DATA SHEET

FireEye

Система безопасности электронной почты FireEye Email Security Серверная версия

Адаптивная, интеллектуальная, масштабируемая защита от угроз, связанных с электронной почтой

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- Обеспечивает комплексную защиту электронной почты от адресного фишинга и других передовых, многоступенчатых атак и атак нулевого дня
- Технология Bursting (посылка большего количества кадров за тот же временной интервал) обеспечивает дополнительную возможность анализа распознавания в периоды максимальной пропускной способности сообщений
- Поддерживает анализ изображений на операционных системах Microsoft Windows и Apple Mac OS X
- Анализирует электронную почту на скрытые в файлах угрозы, включая защищенные паролем и зашифрованные вложения, а также вредоносные URL-адреса
- Автоматически обнаруживает и уменьшает или полностью предотвращает фишинг данных учётных записей пользователей
- Предоставляет контекстные выводы из обработки данных об оповещениях для установления приоритетов и сдерживания угроз
- Интегрируется с различными технологиями FireEye
- Развертывание происходит локально в режимах активная защита или только отслеживание
- Обеспечивает видимость, отслеживание и управление сообщениями и оповещениями

Рисунок 1. EX 3500, EX 5500 и EX 8500.

Общая информация

Электронная почта — это наиболее уязвимый вектор для кибератак, поскольку это точка входа самого большого объема данных. Организации сталкиваются с постоянно растущим числом вызовов безопасности, начиная со спама и вирусов в электронной почте, и заканчивая передовыми и целевыми угрозами. Большинство угроз поступают по электронной почте в виде превращенных в оружие файловых приложений, вредоносных ссылок и фишинга учетных данных. В то время как антиспам-фильтры и антивирусное программное обеспечение отлично подходят для улавливания традиционных массовых фишинговых атак на электронную почту с известными вредоносными вложениями, ссылками и контентом, они не могут улавливать сложные и целевые фишинговые мошеннические атаки. Электронная почта остается основным методом, используемым для инициирования передовых атак или доставки программ-вымогателей, поскольку она может быть высоко целевой и настроена для увеличения преимуществ использования.

Система безопасности электронной почты FireEye Email Security помогает организациям свести к минимуму риск дорогостоящих уязвимостей. Локальные устройства безопасности электронной почты точно обнаруживают и могут немедленно остановить передовые и целевые атаки, включая фишинг данных и программы-вымогатели,. Система безопасности электронной почты использует механизм мульти-векторного виртуального исполнения Multi-Vector Virtual ExecutionTM (MVX) без подписи для анализа вложений электронной почты и URL-адресов по всеобъемлющей перекрестной матрице операционных систем, приложений и веб-браузеров. Угрозы идентифицируются с минимальным искажением, а ложноположительные срабатывания почти отсутствуют.

FireEye собирает обширную оперативную информацию об угрозах противников, исследования уязвимостей из первых рук и через миллионы датчиков. Безопасность электронной почты основывается на реальных доказательствах и контекстной оперативной информации об атаках и взломщиках для установления приоритетов оповещений и блокировки угроз в режиме реального времени.

Система безопасности электронной почты интегрируется с системой сетевой безопасности FireEye Network Security и системой безопасности конечных точек Endpoint Security для более широкой видимости в целях координации защиты в реальном времени от мульти-векторных смешанных атак.

Эффективное обнаружение угроз

Система безопасности электронной почты – это эффективное решение для защиты от кибер-угроз, помогающее организациям минимизировать риск дорогостоящих уязвимостей, точно обнаруживая и мгновенно останавливая передовые, целевые и другие труднообнаружимые атаки, скрывающиеся в почтовом трафике.

В основе системы безопасности электронной почты лежит механизм мульти-векторного виртуального исполнения MVX, который проверяет подозрительный трафик электронной почты для определения атак, труднообнаружимых традиционными системами защиты с подписью и на основе правил. Механизм мульти-векторного виртуального исполнения MVX обнаруживает инструменты эксплуатации недокументированной уязвимости, многоконтурные и прочие труднообнаружимые атаки с помощью динамического анализа без подписи в безопасной виртуальной среде. Он останавливает фазы заражения и компрометации цепи остановки кибератаки путем выявления ранее не встречавшихся инструментов эксплуатации уязвимости и вредоносных программ.

Технология Bursting в умной энергосистеме мульти-векторного виртуального исполнения FireEye MVX Smart Grid обеспечивает дополнительную мощность для обнаружения и анализа угроз электронной почты в периоды максимальной пропускной способности сообщений.

Защита от угроз электронной почты

Со всей личной информацией, доступной в Интернете, кибер-преступник может в порядке простого общения спровоцировать практически любого пользователя нажать на URL-адрес или открыть вложение.

Система безопасности электронной почты обеспечивает обнаружение в реальном времени и предотвращение попыток адресного фишинга, вымогательства и фишинга данных, труднообнаружимых с помощью традиционных средств защиты. Она снижает фишинг учетных данных с обнаружением доменов близких по написанию с адресами популярных сайтов (тайпсквоттинг).

