Содержание

Предисловие

Реагирование на инциденты ИБ 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 то 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 войны. 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 для эффективного реагирования 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 информация 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 для 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». Реагирование на инциденты не должно быть чисто реактивным. Ваша команда должна активно участвовать в поиске киберугроз, упражнениях для фиолетовых команд и эмуляции действий злоумышленника для 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 вам 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. Ад-

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

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 будете готовы.

Если вы уже являетесь профессионалом в области реагирования на инциденты ИБ, то вы 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.

Следующим шагом является 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 были просмотрены ведущими специалистами по различным областям, о которых идет речь в этой 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 от 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». Обширный опыт Тима в наступательной кибербезопасности помог сделать так, чтобы обсуждаемые здесь методы были теми, которые вы, скорее всего, увидите в случае вторжения в ваше окружение.

Рецензент главы 13 – Эрик Ван Буггенхут, ведущий автор курса «SEC599: Defeating Advanced Adversaries». Эрик также предложил много других тем по предотвращению и обнаружению злонамеренной активности и победе над киберпреступниками, которые освещаются в данной книге.

Каждый из этих людей внес существенные улучшения в эту книгу и, используя свои индивидуальные знания, сделал так, чтобы получившееся в итоге издание предоставило вам 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.

Методы атаки

Киберзлоумышленники используют множество методов. Здесь мы рассмотрим некоторые общие категории, а в следующих главах обсудим конкретные техники. Многие из рассматриваемых ниже категорий пересекаются, но базовое представление об этих методах поможет специалистам, реагирующим на инциденты ИБ, распознавать атаки и сдерживать их.

DoS и DDoS

Атаки типа «отказ в обслуживании» (DoS) стремятся сделать службу недоступной по назначению. Эти атаки могут происходить в результате сбоя или отключения службы, или по причине исчерпания ресурсов, необходимых для функционирования службы. Примеры DoS-атак – злонамеренные пакеты, которые вызывают сбой службы, или ситуация, когда злоумышленник заполняет системный диск данными до тех пор, пока в системе не останется места для работы.

Один из ресурсов, на которые чаще всего посягают злоумышленники, – пропускная способность сети. С помощью объемных сетевых атак (network floods) большие объемы данных отправляются на один хост или службу с целью превышения доступной пропускной способности этой службы. Если вся пропускная способность занята бессмысленным трафиком, легитимный трафик не может добраться до службы, и та не может отправлять ответы законным клиентам.

Чтобы обеспечить максимальное снижение пропускной способности, эти типы атак обычно распространяются на несколько систем; при этом атака идет на одну цель, поэтому они и называются атаками с распределенным отказом в обслуживании (DDoS). Примером такой атаки является DDoS-атака с использованием memcached на GitHub, где применялись публично доступные серверы memcached. Memcached предназначен для того, чтобы позволить другим серверам, например тем, которые генерируют динамические веб-страницы, хранить данные на сервере memcached и иметь возможность быстрого доступа к ним. При публичном доступе по протоколу UDP служба позволяет злоумышленнику хранить большой объем данных на сервере memcached и подделывать запросы на эти данные, как если бы они поступали от предполагаемой жертвы. В результате сервер memcached отвечает на каждый поддельный запрос, отправляя большой объем данных жертве, даже если злоумышленнику необходимо отправить только небольшой объем данных для генерации поддельного запроса. Эта концепция усиления пропускной способности, когда злоумышленник посылает (обычно короткий) запрос уязвимому DNS-серверу, который отвечает на запрос уже значительно большим по размеру пакетом, называется *атакой с усилением*. Коэффициент усиления для memcached был особенно высоким, что привело к наибольшим на сегодняшний день объемам DDoS-атак. К счастью, поскольку по умолчанию ответы memcached исходят от UDP-порта 11211, фильтрация вредоносного

трафика с помощью вышестоящего анти-DDoS-решения была упрощена. Неправильно настроенные серверы, которые позволили первоначальным атакам достичь такой высокой пропускной способности, также должным образом настроены, чтобы запретить UDP и/или быть защищенными брандмауэрами от доступа в интернет.

DDoS-атаки основаны на том, что они могут отправлять больше данных, чем способен поддерживать канал интернет-провайдера (ISP) жертвы. В результате жертва мало что может сделать для сглаживания последствий таких атак в своей сети. Хотя вы можете настроить граничный маршрутизатор или межсетевой экран для блокировки входящих атак, соединение с интернет-провайдером компании будет по-прежнему перегружено, и легитимный трафик будет блокироваться. Сглаживание DDoS-атак обычно обеспечивается интернет-провайдерами или специализированным провайдером, предоставляющим защиту от DDoS-атак, который может выявлять и фильтровать вредоносный трафик в восходящем направлении или через облачную службу, где пропускная способность гораздо выше. В этой книге мы не будем подробно говорить о реагировании на инциденты, связанные с DDoS-атаками, так как большинство мер по сглаживанию рисков будут приниматься в восходящем направлении. Поскольку «бутеры» или «стрессоры» чаще рекламируются в обычном доступе, а также в даркнете за символическую плату, во всех компаниях, которые полагаются на интернет в своих бизнес-операциях, должны быть определены партнеры по борьбе с DDoS и приняты контрмеры.

