Эта книга посвящена сообществу профессионалов, работающих в области информационной безопасности, которые внедряют нововведения, занимаются созданием и информированием с помощью блогов, программного обеспечения с открытым исходным кодом и социальных сетей. Методы, описанные в этой книге, стали возможны только благодаря вашим неустанным усилиям

Содержание

Предисловие

Реагирование на инциденты информационной безопасности требует практических знаний в различных областях. Хороший специалист, имеющий дело с такими инцидентами, должен разбираться в анализе журналов и энергозависимых данных из дампа памяти, извлечении информации, необходимой для компьютерной криминалистики, из образа жесткого диска, анализе вредоносных программ, мониторинге безопасности сети, написании программных сценариев и уметь работать с командной строкой. Это удивительно сложная задача, требующая постоянного обучения в различных дисциплинах. Тут и приходит на помощь данная книга. На ее страницах (или в цифровом файле) вы найдете сведения по каждой из этих специализированных областей. Независимо от того, являетесь ли вы IT-специалистом, стремящимся расширить свое понимание реагирования на инциденты ИБ, студентом, познающим азы, или опытным ветераном кибертраншей, находящимся в поисках краткого справочного руководства, данная книга поможет вам.

Это издание не сосредоточено на теории высокого уровня, подходах к управлению или вызовах глобальной политики. Оно написано практиками и для практиков, которым необходимо ежедневно выявлять действия злоумышленников в своих сетях, сдерживать их и реагировать на них. Опираясь на опыт проведения расследований вторжений для Федерального бюро расследований (ФБР) и Министерства обороны США, консультирования глобальных клиентов, разработки средств для цифровой криминалистики и киберрасследований для десятков национальных полицейских сил и работы со студентами на сотнях курсов, проводимых для Государственного департамента США, Академии ФБР и SANS, я попытался предложить по возможности наиболее эффективные и действенные методы для борьбы с современными киберпреступниками. Я также искал мнения, рекомендации, обзоры и сведения от множества экспертов (которые намного умнее меня) по различным областям, представленным в этой книге, чтобы гарантировать, что в ней точно представлены наиболее актуальные и релевантные методы. Конечный результат может носить имя одного автора, но в действительности это коллективный труд. В результате я буду использовать местоимение множественного числа «мы», обращаясь от первого лица и имея в виду многих специалистов-практиков и редакторов, которые помогли осуществить эту работу.

Во многом эта книга является продолжением книги *Mastering Windows Network Forensics and Investigation*, 2-е изд. (Sybex, 2012). Хотя в ней по-прежнему содержится много полезных приемов, позволяющих справляться с инцидентами уже на протяжении более десяти лет с момента выхода первого издания, с тех пор многое изменилось. Злоумышленники стали более продвинутыми; атаки происходят в более быстром темпе; тактика, методы и процедуры, используемые организованными преступниками и злоумышленниками, на уровне государства слились; а код из каждой кампании атаки регулярно используется другими хакерами. Дни, когда вы извлекали огромное количество

жестких дисков для статического создания образов и проведения полного криминалистического анализа, уступили место целевым криминалистическим экспертизам, поиску в оперативной памяти среди тысяч систем на предмет наличия вредоносных программ, опросу системы с помощью программных сценариев для выявления признаков компрометации и использованию методов визуализации данных для обнаружения дальнейшего распространения по сети. Современные киберугрозы требуют другого, более динамичного подхода, и это именно то, что вы и найдете здесь: эффективные методы реагирования на инциденты ИБ, которые можно незамедлительно применять в своем окружении.

