xello

Предотвращение целенаправленных атак с помощью технологии кибероблана

Участник

Московский инновационный кластер

Основной особенностью **Xello Deception** является возможность выявления нелегитимных действий, даже если злоумышленник уже проник в корпоративную сеть.

ТЕХНОЛОГИЯ КИБЕРБОБМАНА — НОВЫЙ ПОДХОД ВЫЯВЛЕНИЯ УГРОЗ

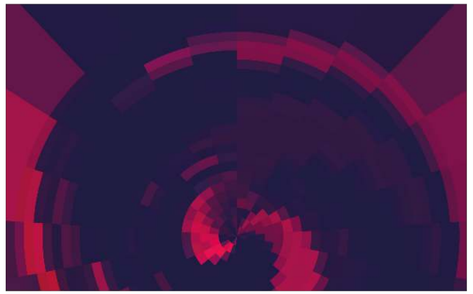
Чтобы выявить нелегитимные действия в корпоративной сети предприятия и предотвратить кибератаку, технология не использует каких-либо предварительных знаний: индикаторы компрометации или атак (IoC, IoA), сигнатуры, репутационные списки, определенное зловредное поведение и другие. Она ориентирована на введение злоумышленника в заблуждение, предоставляя ему ложные данные и сервисы с целью детектирования его действий.

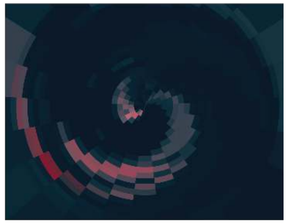
Это возможно благодоря приманкам (англ. lures) и ловушкам (англ. decoys или traps), которые создают инфраструктуру из ложных активов. Приманками могут являться конфигурационные файлы, учетные записи, сохраненные пароли в памяти ОС или браузерах и другие. Ловушки представляют собой эмуляции реальных элементов ИТ-инфраструктуры компании (ОС, базы данных, приложения и другие).

Полностью автоматизированные Deception-платформы дают представление о вредоносной активности в корпоративной сети, которая может быть невидима для других средств защиты. При взаимодействии злоумышленника с ложным слоем данных автоматически отправляются уведомления (алерты).

Приманки и ловушки невидимы для авторизованных пользователей и направлены исключительно на злоумышленника, поэтому подобный алерт с высокой долей вероятности будет считаться инцидентом безопасности, а не ложным срабатыванием.

Они грамотно распределяются среди рабочих ИТ-активов компании, покрывая всю сеть, так что злоумышленник не имеет шанса избежать их.





21 день

медианное время присутствия злоумышленника в инфраструктуре

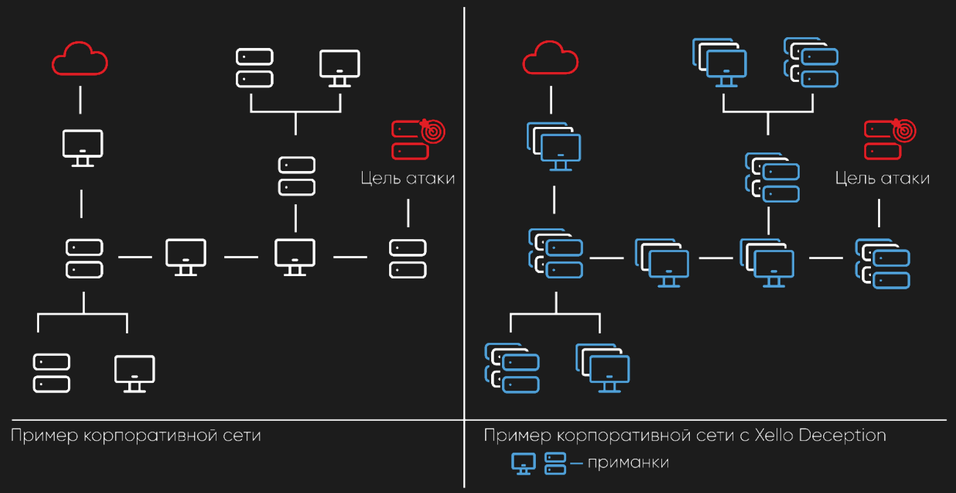
ПРИМЕРЫ ИМИТАЦИОННЫХ АКТИВОВ:

- ИТ-серверы
- Сетевые устройства
- Хранилища и базы данных
- IoT-устройства
- Учетные записи пользователей
- Сохраненные подключения к ресурсам
- Ветки реестра ОС и стороннего ПО
- Ключи от ИТ-систем
- И другие

*M-Trends 2022 Mandiant special reports // Mandiant

РЕШАЕМЫЕ ЗАДАЧИ

- Предотвращение целенаправленных атак (APT)
- Ускорение процесса реагирования за счет выявления только реальных инцидентов
- Сокращение времени разбора инцидента благодаря неприрывному сбору и хранению данных форензики
- Снижение нагрузки на специалистов кибербезопасности за счет минимизации количества ложных срабатываний
- Повышение эффективности существующих систем защиты: SIEM, EDR, NGFW и других
- Оптимизация стратегии кибербезопасности



ОСОБЕННОСТИ XELLO DECEPTION

01 Адаптивная генерация приманок

Современные сети отличаются быстрой изменчивостью и динамичным развитием. Именно поэтому Xello Deception регулярно обновляет приманки с учетом текущих особенностей инфраструктуры компании. Система тщательно анализирует модель поведения каждого пользователя. Независимо от конфигурации и предназначения защищаемого хоста (компьютер бухгалтера, сервер базы данных или ноутбук разработчика и другие) подбирает приманки такого типа, программное обеспечение которого используется на этом хосте.

