ОСОБЕННОСТИ ТАРГЕТИРОВАННОЙ ИНФОРМАЦИОННОЙ АТАКИ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОТРУДНИЧЕСТВА РОССИЙСКИХ И ЗАРУБЕЖНЫХ ВУЗОВ

Шмелев А. В.,
Сухотерин А. И.
Московский государственный областной технологический университет, Королев, Российская Федерация.

Как бороться с таргетированными атаками? Очевидно, что нужно какое-то технологическое решение, в котором были бы объединены лучшие идеи по обнаружению неизвестных угроз. Но прежде чем говорить о нем, стоит определиться с тем, что считать таргетированной атакой, и разобрать, как они работают.

Ключевые слова: информационная безопасность, таргетированная атака, компрометация.

FEATURES OF THE TARGETED ATTACK IN THE INFORMATION SECURITY SYSTEM OF COOPERATION RUSSIAN AND FOREIGN UNIVERSITIES

Shmelev A.V.,
Sukhoterin A.I.
University of Technology, Korolev, Russian Federation

How to deal with targeted attacks? Obviously, we need some technological solution in which the best ideas for detecting unknown threats would be combined. But before talking about it, it is necessary to decide what to consider as the target attack, and to understand how they work.

Keywords: information security, targeted attack, compromise.

Таргетированные атаки (они же APT - Advanced Persistent Threat "Развитая устойчивая угроза") — настоящий бич нашего времени, и на защите от них уже построен не один многомиллионный бизнес. Заглядывая на любую выставку, посвященную ИБ, можно увидеть: для продающей стороны APT — это теперь важная часть предложения, а для покупающей — одна из насущных проблем. Причем актуальна она уже не только для крупного бизнеса, наученного горьким опытом, но и для среднего и даже малого. Если атакующий хочет добраться до корпорации, то мелкий подрядчик вполне может оказаться промежуточной целью.

К сожалению, термины «таргетированная атака» и «целенаправленная атака» некорректны. Почему? Вспомним классическое определение компьютерной атаки: «Компьютерная атака — целенаправленное несанкционированное воздействие на…». Получается, что цель-то есть у любой атаки, а не только у «таргетированной».

Отличительная особенность целенаправленных атак заключается в том, что атакующий активно и интеллектуально подходит к выбору точки входа в конкретную инфраструктуру, достаточно долго анализирует циркулирующую в ее компонентах информацию и использует собранные данные для получения доступа к ценной информации.

Исследователи обычно рассматривают отдельные аспекты атак и не проводят комплексный анализ проблемы. Поэтому несовершенны и методы выявления атак и борьбы с ними в уже скомпрометированной среде.

Например, многие методы и системы безопасности основаны на статических списках шаблонов, то есть на базах для эвристического анализа, «белых списках», базах сигнатур и так далее. Однако такие списки оказываются неэффективными для определения «нешаблонных» угроз, при которых злоумышленники стараются скрыть свое присутствие в скомпрометированной инфраструктуре.

Метод, который в соответствии с требованиями различных стандартов обеспечения ИБ гарантирует отсутствие в системе нарушителя, заключается в создании и поддержании замкнутых доверенных программно-аппаратных сред. Именно так «бумажная безопасность» исключает компрометацию на любом этапе.

Увы, с практической точки зрения этот метод неэффективен. Современные программно-аппаратные среды обычно построены на основе оборудования и софта разных производителей, которые используют разные подходы при разработке, разные методы обновления и поддержки. Исследовать все продукты, нет ли в них закладок, нереально, а без этого никаких доверенных сред не выйдет.

Другой метод защиты ценных ресурсов от целенаправленного несанкционированного доступа основан на физической изоляции защищаемых объектов. И он тоже неэффективен в реальных условиях. Даже если удастся закрыть все побочные каналы связи, которые могут быть использованы злоумышленниками для вывода данных, остается человеческий фактор. Нередко побочные каналы связи создают именно люди, взаимодействуя с системами, — непреднамеренно или же умышленно.

Получается, что избежать риска компрометации фактически невозможно. Соответственно, нужны системы выявления неизвестных атак в уже скомпрометированной среде. Этот класс решений носит гордое название post-breach («после взлома») и чаще всего решает задачу response/mitigation, то есть реагирования и смягчения.[5]

А вот методов и построенных на их основе решений для своевременного детектирования угроз (post-breach detection) в действительности не так много. Например, один из них — это сети ловушек, которые широко известны как «ханипоты» (рис. 1).

