Traps: расширенная защита рабочих станций

Технологический обзор

Март 2015 г.

Уважаемый читатель!

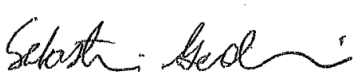
За три недели до того, как я начал писать это письмо, я работал главным ИТ-специалистом по обеспечению безопасности в крупной международной корпорации. Наши корпоративные и клиентские данные хранились в 400 офисах в 20 странах мира.

Если вы находитесь в том же положении, это значит, что коллеги, инвесторы и клиенты доверяют вам сохранность своей информации. Несомненно, вы используете многоуровневую защиту, чтобы гарантировать безопасность данных. Проблема в том, что существующие технологии не справляются со своими задачами. Наши рабочие станции все равно заражаются вирусами. Мы тратим много времени на установку исправлений, сбор данных о системах, их восстановление в случае неполадок и даже на повторное развертывание образов. Но гораздо эффективнее было бы потратить его на предотвращение атак.

Из этого документа вы узнаете, как это сделать. Решение Traps для расширенной защиты рабочих станций — это уникальный продукт. За годы своей работы я встречался со множеством разработчиков, которые демонстрировали свои решения по защите от вредоносных программ и комплексных постоянных угроз, средства обнаружения угроз и реагирования для рабочих станций, а также инструменты кибербезопасности. И только продукт Traps действительно оказался способен предотвращать эксплойты, которые раньше никак не удавалось контролировать, — даже угрозы нулевого дня! Это решение так мне понравилось, что я решил сам перейти работать в Palo Alto Networks и рассказать о нем коллегам в моей отрасли.

Traps — это не просто новый продукт, но целая новая категория систем, с которой мы сможем совершенно по-другому взглянуть на защиту рабочих станций. Читайте дальше, и я расскажу вам, как она работает.

С уважением,



Себастьян Гудвин (Sebastian E. Goodwin)
Директор Traps Advanced Endpoint Protection

Введение

Кибератаки — это атаки, направленные на сети или рабочие станции с целью нанесения ущерба, кражи данных или для чего-либо другого, связанного с захватом чужих компьютерных систем. Кибератаки обычно осуществляются следующим образом: либо пользователь непреднамеренно запускает вредоносный исполняемый файл, либо для запуска вредоносного кода без ведома пользователя используется какая-то уязвимость в обычной программе.

Хотя на рынке имеется множество продуктов для обеспечения безопасности рабочих станций, которые якобы способны решить эту проблему, достаточно открыть любую газету и убедиться, что вирусные атаки по-прежнему происходят с пугающей частотой. Для защиты рабочих станций от комплексных угроз необходим новый подход.

Почему рабочие станции по-прежнему заражаются вирусами?

В традиционных решениях вопроса безопасности используются методы, которые уже не справляются с постоянно меняющимся ландшафтом угроз. Самые совершенные на сегодняшний день угрозы используют уязвимости в регулярно запускаемых программах. Они попадают на компьютеры в виде стандартных документов (например PDF, RTF, DOC, PPT, XLS), либо могут быть адаптированы для атаки специализированного отраслевого ПО. Эти файлы открываются в своих приложениях и отображают содержимое без каких-либо ошибок, однако в них встроен вредоносный код. Этот код использует уязвимость в открытом приложении для запуска атакующего алгоритма. При этом ваш пакет защиты от вредоносного ПО может работать, но ничего не обнаружит, а вместо этого будет искать зараженный исполняемый файл со знакомым ему вирусом или какой-то другой проблемный сигнал. К сожалению, о проблеме может вообще ничего не сигнализировать. До недавнего времени единственным способом защиты от известных уязвимостей была установка исправлений. Надежного способа обезопасить систему от неизвестных угроз не существовало.

А поскольку исправления выходят не сразу, уязвимости долгое время оставляют систему незащищенной и приводят к рискам.

Лучше предотвратить, чем обнаружить

Еще не так давно специалисты в области информационной безопасности считали, что защитить рабочие станции от подобных потенциальных угроз практически невозможно. Наши усилия были направлены на обнаружение и реагирование. Однако с тех было обнаружено немало вредоносного ПО, которое спокойно похищало наши данные в течение многих месяцев и даже лет. Большинство из нас не хотят больше использовать существующую стратегию. Необходим новый подход, который позволит нам снова поверить в безопасность рабочих станций. В его основе должен лежать принцип реального предотвращения атак, а не только их обнаружения. Мы назвали этот подход “расширенной защитой рабочих станций”.