Черви

Черви представляют собой общий класс вредоносных программ, характеризующийся тем, что они самовоспроизводятся. Среди давних примеров – LoveBug, Code Red и SQL Slammer, которые нанесли огромный ущерб системам по всему миру в начале 2000-х годов. Обычно черви нацелены на определенную уязвимость (или уязвимости). Они сканируют системы, которые подвержены этой уязвимости, эксплуатируют уязвимую систему, копируют в нее свой код и начинают сканирование заново для обнаружения других жертв. Благодаря своей автоматической природе черви могут распространяться по земному шару за считанные минуты. Программа-вымогатель WannaCry – еще один пример червя, который использовал эксплойт EternalBlue для операционных систем Windows для распространения и доставки своего вредоносного кода. Согласно сообщениям, он заразил более 250 000 систем в 115 странах, нанеся ущерб в миллиарды долларов.

Обнаружить червя вообще-то не сложно. Масштабная атака вызовет всеобщую панику в сфере IT, что приведет к всплеску активности компьютерных групп реагирования на чрезвычайные ситуации (CERT), а исследователи будут регулярно сообщать сообществу профессионалов в области информационной безопасности о характере атаки. С точки зрения реагирования на инциденты ИБ задача состоит в том, чтобы должным образом изолировать затронутые системы, определить механизм, с помощью кото-

рого червь распространяется, и предотвратить заражение других систем за очень короткое время.

Программы-вымогатели

Программы-вымогатели относятся к категории вредоносных программ, которые пытаются зашифровать данные жертвы с помощью ключа, известного только злоумышленникам. Чтобы получить ключ, необходимый для расшифровки и, следовательно, восстановления затронутых данных, жертвам предлагается заплатить авторам программы-вымогателя. Обещается, что после этого жертва получит свой уникальный ключ и сможет расшифровать и восстановить все затронутые данные. Чтобы облегчить процесс оплаты максимально возможному числу жертв, некоторые злоумышленники даже предоставляют службы поддержки тем, у кого возникают проблемы с оплатой (обычно криптовалютой) или расшифровкой файлов после предоставления ключа.

Конечно, нет никакой гарантии, что после того как будет проведен платеж в криптовалюте, который не подлежит отмене, вы получите ключ. По этой причине, а также для предотвращения подобных атак в целом специалисты в области IT-безопасности обычно советуют не платить мошенникам. Тем не менее многие компании, которые недостаточно подготовлены и не имеют подходящих планов аварийного восстановления, считают, что у них нет иного выбора, кроме как заплатить, несмотря на отсутствие гарантий.

Программы-вымогатели стали значительной угрозой, по крайней мере с середины 2000-х годов. CryptoLocker появился в 2013 году, и с тех пор было разработано несколько вариантов этой программы. Червь WannaCry, о котором упоминалось выше, нанес значительный ущерб в 2017 году. С тех пор более целенаправленные атаки с использованием программ-вымогателей нанесли удар по городам, включая Атланту, Балтимор и 23 города в штате Техас. Все это этапы одной и той же кампании. В последние годы имели место подобные атаки на медицинские и корпоративные ресурсы. Программа-вымогатель GrandCrab предназначалась для различных организаций, включая компании, занимающиеся IT-поддержкой, чтобы использовать их инструменты удаленной поддержки для заражения бóльшего количества жертв. Целевые атаки – по-прежнему распространенная стратегия для групп злоумышленников, которыми движет жажда наживы. Они используют такие программы-вымогатели, как SamSam, Sodinokibi и другие. Компании меньшего размера, в которых, как считается, не так хорошо обеспечена непрерывность бизнеса и хуже проработаны планы аварийного восстановления, по-прежнему остаются мишенью вредителей. Банковское вредоносное ПО Emotet расширило свои атаки, чтобы внедрять модульный троян Trickbot, используя его для кражи конфиденциальных файлов и дальнейшего распространения по сети. Это позволило злоумышленникам понять целевое окружение, а затем загрузить программу-вымогатель Ryuk и требовать оплаты для восстановления доступа к критически важным данным. Пока програм-

мы-вымогатели приносят прибыль, они будут оставаться угрозой, к которой должны быть готовы все компании.

Фишинг

Фишинговые атаки существуют уже целую вечность, и сегодня они остаются одним из наиболее распространенных типов атак. Хотя качество фишинговых писем продолжает улучшаться, общая концепция по сравнению с предыдущими годами не изменилась. В сообщениях электронной почты, рассылаемых якобы от компаний, которым доверяет жертва, предлагается пройти по ссылке, загрузить вложение или предоставить учетные данные для аутентификации, чтобы решить некую проблему или откликнуться на запрос. Благодаря повышению осведомленности пользователей подобные рассылки чаще всего игнорируются, однако низкая стоимость, связанная с отправкой десятков тысяч электронных писем (обычно через скомпрометированные серверы или ботнеты), означает, что такая кампания может быть успешной даже при очень небольшой доле получателей, которые становятся жертвами.

