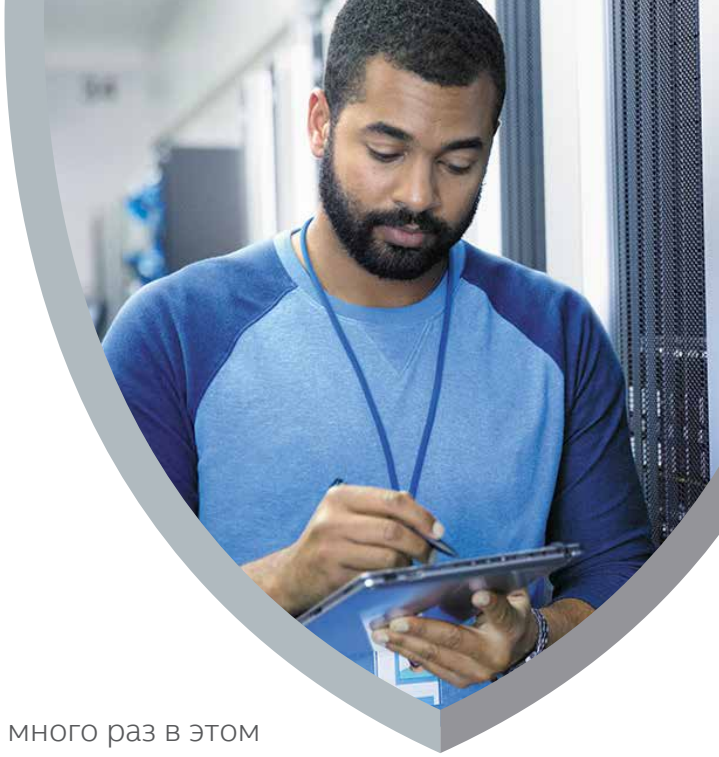
Краткий обзор решения



Злоупотребление доверием

Охота на доверчивых

Поговорка «доверие нужно заслужить» истинна, и мы много раз в этом убеждались. С другой стороны, то, на что уходят годы созидательного труда, бывает, рушится в считанные секунды. Доверие — это не константа, и мы в этом в очередной раз убеждаемся, когда мир всё больше полагается на Интернет.

Что же такое злоупотребление доверием?

Злоупотребление доверием подробно описано в **отчете McAfee Labs об угрозах за ноябрь 2014 года**. В сетевом мире мы предполагаем, что всё, с чем мы сталкиваемся, заслуживает доверия — будь то загружаемое на телефон приложение, безобидная на вид реклама на популярном веб-сайте или электронное письмо от имени компании, с которой мы ведем дела. А злоумышленники используют институт доверия в своих интересах и успешно атакуют ничего не подозревающих пользователей. Вот лишь некоторые виды атак, описанные в отчете:

- **Вредоносная реклама.** Когда безвредная на вид реклама на веб-сайте компании является на самом деле источником атаки на ничего не подозревающего пользователя, он начинает задумываться, тем ли он доверяет. **Сети вредоносной рекламы, такие как Kyle and Stan**, распространяют вредоносное содержимое посредством рекламных объявлений на таких веб-сайтах, как amazon.com и youtube.com, а также в **крупных рекламных сетях вроде Double-Click и Zedo**.
- **Вредоносные программы с цифровой подписью.** Среди авторов вредоносных программ всё более популярной становится практика получения сертификатов от центров сертификации для последующего распространения угроз с использованием репутации заслуживших доверие компаний или под видом легитимных источников. Здесь злоумышленники используют в своих интересах тот факт, что пользователи доверяют центрам сертификации. Совсем недавно одна такая вредоносная кампания в рекламной сети Zedo **принесла ущерб пользователям ведущих веб-сайтов в рейтинге компании Alexa**, внедрив в их компьютеры модификации «троянского коня» CryptoWall с цифровыми подписями. Цифровая подпись, полученная на имя «Trend», вероятно, предназначалась для имитации подписи компании Trend Micro. Это хороший пример того, как злоумышленникам удается заставить пользователей «по ассоциации» принимать их рекламу за безопасную.
- **Приложения-подделки.** Компании тратят значительное количество времени и средств на защиту своих потребителей от подделок, которые могут принести злоумышленникам прибыль за счет злоупотребления доверием. Когда приложения предоставляют функции, выходящие далеко за пределы цифрового мира, неудивительно, что предприимчивые злоумышленники тут же стремятся создавать подделки, имитирующие подлинные и, как правило, популярные программы.

intel Security

В последнем квартале специалисты компании McAfee отметили ряд попыток распространения приложения, имитирующего Adobe Flash Player 11. По данным счетчиков загрузок магазина Google Play и телеметрии McAfee Mobile Security, мошенникам удалось добиться некоторого успеха в обмане пользователей.

