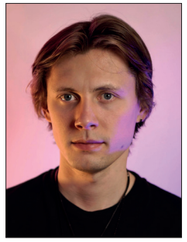

Алексей МАКАРОВ
технический директор Xello

Владимир СОЛОВЬЁВ
руководитель направления внедрения средств защиты АО «ДиалогНаука»

ОБМАНИ МЕНЯ!

ИСПОЛЬЗОВАНИЕ СИСТЕМ КИБЕРОБМАНА ДЛЯ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ СТРАТЕГИИ ИБ

Сегодня не существует универсального решения для выполнения всех задач информационной безопасности. Поэтому при реализации требований ИБ специалистам следует учитывать абсолютно все имеющиеся средства защиты на рынке. При этом комплексные системы, состоящие из решений разных вендоров, чаще всего приводят к разрозненности данных, что создаёт повышенный риск угроз. Чтобы решить данную проблему, необходимо объединение всех средств, методов и мероприятий, используемых для защиты информации, в единый целостный механизм. Что выполнить иногда крайне сложно.

В этой статье рассмотрим использование систем киберобмана (deception) для обеспечения комплексной информационной безопасности в сети компаний.

КИБЕРОБМАН — НОВЫЙ ПОДХОД ВЫЯВЛЕНИЯ КИБЕРУГРОЗ

Системы киберобмана, или решения класса DDP (Distributed Deception Platform), на российском рынке присутствуют уже более семи лет. Но активно использоваться стали только последние два года. Это связано как с ростом количества изощрённых кибератак на российские компании (по данным компании Positive Technologies, в 2022 году 67% успешных атак имели целенаправленный характер), так и с потребностями специалистов ИБ в решениях, выдающих точный результат — без «лишнего шума». Решения, которые выдают большой поток ложноположительных сообщений о потенциальных инцидентах ИБ, требуют больших ресурсов от бизнеса. Актуальной становится также проблема нехватки специалистов с необходимыми навыками в области кибербезопасности.

Обнаружение на основе киберобмана может стать дополнением к обнаружению на основе аномалий. В основе последнего подхода — формирование «нормального поведения» различных компонентов сети — хостов, доступа к данным. Любая активность, которая не соответствует данному поведению, отмечается системой как подозрительная. Этот подход имеет ряд недостатков:

— сети компаний динамичны, поэтому ложные срабатывания происходят с регулярной частотой;

— сбор и хранение всех данных требуют времени и большого количества вычислительных ресурсов.

Системам киберобмана не требуются знания о поведении злоумышленника или атаки. Им не требуются написания сложных правил обнаружения с использованием нестандартных средств. Любой компонент корпоративной сети (информационная система, служба, учётные данные, элемент данных) может быть использован для обнаружения. Киберобман не является частью нормальной работы предприятия или сети и обнаруживается только в результате кибератаки, когда злоумышленник использует ложный актив или данные в ходе своей нелегитимной деятельности.

Таким образом, одной из задач, которую выполняют решения класса DDP, является закрытие слепых зон классических СЗИ.

ТОЧНОСТЬ — РЕШАЮЩЕЕ ЗВЕНО ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССА РЕАГИРОВАНИЯ НА КИБЕРИНЦИДЕНТЫ

Ложноотрицательные результаты работы систем кибербезопасности сегодня являются серьёзной проблемой. Пока аналитики разбираются с бесконечными алертами, злоумышленники успешно остаются незамеченными в сети жертвы в течение длительного времени.

Системы киберобмана используют собственные высокодоверенные индикаторы компрометации сети, что позволяет автоматизировать и усилить процесс реагирования на киберинциденты. Например, при интеграции с песочницей система может автоматически отправлять подозрительные исполняемые файлы для динамического анализа. Для автоматической блокировки или изоляции скомпрометированного хоста потребуется интеграция с системами NAC или EDR.

Также системы киберобмана могут быть использованы для динамического изменения ландшафта инфраструктуры — того, что видит злоумышленник, затрудняя его перемещение к ценным активам. При получении киберинцидента специалисты ИБ могут оценить ситуацию в единой консоли управления, где представлена вся необходимая информация об инциденте. Они могут развернуть дополнительные ложные системы и сервисы на пути злоумышленника, что даст дополнительное время на реагирование.

THREAT HUNTING

Поиск угроз (threat hunting) — это проактивный метод, сочетающий в себе аналитику, инструменты и экспертный анализ разрозненных данных. Как правило, к поиску прибегают, если:

— известно, что сеть уже скомпрометирована, чтобы найти вредоносную активность и изучить её;

— есть гипотеза о том, что сеть скомпрометировали;

— необходимо найти слабые места в защите и системах кибербезопасности.

Основная задача — сократить время присутствия злоумышленника в инфраструктуре (по данным Mandiant, сегодня эта цифра составляет 16 дней). При поиске угроз используется информация из различных источников: внутренних систем ИБ (DDP, EDR, NTA), открытых источников (OSINT).

