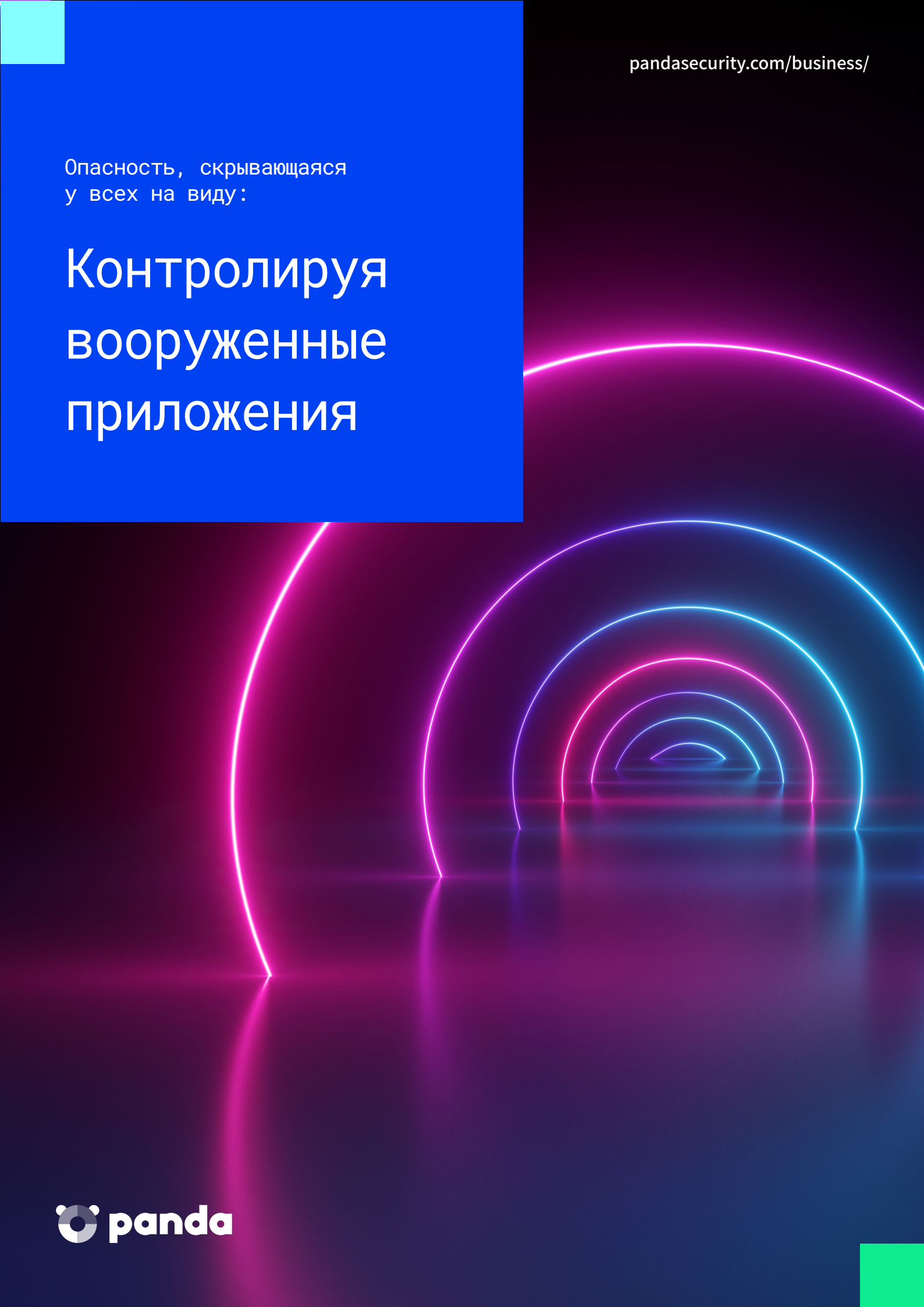
pandasecurity.com/business/

Опасность, скрывающаяся
у всех на виду:

Контролируя вооруженные приложения



panda

Содержание :

Введение

Когда большинство технологических компаний говорит о внутренних угрозах, чаще всего они имеют в виду самый распространенный "шлюз" в корпоративной сети: сотрудники самой компании.