- **«Боковая загрузка» DLL-файлов.** Злоумышленники знают, что если вредоносный код удается протащить под прикрытием доверенного приложения, то шансы на успех значительно возрастают. Вредоносные программы используют этот трюк уже много лет, реализуя так называемый механизм «боковой загрузки» DLL-файлов. Этот механизм предполагает выполнение легитимного приложения, которое, в свою очередь, выполняет код из внешней библиотеки DLL. Злоумышленники создают вредоносное содержимое, имитирующее внешний DLL-файл, заставляя таким образом заведомо «чистое» приложение выполнять вредоносный код.

  В третьем квартале специалисты McAfee Labs наблюдали атаки на приложение Google Updater. Новая модификация вредоносной программы PlugX выступает в роли импортируемого файла goopdate.dll, но не ограничивается этим в стремлении скрыть свои действия. Модуль goopdate.dll — это не более чем посредник, который считывает данные из зашифрованного файла goopdate.dll.map, расшифровывает их в память и передает управление выполнением полученному вредоносному коду.

- **Операционные системы и программное обеспечение для работы в сети.** Есть множество примеров атак, построенных на злоупотреблении доверием в отношении операционных систем и программного обеспечения для работы в сети. В некоторых атаках используются функции программ, устанавливающих безопасные интернет-соединения. «Ничего не подозревающие» приложения доверяют соединениям, предоставленным операционной системой, которая, в свою очередь, полностью полагается на программы, предположительно обеспечивающие защиту соединений. В других атаках используются уязвимости самих операционных систем и программного обеспечения для работы в сети. При этом в атаках часто замешаны компоненты с открытым исходным кодом, входящие в состав ОС и прикладных программ.

  BERserk — это **одна из недавно замеченных уязвимостей**, которая позволяет подделывать цифровые подписи и использовать в корыстных целях доверие к ОС и сетевым приложениям. Уязвимость BERserk предоставляет злоумышленникам возможность проводить атаки с использованием «незаконного посредника», подделывая электронные подписи RSA и обходя алгоритмы проверки подлинности на веб-сайтах, использующих протоколы SSL/TLS.

Решения компании McAfee

Технологии обеспечения безопасности McAfee помогают защититься от атак, основанных на злоупотреблении доверием в повседневной деятельности. Ниже перечислены некоторые продукты McAfee, помогающие предотвратить использование злоумышленниками принятой в компании модели доверия в своих интересах.

McAfee Application Control

Очень важно обеспечить защиту компании и легитимных приложений от вредоносного кода вроде BERserk. **McAfee Application Control** позволяет управлять разрешениями на запуск приложений в среде предприятия при помощи белых списков и политик принудительного соблюдения правил, действующих как на подключенных, так и на не подключенных к сети конечных точках.

- **Динамические белые списки.** Автоматическое создание белых списков приложений при установке исправлений и обновлении систем позволяет организации эффективно управлять разрешениями на запуск приложений. McAfee Application Control снижает подверженность систем уязвимости BERserk, не позволяя выполнять приложения, обращающиеся к коду уязвимого алгоритма проверки цифровых подписей RSA.

- **Репутация файлов.** Интеграция с McAfee Global Threat Intelligence дает решению McAfee Application Control возможность в режиме реального времени запрашивать информацию о безопасных, опасных и неизвестных типах файлов, что помогает компании поддерживать осведомленность о новых угрозах вроде BERserk.
- **Защита независимо от наличия подключения к сети.** Обеспечение защиты на подключенных и не подключенных к сети серверах, виртуальных машинах, конечных точках и устройствах с фиксированными функциями, таких как терминалы для приема платежей.

McAfee Email Gateway
Компаниям важно знать наверняка, является ли электронное сообщение в папке «Входящие» безопасным или вредоносным. Злоумышленники могут применять направленный фишинг, заставляя ничего не подозревающих жертв самостоятельно инициировать потенциально опасные для них действия с помощью встроенных в сообщения вредоносных программ или URL-адресов. **McAfee Email Gateway** обеспечивает защиту от такого рода атак несколькими способами.

