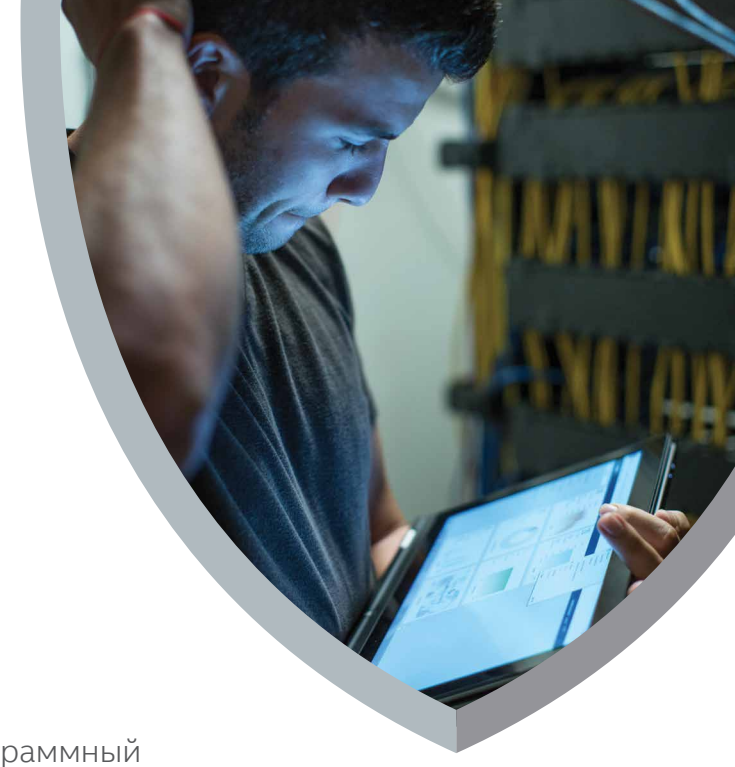
Краткий обзор решения



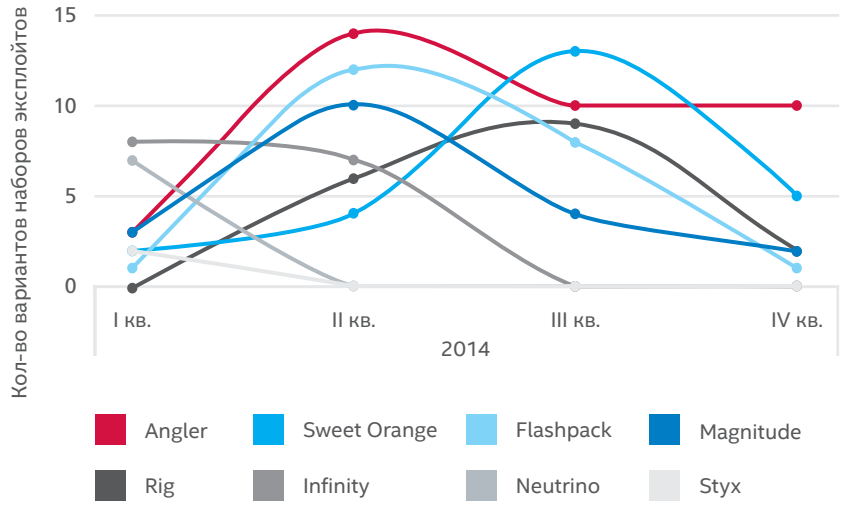
Как бороться с набором эксплойтов Angler

Набор эксплойтов представляет собой готовый программный пакет, содержащий (в упакованном виде) простые в использовании средства проведения атак на известные и неизвестные уязвимости («нулевого дня»). Эти наборы нацелены на уязвимости, имеющиеся на стороне клиента. Объектами их атак являются в основном веб-браузер и приложения, к которым у веб-браузера есть доступ. Наборы эксплойтов могут также отслеживать статистику заражений и иметь надежные функции управления.

Что собой представляет набор эксплойтов Angler?

Набор эксплойтов Angler подробно описан в **«Отчете McAfee® Labs об угрозах за февраль 2015 года»**. Angler получил широкое распространение и привлек к себе внимание специалистов во второй половине 2014 года. Причиной тому стало наличие у него таких функциональных возможностей, как бесфайловое заражение (заражение памяти), обнаружение виртуальных машин и защитных продуктов, а также способность транспортировать широкий спектр действующих нагрузок: троянских коней для кражи банковской информации, руткиты, программы-вымогатели, модули CryptoLocker, троянских коней с бэкдором и пр. Кроме того, для использования Angler не нужно быть специалистом по компьютерной технике, а возможность приобрести его на анонимных хакерских рынках в Интернете привела к его широкой распространенности.

