КРАТКИЙ ОБЗОР ПРОДУКТА

DeceptionGrid™ 6.0

Знакомство с DeceptionGrid. Что это?

В современном мире вопрос проникнут ли взломщики в ваши сети уже не стоит. Вопрос только в том, когда и как часто это будет происходить. Преступники используют все более сложные техники для преодоления средств защиты периметра и конечных точек.

Как узнать, что взломщик проник в вашу сеть? Как его быстро вычислить? Какие у него намерения? Насколько быстро вы сможете остановить атаку и вернуться к нормальной работе?

Архитектура TrapX Deception in Depth дает ответы на эти важные вопросы с помощью мощной технологии DeceptionGrid для дезинформации, отвлечения и обнаружения изощренных преступников на каждом этапе..

DeceptionGrid — это полный набор техник маскировки, включая создание автоматических ложных маркеров (приманок), а также ловушек со средним и высоким уровнем взаимодействия (ложных целей). Она привлекает атакующих путем внедрения скрытых ловушек и маркеров в ваши реальные IT-ресурсы. Наши ловушки выглядят во всех смыслах идентично вашим реальным рабочим IT-активам и подключенным устройствам интернета вещей (IoT). Deception in Depth идет еще дальше и дезориентирует злоумышленников, создавая и поддерживая имитацию реального сетевого трафика между нашими ловушками.

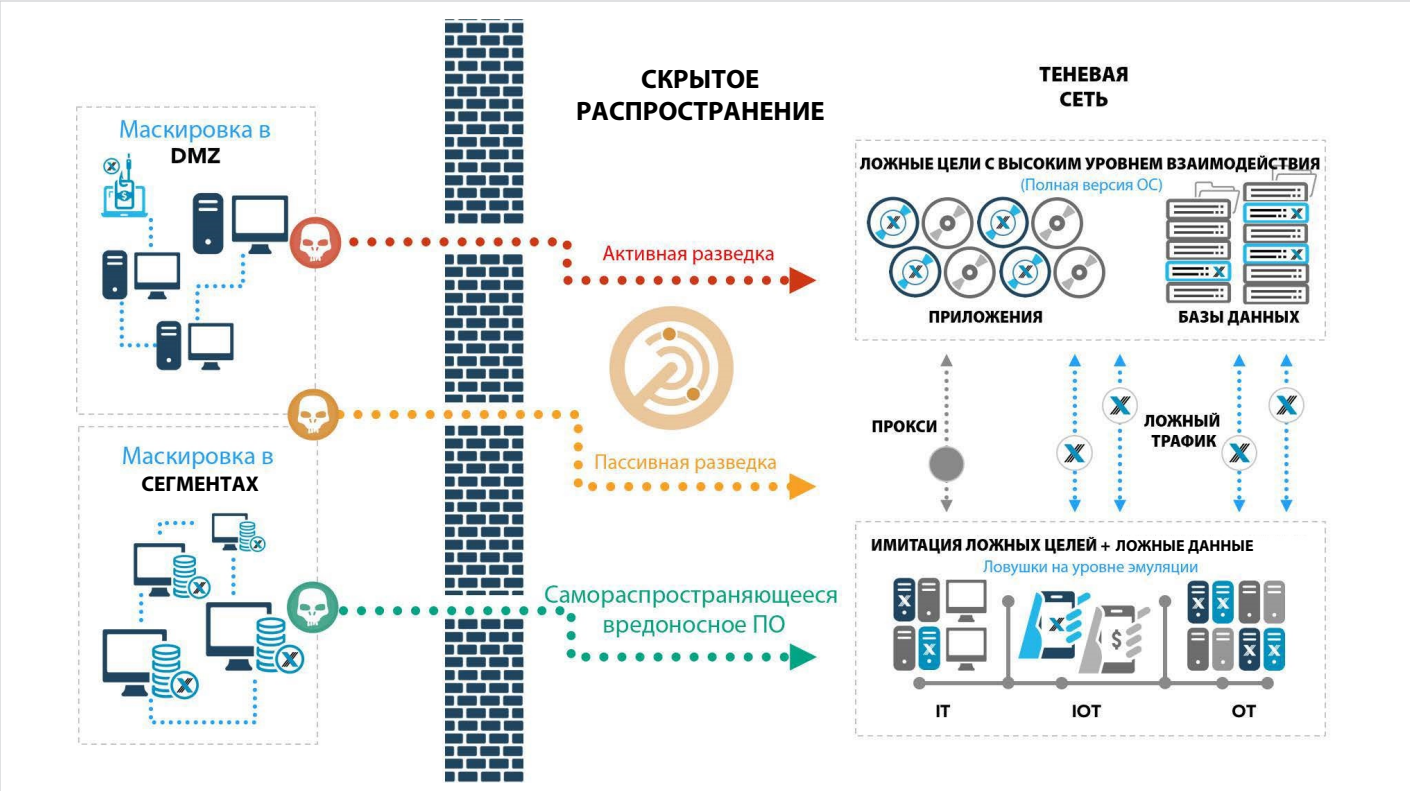
DeceptionGrid динамически дезинформирует, отвлекает и обнаруживает взломщиков на всех этапах атаки.

