xello Deception

ОБЗОР РЕШЕНИЯ

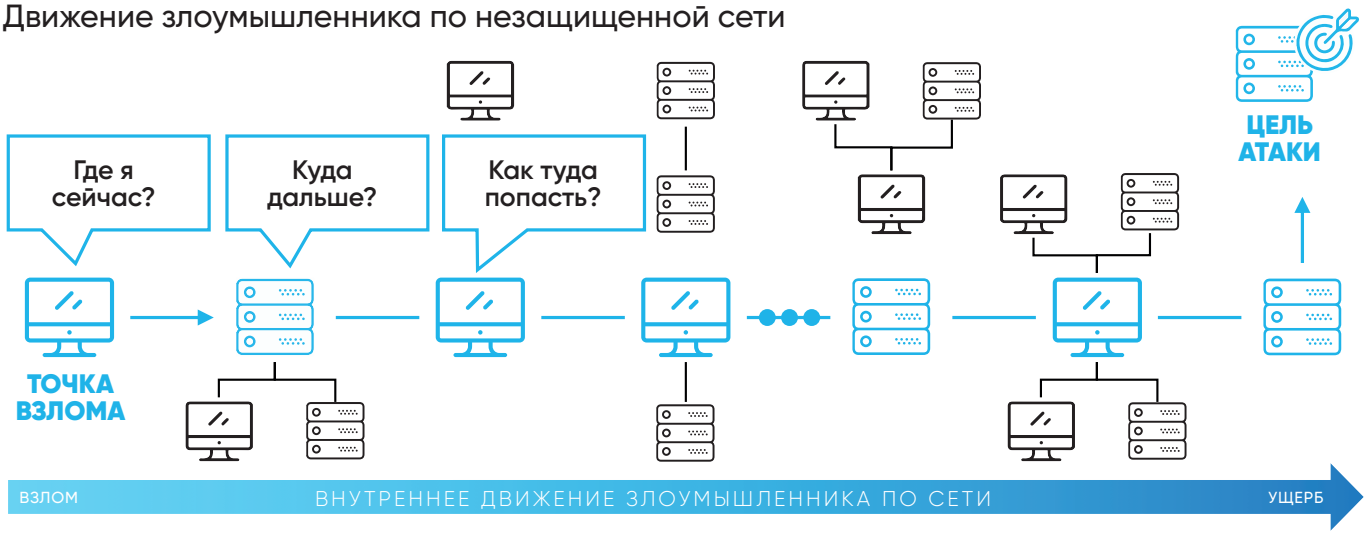
ТЕХНОЛОГИЯ DECEPTION – последний рубеж защиты

Технология Deception является наиболее эффективным способом обнаружения APT-атак, так как она использует тактику атакующих против них. Используя ловушки и приманки с высоким уровнем интерактивности, Deception обманывает злоумышленников, заставляя их раскрывать себя, тем самым закрывая те угрозы, с которыми не справились другие средства защиты. Используя такие приманки, как: учетные данные пользователей, серверы, сайты, вы можете обнаружить хакеров до того, как им станет доступна конфиденциальная информация.

