Защита от сложных угроз

Windows IT Pro/RE

№7 ИЮЛЬ 2017 | WWW.WINDOWSITPRO.RU | ИНФО ДЛЯ ИТ-ПРО

Мобильная версия

App Store

Google play

Готовимся к экзаменам

Разработка инфраструктуры SharePoint

Оптимизация прикладных приложений SharePoint

Прикладные службы

Оптимизация и мониторинг SharePoint

ISSN 1563-101X

17007

9 771563 101008

Защита от сложных угроз

Противодействие вирусам-шифровальщикам с помощью технологий Microsoft

Владимир Безмалый

Вирусы-шифровальщики стали настоящим бичом нашего времени, и следует признать, что мы живем в эпоху бурного развития данного типа угроз. По статистике компании Kaspersky Lab, в 2016 году возникло 62 новых семейства программ-вымогателей, а количество новых модификаций вымогателей выросло в 11 раз: с 2900 в период с января по март до 32091 в июле–сентябре. С января по конец сентября число атак на компании возросло в три раза: если в январе атаки проводились в среднем каждые две минуты, то в сентябре — уже каждые 40 секунд. Интенсивность атак на пользователей удвоилась: атаки проводились в среднем раз в 20 секунд в начале периода и раз в 10 секунд в конце. Кроме того, каждое пятое предприятие малого или среднего бизнеса, заплатившее выкуп, так и не получило доступ к своим данным.

Как видите, ситуация совсем неутешительна. Что же делать? Естественно, первое, что приходит на ум, — создавать резервные копии, а внутри компании не хранить никакие данные на рабочих станциях сотрудников. Ведь делать резервные копии серверов куда проще, тем более регулярно, несколько раз в сутки. Однако при любых правильно организованных мероприятиях по серверному резервированию всегда существуют риски, что пользователи будут хранить какие-то данные на своем компьютере. Особенно привилегированные пользователи, считающие, что правила написаны не для них. Ведь очень сложно возразить руководителю своей компании и вряд ли даже самому пунктуальному сотруднику отдела ИТ захочется срочно искать новую работу.

Для успешного отражения атак вирусов-шифровальщиков необходимо понимать, как происходит заражение. Атака может идти по нескольким направлениям. Как правило, самый распространенный путь заражения — электронная почта. Сегодня злоумышленники активно используют методы социальной инженерии, эффективность которых, увы, со временем не падает. Преступник может позвонить сотруднику вашей компании и после беседы направить письмо с вложением, содержащим вредоносную ссылку. Сотрудник, безусловно, откроет этот файл, ведь он только что говорил с отправителем по телефону. Это, естественно, один из примеров. К сожалению, от таких атак не застрахован никто. Снизить вероятность подобной атаки можно лишь путем обучения пользователей.

Источником атаки может служить фишинговый сайт, на который пользователь зашел по мошеннической ссылке или случайно нажав

ссылку в почтовом вложении. Все чаще заражение происходит через мобильные устройства сотрудников, с которых они получают доступ к корпоративным ресурсам. И тут привычный антивирус больше не спасает.

Кроме того, часто администраторы либо не устанавливают обновления для системы безопасности, либо делают это значительно позже необходимого срока. Что можно посоветовать в такой ситуации? В данной статье мы рассмотрим несколько технологий от компании Microsoft.

Windows Defender Advanced Threat Protection

Перечислю ключевые особенности данной службы Windows Defender Advanced Threat Protection (WD ATP).

