в вашу сеть. [AC-4: Information Flow Enforcement | (21) Physical/Logical Separation of Information Flows; AC-19: Access Control for Mobile Devices; AC-20: Use of External Information Systems | (3) Non-Organizationally Owned Systems/Components/Devices; SC-7: Boundary Protection]
2. Обеспечьте соблюдение правил защиты беспроводного доступа, чтобы блокировать или обнаруживать несанкционированные беспроводные сигналы, наводящие мосты через сети на микроволновых, UHF/VHF, Bluetooth, 802.11x и других частотах. [AC-18: Wireless Access; SC-40: Wireless Link Protection]
3. Проводите аудит сетевого доступа и межсоединений, выявляя внешние сети и системы - например, удалённые сетевые принтеры, - которые способны передавать данные через мост в вашу сеть. [CA-3: System Interconnections; CA-9: Internal System Connections]
4. Установите строгие правила для переносных носителей, чтобы предотвращать несанкционированные мосты. Требуйте идентификации и аутентификации внешних носителей и устройств, прежде чем разрешать чему-либо подключаться к среде. [IA-3: Device Identification and Authentication; MP-1: Media Protection Policy and Procedures; MP-2: Media Access; MP-5: Media Transport]
5. Испытывайте системы на утечку TEMPEST и другие сигналы вне основного канала. По результатам определите места для внедрения защиты, которая не позволит использовать сигнал как мост. [PE-19: Information Leakage; SC-37: Out-of-Band Channels]

Разбор

В этой главе мы поговорили о философии вражеского наведения мостов, соединении сегментов сети и традиционных передовых методах. Мы рассмотрели многочисленные приёмы наведения мостов - мосты, способные преодолевать разрывы способами, о которых вы, возможно, прежде не задумывались. Мысленное упражнение этой главы было призвано побудить к размышлению о сооружении физических средств защиты между лестницами и стенами; теоретически такие идеи могут стать основой для новаторской современной защиты входов и выходов системы.

В следующей главе мы обсудим замки и практику вскрытия замков синоби, основанную на убеждении, что любой замок, созданный человеком, может быть вскрыт человеком. Мы также увидим подход синоби к безопасности, когда ему приходится полагаться на замок, которому он сам не доверяет. Мы обсудим применение замков в кибербезопасности и то, чему можно научиться у синоби для совершенствования подхода к замкам и их вскрытию.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), p. 183.
[2] [назад] Cummins and Minami, «Ninki I - Ninja Tools I», in *The Book of Ninja*, pp. 317-325.
[3] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), pp. 104-105.
[4] [назад] Cummins and Minami, *The Book of Ninja*, pp. 318-320.
[5] [назад] Cummins and Minami, *The Book of Ninja*, p. 317.
[6] [назад] Antony Cummins and Yoshie Minami, *True Path of the Ninja* (North Clarendon, VT: Tuttle Publishing, 2017), p. 82.
[7] [назад] Cummins and Minami, *The Book of Ninja*, p. 29.
[8] [назад] *TEMPEST Equipment Selection Process*, NCI Agency, по состоянию на 25 сентября 2018 г., https://bit.ly/2LfB3SK.

Глава 11. Замки

> Нет навесного замка, который вы не могли бы открыть. Однако всё зависит от вашего мастерства, поэтому всегда упражняйтесь на практике.

> Инструменты для открывания предназначены для того, чтобы вы могли легко отпереть двери вражеского дома. Поэтому из всех искусств это применяется ближе всего к врагу.
>
> - «Бансэнсюкай», «Нинки III»[1]

В древней Японии замки были проще современных запирающих устройств, поскольку производственные возможности того времени не позволяли изготавливать сложные штифты, сувальды и другие компоненты нынешних замков. И всё же старые замки отличались изящной конструкцией и образцово использовали «зубцы, защёлки и естественные силы тяжести и натяжения», оберегая ценности от нарушителей и воров.[2]

На заданиях синоби регулярно сталкивались со сложными замками и изобретали способы открыть каждый из них. Согласно свиткам, ни один замок, преграда или иной механизм не мог устоять перед синоби с качественно изготовленными инструментами, достаточной подготовкой, изобретательностью и оптимистическим образом мыслей. Значительные части всех трёх свитков документируют изготовление и применение разнообразных отмычек, прокладок и других щупов для открывания замков, дверей и ворот (рисунок 11-1).[3]

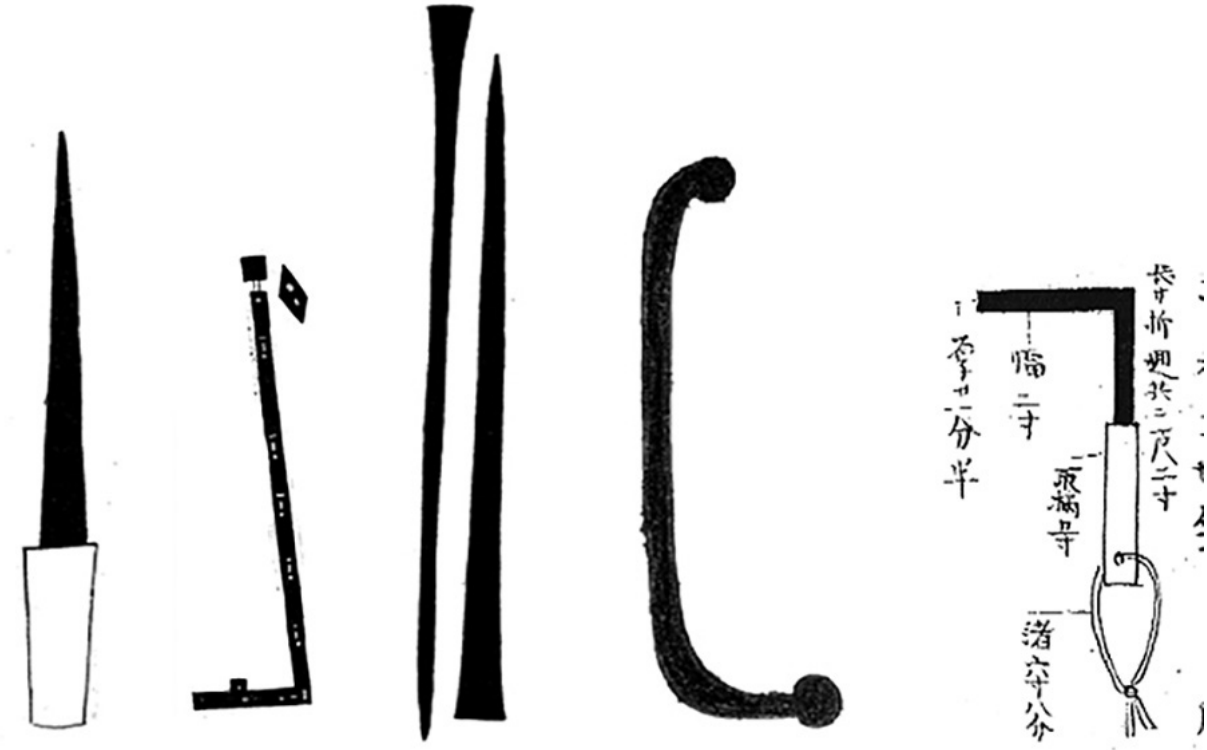

Рисунок 11-1. Разнообразные инструменты для открывания замков, дверей и ворот. Слева направо: железный щуп, выдвижной ключ, прокладки для вскрытия замков, отмычка для направляемых навесных замков и инструмент для открывания дверей («Бансэнсюкай» и «Нинпидэн»)

Кольцевые защёлки и верёвки, запирающие брусья, крючки и колышки, сложные замочные защёлки и примитивные самодельные приспособления - каким бы ни был замок, у синоби находились способы и инструменты для его обхода. По сути синоби умели преодолевать любую защитную

систему или средство сдерживания своего времени.[4] Понимая, что замкам нельзя полностью доверять, синоби сами разработали приёмы, позволявшие взять безопасность в собственные руки. Некоторые были предельно просты: ночуя в помещении, запертом ненадёжными, по их мнению, замками, синоби иногда привязывали нитку от двери или окна к узлу волос на макушке и непременно просыпались, если во сне кто-нибудь открывал дверную защёлку или замок.[5]

Сегодня, как и во времена синоби, люди защищают имущество замками, а субъекты угроз по-прежнему преодолевают их отмычками. Замок, как и всегда, служит нескольким целям. Он сдерживает. Представляет для владельца видимое заверение в сохранности имущества. Создаёт систему ответственности владельца или владельцев ключей, если замок был открыт ключом. Он также служит преградой и сигнализацией, поскольку воры потратят время и произведут шум, пытаясь его обойти. В этой главе мы обсудим, как хакеры, подобно синоби, по-прежнему вскрывают замки и обходят защиту. Кроме того, поговорим о значении физических замков для цифровых систем и подробно рассмотрим необходимые сопутствующие меры предосторожности. Мы также исследуем некоторые технологические достижения в замках и отмычках и узнаем, чему ещё синоби могут научить нас в вопросах безопасности.

Физическая безопасность

Подобно тому как вскрытие замков часто становится увлечением, открывающим дорогу к хакингу, преодоление замка служит распространённой точкой входа в кибербезопасность. Поиск недостатков в предмете, который должен быть защищён, или получение физического доступа к нему - видимая, осязаемая и слышимая обратная связь от открывающегося в руке замка после победы над его защитой - способны вызывать сильное чувство. Оно может пробудить интерес к сфере безопасности и укрепить уверенность в зарождающихся способностях.

Индустрия кибербезопасности применяет запирающие устройства, чтобы ограничивать физический доступ к зданиям, центрам обработки данных, коммутационным шкафам и отдельным кабинетам.[6] На более подробном уровне замки стоек ограничивают доступ к серверам, замки корпусов - к физическим компонентам системы, блокираторы портов не позволяют несанкционированно пользоваться USB или консольными разъёмами, тросовые замки мешают уносить системы с места, а блокираторы питания вообще не дают включить устройство. Ограничение физического доступа к системам - важнейшая часть стратегии кибербезопасности организации. Если системы уязвимы перед физическим вмешательством, многие цифровые средства защиты могут стать бесполезными, как только противник получит физический доступ. Следует считать, что, добравшись до компьютера физически, противник одновременно получает в системе полномочия администратора и находящиеся на ней данные.

Несмотря на распространение незаконных инструментов и приёмов вскрытия, организации год за годом пользуются одними и теми же замками, оставаясь чрезвычайно уязвимыми для нападения. В большинстве замков информационных систем и зданий используются слабые штифтовые цилиндры, например цилиндрический замок Yale, запатентованный в 1860-х годах и ставший самым распространённым в мире благодаря дешевизне и простоте массового производства, а также трубчатые, или «круглые», замки - самый распространённый вид велосипедного замка. Преступники изготавливают, продают и применяют инструменты, которые легко преодолевают эти серийные замки. Например, прокладка из банки газировки открывает замок рычагом, колпачок ручки имитирует трубчатый ключ, а пластиковый ключ можно легко напечатать на 3D-принтере по фотографии оригинала. За неквалифицированного преступника всю работу по вскрытию каждого штифта цилиндра за несколько секунд выполнит автоматическая электронная отмычка - достаточно нажать на спуск.

Масштабные контрмеры против вскрытия редки, а некоторые больше заботятся об ответственности, чем о безопасности. Например, отдельные страховые полисы не покрывают взлом и кражу, если во время преступления были вскрыты или обойдены некачественные замки - в том числе наиболее распространённые в США. Некоторые государства издают для производителей стандарты соответствия и запрещают продавать гражданам замки недостаточного качества. В сфере кибербезопасности отдельные государства защищают секретные системы и данные сочетанием кодовых или других высоконадёжных замков с дополнительными средствами безопасности, смягчающими недостатки замка.

Однако слишком многие двери и системы по-прежнему защищены слабыми замками и ключами, которые без труда преодолеет даже умеренно искушённый субъект угроз. Замки и преграды информационных систем необходимо совершенствовать, чтобы смягчить распространённые атаки: открывание прокладкой или отмычкой, кражу, копирование и силовой взлом.

Совершенствование замков

Вероятно, предотвратить любое вскрытие невозможно. Но существует множество предупредительных шагов, повышающих устойчивость замков. Совершенствование замков одновременно улучшит состояние кибербезопасности, смягчив атаки посредством несанкционированного физического доступа к системам.

- **Модернизируйте замки.** Оцените более совершенные запирающие системы, например европейские перфорированные замки, и определите, какие из них соответствуют деловым требованиям и бюджету. Получите одобрение заинтересованных лиц и команды физической безопасности, а затем замените все замки на более устойчивые к нападению модели.
- **Мыслите за пределами замка.** Рассмотрите нетрадиционные запирающие решения для организации, например многоступенчатые замки. Если механизм первой ступени управляет доступом к замку второй, нарушитель не сможет быстро и легко открыть оба одновременно или один сразу за другим.

  Например, закройте проход двумя независимыми запирающими системами, дополняющими друг друга. Первой ступенью может стать цифровой замок с четырёхзначным PIN, временно освобождающий штифты второй ступени - цилиндрического замка. Пока штифты второго замка зафиксированы, вскрыть их невозможно, но в ожидании активации первой ступенью можно вставить ключ. После краткого освобождения штифтов физический ключ поворачивается и проход отпирается. Однако это окно возможности открывается лишь на три секунды. Затем цифровой замок сбрасывается и снова фиксирует штифты. Для успеха нарушителю потребуется сначала узнать PIN, а потом вскрыть дверной замок менее чем за три секунды - возможно, физически недостижимый для человека результат.

• **Добавьте усиление.** Подумайте об укреплении предмета, который защищает замок. Можно защитить петли от вмешательства или установить ответные планки, усилители двери и коробки, щитки дверных ручек либо напольные ограничители.
• **Обратитесь к индустрии замков.** Призывайте индустрию к нововведениям и внедрению новых конструкций в изделия, защищающие информационные системы. Пока давление потребителей не станет достаточным для обновления устаревших продуктов, производители продолжат продавать то же привычное и уязвимое оборудование.

> **Упражнение «Теория замка».** Представьте, что вы правитель средневекового замка, внутри которого находятся ценные ресурсы. Вы знаете, что все ценности хранятся под замком и ключом - в сундуках и хранилищах, за дверями и воротами, - но также знаете, что синоби способен обойти все эти замки.
>
> Как усилить безопасность замков? Узнаете ли вы, что замок был открыт или обойдён? Как закрыть синоби доступ к замкам? Как настроить ложные замки, чтобы обмануть синоби и получить предупреждение о попытке проникновения?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую из них следует оценивать с учётом понятия замков.

1. Храните бумажные документы, магнитные ленты, жёсткие диски, флеш-накопители, диски и другие физические носители в запертых контролируемых контейнерах. [MP-4: Media Storage; MP-5: Media Transport]
2. Используйте защищённые ключи или другие запирающие устройства для обеспечения физического контроля доступа и авторизации к системам и среде. [PE-3: Physical Access Control | (1) Information System Access | (2) Facility/Information System Boundaries | (4) Lockable Casings | (5) Tamper Protection; PE-4: Access Control for Transmission Medium; PE-5: Access Control for Output Devices]

Разбор

В этой главе мы поговорили о замках и их назначении. Мы отметили, что противник любой эпохи будет разрабатывать инструменты и приёмы для обхода замков. Мы затронули распространённые технологии замков, которыми защищают доступ к системам, и важность их обновления. Особенно важно помнить: если противник получает физический доступ к системе, следует считать, что он способен её скомпрометировать, - отсюда значение физического предотвращения доступа к системам посредством замков.

В следующей главе мы обсудим передовой приём синоби для целей с чрезвычайно надёжными замками: он фактически заставлял противника самостоятельно отдать ключ. В некотором смысле защита организации не слишком отличается. Даже самый лучший замок не поможет, если вы отдадите ключ нарушителю.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), pp. 354-355.
[2] [назад] Cummins and Minami, «A Short Introduction to Japanese Locks and the Art of Lock-picking», in *The Book of Ninja*, pp. xxix-xxxii.
[3] [назад] Cummins and Minami, *The Book of Ninja*, p. 342.
[4] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), p. 34.
[5] [назад] Antony Cummins and Yoshie Minami, *True Path of the Ninja* (North Clarendon, VT: Tuttle Publishing, 2017), p. 102.
[6] [назад] Хотя замки в информационных системах и данных, несомненно, заслуживают обсуждения, в этой главе под замками понимаются физические замки, преграждающие доступ к информационным системам и среде.

Глава 12. Луна на воде

> Договорившись со своим господином, вы должны выманить врага приманкой, чтобы проникнуть сквозь его защиту.
>
> При этом следует манить врага соблазнительной наживкой, как при ловле рыбы в море или реке, чтобы враг, который обычно не выходит, действительно покинул свою защиту.
>
> - «Бансэнсюкай», «Ё-нин II»[1]

Словно образ из хайку, «Бансэнсюкай» называет один из приёмов проникновения под открытой маскировкой *суйгэцу-но дзюцу* - искусством «луны на воде».[2] У приёма было множество применений, но синоби прежде всего использовали его против сильно укреплённых вражеских лагерей, где людям запрещали выходить, входить и даже приближаться. Вместо силового преодоления защиты лагеря синоби выманивал цель и фактически обманом заставлял её раскрыть протоколы входа: знаки различия и другие опознавательные знаки, пароли, кодовые слова и сигналы типа «запрос-ответ». Этот приём также позволял синоби проследить за целями при возвращении в лагерь, выманить защитников с постов и беспрепятственно проникнуть внутрь либо непосредственно взаимодействовать с целями и проникать посредством обмана или наступательных действий.

Если цель особенно неохотно покидала тщательно укреплённую защиту, свиток предписывал синоби обратиться к своим командирам за помощью в сложной операции обмана.[3] Например, командир мог выдвинуть войска на уязвимые позиции, побуждая врага напасть и тем самым ослабить оборону настолько, чтобы синоби сумел проникнуть. Другой вариант - одолеть врага по возвращении, когда тот утомлён боем. Командир мог даже разыграть нечто более сложное, например начало полноценной длительной осады замка. Тогда синоби мог послать солдата под видом гонца союзного полководца, чтобы убедить врага покинуть замок, присоединиться к контрнаступлению и прорвать осаду. Для завершения уловки командир синоби отправлял небольшой отряд, изображавший союзное подкрепление: это одновременно выманивало цель из лагеря и позволяло синоби проникнуть внутрь, пока ворота открыты.

Согласно свитку, успешно проникнув к цели посредством *суйгэцу-но дзюцу*, синоби должен был помнить следующее:

• сохранять спокойствие и не выглядеть заблудившимся;
• подражать людям в замке;
• в первую очередь собирать кодовые слова, пароли, ответы на запросы и знаки различия;
• как можно скорее подать сигнал союзникам.[4]

В этой главе мы исследуем, как древний приём может применить субъект киберугроз, и сопоставим его с распространённой тактикой социальной инженерии. Мы предложим способ абстрактно рассматривать сигналы сетевого обмена как входящие в периметры и/или выходящие из них, хотя компьютерная система физически не перемещается, и подробно опишем понятия противодействия приёму луны на воде и атакам социальной инженерии вообще. Наконец, мы попробуем выполнить мысленное упражнение, имитирующее затруднение, с которым, должно быть, сталкивались древние японские полководцы, ставшие целью луны на воде.

Социальная инженерия

Атака синоби «луна на воде» поразительно похожа на современные атаки социальной инженерии, которые эксплуатируют процессы принятия решений и когнитивные искажения человека, заставляя его раскрывать критически важные сведения или совершать действия себе во вред. В кибербезопасности большинство приёмов социальной инженерии применяют противники, действующие на вражеской территории и эксплуатирующие доверие цели. К типичным атакам относятся:

- **Фишинг.** Противник отправляет письмо, убеждающее получателей открыть опасный документ или перейти по вредоносной гиперссылке, в результате чего происходит заражение вредоносным ПО, запуск программы-вымогателя, кража данных или иная атака.
- **Претекстинг.** Противник звонит или отправляет письмо с вымышленным сценарием, призванным убедить цель раскрыть критически важные сведения или совершить вредоносное действие.
- **Приманка.** Противник стратегически оставляет вредоносный переносной носитель, например USB-накопитель, в физическом месте, чтобы побудить цель поднять его и подключить к внутренним системам, открыв путь к компрометации.

Социальная инженерия представляет собой особенно сложную проблему безопасности, поскольку эксплуатирует человеческую природу способами, от которых не всегда защищают технические средства. По мере роста осведомлённости целей и жертв об угрозах социальной инженерии многие организации всё больше полагаются на специализированные технические средства, протоколы безопасности и обучение пользователей для защиты ценных ресурсов. Сотрудников учат правильно обращаться с критически важными сведениями и системами и заботиться о них, а службы безопасности документируют процедуры проверки личности неизвестных или незваных посетителей и требуют физически сопровождать посторонних на территории компании. Красные команды проводят среди прочих упражнений внутренние испытания на фишинг и проход «в хвосте», чтобы оценивать осведомлённость сотрудников и прививать им устойчивость к приёмам социальной инженерии. Администраторы внедряют технические средства для блокировки вредоносных документов и гиперссылок, применяют программы предотвращения утечки данных (DLP), не допускают несанкционированных изменений систем, вносят незарегистрированные системы и внешние носители в чёрный список и пользуются определителем номера.

Все эти меры безопасности хороши и необходимы, но способы работы людей изменились. При этом представления об атаках социальной инженерии ещё не развились настолько, чтобы в полной мере учитывать защиту от нападений в стиле луны на воде - тех, что пытаются выманить цель за пределы собственной защиты. Современные правила «принеси собственное устройство» (bring your own device, BYOD), постоянная удалённая работа и многопользовательские облака делают сотрудников и организации гибче. Однако они одновременно ослабляют традиционно надёжную архитектуру защиты периметра и подвергают сотрудников новым угрозам социальной инженерии. Например, правила межсетевого экрана с отслеживанием состояния в большинстве случаев не разрешают внешнему обмену из Интернета проходить через экран к внутреннему узлу. Сначала внутренняя система интрасети должна сама установить связь, и только тогда экран разрешит ответам внешней системы пройти к внутреннему узлу. Поэтому, хотя внутренний узел физически не покидает защиту организации, виртуальный выход - например, посещение вредоносного сайта - может позволить субъектам угроз проникнуть внутрь вместе с ответным обменом. По сути это цифровой проход «в хвосте».

Помимо непосредственной компрометации традиционной архитектуры защиты, субъекты угроз могут использовать для проникновения в тщательно укреплённые организации целый ряд приёмов в стиле луны на воде. Рассмотрим следующие сценарии:

- Противник включает пожарную сигнализацию в защищённом учреждении, заставляя сотрудников массово выйти. Пока пожарные проверяют здание, противник смешивается с толпой и крадёт или документирует пропуска, ключи, жетоны, лица, отпечатки пальцев и многое другое. Чтобы ускорить возвращение сотрудников к работе, учреждение временно отключает считыватели пропусков, турникеты и другие средства физического контроля доступа, либо службу безопасности настолько захлёстывает поток людей, что она не замечает проходящих «в хвосте».
- Противник использует фургон с едой, чтобы выманить сотрудников из защищённого учреждения. Затем, пользуясь тем, что не он начал взаимодействие, применяет к цели социальную инженерию по принципу взаимной услуги, со временем налаживает отношения и убеждает её совершить действия, которых она не выполнила бы в обычном сценарии социальной инженерии.
- Противник компрометирует сеть Wi-Fi в кафе напротив деловой конференции, чтобы похитить учётные данные сотрудников целевой организации. Войдя в кафе с устройствами, эти сотрудники покидают защиту организации и по незнанию оказываются в среде, контролируемой противником.
- Противник проводит масштабные нарушающие, блокирующие или разрушительные атаки на целевых людей, системы и данные, побуждая их переместиться на менее защищённую резервную площадку аварийного восстановления, куда проникнуть легче, чем в постоянную штаб-квартиру организации.

Учтите: хотя сами по себе такие атаки не обязательно достигают конечной цели противника, они способны предоставить средства или сведения, которые в сочетании с другими эксплойтами обеспечат выполнение вредоносных задач.

Защита от социальной инженерии

Большинство организаций проводит обучение по осведомлённости о социальной инженерии и регулярно испытывает сотрудников внутренним фишингом. Такая стратегия повышает устойчивость к атакам, но значительная доля персонала неизменно проваливает проверки. К сожалению, в большинстве организаций сотрудники остаются уязвимыми перед социальной инженерией. Нужно делать больше, предоставляя им средства защиты от подобного обмана.

1. **Установите защитные меры.** Внедрите для сотрудников стандартные модели доверия, снижающие риск компрометации социальной инженерией. Выявите особо ценные цели в среде, а затем установите протоколы, политики и процедуры безопасности для правильного контроля критически важных сведений в этих системах и обращения с ними; со временем распространите меры на все системы. Проводите в организации обучение, повышение осведомлённости и проверочные упражнения, чтобы сотрудники лучше понимали социальную инженерию; одновременно итеративно моделируйте угрозы, пересматривая и совершенствуя связанные средства безопасности.

2. **Внедрите «медленное мышление».** Раздайте службе безопасности книгу Даниэля Канемана *Thinking, Fast and Slow*[5] и обсудите её. В книге описаны две системы мышления: более быстрая и импульсивная «Система 1» и более медленная и логичная «Система 2». Разрабатывайте решения, заставляющие сотрудников замедлиться и мыслить в терминах Системы 2, избегая когнитивных искажений и коротких путей, которые чаще всего эксплуатируют социальные инженеры. Возможные примеры:

   • настройте телефонную коммутационную систему так, чтобы сотрудник, принимающий внешний звонок, должен был ввести чётные цифры телефонного номера звонящего, прежде чем система установит соединение;
   • настройте почтовый клиент так, чтобы перед открытием вложения внешнего письма сотрудник должен был ввести адрес отправителя из поля From задом наперёд;
   • требуйте от пользователей, посещающих URL вне белого списка, правильно вводить число символов в домене, прежде чем браузер выполнит запрос DNS.

   Все эти меры замедлят деловую деятельность, но одновременно помогут смягчить атаки социальной инженерии.

> **Упражнение «Теория замка».** Представьте, что вы правитель средневекового замка, внутри которого находятся ценные ресурсы. Ваш замок осаждён, и вы не уверены, достаточно ли продовольствия, чтобы прокормить людей. Вы получаете письмо от союзного полководца, который обещает прислать еду и другие припасы, если в определённый день и час вы отвлечёте внимание окружающего замок вражеского войска. В письме вас просят отправить своего заместителя в расположенный поблизости лагерь союзного полководца, чтобы помочь спланировать контрнаступление против осады.
>
> Как определить, не является ли письмо вражеской уловкой? Можно ли независимо проверить его подлинность? Если предположить, что письмо настоящее, как выманить осаждающее войско? Наконец, какие меры предосторожности позволят получить припасы и одновременно не допустить проникновения в собственный замок во время обмена?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую из них следует оценивать с учётом понятия луны на воде.

1. Поскольку защитные системы и средства могут оберегать сведения только внутри установленных границ, внедрите меры, не позволяющие сведениям и системам выходить за эти границы и попадать в руки социальных инженеров. [AC-3: Access Enforcement | (9) Controlled Release; PE-3: Physical Access Control | (2) Facility/Information System Boundaries; SC-7: Boundary Protection]

2. Управляйте потоками информации так, чтобы даже за пределами обычных защитных границ данным не разрешалось перемещаться к несанкционированным информационным системам или между ними. [AC-4: Information Flow Enforcement; PL-8: Information Security Architecture; SC-8: Transmission Confidentiality and Integrity]
3. Для всего нелокального, то есть сетевого, обслуживания систем установите протоколы утверждения, требуйте строгих аутентификаторов и документированных политик и внедрите наблюдение. [MA-4: Nonlocal Maintenance]
4. Установите защиту данных за пределами контролируемых зон и разрешайте обрабатывать данные только уполномоченным лицам. [MP-5: Media Transport | (1) Protection Outside Controlled Areas]

Разбор

В этой главе мы описали передовой приём синоби «луна на воде». Мы рассмотрели различные сценарии, в которых этот приём можно осовременить и направить против предприятий. Мы исследовали сложности социальной инженерии и разнообразные формы, которые она принимает. Мы изучили существующие методы безопасности для противодействия социальной инженерии и рассмотрели новые понятия защиты. Наконец, мы позаимствовали из свитков синоби мысленное упражнение, показывающее, насколько хрупка наша модель доверия и как трудно бывает защищаться от социальной инженерии.

В следующей главе мы обсудим внутренние угрозы - одну из самых увлекательных тем безопасности. В свитках синоби подробно рассказано, как с помощью некоторых приёмов социальной инженерии выявлять людей, которых можно завербовать как своих агентов; кроме того, там предлагается способ защиты от внутренних угроз, противоречащий современным передовым методам.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), p. 133.
[2] [назад] Cummins and Minami, *The Book of Ninja*, p. 133.
[3] [назад] Cummins and Minami, *The Book of Ninja*, p. 134.
[4] [назад] Cummins and Minami, *The Book of Ninja*, p. 134.
[5] [назад] Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2013).

Глава 13. Агент-червь

> Превратите врага в *миномуси*, или агента-червя, то есть внутреннюю угрозу.

> *Миномуси* - человек, который служит врагу, но становится ниндзя, работающим на вашей стороне. Такой агент в точности подобен червю в животе врага, пожирающему его изнутри.
>
> - «Бансэнсюкай», «Ё-нин I»[1]

«Бансэнсюкай», как всегда щедрый на выразительные образы, описывает приём проникновения под открытой маскировкой под названием «искусство червя в животе», или «агент-червь», при котором синоби вербует людей внутри вражеской организации, чтобы те выполняли задачи от его имени. Такая вербовка требовала высокого эмоционального интеллекта. Синоби должен был выбрать подходящую цель, создать возможности для сближения и незаметно понять, что цель думает о работодателе, собственной ценности и тайных амбициях.[2] Свиток предупреждает: кандидата нужно выбирать чрезвычайно осторожно, поскольку попытка завербовать неподходящего человека как агента-червя, или *миномуси*, могла серьёзно навредить заданию синоби. Чтобы максимально повысить вероятность успешной вербовки, синоби разработали восемь типажей вероятных агентов-червей:[3]

- люди, которых нынешний работодатель несправедливо или чрезмерно наказал за прежние проступки и которые вследствие этого затаили глубокую обиду;
- люди, которые, несмотря на привилегированное происхождение или впечатляющие способности, занимают должность ниже своего положения, остались без повышения и возмущены недостаточным использованием их талантов;
- привычные отличники, неизменно приносящие работодателю хорошие результаты, но получающие в награду ничего не значащие должности, небольшие премии, недостаточную прибавку или вообще ничего. Считая свой вклад преуменьшенным, они полагают, что могли бы построить более плодотворную карьеру у другого работодателя. Они также считают, что организация принимает глупые решения, поскольку руководство ценит подхалимов и интриганов выше верных сотрудников с реальными достижениями;
- умные и талантливые работники, которые не ладят с руководством. Поскольку такие люди легко вызывают неодобрение и считаются помехой, работодатель назначает их на низкие должности, создаёт почву для конструктивного увольнения и вообще заставляет чувствовать себя нежеланными;
- специалисты в своей области, чьи обстоятельства - например, клятвы верности или семейные обязательства - работодатель эксплуатирует, удерживая их на низких должностях;
- люди, чьи служебные обязанности прямо противоречат их личности, семейным потребностям или убеждениям, из-за чего они сожалеют о своей работе;

• жадные и коварные люди без верности и нравственных ориентиров;
• сотрудники - «паршивые овцы», имеющие дурную репутацию из-за прошлых проступков и испытывающие раздражение из-за утраченного положения.