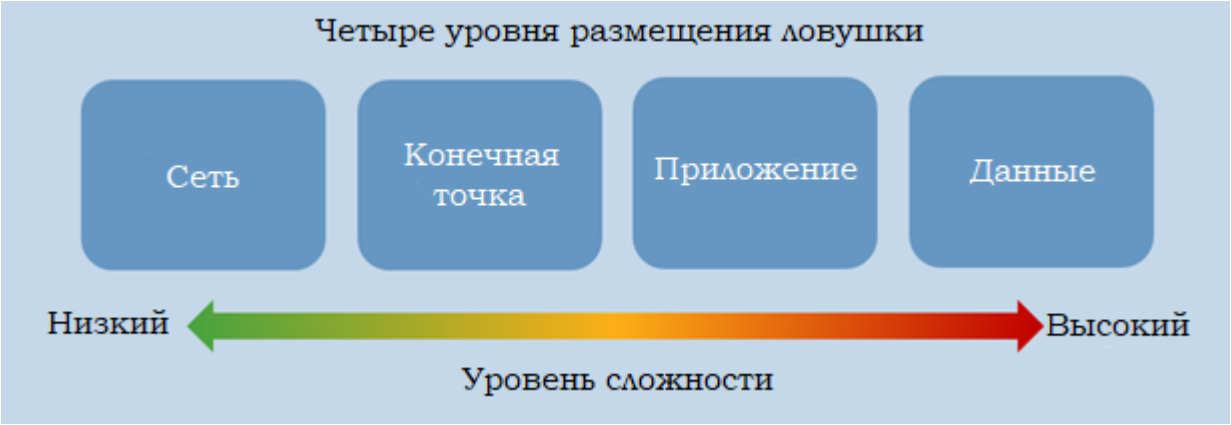

Рисунок 1 - Уровни, на которых может быть реализована система ловушек (по мнению Gartner)

Правильно сделанная ловушка действительно может помочь обнаружить целенаправленную атаку на определенной стадии. Но при этом классический ханипот вряд ли чем-то поможет в выявлении других точек присутствия атакующего.

Известны способы адаптивного развертывания систем ловушек, а также поиска аномалий в функционировании компонентов системы. Гораздо сложнее найти рекомендации, как выбирать параметры развертывания ханипотов. Сколько нужно

фейковых рабочих станций в сети? Какие фейковые аккаунты и на каких машинах создать? Еще сложнее проанализировать полученные таким способом данные.

Чтобы не вносить терминологическую путаницу, будем использовать термин «неизвестная компьютерная атака». Она может включать в себя свойства целенаправленных атак, но не ограничиваться ими. Неизвестная компьютерная атака — это непрерывное целенаправленное несанкционированное воздействие при помощи программных или программно-аппаратных средств с такими параметрами функционирования, которые не позволяют защитным решениям его обнаружить в реальном времени. [1]

Звучит сложно? На самом деле все сводится к трем ключевым особенностям: непрерывности, целенаправленности и нетривиальности.

Непрерывность — характеристика, определяющая временной интервал, в течение которого атакующий сохраняет несанкционированный доступ к ресурсу или воздействует на него. В частности, целенаправленные атаки отличаются продолжительным контролем точек присутствия в целевой информационной системе. [2]

Целенаправленность — характеристика, которая определяет степень ручной работы со стороны атакующего для реализации несанкционированного доступа или воздействия и учитывает индивидуальные особенности целевой инфраструктуры.

Нетривиальность для систем обнаружения атак — это характеристика, определяющая сложность обнаружения этого класса атак защитными системами атакуемого объекта. Связана с целенаправленностью. Это ключевая характеристика для оценки эффективности методов и систем защиты. [1]

Жизненный цикл атаки

Любую кибератаку можно поделить на стадии, названия которых пришли к нам из военной науки. Каждая стадия подразумевает набор стратегий и методов для их реализации. И для каждой из стадий существуют превентивные меры и стратегии ответных действий (рис. 2). [3, 4]