Расширенная защита рабочих станций должна обеспечивать следующие возможности:

1. Предотвращение любых эксплойтов, в том числе использующих неизвестные уязвимости нулевого дня.
2. Предотвращение запуска любых вредоносных исполняемых файлов даже при отсутствии информации об этих файлах.
3. Запись подробных аналитических данных о предотвращенных угрозах, позволяющая определить цели и использованные методы атаки, усилив таким образом защиту организации на всех уровнях.
4. Широкие возможности масштабирования, низкое потребление ресурсов и минимальное вмешательство в работу имеющихся систем.
5. Тесная интеграция с сетевыми и облачными системами обеспечения безопасности для быстрого обмена данными и одновременной защиты информации множества компаний.

Принцип работы Traps

Traps™ представляет собой решение для расширенной защиты рабочих станций, способное предотвращать изощренные атаки с использованием эксплойтов или вредоносных исполняемых файлов еще до выполнения каких-либо злонамеренных действий вне зависимости от установленных исправлений программ.

При попытке атаки Traps сразу же блокирует выполняемые ей операции, завершает процесс

и сообщает о предотвращении угрозы пользователям и системным администраторам. После блокирования атаки Traps собирает подробные аналитические данные, включающие название вредоносного процесса, состояние памяти во время блокировки и другую информацию, а затем создает отчеты для Endpoint Security Manager.

Полная защита от множества типов атак

Атаки бывают разного вида и происходят через множество каналов, в том числе через веб-страницы, электронную почту или внешние накопители. Большинство традиционных продуктов для обеспечения безопасности рабочих станций защищают их от вредоносных исполняемых файлов — наименее изощренной из имеющихся угроз. Однако самыми эффективными и целенаправленными являются атаки, осуществляемые с использованием вроде бы безобидных файлов данных, открываемых самыми обычными приложениями. Например, вредоносный код может содержаться в файлах Microsoft Word или PDF-документах. Сразу после открытия файла в обычной программе вредоносный код активизируется и начинает эксплуатировать ее уязвимости. Таким образом он получает возможность запускать новый код и в результате полностью захватить контроль над рабочей станцией. Такая атака называется эксплойтом.

Решение Traps защищает рабочие станции как от вредоносного ПО в виде исполняемых файлов, так и от эксплойтов, содержащихся в файлах данных, а также от атак, осуществляемых по сети.

Предотвращение эксплойтов

Большинство изощренных угроз работают путем помещения вредоносного кода в кажущийся безобидным файл данных. При открытии файла этот код использует уязвимость в запущенном приложении для активизации атакующего алгоритма. Поскольку политика безопасности не блокирует эксплуатируемое приложение, атаки подобного типа обходят разрешенный список системы защиты. Отличие Traps от других систем безопасности состоит в том, что данное решение обнаруживает типичные алгоритмы, используемые большинством программ-эксплойтов. Несмотря на то, что существуют тысячи эксплойтов, они на самом деле используют лишь небольшой набор алгоритмов, который редко меняется. Более того, для успеха эксплойта должен сработать целый ряд таких алгоритмов. Traps делает все эти приемы абсолютно неэффективными, гарантируя, что приложение перестанет быть уязвимым.

В каждый запускаемый процесс внедряется агент Traps. Если атакующий процесс попытается воспользоваться программной уязвимостью, то эксплойт потерпит неудачу, поскольку защитные модули Traps уже обезопасили процесс от подобных действий. После предотвращения угрозы агент Traps завершает вредоносный процесс и передает всю информацию о нем на сервер Endpoint Security Manager (ESM).

По умолчанию политика Traps блокирует более 100 процессов. Для каждого из них используются десятки специализированных модулей предотвращения эксплойтов. Но в отличие от других

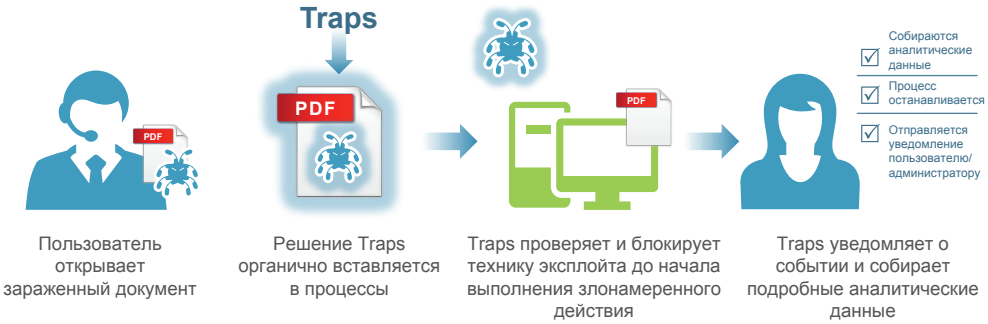


Рисунок 1: Предотвращение эксплойтов — как это выглядит для пользователей.