Когда кибер-взломщики проникают в сеть предприятия, они начинают скрытно перемещаться, захватывая новые и новые цели, в поисках пути к интересующих их активам. DeceptionGrid динамически дезинформирует, отвлекает и обнаруживает злоумышленников на всех этапах атаки. Всего одно взаимодействие взломщика с любым элементом DeceptionGrid генерирует эффективный сигнал тревоги. DeceptionGrid интегрируется с ключевыми элементами сетевой инфраструктуры и экосистемы безопасности, сдерживая атаки и обеспечивая быстрый возврат бизнеса к нормальному режиму работы.

Deception in Depth — Оптимальная архитектура

TrapX Deception in Depth сочетает в себе разнообразные возможности маскировки для отвлечения, дезинформирования и обнаружения взломщиков, предлагая им целую сеть ложных векторов атак. Такая многоуровневая архитектура создает привлекательную с точки зрения взломщиков среду внутри сети. Везде, куда бы они не направились, они будут моментально обнаружены.

Такие приманки, как кэшированные пароли, связи с базами данных, серверами, сетевые ресурсы и прочее привлекают взломщиков в ловушки. С помощью наших smart deception прокси мы можем расширить нашу систему и привести атакующих на наши мониторинговые серверы, которые позволят собрать наиболее полную информацию о тактике и инструментарии атакующих.



Архитектура DeceptionGrid

Высокая точность — Минимум ложных срабатываний

На крупных предприятиях стандартные технологии кибер-защиты, такие как файрволы и Endpoint Security, решения могут генерировать тысячи или даже миллионы оповещений в день, требуя огромные ресурсы для качественной их обработки. К сожалению, всего одно успешное проникновение может легко потеряться в этом потоке информации и поставить под угрозу всю сеть.

DeceptionGrid использует другой подход. В отличие от традиционных средств, которые генерируют сигналы тревоги основываясь на сигнатурах или математических расчетах уровня риска, оповещения DeceptionGrid бинарны. Взломщики либо пытаются попасть в наши ловушки, либо нет. Если они соприкасаются с ловушкой, мы знаем, что это взлом, с вероятностью почти 100 процентов.

Основные компоненты DeceptionGrid

Основные функции DeceptionGrid – DeceptionGrid сканирует вашу действующую сеть и разворачивает от сотен до тысяч компонентов маскировки. Маркеры маскировки или приманки, выглядящие как обычные файлы, закладки, ссылки, базы данных, встраиваются в реальные IT-активы. Ловушки — ложные цели, которые имитируют серверы, рабочие станции, сетевые коммутаторы и пр. — внедряются быстро, включая специальные ложные цели, имитирующие медицинские устройства, банкоматы, торговые терминалы, компоненты финансовой сети SWIFT™ и пр.