- **ClickProtect.** Устранение угроз, исходящих от внедренных в электронные сообщения URL-адресов, путем проверки адреса в момент перехода по ссылке. Проверка URL-адреса включает проверку репутации и упреждающую эмуляцию действий средствами ядра McAfee Gateway Anti-Malware Engine.
- **Интеграция с McAfee Advanced Threat Defense.** Обнаружение сложных и скрытых вредоносных программ путем глубинного статического и динамического анализа кода в подозрительных файлах вложений с последующим блокированием вредоносных файлов до того, как они попадут в папку «Входящие».
- **Интеграция с McAfee Global Threat Intelligence.** Благодаря объединению информации о сетевой активности с данными проверки репутации с помощью McAfee Global Threat Intelligence обеспечивается наиболее полная защита от угроз во входящих сообщениях, от нежелательной почты и вредоносных программ.

McAfee Global Threat Intelligence
McAfee Global Threat Intelligence (GTI) — комплексная облачная служба, которая выполняет сбор информации об угрозах в режиме реального времени. Интегрированная в продукты безопасности McAfee технология блокирует киберугрозы по всем направлениям, включая файлы, веб-трафик, электронную почту и сеть. Упреждающая защита от злоупотребления доверием обеспечивается следующими функциями.

- **Репутация сертификатов.** Запрос в режиме реального времени информации о надежных и опасных сертификатах для защиты вашей компании от таких угроз, как вредоносные программы с цифровыми подписями, распространяемые сетями вредоносной рекламы.
- **Репутация файлов.** Защита от приложений-подделок и осведомленность о приложениях, подверженных уязвимости BERserk. Запрос в режиме реального времени информации о надежных, опасных и неизвестных файлах для поддержания уровня безопасности.
- **Сбор информации путем сопоставления векторов угроз.** Сбор и сопоставление информации по всем ключевым направлениям угроз — файлы, веб-трафик, электронная почта, сеть — с целью обнаружения таких угроз, как распространение рекламными сетями вредоносных программ с цифровыми подписями, направленный фишинг посредством электронных сообщений, попутная загрузка вредоносных файлов с опасных веб-сайтов или взломанных «доверенных» узлов.
- **Security Connected.** Интеграция с другими технологиями McAfee обеспечивает получение всесторонней информации об угрозах, позволяет наиболее точно сопоставлять данные и гарантирует высочайшую степень интеграции для защиты от атак, основанных на злоупотреблении доверием.

McAfee Vulnerability Manager
Атаки, подобные BERserk, формируют постоянно меняющийся ландшафт угроз, ставящий под удар модель доверия. Оценка наличия риска и масштабов уязвимости предприятия для этих новых атак может казаться пугающе сложной задачей. Вот лишь некоторые возможности **McAfee Vulnerability Manager** и **McAfee Asset Manager**, использование которых поможет вашей компании выявить уязвимости, подобные BERserk, и принять необходимые меры по эффективному их устранению:

- **Комплексная проверка на наличие уязвимостей.** McAfee Vulnerability Manager — автономное решение с высоким уровнем масштабируемости для обнаружения узлов, управления активами, оценки уязвимостей и составления отчетов обо всех подключенных к сети устройствах. McAfee Vulnerability Manager может выполнять проверку на наличие уязвимости BERserk, анализируя системы, в которых выполняются уязвимые версии Firefox, Chrome и других продуктов, использующих код уязвимого алгоритма проверки цифровых подписей RSA.
- **Настраиваемые алгоритмы проверки для поиска новых угроз.** Редактор сценариев Foundstone Scripting Language (FSL) Editor позволяет расширять набор стандартных проверок и обновлений, необходимых для обнаружения угроз «нулевого дня» и уязвимостей вроде BERserk, путем создания собственных сценариев и правил проверки для оценки вашей среды. Решение McAfee Vulnerability Manager способно обнаруживать системы, подверженные уязвимости BERserk, используя алгоритмы проверки, уже имеющиеся в комплекте поставки по состоянию на 24 сентября 2014 года.
- **Гибкие средства отчетности и устранения уязвимостей.** McAfee Vulnerability Manager и McAfee Asset Manager совместно предоставляют автоматизированные средства мониторинга и управления для проверки, устранения уязвимостей, принудительного соблюдения правил и формирования отчетов. Это позволяет избегать беспорядочных и неорганизованных процессов, отнимающих время, исключает возможные ошибки и повышает эффективность защиты систем.
- **Знание слабых мест.** Сопоставляя результаты поиска уязвимостей с результатами обнаружения узлов, McAfee Asset Manager позволяет определять, какие именно системы предприятия подвержены уязвимости BERserk. Системы, в которых выполняются уязвимые версии приложений, обнаруживаются в режиме реального времени, благодаря чему меньше времени затрачивается на поиск уязвимостей и больше времени остается на их устранение.