Целевой фишинг

Целевой фишинг относится к целевым атакам, направленным против конкретных особо важных лиц. Злоумышленники будут следить за этими пользователями, чтобы понять, какие типы электронных писем они обычно получают. Узнав имена и адреса электронной почты сотрудников, их отношения с жертвой и типы документов, которые они отправляют на регулярной основе, злоумышленник может придумать правдоподобную приманку, чтобы заставить жертву предпринять действие, которое скомпрометирует ее системы. Атаки с использованием целевого фишинга могут включать в себя сложные кампании с привлечением методов социальной инженерии, где применяются электронная почта, социальные сети, SMS-сообщения и даже голосовые вызовы. Чем более правдоподобна эта кампания, тем больше вероятность того, что жертва предпримет желаемое действие, предоставив злоумышленнику точку опоры в целевой сети.

Разновидности включают в себя атаки на деловую электронную почту, когда злоумышленник получает несанкционированный доступ к системе электронной почты и использует его для отправки фишинговых электронных писем другим сотрудникам или партнерским организациям. Тот факт, что они отправляются из учетной записи реального пользователя, и тот факт, что злоумышленник имеет доступ к электронным письмам, которые можно использовать для создания более убедительной приманки, повышает эффективность атак. Они часто используются в мошеннических кампаниях по выставлению счетов, чтобы заставить организации совершать платежи на счет злоумышленника. Последние же в свою очередь полагают, что оплачивают счет от реального партнера.

Атака типа «водопой»

Часто совершаемая в сочетании с фишинг-атаками, эта атака направляет жертв на веб-сайт, который доставит вредоносный код всем, кто его посещает. Ythtlrj это достигается с помощью вредоносной рекламы, которая затем распространяется на безобидные веб-сайты, заражая уязвимых посетителей, которые заходят на сайт. Тщательно выбирая ресурс для размещения вредоносного ПО или ключевые слова, с которыми будет связано вредоносное объявление, злоумышленник может настраивать атаку на жертв из определенной компании, региона или группы. Фишинговые электронные письма или сообщения в социальных сетях, содержащие ссылку на зловредный сайт, также являются эффективным средством таргетирования атак. Еще одна распространенная тактика – компрометация безопасного веб-сайта, который могут посетить предполагаемые жертвы, и использование этого сайта для запуска новых атак, направленных на его пользователей. Группу хакеров APT38 обвинили в запуске нескольких успешных атак подобного рода, которые были ориентированы на сотрудников финансовых учреждений и ставили целью открыть доступ к их банковским сетям.

Успешные кампании с использованием такого рода атак могут привести к тому, что несколько сотрудников в рамках одной компании за короткое время заразят свои системы. Поэтому важно быстро выявить атаки, чтобы свести к минимуму ущерб, нанесенный злоумышленниками, и предотвратить последующее заражение других систем по сети.

Веб-атаки

Веб-атаки – это атаки на сервисы, которые используют протокол передачи гипертекста (HTTP). Хотя традиционно под этим подразумеваются веб-серверы, быстрое внедрение мобильных приложений и их зависимость от веб-технологий означает, что эти атаки применимы и к большому сегменту мобильной активности. Они могут принимать различные формы, включая прямую эксплуатацию серверов, межсайтовые скриптовые атаки на браузеры, межсайтовые подделки запросов и логические атаки на приложения. Таким атакам часто способствует прокси-сервер для манипулирования веб-приложением, который может перехватывать и изменять обмен данными между клиентом и сервером. Интерфейсы прикладного программирования (API) становятся все более распространенным средством обмена информацией между приложениями, и атаки на уязвимости в этих API – обычное явление.

Быстрые темпы развития и изменений в пространстве мобильных приложений привели к возрождению старых уязвимостей веб-приложений. Многие атаки, которые считались устаревшими, снова получили распространение, а веб-технологии для недорогих и быстро развивающихся мобильных приложений были переосмыслены.

Атаки на беспроводные сети

Поскольку мобильность становится все более важной частью нашей повседневной жизни, растет и наша зависимость от беспроводных технологий. Естественно, это расширяет охват атак на беспроводные сети с использованием таких технологий, как Wi-Fi, Bluetooth и даже GSM. Хотя WPA3 (Wi-Fi Protected Access, версия 3) обеспечит дополнительную защиту множества беспроводных сетей, на момент написания книги этот протокол внедряется крайне медленно, а уязвимости уже выявляются. Предыдущие протоколы, такие как WPA2, предлагают разумные уровни защиты при правильной реализации, но при неправильном развертывании могут быть скомпрометированы. Даже системы мобильной телефонной связи, такие как GSM, подвергаются атакам через протокол SS7, уязвимости сигнальных сетей, перехватчики международных идентификаторов мобильных абонентов (IMSI), а также атакам на SIM-карты и др.

