Ловушки:
как исследовать повадки хакера, не подвергая корпоративные ресурсы угрозам

Константин РОДИН,
руководитель отдела развития продуктов компании «АйТи Бастион»

Информационная безопасность стала одним из самых горячих и важных вопросов для бизнеса в наше время. Киберзлоумышленники совершенствуются день ото дня, постоянно ищут новые способы вторжения в корпоративные сети и ИТ-системы. Компании принимают вызов и активно работают в этом направлении, стараясь защитить свой периметр от вторжения хакеров: создают ложные цели и «расставляют» для них так называемые ловушки, которые позволяют исследовать и анализировать поведение хакера без риска для реальных данных. Как они работают? Как понять поведение преступника, попадающего в такие «сети», не подвергая при этом информационные ресурсы угрозам?

Почему ловушки важны?

Прежде чем погрузиться в детали того, как ловушки помогают исследовать поведение хакера и надежнее защищать инфраструктуру, разберемся, почему они так важны. Известные как Honeypots они представляют собой вымышленные информационные ресурсы, которые создаются для намеренного и, что важно, контролируемого привлечения киберпреступников. Эти ресурсы имитируют реальные корпоративные системы и служат первоочередной целью для взлома злоумышленниками. Причем они не содержат настоящих уязвимых данных, следовательно, атаки на ловушки не представляют собой угрозу для корпоративных бизнес-систем.

Рассмотрим, какие методы и инструменты используются для исследования поведения хакера, когда он атакует ловушку.

Захват и анализ трафика

Когда хакер атакует Honeypots, весь сетевой трафик между ним и ловушкой может быть захвачен и записан: входящий и исходящий трафики, команды, которые киберзлоумышленник выполняет в системе, данные, которые он пытается оттуда извлечь. Захваченный трафик можно потом проанализировать, чтобы понять, какие методы атаки использует преступник и какие уязвимости ИТ-периметра пытается эксплуатировать.

Регистрация действий хакера

Ловушки также могут регистрировать все действия, совершаемые хакером в системе: команды, которые он выполняет, попытки изменения файловой системы, запросы на доступ к конфиденциальным данным и многое другое. Регистрация этих действий позволяет более подробно изучить методы работы киберпреступников и цели их действий.

Анализ идентификационных данных

Если хакер попытается аутентифицироваться или передать идентификационные данные, ловушки фиксируют эти сведения для дальнейшего подробного анализа: логины, пароли или сертификаты, которые киберпреступник пытается использовать для доступа к информационной системе компании. Анализ таких данных позволяет выявить, какие учетные записи или ресурсы были скомпрометированы.

Изучение характеристик атаки

Honeypots способны собирать информацию о характеристиках атаки, такие как IP-адреса хакера, используемые уязвимости и методы обхода систем безопасности. Эти сведения могут быть использованы для обновления и усовершенствования мер информационной безопасности корпоративной сети.

«Анатомия» взлома ИТ-системы хакером

Киберугрозы стали неотъемлемой частью современного мира бизнеса и информационных технологий. Хакеры постоянно ищут слабые места в ИТ-системах

организаций и предприятий. Понимание того, как именно происходит их взлом киберпреступником, а также методов защиты корпоративных ресурсов, критически важно для компаний.

Если кратко, то взлом информационной системы – это процесс, в ходе которого злоумышленник получает несанкционированный доступ к компьютерной сети, серверам или данным организации. Процесс взлома обычно состоит из нескольких этапов.

Разведка

Первым шагом хакера является сбор информации о целевой компании: исследование внешних сетевых ресурсов, поиск уязвимостей в общедоступных базах данных или анализ социальных медиа для поиска информации о сотрудниках и структуре организации.

Сканирование и обнаружение уязвимостей

Как правило, киберпреступники используют сканеры и инструменты для поиска уязвимостей в сети или приложениях компании: поиск необновленных программ, слабых паролей или недостаточных настроек безопасности.

Эксплуатация уязвимостей

Как только хакер обнаруживает уязвимость, он будет пытаться ее эксплуатировать: использование зловредных программ, внедрение в корпоративный ИТ-периметр через недостаточно защищенные точки входа, ставшие такими зачастую в результате неконтролируемого доступа пользователей с привилегированными правами, социальная инженерия для обмана сотрудников и получения необходимой информации с целью внедрения в систему.

Поддержание доступа

После успешного взлома хакер может попытаться сохранить доступ к системе, устанавливая скрытых «пользователей», «черные ходы» или исследуя систему для поиска дополнительных уязвимостей.