Выбрав возможного *миномуси*, синоби составлял план знакомства и построения отношений с кандидатом. «Бансэнсюкай» велит синоби изображать богача и добиваться расположения цели деньгами; в дружеских шутках выяснять её предпочтения, убеждения и чувство юмора; а в лёгкой беседе тайно узнавать сокровенные мысли. Если характер цели соответствовал типажу агента-червя, синоби пытался эксплуатировать эти черты *миномуси*, обещая богатство, признание и помощь в осуществлении тайных амбиций - либо, говоря прямее, алкоголь и секс - в обмен на предательство работодателя.[4]

Прежде чем использовать новообращённого *миномуси*, синоби советовали получить от него клятву предательства, собрать залоговые ценности в обеспечение верности агента-червя и установить сигналы и другие меры оперативной безопасности (operational security, OPSEC).[5]

В этой главе мы рассмотрим внутренние угрозы. Мы сравним недовольного работника с завербованным внутренним агентом. Мы также затронем способы обнаружения и сдерживания, которыми организации противодействуют внутренним угрозам, а также новый адресный подход, вдохновлённый свитками синоби, для упреждающего предотвращения превращения сотрудников из группы риска во внутренние угрозы. Наконец, мысленное упражнение предложит вам представить, кто из бывших и/или нынешних сотрудников способен стать внутренней угрозой, и исследовать собственное взаимодействие с ними.

Внутренние угрозы

Внутренняя угроза - сотрудник, пользователь или другой внутренний ресурс, действия которого способны причинить организации вред, намеренно или нет. Несчастный сотрудник, открывший фишинговое письмо и заразивший рабочую станцию вредоносным ПО, представляет собой неумышленную внутреннюю угрозу, поскольку не собирался совершать вредоносное действие. Напротив, недовольный работник, намеренно выпустивший в организацию вирус по личным причинам или от имени противника, - умышленная внутренняя угроза. Внутренние угрозы представляют собой законных уполномоченных пользователей с аутентификацией, полномочиями и доступом к информационным системам и данным, поэтому их смягчение относится к самым трудным проблемам кибербезопасности.

Для раннего обнаружения внутренних угроз многие организации полагаются на технические средства и охотников за угрозами. Технические приёмы обнаружения, например поведенческая эвристика, помогают выявлять возможные внутренние угрозы. Бдительные защитники и охотники могут расследовать действия пользователей, которые ведут себя нехарактерно или недопустимо: загружают все файлы на внешний переносной носитель; ищут конфиденциальные или закрытые данные, не связанные с их работой; входят в выходные или праздники для выполнения неприоритетной работы; обращаются к системам-приманкам и файлам с явной пометкой ограниченного доступа; либо загружают и применяют похожие на хакерские инструменты для действий за пределами своих обязанностей.

Однако даже для зрелой организации технические средства - лишь часть надёжной стратегии защиты. Проверяя рекомендации и биографические сведения, включая судимости и финансовую историю, а также проводя тесты на наркотики, работодатель может удостовериться, что сотрудник не выглядит явно уязвимым для ненадлежащего влияния. Ключевую роль в выявлении возможных внутренних угроз играет отдел кадров. Некоторые отделы проводят ежегодные опросы сотрудников для выявления возможных проблем; другие упреждающе увольняют работников из группы риска

или по тревожным результатам рекомендуют отозвать определённые права доступа. К сожалению, организации часто принимают минимальные меры предосторожности. Большинство доверяет сотрудникам, другие игнорируют проблему, третьи принимают риск внутренних угроз ради беспрепятственной деловой деятельности.

Организации, которые агрессивнее борются с внутренними угрозами, например в оборонной промышленности и разведывательном сообществе, внедряют передовые средства обнаружения и предупреждения: полиграф, регулярную проверку допусков, контрразведывательные программы, компартментализацию и суровые правовые наказания, не говоря уже о передовых технических средствах. Однако даже они не гарантируют обнаружение и предотвращение вредоносных действий всех внутренних угроз, особенно при помощи искушённых противников. Кроме того, их внедрение и эксплуатация создают особые трудности.

Новый подход к внутренним угрозам

Организации, которые сосредоточены на тщательной проверке сотрудников и пытаются поймать их за делом, слишком долго ждут, прежде чем заняться угрозой. Более упреждающий подход состоит в создании рабочей среды, не порождающей условия для расцвета внутренних угроз. Некоторые из следующих предложений направлены на исправление конкретных типажей внутренних угроз.

1. **Разработайте приёмы обнаружения и смягчения.** Исследуйте продукты и технические средства, которыми организация выявляет и смягчает внутренние угрозы. Проводите обучение и занятия по осведомлённости сотрудников, изучайте отчёты об инцидентах безопасности и выполняйте упражнения красной команды, например фишинговые испытания, чтобы выявлять людей, которые неоднократно становятся неумышленными внутренними угрозами. Затем обучайте и предупреждайте их и смягчайте угрозу, внедряя дополнительные средства безопасности для их учётных записей, систем, полномочий и доступа. Например, служба безопасности может строгими средствами и политиками ограничить способность и возможность сотрудников совершать действия внутренней угрозы. Среди примеров:

   • ввести правило, запрещающее включать и выполнять макросы в системах;
   • настроить получение всех писем открытым текстом с отключёнными гиперссылками;
   • по умолчанию помещать в карантин все вложения внешней почты;
   • отключить просмотр веб-страниц или разрешить его только через изолированную интернет-систему, не соединённую с интрасетью организации;
   • отключить USB-порты и внешние накопители в определённых системах.

   Наблюдение за умышленными внутренними угрозами требует и передовых приёмов обнаружения, и технологий, способных к обману и сокрытию. Выбирайте их на основе надлежащего моделирования угроз и оценки рисков организации.

2. **Внедрите кадровые политики против миномуси.** После внедрения и испытания предыдущих технических средств и приёмов обнаружения займитесь контролем персонала. Позаботьтесь, чтобы отдел кадров вёл записи о нынешних и прежних сотрудниках и кандидатах, включающие признаки профилей *миномуси*. Задавайте конкретные вопросы при проверке кандидатов, оценке результатов работы и собеседованиях при увольнении, чтобы собирать эти диагностические признаки.

3. **Особенно тщательно предотвращайте обстоятельства, создающие сотрудников-миномуси.** Отделу кадров следует рассмотреть следующие политики на уровне всей организации, представленные в порядке восьми типажей *миномуси*:

   • пересмотрите дисциплинарные протоколы для сотрудников, чтобы предотвращать несправедливое или чрезмерное - реальное либо воспринимаемое - наказание. Требуйте от работников и соискателей сообщать, работали ли члены их семей в организации. Побуждайте отдел кадров оценивать, считают ли сотрудники дисциплинарные меры против них несправедливыми или чрезмерными, а затем совместно искать решения для смягчения враждебности;
   • регулярно распространяйте опросы сотрудников, оценивая моральное состояние и выявляя недостаточно используемые таланты работников низшего уровня. Проводите откровенные собеседования с сотрудниками и руководством, чтобы определить: готов ли работник к повышению, остались ли без признания его недавние достижения или нужно ли ему развить конкретный навык; есть ли в компании должность для его повышения или бюджет для прибавки; считают ли определённые сотрудники себя лучше или ценнее коллег и не требуется ли им столкнуться с реальностью. Совместно с руководством подумайте, как ослабить озлобленность работников и исправить представление, будто организация не является меритократией;
   • в рамках оценки результатов работы запрашивайте отзывы коллег, чтобы определить руководителей, которых сотрудники низшего уровня считают наиболее ценными, а также работников, полагающих, что они не получили должного признания. Устраните эти претензии наградами и/или прозрачностью решений руководства компании;
   • побуждайте руководство лично наставлять умных, но социально неловких работников, деликатно рассказывать им, как их воспринимают, и помогать им чувствовать себя более принятыми обществом и менее изолированными;
   • пересмотрите и отмените политики компании, сдерживающие лучших специалистов. К ним могут относиться соглашения о неконкуренции, несправедливое присвоение интеллектуальной собственности сотрудников и недостаточные премии за результаты или стимулы к удержанию. Эти правила призваны защищать компанию, но могут давать обратный результат;
   • проведите профилирование нынешних сотрудников и соискателей по открытым источникам и определите, выражали ли они публично сильные чувства по поводу миссии организации или имеют ли конфликт интересов с ней. Если да, переведите сотрудников на должности, где личные ценности лучше соответствуют работе, либо облегчите их уход из организации;
   • разработайте приёмы профилирования характера и ищите признаки восприимчивости сотрудников и соискателей к подкупу. Рассмотрите сокращение системного доступа и уровня полномочий таких сотрудников, тем самым уменьшая их полезность для противника.

   Тесно работайте с сотрудниками, для которых риск возникновения условий *миномуси* высок. Дайте им дополнительные ресурсы, время и мотивацию, чтобы преодолеть накопленные обиды, воспользоваться возможностями личного роста и развить самоуважение. Сведите к минимуму или прекратите действия организации, которые укрепляют плохие воспоминания или продолжают наказывать человека за прошлые проступки.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка, внутри которого находятся ценные сведения, сокровища и люди. Вы получаете достоверные разведывательные сведения о том, что синоби намерен завербовать кого-либо внутри замка и обратить доверие к нему и его доступ против вас. Вы получаете список восьми типов людей, которых, вероятнее всего, завербуют. Неясно, на кого именно нацелен синоби и чего он желает добиться.

Кого вы первым заподозрите как внутреннюю угрозу? Почему этот человек находится в уязвимом положении и как исправить ситуацию? Как обнаружить вербовку одного из подданных или поймать вербовщика за делом? Как расставить стражников, чтобы не допустить действий внутренней угрозы? Как научить подданных сообщать о внутренних угрозах, не заставляя всех ополчиться друг против друга? Как долго следует поддерживать такую программу против внутренних угроз?

Чтобы избежать политических ловушек при групповом выполнении упражнения на нынешнем рабочем месте, попробуйте составить и использовать список бывших сотрудников. Если упражнение можно провести деликатно с небольшой группой заинтересованных лиц, рассмотрите и бывших, и нынешних работников.

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую из них следует оценивать с учётом понятия завербованных внутренних угроз. Дополнительные сведения см. в PM-12: Insider Threat Program.

1. Поручите SOC конфиденциально работать с отделом кадров и сопоставлять сведения о возможных внутренних угрозах, проявляющих особенности *миномуси*. SOC должен пристальнее наблюдать за этими людьми из группы высокого риска, проводить их аудит и ограничивать их. Он может также совместно с отделом кадров создавать приманки для внутренних угроз - например, файлы в сетевых общих ресурсах с надписью «RESTRICTED DO NOT OPEN», - выявляющие сотрудников, чьи действия соответствуют внутренним угрозам. [AC-2: Account Management | (13) Disable Accounts for High-Risk Individuals; AU-6: Audit Review, Analysis, and Reporting | (9) Correlation with Information from Nontechnical Sources; SC-26: Honeypots]
2. Используйте собственную учётную запись для совершения действий внутренней угрозы без возможностей красной команды с файлами и системами, которые, как вам известно, не причинят организации вреда. Можно изменять или удалять данные, вставлять ложные сведения или красть данные. Задокументируйте системы и данные, доступные вашей учётной записи, а затем воспользуйтесь привилегированной записью, например `admin` или `root`, для вредоносных привилегированных действий. Например, можно создать нового администратора с именем несуществующего сотрудника. Попросите SOC определить, какие данные вы украли, удалили или изменили в заданном диапазоне дат, и тем самым проверьте способность SOC правильно провести аудит выполненных привилегированных действий. [AC-6: Least Privilege | (9) Auditing Use of Privileged Functions; CA-2: Security Assessments | (2) Specialized Assessments]
3. Обучите сотрудников распознавать особенности *миномуси* и поведение внутренней угрозы. Дайте им возможность легко и анонимно сообщать о возможных условиях *миномуси* применительно к подозреваемым внутренним угрозам - подобно сообщениям о фишинге. Включите упражнения по осведомлённости о внутренних угрозах в регулярное обучение безопасности. [AT-2: Security Awareness | (2) Insider Threat]

Разбор

В этой главе мы рассмотрели приём синоби по вербовке уязвимых людей внутри целевой организации для совершения вредоносных действий. Мы подробно описали восемь типажей кандидатов во внутренние угрозы и обсудили разные программы обнаружения внутренних угроз и защиты от них, которыми сейчас пользуются организации. Мы описали новый оборонительный подход, основанный на сведениях из свитков синоби, - сочувствие к недовольному сотруднику. Мысленное упражнение этой главы заставляет участников оценить не только возможных внутренних агентов, но и собственные действия по отношению к коллегам; оно побуждает задуматься о более совместном подходе к возможным внутренним угрозам.

В следующей главе мы обсудим долгосрочных внутренних агентов - сотрудников, завербованных противником до поступления в вашу организацию. Поскольку они намеренно скрывают любую обиду или злобу по отношению к организации, обнаружить их ещё труднее.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), pp. 109-110.
[2] [назад] Cummins and Minami, *The Book of Ninja*, pp. 109-110.
[3] [назад] Cummins and Minami, *The Book of Ninja*, pp. 109-110.
[4] [назад] Cummins and Minami, *The Book of Ninja*, p. 110.
[5] [назад] Cummins and Minami, *The Book of Ninja*, p. 110.

Глава 14. Призрак на луне

> Согласно японской легенде, если знать, как найти призрака, ухаживающего за деревьями на Луне, он может пригласить вас туда съесть листья своего дерева, которые сделают вас невидимым.

> В обычное время, прежде чем возникнет необходимость, следует найти человека, который станет тайным агентом и предателем: посадить его во вражеской среде, превратить в своего ниндзя и держать во вражеском замке, лагере или вассальном владении в точности так, как призрак из легенды Кацура-отоко размещён на Луне.
>
> - «Бансэнсюкай», «Ё-нин I»[1]

Среди сложных приёмов проникновения «Бансэнсюкай» описывает долгосрочную тактику открытой маскировки под названием «призрак на Луне». Она предназначалась для получения привилегированных сведений и доступа через внедрённого тайного агента. Сначала синоби вербует заслуживающего доверия, умного, мудрого, отважного и верного человека. Если же завербованный изначально не верен, свиток предлагает на время задания взять членов его семьи в заложники и тем самым сделать его «верным». Затем синоби внедряет агента в чужую провинцию или замок. Там тот годами добросовестно работает с целью, наращивая репутацию, связи, знания и доступ. В идеале внедрённый агент будет тесно работать с руководством врага. Крот обязан всегда поддерживать правдоподобный, надёжный и заметный способ связи с синоби. Если эта вражеская крепость когда-либо станет целью нападения, ведущий синоби сможет обратиться к тайному агенту за разведывательными сведениями с высокой степенью достоверности, внутренней помощью, диверсиями и наступательными действиями против врага, включая убийство.[2] И хотя замысел «призрака на Луне» окупался лишь через годы, для терпеливого и тактичного синоби награда стоила потраченного времени.

В этой главе мы рассмотрим призрака на Луне как разновидность внутренней угрозы. По аналогии аппаратные имплантаты можно представить как попытку разглядеть в телескоп призраков на Луне. Поэтому мы затронем имплантаты, безопасность цепочек поставок и скрытые аппаратные чёрные ходы. Мы также сопоставим особенности внедрённого призрака на Луне с идеальными аппаратными имплантатами. Мы коснёмся управления рисками цепочки поставок и стратегий охоты за угрозами с оговоркой, что из-за фундаментальных проблем от этой угрозы почти невозможно защититься полностью.

Имплантаты

Корпоративный шпионаж и разведывательная деятельность государств исторически полагались на стратегически размещённых агентов для выполнения конкретных долгосрочных заданий. Сегодня технологии предлагают более новые и дешёвые способы получать результаты, которые традиционно были возможны только с участием людей. Предположим, например, что много лет назад ваша организация приобрела и установила в сети маршрутизатор зарубежного производства и тот работал безупречно. Но без ведома службы безопасности противник только что активировал скрытый имплантат, установленный на заводе, и получил прямой, нефильтрованный доступ через чёрный ход к наиболее критически важным системам и данным.

Индустрия кибербезопасности классифицирует такое нападение как атаку на цепочку поставок. Здесь *цепочка поставок* означает продукты и услуги, связанные с деловой деятельностью или системами организации; к ним относятся оборудование, программное обеспечение и облачный хостинг. В предыдущем примере маршрутизатор выполняет необходимую деловую операцию - перемещает цифровые сведения по сети для электронной коммерции.

Хотя эвристика и охота за угрозами могут выявить необычное поведение маршрутизатора, безошибочного способа защиты от скрытых имплантатов нет. Некоторые организации привлекают представителей отдела обеспечения качества для наблюдения за производством, но те не способны гарантировать правильную сборку каждой системы. И всё же несколько передовых методов кибербезопасности могут смягчить атаку на цепочку поставок через маршрутизатор. Организация с упреждающим подходом могла бы:

1. провести анализ угроз всех производителей маршрутизаторов и по результатам приобрести маршрутизатор, который с меньшей вероятностью поставляется со скомпрометированным оборудованием или программным обеспечением;
2. воспользоваться доверенной безопасной службой доставки и документировать цепочку ответственного хранения маршрутизатора, чтобы предотвратить вредоносный перехват;
3. после доставки провести криминалистическое исследование маршрутизатора и подтвердить, что он не скомпрометирован и не отличается от ожидаемых характеристик;
4. защитить маршрутизатор средствами предотвращения и обнаружения вмешательства, чтобы выявлять и смягчать несанкционированные изменения.

Обратите внимание: эти шаги применимы не только к маршрутизаторам. Организации могут принимать такие меры предосторожности для каждой услуги, устройства, системы, компонента и программы в цепочке поставок.

Скрытые имплантаты столь же ценны для современных государств, как когда-то для синоби, поскольку необходимость их обнаружения и защиты создаёт для организаций сложные долгосрочные проблемы. Специалисты по кибербезопасности непрерывно испытывают новые концепции их решения. Например, организация может ограничить доверие и доступ ко всем системам в предположении, что те уже скомпрометированы. Однако значительное воздействие на деловую деятельность делает многие подобные идеи практически неосуществимыми.

Защита от имплантатов

Организация, которая попытается взвешивать или просвечивать рентгеном каждую систему в поисках постороннего предмета, скорее всего, потеряется в процессе управления цепочкой поставок. Более того, развитые субъекты угроз, способные компрометировать цепочки поставок, вероятно, встроят вредоносные функции в стандартную конструкцию системы. Тогда только они будут знать секрет включения имплантата, а сам он будет присутствовать в каждой системе. И хотя процесс проверки организации способен увидеть угрозу, он может не понять, на что смотрит. Таков масштаб проблемы: это всё равно что искать призрака на Луне. Тем не менее для защиты организации от имплантатов можно дать следующие рекомендации:

1. **Выявите условия атаки на цепочку поставок.** Составьте список компонентов цепочки поставок, обладающих потенциалом призрака на Луне. Включите элементы, которые:

   • считаются высокодоверенными;
   • способны обмениваться данными;
   • способны предоставлять боковой или прямой доступ к критически важным сведениям или системам;
   • трудно исследовать;
   • редко заменяются или обновляются.

   В частности, изучите программы и оборудование, которые связываются с внешними системами или управляют системами, способными выполнять сигнальные функции или обмениваться данными, например микропрограммы маршрутизаторов, платы сетевых интерфейсов (network interface card, NIC) и концентраторы VPN. Имплантат может также существовать как аппаратное устройство, например чрезвычайно тонкий металлический интерфейс внутри разъёма PCI, выполняющий атаку посредника на NIC и изменяющий поток, целостность, конфиденциальность и доступность сетевого обмена этого интерфейса.

   Представьте, что антивирус, гипервизор, сканер уязвимостей или криминалистический аналитик не способен исследовать или испытать в вашей среде. Ключевая особенность кандидатов в цепочке поставок для призрака на Луне - способность сохраняться в среде цели. Вероятно, для этого выбираются компоненты, которые не ломаются и не изнашиваются регулярно, со временем не заменяются и не обновляются более дешёвыми версиями, слишком важны для отключения или утилизации и с трудом поддаются изменению и обновлению, например микропрограммы, BIOS, UEFI и MINIX. Требования автономности и скрытности для такого класса имплантатов цепочки поставок означают, что имплантат должен избегать исследования, сканирования и других проверок целостности, одновременно имея доступ к некоторой форме процессорных инструкций или исполнения.

2. **Внедрите защиту цепочки поставок.** По необходимости внедрите меры защиты цепочки поставок. Атака на неё посредством призрака на Луне относится к наиболее сложным для обнаружения, предотвращения или смягчения. Поэтому многие организации просто принимают или игнорируют риск. Полезно начать с первых принципов - фундаментальных истин о безопасности и назначении предприятия, - а затем оценивать по ним угрозу, стоящую перед организацией. Изучите статью «A Contemporary Look at Saltzer and Schroeder’s 1975 Design Principles»[3] или другие основополагающие труды по безопасности, чтобы определить подходящие способы смягчения. Может быть полезно и абстрагировать проблемы до понятий более высокого уровня, где они становятся знакомыми и понятными, а затем попытаться решить их. Рассмотрите следующее упражнение «Теория замка».

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка, внутри которого находятся ценные ресурсы. Вы получаете достоверные разведывательные сведения о том, что один служащий у вас писец - вражеский внедрённый «призрак на Луне». Последние десять лет этот агент учился копировать ваш почерк, лексику и способы наложения печати и запоминал имена и адреса всех важных людей, с которыми вы общаетесь. Внедрённый агент способен изменять исходящие приказы - например, направить постоянное войско далеко от ключевых оборонительных позиций. Неясно, кто именно из писцов внедрён и был ли он уже активирован вражеским синоби. Писцы редки в вашем королевстве, их приобретение и обучение дороги и занимают много времени, но они критически важны для деятельности.

Как обнаружить вражеского внедрённого среди писцов до и после активации? Подумайте, какие защитные меры не позволят писцу отправлять изменённые приказы от вашего имени. Какие протоколы аутентификации предотвратят подделку сообщений? Какие меры целостности не позволят изменять сообщения? Какие средства неотказуемости опровергнут ложные сообщения, отправленные от вашего имени? Как удостовериться, что будущие писцы не являются скомпрометированными вражескими агентами? Наконец, рассмотрите все эти вопросы для сценария с несколькими вражескими писцами.

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую из них следует оценивать с учётом понятия призрака на Луне.

1. Рассмотрите возможность внести неоднородность в цепочку поставок посредством изоляции, сегментации и многослойного сочетания разнообразных компонентов. Разнообразие цепочки поставок значительно сокращает возможное воздействие скомпрометированного компонента. [SC-29: Heterogeneity]
2. Проанализируйте процесс закупок организации и выявите участки, где можно снизить риск атаки на цепочку поставок. Применяйте такие приёмы, как слепая покупка, доверенная доставка, ограничение приобретений у определённых компаний или из некоторых стран, изменение формулировок договоров закупки и рандомизация либо сокращение времени приобретения. [SA-12: Supply Chain Protection | (1) Acquisition Strategies/Tools/Methods]
3. Подумайте об отсрочке обновлений, не связанных с безопасностью, и приобретения новых, неиспытанных программ, оборудования и услуг на максимально возможный срок. Внедрите передовые контрмеры, ограничивающие возможности искушённого субъекта нацелиться на организацию. [SA-12: Supply Chain Protection | (5) Limitation of Harm]

4. Приобретайте или оценивайте несколько экземпляров одного оборудования, программы, компонента или услуги через разных поставщиков, чтобы выявлять изменения и неподлинные элементы. [SA-12: Supply Chain Protection | (10) Validate as Genuine and Not Altered; SA-19: Component Authenticity; SI-7: Software, Firmware, and Information Integrity | (12) Integrity Verification]
5. Установите независимые внеполосные механизмы наблюдения и проверки здравого смысла, чтобы удостоверяться, что высокодоверенные компоненты, подозреваемые в атаке на цепочку поставок, не ведут скрытый обмен и не изменяют потоки данных. [SI-4: Information System Monitoring | (11) Analyze Communications Traffic Anomalies | (17) Integrated Situational Awareness | (18) Analyze Traffic/Covert Exfiltration]

Разбор

В этой главе мы рассмотрели приём синоби по найму доверенных союзников, которые должны работать внутри организации и занять положение, позволяющее быть максимально полезными синоби. Мы сопоставили такой вид внедрённого агента с аппаратными имплантатами и обсудили теорию выбора устройств и систем, подходящих для аппаратного внедрения. Мы поговорили об атаках на цепочки поставок и возможных способах их обнаружения. Мысленное упражнение предложило обнаружить скомпрометированного писца с привилегированным доступом к обмену; писец представляет маршрутизатор, VPN или другое устройство уровня 3, которое должно быть прозрачным для участников обмена, и подчёркивает сложность определения компрометации такого устройства.

В следующей главе мы обсудим запасной план синоби на случай, если вам всё же удастся поймать его или внедрённого агента. Задолго до тайного задания синоби часто подкладывал ложные улики, позволяющие в случае поимки переложить вину. При успехе эта тактика убеждала жертву, что её предал союзник, и уже сам обман причинял цели вред.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), p. 104.
[2] [назад] Cummins and Minami, *The Book of Ninja*, pp. 104-106.
[3] [назад] R. E. Smith, «A Contemporary Look at Saltzer and Schroeder’s 1975 Design Principles», *IEEE Security & Privacy* 10, no. 6 (2012), pp. 20-25.

Глава 15. Искусство светлячков

> Искусство светлячков следует применять лишь после того, как вы во всех подробностях узнаете о враге всё, чтобы построить обман в соответствии с образом мыслей цели.

> Прежде чем приступить к наблюдению или тайной деятельности синоби, следует оставить записку для своей будущей репутации.
>
> - «Ёсимори хякусю», стихотворение 54

«Бансэнсюкай» описывает приём проникновения синоби под открытой маскировкой под названием «искусство светлячков» (*хотаруби-но дзюцу*).[1] Мне нравится думать, что он назван в честь того, как вспышка светлячка остаётся в ночном зрении после того, как тот переместился, заставляя хвататься за пустоту. «Сёнинки» описывает тот же приём как «искусство камуфляжа» (*кото-о магиракасу-но нараи*).[2] С помощью этого приёма синоби подкладывает вещественные улики, побуждающие врага совершить желаемое действие: неверно приписать синоби определённому хозяину, сделать ложные предположения о его мотивах или необдуманно отреагировать на попытку нападения и тем самым подставиться под дальнейшие наступательные действия.

Самым распространённым приёмом *хотаруби-но дзюцу* было поддельное письмо с компрометирующими подробностями или вводящими врага в заблуждение уликами; оно имело несколько вариантов. В свитках рассказывается, как синоби вшивал письмо в воротник, чтобы при поимке или обыске его быстро нашли.[3] В другом варианте синоби вербовал готового помочь, но неумелого человека на роль «ниндзя», вручал ему письмо с планом, прямо противоположным настоящим намерениям синоби, и отправлял на задание во вражескую среду, прекрасно понимая, что этого «обречённого агента» непременно поймают. Важно, что сам завербованный не знал об этой части замысла. При обыске стражники находили поддельное письмо, уличавшее особо ценную цель - например, самого способного вражеского командира - в предательском заговоре. Под пытками «ниндзя», вероятнее всего, ломался и подтверждал подлинность послания, ещё сильнее обвиняя цель.[4] Всё это должно было обманом заставить врага напасть на собственных союзников или избавиться от них.

В ещё более сложном варианте синоби до задания тщательно подкладывал улики в подтверждение ложной истории из письма, а само поддельное письмо помещал в компрометирующее место, например в покои доверенного советника вражеского командира. После этого письмо становилось страховкой. Если синоби ловили, он терпел пытки, пока не понимал цели врага, а затем раскрывал тайное знание о письме. Враг находил письмо и связанные с ним улики. Заслужив доверие, синоби предлагал стать двойным агентом или поделиться секретами работодателя в обмен на сохранение жизни.[5] Этот приём оставлял врага в замешательстве относительно мотивов синоби, заставлял опасаться возможного предательства и сомневаться в том, кто является настоящим противником.

В этой главе мы рассмотрим трудности установления принадлежности угрозы конкретному противнику и/или источнику. Мы разберём расследования принадлежности с помощью аналитики угроз, наблюдаемых улик и оценок разведывательных данных по поведению. Мы также обсудим проблему искушённых противников, которые знают об этих методах атрибуции и потому применяют контрмеры. Чем больше внимания защитник уделяет установлению принадлежности, тем труднее и рискованнее субъекты киберугроз могут сделать преследование зацепок, поэтому мы также поговорим о способах справиться с повышенным риском.

Установление принадлежности

В контексте кибербезопасности *установление принадлежности*, или атрибуция, означает оценку наблюдаемых улик, позволяющих выявлять субъектов в киберпространстве. Улики принимают множество форм. Поведение, инструменты, приёмы, тактика, процедуры, возможности, мотивы, возможности для действия и намерения субъекта угроз среди прочих сведений создают ценный контекст и определяют реакцию на события безопасности.

Предположим, например, что сработала домашняя сигнализация, сообщая о разбитом окне. Ваша реакция сильно зависела бы от знаний о принадлежности: пожарный, который проник в дом для тушения пожара, вызвал бы иную реакцию, чем вор, забравшийся за имуществом, или случайный мяч для гольфа, влетевший в окно. Разумеется, принадлежность не всегда легко установить. Вор способен отчасти управлять наблюдаемыми уликами, надев перчатки и маску. Он может даже облачиться в форму пожарного, скрыть личность и обманом заставить хозяев согласиться впустить его. Во время преступления или после него вор может подложить, уничтожить или не создать улики и тем самым затруднить последующую работу криминалистов. По-настоящему искушённый преступник способен даже подставить другого с помощью поддельных накладок с отпечатками пальцев, украденных образцов волос, крови или одежды, реалистичной маски, напечатанной на 3D-принтере, или оружия, полученного у ничего не подозревающей жертвы подставы. Если у подставленного нет алиби или преступление совершено против цели, соответствующей его мотивам, у властей будут все основания подозревать или арестовать его.

Специалисты по кибербезопасности сталкиваются с такими и ещё более сложными проблемами атрибуции. Установление принадлежности особенно затруднено из-за присущей киберсреде анонимности. Даже выполнив сложную задачу и проследив атаку или событие до исходного компьютера и физического адреса, специалисты могут столкнуться с чрезвычайной трудностью проверки личности атакующего человека. Попытки проследить происхождение субъекта угроз на скомпрометированном компьютере часто приводят к туннелям, VPN, шифрованию и арендованной инфраструктуре без содержательных журналов или улик. Искушённые субъекты угроз могут даже компрометировать чужие компьютеры и удалённо подключаться к ним, используя как площадки для атак на другие системы. Даже после обнаружения противника в некоторых случаях разумно не блокировать его немедленно и не закрывать ему доступ, а некоторое время наблюдать, чтобы определить цели и отличительные особенности.[6]

Иногда группы угроз намеренно оставляют инструменты или другие наблюдаемые признаки, чтобы навязать определённую версию принадлежности. По имеющимся сведениям, США, Россия и Северная Корея изменяли или копировали фрагменты кода, строки, инфраструктуру и артефакты в своих киберинструментах, добиваясь ошибочной атрибуции.[7] Когда специалисты обнаруживают и подвергают обратной разработке особенно скрытное вредоносное ПО, они порой видят в его следах уникальные лишние строки. Возможно, строки были пропущены - это ошибка оперативного искусства оператора или разработчика. Но они могут оказаться и «искусством светлячков» - уликами, специально предназначенными для обнаружения и применения в правильной или ошибочной атрибуции.

