FireEye

Техническое описание

FireEye NX

Решение для предотвращения кибератак, поступающих по Web

Ключевые возможности

- Устанавливается в режиме in-line (режимы блокирования/мониторинга) или out-of-band (режим сброса TCP-подключений/мониторинга)
- Анализирует все подозрительные веб-объекты, включая PDF, флэш, мультимедийные форматы, ZIP/RAR/TNEF архивы, а также блокирует исходящие коммуникации вредоносного ПО с целью предотвращения кражи данных
- Упрощенная приоритезация реакции на инциденты безопасности с помощью интеграции с AV-Suite
- Интегрируется с устройствами FireEye EX-серии для борьбы со смешанными атаками направленного фишинга
- Распространение информации об угрозах локально среди установленных в организации устройств FireEye и глобально через облачный сервис FireEye Dynamic Threat Intelligence (DTI)
- Поддерживает удаленные AAA-сервисы сторонних производителей в дополнение к локальной базе

NX 2400, NX 4420, NX 7420, NX10000
(не показаны NX 1400, NX 4400, NX 7400)

Устройства FireEye NX-серии обнаруживают и блокируют Zero-day веб-эксплоиты, бинарные файлы и попытки вредоносного ПО установить обратную связь с Command & Control сервером (callback) по различным протоколам с целью кражи конфиденциальных данных. FireEye NX позволяет организовать защиту от APT атак по всей организации, начиная от главного офиса с мультигигабитными каналами, заканчивая удаленным филиалом или мобильным офисом.

Киберпреступники используют Web, как основной канал для доставки Zero-day эксплоитов и вредоносных URL в сообщениях электронной почты для последующей кражи данных. FireEye NX – это решение, которое спроектировано специально для защиты от непреднамеренной (drive-by) загрузки шпионского ПО на ПК пользователя, и смешанных веб и email атак.

Защита от Web атак в режиме реального времени

FireEye NX может быть установлен вразрез в режиме in-line, для блокирования веб-эксплоитов и исходящих мультипротокольных callback. Благодаря технологии FireEye «Multi-Vector Virtual Execution», NX обнаруживает атаки нулевого дня, моментально создает их профиль и захватывает адреса динамических callback. Во режиме out-of-band FireEye NX выполняет сбросы TCP подключений для блокирования опасных TCP, UDP, или HTTP соединений.

Противодействие смешанным атакам по Web и email

Платформа FireEye защищает от смешанных атак, когда вредоносная ссылка отправляется в электронном сообщении, продвинутых атак, которые используют Web, направленные фишинговые (spear-phishing) сообщения и Zero-day эксплоиты. С помощью комбинации устройств FireEye NX, EX и централизованной консоли CM, организации получают защиту от вредоносных URL в режиме реального времени, а так же имеют возможность увидеть полную картину и взаимосвязь угроз при смешанных атаках.

Защита против неизвестных Zero-day

Устройства FireEye NX используют безсигнатурную технологию FireEye MVX (Multi-Vector Virtual Execution), которая «детонирует» подозрительные бинарные коды и веб-объекты в изолированной среде и обнаруживает эксплоиты уязвимостей, повреждение памяти и другие вредоносные действия. В изолированной среде реализовано множество вариаций пользовательских рабочих станций с типичным набором браузеров, плагинов, приложений и операционных систем различных версий, что обеспечивает высокий показатель обнаружения угроз. После воспроизведения атаки с помощью FireEye MVX происходит захват вредоносных callback, в режиме реального времени создаются правила блокирования и противодействия атаке, в результате чего платформа NX получает полноценный профиль угрозы.

Гибкая настройка с YARA-правилами

С поддержкой настраиваемых YARA-правил специалисты безопасности могут назначить, какие веб-объекты должны быть проанализированы на наличие угроз.

Приоритезация инцидентов

С помощью FireEye AV-Suite каждый вредоносный объект может быть проанализирован для определения, способен ли анти-вирусный вендор обнаружить угрозу остановленную FireEye NX. Это позволяет настроить приоритетность реакции на инциденты.

Обмен информацией о вредоносных программах

Динамически сгенерированная в режиме реального времени устройством FireEye NX информация об угрозе, позволяет всем продуктам FireEye защитить инфраструктуру локальной сети. Эта информация также включает координаты исходящих callback и дополнительные характеристики вредоносных коммуникаций, которые могут быть распространены глобально с помощью облачного сервиса Dynamic Threat Intelligence (DTI) с целью оповещения всех подписчиков об обнаружении новой угрозы.

Никаких правил и политик и минимум ложных срабатываний

FireEye NX – это легко управляемая платформа, которая устанавливается в течение 60 минут и не требуют никаких настроек или установки клиента на конечные станции. NX может быть развернут в режиме out-of-band через TAP\SPAN, in-line мониторинг или in-line активное блокирование.

Техническая спецификация

	NX 900	NX 1400	NX 2400	NX 4400/4420	NX 7400/7420	NX 10 000
Форм-фактор	1U	1U	1U	1U	2U	2U
Вес	7,7 кг	9,9 кг	9,9 кг	13,6 кг	22,7 кг	27,2 кг
Размеры (Ширина x Глубина x Высота)	42,6x35,6x4,3 см	42,6x35,6x4,3 см	42,6x35,6x4,3 см	43,7x65,0x4,3 см	43,7x65,0x8,9 см	43,7x70,9x8,9 см
Монтаж	19'' – стойка	19'' – стойка	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	2x10/100/1000 BASE-T	2x10/100/1000 BASE-T
Порты мониторинга	2x10/100/1000 BASE-T	2x10/100/1000 BASE-T	4x10/100/1000 BASE-T	4400:4x10/100/1000 BASE-T 4420:4x1000 BASE-SX оптоволоконные порты (LC-много-модовые)	7400:4x10/100/1000 BASE-T 7420: 4x1000 BASE-SX оптоволоконные порты (LC-много-модовые)	2x10Гб BASE-SR/SW 850нм оптово-локонные порты (LC-много-модовые)
Производительность	До 10 Мбит/с	До 20 Мбит/с	До 50 Мбит/с	До 250 Мбит/с	До 1 Гбит/с	До 4 Гбит/с
Количество пользователей	50	100	500	2500	10 000	40 000
Напряжение питания	Автопереключение 100 ~ 240В	Автопереключение 100 ~ 240В	Автопереключение 100 ~ 240В	Автопереключение 100 ~ 240В	Автопереключение 100 ~ 240В	Автопереключение 100 ~ 240В
Сила тока питания	4,8 - 2,0 А	4,8 - 2,0 А	4,8 - 2,0 А	8,5 - 6,0 А	8,5 - 6,0 А	9,0 - 7,0 А
Блок питания/ RAID	1x200 Вт/ Отсутствует	1x260 Вт/ Отсутствует	1x260 Вт/ Отсутствует	2x700 Вт/ 2xSAS HDD в RAID1	2x700 Вт/ 2xSAS HDD в RAID1	2x1200 Вт/ 2xSAS SSD в RAID1
Максимальное энергопотребление	0,153 кВт/ч	0,19 кВт/ч	0,2 кВт/ч	0,27 кВт/ч	0,255 кВт/ч	1,2 кВт/ч
Частота питания	50-60 Гц	50-60 Гц	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	10- 35 °C	10- 35 °C

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