О чем пойдет речь в этой книге

В этой книге реагирование на инцидент ИБ рассматривается как цикл, а не как отдельный процесс. Хотя мы изучим несколько различных моделей реагирования на инциденты, для достижения киберустойчивости обработка инцидентов должна быть включена в общий цикл предотвращения, обнаружения и реагирования. Сети больше не могут полагаться исключительно на превентивные меры безопасности, рассматривая обработку инцидентов как изолированные и осторожные действия. Вместо этого реагирование на инциденты должно быть неотъемлемой частью активных оборонительных операций, предоставляя разведданные и информацию специалистам по защите сетей, чтобы не только реагировать на текущие киберугрозы, но и помогать сглаживать результаты атак в будущем. Мы охватим целый ряд технических навыков, необходимых для достижения этой цели, в этих главах:

- Часть I «Подготовка»
  - Глава 1 «Картина угроз». За последнее десятилетие агрессивные кибероперации стали ведущим источником доходов для организованной преступности, ключевым методом шпионажа между государствами и новым оружием в войне. Понимание современных злоумышленников и векторов их атак является ключевым шагом для эффективной защиты сети.
  - Глава 2 «Готовность к инцидентам». Если вы не готовы к битве, война закончится еще до того, как начнется. Эта глава предоставляет вам инструменты, необходимые для подготовки вашей сети, команды и процесса к эффективному реагированию на инциденты.
- Часть II «Реагирование»
  - Глава 3 «Удаленная сортировка». Инциденты могут быстро перерасти из одиночного плацдарма в полную власть над доменом. Чтобы правильно оценить инцидент и отреагировать на него, вам необходима способность сортировать системы, оценивать влияние инцидента и выявлять уязвимые системы по всему предприятию. Эта глава вооружит вас знаниями, необходимыми для поиска вредоносной активности в вашем окружении.
  - Глава 4 «Инструменты удаленной сортировки». Основываясь на знаниях, полученных в главе 3, эта глава предоставляет вам конкретные

методы и инструменты для опроса систем по всей сети, выявления тех, которые могут быть скомпрометированы, и инициирования действий по локализации и смягчению.

- Глава 5 «Создание дампа памяти». Как только система будет идентифицирована как потенциально скомпрометированная, следующим логическим шагом для специалиста, имеющего дело с инцидентами ИБ, является работа с содержимым энергозависимой памяти из системы. В этой главе рассматриваются различные методы и инструменты для снятия дампа памяти из локальных или удаленных систем с помощью средств компьютерной криминалистики.
- Глава 6 «Создание образа диска». Помимо энергозависимых данных, вам может потребоваться иметь дело с энергонезависимыми запоминающими устройствами, такими как жесткие и твердотельные диски, для сохранения улик и облегчения анализа скомпрометированной системы. В этой главе представлены инструменты и методы для получения побитовой копии исходного устройства (forensic image) из локальных и удаленных систем.
- Глава 7 «Мониторинг сетевой безопасности». Мониторинг и анализ сетевых коммуникаций обеспечивают критическую видимость и дают информацию специалистам, реагирующим на инциденты ИБ. В этой главе рассматривается телеметрия, собранная из сети, что может помочь в процессе реагирования на инциденты, и способы объединения этой информации с данными конечной точки для получения более полной картины сетевой активности.
- Глава 8 «Анализ журнала событий». Журналы событий Windows записывают подробные сведения о деятельности системы в среде Windows. Агрегируя и анализируя эти журналы, специалисты могут восстановить активность злоумышленника. Эта глава обучает вас навыкам, необходимым для понимания и интерпретации этих жизненно важных улик.
- Глава 9 «Анализ памяти». Современные злоумышленники все чаще избегают вносить изменения в диск в качестве механизма уклонения от обнаружения, превращая энергозависимую память в главное поле битвы. Анализируете ли вы ранее собранный дамп ОЗУ или энергозависимую память из работающей системы, возможность анализировать структуры данных в оперативной памяти, чтобы понять детали деятельности системы, является ключевым навыком любого специалиста, работающего с инцидентами.
- Глава 10 «Анализ вредоносных программ». Даже с ростом техник «кормление с земли» вредоносное ПО остается важным средством в инструментарии злоумышленника. Эта глава дает вам практические навыки, которые можно использовать для анализа подозрительной вредоносной программы, используя статический и динамический подходы.
- Глава 11 «Извлечение информации с образа жесткого диска». Анализ энергонезависимого хранилища из уязвимых систем может выявить индикаторы компрометации, раскрыть техники, тактики

и процедуры вашего противника и задокументировать последствия вторжения. В этой главе вы получите навыки, необходимые для проведения глубокого анализа уязвимой системы.

