Техническое описание

FireEye EX

Защита от продвинутых атак, распространяющихся через электронную почту

Ключевые возможности

- Защита от атак направленного фишинга
- Интеграция с FireEye NX серией для борьбы со смешанными атаками, которые поступают по нескольким векторам угроз
- Анализ почтовых сообщений на предмет эксплоитов нулевого дня, а также атак, спрятанных в ZIP/RAR/TNEF архивах и вредоносных URL
- Дополняет существующую инфраструктуру контроля электронной почты (анти-спам, шлюзы безопасности электронной почты)
- Устанавливается в режиме активной защиты (MTA) или в режиме мониторинга (SPAN\BCC)
- Вносит в карантин вредоносные электронные письма с возможным уведомлением пользователя

EX 5400 и EX 8420
(не показаны EX 3400, EX 8400)

FireEye EX предназначен для защиты от направленных фишинговых (spear-phishing) атак, распространяющихся через электронную почту, изощрённость которых, позволяет им легко обходить репутационные и анти-спам технологии защиты. Являясь частью комплексной системы защиты от угроз FireEye Threat Prevention Platform, устройства FireEye EX используют безсигнатурную технологию для анализа каждого вложения в почтовом сообщении и для внесения в карантин электронных писем направленного фишинга, которые используются в продвинутых постоянных атаках (APT).

Имея в распоряжении огромное количество персональной информации доступной онлайн, киберпреступник, используя методы социальной инженерии, может запросто заставить любого пользователя перейти по ссылке или открыть вложение которое заразит систему. Устройства FireEye EX в режиме реального времени обеспечивают защиту от направленных фишинговых атак, которые с легкостью обходят традиционные методы защиты. EX является эффективным решением при борьбе со смешанными атаками, когда в фишинговом электронном сообщении присылается ссылка на зараженный ресурс. Это становится возможным благодаря интеграции с устройствами серии NX. Совместная работа двух решений позволяет отправлять в карантин сообщения, содержащие вредоносные ссылки, и отслеживать к какому фишинговому сообщению имеет отношение данная Web-атака.

Карантин вредоносных сообщений в режиме реального времени

Для блокирования электронных писем направленного фишинга, FireEye EX анализирует каждый файл, вложенный в электронное письмо, используя специализированную технологию FireEye «Multi-Vector Virtual Execution» (MVX), которая с высочайшей точностью идентифицирует продвинутые атаки. FireEye MVX, используя перекрестную матрицу различных ОС и их версий, браузеров, приложений, плагинов, таких как Adobe Reader и Flash, открывает вложенный файл, тем самым активируя скрытое в нем вредоносное ПО. Если атака подтверждена, то EX отправляет вредоносное письмо в карантин для дальнейшего анализа или удаления.

Борьба со смешанными атаками поступающих по почте и Web

Современные атаки используют направленный фишинг в качестве начала мультивекторной атаки. Для того, что бы проследить весь жизненный цикл такой атаки, EX часто устанавливают совместно с решением по защите Web трафика FireEye NX, а так же с системой управления FireEye CM, для поиска взаимоотношений и связей между вредоносными URL и исходным сообщением, предназначенным для жертвы атаки.

«В дополнение к возможности быстрой установки FireEye, данная платформа является единым решением для эффективного блокирования атак нулевого дня по всему предприятию. Принцип осуществления защиты не зависит от сигнатур, что обеспечивает невероятно низкий уровень ложных срабатываний».

- Специалист по информационной безопасности, Всемирно известное производство

FireEye™

Техническое описание

Динамический анализ атак «нулевого дня»

Устройства серии EX используют безсигнатурный механизм FireEye MVX, который останавливает продвинутые атаки, использующие ранее неизвестные разработчикам уязвимости в ОС, браузерах или приложениях, а так же вредоносный код, встроенный в обычные файлы или мульти-медиа контент. FireEye MVX создает отчет с детальным описанием угрозы, с информацией о том, какая уязвимость используется при переполнении буфера или координаты исходящих коммуникаций (callback), используемые для связи с Command & Control сервером для передачи украденных данных (эксфильтрации).

Глобальное информирование об угрозах

Создаваемая в режиме реального времени база угроз, становится доступной всем продуктам FireEye, находящимся в вашей сети это становится возможным благодаря интеграции с платформой централизованного управления FireEye CM. Помимо этого информация о новых угрозах становится доступной для любого подписчика услуги, благодаря оповещениям с облачного сервиса FireEye Dynamic Threat Intelligence (DTI).

Настройка YARA-правил

Устройства серии EX поддерживают импорт настраиваемых YARA правил, что позволяет аналитикам безопасности задавать правила для анализа вложений почтовых сообщений на предмет угроз, присущих их организации.

Управление угрозами поступающими по электронной почты

С помощью FireEye AV-Suite, каждый вредоносный объект анализируется с целью выяснить, может ли сторонний производители антивирусного ПО остановить угрозу. Это позволяет настроить приоритетность реакции на инциденты.

Простота использования

FireEye EX не требует дополнительной настройки и может быть установлен, как MTA, SPAN-устройство или прозрачное BCC место назначение. В дополнении к уже имеющейся системе аутентификации, FireEye поддерживает доступ к AAA протоколу сторонних разработчиков.

Техническая спецификация

	EX 3400	EX 5400	EX 8400	EX 8420
Форм-фактор	1U	1U	1U	1U
Вес	11,4 кг	13,6 кг	22,7 кг	22,7 кг
Размеры (Ширина x Глубина x Высота)	43,7x65,0x4,3 см	43,7x65,0x4,3 см	43,7x70,9x8,9 см	43,7ч70,9x8,9 см
Монтаж	19'' – стойка	19'' – стойка	19'' – стойка	19'' – стойка
Порты управления	2x10/100/1000 BASE-T	2x10/100/1000 BASE-T	2x10/100/1000 BASE-T	2x10/100/1000 BASE-T
Порты мониторинга	2x10/100/1000 BASE-T	2x10/100/1000 BASE-T	2x10/100/1000 BASE-T	2x1000 BASE-SX оптоволоконные порты (LC-многомодовые)
Производительность	До 150 000 электронных писем в день	До 300 000 электронных писем в день	До 750 000 электронных писем в день	До 750 000 электронных писем в день
Производительность с применением TLS	До 100 000 электронных писем в день	До 200 000 электронных писем в день	До 500 000 электронных писем в день	До 500 000 электронных писем в день
Напряжение питания	Автопереключение 100 ~ 240В	Автопереключение 100 ~ 240В	Автопереключение 100 ~ 240В	Автопереключение 100 ~ 240В
Сила тока питания	8,5 - 6,0 А	8,5 - 6,0 А	9,5-7,2 А	9,5-7,2А
Блок питания/RAID	2x700 Вт/2xSAS HDD в RAID1	2x700 Вт/2xSAS HDD в RAID1	2x1400 Вт/2xSAS HDD в RAID1	2x1400 Вт/2xSAS HDD в RAID1
Максимальное энергопотребление	0,26 кВт/ч	0,44 кВт/ч	0,47 кВт/ч	0,47 кВт/ч
Частота питания	50-60 Гц	50-60 Гц	50-60 Гц	50-60 Гц
Диапазон рабочих температур	10- 35 °C	10- 35 °C	10- 35 °C	10- 35 °C

Заметка: все значения производительности варьируются в зависимости от конфигурации системы и профиля обрабатываемого трафика.