1. Отказоустойчивый, полноценный датчик уровня ядра, который подвержен меньшим рискам, чем установленное «поверх» средство защиты разработки сторонней компании.
2. Высокая производительность, гарантированная Microsoft; решение прошло строгое тестирование в Windows и отвечает требованиям к производительности.
3. Может работать одновременно с любым сторонним антивирусом и файерволом, проблем совместимости приложений нет, так как данная служба работает на базе службы Microsoft Azure и доступ к консоли WD ATP предоставляется через портал securitycenter.windows.com. Компонент ATP разработан Microsoft как часть Windows 10 (модель «Windows как услуга», WaaS), при обновлении операционной системы не возникает ошибок типа «синий экран смерти» (так как для активации расширенных средств обнаружения не требуется реконструирование ядра Windows, достаточно скачать с портала скрипт и распространить его с помощью групповых политик).
4. Возможность проведения расследования:
   - ретроспективный анализ ВСЕХ событий на ВСЕХ конечных пользовательских системах за период до 6 месяцев и глобальный поиск;
   - удобный доступ к функциям глубокого анализа;
   - аналитика угроз из ведущих источников (Microsoft, iSIGHT) встроена в решение.
5. Поведенческий анализ:
   - обнаружение на основе анализа поведения позволяет выявлять неизвестные угрозы и даже «угрозы нулевого дня»;
   - масштабы отслеживания — создание базовой модели нормального поведения для каждой машины на основе данных, полученных с более 1 млрд устройств под управлением Windows;
   - глубина анализа.
6. Это решение на базе «облака», следовательно:
   - не нужны локальные компоненты, имеются неограниченные возможности масштабирования;
   - логика обнаружения с помощью использования «облачных» служб недоступна злоумышленникам для изучения;
   - контроль конечных пользовательских систем, даже когда они не подключены к корпоративному домену;
   - высокий уровень соответствия требованиям и конфиденциальности данных, основанный на строгих отраслевых стандартах.

> С января по конец сентября число атак на компании возросло в три раза: если в январе атаки проводились в среднем каждые две минуты, то в сентябре — уже каждые 40 секунд. Интенсивность атак на пользователей удвоилась: атаки проводились в среднем раз в 20 секунд в начале периода и раз в 10 секунд в конце

Для работы Windows Defender ATP использует:

- ***Датчики поведенческого анализа, встроенные в Windows 10.*** Эти датчики собирают поведенческие сигналы от компонентов операционной системы.
- ***«Облачную» аналитику.*** С помощью технологий Machine Learning в Azure информация собирается с Windows 10, продуктов набора Office, EMS, проводится анализ и рекомендуется то или иное поведение.
- ***Анализ угроз.*** В результате анализа Windows Defender ATP идентифицирует инструменты атакующего, методы и процедуры и генерирует предупреждения, если обнаруживается угроза.

На приведенном рисунке показаны служебные компоненты Windows Defender ATP.

Windows Defender ATP работает как с существующими технологиями безопасности Windows на конечных системах пользователей, такими как Windows Defender, AppLocker и Device Guard, так и со сторонними решениями по обеспечению

