Корпоративное минное поле

Виктор СЕРДЮК,
генеральный директор
АО «ДиалогНаука»

Роман ВАНЕРКЕ,
технический директор
АО «ДиалогНаука»

На сегодняшний день большая часть средств защиты информации, таких как межсетевые экраны, системы обнаружения вторжений, антивирусы, песочницы и т. д., направлены в первую очередь на защиту периметра организации. Причем не важно, где они установлены – на границе сети или на рабочей станции, – средства предназначены для выявления и предотвращения внешних атак нарушителя.

Можно выделить классы решений, направленные на выявление злоумышленника с помощью анализа контекста или его поведения, например системы класса SIEM или UEBA. Но такие системы требуют длительного времени для обучения и тонкой настройки. Как же быть в случаях, когда хакер уже находится в вашей сети, пройдя все рубежи защиты? Ведь проникновение хакеров внутрь периметра предприятия неизбежно – на это указывают публикации по происходящим регулярно взломам сетей промышленных предприятий, государственных институтов и банков, об этом же говорят различные аналитические материалы. Рано или поздно это может произойти со всеми, просто большинство молчит о своих проблемах либо просто не знает о них. Однако само проникновение – не самое опасное. Злоумышленнику важно добраться до наиболее ценных ресурсов, не подняв при этом тревоги.

Для эффективного противодействия нарушителю разработчики средств защиты начали выпускать продукты нового класса, базирующиеся на механизмах приманок (deceptions) и ловушек (honeypot), которые создают для нападающих виртуальные привлекательные цели и позволяют быстро обнаружить нападение с помощью простого правила: любой запрос к подобной ловушке или любое использование приманки исходит от злоумышленника. Далее более подробно будут рассмотрены возможности применения этих двух механизмов защиты.

Ловушки

Собственно, сами ловушки (honeypot) были разработаны довольно давно – именно с их помощью специалисты производителей решений по информационной безопасности изучают актуальные угрозы в Интернете и определяют репутации файлов, URL и почтовых адресов. С распространением технологии виртуализации такие ловушки становились все сложнее, появилась возможность использовать их не только для изучения действий злоумышленников в Сети, но и для защиты корпоративной сети посредством создания для нарушителя ложных целей внутри ЛВС организации. В последнее время к таким системам был добавлен функционал противодействия хакерам: попав в сеть ловушки, злоумышленник тем самым выдает себя, и все его дальнейшие действия будут зафиксированы для расследования инцидентов и доказательства его вины. Функционально такая ловушка очень похожа на зеркальное измерение из фильма «Доктор Стрэндж», в котором маги могли сражаться друг с другом, не затрагивая реальный мир.

Итак, современные ловушки выполняют следующие функции:

- выявляют целенаправленные и неизвестные атаки в режиме реального времени: любого, кто будет обращаться к ловушке, можно считать злоумышленником независимо от того, пришел он снаружи или изнутри корпоративной сети;
- защищают реальные ИТ-активы компании путем создания более привлекательных для хакеров целей и переключения их активности на виртуальную сеть ловушки;
- собирают полную информацию о тактике атакующих и используемых ими инструментах с возможностью оперативного применения адекватных мер противодействия при попытке хакеров атаковать реальные ИТ-активы;
- собирают доказательства его неправомерных действий;
- сокращают временные затраты на обнаружение атак и минимизируют расходы на устранение последствий атак.

Конечно, ловушка не может заменить другие средства защиты, такие как межсетевые экраны, средства обнаружения вторжений, сканеры уязвимостей и др. Для ее эффективной работы нужно создать для хакеров хотя бы видимость защиты реальных ИТ-ресурсов. Таким образом, будет не очень эффективно установить ловушку в незащищенной сети – она будет фиксировать только часть атак, остальные все-таки попадут в цель. Поэтому при внедрении ловушек следует обеспечивать хотя бы базовый уровень защиты реальных ИТ-систем: устанавливать обновления, проверять качество паролей, блокировать прямой доступ к системам из сети Интернет и реализовывать минимально необходимый набор защитных мер, перечисленных в лучших практиках.

Возможность демаскировать хакеров очень важна, поскольку они, как и подводные лодки, сильны только в том случае, если действуют скрытно. Как только их действия обнаружены и координаты определены, хакеры могут быть достаточно быстро нейтрализованы. Поэтому одно из основных требований к ловушкам заключается в том, чтобы злоумышленник не смог ее отличить от реальных объектов, которые она эмулирует.

Ловушки позволяют защищаться не только от внешних хакеров, но и от инсайдеров. Можно выделить два варианта использования ловушки: от внешних нападений и от внутренних. В первом случае ловушка устанавливается на периметре, имитируя для внешних хакеров внутренность корпоративной сети. Во втором – рядом с ценными ресурсами: базами данных, технологическими сетями или лабораториями разработки. В такой ситуации имитировать придется именно ту инфраструктуру, рядом с которой ловушка будет установлена. К счастью, современные решения автоматически сканируют защищаемый объект и сами создают достаточно правдоподобное сходство.

> Хакеры как и подводные лодки, сильны только в том случае, если действуют скрытно.

Приманки

Приманки (deception) – уникальный механизм защиты, который сам по себе ничего не защищает. Что делает злоумышленник, оказавшись на узле? Проверяет, какие пароли закэшированы, какие сетевые ресурсы доступны, просматривает историю в браузере и т. д. Основная цель такой активности – продвинуться дальше к ценным ресурсам и активам. Таким образом, для выявления злоумышленника на узлах размещаются несуществующие, но очень похожие на настоящие данные, чтобы хакер смог ими воспользоваться и тем самым раскрыть свое присутствие. По сути, каждый узел в сети становится ловушкой, которую невозможно избежать. Поскольку приманки записываются в кэш на узле, они невидимы для администраторов и не влияют на существующие ИТ-процессы компании.