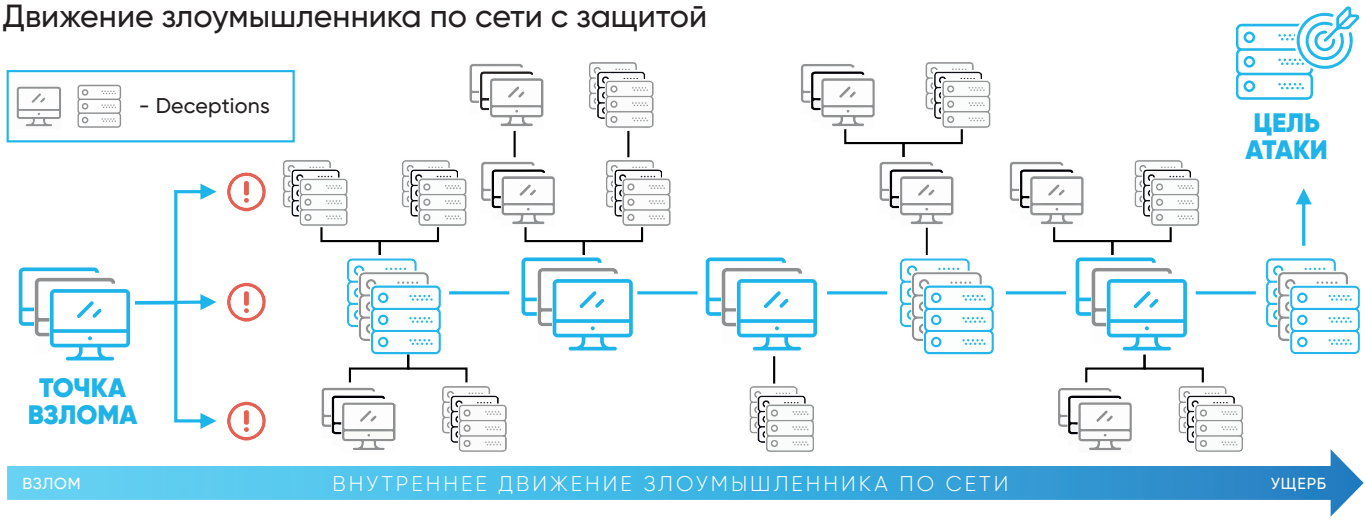
В 2019 году многие аналитики снова признали эффективность технологии Deception в обнаружении продвинутых угроз, и Gartner, Inc. четвертый год подряд рекомендует использовать Deception в качестве главного стратегического приоритета безопасности. Различные недавние исследования также зафиксировали намерение рынка добавить технологию Deception к своим средствам контроля безопасности, учитывая ее эффективность и оперативность в сдерживании злоумышленников.

Gartner

Движение злоумышленника по незащищенной сети



Движение злоумышленника по сети с защитой



Адаптивные приманки – интеллектуальная защита

Для того чтобы остановить даже самые современные атаки, приманки и ловушки должны прекрасно вписываться в сеть и адаптироваться, даже без использования агентов по мере изменения среды. Чтобы быть всегда на шаг впереди, современные и оптимизированные для инфраструктуры приманки автоматически и динамически создают ложный слой информации на всей вашей сети, не оказывая влияния на ИТ-структуру.

Постоянно создавая среду, в которой злоумышленники не могут отличить реальную информацию от поддельной, приманки обеспечивают постоянную ненадежность сбора данных злоумышленниками. Благодаря этому, злоумышленники не могут опереться на собранные данные, и не могут продолжать атаку.

Единая централизованная система управления

Xello Central Management - это соответствие лучшим мировым практикам и наивысшим отраслевым стандартам. Управляйте всеми приманками/ловушками на защищаемых хостах, без использования агента.

XCM автоматически создает оптимизированную ложную поверхность для вашей сети. XCM занимается созданием, размещением и динамической модификацией приманок/ловушек, распространяя их по сети без влияния на инфраструктуру, чтобы создать наиболее эффективный уровень защиты.

Защита корпоративной сети стала проще

Для того, чтобы извлечь выгоду из действенных и надежных оповещений, Xello предлагает ловушки, созданные специально под вашу инфраструктуру, которые не будут прерывать работу вашей ИТ и ИБ команд. Эффективное решение «Из коробки», автоматическое обнаружение и мгновенный анализ AD, моментальное создание приманок и безагентский способ их распространения обеспечивают отсутствие сбоев в работе пользователей.

По мере изменения и развития вашей организации Xello Deception будет адаптироваться, для обеспечения обнаружения атак в начальной стадии. Размещая приманки в новых местах и обновляя их для адаптации к изменениям, Xello Deception постоянно следит за вашей сетью и адаптирует защиту, чтобы предоставить инструменты, которые будут развиваться вместе с вашей организацией.