Но существует намного больше внутренних угроз, нежели только человеческий фактор, и во главе этого списка расположены часто используемые приложения. Факт: в 2018 году рост числа безфайловых атак составил 94% – это в 3 раза чаще атак шифровальщиков на конечные устройства. Безфайловое вредоносное ПО использует уязвимости в легитимных приложениях (Lotl*), установленных по умолчанию и ежедневно используемых персоналом компаний в своей работе, таких как Microsoft Office, WMI, Adobe и пр. Отказ от использования этих приложений не является разумным решением. В этом случае, как Вы можете гарантировать то, что хакеры не будут использовать их против Вас и Вашей компании?

В этой белой книге мы рассмотрим, как определить, что легитимное приложение не было вооружено хакерами, а также обсудим самые распространенные методы (например, PowerShell), используемые для проведения таких атак, и методы, обеспечивающие защиту Вашей сети от подобного рода угроз.

Безфайловое вредоносное ПО использует уязвимости в легитимных приложениях

94%

рост безфайловых атак в 2018 году

*Living-off-the-land (Lotl): Методы LotL применяются злоумышленниками для использования во вредоносных целях на устройствах и серверах уже существующих легитимных приложений, а также для их непреднамеренного использования администратором.

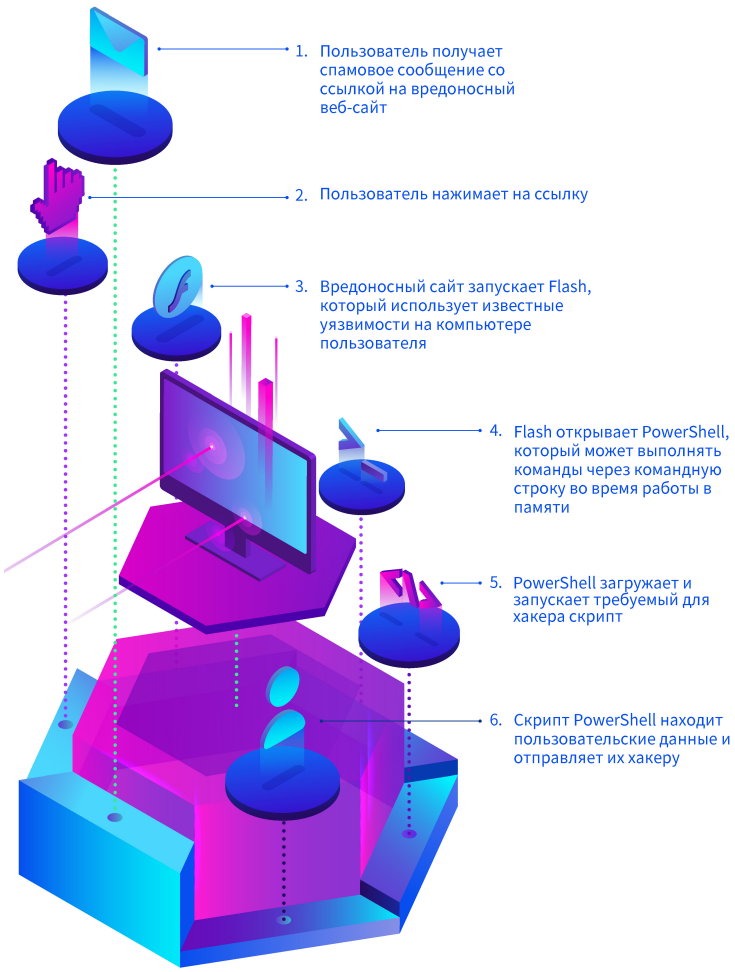
Безфайловое вредоносное ПО

Эта тенденция существует много лет: хакеры ищут новые, креативные способы обхода решений информационной безопасности и проникновения в корпоративные сети.

Одной из самых успешных новых стратегий для кибер-преступников стали безфайловые атаки. Они могут принимать различные формы, включая использование макросов, скриптовых движков и исполняемых в памяти процессов. Хотя природа этих атак различна, но все они разработаны таким образом, чтобы ничего не записывать на жесткий диск, а выполнять все процессы только в оперативной памяти компьютера (ОЗУ). Отсутствие известных вредоносных или потенциально опасных файлов на жестком диске компьютера делает невозможным обнаружение угрозы традиционными системами защиты.

Хотя существуют различные вариации безфайловых атак, но они все имеют несколько ключевых характеристик. Прежде всего, известно, что их крайне сложно обнаружить из-за отсутствия идентифицируемого кода, которое может быть найдено антивирусным ПО. В дополнение к этому, эти атаки обходят традиционные решения безопасности за счет использования при выполнении атаки "родных" для системы приложений и процессов, в результате чего почти невозможно выделять несвойственное поведение.