- Глава 12 «Анализ дальнейшего распространения по сети». Многие вторжения начинаются с атаки со стороны клиента, за которой следует дальнейшее распространение по сети. Мы объединяем навыки, полученные в предыдущих главах, и применяем их для определения этого явления в вашем окружении. В данной главе описываются методы, используемые злоумышленниками для распространения по сети, и действия, которые вы можете предпринять, будучи специалистом по работе с инцидентами ИБ, для противодействия им.

- Часть III «Улучшение»
  - Глава 13 «Непрерывное улучшение». После того как вы эффективно разобрались с предполагаемым инцидентом, нужно поработать с информацией, полученной в ходе реагирования на инцидент. Понимание средств управления, телеметрии, процедур и обучения, которые могут сгладить последствия будущих инцидентов, помогает подготовить ваше окружение к следующей атаке.
  - Глава 14 «Активные действия». Подход к инцидентам не должен быть чисто реактивным. Специалисты должны активно участвовать в поиске киберугроз, тренингах для фиолетовых команд и эмуляции действий злоумышленника с целью выявления потенциальных противников, слепых зон и пробелов в силах и средствах защиты. В этой главе обсуждаются способы, как сделать так, чтобы ваша команда постоянно старалась перехитрить противника.

Как использовать эту книгу

Лучший способ получить отдачу от этой книги зависит от вашего текущего уровня квалификации. Мы предполагаем, что у вас есть базовые знания в области сетевых технологий, поэтому если вы еще незнакомы с основными концепциями работы в сети, такими как порты, протоколы и IP-адреса, возможно, это не самое подходящее место, чтобы начать свое путешествие в мир реагирования на инциденты.

Если вы студент и хотите использовать базовые знания в области IT и приступить к следующему этапу своего путешествия в области информационной безопасности, тогда добро пожаловать! Работа с каждым разделом в рамках курса или самостоятельно предоставит вам подробный обзор области и даст возможность определить аспекты реагирования на инциденты, которые наиболее привлекательны для дальнейшего изучения.

IT-администраторы, стремящиеся лучше защитить свои сети, также являются частью целевой аудитории. Требования по защите сетей сместились с чисто превентивных подходов на сочетание предотвращения, обнаружения и реагирования. Современные противники преданы своему делу и довольно способны. При достаточных усилиях они могут взломать любую сеть. Адми-

нистраторы должны знать, как распознать, сдерживать инциденты, которые могут произойти в их окружении, и реагировать на них.

Изучение основных навыков реагирования на инциденты поможет IT-специалистам лучше защитить свои сети для обеспечения безопасности операций. Просмотрите всю книгу и сосредоточьтесь на областях, представляющих наибольший интерес для вас, зная, что вы всегда можете обратиться к оставшейся части книги для более глубокого их понимания, когда в этом возникнет необходимость.

Если вы уже являетесь профессионалом в области реагирования на инциденты ИБ, то знаете, как непросто стараться отслеживать различные навыки, необходимые для выполнения вашей работы. Мы предлагаем вам возможность ознакомиться с новейшими методиками, отточить свои навыки в областях, где вам, возможно, не очень комфортно, и предоставить ценную справочную информацию для быстрого поиска кода события, ключа реестра, командлета PowerShell или других технических деталей, необходимых для решения вашей текущей проблемы. Вы, вероятно, найдете несколько полезных советов и приемов, которые сделают вас более эффективным специалистом по работе с инцидентами.

Независимо от вашей отправной точки, вы найдете дополнительные ссылки по адресу www.AppliedIncidentResponse.com. Это официальный сайт книги. Мы продолжим пополнять сайт новыми методами и обновлениями, связанными с темами, которые здесь рассматриваются, чтобы обеспечить вам доступ к текущей информации.

В этой книге мы используем несколько различных форматов:

- команды написаны моноширинным шрифтом;
- команды, которые должны быть набраны пользователем (в отличие от приглашения командной строки или вывода), выделены **жирным шрифтом**;
- такие вещи, как, например, IP-адреса, выделены *курсивом* или <моноширинным шрифтом в угловых скобках>;
- если команда слишком длинная, чтобы уместиться на одной строке в печатном издании, мы будем использовать знак ↵, дабы указать на продолжение строки.

