Traps: расширенная защита рабочих станций

TRAPS:

Расширенная защита рабочих станций должна обеспечивать следующие возможности:

- Предотвращение любых эксплойтов, в том числе использующих неизвестные уязвимости нулевого дня.
- Предотвращение запуска любых вредоносных исполняемых файлов даже при отсутствии информации об этих файлах.
- Запись подробных аналитических данных о предотвращенных атаках.
- Широкие возможности масштабирования, низкое потребление ресурсов и минимальное вмешательство в работу имеющихся систем.
- Тесная интеграция с сетевыми и облачными системами обеспечения безопасности.

Решение Palo Alto Networks® Traps обеспечивает расширенную защиту рабочих станций, которая предотвращает изощренные атаки эксплойтов, использующих уязвимости системы безопасности, и атаки с помощью ранее неизвестного вредоносного ПО. Traps обеспечивает защиту с помощью облегченного агента с высоким уровнем масштабируемости, основанного на инновационном методе отражения атак без потребности в предварительном знании специфики атаки. Таким образом решение Traps предоставляет организациям мощное средство защиты оконечных устройств практически от всех направленных атак.

Хотя на рынке имеется множество продуктов для обеспечения безопасности рабочих станций, вирусные атаки по-прежнему происходят с пугающей частотой. В традиционных решениях безопасности используются методы, которые уже не справляются с постоянно меняющимся характером угроз. Вместо попыток идентифицировать миллионы отдельных атак или выявить злонамеренное поведение, которое может не поддаваться обнаружению, Traps фокусируется на основных техниках, которые любой злоумышленник использует для реализации атаки. Такой подход позволяет предотвращать атаки еще до того, как нанесен какой-либо вред.

Рисунок 1: Недостатки традиционных подходов к обеспечению безопасности.

Полная защита от разных 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. 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.

Самые совершенные на сегодняшний день угрозы используют уязвимости в регулярно запускаемых программах. Они попадают на компьютеры в виде стандартных документов (PDF, RTF, DOC, PPT, XLS и т. п.), либо могут быть адаптированы для атаки специализированного отраслевого ПО.

paloalto NETWORKS®

Сразу после открытия файла в самой 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.

Принцип действия механизма предотвращения эксплойтов

Независимо от типа атаки и ее сложности, для успеха эксплойта злоумышленнику потребуется выполнить несколько приемов в определенном порядке. Некоторые атаки могут включать в себя больше действий, некоторые — меньше. В любом случае для проникновения на целевое устройство потребуется использовать по крайней мере две или три техники. В решении Traps используется несколько модулей предотвращения эксплойтов, которые помогают минимизировать и блокировать различные техники эксплойта, доступные злоумышленникам. Более того, для успеха эксплойта должен сработать целый ряд таких техник. Traps делает все эти приемы абсолютно неэффективными, гарантируя, что приложение перестанет быть уязвимым.

В каждый запускаемый процесс внедряется агент Traps. Если процесс попытается выполнить какие-либо стандартные алгоритмы атаки, то эксплойт потерпит неудачу, поскольку программа Traps уже обезопасила процесс от подобных действий. Программа сразу же заблокирует эту атаку, завершит выполнение процесса и сообщит о предотвращении атаки пользователю и системному администратору. Кроме того, будет направлен подробный отчет на сервер Endpoint Security Manager (ESM). Поскольку в основе эксплойта лежит последовательная цепочка действий, предотвращения всего одной техники в этой цепи достаточно для блокирования всей атаки.

По умолчанию политика Traps блокирует более 100 процессов. Для каждого из них используются десятки специализированных модулей предотвращения эксплойтов. Но в отличие от других продуктов, Traps позволяет защитить не только эти процессы и приложения.

Фокусируясь на техниках эксплойта, а не на самой атаке, Traps может предотвратить атаку без предварительного знания о наличии уязвимости, независимо от выполненных исправлений и без сигнатур или обновлений ПО. Важно отметить, что Traps не выполняет проверку или мониторинг злонамеренной активности, поэтому, в силу минимального использования ресурсов ЦП и памяти, данный метод предоставляет высокие возможности масштабирования.