Полностью автоматизированный ретроспективный анализ – автоматизация в реальном времени изолирует инструменты и вредоносное ПО взломщика и может передавать их в «песочницу» для расширенного анализа. Мы сочетаем дополнительные интеллектуальные аналитические возможности с действиями ловушек и обеспечиваем оперативную комплексную оценку рисков для вашей команды центра обеспечения безопасности. Интеллектуальный анализатор сети DeceptionGrid проводит анализ исходящего трафика и в сочетании с анализом действий ловушки, составляет полную картину активов под угрозой и действий взломщика.

Модуль AIR —модуль AIR, разработанный для быстрого автоматизированного анализа скомпрометированных точек, является основным компонентом DeceptionGrid и ключевой частью нашей архитектуры Deception in Depth.

Автоматизированный анализ запускается при наличии признаков угрозы (IOC), определяемых DeceptionGrid, которые чаще всего указывают на скомпрометированные ПК. Модуль AIR выполняет комплексный, полностью автоматизированный анализ любых рабочих мест, после чего загружает артефакты из конечных точек в модуль AIR, где они анализируются. После этого предоставляется результат в виде отчета.

Встроенное управление событиями и разведка угроз безопасности — вся информация передается в систему управления, помечается уникальным ID и сохраняется во встроенную базу данных управления событиями. Сервис сетевой аналитики следит за исходящей активностью на реальных узлах, основываясь на информации о вредоносных действиях, выявленных в системах постановки ложных целей.

Модуль CryptoTrap™ — CrytoTrap представляет собой еще один важный компонент DeceptionGrid и ключевую часть нашей архитектуры Deception in Depth. Модуль CryptoTrap разработан с целью активного противодействия программам-вымогателям на раннем этапе цикла работы, останавливая взлом, тем самым защищая ценные ресурсы. Ловушки создаются таким образом, что программы-вымогатели считают их ценными сетевыми ресурсами. Клиенты могут также предоставлять собственные ложные данные, чтобы информация выглядела более естественно. CryptoTrap оперативно реагирует на программы-вымогатели, сдерживает их распространение отключая источник атаки.

DeceptionGrid использует другой подход. В отличие от методов файрволов и Endpoint Security, которые генерируют сигналы тревоги основываясь на вероятности, сигналы DeceptionGrid бинарны. Взломщики либо пытаются попасть в наши ловушки, либо нет. Если они соприкасаются с ловушкой, мы знаем, что это взлом, с вероятностью почти 100%.

Развертывание в облаке или на объекте

Система DeceptionGrid разработана для быстрого развертывания и соответствует требованиям даже самых крупных предприятий. В большинстве случаев автоматизация позволяет командам IT-специалистов выполнять полное развертывание в течение всего нескольких часов. Также мы можем реализовать DeceptionGrid через поставщиков услуг по управлению информационной безопасностью (MSSP). Консоль управления DeceptionGrid предоставляет поддержку MSSP для мониторинга состояния большого количества клиентов.

Автоматизация для обслуживания крупных предприятий

Система DeceptionGrid создана с целью преодоления ограничений стандартных способов защиты, инструментов, основанных на анализе сигнатур, традиционных IDS и "хинапотов". Наша многоуровневая архитектура Deception in Depth включает мощные возможности автоматизации для масштабирования, что важно для поддержки крупных предприятий и правительственных систем без огромных затрат на ручную настройку отдельных маскировочных узлов.

Партнерская экосистема

DeceptionGrid обеспечивает профессиональный анализ с применением облачных технологий, доступный для использования всей нашей партнерской экосистемой. Мы доверяем нашим партнерам принимать решения в отношении безопасности на основании этих данных, привлекать клиентов, управлять средой заказчиков и помогать им добиваться выдающихся конкурентных преимуществ.