Обратите внимание: те же механизмы, которые делают возможным обман, дают и мощные средства идентификации. Дампы памяти, образы дисков, реестры, кеши, перехваты сети, журналы, сетевые потоки, анализ файлов, строки, метаданные и многое другое помогают выявлять субъектов киберугроз. В установление принадлежности вносят вклад разные разведывательные дисциплины: радиоэлектронная разведка (signals intelligence, SIGINT), киберразведка (cyber intelligence, CYBINT) и разведка по открытым источникам (open source intelligence, OSINT), а средства агентурной разведки (human intelligence, HUMINT) собирают у конкретных источников данные, которые после обработки и анализа помогают определить возможных исполнителей кибератак. Эти возможности обычно хранятся в тайне, поскольку раскрытие их существования

подскажет целям, как избегать таких систем, отказывать им в сведениях или обманывать, и тем самым ослабит способность создавать полезные разведывательные сведения и устанавливать принадлежность угроз.

Подходы к установлению принадлежности

Стремление организаций узнать личность и происхождение субъектов угроз, скомпрометировавших их системы и сети, вполне обоснованно. Понятно и желание многих принять активные меры, например нанести ответный взлом, чтобы выяснить, кто эти люди. Однако субъекты угроз, подобно синоби, всегда найдут способы скрытно совершать вредоносные действия посредством отрицания и обмана, делая атрибуцию неопределённой. Более того, история учит: необходимость устанавливать принадлежность действий синоби исчезла лишь после объединения Японии под мирным правлением, когда синоби больше не осталось. В обозримом будущем мир едва ли достигнет единства, поэтому государственные кибератаки, вероятно, продолжатся. До наступления мира следующие подходы к атрибуции помогут понять, что вообще можно сделать с продолжающимся киберконфликтом:

1. **Избавляйтесь от когнитивных искажений.** Задумайтесь о собственных когнитивных искажениях и ошибочной логике. В мышлении каждого есть пробелы, но их можно осознавать и исправлять. Составляйте собственные разборы случаев. Пересматривайте прежние суждения, оказавшиеся неверными, выявляйте ошибки и думайте, как улучшить аналитические способности. Эту важную работу можно вести небольшими шагами - логические задачи, кроссворды и головоломки отлично улучшают когнитивные функции - или большими скачками. Изучайте статьи и книги по психологии об известных когнитивных искажениях и логических ошибках и осваивайте структурированные аналитические приёмы для их преодоления.[8]
2. **Развивайте возможности атрибуции.** Исследуйте источники данных, системы, знания и средства, которыми можно влиять на установление принадлежности в организации. Не используете ли вы открытую незащищённую сеть Wi-Fi, позволяющую незарегистрированным, неаутентифицированным и неопознанным субъектам угроз анонимно подключаться к сети и проводить атаки? Не управляются ли вами маршрутизаторы, которые допускают поддельные IP-адреса, и применяют ли они защитные технологии пересылки по обратному пути (reverse-path forwarding, RFP) для предотвращения анонимных атак из вашей сети? Правильно ли опубликована структура политики отправителей, не позволяющая субъектам угроз подделывать адреса почты и выдавать себя за организацию?

   Хотя многие из этих изменений конфигурации не требуют прямых затрат, время, труд и альтернативные издержки при столь широком внедрении могут заставить руководство заколебаться. Но подумайте, помогает ли прежнее решение вложиться в хорошие камеры и освещение владельцу магазина правильно опознать вандала. Надёжное журналирование, документирование и сбор улик улучшают возможности атрибуции, усиливают технологическую ответственность и дают конечным пользователям лучшую видимость сетевых угроз.
3. **...Или забудьте об атрибуции.** Совместно с заинтересованными лицами организации определите масштаб работ по установлению принадлежности, необходимый для смягчения риска. Для организаций, способных арестовывать субъектов угроз или проводить контрнаступления, атрибуция необходима. Но большинство организаций не может или не должно пытаться ловить субъектов угроз либо нападать на них, узнавать личности и картографировать возможности. В действительности установление конкретного субъекта угроз нужно не всегда. Для анализа угрозы и защиты от неё может быть достаточно знать о её существовании.

Предположим, например, что два субъекта угроз выбрали интеллектуальную собственность организации. Один желает продать сведения на чёрном рынке ради денег, другой - помочь своей стране строить системы вооружения. На деле это не имеет значения. Независимо от цели субъектов и способности организации выследить их защитники в конечном счёте обязаны ограничить или исключить возможности эксплуатации недостатков безопасности. Организации необязательно оценивать мотивацию субъекта, чтобы избежать угрозы.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка, внутри которого находятся ценные активы. Ваши стражники ловят незнакомца, когда тот роет туннель под одной из замковых стен. После напряжённого допроса незнакомец заявляет, что ему заплатили за прокладку туннеля к замковому хранилищу продовольствия, чтобы разбойники могли похитить припасы. Однако при обыске пленника стражники обнаруживают записку с инструкциями по связи с одним из ваших доверенных советников. В записке говорится, что советник задумал вызвать восстание против вашей власти, лишив жителей деревни пищи. Послание выглядит подлинным. Стражники не могут установить ни личность нарушителя, ни того, на кого он работает.

Подумайте, как вы проводили бы атрибуцию, чтобы определить, кто этот нарушитель, откуда он, какова его возможная мотивация и на кого он может работать. Как проверить утверждение незнакомца, будто его конечная цель - похитить пищу, а не, скажем, уничтожить её, проложить путь проникновения для иного субъекта угроз, напасть на обитателей замка или даже поднять восстание? Как подтвердить роль советника во вражеских замыслах? Что вы предпримете, если найдёте дополнительные доказательства версии нарушителя о принадлежности? А что будете делать, если доказать её не удастся?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую из них следует оценивать с учётом концепции атрибуции.

1. Сопоставляйте учётные записи с личностями пользователей. Проверяйте личность человека, связанного с учётной записью, с помощью биометрии, удостоверяющих документов, логических или вещественных доказательств либо средств контроля доступа. [SA-12: Supply Chain Protection | (14) Identity and Traceability]
2. Разработайте план, определяющий порядок работы организации с оценками принадлежности субъектов угроз. [IR-8: Incident Response]
3. Создайте программы осведомлённости об угрозах, которые собирают сведения о характеристиках субъектов угроз, способах их выявления в вашей среде, доказательствах принадлежности и иных наблюдаемых признаках и обмениваются этими сведениями. Для установления принадлежности применяйте специальные средства сбора данных, например приманки. [PM-16: Threat Awareness Program; SC-26: HoneyPots]
4. Применяйте средства безопасности и сбора данных. Выполняйте моделирование угроз, чтобы выявлять их субъектов. [SA-8: Security and Privacy Engineering Principles]

Разбор

В этой главе мы рассмотрели искусство светлячков - применявшийся синоби приём ошибочной атрибуции. Группы киберугроз непрерывно совершенствуются и, скорее всего, включат этот приём в свои процедуры оперативной безопасности, если ещё этого не сделали. Мы отметили, что несколько групп угроз, по имеющимся сведениям, уже используют методы ошибочной атрибуции, обсудили подходы к установлению принадлежности и объяснили, почему будущее атрибуции выглядит мрачно.

В следующей главе мы поговорим о тактике, с помощью которой синоби сохраняли правдоподобное отрицание при допросах защитниками. В ней также будут рассмотрены передовые методы допроса синоби и инструменты, применявшиеся при поимке вражеских синоби.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), 111.
[2] [назад] Antony Cummins and Yoshie Minami, *True Path of the Ninja* (North Clarendon, VT: Tuttle Publishing, 2017), 122.
[3] [назад] Cummins and Minami, *The Book of Ninja*, 112.
[4] [назад] Cummins and Minami, *The Book of Ninja*, 114.
[5] [назад] Cummins and Minami, *The Book of Ninja*, 112.
[6] [назад] Подробнее это описано в книге Клиффа Столла *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (New York: Pocket Books, 2005).
[7] [назад] Cameron H. Malin et al., *Deception in the Digital Age: Exploiting and Defending Human Targets Through Computer-Mediated Communications* (London: Elsevier, 2017), 221; Brandon Valeriano et al., *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018), 138.
[8] [назад] Дополнительные сведения см. в книге Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Los Angeles: CQ Press, 2015).

Глава 16. Захват вживую

> Рассудите здраво, действительно ли цель невнимательна или же применяет уловку, чтобы заманить ниндзя и схватить их.

> Если во время ночного патрулирования вы обнаружите подозрительного человека, следует призвать на помощь все свои средства и взять его живым.
>
> - «Ёсимори хякусю», стихотворение 74

Хотя смертельное насилие было для синоби повседневной частью работы, «Бансэнсюкай» рекомендует брать врагов, особенно подозреваемых ниндзя, живыми, а не убивать сразу. Обыск и допрос пленённого ниндзя позволяют синоби выяснить, что нападавший уже сделал или намерен сделать, определить его нанимателя и узнать ценные секреты и профессиональные приёмы. Всё это может существенно помочь стражникам защищаться от нападений ниндзя, а господам - понимать стратегические угрозы. Кроме того, захваченный враг может оказаться замаскированным товарищем, что прояснится лишь при глубоком допросе.[1] «Нинпидэн» предписывает связать подозреваемому ниндзя руки и ноги и посадить его на привязь. Там же рекомендуется применять такие средства, как шипованный кляп, чтобы пленник не мог говорить: умелый ниндзя способен предупредить союзников, убедить пленившего его человека отпустить его или даже откусить себе язык и покончить с собой.[2]

Свитки признают, что взять вражеского ниндзя живым совсем не просто. Один из наиболее прямолинейных приёмов «Бансэнсюкай» предполагает зарядить мушкет ватным шариком, пропитанным порошком чили, - своего рода древним слезоточивым газом или перцовым аэрозолем. При выстреле с близкого расстояния такой снаряд вызывал мучительное раздражение глаз и носа цели, облегчая её захват. Свитки описывают и более косвенные тактики, например засады и ловушки *фуси-камари*. Так, описанная в «Бансэнсюкай Гунъё-хики» «тигровая яма» (*могари* или *кораку*) первоначально предназначалась, как следует из названия, для поимки тигров, но позднее была приспособлена для захвата ниндзя. Ограждения направляли нарушителя через лабиринт скрытых ловушек. Союзники знали безопасный путь, а ниндзя, проникавший в одиночку ночью, - нет, поэтому с большой вероятностью попадался. В других ловушках применялись *цуйритэй*, или «ложные подвесные участки стены», - облицовка, выглядевшая как настоящая стена, но державшаяся на клиньях и поддельных стойках. Когда ниндзя пытался взобраться по такой стене, она обрушивалась, заставала его врасплох и, скорее всего, ранила, после чего его было легко схватить.[3]

«Бансэнсюкай» предлагает и защитные меры против захвата, в том числе способы обнаруживать и избегать засад *фуси-камари*. Синоби советовали осматривать леса, поля, долины, рвы и другие места, замечая неестественное поведение птиц, прочих животных и даже травы - всё это могло указывать на ловушку. Чучела и необычные запахи также выдавали возможную засаду.[4] На вражеской территории синоби могли применять несколько приёмов уклонения:

- **Перепелиное укрытие (*удзура-гакурэ*).** Синоби сворачивался клубком на земле и сосредоточивался на том, чтобы ничего не видеть, не осознавать и ни на что не реагировать, благодаря чему враг с меньшей вероятностью его замечал. Даже если стражник тыкал его копьём или мечом, он не отзывался.
- **Отступление енотовидной собаки (*тануки-ноки*).** Убегая пешком, синоби решал позволить более быстрому преследователю себя «догнать». Когда расстояние между ними сокращалось, синоби без предупреждения падал на землю и направлял меч в пояс преследователя, пронзая того прежде, чем он успевал отреагировать.
- **Отступление со ста петардами (*хякурай-дзю*).** Синоби раскладывал рядом с целью петарды, снабжая их фитилём замедленного действия или поручая союзникам поджечь их. Шум отвлекал преследователей.
- **Лисье укрытие (*кицунэ-гакурэ*).** Синоби уходил от погони по вертикали. Вместо попытки покинуть вражескую территорию, переместившись из точки А в точку Б, он взбирался на высокое дерево или прятался во рву, меняя измерение погони. Такая тактика часто ставила врага в тупик: тот обычно не догадывался искать цель сверху или снизу.[5]

К другим способам бегства относились имитация - подражание собаке или иному животному для обмана преследователей - и ложный разговор, который вводил врага в заблуждение и позволял синоби скрыться.[6] Например, зная о погоне, синоби мог сделать вид, будто не слышит преследователей, и прошептать что-нибудь воображаемому союзнику так, чтобы настороженные стражники подслушали. Услышав: «Давай тихо проберёмся в спальню господина и убьём его во сне», стражники, вероятно, направили бы силы к спальне, а синоби получил бы возможность бежать в другую сторону.

Разумеется, лучший способ не попасть в плен - вовсе не оставлять улик, по которым следователи могли бы заподозрить проникновение. Свитки подчёркивают, что задания нужно выполнять бесследно, чтобы у цели не возникло оснований подозревать присутствие синоби. В свитках множество наставлений о скрытных действиях, иногда изложенных удивительно образно. В стихотворении 53 «Ёсимори хякусю» сказано: «Если вам приходится тайно проникать как синоби во время снегопада, прежде всего остерегайтесь собственных следов».[7]

К сожалению, многие организации далеко не всегда в первую очередь думают о захвате угроз живыми. Обнаружив угрозу в системе, некоторые поступают прямо противоположно рекомендациям свитков синоби: немедленно отключают компьютер, стирают все данные, форматируют накопитель и устанавливают чистую операционную систему. Такой подход «стереть и забыть» уничтожает угрозу, но вместе с ней и любую возможность захватить её, не говоря уже о расследовании, анализе её целей, уже достигнутых результатов и использованных способов.

В этой главе мы обсудим, почему важно уметь захватывать киберугрозы и взаимодействовать с ними, пока они «живы». Мы рассмотрим существующие методы криминалистического анализа и захвата, а также способы, которыми субъекты угроз пытаются их избегать. Мы подумаем, как захватывать киберугрозы «живыми» с помощью тигровых ловушек и медовых засад - приёмов, вдохновлённых древними синоби. Кроме того, кратко рассмотрим современные реализации тактик уклонения синоби, например перепелиного и лисьего укрытия, которыми пользовались устойчивые угрозы. Наконец, разберём многие наставления свитков о захвате и допросе: как правильно удерживать угрозу, чтобы она не предупредила союзников и не самоуничтожилась.

Анализ вживую

В кибербезопасности криминалистический образ компьютера даёт необходимые разведывательные сведения об угрозе. Такие образы обычно создают после инцидента безопасности, например заражения вредоносной программой, или нарушения правил использования, например загрузки детской порнографии на устройство. Образ получают так, чтобы сохранить доказательства и не нарушить целостность данных исследуемой системы. Доказательства из криминалистического образа помогают специалистам понять, что представляла собой угроза и как она эксплуатировала уязвимости. Со временем они дают сведения, необходимые для создания сигнатур, защитных мер и упреждающих механизмов блокирования.

Например, выяснив, что злоумышленник охотился за конкретной интеллектуальной собственностью в одной критически важной системе, защитники понимают, какие данные следует защищать. Если криминалистический анализ показывает, что атака удалась и конфиденциальные данные скомпрометированы, организация может учесть это при выборе стратегической деловой реакции. Если угроза потерпела неудачу, можно подготовиться к возможным повторным атакам. Криминалистические индикаторы способны также указать виновника угрозы и тем самым дополнительно определить реакцию. Стратегия организации должна учитывать серьёзность угрозы - например, был ли нападавшим иностранный государственный орган, недовольный сотрудник или ребёнок, который безобидным взломом пытался прославиться.

Сбор данных устройства для анализа включает захват вживую, также называемый анализом или сбором данных вживую, и создание образа, также называемое криминалистическим созданием образа или зеркалированием. Для захвата злоумышленников вживую и даже взаимодействия с ними организации используют приманки и другие обманные виртуальные среды. Такие системы часто настраивают так, чтобы привлекать хакеров или быть легкодоступными для вредоносных программ. Когда угроза проникает внутрь, скрытые средства журналирования и наблюдения точно фиксируют её действия и способы их выполнения вместе с другими наблюдаемыми признаками. К сожалению, многие злоумышленники знают о приманках и проверяют, не находятся ли они в моделируемой среде, предназначенной для сбора разведывательных данных. Если подозрения подтверждаются, злоумышленники меняют поведение или прекращают работу, сводя на нет усилия группы безопасности. Устройства контроля доступа к сети (network access control, NAC) также могут сдерживать живые угрозы, динамически переключая систему в заражённую VLAN, где та остаётся подключённой и «живой», пока защитники реагируют.

Криминалистический анализ обычно проводят не на живом объекте. Аналитик исследует статичные, инертные или мёртвые данные, которые могли утратить некоторые сведения или уникальные особенности угрозы. Такое часто происходит с бестелесными вредоносными программами, находящимися в памяти, или с особыми вредоносными конфигурациями и артефактами, например в кешах таблиц маршрутизации. Анализ вживую проводится нечасто по нескольким причинам:

• нужны специализированные технологии;
• приходится обходить правила организации, требующие отключать, обесточивать, помещать в карантин или блокировать скомпрометированные системы;
• на месте нет подготовленных специалистов по криминалистике, способных провести анализ вживую;
• во время расследования сотрудникам недоступны жизненно важные системы.

Пожалуй, важнее всего то, что при неверном проведении анализа вживую угроза может обнаружить криминалистическое программное обеспечение в системе и решить скрыться, удалить себя, применить контрмеры против криминалистики или выполнить разрушительную атаку на систему.

Чтобы обходить методы криминалистического захвата, угрозы развёртываются в несколько этапов. На первом этапе, во время разведки, угроза ищет технологии захвата и загружает вредоносные программы и инструменты лишь после того, как убедится в безопасности работы внутри среды. Такие предосторожности необходимы субъекту угрозы. Если захват и криминалистический анализ проходят успешно, его инструменты и приёмы могут передать другим организациям и защитникам, которые изучат атаку, установят исправления или разработают контрмеры. Правоохранительные органы могут даже применить тактику криминалистического захвата, чтобы выследить субъектов угроз или получить доказательства против них.

В последнее время искушённые субъекты перемещаются по горизонтали в области компьютеров и сетей, которые стандартные средства создания образов, захвата и анализа не проверяют или не способны проверить. Среди их новшеств - установка микропрограммы жёсткого диска, создающей скрытую зашифрованную файловую систему; внедрение вредоносных программ в хранилище BIOS; использование локальной памяти микросхем для работы вне обычной оперативной памяти; изменение низкоуровневых модулей и кода сетевого оборудования, такого как маршрутизаторы, коммутаторы, умные принтеры и другие устройства, которые традиционно не исследуют криминалистическими образами или для которых это непрактично. Некоторые угрозы имитируют ключевые компоненты ОС или доверенные средства безопасности, проникая к исходному производителю, которому безоговорочно доверяют и потому не рассматривают в ходе криминалистического анализа. Другие скрываются, удаляя криминалистические улики и перемещаясь в память системы, которая редко перезапускается, например контроллера домена, а затем ждут, пока пристальное внимание криминалистов к интересующим системам ослабнет, и возвращаются к намеченной цели.

Противодействие живым угрозам

Слишком часто организация сталкивается с активным инцидентом безопасности именно тогда, когда единственного сотрудника, обученного работе со средствами криминалистического создания образов, нет на месте. Иногда проходит несколько дней, прежде чем помещённый в карантин компьютер удаётся доставить этому специалисту для исследования, и к тому времени атака уже не представляет живую картину текущей угрозы. Неспособность действовать с той же скоростью, что и угроза, или быстрее отводит защитникам роль криминалистических уборщиков - людей, которые собирают улики и устраняют заражение после того, как субъект угроз уже достиг своих целей. Для захвата угрозы живой и её тщательного допроса необходимо заранее создавать возможности, ловушки и засады для противодействия.

1. **Создайте криминалистические возможности.** Примите обязательство и вложите средства в создание специализированной группы, имеющей оборудование, опыт, сертификацию и полномочия для компьютерной криминалистики. Подготовьте криминалистические комплекты с блокираторами записи, защищёнными жёсткими дисками и другим специальным программным обеспечением и устройствами. Убедитесь, что во всех системах, используемых для захвата и анализа, установлены надлежащие криминалистические агенты, позволяющие группе немедленно выявить, найти и изолировать объект и собрать данные. Все сотрудники должны понимать, как помочь группе найти затронутые системы и сохранить доказательства. Если с последнего криминалистического расследования прошёл месяц, проведите повторное обучение или учения. И самое главное: завершив криминалистический отчёт, прочитайте его, чтобы выявить первопричины инцидентов и принять упреждающие меры по устранению использованных уязвимостей.
2. **Устраивайте медовые засады.** Там, где это уместно, дайте группе возможность устраивать засады на субъектов угроз, а не просто идти по их следу или ловить в приманку. Агрессивный захват угроз в ловушки и засады требует тесного сотрудничества с облачными хостингами, интернет-провайдерами, регистраторами, поставщиками VPN, Центром приёма жалоб на интернет-преступления (Internet Crime Complaint Center, IC3), финансовыми службами, правоохранительными органами, частными охранными предприятиями и коммерческими компаниями. Поддерживайте цель создания сетевой территории, враждебной субъектам угроз, где объединённые силы вашей организации и партнёров смогут устраивать засады на отдельных субъектов, группы или кампании и захватывать доказательства, вредоносные программы, инструменты и эксплойты.
3. **Ставьте тигровые ловушки.** Подумайте о создании тигровых ям в вероятных целях внутри сети, например на контроллере домена. На рынке есть место для продукта, который служил бы рабочей производственной системой с возможностями приманки, срабатывающими при неправильном действии. Поскольку субъекты угроз при обходе средств безопасности обычно переходят из одной системы в другую или перемещаются по горизонтали между системами и сетями, можно создать ложные либо заминированные промежуточные узлы, которые выглядят как маршруты в другие сети, но в действительности захватывают угрозу. Разворачивайте такие ловушки так, чтобы неправильное действие замораживало или блокировало систему либо изолировало атаку, позволяя защитникам исследовать угрозу, взаимодействовать с ней или выполнить её криминалистический захват вживую. Для этого можно заморозить тактовый генератор процессора, заставить жёсткий диск работать только в буферном режиме либо с помощью гипервизора перехватывать и журналировать действия. Обучите системных администраторов и других ИТ-специалистов удалённо проходить по законному пути, не попадая в ловушку.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка с ценными активами внутри. Недавно стражники схватили нарушителя, которого сочли ниндзя, быстро убили подозреваемого, а затем сожгли тело. По их словам, так они устранили всякий остаточный риск, исходивший от ниндзя. Но когда вы спрашиваете, почему они решили, что нарушитель был ниндзя, что находилось при нём, что он делал в замке и как незнакомцу удалось проникнуть в твердыню, стражники не знают ответа. Похоже, они ждут похвалы за быстрое устранение угрозы при минимальном ущербе для себя.

Как можно создать более надёжные правила, процедуры и инструменты, чтобы стражники безопасно задерживали подозрительных нарушителей? Как вы допросили бы ниндзя, если нарушитель действительно был ниндзя и стражники не убили бы его? Что вы искали бы среди его вещей, если бы их не сожгли? Как, по-вашему, ниндзя проник в замок и как проверить эти подозрения? Как обыскать замок, чтобы выяснить, совершил ли ниндзя диверсию, установил ловушки или передал сигнал перед смертью? Что вы спросите у обнаружившего ниндзя стражника и как ответы помогут обучить остальных? Что вы рассчитываете узнать из расследования и какие решения или действия можете принять по его итогам?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую следует оценивать с учётом концепции захвата вживую.

1. Ограничивайте использование внешних систем и компонентов в организации, если у вас нет полномочий или возможностей проводить их криминалистическое исследование. [AC-20: Use of External System | (3) Non-Organizationally Owned Systems and Components]
2. С помощью внешних датчиков и SIEM, к которым трудно получить доступ, внедрите автоматизированные механизмы полного сбора живых данных, PCAP, системных журналов и иных данных, необходимых для криминалистического анализа. [AU-2: Audit Events; AU-5: Response to Audit Processing Failures | (2) Real-Time Alerts; IR-4: Incident Handling | (1) Automated Incident Handling Processes; SA-9: External System Services | (5) Processing, Storage, and Service Location; SC-7: Boundary Protection | (13) Isolation of Security Tools, Mechanisms, and Support Components]
3. Если вы решите использовать непостоянство как контрмеру против угроз, например регулярно заново создавать образы или перестраивать все системы для уничтожения несанкционированного доступа, перед этим подумайте о криминалистическом захвате, чтобы сохранить доказательства угроз. [AU-11: Audit Record Retention | (1) Long-Term Retrieval Capability; MP-6: Media Sanitization | (8) Remote Purging or Wiping of Information; SI-14: Non-Persistence; SI-18: Information Disposal]

4. Внедряйте, документируйте и обеспечивайте соблюдение базовых конфигураций систем организации, чтобы криминалистам было легче определить, какие сведения могла изменить угроза. [CM-2: Baseline Configuration | (7) Configure Systems and Components for High-Risk Areas; SC-34: Non-Modifiable Executable Programs]
5. Проводите обучение и моделируемые учения для специалистов по криминалистике, чтобы при инциденте безопасности они могли эффективно отреагировать. [IR-2: Incident Response Training | (1) Simulated Events]
6. Создайте группу криминалистического анализа, имеющую возможности и полномочия для сбора данных и расследования в реальном времени. [IR-10: Integrated Information Security Analysis Team]
7. Применяйте защитные меры для проверки того, что криминалистические системы, программы и оборудование не были подделаны. [SA-12: Supply Chain Risk Management | (10) Validate as Genuine and Not Altered | (14) Identity and Traceability]

Разбор

В этой главе мы рассмотрели приёмы синоби для захвата и допроса вражеских синоби, а также тактики уклонения от плена. Мы кратко обсудили, почему сбор большего количества криминалистических доказательств даёт субъекту угроз больше возможностей снабжать следователей ложными данными и почему взаимодействие с живыми угрозами может быть предпочтительнее. Мы разобрали передовые методы создания криминалистических возможностей для наблюдения за угрозами и более сложные приёмы противодействия им - засады и ловушки.

В следующей главе мы обсудим самый разрушительный вид нападения из арсенала синоби - атаку огнём.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), 96.
[2] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), 102.
[3] [назад] Cummins and Minami, *The Book of Ninja*, 160, 420, 464, 467.
[4] [назад] Cummins and Minami, *The Book of Ninja*, 161.
[5] [назад] Cummins and Minami, *The Book of Ninja*, 213, 219, 221.
[6] [назад] Cummins and Minami, *The Book of Ninja*, 216.
[7] [назад] Cummins and Minami, *Secret Traditions*, 154.

Глава 17. Огненная атака

> Во-первых, разжечь пожар легко; во-вторых, врагу непросто его потушить; и, в-третьих, если в это же время ваши союзники идут на штурм замка, враг лишится всех преимуществ, поскольку укрепления останутся без достаточной охраны.

> Если вы собираетесь поджечь замок или лагерь врага, нужно заранее согласовать с союзниками время возгорания.
>
> - «Ёсимори хякусю», стихотворение 83

Одним из самых действенных поступков синоби после проникновения в замок или укрепление был поджог - в идеале внутри или рядом со складами пороха, древесины, продовольствия и припасов либо с мостами. Правильно устроенный пожар быстро распространялся, оставаясь незаметным; его было трудно сдержать или потушить; он немедленно создавал опасность для целостности замка, его запасов и обитателей. Защитникам приходилось выбирать между тушением пламени и боем с вражеской армией, которой поджигатель подал сигнал к нападению. Попытка вести оба сражения сразу ослабляла способность цели справиться с каждым из них. Тушивших пожар легко сметали наступавшие воины, а игнорировавшие огонь ради оружия в итоге проигрывали битву, как бы хорошо ни сражались.[1]

Свитки подробно рассказывают об огненных атаках, в том числе о разнообразных инструментах, тактике и навыках их проведения. До нападения синоби изучали обитателей замка, выясняя, когда те спят и в какое время ключевые позиции остаются без охраны. Затем они согласовывали время с другими нападавшими. Для таких атак синоби создавали множество специальных средств: зажигательные стрелы, скрытые цилиндры для переноса огня, наземные мины, бомбы и метательные факелы.[2] Одним из самых зрелищных видов оружия были «огненные кони» - лошади, к сёдлам которых привязывали специальные факелы, после чего животных отпускали бешено носиться внутри укреплений. Они хаотично разносили огонь, отвлекали стражников и жителей, и остановить их было трудно. Среди сумятицы синоби связывались с силами, скрывавшимися снаружи замка, и подавали сигнал к нападению, когда пожар достаточно распространялся.[3]

Средневековые армии могли начинать огненную атаку издалека - например, выпускать лучников с зажигательными стрелами, - однако «Бансэнсюкай» советует полководцам поручать поджог синоби. По сравнению с внешним нападением устроенный синоби пожар заметили бы и потушили не так быстро. Кроме того, синоби мог разжечь его рядом с горючими или стратегически ценными предметами и поддерживать пламя, пока оно не усилится.[4]

Огненные атаки оказались настолько успешными и повсеместными в феодальной Японии, что во многих замках начали применять специальные контрмеры. Укрепления защищали от огня методом *додзо-дзукури* - «оштукатуренной огнезащитой» - или огнестойким лаком,[5] строили из негорючих либо огнестойких материалов, таких как глина и камень, использовали огнестойкую черепицу, создавали пожарные дозоры и противопожарные разрывы, выделяя малозначимые здания, которыми можно было пожертвовать, чтобы пламя не достигло критически важной инфраструктуры.[6] Стражников также предупреждали, что пожар может быть намеренным отвлечением, облегчающим кражу, нападение или иные действия.[7] Позднее тот же совет появился в руководстве «Гунпо дзийосю».[8]

Важно помнить, что у синоби не было автоматических зажигалок, а защитники постоянно высматривали поджигателей, подобно современным организациям, которые повсюду поддерживают антивирусы и средства обнаружения угроз. Синоби разрабатывали изобретательные способы скрытно доставлять огонь, превращать его в оружие и использовать

горючие цели. Размышляя о доставке и применении кибератак против целей, не забывайте об изобретательности синоби в огненных атаках.

В этой главе мы увидим, что в контексте кибервойны огненные атаки синоби удивительно похожи на современную гибридную тактику. Огонь - прекрасная аналогия для червеобразных, самораспространяющихся кибератак, поскольку он охватывает всё, к чему может прикоснуться. Мы рассмотрим примеры разрушительных кибератак и способы, которыми современные противники выбирают время и координируют их. Кратко разберём разнообразные средства, применяемые организациями для предотвращения, смягчения, сдерживания атак и восстановления после них. Выводы из этой главы относятся как к межсетевым экранам, так и к новым, более совершенным стратегиям защиты сетей.

Разрушительные кибератаки

Вскоре после появления у компьютеров способности соединяться и обмениваться данными родились самораспространяющиеся вирусы и черви. Со временем разрушительные атаки становились лишь многочисленнее. Теперь такая атака на сеть одной организации способна быстро распространиться, словно огонь, уничтожая системы и данные по всему интернету. С учётом растущей взаимосвязанности систем в киберпространстве и присущих им недостатков безопасности подключённая к интернету сеть или машина без исправлений и иных защитных мер - это, по сути, растопка, которая только и ждёт искры.