Создание тестовой лаборатории

Одним из лучших способов изучения любого предмета, связанного с IT, является создание тестовой среды и практика. Реагирование на инциденты не исключение. В ходе нашей работы мы предоставим вам широкий спектр команд, инструментов и методик. Наличие тестовой лаборатории, в которой вы сможете проводить практические эксперименты, неоценимо для применения этих навыков в вашей производственной среде. Чтобы было проще, мы дадим несколько советов (и скрипт), которые помогут вам быстро запустить тестовый домен.

Сначала вам нужно будет выбрать платформу виртуализации. VMWare – это популярный и надежный выбор. Если вам нужно запустить тестовую

среду поверх существующей хостовой операционной системы, то можно рассмотреть в качестве варианта бесплатный программный продукт VMWare Workstation Player (www.vmware.com/products/workstation-player.html). Если вы можете сэкономить отдельный раздел или отдельную систему без железа, то VMWare ESXi (www.vmware.com/products/esxi-and-esx.html) предоставляет бесплатную платформу и преимущество работы с продуктом, который реализован во многих производственных средах. Конечно, если вы предпочитаете HyperV или другие (возможно, с открытым исходным кодом) продукты для виртуализации, они также будут отлично работать.

Следующий шаг – определение операционных систем, которые вы хотели бы включить в свою тестовую среду. Компания Microsoft предлагает бесплатные пробные лицензии для многих своих продуктов с пользовательским соглашением, которое позволяет проводить оценку для тестирования. Для серверных продуктов вы можете найти лицензии и файлы для скачивания по адресу www.microsoft.com/en-us/evalcenter/evaluate-windows-server, а для клиентских систем файлы для скачивания доступны на странице https://developer.microsoft.com/en-us/microsoft-edge/tools/vms. Вы также можете найти в свободном доступе широкий спектр дистрибутивов ОС Linux/UNIX (которые в этой книге мы называем «*nix»). Многие из них, такие как Security Onion, SANS Investigative Forensics Toolkit (SIFT) и Paladin от компании Sumuri, ориентированы на обеспечение возможностей безопасности и криминалистики, которые конкурируют с коммерческими продуктами или превосходят их. Мы рассмотрим каждый из них в последующих главах.

После получения программного обеспечения для виртуализации и тестирования операционных систем вам потребуется настроить их в подходящий тестовый домен. Мы предоставляем программный сценарий PowerShell на сайте www.AppliedIncidentResponse.com, чтобы помочь вам создать то же окружение, которое мы используем в этой книге, наряду с учетными записями пользователей и групп.

Об авторе

Стив Энсон – бывший федеральный агент США, имеющий опыт работы со всеми видами дел, связанных с киберпреступностью, в целевой группе ФБР по борьбе с киберпреступлениями и Службе уголовных расследований Министерства обороны США. Стив преподавал расследование компьютерных вторжений в Академии ФБР и сотрудничает с национальными полицейскими агентствами по всему миру по контракту в Программе помощи по борьбе с терроризмом Государственного департамента США, где он помогает в разработке устойчивых организационных ресурсов в области цифровой криминалистики и киберрасследований. Являясь соучредителем ведущей компаний по информационной безопасности Forward Defense (www.forward-defense.com), он предоставляет консалтинговые услуги в области безопасности клиентам из государственного и частного секторов по всему миру. Стив – сертифицированный инструктор Института SANS и ведет курсы по безопасности и защите сетевых окружений.

О тех, кто участвовал в написании этой книги

Несколько человек занимались рецензированием и давали советы, чтобы эта книга вышла в свет. Во главе этого списка стоит технический редактор Мик Дуглас. Мик – основатель Infosec Innovations и сертифицированный инструктор SANS, который щедро предоставил подробное техническое редактирование для каждой страницы. Он провел бесчисленные часы, работая с автором, чтобы уточнить техническую информацию, представленную в этой книге, обеспечить ее точность и предложить темы, которые можно будет включить в окончательный вариант. Вклад Мика чувствуется в каждой главе, поскольку он предложил инструменты и методы для улучшения информации, предоставляемой на каждом этапе.

