Trend Micro™

DEEP DISCOVERY™ EMAIL INSPECTOR

Останавливает направленные атаки по электронной почте и предотвращает потерю данных или проникновение программ-вымогателей

Направленные атаки и сложные угрозы способны обходить традиционные средства защиты и извлекать конфиденциальную информацию или зашифровывать критические данные и требовать выкуп. По данным исследования Trend Micro, более 90 % таких атак начинаются с целевого фишингового сообщения с вредоносным вложением или URL-адресом, которые стандартные средства защиты электронной почты или конечных устройств не обнаруживают.

Deep Discovery Email Inspector использует усовершенствованные средства обнаружения, чтобы выявить и заблокировать целевые фишинговые письма, через которые ничего не подозревающие сотрудники зачастую получают вредоносный код и программы-вымогатели. Email Inspector отлично дополняет работу защищенного почтового шлюза, безотказно обнаруживает и блокирует специально составленные целевые фишинговые письма (которые обычно заносят вредоносные вложения и URL-адреса при направленных атаках), а также сложные угрозы и программы-вымогатели. Deep Discovery Email Inspector можно развернуть в режимах MTA (блокировка), BCC (только мониторинг) или SPAN/TAP.

КЛЮЧЕВЫЕ ФУНКЦИИ

Прозрачность
Безупречно работает с имеющимся фильтром спама или защищенным почтовым шлюзом и обнаруживает направленные фишинговые атаки по электронной почте, которые используют вложения и ссылки, чтобы спрятать вредоносные программы, в том числе программы-вымогатели (часто скрытые в макросе).

Усовершенствованные методы обнаружения
Обнаруживает эксплойты нулевого дня, сложные угрозы, программы-вымогатели и вредоносное поведение. Выявляет известные и неизвестные угрозы с помощью таких методов, как проверка репутации файлов, IP и сайтов, статический анализ, эвристический анализ, анализ алгоритмов и пользовательских «песочниц». Таким образом, локальная аналитическая информация об угрозах сравнивается с информацией об угрозах компании Trend Micro.

Гибкость
Доступны следующие варианты развертывания: встроенная блокировка или карантин, регистрация или удаление обнаруженной угрозы из электронной почты и уведомление пользователя.

Анализ «песочницы»
Использует виртуальные образы, которые настроены так, чтобы точно соответствовать конфигурациям вашей системы, драйверам, установленным приложениям и языковым версиям. Такой подход позволяет лучше обнаруживать сложные угрозы, которые обходят стандартные виртуальные образы. Среда «песочницы» включает безопасный внешний доступ в режиме реального времени для идентификации и анализа многоэтапных загрузок, URL-адресов, командных серверов и т. д. Возможности «песочницы» предлагаются как часть интегрированного устройства или как масштабируемая автономная возможность.

Защита от атак программ-вымогателей
С момента запуска направленной фишинговой атаки до момента, когда первый пользователь откроет письмо, проходит всего одна минута 40 секунд. Учитывая факт, что электронная почта — это тот вектор угроз, через который в сеть попадают программы-вымогатели, все пользователи вашей организации подвержены риску.

Ключевые преимущества

Улучшенная защита

- Останавливает целевые фишинговые письма, с которых начинается большинство направленных атак.
- Обнаруживает программы-вымогатели до того, как они навредят организации.
- Находит угрозы, невидимые для стандартных средств защиты электронной почты, благодаря использованию настраиваемых «песочниц».

Существенная рентабельность инвестиций

- Останавливает направленные фишинговые атаки и программы-вымогатели, что позволяет избежать дорогостоящего восстановления.
- Безупречно работает с имеющимися решениями по защите электронной почты.
- Предоставляет сведения об индикаторах компрометации другим решениям, обеспечивающим безопасность сети и конечных устройств.

Email Inspector обнаруживает и блокирует попытки проникновения программ-вымогателей, так как:

- находит известные программы-вымогатели с помощью анализа шаблонов и репутационных списков;
- обнаруживает неизвестные программы-вымогатели с помощью создания цифровых отпечатков, эмуляции скриптов, эксплойтов нулевого дня, целевых и защищенных паролем вредоносных программ;
- настраиваемая «песочница» позволяет обнаруживать массовые изменения в файлах, признаки шифрования данных и изменения в резервных копиях.

Когда программы-вымогатели обнаружены, они блокируются и не доходят до получателя, а значит, не шифруют данные. Deep Discovery Email Inspector может автоматически сообщать сведения об индикаторах компрометации средствам управления сетью и конечными устройствами, чтобы остановить последующие атаки.

