Александр ЩЕТИНИН
генеральный директор Xello

Владимир СОЛОВЬЁВ
руководитель направления внедрения средств защиты АО «ДиалогНаука»

ТЕХНОЛОГИЯ ОБМАНА

ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ С ПОМОЩЬЮ DECEPTION

Защищённость корпоративной сети организации — одна из ключевых задач специалиста по информационной безопасности. Если не уделять должного внимания противодействию атакам, то корпоративная сеть становится интересной для злоумышленника, ведь для проникновения в неё не нужно прилагать множества усилий и можно добраться до цели без особых преград.

Сегодня есть множество решений для обеспечения защиты: многие компании строят свои ситуационные центры информационной безопасности (SOC) или используют коммерческие, внедряют «песочницы», используют интеллектуальные межсетевые экраны, проводят аудиты и т.д. Однако все эти меры не гарантируют полную защищённость организации — нападения неизбежны, и нужно уметь чётко понимать, каковы могут быть последствия для организации в случае успешного нападения.

С середины 2020 года существенно увеличилось число различных атак, которые отчасти связаны с тем, что многие организации не были готовы к удалённой работе сотрудников. Сотрудники столкнулись с перебоями в подключении к корпоративной сети, не были готовы к использованию удалённых рабочих мест, VDI, быстрого масштабирования корпоративных облаков и т.д. — и это лишь малая часть причин, которые подтолкнули директоров по информационной безопасности к пересмотру стратегии защищённости организации. Не менее важной причиной является дефицит профессиональных кадров в сфере информационной безопасности.

Согласно последнему исследованию американской компании IDG по приоритетам безопасности, 32% компаний начали внедрять в своих организациях технологию Deception. Это связано с тем, что технологии злоумышленников в развитии целенаправленных атак (APT-атак) динамично развиваются и тем самым специалисты по всему миру понимают, что защитные меры должны быть соответствующими и опережающими.

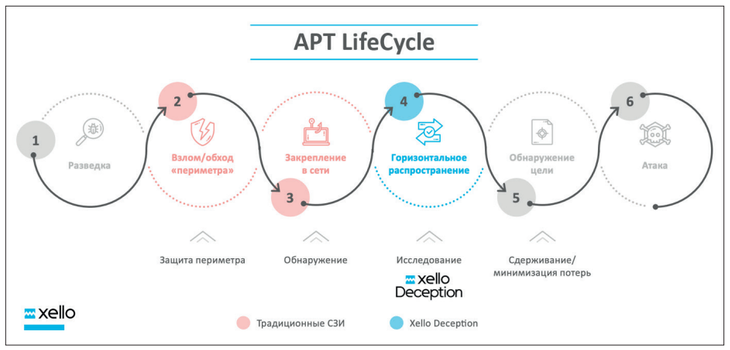

Рисунок 1. Технология Deception может как предотвратить злонамеренные действия, так и оповестить ответственных сотрудников о проникновении во внутренний контур

КАК ДЕЙСТВУЕТ ЗЛОУМЫШЛЕННИК ПРИ ЦЕЛЕНАПРАВЛЕННЫХ АТАКАХ?

Мошенники продолжают использовать уникальные технологии и методы социальной инженерии для проникновения в корпоративную сеть организации. Проникая во внутренний контур, они в основном используют стратегию замедленного действия, то есть перед каждым следующим шагом происходит оценка рисков и принимается решение о дальнейшем ходе событий. Это позволяет быть незамеченным в инфраструктуре, обойти системы мониторинга и добраться до цели. Важно также учесть, что если злоумышленник прошёл периметровые средства защиты и смог закрепиться в сети в обход систем защиты конечных узлов, то дальше его уже обнаружить крайне сложно без специализированных решений.

КАК ЗАПУТАТЬ ЗЛОУМЫШЛЕННИКА?

Представим ситуацию, когда злоумышленник бесследно проник в сеть и закрепился на любом конечном узле внутри. Решения класса SIEM, NGWF в нужный момент его не обнаружили, и, по сути, компания не знает о проведении атаки. В этом случае поможет технология Deception: она сможет как предотвратить злонамеренные действия, так и в нужный момент оповестить ответственных сотрудников о проникновении злоумышленника во внутренний контур (рис. 1). Решение автоматически анализирует структуру и состав Active Directory для того, чтобы на основании анализа создать подходящие приманки и ловушки в виде «ложных» учётных записей, ведущих на несуществующие сервисы, запутывая тем самым мошенника. Deception усложняет задачу нежданному гостю, служит последним рубежом защиты для компании и моментально уведомляет об аномалиях, а также о том, где находится сейчас мошенник и какие осуществляет действия.