McAfee Web Gateway
Вредоносная реклама, попутная загрузка и потенциально опасные URL-адреса, встроенные в ссылки на доверенные URL-адреса, — это лишь некоторые виды атак, основанных на злоупотреблении доверием. **McAfee Web Gateway** усилит защиту вашей компании от такого рода угроз.

- **Ядро McAfee Gateway Anti-Malware Engine.** Бессигнатурные средства анализа намерений 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. Благодаря уникальным функциям проверки ядро McAfee Web Gateway является лучшим на рынке средством блокирования загрузки вредоносных файлов.
- **Интеграция с 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 SiteAdvisor® Enterprise
Оставаться на высоте при постоянно меняющемся ландшафте угроз достаточно сложно, особенно если стоит задача защитить пользователей от таких угроз, как злоупотребление доверием, без применения жестких политик, создающих неудобства в работе.

- **Простое выявление угроз наподобие вредоносных веб-сайтов, представленных под видом легитимных.** Благодаря наглядной системе цветового кодирования **McAfee SiteAdvisor Enterprise** обеспечивает дополнительный уровень защиты на персональном компьютере. McAfee SiteAdvisor Enterprise отклоняет подключения к заведомо вредоносным веб-сайтам и сообщает пользователям об опасности.
- **Усиленная защита благодаря службе McAfee GTI.** Служба McAfee GTI в режиме реального времени предоставляет системе McAfee SiteAdvisor Enterprise информацию об угрозах, позволяя последней оценивать веб-сайты на основе актуальных сведений.

McAfee Threat Intelligence Exchange
Злоупотребление доверием может принимать различные формы. Именно поэтому жизненно необходимо иметь интеллектуальную платформу, способную адаптироваться с учетом постоянно меняющихся потребностей. **McAfee Threat Intelligence Exchange (TIE)** значительно снижает подверженность атакам благодаря способности обнаруживать вредоносные сертификаты в среде организации.

- **Репутация сертификатов.** Интеграция с McAfee GTI позволяет в режиме реального времени запрашивать информацию об опасных и безопасных сертификатах, обеспечивая защиту от атак, основанных на использовании вредоносного кода с цифровыми подписями. McAfee TIE может защитить конечные точки от вредоносных сертификатов, используя централизованно управляемые политики, которые могут быть развернуты на всех конечных точках независимо от того, подключены они к сети или нет.
- **Предотвращение «боковой загрузки» DLL-файлов, блокирование программ-подделок и защита от других атак.** Передовая технология защиты конечных точек принимает решения о запуске исполняемых файлов на основании установленных правил, учитывающих контекст конкретной конечной точки (файл, процесс, характеристики среды) и общую информацию об угрозах.
- **Признаки взлома.** Импорт хэшей известных вредоносных файлов и опасных сертификатов в McAfee TIE позволяет защитить среду от их воздействия путем принудительного применения политик. Если в системе обнаружены какие-либо признаки взлома, McAfee TIE завершает все процессы и прекращает работу всех приложений, связанных с данными признаками взлома.

McAfee VirusScan® Mobile Security

- **Блокирование программ-подделок.** При поддержке службы McAfee GTI решение **McAfee VirusScan Mobile Security** блокирует приложения, содержащие вредоносные программы-подделки, практически в режиме реального времени. Решение обнаруживает вредоносные программы в течение менее чем 200 миллисекунд, при этом не оказывая негативного влияния на производительность и скорость беспроводного соединения.

Защита компании от действий злоумышленников, стремящихся злоупотреблять моделью доверия, может оказаться трудной задачей. Однако технологии защиты McAfee помогают реализовать упреждающую защиту от атак, основанных на злоупотреблении доверием пользователей.

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