Варианты наборов эксплойтов в 2014 г.



Источник: McAfee Labs, 2015 г.

intel Security

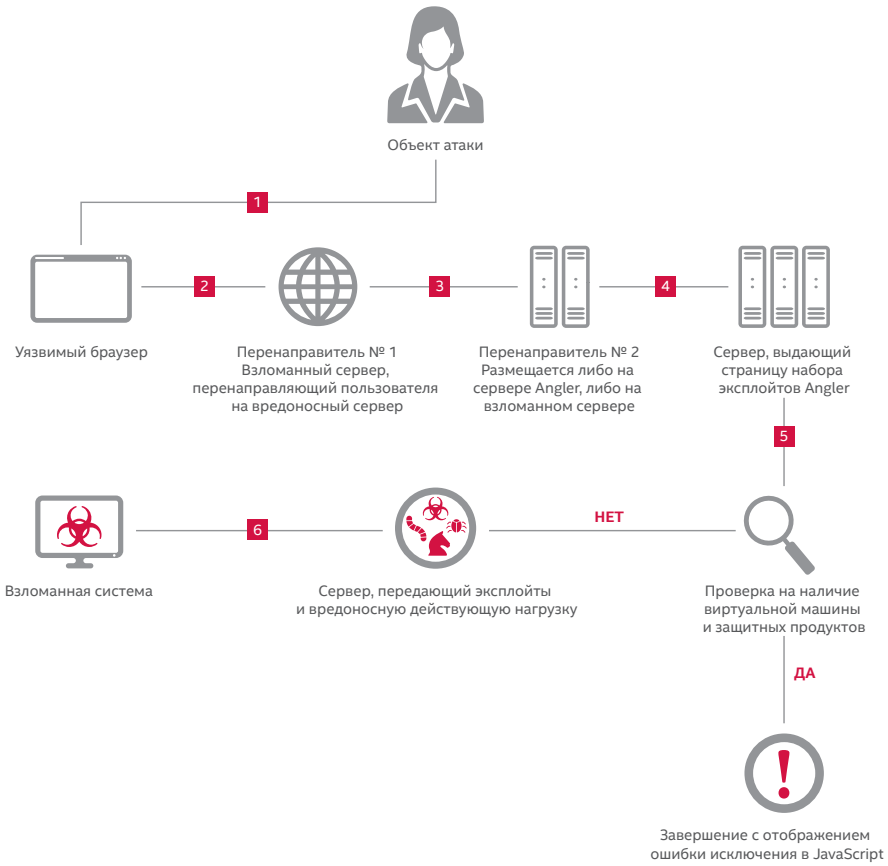
Стремясь помешать защитным продуктам обнаруживать наличие действующего набора эксплойтов, Angler часто меняет модели поведения и содержимое. Чтобы избежать обнаружения, Angler использует ряд методов обхода защиты:

- целевую страницу он выдает после двух перенаправлений;
- взломанные веб-серверы, на которых размещена целевая страница, можно посетить только один раз с одного IP-адреса. Злоумышленники явно ведут активный мониторинг компьютеров;
- он обнаруживает наличие виртуальных машин и защитных продуктов в системе;
- он генерирует «мусор» и бессмысленные вызовы, затрудняя тем самым процесс обратной разработки;
- он шифрует действующую нагрузку перед доставкой и расшифровывает на зараженном компьютере;
- он использует метод бесфайлового заражения (размещение кода непосредственно в памяти).

Успешная атака с использованием Angler проводится в несколько этапов:

- Объект атаки заходит на взломанный веб-сервер через уязвимый браузер.
- Взломанный веб-сервер перенаправляет пользователя на промежуточный сервер.
- Промежуточный сервер перенаправляет его на вредоносный веб-сервер, на котором размещена целевая страница набора эксплойтов.
- Целевая страница осуществляет проверку на наличие уязвимых подключаемых модулей (Java, Flash и Silverlight), и собирает сведения об их версиях.
- При обнаружении уязвимой версии браузера или подключаемого модуля набор эксплойтов производит доставку действующей нагрузки и заражает систему.