Мэри Эллен Шуц, Джефф Паркер и остальная часть команды редакторов Wiley проделали большую работу, чтобы обеспечить соответствие конечного продукта высоким стандартам, установленным издательством. Николь Цёллер также предоставила свои навыки управления качеством для проекта, просматривая каждую главу, прежде чем книга пошла в печать. Помимо основной команды, отдельные главы просмотрели ведущие специалисты в различных областях, о которых идет речь в книге. Эти эксперты нашли время, чтобы предложить изменения в главах, дабы книга содержала самые актуальные и нужные темы.

Глава 2 была просмотрена Майклом Мурром, опытным специалистом в области реагирования на инциденты ИБ, исследователем и разработчиком. Будучи соавтором курса *SEC504: Hacker Techniques, Exploits, and Incident Handling*, в этой главе Майк дал ценную информацию о подготовке к инцидентам.

Алиса Торрес, ведущий автор курса *FOR526: Memory Forensics In-Depth*, и Анураг Ханна (@khannaanurag) предложили темы и советы, которые мы включили в главы 5 и 9.

Глава 7 о мониторинге сетевой безопасности была рассмотрена и улучшена Джоном Хаббардом. Джон – бывший руководитель SOC для GlaxoSmithKline, имеющий многолетний опыт защиты сетей от продвинутых злоумышленников. Он является автором курсов *SEC450: Blue Team Fundamentals* и *SEC455: SIEM Design and Implementation*.

Главе 11, посвященной извлечению информации с образа жесткого диска, очень помогли обзор и предложения Эрика Циммермана. Эрик – бывший специальный агент ФБР, который сейчас работает старшим директором по кибербезопасности и практике расследований компании Kroll. Эрик ведет несколько курсов по криминалистике в SANS в качестве сертифицированного инструктора и является соавтором курса *FOR498: Battlefield Forensics & Data Acquisition*.

Глава 12, посвященная техникам дальнейшего распространения по сети, была просмотрена Тимом Мединым, основателем компании Red Siege (www.redsiege.com), человеком, который открыл Kerberoasting, и ведущим автором курса *SEC560: Network Penetration Testing and Ethical Hacking*. Благодаря обширному опыту Тима в наступательной кибербезопасности методы вторжения, с которыми вам придется иметь дело на практике, скорее всего, отражены в этой книге.

Рецензент главы 13 – Эрик Ван Буггенхут, ведущий автор курса *SEC599: Defeating Advanced Adversaries*. Эрик также предложил включить в книгу много других тем по предотвращению и обнаружению злонамеренной активности и победе над киберпреступниками.

Каждый из этих людей внес существенные улучшения в книгу и, используя свои индивидуальные знания, сделал так, чтобы получившееся в итоге издание содержало самые ценные темы и технические подробности. Мы надеемся, что это поможет вам улучшить оборонительную позицию вашей сети сейчас и в будущем.

Наконец, автор хотел бы поблагодарить своих родителей за предоставленные возможности и помощь.

От издательства

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Скачивание исходного кода примеров

Скачать файлы с дополнительной информацией для книг издательства «ДМК Пресс» можно на сайте www.dmkpress.com или www.дмк.рф на странице с описанием соответствующей книги.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Wiley очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Часть I

ПОДГОТОВКА

Глава 1

Картина угроз

Прежде чем мы подробно рассмотрим детали реагирования на инциденты ИБ, стоит понять мотивы и методы, которыми руководствуются различные злоумышленники. Прошли те времена, когда компании могли надеяться, что они остаются незамеченными в интернете, полагая, что имеющиеся в их распоряжении данные не стоят того времени и ресурсов, которыми киберпреступник готов пожертвовать. К сожалению, реальность такова, что все компании подвергаются большому количеству организованных широкомасштабных атак. Организованные преступные группировки стремятся заработать с помощью мошенничества, шантажа, вымогательства и прочих незаконных методов. Таким образом, любая система может стать подходящей целью. Понимание мотивов и методов злоумышленников помогает специалистам по обеспечению сетевой безопасности подготовиться к неизбежным атакам и отреагировать на них.