продуктов, Traps позволяет защитить не только эти процессы и приложения. С помощью Traps наши пользователи могут сами обеспечивать безопасность самых разных приложений и процессов, просто добавляя их в настройки. Это оказывается особенно удобно для специализированных программ в конкретных отраслях. Traps позволяет защитить от эксплойтов системы для торговых точек (POS), торговые автоматы, системы SCADA и любые другие

приложения.

Если по какой-то причине возникает конфликт между приложением и защитным модулем, просто отключите этот модуль для данного компьютера и приложения. Приложение будет по-прежнему защищено десятками других модулей. Поскольку для успешного запуска эксплойтам необходимо использовать последовательность различных алгоритмов, другие защитные модули заблокируют как минимум один из этих алгоритмов и таким образом разорвут цепочку.

Модули предотвращения эксплойтов позволяют избежать следующих типов атак:

- Перехват динамической библиотеки (DLL) — замена обычной DLL на вредоносную DLL с таким же именем
- Перехват потока управления программой
- Вставка вредоносного кода в качестве обработчика исключений

Защита от вредоносных исполняемых файлов

Traps позволяет не только защититься от эксплойтов, скрытых в файлах данных или запускаемых по сети, но и использует комплексный подход для предотвращения запуска вредоносных исполняемых файлов. Пользователи часто непреднамеренно загружают и запускают вредоносные исполняемые файлы (вредоносное ПО), не подозревая об опасности. Механизм Traps для защиты от вредоносного ПО сочетает ограничения на базе политик, анализ WildFire™ и защитные модули, которые позволяют избежать запуска вредоносных исполняемых файлов. При одновременном использовании этих методов уровень защиты от вредоносного ПО становится поистине беспрецедентным. Вот как работает этот процесс.

Ограничения на основе политик: Ограничения на основе политик предотвращают выполнение программ в сценариях с высоким риском, что позволяет значительно сократить потенциальные возможности для атак. Например, можно запретить запуск файлов определенного типа напрямую с USB-накопителя или из папок, не являющихся папками приложений.

Расширенный контроль выполнения: Для эффективного предотвращения атак необходим многоуровневый подход с постоянным контролем потенциальных каналов проникновения угроз на каждом этапе атаки. Решение Traps поддерживает функции детализированного управления запуском программ, позволяющие существенно ограничить возможность выполнения вредоносного кода. К ним относятся следующие функции:

1. Ограничения выполнения. Предусмотренный в Traps расширенный контроль ограничений обеспечивает детализированное управление политиками в отношении локальных и сетевых папок, дочерних процессов, внешних накопителей и неподписанных исполняемых файлов. Эти ограничения позволяют вашему бизнесу легко адаптироваться и исключать риски, связанные с безопасностью.

2. Детализированная защита системы. Для относительно статичных или узкоспециализированных систем можно единоразово указывать допустимые и запрещенные исполняемые файлы. Это осуществляется при помощи файловых хеш-кодов. Хотя интеграция с WildFire обеспечивает динамический анализ файлов, данные параметры политик позволяют на локальном уровне отказываться от рекомендаций WildFire и выбирать другое решение.

Анализ и предотвращение запуска исполняемых файлов с помощью WildFire: Интеграция с WildFire позволяет задавать детализированные параметры запуска и одновременно использовать динамические политики безопасности с автоматическим анализом неизвестных исполняемых файлов. Если на рабочей станции появился новый, никогда ранее не виденный исполняемый файл, Traps может незамедлительно отправить хеш-код файла в WildFire для идентификации. Если WildFire сообщит о том, что файл является вредоносным, Traps предотвратит его запуск и не позволит этому файлу нанести какой-либо ущерб. Каждый день в WildFire анализируется почти два миллиона образцов, так что скорее всего система уже сталкивалась с потенциально опасным файлом и обязательно уведомит об этом Traps. Если файл окажется незнакомым WildFire, можно автоматически загрузить его в систему и быстро проанализировать на предмет угроз. Поскольку загружать файлы в WildFire может как Traps, так и межсетевые экраны нового поколения, происходит эффективный обмен данными об угрозах между межсетевыми экранами и рабочими станциями.