02 Простое внедрение и отсутствие дополнительной нагрузки на инфраструктуру

Xello Deception не использует хостовой агент для распространения приманок и поддержания связи с сервером, поэтому не оказывает дополнительной нагрузки на реальную инфраструктуру компании. Приманки распространяются с помощью различных протоколов удаленного взаимодействия (WMI, WinRM, SSH и других). Также для Xello Deception можно задействовать системы управлением ПО (SSM, GPO, Ansible, JAMF, Puppet и другие). Вся информация о распространенных по сети приманках хранится в системе. Их удаление не влияет на инфраструктуру.

03 Интеграция с существующими системами защиты

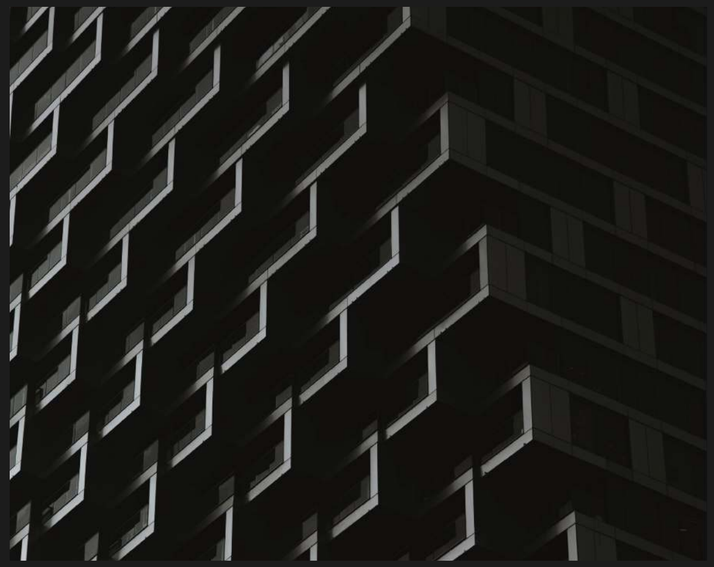
Открытий API позволяет повысить эффективность большинства систем защиты.

04 Единая консоль управления

Результаты работы платформы отражены в единой консоли управления. С ее помощью можно управлять приманками на защищаемых хостах и настраивать индивидуальные политики защиты. Консоль позволяет производить маппинг инцидентов по модели MITRE ATT&CK.

05 Модуль цифровой гигиены Credential Defender

Модуль позволяет управлять группами локальных администраторов, очищать закэшированные учетные данные пользователей (в том числе привилегированных), производить мониторинг теневых администраторов.



ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ:

- Поддержка инфраструктуры виртуальных рабочих мест (VDI)
- Поддержка операционных систем: **Windows, Linux, MacOS**
- Поддержка терминальных серверов
- Сбор и хранение форензики

МЕСТО XELLO DECEPTION ПРИ ЦЕЛЕНАПРАВЛЕННОЙ АТАКЕ

Целенаправленная или APT-атака характеризуется направленностью на определенный объект, продолжительностью и тщательным планированием.
Ее целью может стать компания, отрасль или частное лицо. Успех реализации всегда высок, поскольку киберпреступники тщательно исследуют свою жертву и на основе полученных данных планируют дальнейшие действия. Помимо этого, злоумышленники обладают финансовыми ресурсами и техническими возможностями.

Xello Deception может использоваться для прерывания цепочки атаки, ее продления, истощения ресурсов злоумышленника и для выявления деталей (инструментов) реализации атаки.

О КОМПАНИИ

Xello (Кселло) — команда, которая занимается развитием первой российской платформы для предотвращения атак с помощью технологии киберобмана (Deception). Решение относится к классу Distributed Deception Platform, DDP.

Компания основана в 2018 году. Первый коммерческий релиз Xello Deception состоялся в 2019 году. До этого времени команда в течение длительного времени занималась исследованиями технологии киберобмана и различных ловушек (honeypot).

Сегодня платформа зарекомендовала себя как эффективный инструмент для решения различных задач по информационной безопасности: от повышения защищенности корпоративной сети компании до ускорения процесса реагирования на киберинциденты.

Чтобы получить консультацию или бесплатно протестировать платформу Xello Deception, свяжитесь с нами удобным для вас способом:

+ 7 (495) 786 03 35 info@xello.ru

xello.ru

xello

Xello – первый разработчик российской Deception-платформы

Контакты:

+ 7 (495) 786 03 35

info@xello.ru