Мотивы злоумышленника

Существует множество факторов, которые могут побудить злоумышленника к активным действиям, и, будучи специалистом, реагирующим на инцидент ИБ, вы часто не будете знать, что именно его спровоцировало, а возможно, вам так и не удастся определить истинную причину атаки. Определение повода для атаки – в лучшем случае процесс непростой, и зачастую он и вовсе не приносит результата. Хотя кибербразведка и дает важные подсказки, тщательно изучая тактики, методы, процедуры и инструменты, используемые различными группами злоумышленников, сам факт существования этих фрагментов создает реальную возможность использования злоумышленниками флагов, мер противодействия кибербразведке и дезинформации с целью скрыть свое происхождение и направить вас по ложному пути. Приписать каждую атаку определенной группе, может быть, и не удастся, но понимание общих мотивов злоумышленников может помочь тем, кто реагирует на инциденты ИБ, предсказать поведение атакующих и осуществить контрнаступление, что позволит более успешно противостоять атаке.

В целом наиболее распространенными целями взломов являются разведка (шпионаж), финансовые махинации или нарушение работы системы. Злоумышленники пытаются получить доступ к информации, чтобы извлечь

финансовую или иную выгоду, или же стремятся нанести ущерб информационным системам и лицам или объектам, которые их используют. Мы рассмотрим различные мотивы, побуждающие к совершению кибератак, чтобы лучше понять образ мыслей ваших потенциальных противников.

Кража интеллектуальной собственности

Большинство компаний используют некую информацию, чтобы отличаться от своих конкурентов. Ноу-хау используются самые разные: это могут быть секретные рецепты, запатентованные технологии или любые другие знания, которые дают преимущество данной компании. Когда информация имеет ценность, она является отличной мишенью для кибератак. Самоцелью может быть кража интеллектуальной собственности, если злоумышленник в лице отдельного государства или конкурента из отрасли может напрямую применить эти знания в своих интересах. В качестве альтернативы злоумышленник может продать эту информацию или вымогать деньги у жертвы в обмен на нераспространение секретных сведений, как только они окажутся в его распоряжении.

Атака на цепочку поставок

Большинство организаций используют партнерскую сеть, включая поставщиков и клиентов, для достижения своих конечных целей. При таком большом количестве взаимосвязей злоумышленникам зачастую легче выбрать своей мишенью средние звенья цепи поставок, вместо того чтобы совершать атаки непосредственно на целевые системы. Например, атака на компанию, производящую программное обеспечение, и встраивание вредоносного кода в продукты, которые затем будут использоваться другими компаниями, обеспечивают эффективный механизм внедрения программного обеспечения злоумышленника таким образом, как будто оно идет из надежного источника. Атака с использованием вредоносной программы NotPetya скомпрометировала компанию-разработчика бухгалтерского ПО. В ходе этой атаки была использована функция обновления программного обеспечения, позволившая перенести вредоносное ПО для уничтожения данных в системы клиентов. Как сообщается, сумма нанесенного ущерба составила более 10 млрд долларов. Еще один способ атаковать промежуточные звенья – нападение на технологические системы производственных предприятий, что может привести к созданию деталей, которые не соответствуют техническим требованиям. Если такие изделия затем поступают в военную отрасль или другие важные отрасли промышленности, это может привести к катастрофическим сбоям.

Финансовые махинации

Финансовые махинации, один из самых первых мотивов организованных кибератак, сегодня по-прежнему остаются движущим фактором для зло-

умышленников. Существует множество различных подходов для достижения прямой финансовой выгоды. Кража информации о кредитных картах, фишинг учетных данных онлайн-банкинга и компрометация банковских систем, в том числе банкоматов, – эти и другие методы продолжают успешно использоваться для пополнения карманов злоумышленников. Несмотря на то что осведомленность пользователей и повышенная оперативность банков усложнили осуществление этого типа атак по сравнению с предыдущими годами, финансовые махинации нередки и сегодня.

