FireEye
Next Generation Threat Protection

Multi-Vector Virtual Execution (MVX)

Ядром платформы FireEye является патентованная технология Multi-Vector Virtual Execution (MVX) которая проводит динамический анализ продвинутых угроз в режиме реального времени. MVX захватывает и подтверждает Zero-day атаки и постоянные направленные угрозы (APT) путем «детонации» подозрительных файлов, Web-объектов и вложений электронной почты в специально-настроенной виртуальной среде.

Виртуализированная модель обнаружения угроз

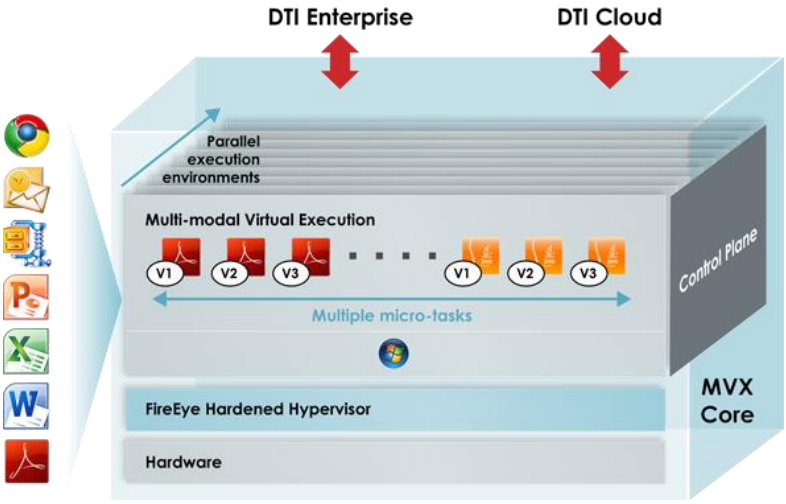
Современные атаки характеризуются скрытностью, динамичностью, нацеленностью и хорошим финансированием. Такие мульти-векторные и много-этапные атаки способны легко обойти традиционную защиту в виде NG Firewall, IPS, шлюза безопасности и антивируса, доказательством тому являются множество успешных атак на крупные организации, которые тратят миллиарды долларов на безопасность. Для борьбы с продвинутыми атаками, нужен новый утонченный подход.

Технология MVX осуществляет многоэтапный анализ что дает ей полное понимание целей и задач кибератаки. Анализ состояния атаки и понимание этапа, на котором она находится, имеет решающее значение для анализа всего ее жизненного цикла, от начального эксплоита, до эксфильтрации данных. Именно поэтому точечные решения, которые фокусируются на одном объекте (зараженные *.exe, DLL или PDF файлы) пропускают большинство атак, т.к. не видят их полной картины происходящего.

Все основы технологии MVX лежит специально разработанный физический гипервизор, в котором встроены контрмеры от вредоносного ПО. Он поддерживает большое количество виртуальных сред и виртуальных машин, которые действуют одновременно и сочетают в себе различными комбинациями операционных систем, сервисных пакетов и приложений. Каждая из этих виртуальных машин осуществляет многопоточный анализ содержимого среды с целью обнаружения вредоносных элементов и их характеристик. Обнаруженное вредоносное ПО, устанавливается и исполняется до тех пор, пока MVX не получит о нем полную информацию, включая расположение файла, данные регистра, запускаемые процессы и направление callback. Таким образом, анализ полиморфных угроз может быть успешно автоматизирован для создания динамичного блокирования входящих Zero-day атак и их исходящих коммуникаций. Патентованный безсигнатурный подход к анализу и обнаружению угроз позволяет решениям FireEye эффективно предотвращать скрытные Zero-day и направленные атаки.

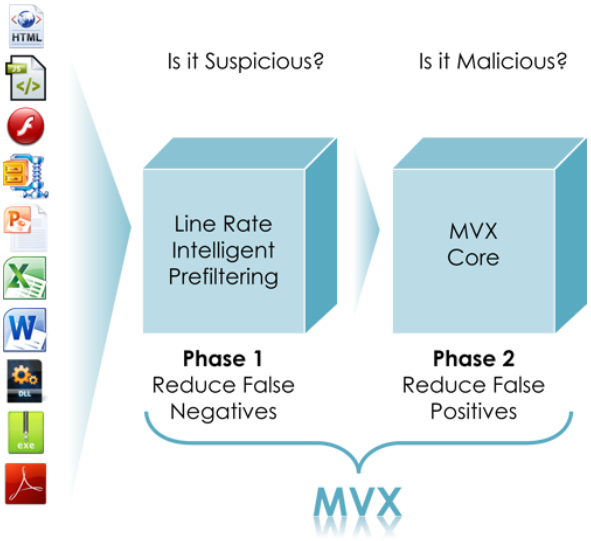
Локальное исследование угроз, которое осуществляется каждым MVX, предоставляет результаты экспертного анализа угроз в режиме реального времени, что позволяет защиты сеть. Данные анализа могут быть распространены локально, среди других устройств FireEye на предприятии (Dynamic Threat Intelligence) тем самым обеспечивая своевременную защиту от атак по различным векторам. Так же данные анализа могут быть распространены глобально посредством облачного сервиса Dynamic Threat Intelligence (DTI).

FireEye Dynamic Threat Intelligence



Технология MVX выгодно сочетает скорость, точность и масштабируемость. Гипервизор FireEye спроектирован для анализа угроз и позволяет одновременно запускать несколько виртуальных машин на одном устройстве. В свою очередь одна виртуальная машина поддерживает выполнение множества задач одновременно, что ускоряет процесс исполнения подозрительных объектов. Масштабируемость технологии MVX, дополняется возможностью осуществлять много-этапный анализ, что позволяет без задержек обрабатывать большие объемы высоко-скоростного трафика.

Много-этапный анализ MVX



Ключевые технологические возможности:

- **Активный анализ неизвестного кода и подозрительных Web объектов –** объекты исполняются в среде, где реализована реальная пользовательская среда с использованием различных браузеров, плагинов, приложений и операционных систем. Безсигнатурная технология MVX идентифицирует Zero-day эксплоиты и «на ходу» подтверждает Web атаку, блокирует callback и последующую загрузку вредоносного ПО по различным протоколам.
- **Детонация всех вложений электронной почты в виртуальной среде –** Все вложения могут быть аккуратно и точно проанализированы на предмет наличия Zero-day эксплоитов. В отличии от сигнатурного и репутационного методов, технология MVX может определить, что, в прошлом безвредный файл, был заражен и отправлен направленным фишинговым письмом для преодоления системы защиты предприятия.
- **Анализ общих папок на предмет зараженных файлов** – Технология MVX может быть использована для сканирования CIFS-совместимых папок для обнаружения и блокирования продвинутых атак которые встроены в офисные файлы, изображения, PDF, или ZIP/RAR/TNEF архивы.
- **Патентованная технология виртуализации** - Физическая виртуализация FireEye спроектирована для анализа угроз и располагает множеством контрмер, что не дает вредоносному ПО обойти ее.
- **Много-этапная инспекция и технология блокировки** – Останавливает неизвестные атаки и Zero-day угрозы, одновременно устраняя ложные срабатывания. Много-этапная инспекция осуществляется благодаря использованию интеллектуальных технологий для масштабирования и точного блокирования продвинутого вредоносного ПО, которое используется для проникновения в сеть и кражи конфиденциальных данных.