Если атака подтверждена, система безопасности электронной почты помещает в карантин вредоносное письмо для дальнейшего анализа или удаления. Она проводит анализ вредоносных программ, скрытых в:

- Типах вложений, включая без ограничений: EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 и архивы ZIP/RAR/TNEF
- Защищенных паролем и зашифрованных вложениях
- URL-адресах, вставленных в электронные письма, документы MS Office, файлы PDF и архивы (ZIP, ALZip, JAR) и прочих типах файлов (незашифрованные, HTML)
- Файлах, загруженных через URL-адреса, и даже FTP-ссылках
- Вводящих в заблуждение, поддельных, укороченных и динамически перенаправляемых URL-адресах
- Фишинге учетных данных и тайпсквоттинговых URL-адресах
- Неизвестных изображениях операционных систем Microsoft Windows и Apple Mac OS X, уязвимости браузера и приложений
- Вредоносных кодах, встроенных в электронные письма целевого фишинг-мошенничества

Тогда как атаки через программы-вымогатели начинаются с электронной почты, для шифрования данных обычно требуется обратный вызов на командный сервер. Система безопасности электронной почты идентифицирует и останавливает эти труднообнаружимые многоступенчатые кампании вредоносных программ. Эффективный ответ на оповещения системы безопасности электронной почты анализирует каждое вложение и URL-адрес, чтобы точно идентифицировать передовые атаки. Обновления в реальном времени всей экосистемы безопасности FireEye в сочетании с соотнесением оповещений с известными злоумышленниками обеспечивают контекст для определения приоритетов и ответных действий на критические оповещения и блокировку электронных писем целевого фишинг-мошенничества. Известные и неизвестные угрозы и угрозы, основанные на безвредных программах, идентифицируются с минимальными искажениями и ложноположительными срабатываниями, поэтому ресурсы сосредоточены на реальных атаках для снижения операционных расходов. Категоризация потенциально опасных программ отделяет попытки подлинного проникновения от нежелательной, но менее вредоносной деятельности (например, рекламного ПО и шпионских программ) для определения приоритета ответа на оповещения.

Быстрая адаптация к развивающейся картине угроз

Система безопасности электронной почты Email Security помогает вашей организации постоянно адаптировать вашу активную защиту от угроз электронной почты, используя глубокие оперативные данные об угрозах и взломщиках. Она объединяет оперативные данные противников, машин и жертв для:

- Обеспечения своевременной и более широкой видимости угроз.
- Определения конкретных возможностей и функций обнаруженных вредоносных программ и вложений.
- Предоставления контекстных выводов из обработки данных для определения приоритетов и ускорения реакции.
- Определения вероятной личности и мотивов взломщика и отслеживания его активности внутри вашей организации.
- Ретроактивной идентификации целевого фишинг-мошенничества и предотвращения доступа к фишинговым сайтам путем выделения вредоносных URL-адресов.

Режимы активной защиты или только отслеживания

Система безопасности электронной почты может анализировать электронные письма и отправлять угрозы в карантин для активной защиты. Она использует детонационную камеру без подписи, механизм мульти-векторного виртуального исполнения MVX, чтобы анализировать каждое вложение и URL-адрес на предмет угроз и останавливать передовые атаки в реальном времени. Для развертываний в режиме только отслеживание организации устанавливают прозрачное правило символа контроля блока (BCC) для отправки копий электронных писем в систему безопасности электронной почты для анализа механизмом мульти-векторного виртуального исполнения MVX.

Контроль операций безопасности

Система безопасности электронной почты беспрепятственно работает с платформами операций безопасности FireEye Helix и центрального управления FireEye Central Management.

- В качестве компонента платформы операций безопасности FireEye Helix она обеспечивает область видимости по всей инфраструктуре. Платформа операций безопасности FireEye Helix дополняет оповещения электронной почты и сторонние оповещения с учетом оперативных данных, соотнесения с ко-

нечной точкой, автоматизации и рекомендаций исследований. Благодаря этим возможностям платформа операций безопасности FireEye Helix выводит на поверхность неявные угрозы и стимулирует экспертные решения.

- Платформа центрального управления Central Management соотносит оповещения как от системы безопасности электронной почты, так и от системы сетевой безопасности для более широкого обзора атаки и установления правил блокировки для предотвращения распространения атаки.
- Платформа центрального управления Central Management поддерживает установление меток на основе ролей, чтобы узнать, на кого нацелена атака.
- Платформа центрального управления поддерживает реагирование на оповещения и устранение ошибок на основе ролевых критериев.

Правила, основанные на инструментах YARA, предлагают индивидуальную настройку

Система безопасности электронной почты — Серверная версия поддерживает настраиваемые правила YARA, чтобы позволить аналитику безопасности устанавливать и тестировать правила для анализа вложений электронной почты, содержащих угрозы, нацеленные на их организацию.

Очередь сообщений, оповещение и управление карантином

Система безопасности электронной почты обеспечивает высокую степень контроля над сканируемыми ею электронными сообщениями. При развертывании в режиме активной защиты сообщения можно отслеживать и управлять ими, когда они перемещаются по очереди почтового транспортного агента MTA. Атрибуты электронной почты могут использоваться для поиска и проверки того, что сообщения были получены, проанализированы и доставлены на следующий транзитный участок, а со временем тенденции можно будет отслеживать с помощью интуитивной панели мониторинга. Списки лиц с разрешенным доступом и списки блокировки обеспечивают индивидуальный контроль над обработкой электронной почты. Стандартные атрибуты оповещений можно искать и выбирать, а массовые операции могут выполняться в отношении оповещений и сообщений в карантине.

Для получения дополнительной информации о FireEye, перейдите по адресу: **www.FireEye.com**

Компания Axoft является официальным дистрибутором решений FireEye в России и оказывает полный спектр услуг в части поддержки и продвижения продуктов вендора.

О компании FireEye, Inc.

FireEye - мировой разработчик решений по защите от современных киберугроз. Объединяя лучшие отраслевые технологии, многолетний опыт и аналитику, FireEye предлагаетширокий выбор универсальных адаптивных технологий для защиты от основных векторов атак, способных обходить традиционные решения на основе сигнатурного анализа, а также традиционные решения-«песочницы». Заказчики FireEye – это свыше 6 600 клиентов в 67 странах, включая более 45% из списка Forbes Global 2000.

FireEye®