Набор эксплойтов Angler: процесс заражения



Как защититься от набора эксплойтов Angler

Вот несколько рекомендаций по защите систем от набора эксплойтов Angler:

- Используйте такого поставщика услуг Интернета, который уделяет должное внимание безопасности и реализует надежные процедуры защиты от спама и фишинга.
- Включите автоматическое обновление операционной системы или регулярно загружайте обновления операционной системы, чтобы своевременно исправлять известные уязвимости. Устанавливайте пакеты исправлений, получаемые от разработчиков другого программного обеспечения, сразу после их получения. Наилучшей защитой от троянских коней и шпионских программ является компьютер, на котором установлены все пакеты исправлений и который защищен брандмауэром.
- Открывая вложения, соблюдайте крайнюю осторожность. Настройте антивирусную программу на автоматическое сканирование всех файлов, вложенных в сообщения электронной почты и мгновенные сообщения. Программы электронной почты не должны автоматически открывать вложения и показывать изображения. Предварительный просмотр должен быть отключен. Никогда не открывайте непрошеные сообщения электронной почты и неожиданные вложения, даже если вы знаете отправителя.
- Остерегайтесь фишинговых атак с использованием спама. Не переходите по ссылкам в сообщениях электронной почты и в мгновенных сообщениях.
- Используйте специальный подключаемый модуль браузера, блокирующий выполнение сценариев и элементов iframe.

Как защититься от набора эксплойтов Angler с помощью Intel Security

McAfee Web Gateway

Вредоносная реклама, попутные загрузки и вредоносные URL-адреса, встроенные в доверенные веб-сайты, — вот лишь некоторые виды атак, целью которых является доставка набора эксплойтов Angler. **McAfee Web Gateway** — надежный продукт, который повысит уровень защиты вашей компании от такого рода угроз.

- **McAfee Gateway Anti-Malware Engine.** Средства анализа намерений без использования сигнатур в режиме реального времени отфильтровывают имеющееся в веб-трафике вредоносное содержимое. Эмуляция и анализ поведения обеспечивают упреждающую защиту от целенаправленных атак и атак «нулевого дня». Ядро McAfee Gateway Anti-Malware Engine выполняет проверку файлов и в случае признания их вредоносными блокирует возможность их загрузки пользователями.
- **Интеграция с McAfee Global Threat Intelligence (McAfee GTI).** Оперативное получение информации о репутации файлов, репутации веб-сайтов и категориях веб-содержимого от службы McAfee GTI позволяет обеспечить защиту от новейших угроз, поскольку ядро McAfee Web Gateway отклоняет попытки подключения к заведомо вредоносным веб-сайтам и узлам, связанным с сетями распространения вредоносной рекламы.

McAfee VirusScan® Enterprise

McAfee VirusScan Enterprise позволяет легко обнаруживать и удалять вредоносные программы, в том числе и те, которые доставляются с помощью Angler. В McAfee VirusScan Enterprise используется получивший широкое признание специалистов модуль сканирования McAfee, позволяющий обеспечить защиту файлов от вирусов, червей, руткитов, троянских коней и других сложных угроз.

- **Упреждающая защита от атак.** Интеграция технологий защиты от вредоносных программ со средствами предотвращения вторжений позволяет обеспечить защиту от таких атак на уязвимости приложений, для проведения которых используется метод переполнения буфера.
- **Непревзойденный инструмент обнаружения и удаления вредоносных программ.** Наличие расширенного набора функций анализа поведения позволяет обеспечить защиту от таких угроз, как руткиты и троянские кони. Для борьбы с распространением

вредоносных программ используются такие методы, как блокирование портов, блокирование файлов по именам, блокирование папок/каталогов, блокирование возможности совместного доступа к файлам, трассировка заражения и его блокирование.

- **Защита в реальном времени благодаря интеграции с McAfee GTI.** Использование самой современной из представленных на рынке платформ сбора информации об угрозах позволяет обеспечить защиту от уже известных и еще только формирующихся угроз по всем основным направлениям их распространения — файлы, веб-трафик, электронная почта и сети.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense представляет собой многоуровневое решение для обнаружения вредоносных программ, в котором используется сочетание нескольких разных модулей проверки. Эти модули проверяют файлы с помощью сигнатур и сведений о репутации, эмулируют поведение в режиме реального времени, проводят полный статический анализ кода и динамический анализ кода в «песочнице». Сочетая все эти разнообразные модули, McAfee Advanced Threat Defense обеспечивает защиту от распространенных наборов эксплойтов (типа Angler) и развертываемых ими вредоносных программ.

- **Обнаружение на основе сигнатур.** Обнаружение вирусов, червей, шпионских программ, бот-сетей, троянов, переполнения буфера и смешанных атак. Для этого используется обширная база знаний, созданная и регулярно пополняемая сотрудниками McAfee Labs. На данный момент в ней содержится более 150 миллионов сигнатур, в том числе сигнатур Angler и его вариантов.
- **Обнаружение на основе оценки репутации.** Обнаружение только что возникших угроз с помощью данных о репутации, получаемых из сети McAfee GTI.
- **Статический анализ и эмуляция в режиме реального времени.** Статический анализ кода и эмуляция поведения в режиме реального времени позволяет быстро обнаруживать вредоносные программы и угрозы «нулевого дня», не выявленные с помощью сигнатур и данных о репутации.
- **Полный статический анализ кода.** Обратная разработка кода файла, позволяющая проанализировать все атрибуты и наборы инструкций, и полностью оценить исходный код без его выполнения. Использование расширенных функций распаковки позволяет открывать все виды упакованных и сжатых файлов и дает возможность проводить полный анализ и классификацию вредоносных программ. Благодаря этому ваша компания всегда будет знать, какая именно угроза исходит от той или иной вредоносной программы.
- **Динамический анализ в «песочнице».** Выполнение кода файла в виртуальной среде с наблюдением за его поведением. Виртуальные среды можно настроить таким образом, чтобы они соответствовали операционным системам, используемым в вашей компании. Поддерживаются пользовательские образы Windows 7 (32- и 64-разрядная версии), Windows XP, Windows Server 2003, Windows Server 2008 (64-разрядная версия) и Android.