Доступ к общедоступным сетям Wi-Fi все еще остается распространенным методом закрепления злоумышленников в системе клиента. Известно, что продвинутые злоумышленники, такие как организаторы кампании DarkHotel, нацелены на общедоступный Wi-Fi в отелях или других местах, к которому могут подключаться бизнес-пользователи или другие особо важные лица. Скомпрометировав точки доступа или разместившись между точкой доступа и подключением к интернету, злоумышленники могут изменять передаваемые данные, перенаправляя соединения или даже вставляя вредоносный код в доверенные потоки данных. Использование виртуальной частной сети (VPN) снижает риск, связанный с этим типом атак, и к VPN следует прибегать всякий раз, когда приходится подключаться к ненадежной сети; однако надо понимать, что ненадежная беспроводная сеть в любом случае повышает ваши риски.

Анализ сетевого трафика и атака посредника

Как и в случае с атаками на общедоступные точки беспроводного доступа, злоумышленники, которые могут вставить свою систему в поток обмена данными, могут перехватывать или изменять данные при передаче. Злоумышленник, закрепившийся в сети, может изменить таблицы кеша ARP для перенаправления трафика от предполагаемого получателя в систему злоумышленника. Затем он может просмотреть или изменить данные и переслать их предполагаемому получателю, поместив систему злоумышленника в положение «человек посередине» (MitM). После этого злоумышленник может оказывать постоянное влияние, будучи в сети, получать особо важную информацию, включая учетные данные, и внедрять вредоносный код, где это необходимо.

Криптомайнинг

Еще один вектор атаки – доставка программного обеспечения для майнинга криптовалюты, в результате чего вся заработанная криптовалюта будет по-

ступать на счета злоумышленника. Рост котировок криптовалюты в 2017 году в сочетании с относительно низкой прибылью от атак с использованием программ-вымогателей привел к резкому росту числа атак такого типа в 2018 году.

Популярность атак этого типа имеет тенденцию к росту или падению в зависимости от котировок криптовалют. Эти типы атак часто предпочитают криптовалюту Monero, поскольку алгоритмы, используемые для майнинга данного типа валюты, хорошо подходят для обычных компьютерных процессоров, а не для графических процессоров (GPU). Жертвы, как правило, испытывают увеличение загрузки процессора, и затраты на электроэнергию растут соответственно, но при этом другие негативные последствия минимальны, поскольку автор вредоносного ПО хочет избежать обнаружения. Многие ботнеты активируют функции криптомайнинга в качестве загружаемой функции в своих клиентах-ботнетах, что позволяет бесплатно сдавать в аренду систему для майнинга наряду с другими видами использования ботнетов, такими как DDoS-атаки.

Атаки с целью получения пароля

Несмотря на растущее применение многофакторной аутентификации, многие компании продолжают использовать аутентификацию по имени пользователя и паролю в качестве единственного средства подтверждения личности. Атаки с целью получения пароля предполагают угадывание паролей методом полного перебора (когда пробуется большое количество возможных паролей для учетной записи), распыления пароля (попытка испробовать небольшое количество паролей, но в отношении многих пользователей – чтобы уменьшить вероятность блокировки учетной записи), кражи паролей из скомпрометированных баз данных и взлома украденных паролей или паролей, перехваченных в ходе анализа трафика. Многие организации до сих пор хранят пароли в небезопасном виде (например, MD5 без использования соли) или, что еще хуже, в виде простого текста, поэтому, когда происходит компрометация и база данных попадает в руки злоумышленника, все пароли пользователей также подвергаются риску.

Несмотря на наличие менеджеров паролей и многофакторной аутентификации, слишком много пользователей по-прежнему используют один и тот же пароль на разных сайтах и в разных сервисах. Эта проблема приобрела такие масштабы, что Национальный институт стандартов и технологий США (NIST) изменил свои давние рекомендации, касающиеся использования паролей, и теперь рекомендует использовать парольные фразы, комбинацию случайных слов, чтобы фраза была как можно более длинной и злоумышленнику было бы сложнее ее угадать, но самому пользователю легко запомнить.

Правила усложнения паролей (в частности, требование использовать прописные и строчные буквы, цифры и специальные символы) не дали предполагаемого разнообразия. Пользователи склонялись к шаблонному варианту: использованию слов, встречающихся в словарях, с добавлением числа и/или специального символа в конце. Принудительная ротация паролей также не

смогла добавить необходимую энтропию в структуру паролей, поскольку пользователи просто увеличивали число в конце пароля или вносили другие тривиальные изменения, чтобы легче запомнить новый пароль.

Компаниям следует по возможности привести свои методы управления идентификацией в соответствие с обновленной специальной публикацией NIST 800-63B, доступной по адресу https://pages.nist.gov/800-63-3/sp800-63b.html, и требовать многофакторной аутентификации во всем сетевом окружении. Люди должны использовать инструменты управления паролями и удостовериться, что пароли уникальны и не используются повторно в службах.

Анатомия атаки

Хотя каждая кибератака может быть уникальной, полезно проанализировать некоторые общие шаги, предпринимаемые злоумышленниками. Как специалисты, реагирующие на инциденты ИБ, пользуются системным подходом, так и злоумышленники четко организуют свою деятельность, чтобы добиться эффективности и результативности. За эти годы были предложены различные модели описания методологии злоумышленника, включая Lockheed Martin Cyber Kill Chain, Unified Kill Chain, предложенную Полом Полсом, MITRE ATT&CK и др. Независимо от конкретной используемой модели атака обычно предусматривает перечисленные ниже этапы.