Xello: приманки и ловушки повсюду

Xello находит злоумышленников используя их сильные стороны против них. Наше решение создает обманный слой по всей вашей сети, создавая среду, в которой злоумышленники не могут полагаться на собираемую ими информацию. Если хакеры не могут собрать достоверную информацию, они не могут принимать правильные решения, что приводит к их быстрому обнаружению.

xello Deception

Преимущества:
- Отсутствие агента на рабочих станциях и серверах
- Первое и единственное Российское решение такого класса
- Не позволяет злоумышленникам отличить реальные данные от Приманок и Ловушек
- Увеличение обнаружения атак с помощью оптимального размещения Приманок
- Постоянный контроль сети и адаптивная защита
- Отсутствие обслуживания и перебоев в работе компании
- Минимальное влияние на IT инфраструктуру
- Автономная система без использования других инструментов
- Распространение Приманок и Ловушек одним кликом мыши
- False positive стремится к нулю

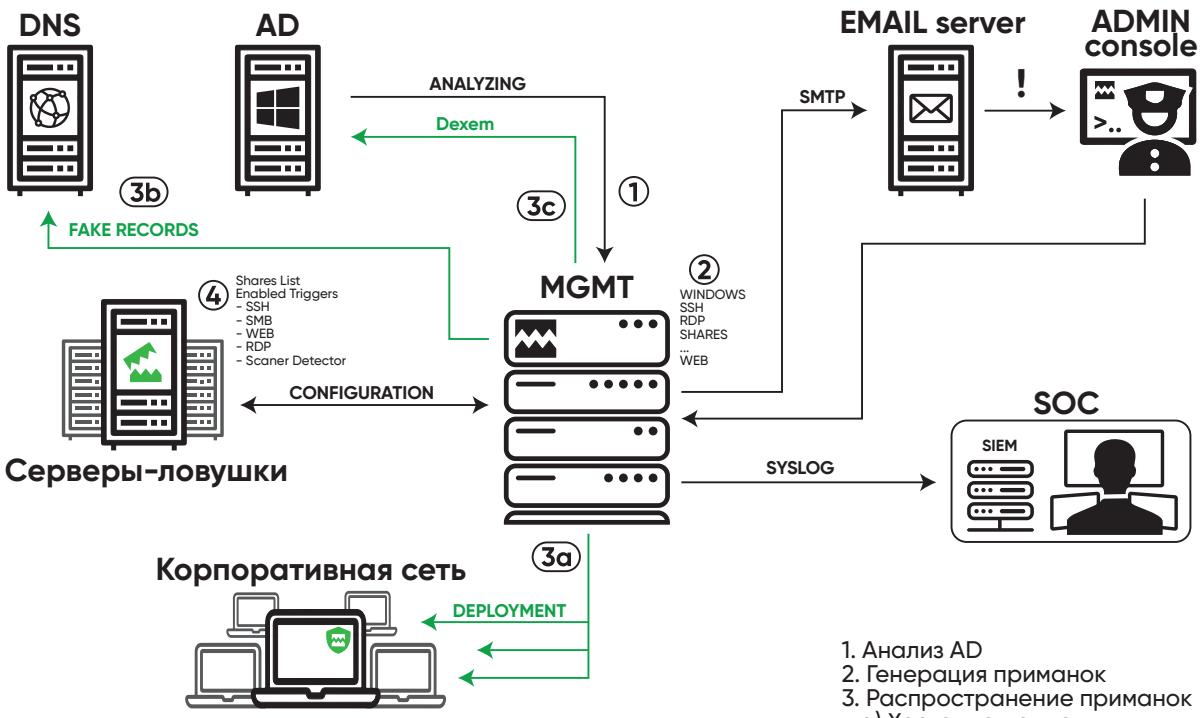
Низкий False positive – новый уровень эффективности SOC

Так как приманки не видны для обычных пользователей, то наличие ложных оповещений стремится к нулю; каждое уведомление об использовании приманки является высокоточным признаком атаки.

Оповещения возникают в режиме реального времени только при подтвержденном взаимодействии злоумышленника с приманкой и, в отличие от других методов обнаружения, не зависят от сигнатур или поведенческого анализа для обнаружения атаки. Оповещения сразу передаются в SIEM, что можно использовать для автоматизации блокировки злоумышленника и/или изоляции зараженных хостов чтобы компания могла полностью устранить угрозу в сети. Ложные срабатывания исключены, а высокоточные оповещения экономят драгоценное для SOC время.