McAfee Network Security Platform

Платформа McAfee Network Security Platform предназначена для проведения углубленной проверки сетевого трафика. Используемое в решении McAfee Network Security Platform сочетание передовых методов проверки позволяет обнаруживать и предотвращать как известные, так и еще неизвестные атаки в сети. К этим методам относятся анализ трафика по всем протоколам, анализ репутации угроз, анализ поведения, усовершенствованный анализ вредоносных программ и др.

- **Комплексная защита от вредоносных программ.** Для обнаружения вредоносных программ, в том числе угроз «нулевого дня», вредоносных программ особого назначения и иных скрытых атак используется сочетание таких методов, как анализ репутации файлов с помощью McAfee GTI, углубленный анализ файлов с проверкой JavaScript и анализ сложных вредоносных программ без использования сигнатур.

- **Использование передовых методов проверки.** Обнаружение и предотвращение как известных, так и еще неизвестных атак в сети. К этим методам относятся анализ трафика по всем протоколам, анализ репутации угроз и анализ поведения.
- **Интеграция с McAfee GTI.** Сопоставление данных о репутации файлов, репутации IP-адресов и о географическом местоположении, получаемых в режиме реального времени, а также подробной контекстной информацией о пользователях, устройствах и приложениях, позволяет быстро и точно реагировать на сетевые атаки.
- **Security Connected.** Интеграция с McAfee Advanced Threat Defense дает платформе McAfee Network Security Platform возможность отправлять подозрительные файлы, обнаруженные в проверяемом трафике, на анализ в McAfee Advanced Threat Defense, и по результатам этого анализа решать, блокировать эти файлы или допускать их в сеть.

McAfee Threat Intelligence Exchange

Очень важно иметь такую платформу для сбора информации об угрозах, которая способна адаптироваться к меняющимся потребностями среды. **McAfee Threat Intelligence Exchange** значительно снижает риск проведения атак такого рода благодаря способности собирать информацию о текущих угрозах, например о неизвестных файлах или приложениях, выполняемых в среде организации.

- **Комплексный сбор информации об угрозах.** Возможность легко настроить комплексную систему сбора информации об угрозах из глобальных источников данных. В качестве источников данных можно использовать McAfee GTI и сторонние источники. Для получения локальной информации об угрозах используются данные о текущих и прошлых событиях, получаемые с конечных точек, шлюзов и других компонентов системы безопасности.
- **Предотвращение выполнения и устранение угрозы.** McAfee Threat Intelligence Exchange может вмешиваться в процессы и предотвращать выполнение неизвестных приложений в среде организации. Если приложение, запуск которого был разрешен, впоследствии признается вредоносным, то благодаря наличию функций централизованного управления и принудительного применения политик McAfee Threat Intelligence Exchange отключает все связанные с этим приложением активные процессы в масштабах всей среды.
- **Сбор информации о происходящем.** McAfee Threat Intelligence Exchange отслеживает все упакованные исполняемые файлы, места их первоначального выполнения в среде, а также все изменения, произошедшие после их выполнения. Такая возможность сбора информации о действиях приложения или процесса, совершенных с момента его установки и до настоящего времени, дает возможность быстрее реагировать на инциденты и устранять угрозы.
- **Признаки взлома.** Импорт хэш-данных известных вредоносных файлов в McAfee Threat Intelligence Exchange позволяет защитить среду от их воздействия путем принудительного применения политик. Если в системе обнаружены какие-либо признаки взлома, McAfee Threat Intelligence Exchange завершает все процессы и прекращает работу всех приложений, связанных с данными признаками взлома.

Растущие темпы распространения таких простых в использовании наборов эксплойтов, как Angler, служат отрезвляющим напоминанием о том, что ландшафт угроз непрерывно меняется. Технологии Intel Security могут помочь вашей компании обеспечить упреждающую защиту от таких угроз, как набор эксплойтов Angler, на конечных точках и в сети.

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com