Deep Discovery Email Inspector является частью решения Trend Micro Network Defense с технологиями XGen™ Security.

СПЕЦИФИКАЦИЯ УСТРОЙСТВА DEEP DISCOVERY EMAIL INSPECTOR

Характеристики устройства	Модель 7100	Модель 9100
Вариант развертывания	Режимы MTA, BCC, SPAN/TAP	Режимы MTA, BCC, SPAN/TAP
Пропускная способность	До 400 000 писем в день	До 800 000 писем в день
Форм-фактор	1U для установки в стойку, 48,26 см (19")	2U для установки в стойку, 48,26 см (19")
Размеры	43.4 (17.09") x 64.2 (25.28") x 4.28 (1.69") см	43.4 (17.09") x 75.58 (29.75") x 8.73 (3.43") см
Вес	19,9 кг (43,87 фунта)	31.5 кг (69.45 фунта)
Порты управления	Порт 10/100/1000 BASE-T RJ45 iDRAC Enterprise RD45 x 1	Порт 10/100/1000 BASE-T RJ45 iDRAC Enterprise RD45 x 1
Порт для обмена данными	10/100/1000 BASE-T RJ45 x 3	10/100/1000 BASE-T RJ45 x 3
Входное напряжение (переменный ток)	от 100 до 240 В переменного тока	от 100 до 240 В переменного тока
Входной ток (переменный ток)	от 7,4 до 3,7 А	от 10 до 5 А
Жесткие диски	2 x 600 ГБ 2,5-дюймовых SAS-диска	2 x 4 ТБ 3,5-дюймовых SATA-диска
Поддержка Интернет-протоколов	IPv4 / IPv6	IPv4 / IPv6
Конфигурация RAID	RAID 1	RAID 1
Источник питания	550 Вт с резервированием	750 Вт с резервированием
Энергопотребление (макс.)	604 Вт	847Вт
Теплоотдача	2133 БТЕ/час (макс.)	2891 БТЕ/час (макс.)
Рабочая температура	10 до 35 °C (50–95 °F)	10 до 35 °C (50–95 °F)
Гарантия на оборудование	3 года	3 года
Поддержка Интернет-протоколов	IPv4 / IPv6	IPv4 / IPv6
Конфигурация RAID	RAID 1	RAID 1
Источник питания	550 Вт с резервированием	750 Вт с резервированием
Энергопотребление (макс.)	604 Вт	847Вт
Теплоотдача	2133 БТЕ/час (макс.)	2891 БТЕ/час (макс.)
Рабочая температура	10 до 35 °C (50–95 °F)	10 до 35 °C (50–95 °F)
Гарантия на оборудование	3 года	3 года
Оптоволоконная сетевая карта	Dual Port Fiber Gigabit (SX/ LX)	Dual Port Fiber Gigabit (SX/LX)

ОБНАРУЖЕНИЕ И ЗАЩИТА

- Направленные атаки и сложные угрозы.
- Фишинг, целевой фишинг и другие угрозы для электронной почты.
- Вредоносные программы нулевого дня и эксплойты в документах.
- Атаки программ-вымогателей.

ЧАСТЬ ПЛАТФОРМЫ DEEP DISCOVERY

Deep Discovery Email Inspector является частью платформы Deep Discovery, которая обеспечивает защиту от сложных угроз самых уязвимых мест вашей организации — сети, электронной почты, конечных устройств, а также дополняет имеющиеся решения по обеспечению безопасности.

Deep Discovery Inspector — это готовое к использованию сетевое устройство, которое наблюдает все порты и более 107 протоколов для обнаружения целевых атак. Усовершенствованные методы обнаружения, включая встроенную «песочницу», позволяют быстро обнаружить целевые атаки.

Deep Discovery Analyzer выполняет расширенный анализ с использованием «песочницы», таким образом повышая ценность прочих систем безопасности, включая системы защиты конечных устройств, интернет-шлюзы и почтовые шлюзы, решения для обеспечения сетевой безопасности и другие продукты Deep Discovery. Подозрительные объекты или URL-адреса можно автоматически или вручную отправить для анализа в Deep Discovery Analyzer. Благодаря усовершенствованным методам обнаружения Deep Discovery Analyzer способен обнаруживать программы-вымогатели, сложные вредоносные программы, эксплойты нулевого дня, сеансы обмена данными с командными центрами, а также многоэтапные загрузки данных через вредоносные вложения или с неблагонадежных URL-адресов в системах Windows, Mac и Android.

1 Отчет компании Verizon о расследовании утечек данных за 2016 г.

Securing Your Journey to the Cloud