Модули защиты от вредоносного ПО: Если вредоносный файл все-таки запустился, его действия все равно можно заблокировать при помощи модуля защиты от вредоносного ПО. В отличие от модулей предотвращения эксплойтов, защитные модули выполняют поиск стандартных

алгоритмов, используемых многими типами программ-злоумышленников. Например, они предотвращают внедрение вредоносного кода в доверенные приложения.

Сбор аналитических данных

Обширную информацию можно получить при помощи агента Traps. Агент постоянно

Рисунок 2: Эффективное предотвращение запуска вредоносных исполняемых файлов.

записывает подробные сведения по каждому запускаемому процессу и отправляет их ESM-серверу. Кроме того, агент выдает предупреждения при обнаружении попыток остановить работу Traps, удалить программу или иным образом вмешаться в ее функционирование. После предотвращения атаки с рабочей станции можно собрать дополнительную информацию, например сделать снимок памяти и зафиксировать действия, предпринятые вредоносным кодом. Сделав снимок, Traps выполняет вторичный анализ содержания инцидента и ищет в памяти возможные следы злонамеренных действий.

Следует учитывать, что аналитические данные, получаемые после предотвращения атаки, неизбежно являются менее полными, чем данные по успешным атакам, причинившим вред.

Преимущества подхода Traps

Защита от уязвимостей нулевого дня и неизвестного вредоносного ПО: Вам больше не придется ждать обновления сигнатур или отслеживать симптомы возможного вторжения — вы уже защищены от самых новых и изощренных угроз.

Удобный вам график установки исправлений: Поскольку исправления выходят не сразу, уязвимости долгое время оставляют систему незащищенной, а установка исправлений отнимает много времени и сил. Необходимо тщательно протестировать исправления и своевременно развернуть их на всех рабочих станциях. Для ИТ-отделов это совсем не простая задача. Более того, практически в каждой организации имеются устаревшие, но необходимые системы, на которые по тем или иным причинам исправления установить нельзя. Расширенная защита рабочих станций позволяет обеспечить их безопасность вне зависимости от наличия исправлений.

Защита любых приложений от эксплойтов: За счет того, что наше решение отслеживает алгоритмы эксплойтов, а не уникальные характеристики отдельных программ, его можно использовать для защиты любых приложений. Большинство систем безопасности рабочих станций способны защитить от эксплойтов лишь несколько самых популярных программ. Однако наш подход позволяет пользователям обеспечить безопасность сотен специализированных приложений.

Минимальный ущерб для производительности: Наш подход не опирается на сканирование системы, виртуализацию и другие ресурсоемкие технологии. Агент потребляет минимум

ресурсов и не затрагивает работу программ. Он может оставаться полностью невидимым для конечных пользователей.

Экономия времени и средств: За счет предотвращения атак вы сможете избавиться от затрат, связанных с простоем работы и восстановлением систем, которые часто оказываются неизбежными при заражении вредоносным ПО, особенно когда необходимо повторное развертывание образов.

Простота управления и нечастые обновления: Одним из недостатков традиционных систем защиты рабочих станций является необходимость постоянно устанавливать обновления сигнатур. Решение Traps выполняет обнаружение по небольшому ряду алгоритмов, обычно используемых вредоносным ПО, поэтому частые обновления не требуются.

Анализ угроз за счет интеграции с WildFire: Благодаря интеграции с WildFire клиентам доступна обширная экосистема по анализу угроз, участники которой ежедневно загружают в нее более миллиона образцов. За счет автоматической загрузки и анализа неизвестных исполняемых файлов вы сможете проанализировать каждый новый исполняемый файл на рабочей станции.

Архитектура системы Traps

Консоль Endpoint Security Manager

Инфраструктура Traps поддерживает множество вариантов архитектуры и возможность масштабирования под крупные распределенные среды. При установке ESM в Microsoft SQL Server создается специальная база данных, а в IIS устанавливается консоль администрирования. Поддерживаются версии Microsoft SQL 2008 и 2012. Под ESM может быть выделен новый сервер SQL, либо можно создать базу данных на уже существующем SQL-сервере.

Сервер для рабочих станций можно установить на физических или виртуальных машинах с Windows Server 2008 R2, Windows Server 2012 или Windows Server 2012 R2.

Серверы Endpoint Security Manager

Серверы ESM по сути выступают в роли посредников между агентами Traps и базой данных ESM. Передача данных между агентами Traps и серверами ESM осуществляется по протоколу HTTPS. Серверы ESM не хранят никаких данных, поэтому можно легко добавлять в существующую среду новые серверы или удалять уже имеющиеся по мере необходимости, обеспечивая требуемое резервирование и географический охват.