В начале 2000-х отрасль столкнулась с первыми атаками программ-вымогателей. Вредоносная программа шифрует данные системы или сети и удаляет резервные копии, пока цель не заплатит за расшифровку. Такие вирусы быстро распространяются из систем в сетевые хранилища и облака, удерживая данные в заложниках или, при отказе от оплаты, уничтожая их посредством шифрования. Как и огненные атаки ниндзя, программы-вымогатели часто отвлекают внимание от более крупных замыслов. Например, противники, которых считают северокорейскими, развернули программу-вымогатель FEIB Hermes, чтобы отвлечь киберзащитников, пока проводилась финансовая атака на SWIFT, принёсшая нападавшим миллионы долларов.[9]

Затем появились атаки вредоносных программ-вайперов: противник устанавливает в нескольких системах вирусы с «часовым механизмом», чтобы в выбранное удобное время удалить все системные данные и стереть резервные копии. Один из примеров - вирус Shamoon, атаку которого приписывают иранским субъектам угроз, действовавшим против Саудовской Аравии. Его запустили в начале праздничных выходных, чтобы уничтожить данные и вывести из строя промышленные нефтяные системы.[10]

В последнее время злоумышленники развёртывают диверсионные вредоносные программы против промышленных систем управления, получая возможность считывать показания датчиков или управлять механическими переключателями, соленоидами и другими физическими исполнительными механизмами доменных печей,[11] электросетей,[12] систем противовоздушной обороны[13] и ядерных центрифуг.[14] Такая атака может вывести критически важные системы из строя или нарушить их работу, что способно привести ко взрывам, иным физическим разрушениям или одновременным кинетическим атакам.

Административные меры против распространения атак включают сокращение поверхности атаки за счёт усиления систем, чтобы при нападении точно настроенные средства безопасности ограничивали ущерб. Полезна и устойчивость: несколько резервных копий систем и данных в других местах и сетях дают организации запасной вариант, когда кибератака успешно компрометирует основные системы. Иногда такими копиями служат даже аналоговые или ручные системы.

К более техническим защитным решениям относится размещение межсетевых экранов по периметру сети. Однако если злоумышленник обходит их, проникает в сеть и запускает самораспространяющуюся разрушительную атаку, межсетевой экран может выпустить её наружу: обычно экраны предназначены для блокирования входящих, а не исходящих атак. К другим средствам обнаружения и остановки разрушительных атак относятся антивирусы, системы предотвращения вторжений (intrusion prevention system, IPS), хостовые системы обнаружения вторжений (host intrusion detection system, HIDS) и объекты групповой политики (Group Policy Object, GPO). Такие технические меры способны немедленно выявить разрушительную атаку, отреагировать на неё и нейтрализовать, но обычно основаны на сигнатурах и потому эффективны не всегда.

Более новый подход - киберстрахование, то есть соглашение, защищающее организацию от правовых и финансовых последствий взлома. Такой полис может снизить ответственность организации при кибератаке, но от самой атаки не защищает, как страховка от пожара не защищает от пламени.

Пожалуй, лучший вариант защиты от разрушительных атак - строгая сегрегация и изоляция сети, включая физический разрыв, которые ограничивают доступ к ресурсам и не дают самораспространяющемуся вирусу идти дальше. Это исключительно эффективный способ блокирования кибератаки, но он не всегда осуществим из-за потенциально серьёзного влияния на деловые функции. Кроме того, его можно обойти посредством переноса данных на физических носителях и внутренних угроз.

Защита от огненных кибератак

Организации обычно приобретают страховку от пожара и следуют стратегиям его предотвращения и сдерживания. Однако некоторые по неизвестной причине покупают киберстрахование, не внедряя защиту от кибератак. Возможно, они не видят в них того же риска, что в настоящем пожаре, где под угрозой в конце концов оказываются имущество и даже человеческие жизни. Но с ростом интернета вещей (Internet of Things, IoT) и всё более тесным сближением физического мира с киберпространством риски будут лишь возрастать. Следующие защитные меры могут чрезвычайно помочь вашей организации:

1. **Проводите учебные киберпожары.** Моделируйте разрушительные атаки, чтобы проверять резервные копии, аварийное переключение, скорость реакции, восстановление и способность своевременно «эвакуировать» данные или системы. Такие учения отличаются от проверки аварийного восстановления или резервных копий тем, что с сетью взаимодействует активная моделируемая угроза, а не воображаемый сценарий. Примите меры, например шифруйте данные известным ключом, чтобы не уничтожить их во время учений.

Netflix постоянно проводит учение под названием Chaos Monkey, которое случайным образом отключает серверы, нарушает конфигурации и выключает службы. Поэтому организация непрерывно проверяет, может ли без проблем плавно и немедленно перераспределить нагрузку или переключиться на резерв. На случай настоящей неполадки группа безопасности уже разработала и испытала работоспособные решения. Netflix бесплатно опубликовала Chaos Monkey, поэтому любая организация может применить его, чтобы улучшить способность обнаруживать разрушительные атаки, противостоять им, реагировать и восстанавливаться.[15]

2. **Защищайте системы от киберогня.** Выделяйте ресурсы на изучение того, как распространяется выбранная разрушительная атака, что она уничтожает и почему ваши системы уязвимы для неё. Внедряйте адаптеры жёстких дисков только для чтения, выполняющие операции в буфере накопителя: данные остаются запертыми «за стеклом», и их невозможно уничтожить, поскольку в режиме только для чтения с ними ничто не взаимодействует. Удаляйте «горючее» программное обеспечение - приложения, библиотеки, функции и иные системные компоненты, о которых известно, что они распространяют разрушительные атаки.

   Разработка специализированных программ, оборудования и устройств для защиты систем от киберогня представляет коммерческую возможность. Такие решения могли бы оказать большое влияние на рынок, сделав серверы или данные устойчивыми к разрушительным атакам либо хотя бы замедлив или остановив их развитие.

3. **Устанавливайте кибернетические огненные ловушки.** Существует большая рыночная возможность для создания автоматизированных обманных «огненных киберловушек», которые заманивают противников или вредоносные программы в бесконечные циклы либо запускают механизмы, заставляющие атаку саму поместить себя в карантин, погасить или сдержать. Один хитроумный публично описанный способ защиты - создать в общих сетевых ресурсах папки с бесконечно рекурсивными каталогами. Когда вредоносная программа пытается перебирать папки в поиске новых данных, она застревает в бесконечном цикле.[16] Специализированные датчики могли бы обнаруживать такое поведение, а затем либо предупреждать группы реагирования на инциденты, либо отдавать команду завершить запустивший бесконечный обход процесс.

4. **Создавайте динамические противопожарные разрывы в сети.** Кибератаки так легко распространяются потому, что системы обычно включены и связаны друг с другом. Даже если атака не может напрямую скомпрометировать конкретную систему, она способна перейти на другие взаимосвязанные системы. Это снова и снова демонстрируют сотни тысяч, если не миллионы, ботнетов, червей и прочих самораспространяющихся вредоносных программ в киберпространстве.

   Хотя сегрегация и изоляция сети чаще всего задаются статической архитектурой, ИТ-подразделения могут внедрять дополнительные ручные и программные линии «разрыва». Известно, что некоторые организации устанавливают главный соленоидный выключатель, вручную отключающий организацию от интернета. Обмен данными во внутренней сети продолжается, но все внешние сетевые соединения немедленно разрываются, создавая физический воздушный зазор. Такая возможность может показаться чрезмерной или ненужной, но при глобальном «киберпожаре» организация сможет быстро и легко отделиться от угрозы, не перерубая кабели пожарным топором.

   В одном из вариантов реализации у каждой системы, комнаты, этажа и здания был бы собственный главный выключатель, позволяющий сотрудникам безопасности быстро принимать решения и срывать разрушительные атаки. Получив от руководства предупреждение об атаке, сотрудники могли бы быстро загрузить критически важные рабочие документы, а затем щёлкнуть выключателем, отделив компьютер от сети и предотвратив распространение атаки.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка с ценными активами внутри. Вы тратите значительную часть состояния на защиту замка от огня: строите его из камня, укрепляете всеми новейшими противопожарными технологиями и обучаете стражников реагированию на пожар.

В чём вы всё ещё уязвимы для огненной атаки? Например, как защитить или переместить склады пороха? Можно ли изолировать их и одновременно удовлетворить военных советников, утверждающих, что без быстрого доступа к пороху армия не защитит замок? Как оградить от огня продовольственные склады, не испортив пищу? Как очищать или фильтровать товары, поступающие в замок, чтобы не допустить оборота горючих материалов? Где устроить противопожарные разрывы в лагерях, казармах и других частях замка? Какие огненные ловушки можно спроектировать, чтобы сдержать или погасить распространяющееся пламя либо поймать поджигателя? Можно ли разработать пожарное учение с настоящим огнём, которое обучит воинов, но не подвергнет замок риску?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую следует оценивать с учётом концепции огненных атак.

1. Отслеживайте признаки разрушительных действий внутри организации. Не допускайте подделки журналов наблюдения за системами, событий аудита и данных датчиков, пересылая сведения в сегментированные сборщики событий. [AU-6: Audit Review, Analysis, and Reporting | (7) Permitted Actions; AU-9: Protection of Audit Information; SI-4: System Monitoring]
2. Внедрите сегрегацию и изоляцию сетей, систем и процессов, чтобы снизить способность разрушительных атак распространяться по сети. [CA-3: System Interconnections; SC-3: Security Function Isolation; SC-7: Boundary Protection | (21) Isolation of System Components; SC-11: Trusted Path | (1) Logical Isolation; SC-39: Process Isolation]
3. Проводите проверку резервных копий и учения на устойчивость, чтобы выяснить, работают ли механизмы восстановления и защиты от отказов должным образом. [CP-9: System Backup | (1) Testing for Reliability and Integrity | (2) Test Restoration Using Sampling; CP-10: System Recovery and Reconstitution | (1) Contingency Plan Testing]
4. Требуйте двойного разрешения от квалифицированных уполномоченных лиц перед выполнением команд, удаляющих или уничтожающих данные. [CP-9: System Backup | (7) Dual Authorization]
5. Внедрите меры для поддержания безопасности организации при разрушительной атаке, вызывающей отказ защитных систем. Например, настройте межсетевые экраны так, чтобы при отключении они блокировали всё, а не разрешали всё, либо переводите системы в «безопасный режим» при обнаружении атаки. [CP-12: Safe Mode; SC-24: Fail in Known State]

6. Поддерживайте механизмы транспортировки носителей, защищённые от разрушительных атак. Например, жёсткий диск с конфиденциальными данными должен быть отключён, не подключён к сети и храниться в безопасном месте, где его не повредит физически разрушительная атака, такая как настоящий пожар. [MP-5: Media Transport; PE-18: Location of System Components; SC-28: Protection of Information at Rest]
7. Перед подключением переносных носителей или устройств к системам либо сетям организации проверяйте и сканируйте их на наличие вредоносного программного обеспечения. [MP-6: Media Sanitization; SC-41: Port and I/O Device Access]
8. Проводите оценку рисков, чтобы определить, компрометация каких данных и систем нанесёт организации наибольший ущерб. Принимайте повышенные меры предосторожности и устанавливайте специальные средства защиты для этих систем и данных. [RA-3: Risk Assessment; SA-20: Customized Development of Critical Components]
9. Создавайте защитные средства, например механизмы противодействия вредоносному коду и камеры детонации, для поиска признаков возможностей разрушительной атаки. [SC-44: Detonation Chambers; SI-3: Malicious Code Protection]

Разбор

В этой главе мы рассмотрели огненные атаки и разнообразные приёмы, с помощью которых синоби скрытно переносили пламя и превращали огонь в оружие. Мы разобрали несколько известных кибератак и способы защиты от них, а также в более общем виде увидели, как киберугрозы становятся цифровым двойником огненных атак.

В следующей главе мы подробно обсудим, как синоби связывались с внешними союзниками и координировали с ними начало огненной атаки. Синоби множеством хитроумных способов осуществляли скрытую связь командования и управления (command and control, C2), и эти способы похожи на методы связи C2, применяемые некоторыми вредоносными программами.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), 62.
[2] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), 31-34, 87-91, 167.
[3] [назад] Cummins and Minami, *Secret Traditions*, 90.
[4] [назад] Cummins and Minami, *The Book of Ninja*, 61.
[5] [назад] Motoo Hinago and William Coaldrake, *Japanese Castles* (New York: Kodansha USA, 1986), 98.
[6] [назад] Cummins and Minami, *Secret Traditions*, 119.
[7] [назад] Cummins and Minami, *The Book of Ninja*, 75-76.
[8] [назад] Cummins and Minami, *Secret Traditions*, 162.
[9] [назад] Pierluigi Paganini, “BAE Systems report links Taiwan heist to North Korean LAZARUS APT,” *Cyber Defense Magazine*, October 18, 2017, https://bit.ly/3s3PCcS.
[10] [назад] Symantec Security Response, “Shamoon: Back from the dead and destructive as ever,” *Symantec Official Blog*, November 30, 2016, https://bit.ly/3oqdkxK.
[11] [назад] Kim Zetter, “A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever,” *WIRED*, January 8, 2015, https://bit.ly/3nqx0Aj.
[12] [назад] Andy Greenberg, “‘Crash Override’: The Malware That Took Down a Power Grid,” *WIRED*, June 12, 2017, https://bit.ly/38oMhgz.
[13] [назад] Sharon Weinberger, “How Israel Spoofed Syria’s Air Defense System,” *WIRED*, October 4, 2017, https://bit.ly/35i67Za.
[14] [назад] Kim Zetter, “An Unprotected Look at STUXNET, the World’s First Digital Weapon,” *WIRED*, November 3, 2014, https://bit.ly/3ooEULS.
[15] [назад] Подробнее см. “Chaos Monkey,” GitHub, Inc., Lorin Hochstein, последнее изменение 31 июля 2017 года, https://bit.ly/3noAJhL.
[16] [назад] Allan Liska and Timothy Gallo, *Ransomware: Defending Against Digital Extortion* (Sebastopol, CA: O’Reilly Media, 2017), 73.

Глава 18. Скрытная связь

> Когда синоби собирается связаться с полководцем после проникновения во вражеский замок, ему необходимо сообщить союзникам, где он находится. Для этого крайне важно заранее согласовать время и место.

> Чтобы ночное нападение завершилось успехом, заблаговременно отправьте синоби выяснить подробности расположения врага, прежде чем отдавать приказы.
>
> - «Ёсимори хякусю», стихотворение 12

Поскольку синоби прежде всего были специалистами по шпионажу, им приходилось безопасно передавать секретные сообщения с отчётами о разведке, планами нападений и другими критически важными сведениями, помогавшими господам и союзникам принимать обоснованные тактические и стратегические решения. Точно так же господа, полководцы и другие синоби должны были скрытно сообщать внедрённому синоби, когда поджечь объект или применить иную тактику. Получатель-синоби должен был легко расшифровать сообщение, а для всех остальных оно обязано было оставаться непонятным.

Свитки «Бансэнсюкай», «Нинпидэн» и «Гунпо дзийосю» описывают тайные способы, которыми синоби после проникновения на вражескую территорию связывались с другими синоби, дружественными армиями или нанимателями. Некоторые были предельно просты и жестоки. «Бансэнсюкай» рассказывает, как послание прятали в брюхе рыбы или даже внутри человека - можете дать волю воображению, - способного без подозрений пересекать границы. Обычно выбирали монахов и нищих. В том же свитке упоминаются способы сокрытия: разрезать сообщение на несколько частей и отправить каждую с отдельным гонцом, чтобы получатель собрал их вместе; приготовить из мандаринового сока, ржавой воды, саке или касторового масла чернила, которые высыхают на бумаге невидимыми, но проявляются над огнём. Синоби даже разработали *синоби ироха* - особую азбуку, непонятную непосвящённым, - и применяли фрагменты слов или знаков, создавая контекстную неоднозначность, которую понимал лишь предназначенный получатель.[1]

Популярным и прямым способом передачи тайных посланий был *ябумэ*: на вид обычная стрела несла тайный свиток, обёрнутый вокруг бамбукового древка, а метки на оперении указывали получателя. Из-за материальных условий феодальной Японии синоби не всегда могли гарантировать выстрел стрелой *ябумэ* в заранее согласованные время и место, поэтому разработали «рукопожатие» стрелами, которое постороннему могло показаться перестрелкой. Заметив, что с одной стороны в одну точку быстро выпустили определённое число стрел, другая сторона отвечала установленным числом стрел, нацеленных так, чтобы упасть перед стрелком. Этот сигнал и ответный сигнал устанавливали дружественное соединение. После этого синоби выпускал стрелу *ябумэ*, которую подбирали и доставляли адресату.[2] Такой способ связи стал настолько распространённым, что руководство «Гунпо дзийосю» предупреждает: враг может отправлять стрелами обманные письма, поэтому получателю следует тщательно исследовать сообщения *ябумэ* с помощью некоторых языковых приёмов, описанных ранее в этой книге.[3]

Для сигналов на большие расстояния или когда отправить свиток было невозможно синоби придумали сигналы флагами, огнём, дымом и фонарями (*хикякуби*). Если не подходили даже они, применялись тайные барабаны, гонги и раковины. Громкий и необычный звук сигнального устройства сообщал синоби во вражеских рядах, что нужно приготовиться принять секретное сообщение. Точный рисунок сигнала согласовывали за один-шесть дней до проникновения, чтобы избежать путаницы. После начального сигнала *хикякуби* сообщение передавали ударами барабана, гонга или звуками раковины.[4]

В этой главе мы увидим, насколько скрытные способы связи синоби похожи на современную связь командования и управления вредоносными программами. Мы обсудим, зачем нужна такая связь и какую роль она играет в действиях угроз. Кратко рассмотрим различные приёмы, которыми современные противники скрытно поддерживают связь, а также защиту от них и связанные с ней трудности. Наконец, приведём обширный перечень лучших методов безопасности против связи командования и управления. То, что свитки синоби не дают наставлений по пресечению тайной связи, наводит на мысль: хорошего решения этой задачи может и не существовать.

Связь командования и управления

Обычно вредоносная программа не может быть полностью независимой и автономной. В противном случае она была бы чрезвычайно большой, сложной, подозрительной и заметной для защитников. Большинству вредоносных программ во время кампании угроз необходимы тактические указания операторов. Поэтому субъекты угроз применяют приём, называемый командованием и управлением (command and control, сокращённо C2, CnC или C&C), чтобы связываться с вредоносными программами, бэкдорами, имплантатами и скомпрометированными системами под своим управлением в целевых сетях. Через C2 операторы отправляют скомпрометированной системе команды, побуждая её загружать данные, обновлять конфигурацию или даже удалять себя. Имплантат C2 тоже может начинать связь: отправлять статистику или ценные файлы, запрашивать новые команды либо передавать маячковый сигнал с сообщением, что система подключена, указывая её местоположение и текущее состояние. Субъекты киберугроз часто создают инфраструктуру C2, такую как доменные имена, IP-адреса и сайты, за одну-шесть недель до проникновения.

Функции C2 широко известны, и многие межсетевые экраны, IDS/IPS и другие защитные устройства и средства способны не дать противнику напрямую связываться с целевыми системами и наоборот. Для обхода этих средств субъекты угроз непрерывно разрабатывают более совершенные методы, тактику и процедуры C2 (techniques, tactics, and procedures, TTP). Например, данные C2 можно встроить в полезную нагрузку ping или спрятать команды в изображениях на общедоступных сайтах. Противники размещали C2 в лентах Twitter и комментариях на доверенных сайтах. Кроме того, с помощью C2 они создавали прокси и почтовые ретрансляторы в скомпрометированных системах, после чего связывались через известные протоколы и безопасные сайты, не блокируемые защитными средствами и устройствами. Подключённый к скомпрометированной системе телефон можно заразить вредоносной программой, которая при соединении по USB «звонит» C2 через вышки сотовой связи, обходя межсетевые экраны и другую сетевую защиту и обеспечивая обмен между заражённым узлом и C2, пока телефон заряжается. Некоторые методы C2 используют мигающие светодиоды, словно сигнальный огонь, изменяют температуру процессора, как дымовой сигнал, задействуют звуки жёстких дисков или динамиков компьютера, как сигнальные барабаны, и используют волны электромагнитного спектра, чтобы преодолеть воздушный зазор до соседней машины.

Субъекты угроз наслаивают на связь C2 запутывание, шифрование и другие методы конфиденциальности, чтобы сохранять контакт со скомпрометированной системой, не раскрывая жертвам свидетельств команд. Противники могут избегать обнаружения следующими способами:

- ограничивать объём ежедневно передаваемых данных, чтобы он никогда не казался аномальным, например не более 100 МБ в день для маскировки загрузки 1,5 ТБ за две недели;
- отправлять или принимать маячковые сигналы только во время активности пользователя, сливаясь с его законным трафиком, например редко подавать сигнал глубокой ночью в воскресенье или праздник;
- переходить к новым, случайным или динамическим точкам C2, чтобы избегать статистических аномалий;
- регулярно создавать псевдозаконный трафик, не вызывая подозрений поведенческого анализа;
- отключать или удалять журналы действий, скрываясь от криминалистики.

Совершенные TTP C2 могут быть особенно зловещими, практически необнаружимыми и трудными для блокирования. Представьте администратора Windows, который установил настолько строгие правила межсетевого экрана, что может посещать только technet.microsoft.com - официальный веб-портал Microsoft для ИТ-специалистов. Разрешён лишь протокол HTTPS, антивирус обновлён и работает, а операционная система полностью исправлена. Ни одна внешняя программа, такая как почта, Skype или iTunes, не запущена; исключение составляет сайт Microsoft TechNet, необходимый администратору для работы. Это может показаться безопасным, однако китайская группа APT17, также известная как Deputy Dog или Aurora Panda, кодировала скрытые IP-адреса в комментариях на страницах Microsoft TechNet. Эти комментарии связывались с трояном удалённого доступа BLACKCOFFEE в скомпрометированной системе.[5] При проверке прокси-трафика, поведенческого анализа, эвристики аномалий, сигнатур IDS, антивирусных данных или предупреждений межсетевого экрана ничто примечательное не указывало бы на вредоносную связь.

Передовые меры против искушённых C2 обычно предполагают физическое разделение систем, однако в последние годы появились новые способы связи. Например, USB-накопитель с руткитами либо скомпрометированной микропрограммой и вредоносным ПО после подключения к системе начинает обмен с имплантатом на скомпрометированной машине, собирает упакованные данные и незаметно выгружает их для вывода на внешний C2.

Контроль связи

Организации часто подписываются на несколько потоков индикаторов угроз. Они непрерывно снабжают организацию вредоносными URL, IP-адресами и доменами, замеченными в роли C2. Затем организация создаёт предупреждения и/или блокирует эти угрозы на межсетевых экранах и защитных устройствах. Это хорошая отправная точка для защиты от C2, но новые URL, IP-адреса и домены появляются без конца, позволяя субъектам угроз принимать новые личности и уходить от потоков индикаторов. Для противодействия C2 нужны и старые, и новые подходы; некоторые предлагаются ниже.

1. **Следуйте лучшим методам.** Предотвратить всю связь C2 может быть непрактично или даже невозможно, но базовую и умеренно сложную связь можно блокировать, внедряя лучшие методы кибербезопасности: знайте свою сеть, устанавливайте средства контроля границ и потоков, создавайте белые списки и уполномочивайте группы охоты упреждающе блокировать либо перехватывать связь C2. Не сокращайте путь ценой отказа от лучших методов. Возьмите обязательство выполнять основательную работу по безопасности. Документируйте, испытывайте и проверяйте свои методы, а за дополнительными мерами и независимой проверкой обращайтесь к сторонним экспертам. Вкладывайтесь в улучшение безопасности, одновременно поддерживая и совершенствуя существующую инфраструктуру лучших методов.
2. **Внедрите сегментацию со средствами «удалённого просмотра».** Сегментация и изоляция сети означают создание нескольких отделённых друг от друга сетей и машин, например компьютера внутренней сети и несекретного компьютера с интернетом. Сегментация должна не позволять связи C2 пересекать границы. К сожалению, пользователи нередко на короткое время подключают компьютер внутренней сети к интернету, чтобы загрузить документы или библиотеки, либо иным образом нарушают правила безопасности. Один из подходов - настроить компьютер внутренней сети для удалённого просмотра другой изолированной машины, подключённой к интернету. Пользователи не имеют к изолированному интернет-компьютеру физического или прямого доступа: они могут отдавать команды и видеть экран, но не получают исходные необработанные данные этой машины в своём окне удалённого просмотра. Такое окно фактически служит телевизором, показывающим компьютер в другой комнате. Поэтому связь C2, вредоносные программы и эксплойты не могут перескочить через видеосигнал и причинить вред.

> **Упражнение «Теория замка».** Представьте, что вы правитель средневекового замка с ценными активами внутри. Каждую неделю писцы создают новые свитки, излагающие государственные тайны, новые исследования и открытия, финансовые сведения и другие конфиденциальные данные. Крайне важно, чтобы эти свитки не оказались у врага. Однако ходят слухи, что кто-то делает копии важных свитков в вашей личной библиотеке, а недавние действия врага, похоже, подтверждают сообщения. Никто не подозревает писцов или архивариусов в копировании и выносе свитков, поэтому вы не ищете внутреннюю угрозу.
>
> Какие ограничения доступа или средства физической защиты можно установить, чтобы предотвратить вынос или копирование свитков? Как отслеживать их кражу или удаление, сохраняя нормальное движение товаров и людей в замок и из него? Можно ли хранить свитки так, чтобы враг не знал, какие из них наиболее ценны? Какими ещё способами субъект угроз способен получить доступ к свиткам или похитить сведения без доступа и как от этого защититься?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую следует оценивать с учётом концепции C2.

1. Внедрите в системах, на сетевых границах и в точках выхода из сети защитные средства, ищущие признаки вывода данных. Это может означать блокирование зашифрованных туннелей, которые датчики не способны перехватить, а также поиск несанкционированных протоколов, форматов данных, водяных знаков, меток конфиденциальности и крупных файлов или потоков, покидающих сеть. [AC-4: Information Flow Enforcement | (4) Content Check Encrypted Information; SC-7: Boundary Protection | (10) Prevent Exfiltration; SI-4: System Monitoring | (10) Visibility of Encrypted Communications]
2. Создайте несколько сетей с изоляцией и сегментацией между ресурсами интернета и внутренней сети. Запретите критически важным внутренним системам подключаться к интернету. [AC-4: Information Flow Enforcement | (21) Physical and Logical Separation of Information Flows; CA-3: System Interconnections | (1) Unclassified National Security System Connections | (2) Classified National Security System Connections | (5) Restrictions on External System Connections; SC-7: Boundary Protection | (1) Physically Separated Subnetworks | (11) Restrict Incoming Communications Traffic | (22) Separate Subnets for Connecting to Different Security Domains]
3. Ограничьте удалённый доступ ко всем системам с критически важными сведениями. [AC-17: Remote Access]
4. Внедрите ограничения и средства контроля конфигурации для обнаружения и предотвращения несанкционированной беспроводной связи. [AC-18: Wireless Access | (2) Monitoring Unauthorized Connections; PE-19: Information Leakage; SC-31: Covert Channel Analysis; SC-40: Wireless Link Protection; SI-4: System Monitoring | (15) Wireless to Wireline Communications]
5. Обучите группу безопасности и сотрудников выявлять связь C2. [AT-3: Role-based Training | (4) Suspicious Communications and Anomalous System Behavior; SI-4: System Monitoring | (11) Analyze Communications Traffic Anomalies | (13) Analyze Traffic and Event Patterns | (18) Analyze Traffic and Covert Exfiltration]
6. Запретите запуск в системах любого несанкционированного программного обеспечения, которое может оказаться бэкдором или имплантатом C2. [CM-7: Least Functionality | (5) Authorized Software-Whitelisting]
7. Защитите прямые физические подключения к системам, обходящие средства и границы безопасности, включая коммутационные шкафы, настенные разъёмы Ethernet и интерфейсы компьютеров. [PE-6: Monitoring Physical Access; SC-7: Boundary Protection | (14) Protects Against Unauthorized Physical Connections | (19) Block communication from non-organizationally configured hosts]
8. Требуйте проверять и сканировать съёмные носители, входящие в организацию и покидающие её, чтобы сотрудники не могли вручную поддерживать связь C2 посредством доставки и удаления внешних носителей. [PE-16: Delivery and Removal]
9. Внедрите белый список, запрещающий связь со всеми ресурсами или адресами, для которых не утверждено исключение. Многие сайты C2 - совершенно новые домены без истории законного использования в вашей организации. [SC-7: Boundary Protection | (5) Deny by Default-Allow by Exception]

Разбор

В этой главе мы рассмотрели различные способы связи, которыми синоби пользовались для получения и передачи команд союзникам. Мы описали современные методы C2 и сопоставимые приёмы синоби. Однако мы лишь коснулись поверхности: весьма вероятно, что самые искушённые методы C2 ещё не обнаружены. Как лучшие способы тайной связи синоби никогда не записывались, так и мы можем никогда не узнать о гениальности и изобретательности самых передовых приёмов C2. Мы обсудили несколько лучших методов, включая белые списки и проверку шифрования, которые смягчают воздействие C2 противника, но идеального решения задачи пока нет.

В следующей главе мы поговорим о позывных синоби. Так союзникам на вражеской территории передавали сообщения, оставляя особые метки или знаки. Подобно тайнику, позывные никогда не покидают границ среды, поэтому традиционные методы блокирования или обнаружения связи C2 против них обычно не работают.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), 67-69, 102.
[2] [назад] Cummins and Minami, *The Book of Ninja*, 70.
[3] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), 96.
[4] [назад] Cummins and Minami, *The Book of Ninja*, 70-72.
[5] [назад] “APT17,” *Advanced Persistent Threat Groups*, FireEye Inc., дата последнего обращения 7 февраля 2020 года, https://bit.ly/2XI1QQ7.

Глава 19. Позывные

> Проникнув внутрь, прежде всего отметьте путь, показывая союзникам выход и способ отступления.

> Успешно проскользнув во владения врага, уделяйте больше внимания тому, чтобы случайно не вступить в бой со своими, чем самому врагу.
>
> - «Ёсимори хякусю», стихотворение 26

Хотя массовая культура часто изображает синоби одиночками, многие из них работали группами. Такие группы особенно искусно и незаметно передавали друг другу сведения на местности. Руководство «Гунпо дзийосю» описывает три позывных, то есть физических метки, разработанных синоби для незаметного общения друг с другом. В зависимости от вида и места размещения позывные среди прочего помогали определить цель, указывали нужную дорогу на развилке, направляли к вражескому укреплению или координировали нападение. Хотя позывные были хорошо известны среди синоби, участники перед заданием согласовывали особые варианты, чтобы цели и даже вражеские синоби не смогли распознать метки на местности. Свитки советуют применять переносные и одноразовые метки, которые можно быстро установить и убрать на уровне земли. Самое важное: метка должна была быть зрительно уникальной, но ничем не примечательной для непосвящённого.

Например, синоби могли условиться сообщать товарищам о своём местонахождении, оставляя окрашенные зёрна риса в заранее выбранном, на вид безобидном месте. Один оставлял красный рис, другой - зелёный и так далее. Увидев несколько цветных зёрен, товарищ понимал, что союзник уже проходил здесь. Красота системы состояла в том, что синоби быстро узнавали эти предметы, тогда как обычные прохожие не замечали нескольких странно окрашенных рисовых зёрен. Подобным образом синоби мог направить обломок бамбука в сторону выбранной тропы для союзника или оставить на земле небольшой кусок бумаги, отмечая дом, который предстояло сжечь, и тем самым снижая вероятность того, что участники группы окажутся жертвами или подозреваемыми в поджоге.[1]

В этой главе мы исследуем способы применения позывных в сетевых средах и причины, по которым субъекты киберугроз могут ими пользоваться. Мы предположим, где в сети можно разместить позывные и как они могут выглядеть. Кроме того, обсудим охоту за такими метками в целевой сети. Мы рассмотрим трудность выявления изобретательных позывных и коснёмся сути этой задачи - контроля среды и наблюдения за действиями противника. В мысленном эксперименте вы сможете построить мысленные модели и найти решения проблемы вражеских позывных. Вы также познакомитесь с мерами безопасности, способными помешать субъектам угроз применять позывные в вашей среде и ограничить их возможности.