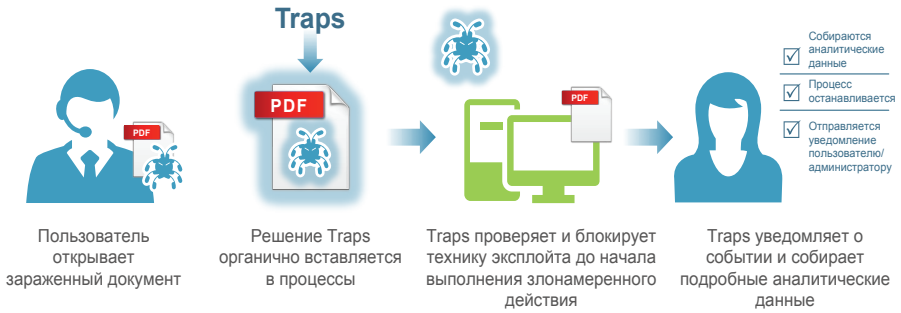

Рисунок 2: Предотвращение эксплойтов — как это выглядит для пользователей.

Защита от вредоносных исполняемых файлов

Traps не только предотвращает эксплойты, но и использует многоуровневый подход для предотвращения запуска вредоносных исполняемых файлов. Для обеспечения комплексной безопасности разработчики решения сосредоточились на трех основных областях. При одновременном использовании следующих методов уровень защиты от вредоносного ПО становится поистине беспрецедентным:

1. **Ограничения на основе политик:** Организации могут легко создавать политики с ограничением конкретных сценариев выполнения. Например, можно запретить запуск файлов из временной папки Outlook или файлов определенного типа с USB-накопителя.
2. **Расширенный контроль выполнения:** Предусмотренный в Traps расширенный контроль обеспечивает детализированное управление глобальными политиками и позволяет контролировать дочерние процессы, папки, неподписанные исполняемые файлы и т. п. Кроме того, защиту можно усилить, если точно указать, каким приложениям и хеш-коду разрешен запуск.

Рисунок 3: Эффективное предотвращение запуска вредоносных исполняемых файлов.

3. **Проверка и анализ WildFire™.** Traps выполняет поиск по хеш-коду в облаке угроз WildFire и отправляет все неизвестные EXE-файлы международному сообществу специалистов для оценки на наличие угроз.
4. **Механизмы минимизации атак с использованием вредоносного ПО.** В Traps используются механизмы минимизации, которые предотвращают угрозы через выявление типичных алгоритмов атак, например внедрения в потоки.

Аналитические данные

Аналитические данные, получаемые после предотвращения атаки, неизбежно оказываются менее полными, чем данные по успешным атакам. Но даже в случае предотвращения атаки можно собрать много важной информации. Собирая аналитические данные о попытке атаки, организации могут применять профилактические меры по защите других оконечных устройств.

Обширную информацию можно получить при помощи агента Traps. Агент постоянно записывает подробные сведения по каждому запускаемому процессу и отправляет их на сервер Endpoint Security Manager (ESM). 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 дамп памяти и зафиксировать действия, предпринятые вредоносным кодом.

Архитектура системы Traps

Endpoint Security Manager — консоль

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.

Endpoint Security Manager — серверы

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.

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 используются различные методы 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 ESM-сервер. 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.

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 позволит совместно контролировать все базы данных журналов.

Охват и поддержка платформ

Traps позволяет обеспечивать безопасность систем без установленных исправлений. Решение поддерживает любые платформы на базе Microsoft Windows, настольные компьютеры, серверы, системы промышленного контроля, терминалы, виртуальные инфраструктуры, виртуальные машины, встроенные системы и т. п. Более того, Traps практически не потребляет ресурсов и позволяет защитить любые процессы, поэтому решение идеально подходит для специализированных систем, таких как ATM, POS или SCADA, и многих других отраслевых приложений с уникальными процессами, защита которых не должна влиять на их работу.

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.

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