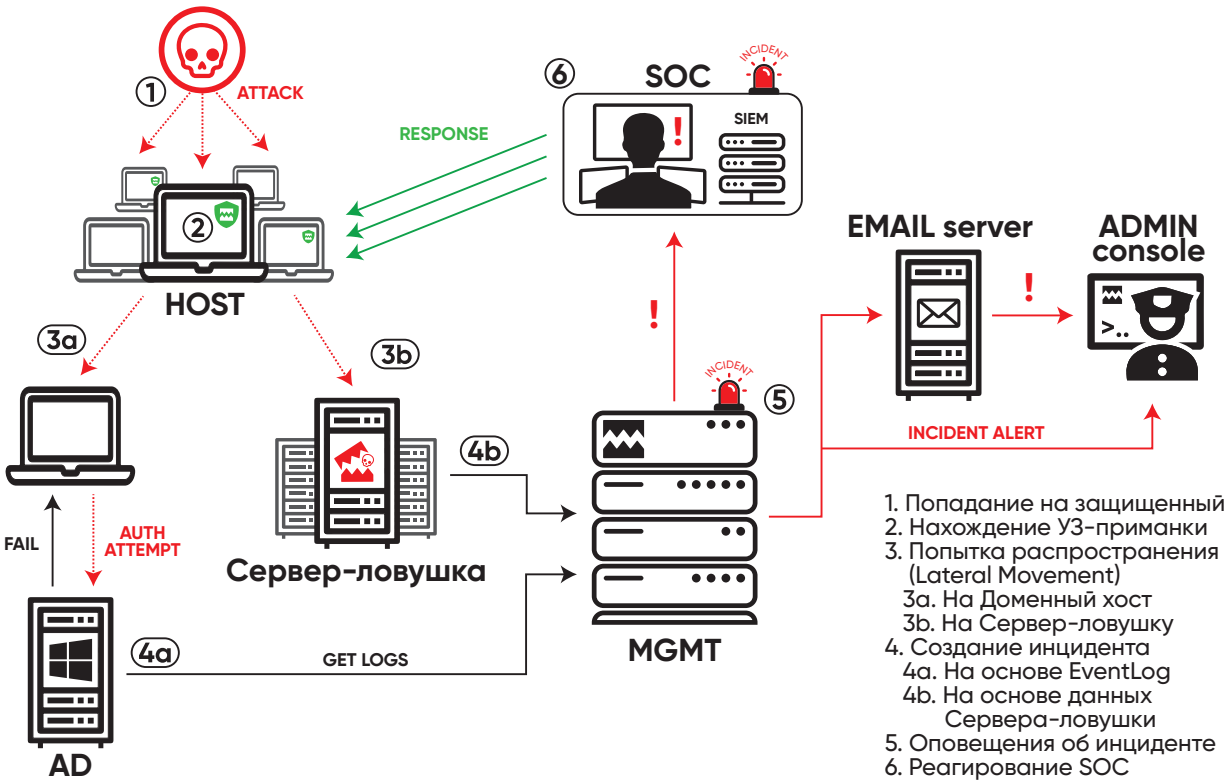
ООО «Кселло»
xello.ru info@xello.ru
+7 495 786 03 35

Архитектура Xello Deception



1. Анализ AD
2. Генерация приманок
3. Распространение приманок
   a) Хостовые приманки
   b) DNS-Алиасы
   c) Dexem-создание
4. Конфигурация Серверов-ловушек

Сценарии реагирования



1. Попадание на защищенный хост
2. Нахождение УЗ-приманки
3. Попытка распространения (Lateral Movement)
   3a. На Доменный хост
   3b. На Сервер-ловушку
4. Создание инцидента
   4a. На основе EventLog
   4b. На основе данных Сервера-ловушки
5. Оповещения об инциденте
6. Реагирование SOC