Оперативное искусство операторов

Во время взлома Национального комитета Демократической партии США в 2016 году российское военное ведомство ГРУ, также известное как APT28 или FANCYBEAR, и союзная ему служба безопасности ФСБ, известная как APT29 или COZYBEAR, действовали в одной сети и одних системах, но не применяли позывные для связи друг с другом. Из-за этого работа дублировалась, а в сети жертвы появлялись наблюдаемые признаки, аномалии и другие индикаторы компрометации, что, вероятно, способствовало провалу обеих операций.[2] Отсутствие связи, скорее всего вызванное разобщённостью двух разведывательных организаций, показывает, чему группы кибершпионажа могли бы научиться у синоби.

Хотя сообщество кибербезопасности ещё не наблюдало, чтобы пересекающиеся группы угроз применяли скрытые метки, взлом Национального комитета Демократической партии демонстрирует необходимость такого протокола. Разумно предположить, что ГРУ и ФСБ провели разбор оперативных приёмов после взлома и, возможно, уже решили внедрить протокол позывных в будущих операциях, где есть риск пересечения целей. Если кибершпионские организации начнут регулярно действовать обособленными, но пересекающимися формированиями, им понадобится способ сообщать различные сведения, включая сам факт своего присутствия в системах и сетях и подробности о целях, когда обычные каналы связи недоступны.

Если такие позывные существуют, как они выглядят? Эффективные кибернетические позывные, вероятнее всего:

- меняются со временем, как метки синоби;
- внедряются в инструменты и вредоносные программы, которые невозможно захватить и подвергнуть обратной разработке; для их обнаружения нужны люди, работающие за клавиатурой;
- находятся там, где пересекающаяся шпионская группа обязательно их обнаружит, например на ценном и уникальном основном контроллере домена (domain controller, DC). Поскольку за файлами наблюдают средства безопасности, а DC редко перезапускаются, группа угроз может поместить метку в память контроллера, максимально увеличив её долговечность и сведя к минимуму заметность.

Остаётся неясным, какие строки или уникальные шестнадцатеричные байты могли бы служить метками, в каком кеше, временной таблице или участке памяти они могли бы находиться и как другому оператору легко их обнаружить. Однако отрасль кибербезопасности наблюдала несколько семейств вредоносных программ, оставляющих особые файлы или ключи реестра как сигнал будущим копиям вируса о том, что заражение уже успешно распространилось на данную машину и повторять попытку не нужно.[3] Хотя против динамично действующих людей такую функцию позывного реализовать не столь просто, защитники могут создавать файлы и ключи реестра, ложно сообщающие о заражении, чтобы вредоносная программа безвредно прошла мимо.

Обнаружение позывных

Многие организации с трудом выясняют даже то, какой пользователь удалил файл с общего сетевого диска, не говоря уже об обнаружении скрытных позывных в удалённых областях системы. Тем не менее защитникам всё чаще придётся противостоять угрозам, которые связываются друг с другом внутри их среды. Чтобы получить шанс поймать субъектов угроз, защитникам понадобятся обучение, средства обнаружения и видимость узлов.

1. **Внедрите расширенное наблюдение за памятью.** Определите наиболее ценные системы сети - те, которые, по вашему мнению, субъект угроз выберет целью или будет вынужден использовать для дальнейшего продвижения. Затем исследуйте имеющиеся в организации возможности отслеживать и ограничивать изменения памяти в этих системах. Изучите также продукты и услуги поставщиков. Оцените объём усилий и время, необходимые для расследования источника таких изменений. Наконец, выясните, сможете ли вы уверенно определить, означают ли изменения компрометацию целевых машин.
2. **Обучайте персонал.** Научите группы безопасности, охоты и ИТ рассматривать криминалистические артефакты в памяти как возможные индикаторы компрометации, особенно если они обнаружены на ценных целях, а не отбрасывать найденные несоответствия.

> **Упражнение «Теория замка».** Представьте, что вы правитель средневекового замка с ценными активами внутри. Вы получаете надёжные разведывательные сведения о том, что группы синоби выбрали целью ваш замок и связываются друг с другом посредством позывных. Среди их тайных сигналов - неброские метки на земле: окрашенный рис, мука и обломки бамбука.
>
> Как обучить стражников замечать эти приёмы, а также методы, о которых вы ещё не подумали? Как помочь им справляться с ложными тревогами, которые неизбежно возникнут, когда ваши люди случайно рассыплют рис или животные и ветер нарушат обстановку? Какие изменения в архитектуре замка и прилегающей территории облегчат обнаружение тайных меток? Какие контрмеры уничтожат, нарушат или ослабят способность этих меток передавать сведения либо обманут синоби, которые отправляют и принимают сигналы?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую следует оценивать с учётом концепции позывных.

1. Следите за тем, чтобы сведения предыдущего пользователя были недоступны нынешним пользователям, получившим доступ к той же системе или ресурсам. [SC-4: Information in Shared Resources]
2. Выявляйте системные средства связи, которые можно применять для несанкционированных потоков информации. Хороший пример возможного скрытого канала даёт мера «PE-8: Visitor Access Records». Бумажные журналы или неограниченные цифровые устройства для регистрации посетителей на объектах могут быть уязвимы для информационных меток, сообщающих разобщённым шпионским субъектам, что другие группы уже посещали это место. [SC-31: Covert Channel Analysis]

3. Ищите индикаторы возможных атак и несанкционированного использования систем и развёртывайте устройства наблюдения для отслеживания представляющих интерес информационных операций. [SI-4: System Monitoring]
4. Защищайте системную память от несанкционированных изменений. [SI-16: Memory Protection]

Разбор

В этой главе мы рассмотрели физические метки, с помощью которых группы синоби подавали друг другу сигналы на вражеской территории. Мы узнали, зачем нужны позывные и какими свойствами, согласно свиткам, обладает хороший позывной. Затем разобрали операцию кибершпионажа, в которой отсутствие позывных и вызванная им несогласованность помогли раскрыть действия групп угроз. Мы обсудили, как современные группы угроз, вероятно, будут становиться всё искуснее и могут перенять приёмы позывных. Мы исследовали возможный вид современных цифровых позывных и способы их обнаружения.

В следующей главе мы поговорим о противоположности позывных синоби - мерах предосторожности, которые синоби по наставлениям свитков принимали, чтобы не оставить следов деятельности на вражеской территории. Передовые приёмы включали создание ложных сигналов для обмана защитника.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), 84.
[2] [назад] Dmitri Alperovitch, “CrowdStrike’s work with the Democratic National Committee: Setting the record straight,” *CrowdStrike Blog*, CrowdStrike, последнее изменение 22 января 2020 года, https://bit.ly/3rYVHr3.
[3] [назад] Charlie Osborne, “Create a single file to protect yourself from the latest ransomware attack,” *Zero Day*, ZDNet, CBS Interactive, June 28, 2017, https://bit.ly/35lPQ5d.

Глава 20. Дисциплина света, шума и мусора

> Древние традиции синоби гласят: прежде чем при свете огня осмотреть врага, следует запереть двери.

> Если вам приходится тайно проникать как синоби во время снегопада, прежде всего остерегайтесь собственных следов.
>
> - «Ёсимори хякусю», стихотворение 53

Избегать нежелательного внимания было одной из основных профессиональных дисциплин синоби, и они усердно упражнялись в скрытности. Если свет фонаря тревожил животных, шаги отдавались эхом и будили спящую цель или пищевые отходы предупреждали стражника о присутствии нарушителя, синоби подвергал опасности задание, если не собственную жизнь. Поэтому свитки дают подробные наставления о тактическом передвижении и действиях с соблюдением дисциплины света, шума и мусора.

Дисциплина света включает общие тактики. Например, свитки советуют проникшему внутрь синоби запереть дверь изнутри до того, как зажечь факел, чтобы не дать свету и находящимся в комнате людям выйти наружу.[1] Она включает и конкретные приёмы. «Бансэнсюкай» подробно описывает несколько хитроумных средств управления светом, например огненное яйцо *ториноко*. Это свёрток особого горючего материала с тлеющим угольком в центре, спрессованный до формы и размера яйца. Яйцо лежало в ладони синоби, и, раскрывая или сжимая руку, тот регулировал поступление кислорода к угольку, усиливал или ослаблял свет и направлял его в определённую узкую сторону.[2] С таким средством синоби мог быстро раскрыть ладонь и увидеть, кто спит в комнате, а затем мгновенно погасить свет, крепко сжав кулак. Таким образом, огненное яйцо обеспечивало то же направленное управление светом по требованию и включение/выключение, что современный тактический фонарь.

Тишина была для синоби критически важна, и свитки описывают множество способов бесшумного проникновения к цели. «Нинпидэн» советует зажимать зубами полоску бумаги, чтобы приглушить дыхание. Некоторые синоби передвигались в тесных местах, обхватывая ладонями подошвы ног и идя на руках, чтобы заглушить шаги. Успешное выполнение такого приёма, должно быть, требовало значительной практики и физической подготовки. Синоби также часто носили масло или другие вязкие вещества для смазывания скрипучих петель ворот и деревянных раздвижных дверей - всего, что могло скрипнуть и выдать их присутствие. Свитки предупреждают и о том, что нельзя наносить слишком много жидкости: заметная лужица могла сообщить стражнику, что здесь побывал нарушитель.[3]

Не все способы дисциплины шума были направлены на его уменьшение. Свитки дают наставления и о намеренном создании грохота. «Сёнинки» описывает приём под названием *куцукаэ*, или «смена обуви», который на самом деле предполагает изменение звука шагов, а не переобувание. Проникающий синоби мог шаркать, подпрыгивать, изображать хромоту, идти рублеными шагами или создавать отчётливый звук необычной походки, обманывая слушателя. Вернувшись затем к естественной походке, он заставлял людей предположить, что они слышат другого человека, или ошибочно поверить, будто преследуемый внезапно остановился.[4] «Нинпидэн» описывает хлопки деревянными колодками либо крики «Вор!» или «Помогите!», имитирующие тревогу и проверяющие реакцию стражников на шум.[5] «Бансэнсюкай» предлагает более управляемую проверку: находясь рядом с целью или стражником, синоби шепчет всё громче, чтобы определить порог обнаружения звука. Такие проверки помогают сделать конкретные наблюдения о реакции цели:

• насколько быстро цель отреагировала;
• спорили ли стражники о том, слышали ли они шум;
• появились ли стражники быстро и настороженно, с оружием в руках;
• застал ли шум цель врасплох;
• осталась ли цель совершенно безучастной.

Эти наблюдения не только сообщают синоби, насколько остры внимание и слух цели, но и раскрывают её навыки и готовность реагировать на события - сведения, позволяющие приспособить проникновение.[6]

Что касается вещественных улик, синоби придерживались принципа «не оставлять следов» задолго до того, как он стал экологическим девизом. Средство под названием *нагабукуро*, или «длинный мешок», помогает сдерживать и шум, и мусор. Взобравшись на высокую стену и столкнувшись с необходимостью прорезать отверстие для прохода, синоби подвешивал под собой большой толстый кожаный мешок *нагабукуро*, подбитый мехом или войлоком. Он ловил падающие обломки стены и приглушал звук. Затем синоби мог тихо опустить мусор в незаметное место внизу. Это было гораздо лучше, чем позволить обломкам с грохотом упасть на землю или с плеском - в ров.[7]

В этой главе мы перенесём свет, шум и мусор проникающих синоби на соответствующие явления киберугроз. Мы рассмотрим некоторые средства и приёмы, которыми группы угроз сводят к минимуму оставляемые улики, а также несколько профессиональных процедурных дисциплин. Обсудим обнаружение угроз, действующих «медленно и незаметно», и изменение среды в свою пользу. В мысленном эксперименте мы рассмотрим способ маскировки шагов синоби, который теоретически применим к современным цифровым системам. В конце главы разберём дисциплину обнаружения как способ противодействия искушённому противнику, который помнит о наблюдаемых признаках, оставляемых или не оставляемых в вашей сети.

Кибернетические свет, шум и мусор

Цифровой мир не всегда ведёт себя так же, как физический. Понять кибернетические аналоги света, шума и мусора и непрерывно охотиться за ними бывает трудно. Защитникам не хватает времени, ресурсов и возможностей для наблюдения и охоты внутри подконтрольных цифровых систем, поэтому след света, шума и/или мусора противника слишком часто остаётся незадокументированным. В результате кибернетическое проникновение может даваться субъектам угроз легче физического.

Многие средства и платформы сканирования и эксплуатации, например Nmap,[8] имеют режимы ограничения скорости или иные «медленные и незаметные» методы, которые пытаются соблюдать дисциплину размера пакетов или полезных нагрузок, частоты пакетов и использования пропускной способности в целевой сети. Противники создали чрезвычайно маленькие вредоносные файлы - например, China Chopper может занимать менее 4 КБ[9] - и эксплуатируют предположение защитников, будто файл со столь малым следом не причинит вреда. Вредоносную программу можно настроить на уменьшение шума посредством редких маячковых обращений к узлам командования и управления (C2) или заставить её уменьшать шум в журналах процессов либо памяти, намеренно надолго засыпая или выполняя пустую операцию (no-operation, NOP). Чтобы не оставлять цифровой мусор, способный выдать присутствие, некоторые вредоносные программы не записывают на диск никаких файлов. Противники и вредоносные программы в соседней сетевой инфраструктуре могут пассивно собирать сведения и медленно, но плодотворно изучать внутреннюю среду цели. Примечательно, что многие такие угрозы всё же принимают риск появления кибернетических света, шума и/или мусора в ходе кампаний.

Разумно предположить, что у достаточно развитых противников есть процедуры ограничения кибернетических света, шума и мусора, например:

- передавать цели менее 100 МБ данных в день;
- следить за тем, чтобы артефакты, файлы и строки вредоносной программы нельзя было легко распознать как мусор, выдающий её присутствие или позволяющий приписать следы конкретной программе;
- «заглушать» журналы, предупреждения, сигнальные растяжки и другие датчики, чтобы защитные средства не узнали о присутствии нарушителя.

Похоже, большинство современных защитных устройств и систем рассчитано на срабатывание при точной сигнатуре известной угрозы: конкретном IP-адресе, событии журнала или последовательности байтов. Даже при наличии специализированного ПО, такого как Wireshark,[10] которое показывает аналитикам действия угрозы в реальном времени, сбор, обработка и изучение сведений требуют значительных усилий. Сравните этот рабочий процесс с простым обнаружением шагов на слух и реакцией на них. Поскольку человек не способен воспринимать цифровую область органами чувств так же, как физическую среду, защитные меры в сущности напоминают стражников с нарушениями зрения и слуха, которые ждут сигнала, чтобы отреагировать на угрозу в другом конце комнаты.

Дисциплина обнаружения

К сожалению, идеального способа поймать того, кто искусно умеет не попадаться, не существует. Некоторые субъекты угроз имеют в этой области такое преимущество над защитниками, что получают несанкционированный доступ к средству регистрации инцидентов группы безопасности и следят за появлением новых расследований, где упоминаются их собственные действия. Однако защиту можно улучшать, персонал - обучать, контрмеры - развёртывать, а защитники могут применять хитрости, чтобы поймать угрозу на профессиональной ошибке.

1. **Развивайте осведомлённость.** В рамках обучения охоте за угрозами, реагированию на инциденты и анализу безопасности научите группу искать признаки света, шума и мусора противника.
2. **Установите скрипучие ворота.** Рассмотрите внедрение обманных индикаторов обнаружения нападения и предупреждения о нём (attack sensing and warning, AS&W), например событий безопасности, срабатывающих каждую минуту на контроллерах домена, других критических системах или сетевых устройствах. Можно создать предупреждение: `[Security Event Log Alert]: Windows failed to activate Windows Defender/Verify this version of Windows`. Оно способно обманом убедить проникшего противника, что вы не следите за предупреждениями, и побудить его «выключить» журналы безопасности или «перенаправить» их подальше от датчиков и аналитиков. Внезапное исчезновение ложного предупреждения сообщит защитникам о присутствии противника, а при настоящем сбое - о необходимости перезапустить систему или поручить ИТ-службе расследовать отказ.
3. **Достаньте деревянные хлопушки.** Подумайте, как развитый противник мог бы намеренно вызвать предупреждения или заметный сетевой шум из защищённой либо скрытой точки среды, например атакуя известные приманки, чтобы проверить способность группы безопасности обнаруживать угрозу и реагировать. Это кибернетический эквивалент ниндзя, который ночью бегает по дому и бьёт друг о друга две деревянные дощечки, проверяя вашу реакцию. Разумно предположить, что некоторые противники могут оценивать защиту таким способом, чтобы выяснить, можно ли без страха разоблачения применить уязвимости нулевого дня или иные скрытные приёмы.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка с ценными активами внутри. Поскольку расставить наблюдателей повсюду невозможно, вы разместили стражников там, где они смогут слышать странные звуки на основных путях выхода. Вы также обучили их замечать необычный шум. Вам сообщают, что у синоби есть специально изготовленные сандалии с мягкими подошвами, набитыми тканью, которые позволяют бесшумно ходить по плитке или камню.

Как использовать эти сведения для обнаружения ниндзя в замке? Какие следы могут оставлять особые сандалии? Какие контрмеры смягчат создаваемую ими угрозу? Как обучить стражников реагировать, заметив человека, который подозрительно тихо идёт по замку?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую следует оценивать с точки зрения света, шума и мусора, которые могут сопровождать нападение.

1. Определите возможности обнаружения в организации, моделируя сетевое проникновение как шумных и быстрых, так и медленных и незаметных противников. Задокументируйте, какие журналы связаны с какими наблюдаемыми действиями и где находятся слепые зоны ваших органов чувств. [AU-2: Audit Events; CA-8: Penetration Testing; SC-42: Sensor Capability and Data]
2. Сопоставляйте журналы инцидентов, предупреждения и наблюдаемые признаки с задокументированными действиями угроз, чтобы лучше обучить сотрудников и проверить ваше представление о том, как угрозы будут «звучать» в сети. [IR-4: Incident Handling | (4) Information Correlation]
3. Настройте песочницы и камеры детонации на поиск индикаторов субъекта угроз, который пытается соблюдать кибернетический аналог дисциплины света, шума и мусора. [SC-44: Detonation Chambers]
4. Применяйте методы обнаружения без сигнатур для поиска скрытной дисциплинированной деятельности, предназначенной для уклонения от сигнатурной идентификации. [SI-3: Malicious Code Protection | (7) Nonsignature-Based Detection]
5. Разверните наблюдение за информационными системами для обнаружения скрытной деятельности. Не устанавливайте чрезмерно чувствительные датчики в местах высокой активности. [SI-4: Information System Monitoring]

Разбор

В этой главе мы рассмотрели меры предосторожности и средства, которыми синоби скрывали свидетельства своей деятельности: например, измеряли, насколько громкий шум можно издать, не предупредив стражников, и выясняли вероятную реакцию цели при обнаружении действий синоби. Мы обсудили несколько кибернетических средств противников и увидели в них аналоги света и шума - доказательства, доступные обнаружению защитниками. Наконец, мы рассмотрели возможные контрмеры защитников.

В следующей главе мы обсудим обстоятельства, помогающие синоби проникать, поскольку они смягчают проблемы света, шума и мусора. Например, сильный ливень маскирует шум, ухудшает видимость и смывает следы присутствия. Киберзащитник может искать аналогичные обстоятельства, чтобы защитить системы.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), 209.
[2] [назад] Cummins and Minami, *The Book of Ninja*, 211.
[3] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), 54.
[4] [назад] Antony Cummins and Yoshie Minami, *True Path of the Ninja* (North Clarendon, VT: Tuttle Publishing, 2017), 63-64.
[5] [назад] Cummins and Minami, *Secret Traditions*, 55.
[6] [назад] Cummins and Minami, *The Book of Ninja*, 178-179.
[7] [назад] Cummins and Minami, *The Book of Ninja*, 188.
[8] [назад] “Nmap: The Network Mapper,” Insecure.org, Gordon Lyon, обновлено 10 августа 2019 года, https://nmap.org.
[9] [назад] “Software: China Chopper,” ATT&CK, The MITRE Corporation, последнее изменение 24 апреля 2019 года, https://bit.ly/3q019YR.
[10] [назад] Wireshark, The Wireshark Corporation, дата последнего обращения 7 февраля 2020 года, https://www.wireshark.org.

Глава 21. Обстоятельства проникновения

> Следует проникать именно в тот миг, когда враг движется, и не пытаться сделать это, когда он неподвижен, - так поступают принципиальные люди.

> Во время сильного ливня, когда дождь достигает наибольшей силы, воспользуйтесь им для действий синоби и ночных нападений.
>
> - «Ёсимори хякусю», стихотворение 1

И «Нинпидэн», и «Бансэнсюкай» советуют синоби при движении к цели пользоваться укрытием, чтобы остаться незамеченными. Можно дождаться обстоятельств, создающих укрытие, или при необходимости создать их самостоятельно. Свитки приводят множество ситуаций, помогающих проникновению: природные явления, такие как сильный ветер и дождь; общественные собрания, такие как праздники, свадьбы и религиозные службы; действия самих синоби - выпуск лошадей, провоцирование драк и поджог зданий.[1] Независимо от происхождения таких обстоятельств проницательный синоби должен уметь использовать отвлекающие события, возбуждение, сумятицу и иные условия, переключающие внимание цели.

Синоби умели превращать ненастье в благоприятные обстоятельства для проникновения. Например, сильный ливень означал пустые улицы, плохую видимость и потоки воды, заглушавшие все издаваемые синоби звуки.[2] Разумеется, плохая погода плоха для всех, и второе стихотворение «Ёсимори хякусю» отмечает, что чрезмерно сильная буря может одолеть и синоби, затруднив применение тактики и приёмов: «Глубокой ночью, когда свирепствуют ветер и дождь, улицы так темны, что синоби нелегко провести ночное нападение».[3]

Синоби пользовались и другими, более личными обстоятельствами, например трагической смертью в семье цели. Свитки отмечают, что во время траура цель может плохо спать две-три ночи. Синоби мог незаметно приблизиться во время похорон или скорби под видом оплакивающего либо отложить проникновение до третьей или четвёртой ночи, когда цель наконец погружалась в глубокий сон.[4]

Разумеется, задание синоби не всегда совпадало с благоприятным стечением обстоятельств. Иногда синоби сами вызывали тяжёлую болезнь в целевом укреплении. Больные были неэффективными защитниками, а обеспокоенные ухаживающие отвлекались и лишали себя сна ради заболевших. Когда пострадавшие начинали выздоравливать, испытавшие облегчение ухаживающие крепко засыпали, и тогда синоби проникали внутрь. Другой вариант - разрушить критически важную инфраструктуру, например мост, дождаться, когда цель начнёт большой и трудный проект восстановления в летнюю жару, а затем проникнуть к изнурённому противнику.[5]

Эффективные отвлекающие действия могли быть и более непосредственно агрессивными. «Бансэнсюкай» описывает приём *кёнин* - «создание бреши внезапностью», - в котором помогают военные силы или другие синоби. Союзники заставляют цель поверить, что началось нападение, например стреляют, бьют в боевые барабаны или кричат, а синоби во время сумятицы проскальзывает внутрь. Когда ему нужно безопасно выйти, приём просто повторяют.[6]

В этой главе мы рассмотрим, как описанное в свитках использование ситуационных факторов для проникновения переносится в цифровую эпоху. Оно основано на том, что внимание защитников, защитных систем и организаций ограничено. Перегружая, запутывая и направляя это внимание не туда, субъект угроз создаёт возможности для эксплуатации. Мы выявим различные возможности в современных сетевых средах и объясним, как они соответствуют обстоятельствам из свитков синоби. Наконец, рассмотрим, как организации могут внедрять защитные меры и устойчивость, готовясь к обстоятельствам, способным ослабить оборону.

Возможности противника

Противники в области кибербезопасности могут отвлекать цели и создавать условия, затрудняющие обнаружение проникновения, столь же разнообразно и разумно, как некогда синоби. Например, при обнаружении внезапной распределённой атаки отказа в обслуживании (distributed denial of service, DDoS) стандартные рабочие процедуры требуют оценить её силу и продолжительность и создать заявку об инциденте безопасности для регистрации действий. Защитники могут не сразу заподозрить, что DDoS прикрывает атаку субъекта угроз на сеть.

Когда нападение перегружает защитные датчики цели, а средства захвата пакетов (packet capture, pcap) и системы обнаружения или предотвращения вторжений (IDS/IPS) не успевают открыть пакет - иначе говоря, данных для проверки слишком много, - защитные системы могут естественным образом пропустить пакет дальше, не исследовав вредоносное содержимое. После прекращения DDoS защитники отметят отсутствие существенного простоя и вернут нормальное состояние, не понимая, что десяти минут потока пакетов хватило противнику для скрытого взлома системы и закрепления в сети. Как во втором стихотворении «Ёсимори хякусю», предупреждающем, что сильная буря мешает и цели, и нападающему, противник вряд ли устроит чрезмерно интенсивную DDoS. В таком случае сетевое оборудование начнёт отбрасывать пакеты и потеряет данные связи, включая его собственные атаки. Скорее всего, нападающий ограничит нагрузку так, чтобы перегрузить защиту, но не нарушить связь.

У противников есть множество других способов создать благоприятные обстоятельства в цели проникновения; пределом служит лишь изобретательность. Может оказаться выгодно атаковать качество и надёжность служб и инфраструктуры, например нарушая работу интернет-провайдеров или межсоединений. Терпеливый нападающий способен дождаться, когда коммерческий поставщик выпустит неисправное обновление или исправление, после чего сотрудники безопасности или ИТ-службы цели временно создадут условия «разрешить всё для всех» либо снимут защитные средства для устранения неполадки. Субъекты угроз могут следить за процессом приобретения активов компании, определяя, когда новые системы и серверы переводятся в эксплуатацию или облако и когда эти цели могут временно оставаться без охраны либо без правильной защиты от атак. Они могут наблюдать за слиянием компаний и пытаться проникнуть через бреши, возникающие при объединении сетей. Иные противники пользуются особыми мероприятиями в здании цели - крупными конференциями, выставками поставщиков и встречами с третьими сторонами, - чтобы смешаться с толпой незнакомцев и проникнуть к цели. По дороге они могут даже получить пакет сувениров.

Неблагоприятные обстоятельства противника

Гарантировать стопроцентную доступность цифровых систем считается невозможным, а обеспечить стопроцентную безопасность тех же систем во все моменты должно быть ещё труднее. Более того, почти наверняка невозможно предотвратить бедствия, опасности, аварии, отказы и непредвиденные изменения, многие из которых создают обстоятельства для проникновения оппортунистических субъектов угроз. Чрезмерная осторожность ради избегания таких обстоятельств может помешать компании смело строить стратегию и достигать целей. Решением дилеммы может стать избыточное наслаивание систем, сокращающее возможности проникновения. Группы безопасности могут создать эквивалент высокодоступной безопасности - избыточно многослойную защиту там, где системы слабее.

Развивайте осведомлённость и готовность. В рамках правил для сотрудников безопасности, действующих при управлении изменениями, мероприятиях, инцидентах, кризисах, стихийных бедствиях и иных отвлекающих или запутывающих обстоятельствах, научите группу искать признаки того, что событие создано или используется противником для проникновения в организацию. Задокументируйте обязанности ролей в политиках и процедурах. С помощью моделирования угроз, кабинетных учений и управления рисками выявляйте возможные отвлекающие обстоятельства, а затем продумывайте защитные меры, контрмеры и средства противодействия им.

> **Упражнение «Теория замка».** Представьте, что вы правитель средневекового замка с ценными активами внутри. Вы заметили, что во время особенно холодных и ветреных ледяных бурь стражники у ворот съёживаются на постах, закрывают лица и греются у маленьких неразрешённых костров, которые ухудшают ночное зрение и делают их силуэты заметными.
>
> Как синоби мог бы воспользоваться экстремальными условиями, например метелью или ледяной бурей, для проникновения в замок? Как он оделся бы? Как приблизился бы? Насколько свободно мог бы действовать рядом со стражниками? Какие ограничения физического доступа и правила безопасности стражники могли бы применять во время метели? Можно ли изменить посты, чтобы в таких условиях воины эффективно следили за происходящим? Какие ещё отвлекающие обстоятельства, помимо погоды, вы можете представить и как будете с ними справляться?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Их следует оценивать с учётом концепции обстоятельств проникновения.

1. Определите и задокументируйте, как во время чрезвычайных ситуаций или иных экстремальных обстоятельств применяются различные средства и правила безопасности, например аутентификация, чтобы смягчить проникновение противника. [AC-14: Permitted Actions Without Identification or Authentication]
2. Установите средства контроля и политики для условий использования внешних информационных систем, особенно при смягчающих обстоятельствах. [AC-20: Use of External Information Systems]
3. Проводите испытания на проникновение во время обучения действиям в моделируемых чрезвычайных ситуациях, например пожарных учений, чтобы проверить возможности защиты и обнаружения. [CA-8: Penetration Testing; CP-3: Contingency Training; IR-2: Incident Response Training]

4. Обеспечивайте ограничения физического доступа для посетителей, а также в обстоятельствах, когда невозможно сопровождать большое число неконтролируемых лиц, например пожарных при пожаре, но всё равно необходимо предотвращать несанкционированный вход в системы и выход из них. [PE-3: Physical Access Control]
5. Разработайте возможность отключать информационные системы и сети при чрезвычайной ситуации, когда есть подозрение, что противник скомпрометировал защиту. [PE-10: Emergency Shutoff]
6. Продумайте, как организация может включить осведомлённость о противнике и охоту на него в планирование непредвиденных обстоятельств. [CP-2: Contingency Plan]
7. Оцените, создаст ли внезапный перенос или возобновление деловых операций на резервных площадках удобные обстоятельства для проникновения противника. Затем предусмотрите надлежащие защитные меры и способы смягчения. [CP-7: Alternate Processing Site]

Разбор

В этой главе мы рассмотрели тактику создания и/или ожидания обстоятельств, прикрывающих проникновение к цели. Мы увидели несколько примеров того, как синоби создавали возможность при хорошей защите цели, и исследовали применение этой тактики в современных сетевых средах. Мы разобрали различные способы управления безопасностью в периоды слабости, а мысленный эксперимент позволил рассмотреть подготовку к обстоятельствам, в которых риск нельзя избежать, передать или нейтрализовать.

В следующей главе мы обсудим уязвимость нулевого дня - способ проникновения, настолько новый или тайный, что никто ещё не придумал защиты от него. У синоби были эксплойты и приёмы, подобные нулевым дням. Они хранились в такой тайне, что их запрещалось записывать, и свитки лишь косвенно на них намекают. Нам остались только загадочные подсказки, предназначенные напомнить синоби изученный секретный приём, но не научить ему. Даже при этом свитки рассказывают, как создавать новые нулевые дни, защищаться от них и профессионально применять. Более того, они описывают несколько исторических приёмов нулевого дня, утраченных из-за раскрытия, что даёт представление о современных эксплойтах нулевого дня и позволяет предвидеть нулевые дни будущего.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), 174, 199, 201.
[2] [назад] Cummins and Minami, *The Book of Ninja*, 175.
[3] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), 133.
[4] [назад] Cummins and Minami, *The Book of Ninja*, 201.
[5] [назад] Cummins and Minami, *The Book of Ninja*, 200-201.
[6] [назад] Cummins and Minami, *The Book of Ninja*, 74.