Разведка и сбор данных

Для целевой компании этот этап является наиболее важным. Целеустремленный злоумышленник потратит значительное количество времени на анализ данных с открытым исходным кодом, чтобы получить как можно больше информации о целевой компании и ее сотрудниках.

При атаках на стороне клиента, таких как фишинг или целевой фишинг, что касается наиболее распространенных векторов атак, то злоумышленник потратит значительную часть времени на то, чтобы провести разведку и создать правдоподобные и эффективные кампании с использованием методов социальной инженерии. Как правило, злоумышленники нацелены на организации, присутствующие в интернете, в том числе располагающие корпоративным сайтом и/или личными веб-сайтами сотрудников и учетными данными в социальных сетях, а также публикующие новостные сообщения о компании и ее сотрудниках. Все это обеспечивает эффективную атаку.

В дополнение к анализу данных с открытым исходным кодом злоумышленник, скорее всего, проведет сканирование IT-систем компании-жертвы. Средства защиты по периметру, очевидно, ограничат начальное сканирование подключенными к интернету устройствами, но целевое сканирование в сети может продолжиться после того, как злоумышленник закрепится в ней, в зависимости от того, насколько хорошо он скрывает свое присутствие. Сканирование может проводиться быстро, практически без учета об-

наружения, или же растягиваться во времени и идти из разных источников во избежание подозрений. Огромное количество автоматических сканеров, например от вредоносных программ, которые нацелены на узлы, подключенные к интернету, затрудняют эффективное обнаружение сканирования по периметру в интернете.

Целеустремленные злоумышленники будут пытаться определить средства защиты, установленные компанией-жертвой. Как только они поймут, что использует компания, они настроят свои методологии атак и вредоносный код так, чтобы избежать обнаружения этими конкретными технологиями. Обход обнаружения конечной точки – обычное дело, которое злоумышленник совершает с учетом установленных средств защиты. Хотя конечные точки и средства защиты сетей критически важны, не менее важно понимать, что ни одна система не является безупречной и что целеустремленный злоумышленник может создать атаку, способную уклониться от автоматических механизмов обнаружения. Глубокая защита и обнаружение имеют решающее значение в том, что касается минимизации воздействия таких целевых атак.

Эксплуатация

После того как злоумышленник определился с целевым окружением, его сотрудниками и средствами защиты, наступает время, чтобы закрепиться в сети жертвы.

Поскольку команды по обеспечению информационной безопасности становятся более эффективными, защищая устройства, подключенные к интернету, использование прямой эксплуатации уязвимостей в системах, подключенных к интернету, становится все более сложной задачей для злоумышленников. Часто проще и эффективнее запускать атаки на стороне клиента, вынуждая клиента посещать вредоносный сайт, открыть вредоносное вложение или поддаться на подобную уловку с использованием методов социальной инженерии. В качестве альтернативы злоумышленники могут попытаться эксплуатировать клиентские системы, когда те покидают пределы защиты сетевого периметра компании. Злоумышленники могут нацеливаться на общедоступный Wi-Fi, используемый сотрудниками компании, устройства, используемые как части программ «принеси свое устройство», либо плохо защищенные удаленные офисы или облачные службы, чтобы закрепиться, а затем уже расширить свое влияние.

Атаки на веб-приложения также могут использоваться как первооснова, когда речь идет о компании. В идеале веб-службы будут работать с ограниченными правами доступа, но компрометация таких серверов может обеспечить доступ к дополнительным конфиденциальным данным или внутренним базам данных, которые можно использовать для дальнейшего проникновения в сеть. Использование открытой и закрытой облачной инфраструктуры означает, что IT-ресурсы целевых компаний часто распределяются между различными хранилищами, поэтому злоумышленники могут искать несколько точек входа, чтобы закрепиться в каждом соответствующем центре обработки данных или провайдере облачных услуг.

К сожалению, многие компании все еще борются с эффективным управлением обновлениями, в результате чего появляются интернет-системы с известными уязвимостями. Благодаря таким проблемам злоумышленнику легче закрепиться в сети, поскольку известные уязвимости часто имеют публично доступные эксплойты. Использование таких эксплойтов довольно легко раскрывается с помощью механизмов обнаружения на базе сигнатур, но если сканирование, проведенное злоумышленником, показало, что периметр компании полон хорошо известных, но не исправленных уязвимостей, злоумышленник может предположить, что команда, отвечающая за обеспечение информационной безопасности, плохо следит даже за очевидными атаками. Поэтому мы по-прежнему встречаем компании, где закрепиться так же просто, как внедрить распространенный вредоносный код в подключенную к интернету систему, которая не содержит исправлений.