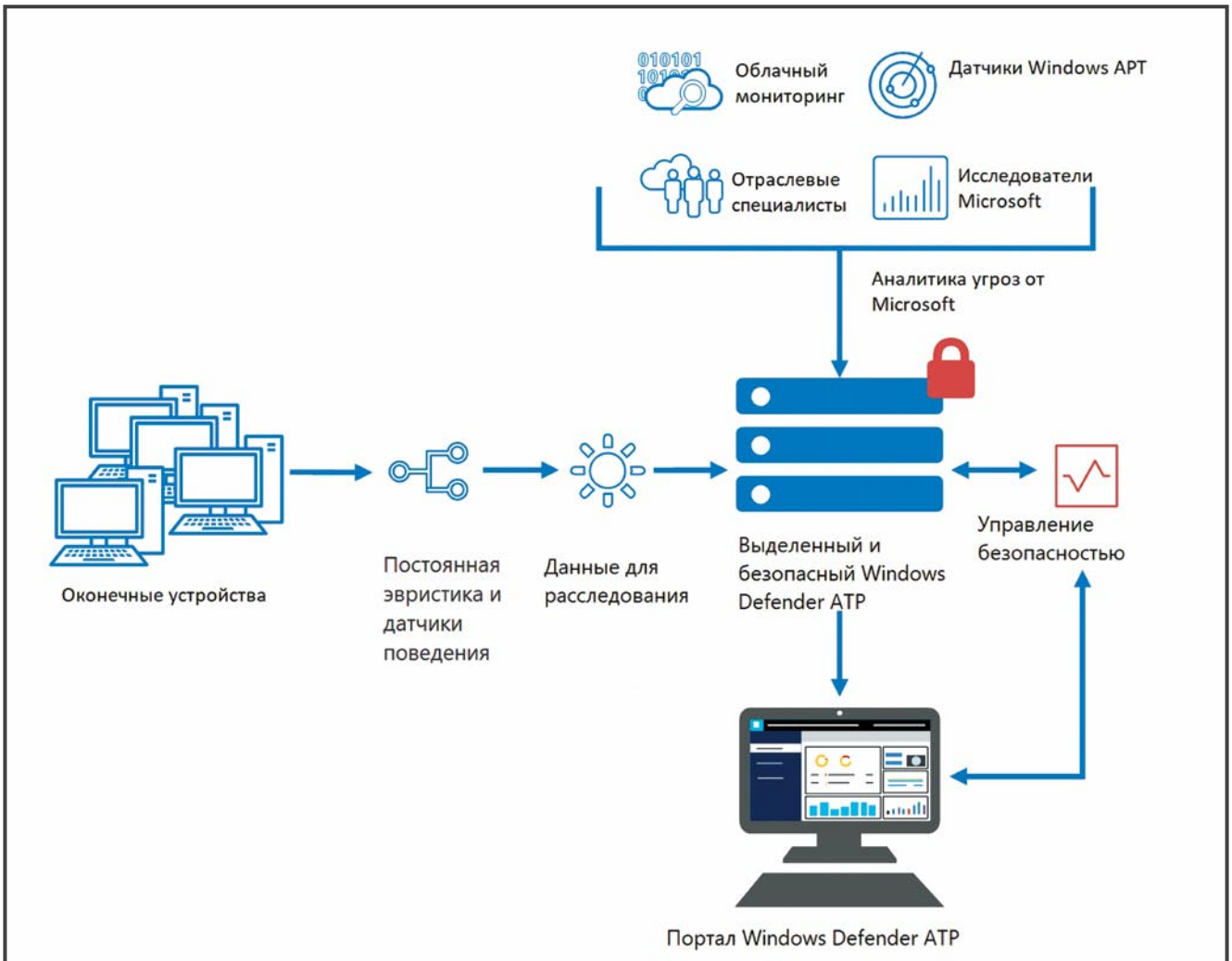

Рисунок. Служебные компоненты Windows Defender ATP

безопасности и антивирусными продуктами.

Device Guard

Служба Device Guard (чаще встречается термин «белый список программ») — метод защиты, основанный на том, что в системе запускается только разрешенное программное обеспечение. Данный метод нуждается в большой подготовительной работе.

Перед внедрением этого метода необходимо составить список программ (с учетом версий), применяемых в вашей организации. Причем не просто составить список, а отсортировать его по компьютерам и пользователям. А затем проверить совместимость компьютеров на предмет возможности настройки на них Device Guard. Увы, стоит признать, что в большинстве организаций подробный учет программ попросту отсутствует и никогда не проводился. Подобная инвентаризация, проводимая в первый раз, занимает много времени и сил. Кроме того, следует учесть, что часто сами пользователи не знают, какое именно программное обеспечение им нужно для выполнения рабочих обязанностей.

Device Guard — сочетание корпоративных функций безопасности оборудования и программного обеспечения, которые можно настроить для блокировки устройства, чтобы на нем запускались только доверенные приложения. Если приложение не является доверенным, оно не будет работать ни при каких условиях. Это также означает, что, даже если злоумышленник получит контроль над ядром Windows, он с гораздо меньшей вероятностью сможет запустить вредоносный код после перезапуска компьютера вследствие метода принятия решений о том, что и когда может запускаться.

Редакция Windows 10 Корпоративная Device Guard задействует новые меры безопасности на основе виртуализации для изоляции службы целостности кода от самого ядра Microsoft Windows, что позволяет службе использовать сигнатуры, определенные корпоративной политикой для выявления надежных объектов. По существу, служба целостности кода работает вместе с ядром в контейнере Windows, защищенном гипервизором.

Device Guard позволяет операционной системе редакции Windows 10 Корпоративная запускать только код, подписанный доверенными источниками, в соответствии с вашей политикой целостности