Глава 22. Нулевые дни

> Тайна действует, пока её хранят; если слова станут известны, вы проиграете.

> Помните: не следует применять известные людям древние способы, иначе вы лишитесь преимущества внезапности.
>
> - «Сёнинки», «Такага-о коэ хикуки-ни хайру-но нараи»[1]

Одним из важнейших тактических преимуществ синоби была секретность. Свитки неоднократно предупреждают: нельзя позволять другим узнавать подробности возможностей синоби, поскольку утечка сведений о приёме способна привести к катастрофическим последствиям. Приём мог утратить силу на поколения, а жизнь применявших его синоби - оказаться под угрозой. И «Сёнинки», и «Нинпидэн» описывают опасность раскрытия посторонним профессиональных секретов ниндзя; некоторые свитки заходят так далеко, что советуют убивать цели, узнавшие секреты, или свидетелей, увидевших синоби в действии.[2]

И «Сёнинки», и «Нинпидэн» приводят древние приёмы, испорченные публичным раскрытием. Например, древние ниндзя (*ямо*)[3] во время разведки иногда пересекали поля. Чтобы остаться незамеченными, они среди прочего одевались как пугала и при приближении людей застывали в убедительной позе.[4] Но после раскрытия приёма местные жители стали регулярно проверять пугала, бросаясь на них и даже протыкая оружием. Какой бы убедительной ни была маскировка и каким бы искусным ни было притворство синоби, приём стал слишком рискованным. Синоби пришлось придумывать новые способы прятаться на виду или вовсе избегать полей. Навык был утрачен.

Подобным образом некоторые синоби в совершенстве подражали кошкам и собакам. Если во время задания они случайно выдавали присутствие, то лаяли или мяукали, убеждая цель, что шум подняло проходившее животное и проверять ничего не нужно. В конце концов раскрыли и этот приём. Стражников научили расследовать незнакомые звуки животных, и синоби оказались под угрозой обнаружения.[5]

Свитки описывают и укрепления, защищённые собаками, которых синоби не мог убить, похитить или приручить, не вызвав подозрений у стражников. В таком случае синоби советовали надушиться китовым жиром, дождаться, пока собака отойдёт от стражников, либо увести её, а затем избить. Это повторяли несколько ночей подряд. Резкий и редкий запах китового жира приучал собаку связывать его с болью и наказанием, и она начинала слишком бояться, чтобы напасть на синоби с таким запахом. После раскрытия приёма стражников научили замечать необычный запах китового жира и внезапные изменения поведения собак.[6]

Разумеется, большинство секретов синоби оставалось нераскрытым до официальной публикации свитков, произошедшей через много лет после того, как сами синоби фактически стали историческим пережитком. Поэтому защитникам той эпохи приходилось создавать способы противодействия атакам, о которых они ничего не знали, - возможно, даже атакам, ещё не придуманным самими нападающими.

Синоби, выступавшим в роли защитников, свитки дают несколько базовых советов. Тома «Наставления полководцам»[7] в «Бансэнсюкай» рекомендуют различные лучшие методы безопасности: пароли, удостоверяющие печати, опознавательные метки, тайные знаки и сигналы. Свиток также советует полководцам размышлять над логикой этих защитных хитростей, сочетать их с другими стандартными правилами, такими как ночные дозоры и охрана, принимать повышенные меры предосторожности, например ставить ловушки, и разрабатывать собственные

секретные, особые и динамические реализации защиты. Вместе эти приёмы защищали от нападающих низкого и среднего мастерства, но не от самых искушённых синоби.[8]

Самый прагматичный совет «Бансэнсюкай» состоит в том, что защитники никогда не будут совершенно защищёнными, непрерывно бдительными и безупречно дисциплинированными. Всегда останутся бреши для эксплуатации синоби. Поэтому свиток подчёркивает важность понимания философии, образа мыслей и хода рассуждений врага и призывает синоби пробовать новые приёмы, иногда прямо на месте: «Трудно точно сказать, как следует действовать в соответствии с ситуацией, временем и местом. Если у вас есть набор неизменных способов или вы пользуетесь постоянной формой, как даже величайший полководец сможет победить?»[9]

Синоби-защитники применяли творческое мысленное моделирование, например представляли обратные сценарии и исследовали возможные бреши. Они черпали вдохновение в природе, воображая, как рыба, птица или обезьяна проникла бы в замок и как подражать её способностям.[10] Новые приёмы выводили из изучения обычных воров (*нусубито*). Прежде всего они доверяли творческой силе человеческого разума и непрерывно учились, применяли логический анализ, решали задачи и развивали метакогнитивную гибкость:

> Хотя для синоби существуют миллионы тонких и постоянно меняющихся уроков, невозможно полностью обучить им через традицию или передачу знаний. Одна из важнейших ваших задач - всегда стараться узнать всё возможное о каждом месте или крае, который только можно познать... Если ваш разум полностью согласован с порядком вещей и действует с безупречной рассудительностью и логикой, вы сможете пройти через «врата без ворот»... Человеческий разум удивителен и гибок. Это поразительно. Со временем, явно или таинственно, вы осознаете сущность вещей, и понимание возникнет словно из ниоткуда... На пути синоби следует овладеть всем, чем только возможно... следует применять воображение и проницательность, чтобы осознать и постичь ход всех дел.[11]

Дальновидный синоби с острым умом и усердием мог построить защиту, достаточно сильную для неизвестных атак, заставляя врага тратить время и ресурсы на новые планы, проверку брешей и борьбу со скрытой обороной - лишь затем, чтобы снова потерпеть неудачу после динамического изменения всей защитной системы.

В этой главе мы исследуем современный ландшафт угроз нулевого дня и выясним, какие элементы философии и оперативного искусства из свитков синоби применимы к кибербезопасности. Кроме того, рассмотрим различные предлагаемые способы защиты. Мысленный эксперимент ставит задачу противодействия неизвестным и возможным нулевым дням, скрытым в современном компьютерном оборудовании, программах, облаках и сетях, в надежде вызвать новые озарения.

Нулевой день

Немногие термины в лексиконе кибербезопасности внушают защитникам и осведомлённым деловым заинтересованным лицам такой страх, как *нулевой день*, или 0-day, - ранее неизвестный эксплойт либо нападение, с которым защитники могут не уметь бороться. Название означает, что общественность знает об атаке или уязвимости ноль дней. Поскольку жертвы и защитники ещё не успели изучить угрозу, субъект, имеющий нулевой день для распространённой технологии, почти всегда добивается успеха. Например, STUXNET применил четыре эксплойта нулевого дня для диверсии на физически изолированном предприятии по обогащению ядерного топлива в Иране, продемонстрировав способность нулевых дней атаковать даже самые защищённые и необычные цели.[12]

Ценность атаки нулевого дня возникает из её неизвестности. Как только субъект угроз применяет нулевой день, жертва получает возможность зафиксировать доказательства датчиками и средствами наблюдения, исследовать их криминалистически и подвергнуть атаку обратной разработке. После появления нулевого дня в реальных условиях специалисты могут быстро разработать способы смягчения, сигнатуры обнаружения и исправления и опубликовать номера CVE для предупреждения сообщества. Не все следят за рекомендациями или устанавливают исправления, но по мере превращения 0-day в 1-day, 2-day и далее вероятность успеха снижается.

Нулевые дни применяют по-разному в зависимости от мотивов нападающего. Киберпреступники, желающие быстро получить крупную прибыль, могут немедленно «сжечь» нулевой день в массовой и очень заметной атаке, максимально увеличивая мгновенный доход. Более развитые субъекты угроз создают процедуры удаления артефактов, журналов и других наблюдаемых доказательств, продлевая срок полезной жизни нулевого дня. По-настоящему искушённые нападающие берегут нулевые дни для усиленных и ценных целей: эксплойт для популярной технологии можно продать киберпреступникам на чёрном рынке за тысячи долларов, а правительствам, стремящимся превратить его в оружие или создать защиту, - более чем за миллион.

Одни нулевые дни возникают из законных, добросовестно допущенных брешей в программном коде, но субъекты угроз способны злонамеренно внедрять их в исходный код приложения посредством соглашений или тайно внедрённых людей. Целевая атака может также скомпрометировать программные библиотеки, оборудование или компиляторы и внести ошибки, бэкдоры и другие скрытые уязвимости для будущей эксплуатации. Это похоже на ниндзя, вступившего в строительную бригаду замка и ослабившего проект тайными входами, известными лишь ему; свитки сообщают, что такое происходило.[13]

Традиционно нулевые дни обнаруживали исследователи безопасности с глубоким знанием кода, охотники за угрозами, творчески размышлявшие об уязвимостях, или аналитики, случайно замечавшие применение эксплойта против них в реальных условиях. Эти методы всё ещё работают, однако новые технологии, такие как фаззинг, помогли автоматизировать обнаружение. Фаззеры и подобные средства автоматически перебирают различные случайные, недопустимые и неожиданные входные данные в попытке найти ранее неизвестные уязвимости системы. Появление фаззеров и защитников на основе ИИ возвещает новую парадигму. Как изобретение пушки, пробивавшей стены замков, вызвало появление новых стратегий защиты, так ИИ даёт надежду, что когда-нибудь защита станет развиваться почти с той же скоростью, что и угрозы. Разумеется, атакующие системы тоже могут научиться подавлять любые защитные возможности, изменив не только методы обнаружения и борьбы с нулевыми днями, но и общий взгляд мира на кибербезопасность.

Пока же эксплуатация и обнаружение образуют цикл. Субъекты угроз осваивают подмножество эксплойтов и уязвимостей, например внедрение SQL, XSS или утечки памяти. Когда защитники учатся бороться с ними, нападающие переходят к эксплуатации других приёмов и технологий, и цикл продолжается. Со временем нынешние защитники и нападающие покинут отрасль, а новое поколение субъектов угроз, вероятно, заново обнаружит те же распространённые слабости в новых программах и технологиях. Старые нулевые дни появятся вновь, и цикл начнётся сначала.

Защита от нулевых дней

Обнаружение нулевых дней и защита от них часто становятся главным обещанием новичков рынка кибербезопасности, которым нравится сулить огромный результат своего решения. Это не означает, что ни одно не работает. Однако здесь легко оказаться на территории шарлатанства. Можете быть уверены: я не пытаюсь продать вам ничего, кроме изложенных ниже практических рекомендаций.

1. **Следуйте лучшим методам.** Безумная сложность защиты от нулевых дней не означает, что от безопасности следует отказаться. Следуйте лучшим отраслевым методам. Они могут не полностью нейтрализовать нулевые дни, но затруднят действия субъектов угроз против вашей среды и повысят шансы организации обнаружить атаку и отреагировать. Вместо праздного беспокойства о возможных нулевых днях исправляйте и смягчайте 1-day, 2-day, 3-day и далее, сокращая время уязвимости организации перед известными атаками.
2. **Используйте группы охоты и синие группы.** Создайте или наймите группу охоты и синюю группу для разработки стратегий защиты от нулевых дней.

   Группа охоты состоит из специализированных защитников, не полагающихся на стандартные сигнатурные средства. Они постоянно выдвигают гипотезы о том, как противники могут применять нулевые дни или иные способы проникновения в сети. На основе гипотез они охотятся с помощью приманок, поведенческого и статистического анализа, прогнозной аналитики угроз и других особых методов.

   Синяя группа состоит из специализированных защитников, которые проектируют, испытывают и внедряют настоящую оборону. Сначала они документируют поток информации системы или сети, затем строят модели угроз, описывающие реальные и воображаемые атаки, способные преодолеть текущую конструкцию. В отличие от группы охоты, задача синей группы - не искать нулевые дни. Она оценивает информационные модели и модели угроз с точки зрения нулевых дней, определяя, как эффективно смягчить риски, защитить, усилить и оградить системы. Синяя группа существует отдельно от обычных сотрудников безопасности, эксплуатации и реагирования на инциденты, но должна изучать прежние отчёты о реагировании, чтобы понять причины провала защиты и построить упреждающую оборону от подобных будущих атак.
3. **Осторожно внедряйте динамическую защиту.** В последние годы специалисты согласованно пытались внедрить сложные динамические меры, которые:

   • стремятся сделать сеть движущейся целью, например посредством ночных обновлений;
   • вводят рандомизацию, например рандомизацию размещения адресного пространства (address space layout randomization, ASLR);
   • динамически меняются при взаимодействии, например квантовая криптография;
   • создают нерегулярные условия защиты или системы иммунного ответа.

   Некоторые из этих динамических средств сначала были весьма успешны, но затем противники нашли способы их побеждать, и со стратегической точки зрения они фактически стали статическими.

Поговорите с поставщиками и практиками кибербезопасности и изучите литературу о современных динамических средствах, чтобы определить подходящие организации. Но действуйте осторожно: сегодняшняя динамическая защита может завтра стать стандартным и легко обходимым слоем.

4. **Постройте более скучную защиту.** По возможности применяйте в среде «скучные» системы, методы программирования и реализации. Подход, начатый проектом Google с открытым исходным кодом BoringSSL,[14] предполагает, что упрощение и уменьшение поверхности атаки, размера, зависимостей и сложности кода, то есть превращение его в скучный, скорее всего устранит ценные или критические уязвимости. На уровне кода, приложения или системы код при таком подходе не замысловат и не изящен, а однообразно защищён, имеет неизменную структуру и простые реализации. Теоретически код, который людям и машинам легче читать, проверять и интерпретировать, с меньшей вероятностью раскроет уязвимости нулевого дня при неожиданных входных данных или событиях.
5. **Применяйте отказ и обман (denial and deception, D&D).** D&D не позволяет противникам получать сведения о вашей среде, системах, сети, людях, данных и других наблюдаемых признаках и может обманом побудить их к выгодным для вас действиям. Затрудняя разведку, создание оружия и доставку эксплойта, вы заставляете противника тратить больше времени на испытания, исследования и проверку того, действительно ли замеченная брешь существует. Например, можно обманно изменить системы, чтобы они объявляли себя другой ОС с иными программами, скажем представить экземпляр Solaris как другую ОС SELinux. В идеале следовало бы действительно перейти на SELinux, но логистика устаревших ИТ-систем может дольше желаемого удерживать организацию на старом ПО. Если обман действует, противник может разработать и доставить вооружённую атаку против экземпляра SELinux, которая, конечно, потерпит неудачу, поскольку на самом деле SELinux не используется.

   D&D следует накладывать на хорошие методы безопасности для их усиления, а не применять самостоятельно как безопасность через неясность. Это завершающая стадия безопасности для чрезвычайно зрелых организаций, ищущих дополнительные способы защиты от устойчивых субъектов угроз, подобная «сверхсекретной тактике» из «Бансэнсюкай».[15]
6. **Отключитесь ради защиты.** В описании защиты отключением «Сёнинки» учит отделяться от врага мысленно, стратегически, физически и во всех прочих отношениях.[16] В кибербезопасности это означает создать самоизолированную синюю группу, которая полностью обращается внутрь, работает отдельно от мира и игнорирует все новости безопасности, разведывательные сведения об угрозах, исправления, эксплойты, варианты вредоносных программ, новые сигнатуры, передовые продукты - всё, что может повлиять на рассуждение, изменить образ мыслей или создать связь с врагом. При правильном применении навык отключения уводит мышление защитников далеко от отраслевого стандарта. Противнику трудно мыслить так же, как отделившиеся защитники, а те создают уникальные тайные стратегии, которых он прежде не встречал, чрезвычайно затрудняя успех атак нулевого дня.

   Как и D&D, этот метод рекомендуется лишь тем, кто уже обладает элитными навыками кибербезопасности. Иначе отчуждение от врага и работа вслепую могут дать обратный результат.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка с ценными активами внутри. До вас доходят слухи, что во время строительства замка синоби проник в бригаду и установил один или несколько потайных входов либо создал иные бреши в защите. Знающие местонахождение и механизм уязвимостей синоби могут свободно входить и выходить из замка, обходя стражников и защитные средства. Вы отправляли стражников, архитекторов и даже наёмных синоби искать скрытые уязвимости, но они ничего не нашли. У вас нет денег, времени и ресурсов для строительства нового замка без потайных входов.

Как продолжать работу замка, зная, что существует скрытый изъян, который синоби способен эксплуатировать в любой момент? Как защитить сокровища, людей и сведения внутри? Как искать скрытую слабость или обороняться от неё, не зная её вида, местонахождения и способа применения? Как ещё можно управлять риском неизвестной уязвимости?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую следует оценивать с учётом концепции нулевых дней.

1. Создайте для организации особые, динамические и адаптивные средства защиты, усиливающие лучшие методы безопасности. [AC-2: Account Management | (6) Dynamic Privilege Management; AC-4: Information Flow Enforcement | (3) Dynamic Information Flow Control; AC-16: Security and Privacy Attributes | (1) Dynamic Attribute Association; IA-10: Adaptive Authentication; IR-4: Incident Handling | (2) Dynamic Reconfiguration; IR-10: Integrated Information Security Analysis Team; PL-8: Security and Privacy Architectures | (1) Defense-in-Depth; SA-20: Customized Development of Critical Components; SC-7: Boundary Protection | (20) Dynamic Isolation and Segregation; SI-14: Non-persistence]
2. Ведите записи о нулевых днях, включая время и способ обнаружения, целевую технологию, результаты сканирования уязвимостей и связь с предсказанными будущими нулевыми днями. [AU-6: Audit Review, Analysis, and Reporting | (5) Integrated Analysis of Audit Records; SA-15: Development Process, Standard, and Tools | (8) Reuse of Threat and Vulnerability Information]
3. Проводите специализированное сканирование и проверку уязвимостей и испытания систем для оценки защиты от нулевых дней. [CA-2: Assessments | (2) Specialized Assessments]
4. Нанимайте специализированных испытателей на проникновение для поиска нулевых дней в программах, системах и других технологиях, чтобы упреждающе защищаться от этих эксплойтов. [CA-8: Penetration Testing; RA-6: Technical Surveillance Countermeasures Survey]
5. Моделируйте угрозы для систем и программ, чтобы оценить возможные нулевые дни и выяснить, как упреждающе перепроектировать их для смягчения. Рассмотрите внедрение «скучного» кода. [SA-11: Developer Testing and Evaluation | (2) Threat Modeling and Vulnerabilities Analyses; SA-15: Development Process, Standard, and Tools | (5) Attack Surface Reduction; SI-10: Information Input Validation | (3) Predictable Behavior]

6. Внедряйте особые, разнообразные и уникальные средства безопасности, смягчающие способность нулевого дня эксплуатировать системы. [SC-29: Heterogeneity]
7. Развёртывайте кампании отказа и обмана, чтобы снизить способность противника вести разведку либо создавать оружие и доставлять атаки нулевого дня против организации. [SC-30: Concealment and Misdirection]
8. Создайте группы охоты и безопасности для поиска индикаторов атак и эксплойтов нулевого дня. [SI-4: System Monitoring | (24) Indicators of Compromise]
9. Регулярно проводите автоматизированное сканирование уязвимостей для проверки 1-day, 2-day, 3-day и далее. Надлежащим образом исправляйте, смягчайте или устраняйте уязвимости. [RA-5: Vulnerability Scanning; SI-2: Flaw Remediation]

Разбор

В этой главе мы рассмотрели профессиональные приёмы синоби и секретность, окружавшую методы эксплуатации, которые они развивали веками. Мы исследовали, насколько многие тайные приёмы синоби похожи на современные эксплойты и уязвимости нулевого дня. Мы рассмотрели современное состояние и возможное будущее атак нулевого дня с точки зрения кибербезопасности, кибервойны и информационного превосходства. Глава кратко показала: разговоры о нулевых днях могут казаться бессмысленными, но на самом деле критически важны для противодействия угрозе.

В следующей главе мы обсудим найм правильных специалистов для борьбы с нулевыми днями и любыми субъектами угроз. Мы рассмотрим наставления свитков синоби о вербовке и исследуем, как применить их к привлечению талантов в кибербезопасность. Постоянно утверждается, что отрасль страдает от нехватки кадров, и я подозреваю, что в периоды раздоров средневековая Япония сталкивалась с похожей нехваткой синоби. Свитки объясняют, как распознать человека, которого можно обучить оперативной работе синоби, где ставки были намного выше, чем в современных офисах. Неудачно выбранный новобранец, скорее всего, вскоре погибал, лишая смысла вложения в обучение и подвергая опасности задания и жизни товарищей.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *True Path of the Ninja* (North Clarendon, VT: Tuttle Publishing, 2017), 105.
[2] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), 67.
[3] [назад] Cummins and Minami, *True Path*, 166.
[4] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), 51.
[5] [назад] Cummins and Minami, *The Book of Ninja*, 212.
[6] [назад] Cummins and Minami, *True Path*, 175.
[7] [назад] Cummins and Minami, “Shochi I: A Guideline for Commanders I” - “Shochi V: A Guideline for Commanders V,” в *The Book of Ninja*.
[8] [назад] Cummins and Minami, *The Book of Ninja*, 502.
[9] [назад] Cummins and Minami, *The Book of Ninja*, 98.
[10] [назад] Cummins and Minami, *The Book of Ninja*, 56.
[11] [назад] Cummins and Minami, *True Path*, 43, 148.
[12] [назад] “W32.Stuxnet,” Symantec Security Center, Symantec Corporation, последнее изменение 16 сентября 2017 года, https://bit.ly/3bfoW2R.
[13] [назад] Cummins and Minami, *The Book of Ninja*, 185.
[14] [назад] “BoringSSL,” Git repositories on boringssl, дата последнего обращения 26 сентября 2018 года, https://bit.ly/3s1mrHk.
[15] [назад] Cummins and Minami, *The Book of Ninja*, 98.
[16] [назад] Cummins and Minami, *True Path*, 154.

Глава 23. Найм синоби

> Чтобы защититься от вражеских замыслов или синоби либо на случай чрезвычайного происшествия, вы можете решить, что желательно иметь множество людей. Однако не следует без тщательного обдумывания нанимать в армию новых людей.

> У синоби должны быть три главных принципа: искусная речь, смелость и стратегия.
>
> - «Ёсимори хякусю», стихотворение 38

Мы знаем о множестве работ, которые синоби выполняли в феодальной Японии: шпионаж и диверсии, руководство набегами, сбор сведений, убийства и, быть может, самое полезное - защита от вражеских синоби. Но чтобы использовать синоби для этих целей, господам и полководцам сначала приходилось делать то же, что руководители и управляющие делают сегодня: искать и нанимать сотрудников.

Разрозненные, но значительные части «Бансэнсюкай» и «Ёсимори хякусю» посвящены советам господам о том, зачем нанимать синоби, как и когда их применять и какие качества делают кандидата успешным, а впоследствии - эффективным синоби. Согласно свиткам, идеальный синоби должен быть:[1]

- **Умным.** Обладать сильным духом, логическим и стратегическим мышлением, хорошей памятью, острым наблюдением и способностью быстро учиться.
- **Терпеливым.** Действовать обдуманно, но решительно, обладать образцовой силой воли и самообладанием.
- **Способным.** Быть находчивым, изобретательным и смелым на местности, иметь подтверждённые достижения и видеть победу даже в отчаянном положении.
- **Верным.** Быть искренним, благородным и доброжелательным к другим, лично отвечать за свои поступки.
- **Красноречивым.** Уметь эффективно общаться с господами и убедительно - с подчинёнными.

Кроме этих качеств синоби, претендующий на руководящую должность, должен эффективно расставлять приоритеты, успешно выполнять сложную тактику и проявлять здравое суждение под давлением.[2]

Свитки указывают и качества, дисквалифицирующие кандидата: эгоизм и глупость; безнравственность, например применение навыков ради личной выгоды; склонность чрезмерно предаваться алкоголю, похоти или алчности.[3] Возможно, существовала и проблема кумовства. Рождение в деревне синоби, особенно Ига или Кока, повышало шансы на успех благодаря ранним ожиданиям, возможностям и подготовке, но родители-синоби не гарантировали успешности ребёнка. Такие дети могли оказаться плохими кандидатами с любым числом перечисленных отрицательных качеств.[4]

Важно, что в длинном перечне желательных и нежелательных свойств нет ни конкретных обязательных навыков, ни прежнего опыта, документов об образовании, социального происхождения, ранга или титула, ни даже возраста или пола. По-видимому, роль синоби давалась по заслугам и зависела от характера, ценностей, квалификации и способностей человека.

Хотя свитки не дают конкретных наставлений о поиске, собеседовании или оценке кандидатов, «Сёнинки» советует, как понять глубокую природу человека: его знания, образ мыслей, убеждения, желания, недостатки и характер. Обычно эти методы применялись в шпионаже и выборе целей, но их можно с пользой приспособить к собеседованию с новобранцами.

Например, «Сёнинки» рекомендует посещать привычные места цели и собирать сведения у хорошо знающих её местных жителей. Лучшие сведения можно получить там, где цель чувствует себя непринуждённо или поддерживает отношения с владельцами и посетителями, а потому с большей вероятностью раскрывает тайны.[5]

Есть и навык *хито-ни курума-о какэру* - «увлечь человека похвалой». Следует задавать цели вопросы и хвалить ответы; лесть заставляет вас выглядеть менее умным и будто бы демонстрирует восхищение способностями кандидата. При убедительном применении приём раскрепощает цель, придаёт уверенность и побуждает с удовольствием рассказывать о себе, что может дать всевозможные ценные разведывательные сведения. Например, когда человек освоится, можно менять темы разговора и наблюдать за реакцией на неожиданные вопросы. Есть ли у него собственное мнение или он лишь повторяет чужую мудрость?[6]

Для синоби вербовка союзников и распознавание врагов были вопросом жизни и смерти. Им часто приходилось решать, можно ли доверить человеку свою жизнь или он подведёт во время опасного задания. Поэтому синоби, вероятно, глубоко усваивали эти и иные критерии и становились мастерами чтения людей, способными быстро и незаметно оценить возможности, знания и характер человека.[7]

В этой главе мы рассмотрим распространённые методы найма современных организаций и выявим возможности применить мудрость синоби к привлечению и обучению талантов. Многие нанимающие руководители и даже исторические синоби, похоже, верят, что после подробного собеседования могут оценить пригодность человека. Иногда это работает, но множество кандидатов вообще не получает возможности пройти собеседование из-за разнообразных сигнальных этапов, косвенных предварительных требований и формальных отметок кадровой службы, которые могут ошибочно их отсеять. Мы исследуем эти процессы найма и причины, по которым они не всегда дают желаемый результат.

Таланты в кибербезопасности

Взрывной рост сектора кибербезопасности привёл к трудностям с наймом достаточного числа людей и именно тех людей, которые способны выполнить всю необходимую работу. Отчасти это связано с относительной новизной области и высоким техническим порогом входа, но современные методы оценки кандидатов тоже проблематичны. Слишком многие частные компании придают чрезмерное значение кандидатам, отметившим правильные пункты резюме или хорошо решающим задачи у доски, но не способным выполнять повседневные обязанности. Кандидаты, вербовщики и учебные программы заметили, что требуется для получения работы, и соответствующим образом себя позиционируют, снижая эффективность традиционной оценки.

Университеты выпускают специалистов по информатике, не способных решить задачу FizzBuzz, проверяющую базовые навыки программирования. Кандидаты дают потенциальным работодателям пристрастные или вымышленные рекомендации. Сотрудники добиваются бессодержательных должностных названий, которые хорошо выглядят в резюме, но редко соответствуют опыту или возможностям. Карьеристы получают сертификаты ИТ или безопасности, зубря перед экзаменом и часто почти сразу забывая сведения; публикуют поверхностные бессмысленные статьи ради известности; подают патентные заявки, добавляя своё имя к проектам, с которыми почти не связаны.

Меры против обхода найма, такие как домашние задания, легко преодолеть с помощью интернета или прямого плагиата. Когда-то новые задачи у доски во время собеседования стали рутиной. Кандидаты приходят после тренировки и могут даже получить точные упражнения из утечек компании. Даже если бы эти оценки не было так легко скомпрометировать, ни одна не измеряет точно способность выполнять работу по кибербезопасности.

Справедливости ради, у кандидатов не меньше причин подозревать работодателей в кибербезопасности. Даже наняв невероятного специалиста, достойного звания «кибериндзя», организация не гарантирует эффективного применения его способностей. Такой риск существует в любой отрасли, но в компаниях кибербезопасности его усиливают многие причины: непонятность высокотехнической профессии, развитие технологий, недостаточная осведомлённость руководства или знакомство с передовыми возможностями сотрудника и важность неограниченного творчества для успеха. Чтобы хорошо работать и влиять на безопасность организации, сотрудникам нужны поддержка руководства и разрешение применять навыки без страха наказания или прямого подавления способностей.

Один из крупнейших вербовщиков, работодателей и учителей специалистов по кибербезопасности - вооружённые силы США. Они способны взять почти не знакомого с компьютерами человека, не окончившего школу, и за 18 месяцев подготовить компетентного специалиста по кибервойне. Разумеется, обучение проходят не все: несколько уровней требований отсеивают слабых кандидатов, что близко соответствует практике для новобранцев-синоби из «Бансэнсюкай».[8]

Особый инструмент военного набора - батарея тестов профессиональной пригодности к военной службе (Armed Services Vocational Aptitude Battery, ASVAB).[9] В отличие от корпоративного найма, подчёркивающего прежние достижения и профессиональные документы, ASVAB оценивает потенциал обучения, способности и общую техническую пригодность. Результаты используются для назначения кандидатов на военные специальности, где после успешной подготовки они, вероятнее всего, преуспеют. ASVAB весьма эффективен для вооружённых сил, но следует отметить, что на некоторых кибернетических должностях неожиданно высоки доли провалов обучения и слабой работы на местах. Вероятная причина - сложные качества, которые ASVAB проверяет не всегда. В структурированном военном мире трудно выявлять или обучать людей, желающих подходить к задачам с творческим, бесстрашным, независимым и ориентированным на решение мышлением - набором навыков, тесно связанным с хакерами.

Управление талантами

Все хотят нанять специалистов по кибербезопасности, но предложение ограничено. Как же каждой организации получить такие таланты? Сначала следует определить, намерена ли она сама развивать необработанный талант или конкурировать с другими за ограниченное число опытных экспертов. Многие приведённые ниже рекомендации подходят для развития, но могут пригодиться и в смешанном подходе. Многие специалисты согласятся, что современные методы найма сломаны и пора оставить косвенные сигналы, попробовав новое. Рассмотрите следующие альтернативные подходы к найму и удержанию талантов.

1. **Начните применять практические оценки способностей на собеседовании.** Вместо викторин, случайных задач у доски, программирования вживую или домашних проектов просите кандидатов выполнять функции той самой работы, на которую их оценивают. Пусть они проходят пробу в той же среде и условиях, где будут работать после найма. Испытывайте и проверяйте оценки, предлагая упражнения нынешним сотрудникам и анализируя результаты, измеряя связь между прохождением теста и настоящей работой. Делайте оценку модульной и регулярно меняйте её, чтобы кандидат не выиграл благодаря утечке упражнения или наставнику. Постоянно включайте недавние задачи сотрудников, сохраняя соответствие теста требованиям работы. В идеале оценка должна определять компетентность за 30 минут или меньше, оставляя кандидату время на обучение посредством интернет-поиска и/или быстрых проб и ошибок.
2. **Внедрите батарею способностей «чёрного ящика».** Дайте кандидату модульную, частично случайную псевдотехнологию и попросите выяснить принцип её работы, а затем попытаться взломать и/или защитить. Упражнение похоже на тест Министерства обороны DLAB (Defense Language Aptitude Battery).[10] Вместо проверки владения существующим языком DLAB применяет вымышленный язык для оценки способности учить новый. Для технологий этот подход, вероятно, ещё полезнее, чем для разговорных языков, поскольку новые технологии и платформы появляются постоянно. Основные критерии теста «чёрного ящика» должны измерять способность кандидата:

   • быстро запоминать спецификации, команды или руководства вымышленной технологии;
   • применять логику и критическое мышление для решения задач или прохождения сценариев;
   • проявлять находчивость для достижения результатов при искусственных препятствиях, например обходить локальную защиту вымышленной технологии.