Расширение/внедрение

Эта фаза процесса атаки стала активным полем битвы между злоумышленниками и теми, кто им противостоит. Эффективность хорошо продуманных атак на стороне клиента и широкий диапазон доступных векторов атак почти гарантировали, что целеустремленный злоумышленник может закрепиться в системе. В результате отделы информационной безопасности должны сосредоточиться не только на предотвращении первоначальной эксплуатации своих ресурсов, но и на признании того, что такая эксплуатация может иметь место, и на расширении возможностей обнаружения вредоносной активности, происходящей в их сетевом окружении. Злоумышленники, которые первоначально закрепились в сети, могут оказаться в системе, не представляющей особой ценности, с доступом только к учетным данным непривилегированных пользователей. Поэтому они будут стремиться расширить свое влияние при дальнейшем распространении по сети, переходя к дополнительным системам и пытаясь украсть данные привилегированных пользователей.

Каждый раз, когда злоумышленник использует вредоносное программное обеспечение или инструменты хакера, он рискует быть обнаруженным средствами защиты на базе хоста или средствами защиты сети. По этой причине злоумышленники часто «кормятся за счет земли», стремясь использовать только то программное обеспечение, которое уже присутствует в сети жертвы. Используя функции операционной системы, консольные команды и встроенные средства системного администрирования, злоумышленники будут стремиться применять действительные учетные данные для входа в другие системы в окружении и распространять свое влияние. Это может принимать форму подключений по протоколу Secure Shell (SSH), протоколу SMB, получения доступа к удаленным компьютерам по сети и запуска на них команд PowerShell (PowerShell Remoting), подключений по протоколу удаленного рабочего стола (RDP) или любых других механизмов, используемых пользователями и администраторами целевого окружения для повседневных задач. Цель злоумышленника – сделать так, чтобы его действия

не отличались от обычной активности, применяя инструменты и протоколы, уже используемые в окружении жертвы, для того чтобы злонамеренное поведение сливалось с обычной сетевой активностью.

К сожалению, период, в течение которого злоумышленники могут находиться в сети, не будучи обнаруженными (известный как *время задержки*), часто измеряется месяцами. Многим командам по обеспечению информационной безопасности в настоящее время не хватает инструментов и тренировок для обнаружения злоумышленника, который работает в их окружении: они часто полагаются на системы обнаружения на базе сигнатур и использование злоумышленником вредоносного ПО в качестве основного механизма обнаружения и оповещения. Такой подход не дает специалистам заметить осторожного злоумышленника. Поэтому данному этапу атаки будет уделено значительное внимание в разговоре о том, как реагировать на инциденты ИБ.

Утечка данных / ущерб

В какой-то момент злоумышленник удовлетворится уровнем доступа к компании-жертве и успешно реализует свой замысел, какими бы ни были намерения, побудившие его проникнуть в сеть. В случае APT-атаки цель может состоять в том, чтобы оставаться в среде как можно дольше, и утечка данных осуществляется мало-помалу, растягиваясь во времени, – возможно, с использованием скрытых каналов во избежание обнаружения. В других случаях злоумышленник достигает своей цели и одним махом извлекает огромное количество данных в течение уик-энда. Если целью злоумышленника было нанести ущерб системе, то однажды утром сотрудники компании могут прийти и обнаружить, что все их системы стерты, зашифрованы или недоступны.

Удаление следов

Большинство злоумышленников, как и большинство преступников, заботятся о том, чтобы их не поймали. Подобно тому как преступник стирает отпечатки пальцев с орудия убийства, взломщики компьютерных систем стремятся скрыть доказательства своей деятельности. Они могут заметать следы по ходу или, в случае быстрой атаки, сделать это в конце, непосредственно перед отключением. Если компания предприняла соответствующие шаги для построения безопасной и отказоустойчивой сети, злоумышленники не получат доступ ко всем системам, необходимым для удаления доказательств их деятельности. Часто они стирают записи журнала из скомпрометированных ими систем, пытаются удалить файлы истории, в которых может быть отражено их присутствие, и удаляют любые инструменты или временные файлы, которые они поместили в уязвимые системы. В некоторых случаях атакующие даже устанавливают фальшивые флаги, пытаясь обвинить кого-то другого в своих деяниях. Наконец, злоумышленники могут попытаться нанести такой сильный ущерб системам, что воссоздать действия, которые они предприняли, будет непросто.

Современный злоумышленник

Злоумышленники понимают, как важно действовать незаметно. Хотя раньше они напоминали пиратов, которые чуть ли не кричат «Аааа!» и стреляют из пушек во время нападения (с тем только отличием, что вместо оружия используются вредоносные программы, сканеры и другие легко обнаруживаемые инструменты), современные злоумышленники обычно не столь откровенны. Теперь они больше напоминают ниндзя, прячась в тени и стараясь себя не выдать, пока они молча занимаются своим делом. Используя такие методы, как «кормление за счет земли», чтобы остаться незамеченным, современный злоумышленник гораздо более дисциплинирован и профессионален. Соответственно, те, кто занимается защитой, должны адаптировать свои подходы к этой новой тактике.