Если необходимы глобальные подключения, клиенты, не использующие мобильное решение, например Palo Alto Networks® GlobalProtect™, могут установить ESM-сервер в сегменте DMZ или в облачной среде с внешними подключениями. ESM-серверы можно установить на физических или виртуальных машинах с Windows Server 2008 R2, Windows Server 2012 или Windows Server 2012 R2.

Агент Traps

Для установки агента Traps используется пакет MSI объемом около 9 МБ. Установить пакет можно с помощью любого инструмента развертывания ПО. Последующие обновления агента осуществляются через ESM. Агент занимает менее 25 МБ на диске и не более 40 МБ в оперативной памяти во время работы. Наблюдаемая загрузка ЦП составляет менее 0,1 процента. В агенте также используются различные методы для предотвращения вмешательства в его работу, которые не позволяют пользователям и вредоносному коду отключить защиту или изменить конфигурацию агента.

За счет того, что структура среды Traps не потребляет много ресурсов, она поддерживает горизонтальное масштабирование и позволяет создавать крупные системы с 50 000 агентов на каждый сервер ESM. При этом настройка политик и хранение их базы данных по-прежнему осуществляются централизованно. Traps может работать параллельно с большинством популярных решений для безопасности рабочих станций, сохраняя невероятно низкую загрузку ЦП и подсистемы ввода-вывода. За счет минимального

вмешательства в работу имеющихся систем Traps идеально подходит для критически важных инфраструктур, специализированных систем и сред виртуальных рабочих станций.

В настоящее время Traps поддерживает следующие операционные системы на базе Windows.

ОПЕРАЦИОННАЯ СИСТЕМА:

- Windows XP (с пакетом обновления 3 (SP3) или более поздней версии, 32-разрядная);
- Windows 7 (с пакетом обновления 1 (SP1), RTM, 32- и 64-разрядная; все версии, кроме Home);
- Windows 8 (32- и 64-разрядная);
- Windows 8.1 (32- и 64-разрядная);
- Windows Server 2003 (с пакетом обновления 2 (SP2) или более поздней версии, 32-разрядная);
- Windows Server 2003 R2 (с пакетом обновления 2 (SP2) или более поздней версии, 32-разрядная);
- Windows Server 2008 (32- и 64-разрядная);
- Windows Server 2012 (все версии);
- Windows Server 2012 R2 (все версии);
- Windows Vista (с пакетом обновления 2 (SP2), 32- и 64-разрядная).

ВИРТУАЛЬНЫЕ СРЕДЫ:

- инфраструктуры виртуальных рабочих станций;
- Citrix;
- виртуальные машины;
- ESX;
- VirtualBox/Parallels.

АППАРАТНЫЕ ПЛАТФОРМЫ:

- SCADA;
- Windows-планшеты.

Ведение внешнего журнала

Системы ESM могут не только сохранять внутренние логи, но и вести журнал при помощи внешней платформы, например SIEM, SOC или syslog. В организациях, где используется множество ESM-серверов, внешняя платформа позволяет совместно контролировать все базы данных журналов.

Интегрированная платформа безопасности

В 2005 году мы поставили цель разработать “с нуля” платформу безопасности нового поколения, с которой организации могли бы ограничить каналы проникновения угроз и предотвратить самые современные кибератаки. Мы понимали, что для этого необходим революционный подход, который позволял бы пользователям эффективно отслеживать весь сетевой трафик, включал бы инструменты управления для пользователей и приложений, а также помогал создать тесно интегрированную систему безопасности, объединяющую сеть, облако и рабочие станции в общую архитектуру для предотвращения любых потенциальных атак.

Нам удалось реализовать эту стратегию, и сегодня мы предлагаем готовую платформу корпоративной безопасности, состоящую из трех ключевых компонентов: межсетевого экрана нового поколения, облака для анализа угроз и системы расширенной защиты рабочих станций. Эта платформа является интегрированной на самом базовом уровне. С ней вам больше не понадобятся узкоспециализированные инструменты и другие разрозненные технологии. Она упрощает повседневные задачи и повышает эффективность системы безопасности организаций за счет использования многоуровневой модели, позволяющей предотвращать угрозы на каждом этапе атак.

Наша корпоративная платформа безопасности защищает всю структуру вашей организации, от мобильных сотрудников до ядра вашего облачного центра обработки данных. Автоматизация платформы позволяет исключить дорогостоящие ручные операции и дает вашей организации возможность еще эффективнее реагировать на возникающие глобальные угрозы.

paloalto networks
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

Основной тел.: +1.408.753.4000
Отдел продаж: +1.866.320.4788
Служба поддержки: +1.866.898.9087

www.paloaltonetworks.com