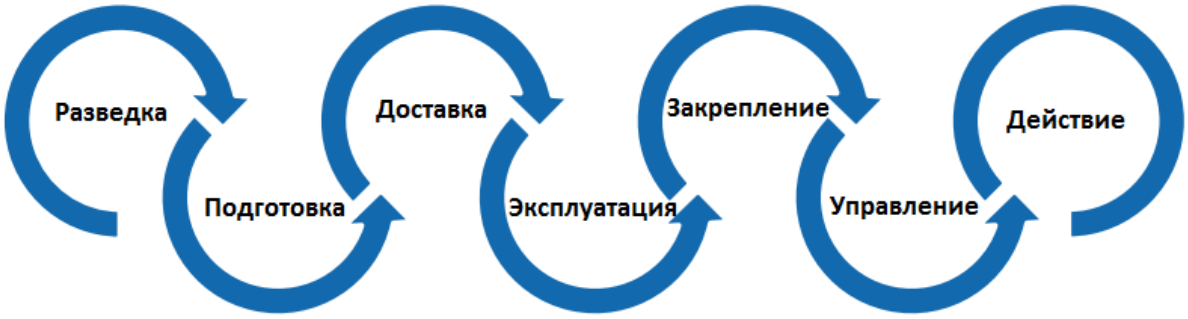

Рисунок 2 - Жизненный цикл атаки (по материалам Gartner)

Давай на примерах разберем каждую стадию жизненного цикла атаки и проиллюстрируем стратегии реализации этапов.

Эти сценарии лишь частный случай из многообразия тактик и средств, которые может использовать атакующий.

Во время разведки злоумышленник пытается обнаружить точки входа в целевую инфраструктуру. Для этого он внимательно изучает отчет своего сканера веб-уязвимостей, который просканировал публичное веб-приложение, принадлежащее жертве.

Кроме того, злоумышленник, анализируя выдачу поисковых систем, ищет используемые ресурсы, IP которых входят в диапазон адресов целевой организации.

Злоумышленник нашел профили нескольких сотрудников организации в социальных сетях и их корпоративные email-адреса. На основе полученных данных подготовил следующий план действий.

1. Попытаться скомпрометировать рабочие стации обнаруженных сотрудников.
2. Если это не удастся, злоумышленник попробует использовать публичные эксплоиты, чтобы атаковать серверы организации, доступные из интернета, а также роутеры Wi-Fi в офисах компании.
3. Параллельно с первыми двумя шагами будет искать уязвимости в публичном веб-приложении в надежде, что скомпрометированное приложение предоставит ему доступ к внутренней инфраструктуре.

Чтобы реализовать все это, злоумышленник готовит текст письма с вредоносным вложением сотрудникам, настраивает найденные эксплоиты, а также запускает перебор пароля для администратора обнаруженного веб-ресурса.

Наиболее вероятным путем атаки будет подмена WiFi сети в офисе компании с помощью ноутбука и последующее подключений мобильных устройств ее сотрудников к этой сети.

На практике часто оказывается так, что злоумышленник вынужден проводить целую спецоперацию и создавать новые точки присутствия для того, чтобы обеспечить себе постоянный контроль (persistent). Ему придется проводить разведку внутри скомпрометированной инфраструктуры и перемещаться к ценным ресурсам. Это называется lateral movement: вряд ли полученный доступ к компьютеру бухгалтера удовлетворит злоумышленника — его скорее интересует интеллектуальная собственность компании. Ну и в конечном счете злоумышленнику нужно будет провести незаметный вывод данных (exfiltration). [5]

Конечно, этап противодействия должен начинаться раньше, а не после всех описанных стадий. Но иногда бывает так, что злоумышленник начинают искать уже после того, как он скрылся с ценными данными. И зачастую это происходит не только из-за некомпетентности защищающейся стороны. Просто злоумышленник имел достаточно времени, чтобы изучить жертву, прежде чем начал какие-то активные действия, и хорошо знал обо всех защитных системах. Да и злоумышленников зачастую много, а некоторые из них прячутся и среди внутренних сотрудников.

Именно по описанным выше причинам нам необходимо узнать о злоумышленнике и его намерениях еще до того, как он реализует все стадии своей атаки. Для этого нужно научиться вовремя определять его появление в защищаемой инфраструктуре.

Литература:

1. Грибунин В.Г. Комплексная система защиты информации на предприятии. // – М.: Academia, -2013;
2. Шаньгин В.Ф. Администрирование и защита. Защита информации в компьютерных системах и сетях. // – М.: ДМК Пресс, -2014;
3. Левцов В. Анатомия таргетированной атаки, часть 1. Левцов В., Демидов Н. // - М.: Information Security №2/ Информационная безопасность. — 2016.
4. Левцов В. Анатомия таргетированной атаки, часть 2. Левцов В., Демидов Н. // - М.: Information Security №4/ Информационная безопасность. — 2016.
5. Джеун И. Практическое исследование передовых постоянных угроз Джеун И., Ли Ю., Вон Д. — Springer Berlin Heidelberg, 2012.