Киберпреступность превратилась в большой бизнес и привлекла внимание организованных преступников. Многие организованные синдикаты полностью переключились на кибердеятельность, направив ее в коммерческое русло, – они занимают целые здания с сотнями или тысячами сотрудников, каждый из которых участвует в преступном сговоре с целью получения финансовой выгоды от незаконных кибероперациий. Коммерциализация киберпреступности привела к сближению методов финансируемых государством целевых кибератак и методов, которые используют преступники, действующие с целью наживы. По мере того как исследователи в области безопасности и лица, реагирующие на инциденты, все больше и больше освещают тактику, методы и процедуры передовых угроз, организованная преступность наблюдает за этим, делает выводы и изобретает новые ходы. В результате злоумышленники учатся друг у друга и ведут нападение с использованием передовых методов, нацеливаясь на более широкий круг потенциальных жертв.

Многие злоумышленники, которые действуют организованно, вкладывают значительные средства в исследования и разработки, приобретая те же устройства обеспечения безопасности, которые используют их жертвы для своей защиты. Преступники нанимают специальные команды, которые работают над разработкой методов обхода для запуска атак, которые не смог бы обнаружить ни один из этих инструментов. Опытные исследователи, занимающиеся изучением деятельности черных хакеров, анализируют специализированные приложения, проекты с открытым исходным кодом и запатентованные технологии, чтобы максимально увеличить эффективность эксплойтов и вредоносного кода, которые доставит злоумышленник. В прошлом эти виды передовых методов были прерогативой злоумышленников, спонсируемых государством, и органов национальной безопасности; но печальная правда состоит в том, что теперь эти возможности доступны организованной киберпреступности и используются ею. Атаки, которые, как мы видели ранее, были направлены только на отдельные государства, теперь используются в широком корпоративном сегменте. Такое развитие событий и вызвало необходимость в написании этой книги, поскольку специалисты по реагированию на инциденты ИБ должны переосмыслить и пересмотреть традиционные подходы для противодействия новым угрозам.

Учетные данные – «ключи от королевства»

Современный злоумышленник понимает преимущества ситуации, когда можно действовать в открытую. Каждая часть специального вредоносного ПО, которое он развертывает, увеличивает вероятность обнаружения и требует дорогостоящего и трудоемкого тестирования и модификации кода, чтобы можно было обойти существующие механизмы безопасности. Использование коммерческих и общедоступных эксплойтов или вредоносных программ почти наверняка приведет к обнаружению практически в любом окружении, за исключением наименее подготовленного. Чтобы оставаться незамеченными, злоумышленники стремятся получить действительные учетные данные и повторно использовать их для доступа к новым системам.

У злоумышленника есть множество разных способов получить эти данные. Как только он закрепится в системе, он предпримет все возможное, чтобы получить любые дополнительные сведения. Поиск в кеше ARP, проверка записей журнала, использование средства просмотра сети и проведение сканирования цели – вот распространенные методы, помогающие злоумышленнику идентифицировать дополнительные системы, к которым можно подключиться. Как только новые цели будут определены, злоумышленнику понадобятся учетные данные, чтобы успешно перейти к новой системе. К сожалению, во время проверки системы первой жертвы злоумышленники нередко находят дополнительные учетные данные безо всякого труда. Несмотря на все усилия команд по обеспечению информационной безопасности и программы обучения сотрудников, некоторые пользователи по-прежнему хранят пароли в виде обычного текста – в файле, предусмотрительно названном password.txt, – на рабочем столе.

БЕЗОПАСНОСТЬ ПАРОЛЕЙ

Никогда не храните пароли в виде простого текста. Системы аутентификации должны использовать представление пароля, получаемое из открытого текста с использованием известного алгоритма. Любая система, которой необходимо проверить, правильно ли пользователь ввел пароль в виде открытого текста, может просто применить известный алгоритм к предоставленному пользователем паролю и рассчитать представление пароля. Затем рассчитанное представление пароля можно сравнить с представлением пароля, сохраненным аутентификатором. Если оба значения совпадают, то исходный текстовый пароль был введен правильно. Однако если сохраненные представления паролей аутентификатора скомпрометированы, злоумышленник, по крайней мере, не будет знать соответствующий пароль в виде открытого текста. Чтобы повысить безопасность таких систем, к паролю часто добавляют соль или псевдослучайное значение перед алгоритмом, применяемым для вычисления представления пароля. Таким образом вводится дополнительная энтропия и предотвращаются так называемые атаки с предварительным вычислением хеша, когда злоумышленник заранее определяет представление пароля для большого количества возможных паролей, а затем просто находит все представления, которые можно скомпрометировать, чтобы определить незашифрованный пароль. Пример такой атаки – радужные таблицы. Мы более подробно обсудим распространенные атаки на системы аутентификации в главе 12.

Часто именно разработчики приложений или системные администраторы упрощают злоумышленнику задачу. СМИ по-прежнему пестрят сообщениями о взломах данных веб-служб, когда компрометируются базы данных имен пользователей и паролей. В ряде таких случаев пароли хранятся в виде простого текста или, что немногим лучше, в представлении пароля, полученном из слабого алгоритма. Алгоритм, который уже неоднократно попадал в новостные заголовки, – MD5 без использования соли, – можно взломать с помощью радужных таблиц или графического процессора (GPU), применяя инструменты для взлома паролей, за короткое время и с минимальными усилиями. Проблема стала настолько распространенной, что передовые практики генерирования паролей включают в себя рекомендации по фильтрации паролей-кандидатов по общедоступным спискам скомпрометированных паролей: это гарантирует, что злоумышленники не смогут перебирать списки ранее раскрытых взломов паролей, чтобы определить вероятные пароли, используемые в целевом окружении.