   Вы можете найти и нанять перспективного кандидата с высокими способностями, но без необходимых технических навыков. В таком случае потребуется дорогостоящее долгосрочное вложение в обучение настоящим техническим умениям. Иначе высокие способности не помогут.

3. **Умейте замечать дисквалифицирующие качества.** Не ограничивайтесь типичными тестами на наркотики, проверкой рекомендаций, биографии, судимости и кредитных отчётов: они не всегда точно описывают характер человека, в лучшую или худшую сторону. Приложите серьёзные усилия для выявления кандидатов, постоянно принимающих плохие решения, вредящие им самим и другим. Такие «вредно-глупые» люди могут иметь дипломы, сертификаты, хорошую кредитную историю, чистые тесты на наркотики и солидный трудовой стаж благодаря другим качествам - стойкости, честолюбию, усердию, природному таланту и удаче. Во время собеседования исследуйте их желания и мотивы, чтобы отсеять неподходящих. Разумеется, прежние вредно-глупые решения могут не отражать нынешний образ мыслей и характер, поэтому дайте кандидату возможность показать, насколько вероятны такие решения в будущем.
4. **Обучайте сотрудников и создавайте культуру превосходства.** Техническим навыкам можно научить, но оттачивание других свойств характера требует огромных усилий. Выявляйте сотрудников, желающих стать «кибернинджя», и помогайте им развивать личные качества из «Бансэнсюкай», непрерывно ставя задачи, закаляя и обучая.

Поручите им:
• ежедневно стремиться решать всё более сложные кибернетические задачи;
• оттачивать разум упражнениями для памяти, испытаниями самодисциплины и технологическими упражнениями на терпение;
• учиться изобретательности, создавая ограниченные кибернетические операционные ситуации с самостоятельно установленными правилами и пытаясь достичь целей, соблюдая их.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка с ценными активами внутри. Вы публично объявляете о намерении нанять и обучить синоби для защиты от вражеских ниндзя и получаете огромное число заявок. Вам неизвестны академии, гильдии или иные организации, способные подтвердить квалификацию кандидата, а из-за тайного характера профессии нельзя проверить опыт у прежних нанимателей. Вы недостаточно понимаете навыки синоби, чтобы самостоятельно проверить или измерить их, а когда просите соискателя продемонстрировать искусства синоби, он либо отказывается, либо требует оплаты.

Как определить, способен ли самопровозглашённый синоби надёжно защищать замок? Как выявить и нанять кандидата с большими задатками, но без опыта синоби, если вы точно не знаете, что делает синоби? Как обучить таких кандидатов без доступа к настоящим синоби?

Рекомендуемые меры безопасности и способы снижения риска

Эти рекомендации представлены с учётом стандарта NIST 800-53 и системы кибернетических кадров NIST 800-16.[11] Учитывайте их при оценке потенциальных сотрудников, которые будут внедрять меры безопасности.

1. Определите знания, навыки и способности, необходимые для исполнения обязанностей по кибербезопасности в организации. Учитывайте эти потребности вместе с эталонами компетентности, навыками персонала и требованиями миссии при поиске, найме и обучении талантов. [PM-13 Security and Privacy Workforce]
2. Определите требования к найму на должности «кибериндзя», изучив и задокументировав необходимые блоки знаний:
   • передовые сетевые технологии и протоколы;
   • цифровая криминалистика;
   • разработка программного обеспечения;
   • соответствие требованиям;
   • защита компьютерных сетей;
   • управление конфигурацией;

- криптография и шифрование;
- безопасность данных;
- базы данных;
- управление идентификацией и конфиденциальностью;
- управление инцидентами;
- промышленные системы управления;
- обеспечение информации;
- информационные системы;
- ИТ-системы и эксплуатация;
- безопасность сетей и телекоммуникаций;
- кадровая безопасность;
- физическая и экологическая безопасность;
- безопасность архитектуры, систем и приложений;
- управление рисками безопасности;
- веб-безопасность.

3. Рассмотрите следующие виды обучения, сертификаты и протоколы:

```
OV-6, ANTP-*, ARCH-*, COMP-1/5/9/10, CND-*, CM-*, CR-*,
DS-*, DB-*, DF-*, IM-*, IR-*, ICS-*, IA-*, WT-*, SI-*,
ITOS-*, NTS-*, PS-*, PES-1, RM-*, SW-*, SAS-*.
```

Разбор

В этой главе мы рассмотрели качества, которые синоби считали необходимыми для успеха в своём ремесле. Кроме того, описали некоторые неофициальные методы собеседования, применявшиеся синоби. Мы исследовали множество современных процессов найма и причины их недостаточной эффективности, а также перечислили несколько новых подходов к выявлению подходящих кандидатов. Мысленный эксперимент этой главы столь же актуален сегодня, как и для средневековых полководцев, которым требовались синоби для защиты от вражеских синоби. Найм людей с хакерским складом ума, у которых может не быть высокого среднего балла, солидного трудового стажа или деловой одежды, вероятно, поможет противостоять киберпреступникам лучше, чем наём обычного человека, всегда действующего строго по шаблону.

После найма талантливых и/или умелых защитников важно установить стандарты и процессы, позволяющие дисциплинированно защищать организацию. Без руководства с ясными ожиданиями защитники могут расслабиться и стать хуже, чем бесполезными. В следующей главе мы обсудим поведение в караульном помещении.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), 77-79.
[2] [назад] Cummins and Minami, *The Book of Ninja*, 37.
[3] [назад] Cummins and Minami, *The Book of Ninja*, 33, 36, 40.
[4] [назад] Cummins and Minami, *The Book of Ninja*, 79-80.
[5] [назад] Antony Cummins and Yoshie Minami, *True Path of the Ninja* (North Clarendon, VT: Tuttle Publishing, 2017), 74.
[6] [назад] Cummins and Minami, *True Path*, 125.
[7] [назад] Cummins and Minami, *True Path*, 158.
[8] [назад] Cummins and Minami, *The Book of Ninja*, 79.
[9] [назад] “The ASVAB Test,” Military.com, Military Advantage, дата последнего обращения 7 февраля 2020 года, https://bit.ly/2Xle3Eu.
[10] [назад] “Entering the Military: DLAB,” Military.com, Military Advantage, дата последнего обращения 7 февраля 2020 года, https://bit.ly/39fvNXc.
[11] [назад] “SP 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model,” Computer Security Resource Center, National Institute of Standards and Technology, опубликовано в апреле 1998 года, https://bit.ly/3otA9QY.

Глава 24. Поведение в караульном помещении

> Не ослабляйте бдительность, даже когда не сталкиваетесь с врагом.

> В караульном помещении запрещается громко разговаривать, пить спиртное, петь, приглашать проституток или играть в азартные игры.
>
> - «Ёсимори хякусю», стихотворение 65

Свитки синоби полны подробностей об обходе сотрудников безопасности цели. Для синоби на местности ни одно защитное препятствие не было столь насущным и сложным, как вражеская стража. Хотя свитки предписывают действовать в слепых зонах, за которыми стражникам трудно наблюдать или которые трудно защищать, самые пригодные для эксплуатации бреши возникали не из плохой военной стратегии или нехватки людей, а из небрежности и недисциплинированности стражников.

Свитки советуют искать явно уставших, ленивых, плохо организованных стражников, не знающих приёмов синоби или проявляющих самоуспокоенность. Существует множество способов оценить и использовать их возможности. Среди прочего «Бансэнсюкай» рекомендует:[1]

- шептать рядом со стражниками, проверяя их внимательность, а затем не менее часа следить за реакцией, чтобы оценить способы и возможности ответа;
- выявлять небрежных стражников, которые действуют по сигналам скрытой охраны, тем самым выдавая присутствие внедрённых защитников, например разведчиков, слушающих или принюхивающихся;
- выбирать караульные помещения, где стражники говорят громко, непрерывно беседуют либо чрезмерно пьют и пируют: всё это указывает на неопытность или небрежность;
- ждать или вызывать событие, вынуждающее стражников покинуть пост.

Тот же свиток советует наблюдать за поведением, движениями, осанкой и действиями стражников, чтобы больше узнать об их дисциплине. Например, если ров и окружающий замок периметр содержатся в чистоте, расчищены и хорошо освещены, охрана, вероятно, бдительна и соблюдает защитную гигиену. Но если общеизвестные пути входа в замок, такие как углы, водосбросы и канализационные выходы, не защищены, это может означать, что стражники или их командиры пренебрегают обязанностями.[2]

Проникновение во вражеские караульные помещения давало синоби важнейшее понимание способов улучшить дисциплину, поведение и возможности собственной охраны. Свитки снова называют небрежность и лень главными препятствиями для успешной защиты и возлагают обязанность преодолеть эти пороки на господ и полководцев. Строгая дисциплина, тяжёлая подготовка и тщательное внимание к деталям могли дать стражникам необходимую душевную стойкость для защиты от вражеских угроз, включая других синоби.[3] «Всё до единой вещи определяется вашим разумом и образом мыслей, - гласят стихи ниндзя. - Если вы всегда считаете, что стоите перед врагом, то никогда и ни в чём не ослабите бдительность».[4]

В этой главе мы сравним караульные помещения времён синоби с современными центрами управления безопасностью (security operations center, SOC). Кратко рассмотрим модернизацию безопасности, которая переложила ответственность за неё со специальных сотрудников на весь персонал. Мы разберём способы, позволяющие внешнему субъекту угроз обнаружить слабые средства и методы безопасности сети. Кроме того, изложим некоторые теоретические соображения о прямом взаимодействии сотрудников безопасности с противниками, особенно если противник может проникнуть в системы заявок SOC/реагирования на инциденты, а также другие идеи о том, как он способен оценить бдительность SOC. Самое важное - мы обсудим, почему поведение

сотрудников безопасности столь существенно, почему со временем оно может ухудшаться и как создать культуру превосходства в безопасности.

Проблемы и ожидания центра управления безопасностью

Сотрудникам кибербезопасности и ИТ особенно легко стать ленивыми, самодовольными, небрежными, уставшими или выгореть. Причин бесчисленное множество.

Одна из крупнейших - неприятная реальность человеческой природы: если никто не смотрит через плечо, многие работники просто уклоняются от обязанностей. У ленивых специалистов по кибербезопасности достаточно прикрытий. Их задачи в основном невидимы коллегам и даже руководителям. Многие операционные центры изолированы за запертыми дверями, где сотрудники работают, отдыхают или спят так, что никто не видит разницы. Их сети и машины находятся в отдельных VLAN или на «исследовательских» компьютерах, позволяющих свободно просматривать интернет без журналирования, проверки и фильтрации.

Сильная зависимость отрасли от процессов тоже может убаюкать сотрудников до небрежности или самоуспокоенности. Из-за процедурного повторения сотрудники безопасности приобретают привычки и узкие представления о том, что значит защищать организацию. Эта тенденция возникает из необходимых повседневных процедур, но одновременно создаёт узкоспециализированных защитников одного инструмента или подхода, которые не рассматривают приёмы и средства нападающих за пределами собственного ежедневного опыта. Столь ограниченное мышление оставляет организации значительные бреши.

У целеустремлённых сотрудников противоположная проблема. Работа в конкурентной сфере, требующей глубоких специализированных знаний, способностей и честолюбия, повышает риск выгорания. После утомительных месяцев охоты за угрозами и инцидентами легко потерять сосредоточенность, полагаться на известные концепции, ждать предупреждения защитной системы или программы и изучать лишь необходимое для отчёта либо устранения конкретных инцидентов по мере их появления.

Специалисты по кибербезопасности не единственные, кто определяет компьютерную грамотность и осведомлённость о безопасности: ответственность несут все сотрудники. К сожалению, это означает, что лень и небрежность нетехнических работников часто создают организации большую угрозу, чем злонамеренный внешний субъект. Они могут случайно открыть сеть или системы компании для угроз, беспечно переходя по ссылкам фишинговых писем или подключая чужие USB-накопители, найденные на парковке. Если руководство в необходимых случаях не обеспечивает бдительность и дисциплину, добросовестные сотрудники вынуждены работать в культуре, где небрежных работников множество и их даже могут награждать. Успех превращается в игру на истощение, в которой повышают тех, кто дольше всех выдержал, не выгорев и не уволившись. Такая среда подрывает трудовую этику, дисциплину и честность эффективных работников и ухудшает весь коллектив, позволяя субъектам угроз эксплуатировать многочисленные бреши, созданные небдительными сотрудниками.

Поддержка и компетентность руководства значительно повышают моральный дух и бдительность, а плохие решения руководителей и организационные стратегии способны ослабить состояние безопасности и доверие сотрудников. Попытки исправить слепые зоны или слабости обычно требуют сотрудничества отделов, общих бюджетов, работы по выходным и неудобств, вызывающих жалобы и сопротивление. В итоге измотанные и побеждённые инженеры по безопасности начинают цинично относиться к улучшениям и закрывать глаза на недостатки. Некоторые даже ждут инцидента, понимая, что реактивная позиция организации не позволит ничего улучшить, пока сначала не произойдёт нечто плохое.

Субъектам угроз бывает легко оценить бдительность организации по внешним наблюдаемым признакам:

• чрезмерному объёму сведений в сообщениях об ошибках сайтов;
• раскрытию подробностей политики паролей при входе;
• отсутствию содержимого заголовков политики безопасности;
• неправильно самостоятельно подписанным сертификатам;
• неверно настроенным механизмам аутентификации, отчётности и соответствия сообщений на основе домена (Domain-Based Message Authentication, Reporting and Conformance, DMARC) и структуре политики отправителей (Sender Policy Framework, SPF);
• плохо настроенным записям DNS;
• открытым интерфейсам управления на доступных из интернета серверах, защитных устройствах или сетевом оборудовании;
• раскрытию версий технологий или используемых средств безопасности.

Чтобы противостоять склонности к потере бдительности, защитники должны непрерывно оценивать себя и стремиться к улучшению. Руководители не всегда хвалят или награждают сотрудников за дополнительную защиту, но постоянная бдительность сообщает противнику, что первая линия обороны сильна, и намекает: внутренняя защита может быть ещё мощнее.

Влияние на поведение

Реакция сотрудников на рабочем месте зависит от их убеждений, рабочей культуры и выработанного опытом поведения. Формирование культуры посредством избирательного подкрепления и содержательных циклов обратной связи побуждает сотрудников стремиться к превосходству. Отсутствие обратной связи, особенно положительной, может быть самой сложной проблемой безопасности: поведение защитника легко скатывается в низкоэнергетическое состояние нигилизма безопасности. Причиной бывает отсутствие положительного подкрепления хорошего поведения. Возможно, сотрудники получают лишь результаты проверок соответствия и числа ключевых показателей эффективности (key performance indicator, KPI), которые не отражают полезности действий. Результаты хорошей работы, например предотвращение кражи интеллектуальной собственности или денег, могут проявиться только через годы, и потому на них трудно опираться. Ниже приведены советы по улучшению и поддержанию хорошего защитного поведения.

1. **Установите стандарты и развивайте культуру.** Министерство обороны США сформировало культуру, ставящую бдительность в безопасности на первое место. Бывшие сотрудники Министерства, переходящие в другие организации, регулярно описывают культурный шок от небрежности на новом месте и, к сожалению, со временем снижают стандарты, принимая новую культуру. Изучите инициативу Министерства обороны по культуре и соответствию в кибербезопасности (Cybersecurity Culture and Compliance Initiative)[5] и определите, какие элементы помогут создать культуру бдительности.

Среди возможных свойств, которые следует явно подчеркнуть:

- **Честность.** Поощряйте сотрудников сообщать об ошибках. Например, работник, случайно нарушивший безопасность сети, не должен скрывать инцидент из страха потерять работу. Он должен чувствовать себя достаточно защищённым, чтобы признать ошибку и помочь организации усилить брешь.
- **Компетентность.** Установите базовые образовательные стандарты для всех, кто действует в киберпространстве. Они должны определять ежедневное поведение, помогать людям выявлять риски и принимать разумные решения благодаря непрерывному обучению. Создание основной компетенции может означать запрет занимать некоторые должности тем, кто её не демонстрирует.
- **Профессионализм.** Для поддержания стандарта превосходства и культуры бдительности требуйте, чтобы сотрудники отвечали за свою работу и не срезали углы.
- **Склонность задавать вопросы.** Нанимайте людей, которые не принимают вещи как есть, а задают вопросы, анализируют и интерпретируют наблюдения. Следите, чтобы сотрудники могли безопасно высказаться и их не отбрасывали сразу либо не заставляли чувствовать себя глупыми.

2. **Обеспечивайте дисциплину.** Небрежность в безопасности влияет не только на работу или продукт одного человека, а подвергает риску целые организации. В разделе «Шесть положений о поведении в караульном помещении» из «Бансэнсюкай» сказано: «Следует соблюдать строгие правила, а если кто-то небдителен, его нужно сурово наказать».[6] Установите официальную процедуру выявления и наказания нарушений кибербезопасности и небдительной практики пользователей, сотрудников безопасности, ИТ и руководства. Не поддавайтесь желанию сделать директора по информационной безопасности (chief information security officer, CISO) или другого сотрудника козлом отпущения при инциденте: это разрушает культуру общей ответственности.
3. **Установите официальные процессы, процедуры и соответствие.** Выявите, задокументируйте и распространите задачи, правила и политики, которым должна следовать и которые должна обеспечивать группа безопасности. Определите способы измерять соблюдение стандартов. Не применяйте поверхностные KPI, например число созданных заявок или расследованных инцидентов: эти показатели не дают содержательной оценки работы. Назначайте руководителей, которые понимают безопасность, заботятся о ней, уделяют время развитию бдительности и выявляют несоответствие.
4. **Развивайте самостоятельность и вовлечённость.** Многие корпоративные сотрудники не чувствуют участия в работе. Они не принимают решений, не действуют в интересах организации и не вкладываются в успех компании или собственный. Скука - распространённая проблема безопасности, которую часто можно уменьшить, устраняя препятствия, удерживающие или лишающие мотивации к упреждающим защитным действиям. Дайте сотрудникам безопасности возможность:

   • экспериментировать с новыми средствами, процедурами и концепциями;

• изучать новые технологии, приёмы и инструменты;
• находить смысл в работе;
• получать положительные результаты, например путь карьерного развития или повышения;
• участвовать в стратегических решениях о риске;
• проводить учения синих и красных групп, например совместные фиолетовые учения, и другие моделирования, чтобы давать друг другу положительную обратную связь;
• отмечать успех обнаружения недостатков безопасности.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка с ценными активами внутри. Во время обхода вы замечаете, что в некоторых караульных помещениях копья странно расставлены, и подозреваете: часть ночной стражи придумала опираться на поддерживающие копья, чтобы отдыхать или спать, сохраняя вид стоящего и бодрствующего на посту человека. Вам не сообщали ни о спящих стражниках, ни об иных проступках охраны, и вы не знаете о недавних инцидентах безопасности.

Какие доказательства, если они вообще нужны, следует получить до принятия мер по улучшению безопасности, процессов и персонала? Как оценить внимательность стражников? Какие сведения о безопасности можно поручить им изучать во время смены, чтобы они не спали? Как получить честную обратную связь об улучшении внимательности и вовлечённости? Как наказать одного заснувшего в ночном дозоре стражника и как - целый полк, поступающий так же? Как создать культуру доверия и честности, чтобы стражники без страха наказания могли сообщить о неполадках?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую следует оценивать с учётом поведения в караульном помещении.

1. Разработайте, задокументируйте и предоставьте всем сотрудникам обучение, процедуры и правила поведения в области безопасности. Создайте особое обучение и процедуры для ролей со значительной ответственностью, например разработки, ИТ, безопасности и руководства. Применяйте строгие дисциплинарные меры за несоблюдение политики и процедур. [AT-1: Awareness and Training Policy and Procedures; AT-2: Awareness Training; AT-3: Role-Based Training; IR-2: Incident Response Training; PL-4: Rules of Behavior; SA-16: Developer-Provided Training]
2. Проводите основанные на результатах испытания скорости реакции, состояния и возможностей инструментов безопасности посредством специализированных оценок, сканирования, испытаний на проникновение и красных групп. Это выявляет несоблюдаемые процессы или процедуры, слепые зоны и небдительных сотрудников. [CA-2: Assessments | (2) Specialized Assessments; CA-8: Penetration Testing; IR-3: Incident Response Testing; RA-5: Vulnerability Scanning; SC-7: Boundary Protection | (10) Test Exfiltration; SI-4: System Monitoring | Testing of Monitoring Tools and Mechanisms; SI-6: Security and Privacy Function]

3. Создайте учебные программы и учения для непрерывного совершенствования знаний, навыков и компетентности сотрудников безопасности. [CA-8: Penetration Testing; IR-3: Incident Response Testing | (3) Continuous Improvement; PM-12: Insider Threat Program; PM-13: Security and Privacy Workforce; PM-14: Testing, Training, and Monitoring; PM-16: Threat Awareness Program]
4. Позволяйте сотрудникам безопасности определять, какие конфигурации и средства следует менять для улучшения защиты. Возлагайте на владельцев, обслуживающих специалистов и разработчиков систем обязанность привести сильные, основанные на доказательствах доводы, почему рекомендованные изменения нельзя внедрить. [CM-3: Configuration Change Control]
5. Внедрите политику и процесс рассмотрения жалоб сотрудников безопасности. Такая обратная связь помогает улучшать процессы, пересматривая или отменяя неправильные средства. Она также позволяет пользователям сообщать о проблемах и предупреждать сотрудников безопасности без страха последствий. [PM-28: Complaint Management]
6. Требуйте, чтобы сотрудники безопасности соблюдали оперативную безопасность (operations security, OPSEC), защищая ключевые сведения об операциях, конфигурации и развёртывании и не раскрывая OPSEC противникам, которые могут испытывать защиту. [SC-38: Operations Security]

Разбор

В этой главе мы рассмотрели способы, которыми синоби прощупывали стражников и караульные помещения, оценивая возможности проникновения по стандартам безопасности цели или их отсутствию. Мы увидели, что сотни лет назад, как и сегодня, стражники часто становились самодовольными и что умелые нарушители пользовались этим. Кроме того, мы кратко рассмотрели, как культура формирует способность организации защищаться; в философии синоби этой концепции придавалась первостепенная важность. Затем культуру синоби сопоставили с современными SOC и рабочими культурами информационной безопасности, в которых есть проблемы, вероятно пригодные для эксплуатации сегодняшними киберпротивниками. Мы описали несколько способов и лучших методов создания и поддержания культуры превосходства в безопасности.

В следующей главе мы обсудим принцип синоби «опасности незнакомца» - запрет подозрительным людям приближаться. Повторение этого сообщения для создания культуры безопасности вместе со строгими средствами, не позволяющими подозрительным событиям стать вредоносными, демонстрирует превосходство организационной безопасности.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), 128, 178-180, 259.
[2] [назад] Cummins and Minami, *The Book of Ninja*, 93, 222.
[3] [назад] Cummins and Minami, *The Book of Ninja*, 93.
[4] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), 164.
[5] [назад] “Department of Defense Cybersecurity Culture and Compliance Initiative (DC31),” U.S. Department of Defense, опубликовано в сентябре 2015 года, https://bit.ly/3s1npTY.
[6] [назад] Cummins and Minami, *The Book of Ninja*, 93.

Глава 25. Управление угрозами с нулевым доверием

> Если вы войдёте в комнату с задней стороны и кто-то внутри не спит, вас не заподозрят как нарушителя. Причина в том, что пришедших сзади не считают возможными ворами или нападающими.

> Никогда не позволяйте никому из-за пределов вашей провинции приближаться к караульному помещению, даже родственнику.
>
> - «Ёсимори хякусю», стихотворение 93

В феодальной Японии странствующие торговцы, монахи, священнослужители, актёры, увеселители, нищие и другие посторонние обычно действовали внутри или рядом с военным лагерем либо замком, поскольку размещённые там воины часто пользовались их услугами.[1] Однако некоторые посторонние были тайными оперативниками, которым враги платили за сбор сведений. Некоторые даже являлись замаскированными синоби: они пользовались близостью к замку, изучали цели или вступали с ними во взаимодействие, собирали разведывательные сведения и даже проникали в лагерь либо нападали на него.[2]

«Бансэнсюкай» описывает, как военные командиры могут блокировать такие угрозы. Самый эффективный подход - не допускать подозрительных действий и братания рядом с лагерем. Обсуждая политику, которую «следует строго внушить всем повторением», свиток предупреждает: любого подозрительно выглядящего человека нельзя впускать в замок или лагерь ни при каких обстоятельствах, что сокращает возможность превращения подозрительной деятельности во вредоносную угрозу.[3] Обученные и дисциплинированные войска позволяли действовать внутри лагеря или рядом с ним лишь доверенным торговцам и активно запрещали неизвестным либо ненадёжным торговцам предлагать услуги поблизости. Более широкая оперативная философия синоби состояла в недоверии ко всем незнакомым.[4] Кроме того, «Бансэнсюкай» рекомендует синоби помогать доверенным торговцам и продавцам защищать хижины и лавки от огня, уменьшая риск распространения пожара от них на лагерь из-за случайности или поджога.[5]

В этой главе мы рассмотрим режим «блокировать только вредоносное», способный превратиться в бесконечную погоню за новыми доменами, IP-адресами, URL и файлами, которые оказались вредоносными. Мы исследуем некоторые причины, по которым многие организации и отрасль безопасности выбирают эту нескончаемую ленту угроз вместо режима «блокировать всё подозрительное». Мы также изложим стратегии и рекомендации по решению технических проблем обратного подхода. В мысленном эксперименте исследуем способы, которыми внутренние сотрудники могут пытаться обойти средство безопасности «блокировать всё подозрительное».

Возможность угрозы

В контексте кибербезопасности представьте, что лагерь - это ваша организация, а торговцы, увеселители и все остальные за периметром - многочисленные внешние службы и приложения интернета. Все законные деловые соединения с внешними сайтами, помогающие сотрудникам работать, не говоря уже о новостях, социальных сетях и развлекательных сайтах, которые они посещают во время перерывов, позволяют подозрительным субъектам подключаться к организации и действовать под видом обычной работы. Субъектам угроз для первоначального доступа, доставки и эксплуатации часто необходимо, чтобы возможности внешней связи оставались без оспаривания, проверки и фильтрации. Среди последующих наступательных приёмов - попутная компрометация посещаемых сотрудниками сайтов, целевые фишинговые письма со ссылками и вложениями, сетевое сканирование среды с недоверенных IP-адресов и применение сайтов командования и управления (C2) для получения сведений и передачи инструкций вредоносным имплантатам на скомпрометированных машинах.

Для борьбы с такими атаками отрасль создала функциональные средства, политики и системы безопасности, вносящие в белый список надлежащую связь с известными и доверенными партнёрами и другими проверенными сторонними деловыми субъектами. Организация может создать белые списки доменных имён, блоков IP-адресов, серверов имён, адресов почты, сайтов и центров сертификации, позволяя сотрудникам связываться только с доверенными партнёрами и наоборот. При строгом белом списке субъект угроз до попытки взлома организации должен потратить время, ресурсы и внимание на проникновение к доверенному партнёру.

Но техническая задача решена, а человеческая остаётся. Человеку свойственно искать стимулы во внешних отношениях, развлечениях и новостях. Поэтому руководству трудно обеспечивать политику «блокировать подозрительное»: она требует силы воли для значительного культурного и поведенческого изменения во всех частях организации.

Предположим, вы замечаете, что большая часть интернет-трафика организации связана с потоковым видео сотрудников на развлекательных сайтах. Эта деятельность не соответствует рабочим обязанностям, и вы решаете заблокировать все крупные развлекательные сайты средствами обнаружения уровня 7.

Хотя разумная мера соответствует деловым потребностям и, возможно, даже задокументированной ИТ-политике, многие прошедшие через это организации пожалели о решении. Сотрудники, вероятно, будут жаловаться или оказывать общественное давление, требуя разблокировать трафик, а некоторые наверняка попытаются обойти политику посредством шифрования или туннелей, обхода прокси либо посещения похожих развлекательных сайтов, не попавших в фильтры, подвергая сеть и системы ещё большему риску.

Популярное решение - предоставить неделовую интернет-сеть либо сеть «принеси собственное устройство» (bring your own device, BYOD), где сотрудники смогут смотреть видео на личных устройствах. Можно даже установить отдельные машины для интернет-исследований и перерывов, но не деловых функций. Министерство обороны США применяет такой подход, предоставляя сотрудникам отдельную специализированную систему для доступа к несекретному интернету (NIPRnet); сетевые шлюзы физически и логически отделяют её для контроля потоков информации.[6] Министерство принимает и дополнительные меры: вносит в белый список все известные невредоносные ресурсы интернета и запрещает крупные блоки IP-адресов и номера автономных систем (ASN), которые считает подозрительными или по меньшей мере ненужными.

Последние десять и более лет организации постоянно потребляют потоки угроз с известными вредоносными IP-адресами, доменами и URL, поэтому блокировать известное вредоносное с помощью чёрного списка достаточно легко. Блокирование подозрительного останавливает неизвестный вредоносный трафик, но даётся организациям намного труднее, часто по

обоснованным причинам. Создать главный белый список всех известных безопасных интернет-ресурсов, сайтов и IP-адресов, которыми будут пользоваться сотрудники, чрезвычайно сложно. И снова Министерство обороны служит образцовым практиком: оно упреждающе устанавливает политику блокирования и предотвращения таких сценариев угроз. Оно также постоянно напоминает сотрудникам посредством плакатов OPSEC, обязательного обучения, условий использования систем и ясных системных предупреждений, что нельзя обходить правила или средства, поскольку это способно скомпрометировать безопасность сети, систем и сведений.

Блокирование подозрительного

«Опасность незнакомца» - простая концепция, которую многие дети изучают в раннем возрасте. Потенциальная угроза ребёнку предотвращается нулевой терпимостью к приближению любого незнакомца. Это несовершенная стратегия, но она может быть эффективна, если все известные субъекты, то есть не незнакомцы, проверены как надёжные. Преимущество стратегии в том, что она не зависит от дополнительных уровней безопасности, реагирующих на угрозу, ранее распознанную как подозрительная. Поскольку дети и многие организации беззащитны после того, как вредоносной угрозе позволили взаимодействовать с ними, политика «блокировать всё подозрительное» может оказаться их первой и единственной защитой. Ниже приведены рекомендации по применению концепций в вашей среде.

1. **Практикуйте идентификацию, осведомлённость и понимание.** Покажите заинтересованным лицам идею необходимости блокировать подозрительные сайты. Хорошая отправная точка - выполнить ping или внешний DNS-запрос к серверу в Иране, Северной Корее (`175.45.178.129`) либо другой известной, но маловероятной угрозе для организации. Успешный ответ означает, что сеть разрешила связь с подозрительной системой без уважительной деловой причины. Такая проверка обычно работает. Организации склонны блокировать вредоносное, а не подозрительное, и, поскольку ни один известный IP-адрес из интернет-пространства этих стран не размещал вредоносное ПО или не проводил атаки, он не попал в известные потоки плохих угроз.

   Получив доказательство того, что нужно блокировать, организация может запретить один IP-адрес или, после запроса группе безопасности на изменение межсетевого экрана, возможно, принадлежащий ему сетевой блок `/24`. Однако необходимо оценить и заблокировать более 14,3 миллиона подсетей IPv4 `/24`, и у организации естественным образом может не быть времени, воли или ресурсов для всеобъемлющего списка подозрительного интернета. Вместо этого начните документировать белый список, понимая, что он создаст ложноположительные результаты, но одновременно заблокирует вредоносное, подозрительное и будущее либо неизвестное вредоносное.