В качестве одного из примеров приманки можно привести запись в память рабочей станции кэша паролей для несуществующих учетных записей. Следовательно, если злоумышленник попадет на рабочую станцию с такой приманкой и при помощи утилиты mimikatz получит доступ к паролю и попробует им воспользоваться, то об этом сразу будет оповещен администратор безопасности.

Продукты

В качестве примеров коммерческих продуктов, использующих механизмы ловушек и приманок, можно назвать решения Deceptions Everywhere компании Illusive networks и DeceptionGrid от компании TrapX.

Продукт под названием Deceptions Everywhere позволяет ввести злоумышленника в заблуждение, заставить его выдать себя неосторожными действиями и остановить его продвижение к ценным ресурсам внутренней сети, после чего можно провести дальнейшее расследование инцидента. Deceptions Everywhere создает привлекательный для злоумышленников слой фальшивых корпоративных данных (более десяти семейств приманок – от закэшированных учетных данных и сетевых ресурсов до связей с базами данных), провоцируя его

обнаружить себя во время исследования среды, при этом собрать данные для расследования и заблокировать атаку на реальную систему.

В состав продукта входит система управления Deception Management System (DMS), в которой использованы методы машинного обучения для предсказания векторов атак и создания для каждого из них наиболее привлекательной приманки. При этом за основу берется реальная корпоративная инфраструктура, что и позволяет постороннему или даже корпоративному нападающему не заметить фальшивки. Например, если в домене организации используются учетные записи в виде i.ivanov, то система создаст похожие приманки – p.ivanov, o.ivanov. Аналогичным образом создаются и другие приманки и ловушки. Приманки создаются автоматически, а затем распределяются по сети в соответствии с корпоративными стандартами компании. Система сама определяет необходимое количество приманок и ловушек, чтобы гарантированно выявлять злоумышленника за два-три шага. Решение регулярно обновляет приманки и ловушки, автоматически подстраиваясь под конкретный защищаемый узел на основе его анализа. Также стоит отметить, что сами приманки не видны ИТ-администраторам и не мешают их работе.

Для контроля за действиями хакеров используется компонент Attacker View, который создает карту сети с возможными векторами атаки. Attacker View представляет сеть так, как ее видит хакер. Это позволяет анализировать, оценивать и закрывать потенциальные риски и уязвимости в реальной сети. Продукт также предупреждает администраторов безопасности о проводимой посторонними атаке в реальном времени и собирает цифровые доказательства с атакованных систем для дальнейшего расследования. Поскольку обычные пользователи не могут попасть в слой ловушек, то система моментально фиксирует любое срабатывание и сообщает об угрозе администратору безопасности. Подробная запись выполняемых хакером действий содержит информацию о месте атаки, пути проникновения, используемых техниках и контексте, что позволяет в дальнейшем провести эффективное расследование инцидента.

Решение TrapX DeceptionGrid сочетает в себе разнообразные возможности маскировки для отвлечения, дезинформации и обнаружения хакеров, предлагая им целую сеть ложных векторов атак. Продукт позволяет создавать такие приманки, как кэшированные пароли, связи с базами данных, серверами приложений, сетевыми хранилищами и прочими привлекательными для взломщиков ресурсами внутри ловушки.

DeceptionGrid, как и Deceptions Everywhere, проводит сканирование сети и по его результатам создает до нескольких тысяч привлекательных для хакеров целей, которые имитируют ресурсы реальной сети. Создаваемые фальшивые данные выглядят, как обычные файлы, закладки, ссылки и базы данных, располагающиеся на существующих ИТ-активах. Ловушки могут имитировать серверы, рабочие станции, сетевые коммутаторы, медицинские устройства, банкоматы, торговые терминалы, компоненты финансовой сети SWIFT и многое другое.

Ключевым элементом решения является мониторинговая система TrapX DeceptionGrid Emulated traps, которая позволяет с помощью одной виртуальной машины создать необходимый набор приманок, привлекательных для атакующих, и сформировать в этой виртуальной сети предприятия набор сенсоров для обнаружения действий хакеров. Хакер видит сервисы на определенном хосте, может с ними взаимодействовать и атаковать их, используя любые инструменты, но для развития атаки они непригодны, поскольку являются всего лишь процессами виртуальной машины DeceptionGrid.

Чтобы реальные средства защиты среагировали на действия злоумышленников, в виртуальной среде используются специальные информационные флаги – Deception Tokens, благодаря которым IDS и другие средства защиты могут понять, что злоумышленник атакует виртуальную сеть ловушки. Их появление в трафике должно вызвать срабатывание сигнала тревоги, и служба безопасности обязана будет приступить к расследованию инцидента. События можно классифицировать по типам, что позволяет ИБ-службе приоритезировать свои действия. Например, когда атакующая сторона пытается установить управляющие соединения (interaction) или в трафике появляются вредоносные коды (infection), эта информация также отображается в системном журнале фиксируемых событий. Информация о событиях Interaction и Infection позволяет сразу автоматически изолировать скомпрометированные рабочие станции в карантинной подсети за счет интеграции с NAC-системами.

Кроме того, DeceptionGrid обеспечивает возможность автоматически провести статический и динамический анализ вредоносного кода, для того чтобы быстро сформировать индикаторы компрометации (IoC) и с помощью, например, SIEM, проверить весь парк компьютеров и серверов на их наличие в других системах предприятия.

Заключение

Технологии виртуальных ловушек и приманок для хакеров дополняют существующие средства защиты информации за счет выявления атак уже после проникновения злоумышленников внутрь корпоративной сети. Кроме того, решения данного класса позволяют собрать необходимую доказательную базу для проведения в расследования выявленного инцидента. ■