Вымогательство

Мы кратко упомянули вымогательство в связи с кражей интеллектуальной собственности, но оно применяется гораздо шире. Любая информация, которая может навредить потенциальной жертве или опорочить ее, является приманкой для вымогателей. Распространенные примеры – использование изображений личного или интимного характера, которые добываются с помощью троянов удаленного доступа или общения по сети, с целью выманивания денег у жертв (подобные схемы часто именуют «секс-шантажом»).

Кроме того, повреждение или угроза повреждения информационных систем могут быть использованы для вымогательства денег у жертв, как это делается при атаках с целью выкупа и распределенных атаках типа DDoS («отказ в обслуживании») на онлайн-компании. Столкнувшись с катастрофическими финансовыми потерями, связанными с потерей доступа к критически важной для бизнеса информации, многие жертвы предпочитают заплатить злоумышленникам, чтобы не страдать от последствий атаки.

Шпионаж

Шпионаж становится все более распространенной причиной для кибератак, будь то интересы отдельного государства или компании. Целевой информацией может быть интеллектуальная собственность, как уже обсуждалось ранее, или же сведения более широкого плана, которые могут предоставить злоумышленнику конкурентное или стратегическое преимущество. Отдельные государства регулярно участвуют в кибершпионаже друг против друга, поддерживая целевые профили критически важных систем по всему миру, которые могут быть использованы для получения информации или подвергнуться атаке, вызывающей сбой в их работе. Компании с поддержкой государства или без нее продолжают использовать киберэксплуатацию в качестве механизма получения сведений, связанных с запатентованными технологиями, методами производства, клиентами, или иной информации, которая позволяет им более эффективно конкурировать на рынке. Существуют и инсайдерские угрозы: например, недовольные сотрудники часто крадут внутреннюю информацию с целью продажи ее конкурентам или используют ее, чтобы получить преимущество при поиске новой работы.

Власть

По мере того как милитаристская сфера все больше переходит в киберпространство, способность использовать кибервласть в условиях войны или военной угрозы становится важной государственной стратегией. Способность нарушать обмен данными и наносить вред другой критически важной инфраструктуре с помощью сетевых атак, а не длительных бомбардировок или других военных действий, дает неоспоримые преимущества: большую эффективность и снижение побочного ущерба. Кроме того, угроза нанесения катастрофического ущерба критически важной инфраструктуре, такой как электрические сети, может привести к беспорядкам среди гражданского населения и подорвать экономику страны, а потому рассматривается как фактор, сдерживающий явные военные действия. По мере того как все больше стран создают военные киберподразделения, риск таких атак становится все более очевидным. Эстония, Украина и другие страны могут засвидетельствовать, что эти типы атак существуют не только в теории и могут быть очень разрушительными.

Хактивизм

Многие группы рассматривают атаки на информационные системы как законное средство протеста, сродни маршам или сидячим забастовкам. Подделка веб-сайтов для выражения своих политических взглядов, DDoS-атаки с целью вывести компании из строя и кибератаки, предназначенные для поиска и публикации информации, порочащей противников, – все это методы, используемые отдельными лицами или группами лиц, стремящимися привлечь внимание к конкретным проблемам. Как бы мы ни относились к праву использовать кибератаки как средство протеста, влияние этих типов атак неоспоримо и по-прежнему остается угрозой, от которой компании должны защищаться.

Жажда мести

Иногда мотивы злоумышленника ограничиваются желанием причинить вред отдельному человеку или компании. Недовольные или бывшие сотрудники, рассерженные клиенты, граждане других стран или бывшие знакомые по каким-то причинам могут затаить злобу и искать возмездия посредством кибератак. Во многих случаях злоумышленник знает, как работают процессы или системы, используемые компанией-жертвой. Это повышает эффективность атаки. Информация с открытым исходным кодом часто доступна через социальные сети или другие источники, где злоумышленник выразил свое недовольство компанией до или после атаки. Некоторые злоумышленники публично берут на себя ответственность, чтобы жертва знала причину и источник нападения.