Системы киберобмана (для выявления вредоносной активности) могут сообщить:

- как злоумышленник получил доступ к инфраструктуре — первоначальная точка компрометации;
- какая учётная запись или система была скомпрометирована;
- с какими другими системами учётная запись или система взаимодействовала до этого;
- список действий злоумышленника на скомпрометированном хосте;
- какое ПО было использовано в рамках реализации кибератаки;
- методы доступа, которые могут стать индикаторами компрометации или тактиками, техниками и процедурами, используемыми в дополнительных действиях по поиску угроз.

Благодаря этому аналитики будут видеть только информацию, относящуюся к инциденту (IOCs и TTPs), тем самым экономя время и снижая необходимость обработки большого количества ненужных данных.

Технология киберобмана и поиск угроз являются составными частями комплексной стратегии кибербезопасности. На данный момент просматривается тенденция интеграции платформ киберобмана в Центры мониторинга и реагирования (Security Operations Platform, или сокращённо SOC). Будучи частью Центра мониторинга и реагирования, они могут дополнять друг друга и способствовать предотвращению киберугроз. SOC может анализировать события от периметровых средств безопасности и развёртывать ловушки и приманки на основе полученных индикаторов. Дополнительно платформы киберобмана имеют возможность сбора и отправки форензики с хоста жертвы для расследования киберинцидентов.

НОВЫЕ ВОЗМОЖНОСТИ XELLO DECEPTION

Компания Xello — разработчик первой российской системы киберобмана. Новая версия Xello Deception значительно расширила возможности:

1. Модуль эмуляции устройств в сети создаёт различные типы устройств конкретных производителей в сети компании (периферийные, сетевые и специализированные). Устройство также может быть связано с интерактивным сервисом, когда злоумышленнику предоставляется возможность, например, ввода реальных команд в терминале SSH. Это позволяет увести злоумышленника от реальных ИТ-активов на ложные. Типы имитационных устройств:

- сетевые: коммутаторы, маршрутизаторы, межсетевые экраны различных производителей (Fortinet, Check Point, Cisco, Huawei);
- рабочие станции и серверы: Windows OS (7, 8, 10), Windows Server (2012, 2016), Debian, Ubuntu, CentOS;
- специализированные: медицинское оборудование, финансовые терминалы;
- мобильные устройства на базе ОС Android;
- интернет вещей (IoT): IP-камеры, видеорегистраторы, принтеры и МФУ.

Также модуль позволяет эмулировать различные типы уязвимостей в ложных устройствах, сервисах и приложениях.

Актуальность модуля обусловлена в первую очередь ростом количества атак на подобные устройства. Например, по данным Лаборатории Касперского, количество атак на IoT-устройства в России выросло на 40% за первое полугодие 2022 года. Крупные компании с обширным парком оборудования зачастую не знают о количестве устройств в сети и параметры их конфигурации. Некоторые из них могут иметь доступ в интернет, что открывает дополнительный вектор для кибератак.

Модуль функционирует наравне с реализованными хостовыми приманками и ловушками и дополняет их.

2. Модуль для компаний с филиальной структурой позволяет гибко управлять ложным слоем данных на распределённых площадках.

3. Детектирование MiTM-атак (Man-in-the-Middle). Модуль выявляет нелегитимные действия с перехватом пользовательских данных на сетевом уровне. Злоумышленники эксплуатируют протоколы LLMNR, mDNS, NBT-NS в ходе реализации кибератак. Платформа в режиме реального времени выявляет вредоносную активность, связанную с данными протоколами.

4. Получение событий аутентификации из Apache Kafka. Крупные компании уходят от windows-инфраструктуры в сторону соответствующих решений на базе ОС Linux или с открытым исходным кодом. Платформа интегрируется с подобными решениями, подписывается на сообщения и выполняет поиск событий, которые связаны с ложными активами, распространёнными в сети ранее. Для интеграции не требуются дополнительные ресурсы в виде сервера управления. Это одна из особенностей систем киберобмана, отличающая их от классических ханипотов (ловушек).

Платформа Xello Deception на рынке уже более четырёх лет и имеет большой набор различных типов приманок и ловушек. Реализовано большое количество функциональных возможностей для различных инфраструктур. Логичным решением стал переход на модульную архитектуру.

ЗАКЛЮЧЕНИЕ

В сочетании с традиционными средствами защиты периметра система киберобмана дополнит и улучшит стратегию активной защиты, усложнив работу злоумышленникам, а также станет для них сдерживающим фактором на пути к ценным активам бизнеса.

Консолидация и интеграция продолжают набирать обороты, так как специалисты ИБ стремятся сократить разрыв в квалификации и добиться максимально быстрого реагирования. Xello Deception, накопив опыт работы с различными инфраструктурами, позволяет гибко интегрироваться как со сторонними системами защиты, так и с внутренней инфраструктурой компании для более эффективной работы.