2. **Вступите в центр обмена и анализа информации (information sharing and analysis center, ISAC) или создайте его.** Чтобы уменьшить нагрузку создания главного белого списка, обменивайтесь с компаниями той же отрасли сведениями о доверенных сайтах, IP-адресах и доменах, которые сотрудники используют для деловых функций. Создание системы профилирования для главных белых списков интернета представляет деловую возможность. Организации могли бы применять такие списки для сокращения числа встречаемых подозрительных сайтов, облегчая построение и обслуживание защищённых сетей.
3. **Ищите взаимную гарантию.** Проводите взаимное сканирование уязвимостей и учения красных групп с доверенными внешними субъектами, с которыми организация ведёт дела. Это соответствует совету «Бансэнсюкай» помогать доверенным торговцам защищать здания от огня ради общей безопасности. Оставьте меру для организаций, относящихся к доверенной

экстрасети, имеющих прямые межсоединения или применяющих иные туннели, обходящие обычные защитные средства.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка с ценными активами внутри. Вы замечаете различных незнакомцев, которые разбивают лагерь, слоняются и торгуют рядом с замковыми стенами. Многих торговцев вы не узнаёте, а стражники жалуются, что их присутствие не только отвлекает, но и затрудняет выявление возможных вражеских агентов рядом с замком. Вы запрещаете лагеря возле замка и создаёте широкий расчищенный периметр, но через несколько недель командиры сообщают, что воины чувствуют себя изолированными. Более того, надеясь обойти запрет, торговцы по ночам подходят к замку и быстро продают товары воинам в скрытых местах. Это приводит к нескольким происшествиям: воины остаются снаружи после комендантского часа, а неизвестные скрытно приближаются к замку, ещё сильнее затрудняя стражникам различение друзей и врагов.

Как изменить запрет, чтобы предотвратить ночные встречи? Какие дополнительные правила или наказания можно ввести для лучшего обеспечения политики «блокировать подозрительное», не причиняя вреда организации? Как разрешить незнакомцам приближаться к замку, не давая вражеским синоби возможности скрытно проникнуть или напасть?

Рекомендуемые меры безопасности и способы снижения риска

Там, где это уместно, рекомендации сопровождаются применимыми мерами безопасности из стандарта NIST 800-53. Каждую следует оценивать с учётом концепции блокирования подозрительного.

1. Внедрите политику «принеси собственное устройство» для пользователей, желающих подключаться к интернету по неделовым причинам, либо предоставьте сотрудникам дополнительную специализированную рабочую станцию для внешних интернет-соединений. [CA-3: System Interconnections | (1) Unclassified National Security System Connections; SC-7: Boundary Protection | (1) Physically separated subnetworks]
2. Для входящих и исходящих соединений создайте белые списки, запрещающие всё, кроме задокументированных исключений. [CA-3: System Interconnections | (4) Connections to Public Networks | (5) Restrictions on External System Connections; SC-7: Boundary Protection | (5) Deny by Default-Allow by Exception]
3. Обменивайтесь сведениями с похожими организациями для создания главного белого списка. [PA-4: Information Sharing with External Parties]

Разбор

В этой главе мы рассмотрели, как командиры укреплений синоби принимали политики безопасности, значительно затруднявшие работу вражеских синоби. Мы также обсудили, насколько трудно современным организациям принять сходную стратегию, включая задачи, которые пришлось бы решить для аналогичного подхода к сетевой безопасности. Мы исследовали несколько идей применения концепции «блокировать подозрительное» в качестве практического руководства.

В следующей главе мы объединим концепции предыдущих глав, чтобы применить их к аналитике угроз. Последняя глава завершает книгу, связывая всё изученное о синоби с настоящими киберугрозами, встречавшимися ранее.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), 83.
[2] [назад] Cummins and Minami, *The Book of Ninja*, 84.
[3] [назад] Cummins and Minami, *The Book of Ninja*, 83.
[4] [назад] Cummins and Minami, *The Book of Ninja*, 84.
[5] [назад] Cummins and Minami, *The Book of Ninja*, 84.
[6] [назад] “Sensitive but Unclassified IP Data,” Network Services, Defense Information Systems Agency, дата последнего обращения 7 февраля 2020 года, https://bit.ly/2Xl9s57.

Глава 26. Оперативное искусство синоби

> Тайные приёмы безошибочного проникновения обманны, разнообразны, гибки и применяются по обстоятельствам. Поэтому за основу следует взять древние способы синоби, служивших великим полководцам прошлого, но не просто держаться этих способов, а приспосабливать каждый к ситуации и моменту.

> Даже если снаружи стоит грохот, помните: караульное помещение нельзя оставлять совершенно пустым. Кроме того, следует прислушиваться ко всем звукам.
>
> - «Ёсимори хякусю», стихотворение 66

Хотя синоби иногда нанимали охранять замки и другие укрепления, как описано в «Сёнинки»,[1] большинство караульных постов феодальной Японии занимали обычные воины или наёмники, обученные отражать рядовых нарушителей. Но «Бансэнсюкай» и руководство «Гунпо дзийосю» советуют полководцам, защищающимся от синоби, нанимать собственных: они могли обучить обычных стражников выявлять тайные тактику, техники и процедуры (techniques, tactics, and procedures, TTP) синоби.[2] Многие TTP описаны в свитках, однако они непрерывно разрабатывались и совершенствовались, а разные кланы владели собственными секретными приёмами, неизвестными другим синоби.

TTP синоби были хитроумными и изящными и часто служили нескольким целям. Например, синоби мог тайно воткнуть в землю обычный зонтик и раскрыть его в поле зрения замковой стражи. Под зонтиком можно было спрятать предметы от стражников, а явный признак человеческой деятельности мог также увести их с постов.[3] Приём использовал и распространённое суеверие эпохи: считалось, что забытые или потерянные зонтики становятся одержимыми и преследуют прежнего владельца; явление называли *цукумогами*, *каса-обакэ* и *ёкай*.[4]

Нанятые для обучения стражников синоби сталкивались с особой педагогической задачей: записывать TTP или сообщать их посторонним было запретно, поскольку это нарушало целостность навыка и подвергало риску жизни других синоби. Некоторые отрывки даже советуют убить свидетеля или жертву, раскрывших TTP.[5]

Поэтому вместо выдачи конкретных приёмов синоби подчёркивали правильный образ мыслей, высокий уровень осведомлённости и тщательность, необходимые для поимки синоби.[6] Эту мысленную позицию подкрепляли оценкой риска лагеря стражников, знанием врага и наиболее вероятных и значимых сценариев угроз. По-видимому, синоби давали стражникам общее представление о возможностях синоби и примеры сценариев, но описывали их так, чтобы не раскрывать профессиональные секреты полностью.[7] Они учили стражников признакам возможной деятельности синоби - видам, звукам и другим наблюдаемым явлениям на посту - и устанавливали правила предотвращения ошибок.[8]

Из-за бесчисленного множества приёмов и отсутствия формального образования у многих стражников синоби передавали знания стихами, облегчая запоминание. Этим объясняется множество стихов об осведомлённости стражи в «Ста стихотворениях ниндзя» из «Ёсимори хякусю»: они предназначались не самим синоби, а для передачи стражникам. Стихи снова давали достаточно подробностей для описания тактики и реалистичных советов, но не настолько много, чтобы перегрузить охрану. Например, стихотворение 66 в начале главы даёт простой совет: не оставлять пост пустым и слушать любые звуки, включая не только первоначально привлёкший внимание грохот, но и шаги, приближающиеся сзади.[9] Стихи объединялись по темам. Стихотворения 64-67, 78, 79, 91, 93 и 94 посвящены поддержанию осведомлённости и предотвращению ошибок: как нести ночную вахту в усталости, куда смотреть и почему нельзя пить, петь и приглашать проституток на службе.

Разумеется, заметив, что стражники активно ищут TTP синоби, вражеский синоби применял контрмеры. Ясный пример из всех трёх главных свитков - синоби, прячущийся в кустах или высокой траве либо ползущий через поле. Его движение тревожит насекомых, которые замирают и умолкают, скрываясь. Для обученного стражника отсутствие жужжания и стрекота означает приближение скрытого человека. Обычно, если стражник внезапно настораживался и начинал поиск, а синоби понимал, что раскрыт, тот тихо отступал.[10] Тогда применялась контрмера: перед следующей попыткой синоби ловил сверчков в коробку. Не обеспокоенные присутствием несущего их синоби сверчки свободно стрекотали и заполняли тишину вокруг приближающегося к посту человека. У стражников больше не было причины подозревать его приближение.[11]

Стихотворение 68 ярко показывает сложность обнаружения TTP и контрмер: «Следует проводить тщательный поиск, идя следом за ночным дозором. Это называется *камарицукэ* [обнаружение засады]».[12] Ночью командир отправлял основную поисковую группу патрулировать периметр с обычными фонарями и снаряжением, но вслед за ней тайно высылал вторую.[13] Советники-синоби учили патрульных искать всё неуместное, особенно звуки, движение и людей.[14] Вражеские синоби знали о наставлении. Свитки описывают, как нападающие прятались в кустах, канавах или иных тёмных местах до прохода патруля, а затем продолжали работу.[15] Иногда враг мог идти следом за патрулём, прикрывая движение звуком и светом защитников, и даже напасть сзади.[16] Поэтому вторая тайная группа за первой могла поймать скрытого вражеского синоби. Тяжеловооружённые воины исследовали вероятные укрытия и искали врага, следующего за основным патрулём.[17]

Однако знающий *камарицукэ* нападающий мог дождаться в тени прохода второго патруля или переместиться туда, где тот не станет искать. Для противодействия этой контрмере, то есть контрмеры против контрмеры против контрмеры, добавили стихотворения 69 и 70:[18]

> **69:** «После проведения ночного дозора важно выполнять *камарицукэ* снова и снова».
>
> **70:** «Говорят, при выполнении *камарицукэ* следует делать несколько обходов через разные промежутки, чтобы обнаружить вражеских агентов-синоби».

Такой совет вводил непостоянный ритм патрулей *камарицукэ*, мешая противнику свободно действовать. Частые и частично непредсказуемые обходы с одной или несколькими следующими группами оставляли вражескому синоби мало возможностей уверенно действовать против укрепления или патрулей защитников.[19]

Добросовестное обнаружение TTP и применение контрмер может быстро обостряться, но в конце концов нападение на укрепление становится слишком опасным или непрактичным. Зачастую это лучший результат, на который защитники могут надеяться в борьбе с вражескими синоби.

В этой главе мы обсудим применение философии оперативного искусства синоби к пониманию TTP субъектов киберугроз. Кратко рассмотрим, как аналитика киберугроз помогает специалистам по реагированию, инженерам безопасности и охотникам лучше защищать организацию, подобно тому как синоби повышали эффективность обычной замковой стражи и воинов обороной на основе разведывательных сведений. Мы исследуем несколько распространённых систем описания TTP киберугроз. Их сочетание со знанием синоби облегчает понимание угроз и пользы TTP. Мы разберём, почему буква P, процедуры, часто остаётся загадкой и, вероятно, останется неизвестной, но также теоретически восстановим процедуры рационального противника из известных действий синоби. Наконец, рассмотрим внедрение аналитики киберугроз в стратегию защиты и причины сложности этой задачи.

Техники, тактика и процедуры

В кибербезопасности TTP описывают подходы к анализу закономерностей поведения, деятельности и методов конкретного субъекта либо группы угроз. *Тактика* описывает оперативные манёвры противника, например разведку, горизонтальное перемещение и развёртывание бэкдоров. *Техники* - подробные технические способы выполнения задач, например применение конкретного инструмента или программы для создания оружия либо эксплуатации. *Процедуры* подробно определяют стандартные политики и направления действий: проверить наличие активных пользователей в эксплуатированной системе до дополнительных задач, выполнить анализ строк вредоносной программы на профессиональные ошибки перед развёртыванием или провести предупредительную самоочистку после проверки связи на целевой машине.

После выявления и определения TTP защитники могут искать их индикаторы в своей среде. Они способны даже предсказывать возможные TTP против них, поддерживая планирование и упреждающее внедрение смягчений или контрмер. Для общего определения и обмена TTP киберпротивников отрасль разработала множество концепций, моделей, анализов и способов обмена:

• Pyramid of Pain;[20]
• платформа ATT&CK;[21]
• модель Attack LifeCycle;[22]
• платформа Cyber Kill Chain;[23]
• Diamond Model of Intrusion Analysis;[24]
• STIX (Structured Threat Information eXpression).[25]

Пирамида боли

Пирамида боли на рисунке 26-1 - прекрасная модель для изображения того, как осведомлённость об индикаторах, инструментах и TTP противника влияет на состояние защиты. Она также показывает, как для защитников и нападающих возрастает сложность внедрения мер и контрмер. Название выражает идею: абсолютную безопасность или предотвращение всех атак гарантировать нельзя, но противник с меньшей вероятностью выберет организацию целью, если вынужден будет мучительно тратить время, ресурсы и усилия.

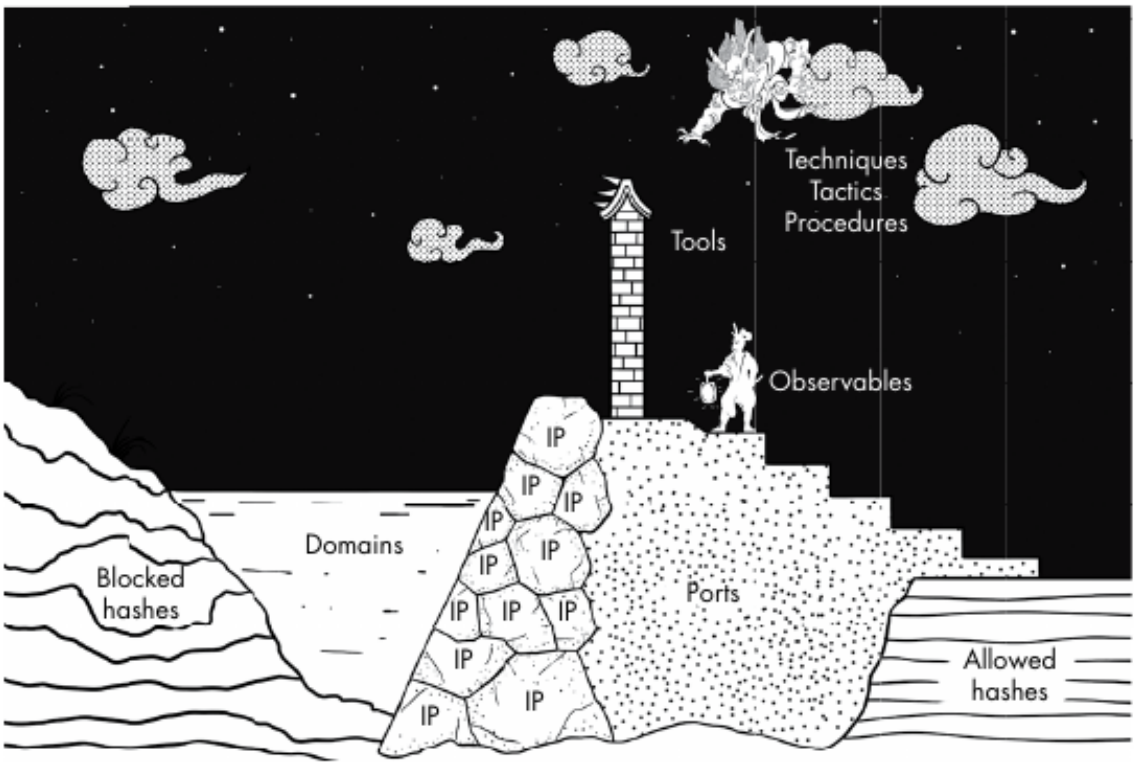

Рисунок 26-1. Укрепление индикаторов компрометации (адаптировано из Pyramid of Pain Дэвида Бьянко[26])

Внизу пирамиды находятся индикаторы компрометации (indicator of compromise, IoC), такие как домены, IP-адреса, хеши файлов и URL, которые однозначно выявляют известные вредоносные признаки. Защитники могут блокировать их или создавать предупреждения, но противник способен их менять.

Над атомарными индикаторами расположены индикаторы узлов: ключи реестра, оставленные файлы и артефакты. Их можно обнаружить или отреагировать на них, но обнаружение либо смягчение не всегда автоматизировано, а противник может изменять их в зависимости от цели или операции.

Следующий уровень - инструменты, программы или устройства, которыми противник проводит либо поддерживает наступательные действия. Ища известные вредоносные инструменты, удаляя доступ к ним или отключая функции, защитники могут обнаружить противника и помешать ему эффективно действовать.

Наверху пирамиды находятся тактика, техники и процедуры. Если их удаётся выявить или смягчить, противнику трудно создавать или осваивать новые TTP против вас, хотя и защитнику болезненно разрабатывать меры либо контрмеры.

Платформа ATT&CK

Платформа MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) выводит многие тактики из Cyber Kill Chain компании Lockheed Martin (рисунок 26-2). Cyber Kill Chain выделяет семь этапов жизненного цикла атаки: разведку, создание оружия, доставку, эксплуатацию, установку, командование и управление и действия ради целей. Каждая тактика ATT&CK перечисляет техники и методы с примерами обнаружения или смягчения.

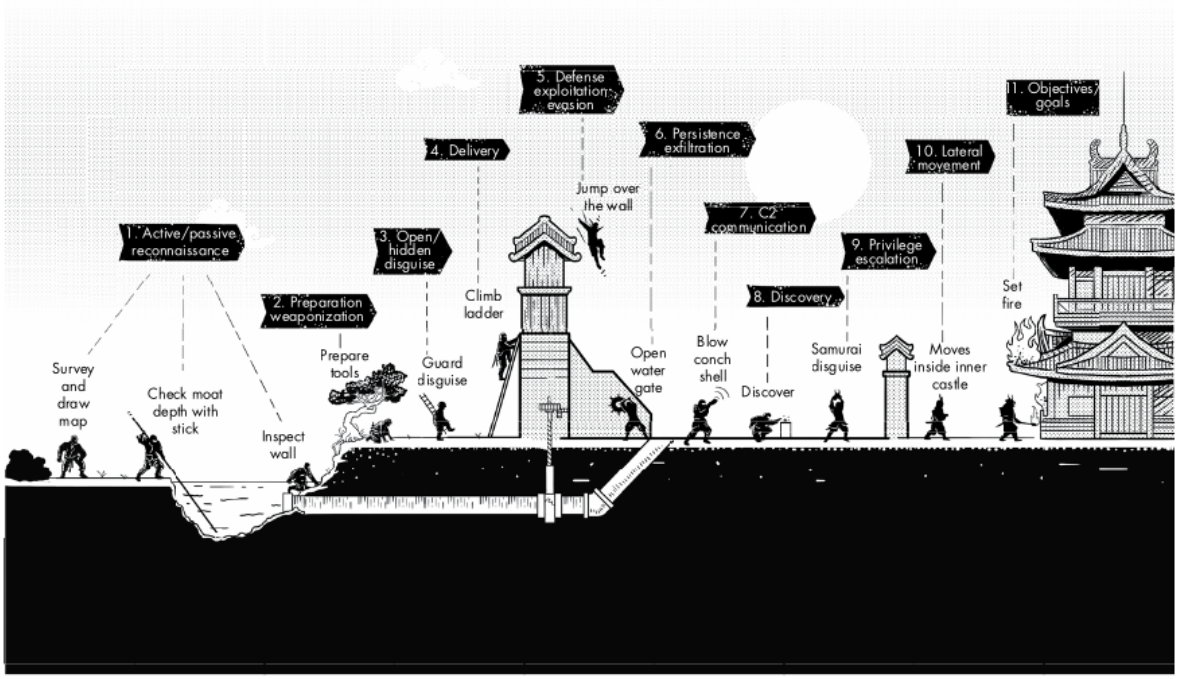

Рисунок 26-2. Цепочка атаки ниндзя (адаптировано из платформы MITRE ATT&CK[27])

Обратите внимание: в ATT&CK отсутствуют процедуры. Это понятно, поскольку для их выявления, вероятно, пришлось бы похитить и проанализировать книгу наступательных кибероперациий государства или вооружённых сил. Именно поэтому тексты «Бансэнсюкай», «Нинпидэн» и «Сёнинки», описывающие процедуры искушённой шпионской группы, так обогащают обсуждение.

Аналитика угроз

Когда группа безопасности понимает эти тактику и техники, выявила поверхности атаки, оценила нынешние средства и проанализировала прежние инциденты для определения эффективности защиты, можно начать предсказывать, какие части среды выберет противник. При хорошем наборе прогнозов можно начинать охоту за угрозами - искать оставленные субъектами индикаторы и доказательства возможной компрометации. Но без глубокого понимания точного образа действий субъектов эффективно охотиться или обнаруживать их присутствие трудно.

Здесь проявляется ценность аналитики угроз. Она не обязательно означает потоки новых IP-адресов, доменов, URL и хешей файлов, связанных с вредоносными программами, хакерской инфраструктурой или группами. *Аналитика киберугроз* (cyber threat intelligence, CTI) означает традиционную разведывательную деятельность по сбору и анализу таких киберугроз, как вредоносные программы, хактивисты, государства, преступники и DDoS. При правильном потреблении CTI даёт пригодные к действию разведывательные сведения и оценки действий, мотивов и TTP угрозы. Проще говоря, CTI - один из лучших способов понимать угрозы и

защищаться, поскольку требует от принимающих решения людей получать сведения и действовать.

К сожалению, многие потребители CTI обращают внимание лишь на IoC, которые легко загрузить в SIEM, межсетевые экраны и другие устройства для блокирования или обнаружения. Это лишает CTI настоящей ценности: подробные наблюдения и оценки аналитиков описывают поведение, закономерности, методы, принадлежность и контекст. Производители CTI не всегда раскрывают способ сбора разведывательных сведений, но часто стремятся прозрачно сообщать, что знают и почему считают, что угроза совершает определённые действия.

Разумеется, читать разведывательные отчёты ради понимания угрозы и одновременно глубоко изучать собственную среду трудно. Требуется широкий набор навыков, включая способность быстро учиться и принимать стратегические решения. Но если потребитель CTI выделяет время на понимание каждого шага, фрагмента кода, тактики и техники, он сможет принимать решения для успешного смягчения, обнаружения, реагирования и даже прогнозирования будущих движений угрозы.

Аналитика киберугроз

Уже купив десятки защитных решений и наняв штатных специалистов для множества векторов, некоторые могут считать CTI последним слоем расходов поверх модели «затраты в глубину». Однако CTI способна улучшить стратегии и усилить эффективность всех остальных уровней, оправдывая стоимость. К сожалению, эффективное применение CTI иногда похоже на чтение отчётов о новых научных открытиях: нужно понять последствия, а затем быстро изменить культуру, деловые стратегии и технологии. Это возможно, но такая интенсивность потребления, синтеза и действий кажется чрезмерно требовательной. В этом главная трудность CTI: это не хрустальный шар с лёгкими ответами, которые легко воплотить. Следующие рекомендации помогут принимать обоснованные решения о программе CTI.

1. **Развивайте аналитику киберугроз и охоту.** Подпишите организацию на бесплатный или платный отчёт CTI. Развивайте внутреннюю CTI, собирая доказательства угроз, атакующих среду сейчас. Создайте группу CTI для сбора и анализа находок и передачи результатов ИТ, безопасности и деловым заинтересованным лицам. Они должны понимать, кто выбирает организацию целью, как проникает, что сделает в сети, каковы предполагаемые цели и как они достигаются. Внедряйте стратегические и оперативные меры, смягчения и контрмеры против наблюдаемой тактики.

   Обучите сотрудников безопасности и разведки охоте. Поскольку не каждую угрозу можно технически разобрать или заблокировать, специализированная группа должна постоянно искать следы в сети, руководствуясь сведениями партнёра, поставщика или собственной группы CTI. Охоту можно усилить учениями фиолетовой группы, где красная группа выполняет враждебные действия в сети, а синяя охотится за ней и учится противодействовать.

2. **Потребляйте и применяйте CTI.** Проведите кабинетное учение с группами почты, ИТ и безопасности, моделируя TTP угрозы и оценивая реакцию. Предположим, поступили сведения о фишинговой кампании против похожих организаций с сокращателями ссылок Google (`http://goo.gl/`). Нельзя просто заблокировать IP-адреса, URL или домен Google, не помешав работе, а многие сотрудники законно используют сокращатели. CTI оценивает, что противник выбрал goo.gl потому, что антивирус, прокси или протокол фишинга не определяет ссылку как вредоносную: защитные системы знают Google как сайт из белого списка.

Сначала поищите такую ссылку в нынешних письмах. Многие организации сразу сталкиваются с препятствием: почтовый администратор не сотрудничает или не имеет видимости либо ресурсов для поиска входящих писем с гиперссылками goo.gl. Другими препятствиями могут быть карантин возможного фишинга, предупреждение сотрудников вне ИТ и безопасности и обучение обнаружению и избеганию угрозы.

Как у противника есть разные инструменты, тактика и техники, так и ваши средства требуют обдумывания, понимания, изобретательности и инженерии для целостного и эффективного блокирования и реагирования. Например, почтовый администратор создаст правило для goo.gl, но что делать с другими сокращателями? Группа CTI должна выявить угрозу фишинга со ссылками и сокращением и рекомендовать способы их обнаруживать, блокировать или смягчать, а также поддерживать осведомлённость людей об этом TTP. Иными словами, нужно искать не только goo.gl, а все сокращатели. Наконец, принимающие решения лица должны стратегически устранить угрозу новой архитектурой, политиками или средствами.

Каким бы болезненным ни был процесс, он необходим для выявления областей, где организации следует улучшить обнаружение, смягчение и реагирование.

Упражнение «Теория замка». Представьте, что вы правитель средневекового замка с ценными активами внутри. Вы получаете разведывательные сведения: протокол осведомлённости, которому вы научили стражников, - внезапная тишина насекомых может указывать на нарушителя - нейтрализован синоби с коробками сверчков. Сверчки обманывают стражников, заставляя думать, что всё в порядке.

Как переобучить стражников справляться с запутанной реальностью, где и тишина, и шум могут указывать на синоби поблизости? Какие дополнительные методы охоты или наблюдения помогут обнаруживать приближение? Как выявить коробку сверчков или применить контрмеры? Наконец, как вражеский синоби может ответить на новые контрмеры и защиту?

Рекомендуемые меры безопасности и способы снижения риска

Эти рекомендации представлены с учётом NIST 800-53; их следует оценивать с точки зрения осведомлённости, TTP и CTI.

1. Обучайте осведомлённости о безопасности персонал всех ролей, помогая быстро реагировать на встреченные угрозы. [AT-2: Security Awareness Training; PM-13: Information Security Workforce]
2. Выделите группу для анализа угроз, инцидентов, разведывательных сведений и TTP противника, а также разработки контрмер и защиты. [IR-10: Integrated Information Security Analysis Team]
3. Сотрудничайте с внешними группами безопасности и учреждениями обмена угрозами, получая сведения, относящиеся к организации. [PM-15: Contacts with Security Groups and Associations]

4. Внедрите программу осведомлённости об угрозах, сообщающую подробности CTI, способы смягчения и индикаторы компрометации. [PM-16: Threat Awareness Program]
5. Применяйте достоверные разведывательные сведения для охоты и наблюдения за деятельностью, поведением, закономерностями и другими признаками угрозы. [SI-4: Information System Monitoring]

Разбор

В этой главе мы рассмотрели несколько TTP синоби, особенно совместное развитие *камарицукэ* и контртактики защитника и противника до возникновения отказоустойчивой системы безопасности. Мы исследовали другую тактику киберугроз, которая тоже может развиваться, пока обе стороны противодействуют друг другу и не возникает устойчивость. Мы обсудили CTI и объяснили, почему недостаточно знать, что делает противник, как и что собирается сделать. Чтобы быть полезной, CTI должна потребляться с намерением каким-либо образом устранить угрозу. В мысленном эксперименте мы увидели ясный пример обнаружения наблюдаемого признака защитниками и последующего изменения тактики. Его можно сравнить с подделкой системных или сетевых журналов для обмана охотников, детекторов аномалий и даже систем машинного обучения, и он способен вновь появиться в современности. Самый важный урок главы и, возможно, всей книги: критически важно потреблять аналитику угроз и новаторски реагировать на динамические угрозы.

Сноски

[1] [назад] Antony Cummins and Yoshie Minami, *True Path of the Ninja* (North Clarendon, VT: Tuttle Publishing, 2017), 19.
[2] [назад] Antony Cummins and Yoshie Minami, *The Secret Traditions of the Shinobi* (Berkeley, CA: Blue Snake Books, 2012), 77.
[3] [назад] Antony Cummins and Yoshie Minami, *The Book of Ninja* (London: Watkins Publishing, 2013), 202.
[4] [назад] *Classiques de l'Orient*, 5 (1921), 193.
[5] [назад] Cummins and Minami, *The Book of Ninja*, 67.
[6] [назад] Cummins and Minami, *Secret Traditions*, 81.
[7] [назад] Cummins and Minami, *The Book of Ninja*, 66.
[8] [назад] Cummins and Minami, *The Book of Ninja*, 93.
[9] [назад] Cummins and Minami, *Secret Traditions*, 159.
[10] [назад] Cummins and Minami, *The Book of Ninja*, 208.
[11] [назад] Donn F. Draeger, *Ninjutsu: The Art of Invisibility* (North Clarendon, VT: Tuttle Publishing, 1989), 65.
[12] [назад] Cummins and Minami, *Secret Traditions*, 160.
[13] [назад] Cummins and Minami, *The Book of Ninja*, 95.
[14] [назад] Cummins and Minami, *Secret Traditions*, 161.
[15] [назад] Cummins and Minami, *The Book of Ninja*, 95.
[16] [назад] Cummins and Minami, *Secret Traditions*, 160.
[17] [назад] Cummins and Minami, *The Book of Ninja*, 95.
[18] [назад] Cummins and Minami, *Secret Traditions*, 160-161.
[19] [назад] Cummins and Minami, *Secret Traditions*, 161.
[20] [назад] Sqrrl Team, "A Framework for Cyber Threat Hunting Part 1: The Pyramid of Pain," *Threat Hunting Blog*, Sqrrl, July 23, 2015, https://www.threathunting.net/sqrrl-archive.
[21] [назад] Blake E. Strom, "Adversarial Tactics, Techniques & Common Knowledge," ATT&CK, The MITRE Corporation, September 2015, https://bit.ly/38oSrNJ.
[22] [назад] "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, FireEye, February 2013, https://bit.ly/2LbnPqg.
[23] [назад] "The Cyber Kill Chain," Lockheed Martin, дата последнего обращения 7 февраля 2020 года, https://bit.ly/2XjYrRN.
[24] [назад] Cris Carreon, "Applying Threat Intelligence to the Diamond Model of Intrusion Analysis," *Recorded Future Blog*, July 25, 2018, https://bit.ly/39kPe1c.
[25] [назад] "Structured Threat Information eXpression (STIX) 1.x Archive Website," STIX, The MITRE Corporation, дата последнего обращения 7 февраля 2020 года, https://stixproject.github.io.
[26] [назад] David Bianco, "The Pyramid of Pain," *Enterprise Detection & Response*, последнее обновление 17 января 2014 года, https://bit.ly/3s31prV.
[27] [назад] "Adversarial Tactics, Techniques, & Common Knowledge Mobile Profile," ATT&CK, The MITRE Corporation, последнее изменение 2 мая 2018 года, https://attack.mitre.org.