Краткий обзор решения

Защита от потенциально нежелательных программ

Потенциально нежелательные программы (ПНП) подробно описаны в **«Отчете McAfee® Labs об угрозах за февраль 2015 года»**. «Потенциально нежелательной программой» можно считать любое приложение, которое пользователь считает полезным, но которое подспудно подвергает его ощутимому риску. Такие приложения, как правило, сами не информируют пользователей о наличии таких рисков. В отличие от троянских коней, вирусов, руткитов и других видов вредоносных программ потенциально нежелательные программы, как правило, не собирают учетные данные пользователей (для входа в социальные сети, интернет-банкинг и прочие системы) и не вносят вредоносные изменения в системные файлы. С точки зрения классификации ПНП находятся в «серой зоне», потому что они не только подвергают пользователей риску, но и нередко приносят им пользу. Их часто бывает трудно обнаружить и классифицировать.

Вот некоторые примеры действий, характерных для ПНП:

- несанкционированное изменение системных настроек, например конфигурации браузера;
- скрытое размещение «непрошеной» программы внутри законного приложения;
- тайный сбор информации о пользователе, посещаемых им веб-сайтах и конфигурации системы;
- сокрытие факта установки приложения;
- процесс удаления приложения затруднен;
- распространение посредством дезориентирующей или лживой рекламы.

ПНП бывают разных видов:

- **программы для показа рекламы:** показывает рекламу, в основном через браузер;
- **взломщик/демаскировщик паролей:** отображает скрытый пароль приложения;
- **средство удаленного администрирования:** отслеживает действия пользователя в локальной системе или позволяет удаленно управлять системой без ведома или согласия пользователя;
- **программа для генерации лицензионных ключей:** генерирует ключи продукта для законных приложений;

intel Security

- **перехватчик браузера:** изменяет домашнюю страницу, страницу поиска, настройки браузера и т. д.;
- **хакерские инструменты:** автономные приложения, дающие возможность проникать в системы или красть критически важные данные;
- **прокси:** перенаправляет пользователя или скрывает информацию, касающуюся IP-адреса;
- **средства слежения за пользователем:** шпионские программы или клавиатурные шпионы, отслеживающие нажатие клавиш пользователем, записывающие личные сообщения, осуществляющие мониторинг действий пользователя в Интернете или создающие снимки экрана без ведома пользователя.

В следующей таблице приведены основные различия между ПНП и другими вредоносными программами (троянскими конями, программами-вымогателями, ботами, вирусами и т. п.):

Свойства	Потенциально нежелательные программы	Другие вредоносные программы: троянские кони, вирусы, боты
Способ установки	Стандартная процедура установки приложений, иногда с лицензионным соглашением. Для полной установки в системе часто требуется согласие и участие пользователя.	Устанавливается в виде автономной программы без участия пользователя. Функционирует в основном как независимый файл.
Упаковка	Поставляется в комплекте с законными приложениями и скрытно устанавливается вместе с законным приложением.	Автономные файлы с небольшим числом дополнительных компонентов. Не упаковываются в виде установщиков.
Удаление	Иногда в пакет входит программа удаления, позволяющая удалить приложение. Процедура удаления часто затруднена.	Исполняемые файлы еще больше усложняют процесс удаления вредоносного ПО из-за наличия точек перехвата других процессов, открытых дескрипторов процессов и других сложных взаимосвязей. Поскольку это не установочные пакеты, в Панели управления они не отображаются.
Поведение	Отображает непрошеную рекламу, всплывающие окна и окна, выскакивающие при закрытии страницы. Изменяет настройки браузера, собирает данные о пользователе и системе или позволяет удаленно управлять системой без ведома или согласия пользователя.	Крадет идентификационные данные и банковскую информацию, изменяет системные файлы, делает систему непригодной для использования, вымогает деньги и т. д.
Скрытность	Поведение, как правило, не является скрытным.	Может скрывать файлы, папки, записи реестра и сетевой трафик.

Среди всех категорий ПНП наибольшее внимание поставщиков средств защиты привлекли программы для показа рекламы, причем не из-за назойливой рекламы, а из-за того, как такие программы злоупотребляют доверием пользователей. Современные программы для показа рекламы стали интеллектуальнее: в них реализован ряд методов, обеспечивающих их постоянное присутствие в зараженных системах. Вот некоторые из этих методов:

- автономный процесс, запущенный в памяти;
- библиотеки DLL, являющиеся и не являющиеся компонентами COM, с функциями, созданными для конкретного приложения;
- разделы реестра, относящиеся к вспомогательным объектам браузера;
- библиотеки DLL, подключенные к системным процессам;
- расширения и подключаемые модули для браузеров;
- зарегистрированные системные службы;
- компоненты драйверов устройств, выполняющие функции управления устройствами;
- низкоуровневые драйверы фильтров;
- троянские кони, доставляемые в виде действующей нагрузки.

ПНП, как правило, распространяются путем злоупотребления доверием ничего не подозревающих пользователей (см. **«Отчет McAfee Labs об угрозах за ноябрь 2014 года**). Самыми популярными методами распространения ПНП являются следующие:

- скрытная загрузка в одном комплекте с законными приложениями;
- социотехнические атаки;
- продажа голосов «Мне нравится» в Facebook;
- публикация мошеннических сообщений в Facebook;
- несанкционированное использование Google AdSense;
- непреднамеренная установка расширений и подключаемых модулей для браузеров;
- принудительная установка вместе с законными приложениями.