Комплексное обслуживание и поддержка

Программа обслуживания и поддержки TrapX создана с целью помогать вам опережать взломщиков на несколько шагов с помощью TrapX. Наши проактивные сервисы для развертывания профессиональной технологии маскировки помогут вам выявить и устранить угрозы, которые чаще всего оказываются незаметными для других решений кибербезопасности, гарантируя наивысший уровень защиты ваших основных активов.

Ключевые отличия

- Более быстрое обнаружение в реальном времени действий кибер-взломщиков в любой точке вашей локальной сети и облачной среды.
- Больше никаких лишних сигналов тревоги. Сигнал TrapX точен и эффективен более чем на 99%.
- Комплексный автоматизированный анализ выявления вредоносного ПО и инструментов взломщиков.
- Автоматическое развертывание тысяч ловушек DeceptionGrid при минимальных ресурсах.
- Предоставляет всё необходимое для центров обеспечения безопасности, чтобы максимально оперативно реагировать на угрозы.
- Мощная технология симуляции позволяет маскировать ловушки под специализированные устройства, включая медицинское оборудование, банкоматы, торговые терминалы, устройства интернета вещей (IoT) и многое другое.
- Модуль эффективного реагирования на событие (Advanced Incident Response, AIR) выполняет автоматический анализ памяти скомпрометированных хостов.
- Архитектура Deception in Depth объединяет преимущества маркеров, ложных ловушек, ловушек FullOS и нашей функции активных сетей в одну многоуровневую архитектуру для оперативного обнаружения, эффективного отвлечения взломщиков и комплексного сдерживания угроз.
- Комплексная интеграция с партнерами позволяет создать законченный цикл устранения угроз и сохраняет ваши инвестиции в средства обеспечения безопасности.

Ключевые преимущества системы DeceptionGrid

- **Нацелена на новое поколение кибер-взломщиков.** Технология Deception находит наиболее продвинутых взломщиков, которых неспособны обнаружить имеющиеся поставщики решений и которые могут уже находиться в вашей сети.
- **Сокращает или устраняет убытки.** Точное и оперативное обнаружение снижает риск убытков в результате разрушения активов предприятия, кражи данных и общего влияния на бизнес операции.
- **Сокращает время, необходимое для обнаружения взлома.** Профессиональная экспертиза и анализ в реальном времени в сочетании с высокой точностью уникальным образом дает вашему центру обеспечения безопасности возможность максимально оперативно реагировать на все атаки внутри сети.
- **Максимальная видимость и охват.** Defense in Depth обеспечивает максимальный уровень видимости внутри сети, обнаруживая действия взломщиков, и тем самым препятствуя взлому.
- **Повышает степень соответствия стандартам,** удовлетворяя требованиям законов об утечке данных PCI и HIPAA, а также прочим нормативным требованиям различных стран.
- **Минимальные расходы на реализацию.** Deception in Depth обеспечивает максимальный охват инфраструктуры при минимальных затратах со стороны вашего предприятия.
- **Защита инвестиций.** Технология Deception может интегрироваться с имеющимися решениями других поставщиков.

О КОМПАНИИ

Компания TrapX создала новое поколение технологии маскировки, обеспечивая обнаружение и предотвращение взломов в реальном времени. Наше решение, доказавшее свою эффективность на практике, противодействует потенциальным взломщикам с помощью созданных «под ключ» ложных целей (ловушек), «имитирующих» ваши реальные активы. При небольших усилиях можно внедрить сотни или даже тысячи ловушек, тем самым создав виртуальное минное поле для кибер-атак, которое будет немедленно уведомлять вас о любых вредоносных действиях, предоставляя достоверные разведданные. Наши решения позволяют нашим клиентам оперативно изолировать, обнаруживать и обезвреживать новые атаки нулевого дня и APT в реальном времени.

Тысячи клиентов по всему миру, включая правительственные органы, силовые ведомства, крупнейшие глобальные компании в сфере здравоохранения, финансов, производства, энергетики доверяют свою безопасность TrapX Security.

Softprom by ERC
Официальный дистрибьютор TrapX Security

trapx@softprom.com
www.softprom.com