> Киберугрозы стали неотъемлемой частью современного мира бизнеса и информационных технологий.

Удаление следов

Преступники могут стараться скрыть свои действия в системе, чтобы оставаться незамеченными как можно дольше. Для этого они с помощью специальных инструментов «подчищают» за собой все следы.

Автор фото: dj-applej-sound

Как защитить корпоративные ресурсы от киберугроз?

Только комплексным подходом к решению задачи. Вот несколько основных шагов для обеспечения кибербезопасности.

Регулярное обновление программного обеспечения

Необходимо внедрить патч-менеджмент, т. е. выстроить процесс управления обновлениями для оперативного закрытия уязвимостей и проверки самих обновлений операционных систем, приложений.

Сильные пароли и двухфакторная аутентификация

Использовать сложные пароли и включить двухфакторную аутентификацию для обеспечения дополнительного уровня защиты.

Сетевая безопасность

Обеспечить корректную настройку межсетевых экранов, средств обнаружения и предотвращения вторжений (IDS/IPS), других доступных инструментов защиты корпоративной сети.

Обучение персонала

Важно на регулярной основе проводить обучение сотрудников в области кибербезопасности, повышать их ИБ-компетенции и актуализировать знания, учить специалистов определять потенциальные угрозы и своевременно на них реагировать.

Мониторинг и анализ событий

Необходимо применять современные системы мониторинга безопасности и анализа событий для раннего обнаружения аномальной активности.

Контроль доступа пользователей

Критически важно контролировать доступ пользователей, особенно с привилегированными правами, в ИТ-периметр компании. Это фундаментальный элемент качественной стратегии кибербезопасности. Компании должны внедрять комбинацию решений управления доступом, систем контроля доступа на основе ролей и систем непрерывного мониторинга для защиты от потенциальных угроз. Для этого нужно использовать специализированные инструменты, например PAM-системы.

Использование ловушек

Полезно создавать собственно ловушки для привлечения хакеров, осуществлять мониторинг и анализировать их методы воздействия без риска для реальных данных.

Точки внимания

Honeypot стоит рассматривать как альтернативную технологию противодействия кибератакам и потенциальным кибернападениям, поскольку в постоянной борьбе между атакующими и защищающимися сторонами в информационных системах всегда есть и будут уязвимости. Тут важно подходить к проблеме комплексно и начать с главного – контроля доступа в периметр со стороны пользователей.

При «расстановке» таких «приманок» следует учитывать следующие аспекты.

- Honeypot действительно привлекают злоумышленников, потому что видятся им как уязвимые и интересные цели. Благодаря этому компании могут не только отвлекать их на ложные цели, но и наблюдать за их действиями, контролируя действия в «безопасном» периметре.
- Технология «киберприманок» не должна быть единственным решением в политике ИБ, но должна гармонично дополнять классические системы защиты информации.
- Для эффективности системы ловушек нужно развернуться «на широкую ногу». Обеспечить максимальное покрытие различными техниками взлома и размещение Honeypot в разных сегментах сети.
- Значимую роль в отслеживании работоспособности системы киберприманок играют автоматизация и настройки системы. Все должно быть «по-настоящему» и функционировать без сбоев.
- Компаниям, внедряющим Honeypot, нужно проводить регулярные киберучения, отрабатывать сценарии противодействия с их применением. Это позволит убедиться в готовности информационной системы к атакам извне.
- В использовании ловушек следует придерживаться разных подходов, например: долговременной дезориентации хакера и расстановки большого количества низко интерактивных приманок. Иными словами, комбинировать варианты навязывания ложных целей.

> Важно подходить к проблеме комплексно и начать с главного – контроля доступа в периметр со стороны пользователей.

Потенциал инструмента

Понимание того, как происходит взлом информационной системы киберпреступниками, и применение соответствующих мер информационной безопасности – ключевые моменты защиты корпоративных ресурсов от киберугроз. Комплексный подход и понимание ключевых принципов выстраивания системы ИБ помогут минимизировать риски и обеспечить надежную защиту бизнес-инфраструктуры.

Таким образом, ловушки – мощный инструмент для исследования поведения хакеров, позволяющий анализировать атаки без риска для реальных данных и информационных систем. Используя их, компании в случае инцидентов могут лучше понять методы и цели киберпреступников и, что особенно важно, усовершенствовать и повысить эффективность своих мер безопасности. Кроме того, Honeypots могут служить ранним предупреждением о потенциальных атаках, способствовать повышению уровня кибербезопасности в целом и помогут найти «брешь» в ИБ-политике предприятия. ■