Процесс атаки безфайлового вредоносного ПО



panda

В дополнение к этим фундаментальным сходствам, безфайловые атаки часто имеют одинаковые точки входа. Некоторые наиболее распространенные для этих атак способы взлома систем[1]:

- {Скриптовые приложения}
- {Приложения для удаленного доступа}
- {Средства администрирования}
- {Системные утилиты}
- {Внутренние компоненты операционных систем}

Среди всех этих точек входа существует одно приложение, которое на сегодняшний день является самым распространенным "кораблем" для этих безфайловых вредоносных атак: **PowerShell.**

1 https://blog.eccu.edu/most-common-malware-attacks-fileless-malware-part-2/

|PowerShell: Главный вектор атаки безфайлового вредоносного ПО

Безфайловое вредоносное ПО может быть внедрено с помощью различных средств, но одним из наиболее распространенных и эффективных средств "доставки" для такого рода атак является PowerShell - системная консоль Windows.

Эта консоль используется для того, чтобы позволить системным администраторам полностью автоматизировать задачи на серверах и компьютерах. Если PowerShell взломан, то его широкий и мощный функционал может быть использован для причинения серьезного ущерба сети. Если хакеры смогут взять его под свой контроль, они смогут получить в корпоративных системах набор прав, позволяющих им легко внедрять еще больше вредоносных программ. Поэтому компаниям стоит беспокоиться не только об операционных системах Windows как таковых: PowerShell также позволяет пользователям контролировать Microsoft Exchange, SQL Server, IIS...

Обладая всеми этими возможностями, безфайловое вредоносное ПО обычно использует PowerShell для внедрения своей "полезной нагрузки", размещая себя в ОЗУ. После выполнения кода в PowerShell, угроза может выполнять горизонтальные перемещения в корпоративных сетях, т.е. она распространяется централизованно, а не полагаясь на внешние точки входа. Обычно эти атаки процветают потому, что они не оставляют на жестком диске первого скомпрометированного компьютера отслеживаемых следов, а значит, Windows Defender и другие традиционные антивирусные решения и системы информационной безопасности не могут обнаружить атаку. Хорошие новости заключаются в том, что есть способы, с помощью которых Вы можете минимизировать риски, связанные с PowerShell. Наиболее эффективным способом, если это возможно для Вашей организации, является полное отключение это консоли. Такой подход может быть приемлемым вариантом для Вашей компании, если Ваш системный администратор использует другие инструменты для автоматизации задач. Другими словами, если Вам не требуется использовать PowerShell, не делайте этого!

В тех случаях, когда отключение PowerShell недопустимо, Вы можете предпринять ряд других проактивных действий для защиты Вашей компании. Например, проверьте, чтобы все конечные устройства в Вашей организации работали на самой последней версии консоли - PowerShell содержит дополнительные средства и меры безопасности для Windows. Еще один шаг, который Вы можете предпринять, - это включить

только определенный набор функций PowerShell, который реально необходим Вашему системному администратору, в режиме ограниченного языка (Constrained Language). Конечно, эти действия не остановят абсолютно все вредоносные атаки, но хотя бы помогут остановить потенциально опасные действия, такие как произвольные вызовы Windows API или деактивация определенных макросов.

В дополнение к упреждающим мерам, Microsoft добавила более расширенные функции ведения журнала в PowerShell, в частности, автоматическую транскрипцию команд, особенно для действий, который имеют потенциальные симптомы кибер-атак. Включение таких функций транскрипций может помочь компаниям обнаруживать безфайловые вредоносные атаки и проводить экспертный анализ для диагностики инцидентов.

|Индикаторы того, что хакер вооружил приложения в сети

Как показывает пример с PowerShell, бывает сложно узнать, что Ваши приложения были вооружены хакерами.

Многие такие атаки были специально созданы для того, чтобы оставаться незамеченными для традиционных решений безопасности. Тем не менее, существуют некоторые "красные флажки", которые Вы можете искать в том случае, если считаете, что стали жертвой инцидента.

Для борьбы с неуловимой природой безфайловых атак разработчики решений ИБ добавляют в свои продукты возможности мониторинга и отчетности на основе поведения процессов. Например, если Word выполняется одновременно с соединением PowerShell, что может говорить о выполнении атаки[2]. В этом случае служба ИТ-безопасности может решить, следует ли поместить процесс на карантин или полностью его остановить. Еще одно поведение, которое может служить таким "красным флажком", - это необычная активность CPU, особенно значительное увеличение его использования. Это может означать, что компьютер был скомпрометирован в результате безфайловой атаки, после чего осуществляются попытки незаметно использовать его для майнинга Bitcoin или других криптовалют.