Часто злоумышленнику не нужно определять полное имя пользователя и пароль, чтобы использовать существующие учетные данные для доступа к другим системам.

В окружении Windows представление пароля, а не пароль в виде открытого текста, используется в процессе аутентификации. Как следствие доступ к представлению хешированного пароля – это все, что требуется злоумышленнику для использования этих учетных данных и доступа к альтернативным системам под видом соответствующего пользователя. Один из наиболее распространенных примеров атак такого типа известен под названием pass-the-hash. Чтобы упростить процесс единого входа, когда пользователь входит в систему Windows, хеш, вычисленный во время аутентификации, хранится в памяти. Когда пользователь пытается получить доступ к удаленному ресурсу, Windows очень кстати использует этот хеш от имени пользователя для аутентификации в удаленной системе без дальнейшего взаимодействия с пользователем. Увы, злоумышленник, который скомпрометировал систему, – например, с помощью атаки на стороне клиента – может использовать эту функцию для запроса доступа к другим удаленным системам с помощью учетных данных, которые хранятся в памяти для скомпрометированной учетной записи пользователя.

Если злоумышленники имеют права локального администратора в скомпрометированной системе, они могут напрямую получить доступ к памяти этой системы, чтобы извлечь учетные данные, сохраненные для любого интерактивно вошедшего в систему пользователя. Наиболее известный инструмент для выполнения атак такого типа – Mimikatz. Используя Mimikatz, злоумышленник может извлечь хеши паролей или тикеты Kerberos для пользователей, которые вошли в систему.

Эти учетные данные затем могут передаваться в другие системы, что позволяет злоумышленнику выдавать себя за соответствующих пользователей. Важно отметить, что даже когда используется многофакторная аутентификация, кража учетных данных у пользователей, вошедших в систему, предоставляет злоумышленнику необходимые и достаточные учетные данные для дальнейшего перемещения по сети. После аутентификации пользователей

уже не дергают по поводу каждого фактора, поскольку они пытаются получить доступ к другим системам внутри одной и той же сети. В результате доступ к резидентным учетным данным, таким как тикет Kerberos, дает злоумышленнику возможность выдавать себя за пользователя даже в отсутствие аппаратных токенов или других механизмов многофакторной аутентификации. Мы рассмотрим детали таких атак, как pass-the-hash, pass-the-ticket и overpass-the-hash, в главе 12.

Атаки на учетные данные настолько распространены, что администраторы должны знать об угрозах сети каждый раз, когда они используют привилегированные учетные данные. Если система скомпрометирована и администратор обращается к ней в интерактивном режиме, учетные данные, используемые администратором, становятся доступными злоумышленнику. Злоумышленники даже могут специально заманить администратора, чтобы тот вошел в систему провести расследование. У злоумышленника будет запущенный экземпляр Mimikatz, находящийся в состоянии ожидания в системе, и он с радостью извлечет учетные данные администратора, как только представится случай.

У каждой компании должна быть строгая политика относительно использования привилегированных учетных данных. Следует всегда использовать концепцию наименьших привилегий, чтобы при раскрытии учетных данных ущерб от такого воздействия был снижен. Учетные данные администратора следует вводить только в выделенные и защищенные административные рабочие станции, системы, которые используются исключительно для задач администрирования и никогда – для интернет-навигации, доступа к электронной почте либо выполнения других опасных действий, способных подставить под удар соответствующий хост. Наряду с защитой учетных данных строгая дисциплина при использовании этих данных значительно облегчит разграничение законного и злонамеренного использования в случае компрометации административных учетных данных. Более подробно эти концепции будут рассмотрены далее.

Те, кто реагирует на инциденты ИБ, должны осознавать вышерассмотренную угрозу в ходе работы. Хотя дампирование памяти скомпрометированной системы является важным шагом в процессе анализа, интерактивный вход в систему с учетными данными администратора домена для создания этого образа потенциально может предоставить эти данные злоумышленнику. В последующих главах мы рассмотрим механизмы, которые специалисты, реагирующие на инциденты ИБ, могут использовать для получения необходимой информации без предоставления привилегированных учетных данных злоумышленникам.

Заключение

За последнее десятилетие тактика и методы злоумышленников стали еще более изощренными и трудно распознаваемыми. У современных хакеров имеется большой набор методов атак на любой вкус и широкий спектр мо-

тивов. Организации, которые предполагают, что они слишком малы или не представляют интереса для взломщиков, ошибаются, поскольку злоумышленники стремятся использовать любые шансы для продвижения своих киберкампаний. Эта книга содержит действенные методики, которые вы можете использовать для обнаружения атак на ваше окружение и своевременного реагирования на них. И первый шаг на этом пути – осознание угрозы как таковой.