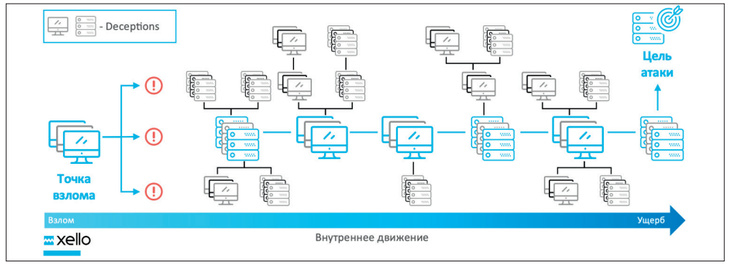

Рисунок 2. Система Deception превращает каждый ПК в ловушку, которой нельзя избежать

ЗАЩИТА С ПОМОЩЬЮ XELLO DECEPTION

Технология продукта Xello Deception уникальна тем, что она не делает точную копию инфраструктуры, а симулирует похожую по синтаксическим признакам. При внедрении и далее в ходе всего цикла использования система непрерывно проводит анализ состава DNS и Active Directory на предмет изучения реальных информационных активов корпоративной сети и на основании полученных данных генерирует приманки и ловушки. Затем приманки, которые злоумышленник не сможет распознать, распространяются безагентским способом на реальные конечные узлы в инфраструктуре организации.

Продукт Xello использует генерацию множества приманок и ловушек, которые имитируют конечные узлы, программное и аппаратное обеспечение, неотличимое от их реальных аналогов в сети. Как только злоумышленник проникает через периметр сети, он проводит разведку, чтобы составить карту сети, и начинает двигаться в сторону обнаружения потенциальной цели. Сеть, содержащая ложные приманки или искусственно созданный трафик, предоставляет злоумышленнику заманчивые цели в виде учётных данных, необходимых для доступа к другим сетевым сегментам.

Эти приманки приводят злоумышленников к ловушкам, имитирующим физические устройства, такие как серверы или отдельные рабочие станции. По мере того как злоумышленник продвигается дальше по пути приманок, технология Xello Deception продолжает свою работу, позволяя злоумышленнику устанавливать вредоносное ПО в ловушки, создавая иллюзию успешной атаки и одновременно изолируя вредоносное ПО от реальной сети. Продукт позволяет реализовать ловушки в масштабе предприятия, которые смогут обеспечить точный перехват злоумышленника (рис. 2).

При взаимодействии злоумышленника с приманками и ловушками Xello Deception автоматически предупреждает специалистов по информационной безопасности об инциденте и о том, где сейчас находится мошенник и что он сейчас делает, — достаточно лишь зайти в консоль управления в веб-интерфейсе. Быстрое реагирование поможет сократить время нахождения угрозы/злоумышленника в сети организации. Информация о нахождении злоумышленника поможет в дальнейшем понять, какая цель была перед ним, и тем самым усилить защиту данного актива.

Продукт управляется через единую консоль, с помощью которой можно настроить регулярность обновления динамических приманок, ловушек, дополнительных функциональных модулей, проводить мониторинг инцидентов и корректировать события информационной безопасности. Также благодаря Xello Deception можно сократить ресурсы на сбор форензики за счёт регулярного встроенного механизма сбора и анализа данных.

DECEPTION ИЛИ HONEYPOT

Зачастую эти технологии кажутся многим специалистам по информационной безопасности схожими, но хочется прояснить существенную разницу между технологиями Honeypot и Deception:

- Honeypot — пассивный инструмент обмана. Ловушки размещаются в сети и не являются динамичными. Злоумышленнику не составит труда их распознать, поэтому концепция не прижилась на мировом рынке;
- Deception — проактивный обман. Приманки меняются динамически, моделируя реальные имена, учётные записи, ключи аутентификации, конфигурационные файлы критичных систем и т.д., благодаря чему максимально похожи на реалистичные данные об инфраструктуре для злоумышленников. К примеру, серверы-ловушки в Xello (TrapServers или High Interactive Honeypot) в этой парадигме — это лишь часть общей экосистемы обмана, которая является лишь одним из множества встроенных средств детектирования.

В частности, в нашей Deception-системе есть кейс, когда не используются серверы-ловушки, а детектирование инцидентов происходит только через ложные данные и корреляцию аутентификационной информации с единого центра аутентификации, например Active Directory. Это далеко не единственный пример, но очень показательный, который всегда отвечает на вопрос «в чём ваше отличие от классических honeypot и чем вы лучше?».

ВМЕСТО ЗАКЛЮЧЕНИЯ

Технология Deception признана Gartner как одна из перспективных. Российский рынок, как и зарубежный, с интересом смотрит на технологию и активно тестирует новинку. Сценарии использования во многих компаниях разные: кто-то применяет продукт при проведении тестирования на проникновение или Red Team и тем самым повышает качество проведения аудитов, кто-то до конца не понимает, что происходит в сети, и хочет понять ситуацию, а у кого-то были инциденты и важно не допустить новых. Тестируйте новые технологии и защищайтесь от инцидентов по-новому!