Наибольшая проблема при выявлении таких атак - это поймать их прежде, чем они причинят ущерб. Потенциальные индикаторы, рассмотренные выше, являются полезными инструментами анализа, но в конечном счете они проявляются только после того, как хакер провел атаку и получил доступ к устройству. Единственный способ проактивно защитить Вашу компанию от безфайловых атак - это внедрить решение безопасности с опциями расширенной защиты.

> Самая большая проблема - поймать эти типы атак прежде, чем они причинят ущерб

2 https://www.csoonline.com/article/3227046/what-is-a-fileless-attack-how-hackers-invade-systems-without-installing-software.html

|Сложные угрозы требуют применения новых передовых технологий

Очевидно, что злоумышленники постоянно наращивают свои возможности для получения доступа к корпоративной сети.

Взламывая используемые приложения и применяя их для внедрения вредоносного ПО или получения доступа к конфиденциальной информации, фактически кибер-преступники создали эдакие невидимые способы взлома, которые невозможно обнаруживать традиционными решениями безопасности.

И хотя есть способы проактивной защиты Вашей компании от подобных атак, все же единственный способ обеспечения безопасности организации - это применение передовых технологий ИБ, которые используют Большие данные, машинное обучение и IoA.

Panda Adaptive Defense 360 - это инновационное решение информационной безопасности, которое сочетает в себе самый широкий спектр технологий защиты (EPP) с автоматизированными возможностями обнаружения атак на конечные устройства и реагирования на них (Endpoint Detection and Response, EDR). Решение позволяет автоматизировать задачи предотвращения, обнаружения, сдерживания и реагирования против сложных атак, неизвестных угроз "нулевого дня", шифровальщиков, фишинга, эксплойтов памяти и безфайловых атак как изнутри, так и снаружи корпоративной сети.

Кибер-преступники создали невидимые способы взлома, которые невозможно обнаруживать традиционными решениями безопасности

Panda Adaptive Defense 360 также предоставляет еще больше возможностей контроля с помощью функции блокировки программ. Помимо того, что она помогает усилить ИТ-безопасность, эта функция также снижает потребление пропускной способности и повышает производительность, блокируя запуск программ по хэшу (MD5) или названию процесса.

Кроме того, встроенная система расширенной отчетности Advanced Reporting Tool включает в себя панели мониторинга, которые обеспечивают полную видимость и контроль над всеми запущенными приложениями, позволяя Вам точно выявлять атаки и необычное поведение пользователей и приложений в Вашей сети. С помощью Advanced Reporting Tool, эти "красные флажки", которые крайне сложно обнаруживать при использовании традиционных решений ИБ, становятся намного более заметными.

Вместе с Panda Adaptive Defense Вы можете также создавать настраиваемые запросы, чтобы легко проверить гипотезу атаки после того, как Вы заметили в Вашей сети какое-то аномальное поведение.

Поскольку бизнес, как и весь мир в целом, становится все более взаимосвязанным и цифровым, предотвращение кибер-преступлений продолжит оставаться основной частью повседневной деятельностью компаний во всем мире. С помощью такого передового решения ИБ с опциями расширенной защиты, как Panda Adaptive Defense 360, Вы сможете чувствовать себя уверенно, зная, что Ваши ИТ-активы надежно защищены от самых сложных кибер-атак.

Два особо ценных управляемых сервиса, включенных в решение:

Сервис 100% классификаций процессов

Сервис 100% классификации отслеживает и предотвращает выполнение вредоносных приложений и процессов на конечных устройствах. При каждом запуске любого процесса сервис в режиме реального времени и без каких-либо неопределенностей осуществляет его классификацию (вредоносный или легитимный).

Сервис Threat Hunting and Investigation

Управляемый сервис Threat Hunting and Investigation управляется командой "охотников за угрозами", оснащенных инструментами профилирования, анализа и корреляции событий, в режиме реального времени и ретроспективы для проактивного обнаружения новых техник взлома и обхода систем защиты.

Предотвращение кибер-преступлений останется основной частью повседневной деятельности организаций в мире.

* Living-off-the-land (Lotl): Методы LotL применяются злоумышленниками для использования во вредоносных целях на устройствах и серверах уже существующих легитимных приложений, а также для их непреднамеренного использования администратором.

Live demo

Давайте обсудим*

+7 (495) 105-94-51
sales@rus.pandasecurity.com

panda