Как защититься от ПНП с помощью Intel Security

McAfee Application Control

McAfee Application Control позволяет управлять разрешениями на запуск приложений в среде предприятия при помощи белых списков и политик принудительного соблюдения правил как на подключенных, так и на не подключенных к сети конечных точках. Это защитит вашу компанию от потенциально нежелательных программ.

- **Динамические белые списки.** Автоматическое создание белых списков приложений при установке исправлений и обновлении систем дает вашей организации возможность эффективно управлять разрешениями на запуск приложений. McAfee Application Control не допускает выполнения известных программ для показа рекламы, снижая тем самым риски, связанные с ПНП.
- **Репутация файлов.** Будучи интегрированным с **McAfee Global Threat Intelligence** (McAfee GTI), McAfee Application Control имеет возможность запрашивать информацию о безопасных, опасных и неизвестных типах файлов, собираемую в режиме реального времени. Эта информация помогает составлять белые списки и выявлять ПНП.
- **Защита вне зависимости от наличия подключения к сети.** Обеспечение защиты на подключенных и не подключенных к сети серверах, виртуальных машинах, конечных точках и устройствах фиксированного назначения, таких как терминалы для приема платежей.

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 ПНП. **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. Ядро McAfee Gateway Anti-Malware Engine выполняет проверку файлов и в случае признания их вредоносными блокирует возможность их загрузки пользователями.
- **Интеграция с McAfee GTI.** Получение собираемой с помощью McAfee GTI информации о репутации файлов, репутации веб-сайтов и категориях веб-содержимого в режиме реального времени позволяет обеспечить защиту от новейших угроз, потому что дает McAfee Web Gateway возможность отклонять попытки подключения к заведомо вредоносным веб-сайтам и веб-сайтам, связанным с сетями распространения вредоносной рекламы.

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence (McAfee GTI) — это комплексная облачная служба, которая выполняет сбор информации об угрозах в режиме реального времени. Она дает продуктам McAfee возможность блокировать киберугрозы по всем векторам: в файлах, в веб-трафике, в электронной почте и в сети. Упреждающая защита от ПНП обеспечивается благодаря наличию следующих функций:

- **Сбор информации путем сопоставления векторов угроз.** Сбор и сопоставление информации по всем ключевым направлениям распространения угроз (файлы, веб-трафик, электронная почта, сеть) позволяет обнаруживать такие комбинированные угрозы, как, например, рекламные сети, распространяющие вредоносные программы с цифровыми подписями.
- **Платформа для комплексного сбора информации об угрозах.** Данные об угрозах поступают с миллионов датчиков, установленных на развернутых у клиентов продуктах McAfee: решениях для защиты конечных точек, веб-трафика и электронной почты; системах предотвращения вторжений в сеть; брандмауэрах и т. п.
- **Репутация сертификатов.** Возможность в режиме реального времени запрашивать информацию о надежных и опасных сертификатах позволяет вам защитить свою компанию от таких угроз, как вредоносные программы с цифровыми подписями, распространяемые вредоносными рекламными сетями.
- **Security Connected.** Интеграция с другими защитными продуктами McAfee позволяет получать широкий спектр данных об угрозах, точно сопоставлять полученные данные и обеспечивать максимально полную интеграцию продуктов с целью защиты от программ для показа рекламы.

McAfee SiteAdvisor® Enterprise

Ландшафт угроз постоянно меняется, поэтому быть всегда на высоте — сложная задача, особенно если необходимо обеспечить защиту пользователей от таких угроз, как ПНП, без применения жестких политик, создающих неудобства в работе.

- **Простой механизм выявления таких угроз, как вредоносные веб-сайты, выдающие себя за безобидные.** Благодаря наглядной системе цветового кодирования **McAfee SiteAdvisor Enterprise** служит дополнительным уровнем защиты пользователя персонального компьютера. Он отклоняет подключения к заведомо вредоносным веб-сайтам и сообщает пользователям о существующей опасности.
- **Усиленная защита на базе McAfee GTI.** Получая от McAfee GTI информацию об угрозах, собираемую в режиме реального времени, McAfee SiteAdvisor Enterprise оценивает веб-сайты на основе самых актуальных данных.

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.
- **Репутация сертификатов.** Интеграция с McAfee GTI дает вашей компании возможность в режиме реального времени запрашивать информацию о надежных и опасных сертификатах, обеспечивая тем самым защиту от атак, проводимых с использованием вредоносного кода с цифровыми подписями. McAfee Threat Intelligence Exchange 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.

McAfee VirusScan® Enterprise

McAfee VirusScan Enterprise позволяет легко обнаруживать и удалять вредоносные программы, включая программы для показа рекламы. В McAfee VirusScan Enterprise используется получивший широкое признание специалистов модуль сканирования McAfee, позволяющий обеспечить защиту систем 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.

Защита компании от ПНП, стремящихся обойти традиционные модели доверия с помощью злонамеренных и нежелательных форм поведения, может оказаться нелегкой задачей. Объединение ведущих в отрасли исследований McAfee Labs и технологий Intel Security помогает компаниям защититься от потенциально нежелательных программ.

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