Таблица. Требуемое Device Guard оборудование и программное обеспечение

Требование	Описание
Редакция Windows 10 Enterprise	Компьютер должен работать под управлением операционной системы Windows 10 в редакции Enterprise
Микропрограммное обеспечение UEFI версии 2.3.1 или старше и поддержка безопасной загрузки	Чтобы убедиться, что микропрограммное обеспечение использует UEFI 2.3.1 или более поздней версии и безопасную загрузку, можно выполнить проверку на соответствие требованиям «Программы совместимости оборудования для Windows», воспользовавшись документом по адресу: https://msdn.microsoft.com/library/windows/hardware/dn932807(v=vs.85).aspx#system_fundamentals_firmware_cs_uefisecureboot_connectedstandby
Расширения виртуализации	Для поддержки механизма обеспечения безопасности на основе виртуализации необходимы следующие расширения виртуализации: • Intel VT-x или AMD-V; • преобразование адресов второго уровня (SLAT)
Блокировка встроенного программного обеспечения	Необходимо заблокировать настройку встроенного программного обеспечения, чтобы не допустить запуска других операционных систем и внесения изменений в параметры UEFI. Кроме того, необходимо заблокировать все остальные методы загрузки, кроме загрузки с жесткого диска
64-разрядная (x64) архитектура	Функции, которые механизм обеспечения безопасности на основе виртуализации использует в низкоуровневой оболочке Windows, могут работать только в 64-разрядных архитектурах
Модуль IOMMU (модуль управления памятью для операций ввода-вывода) VT-d или AMD-Vi	В Windows 10 модуль IOMMU повышает устойчивость системы к атакам на память
Процесс безопасного обновления встроенного ПО	Чтобы убедиться, что встроенное программное обеспечение поддерживает процесс безопасного обновления, его можно проверить на соответствие требованиям программы совместимости оборудования для Windows, воспользовавшись документом по адресу: https://msdn.microsoft.com/library/windows/hardware/dn932807(v=vs.85).aspx#system_fundamentals_firmware_cs_uefisecureboot_connectedstandby

кода ядра при помощи определенных настроек оборудования и безопасности, в том числе:

- целостность кода пользовательского режима (UMCI);
- новые правила целостности кода ядра, включая новые ограничения подписей, установленные лабораториями WHQL;
- безопасная загрузка с ограничениями базы данных (db/dbx);
- безопасность на основе виртуализации для защиты системной памяти, а также приложений и драйверов на основе ядра от возможного взлома;
- доверенный платформенный модуль (TPM) 1.2 или 2.0.

Кроме того, так как устройство запускается с использованием безопасной загрузки UEFI, программы типа boot-kit и root-kit не смогут запускаться.

После безопасного запуска операционная система Windows 10 Enterprise может запустить службы безопасности на основе Hyper-V. Эти службы обеспечивают защиту ядра системы, не позволяя вредоносному коду запускаться на ранних этапах загрузки или в режиме ядра после запуска.

Перед загрузкой и использованием Device Guard необходимо выполнить определенные требования, описанные в таблице.

Прежде чем начать использовать Device Guard, необходимо настроить среду и политики.

Служба Device Guard поддерживает и приложения UWP, и классические приложения для Windows. Доверие между Device Guard и вашими приложениями устанавливается, когда ваши приложения подписываются с помощью подписи, которую вы определяете как надежную. Однако подходят не все подписи. Начиная с Windows 10 сборки 1703 все приложения, развернутые через SCCM, являются доверенными. Подпись ставится следующим образом:

- С помощью процедуры публикации в Магазине Windows. Все приложения в Магазине Microsoft Store автоматически подписываются с помощью специальных подписей, предоставляемых нашим (или вашим) собственным удостоверяющим центром сертификации.
- Использование собственного цифрового сертификата или инфраструктуры открытых ключей (PKI). Поставщики услуг Интернета и организации могут сами подписывать свои классические приложения для Windows, добавляя себя в список доверенных источников.
- С помощью заверителя подписи, отличного от Microsoft. Поставщики услуг Интернета и организации могут использовать доверенного заверителя подписи, отличного от Microsoft, чтобы подписывать собственные классические приложения для Windows.
- С помощью веб-службы, предоставляемой Microsoft (выйдет позже в этом году). Поставщики услуг Интернета и организации смогут использовать более надежную веб-службу, предоставляемую корпорацией Microsoft, для подписания своих классических приложений для Windows.

Применяя две описанные технологии, вы сможете снизить вероятность заражения. Вместе с тем хотелось бы отметить, что только комплексный подход способен обеспечить защиту от вредоносных программ. Надеюсь, что приведенное описание подходов к защите от вирусов-шифровальщиков подтолкнет вас к более глубокому изучению технологий.

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, Kaspersky Lab Certified Consultant, Kaspersky Lab Certified Trainer, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor