Буткиты: эволюция и способы обнаружения

Positive Technologies

ptsecurity.com

Содержание

Что такое буткит и в чем его опасность?

Злоумышленники постоянно ищут новые способы, как закрепиться в системе надолго, получить максимальные привилегии и при этом избежать обнаружения, к примеру, антивирусными средствами защиты. Большинство средств защиты запускается вместе с операционной системой, поэтому если вредонос будет запускаться до загрузки ОС, то вероятность его обнаружения уменьшается. Еще одна цель разработчиков ВПО — сохранить контроль и привилегии после переустановки ОС. Для этого необходимо, чтобы вредоносный код был загружен в низкоуровневое ПО — прошивку устройства или в первые секторы жесткого диска. Так появились буткиты.

Буткит — это вредоносный код, который запускается до загрузки ОС.
Основная цель буткита — закрепиться в системе и обеспечить защиту других вредоносов от обнаружения средствами защиты.

Концепция или реальная опасность?

Раньше было распространено мнение, что буткиты существуют преимущественно в формате proof of concept[1] и не используются в реальных атаках. Однако между появлением первого PoC и первой атакой с применением буткита прошло всего два года.

PoC буткитов представляют особый интерес для аналитиков и исследователей, так как, изучив их функции, можно прогнозировать, какие техники и методы будут использоваться злоумышленниками и на что нужно обратить внимание, чтобы обеспечить превентивную защиту.

Сейчас функции буткитов добавляются к разным вредоносным программам: так поступают разработчики шифровальщиков, например Satana и Petya, и ботнетов, к примеру Trickbot. Активными пользователями буткитов являются и APT-группировки, например Careto, Winnti (APT41), FIN1 и APT28.

При подготовке исследования были проанализированы 39 семейств буткитов, как существующих в виде PoC, так и встречающихся в реальных атаках с 2005 по 2021 годы.

В основном для доставки вредоносов в инфраструктуру злоумышленники используют целенаправленный фишинг через электронную почту; так, например, распространяются буткиты Mebromi и Mosaic Regressor. Еще одним путем доставки становятся сайты, в том числе техника drive-by compromise — с ее помощью происходило заражение вредоносами Pitou и Mebroot, причем киберпреступники, распространяющие Mebroot, взломали более 1500 веб-ресурсов для размещения вредоносного кода. Буткит FispBoot попадал на устройство после заражения трояном Trojan-Downloader.NSIS.Agent.jd, который жертва загружала под видом видеоролика.

[1] Proof of concept (PoC) — демонстрация возможности эксплуатировать уязвимость.

В чем отличие буткита от руткита

Буткиты часто путают с руткитами[2]. Основное их различие состоит в том, что буткиты начинают свою работу еще до загрузки ОС. Они имеют такой же уровень контроля, как и легальные загрузчики, — главную загрузочную запись (MBR), загрузочный сектор логического диска (VBR) или UEFI и вмешиваются в процесс загрузки ОС, что позволяет им отслеживать, изменять процесс загрузки, а также внедрять, к примеру, вредоносный код в обход механизмов защиты. Зачастую буткиты создают условия для бесшумного внедрения руткитов уровня ядра.

Главная загрузочная запись (master boot record, MBR) — информация и код, необходимые для правильной загрузки устройства. Хранится в первых секторах жесткого диска.

Загрузочная запись тома (volume boot record, VBR или initial program loader, IPL) подгружает данные, необходимые для загрузки ОС. Хранится в первом секторе раздела на жестком диске.

Какими функциями наделен буткит

Чаще всего буткиты обладают следующими функциями:

- скрытая установка основной нагрузки, такой как руткит или, например, бэкдор в режиме пользователя;
- сокрытие вредоносной активности, обход или даже отключение средств защиты;
- загрузка дополнительных вредоносов;
- повышение привилегий в системе.

Некоторые буткиты позволяют обойти аутентификацию; например, такой возможностью обладают PoC буткитов Vbootkit x64 и DreamBoot.

[2]Руткит — это программа (набор программ), позволяющая скрыть присутствие вредоносного ПО в системе.

Буткиты — инструменты для сверхтаргетированных атак

Разработать собственный буткит — нетривиальная задача для злоумышленника, однако в реальной жизни буткиты встречаются довольно часто. Например, злоумышленники, шпионившие за дипломатами и членами неправительственных организаций из Африки, Азии и Европы, использовали для закрепления в системах буткит Mosaic Regressor. Исследователи, проанализировавшие атаку с использованием еще одного современного буткита MoonBounce, были поражены глубокими знаниями злоумышленников об устройстве ИТ-инфраструктуры жертвы. По их мнению, атакующие досконально изучили прошивку устройства, из-за чего можно предположить, что речь шла о сверхтаргетированной атаке.

Однако киберпреступники используют буткиты не только в целевых, но и в массовых атаках. Например, буткит Rovnix злоумышленники распространяли в рамках фишинговой кампании, использующей в качестве повестки информацию о новой инициативе Всемирного банка в связи с эпидемией коронавируса. Предположительно целью этой кампании был кибершпионаж, так как впоследствии на устройства жертв устанавливались ВПО для удаленного управления и шпионское ПО. Буткит Adushka известен тем, что был нацелен на обычных пользователей и применялся для шпионажа, в том числе для кражи данных из личных аккаунтов в онлайн-играх.

Еще один буткит, который использовался в массовых атаках, — Oldboot. Он ориентирован на устройства на платформе Android. Злоумышленники инфицировали более 350 тыс. мобильных устройств. Вредоносный код был добавлен в загрузочный раздел файловой системы и запускался при первом включении устройства. Буткит создавал условия для внедрения загрузчика и шпионского ПО, которое помогало собирать и удалять SMS-сообщения. Для того чтобы избежать заражения, исследователи рекомендовали не приобретать устройства в недоверенных магазинах и не загружать прошивки, полученные из ненадежных источников.

27 семейств буткитов применяются в реальных атаках

14 из них используются APT-группировками

Сейчас буткиты набирают популярность и все чаще встречаются в арсенале злоумышленников. Этому способствует и регулярное обнаружение уязвимостей в прошивках. Например, для UEFI только в 2021 году в Национальной базе уязвимостей (NDV) появилось 14 записей. Об актуальности буткитов свидетельствует и появление новой функциональности у коммерческого ВПО: в 2021 году разработчики шпионского ПО FinSpy добавили в него функции буткита.

Можно ли обнаружить и удалить буткит

Действенный способ обнаружить буткит — сделать это до его внедрения в прошивку или первые разделы жесткого диска. Установить факт заражения системы буткитом непросто, но даже если это удастся сделать, жертва столкнется с еще большими трудностями при его удалении. Если буткит был внедрен в первые разделы жесткого диска MBR, VBR или — в случае с устройством на базе UEFI — EFI System Partition, то полная переустановка ОС удалит вредоносный код буткита с диска. Однако любая переустановка ОС не затронет память микросхемы, где содержится прошивка BIOS или UEFI, поэтому если произошло изменение прошивки, ОС может быть снова заражена.

Также можно определить, какой именно буткит инфицировал систему, и проверить наличие утилит от производителей антивирусов, с помощью которых можно очистить систему от вредоносного кода.

Эволюция буткитов

В начале 1980-х появились первые подобия буткитов — вирусы, заражавшие загрузочный сектор жесткого диска, или boot sector infectors. После успешного закрепления в системе эти вредоносы стремились распространиться на другие устройства, заражая все подключаемые съемные носители. Наиболее известные представители этого типа ВПО — Elk Cloner, один из первых вирусов, нацеленный на компьютеры Apple, и Brain, вызвавший первую компьютерную эпидемию и подвигнувший разработчиков ПО на создание первого антивируса. Еще один нашумевший boot sector infector — вирус Stoned, который появился в 1987 году. На базе его исходного кода было разработано множество вредоносов, поражающих загрузочный сектор, например Michelangelo, AntiExe и Angelina. Последний был обнаружен в 2007 году на ноутбуках Medion, которые продавались в Германии и Дании. Предустановленный антивирус Bullguard мог только обнаружить факт заражения, однако не был способен очистить систему.

Полноценные буткиты появились в начале 2000-х и были ориентированы на BIOS. Один из первых PoC буткита — eEye BootRoot.

В рамках исследования мы рассматривали как PoC буткитов, так и буткиты, которые встречаются в реальных атаках (in the wild). Доля PoC буткитов в нашей выборке составила 31%, а буткитов in the wild — 69%.

Вредоносный код буткита для атак на устройства на базе BIOS может быть внедрен непосредственно в MBR, VBR или IPL. Буткит может быть внедрен и в саму прошивку, но на практике это сложно осуществить.

Среди проанализированных нами буткитов 76% были разработаны под BIOS. Из них доля буткитов, которые поражают только MBR, составила 80%. Еще 10% внедряются в VBR или IPL, а оставшиеся 10% поддерживают все перечисленные способы внедрения.

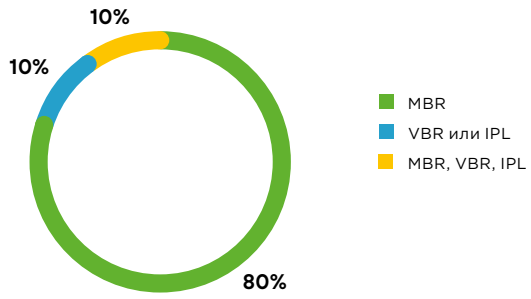

Рисунок 1. Типы буткитов для атак на BIOS (по области памяти)

Буткиты для атак на BIOS могут скомпрометировать любые компоненты системы, в том числе загрузчик ОС, гипервизор, средства безопасности. Компания Intel еще в 2020 году остановила поддержку BIOS, но некоторые компании не могут быстро обновить ИТ-инфраструктуру, из-за этого буткиты для заражения BIOS до сих пор не теряют актуальности.

Почему не все отказались от BIOS. Некоторым организациям сложно обновить ИТ-инфраструктуру. По нашей оценке, в России с такой проблемой чаще сталкиваются госучреждения и промышленные предприятия. Не менее актуальна эта проблема и в случае с виртуальной инфраструктурой, так как даже производители гипервизоров в качестве прошивки по умолчанию рекомендуют использовать BIOS. На наш взгляд, это обусловлено тем, что виртуальные машины на базе BIOS легче обслуживать и поддерживать.

В 2009 году вышла новая версия вируса Stoned, которая представляла собой полноценный PoC буткита. Особенность этой версии заключалась в том, что вирус поражал систему, даже если жесткий диск или его раздел был зашифрован с помощью TrueCrypt. Раньше существовал миф: если использовать шифрование дисков, то это спасет устройство от заражения вредоносами. Stoned доказал обратное. Вредонос внедрялся в MBR, которая даже в случае использования шифрования диска всегда остается незашифрованной. Затем, когда пользователь при работе с устройством вводил пароль, буткит перехватывал его, тем самым получая доступ ко всей зашифрованной информации. Это был первый наглядный случай обхода дискового шифрования. Уже через год на базе Stoned был разработан буткит Whistler, который встречался в реальных атаках. К слову, на основе буткита Stoned в 2011 году был разработан и первый PoC буткита, ориентированный для атак на прошивку UEFI.

Исследовательский проект Stoned стал насколько популярным, что антивирусные компании потребовали не выкладывать в открытый доступ исходный код для его новых версий.

Изучив все недостатки BIOS, производители устройств переключились на более безопасную технологию — UEFI. В сравнении с BIOS UEFI имеет ряд значительных улучшений, но нас больше всего интересует добавленный к ней протокол безопасной загрузки (Secure Boot), который проверяет подписи для драйверов UEFI, UEFI-приложений и самой ОС. Если эти подписи элементов совпадут с данными из хранилища подписей и хеш-сумм доверенных приложений, то UEFI-приложения будут загружены, а прошивка UEFI передаст управление ОС. Само хранилище этих подписей и хеш-сумм располагается в энергонезависимой памяти и заполняется производителем устройства. Более подробно ознакомиться с работой протокола Secure Boot можно на сайте Microsoft.

Технология Secure Boot сработает только в том случае, если злоумышленник не имеет физического доступа к устройству, иначе он может добавить или подменить подписи для собственных вредоносных драйверов.

За счет Secure Boot переход на UEFI должен был сделать невозможным внедрение буткитов, однако ситуация сложилась иначе. Существует несколько возможных вариантов заражения прошивки UEFI:

- в ходе атаки типа supply chain путем внедрения буткита в поставляемое ПО или обновления этого ПО;
- путем физического доступа к устройству;
- вследствие эксплуатации ошибок в конфигурации прошивки или механизме ее обновления;
- удаленное заражение; перед ним злоумышленник повышает свои привилегии для установки полезной нагрузки на уровне ядра ОС, чтобы выполнить код в режиме системного управления (SMM) и тем самым обойти различные механизмы защиты прошивки и получить прямой доступ к ее памяти.

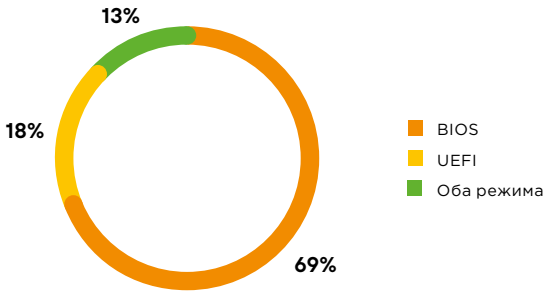

Рисунок 2. Типы буткитов для атак на BIOS (по области памяти)

Если обобщить, то в процессе заражения устройств на базе UEFI злоумышленники могут внедриться в прошивку, которая хранится в памяти SPI-flash, внести изменения в существующий модуль или создать новый в EFI System Partition.

EFI System Partition (ESP) — специальный скрытый раздел жесткого диска в устройствах на базе UEFI. В этом разделе хранится менеджер загрузки. В процессе загрузки устройства UEFI подгружает файлы (модули) из ESP, чтобы запустить ОС и установленные утилиты.

После выхода первого PoC буткита для заражения UEFI и до первого буткита, использованного в атаке, прошло шесть лет, когда в 2017 году был замечен буткит LoJax. Для перезаписи прошивки в SPI-flash разработчики этого буткита использовали как уязвимости прошивки, так и пробелы в конфигурации Secure Boot. TrickBoot, являющийся составной частью вредоноса TrickBot, нашумевшего в 2020 и 2021 годах, также ориентирован на UEFI.

Начиная с 2020 года все буткиты, встречающиеся в реальных атаках, ориентированы на UEFI, в частности Mosaic Regressor, Trickboot, FinSpy, ESPEcter, MoonBounce.

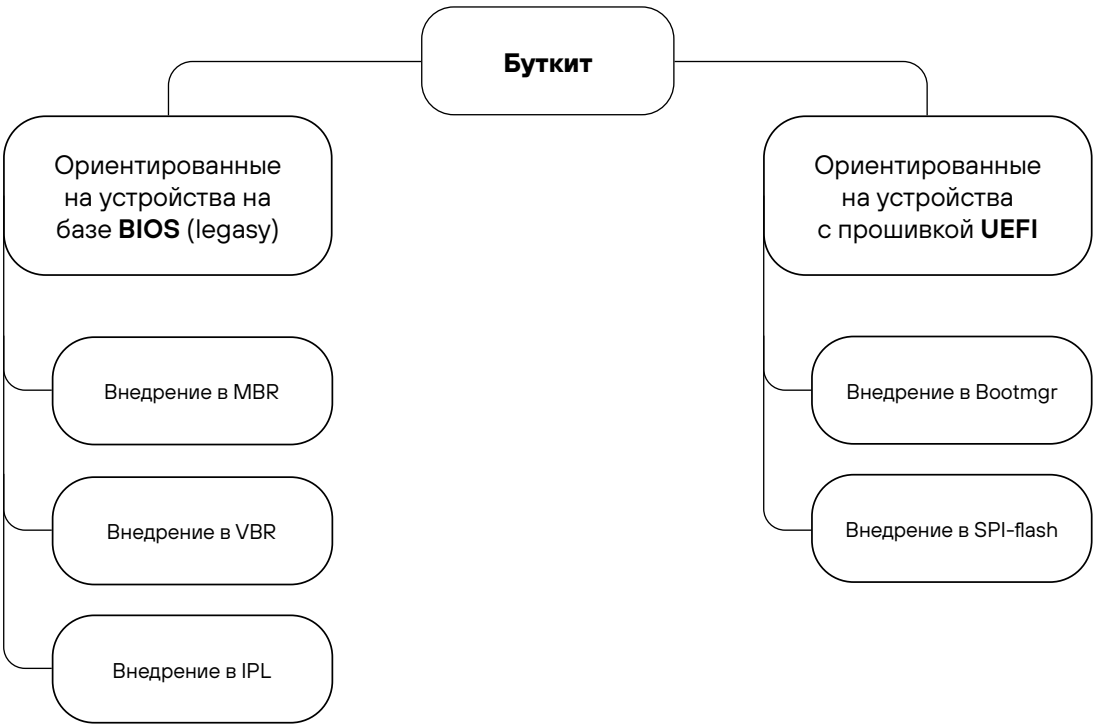

Рисунок 3. Классификация буткитов

Некоторые буткиты совмещают в себе несколько режимов работы при ориентации на один тип прошивки, то есть могут, к примеру, внедряться и в MBR, и в VBR. Один из представителей таких буткитов — Gapz. Есть и универсальные варианты буткитов для атак на устройства как на базе BIOS, так и с прошивкой UEFI, например FinSpy и Trickboot.

БУТКИТЫ

ptsecurity.com

Хронология появления

2005

eEye BootRoot	B

2007

Mebroot	B
Vbootkit	B

2008

TDSS	B

2009

Stoned bootkit	B
Mebroot v2	B
Vbootkit x64	B

2010

Olmarik (TDL4/TDSS)	B
Mebratix	B
Whistler bootkit	B

2011

Rovnix	B
DeepBoot	B
Evil Core	B
Mebromi	B
Stoned Vienna	U
FispBoot/Fisp.A	B
Halcbot bootkit	B
Olmasco (MaxSS)	B

2012

DKFBootkit	B
XPAJ (Goblin)	B
Gapz	B

2013

Aduska bootkit	B
DreamBoot	U

2014

Pitou	B
OldBoot	B

2015

BOOTRASH	B
HDRoot	B
Thunderstrike	U

2016

Petya	B U
Satana	B

2017

LoJax	U

2018

DarkCloud bootkit	B
Pitou	B

2019

EfiGuard	U

2020

Trickboot	B U
Mosaic Regressor	U

2021

MoonBounce	U
ESPEcter	B U
FinSpy	B U

Классификация буткитов:

Буткиты, использованные в реальных атаках

Буткиты Proof of Concept

Ориентация буткитов по объектам атак:

B BIOS

U UEFI

Уязвимые прошивки

Злоумышленники активно ищут уязвимости в BIOS и UEFI, позволяющие внедрить буткит. Аналитики компании Binarly выявили 23 критически опасные уязвимости, связанные с управлением памятью в режиме SMM в UEFI от InsydeH2O, которую используют такие крупные производители техники, как Bull (Atos), Dell, Fujitsu, HP, Intel, Lenovo, Microsoft и Siemens. Эксплуатируя эти уязвимости, злоумышленники могли отключить аппаратные функции безопасности, разместить буткит и ВПО для удаленного управления. По оценкам аналитиков, уязвимости могли затронуть миллионы устройств от ноутбуков до серверов, сетевое оборудование и промышленные контроллеры (ICS).

На конференции Black Hat Asia в 2017 году специалисты компании Cylance продемонстрировали, как с помощью двух уязвимостей (CVE-2017-3197 и CVE-2017-3198) в прошивках Gigabyte UEFI можно внедрить вредоносный код. Обе уязвимости — недочеты в разработке компонентов. Первая связана с неправильной реализацией защиты от записи, а вторая — с отсутствием проверки подписи компонентов.

Прошивка BIOS тоже имеет уязвимости. Например, в конце марта 2022 года компания Dell рекомендовала своим клиентам как можно скорее обновить BIOS на компьютерах Alienware, Inspiron, Vostro и Edge Gateway серии 3000. Эти модели оказались подвержены уязвимостям, позволяющим удаленному злоумышленнику в обход аутентификации использовать прерывание системного управления (SMI) для выполнения произвольного кода во время обработки системных функций (CVE-2022-24415, CVE-2022-24416, CVE-2022-24419, CVE-2022-24420 и CVE-2022-24421).

Буткит на продажу

Ранее мы говорили о том, как злоумышленникам сложно разработать руткит. С буткитом дела обстоят еще сложнее. Ошибки в их разработке могут привести, например, к невозможности загрузки устройства, из-за чего будет проведено расследование, в результате которого будет обнаружен вредонос и раскрыты действия киберпреступника. Осложняет ситуацию и то, что в интернете не так много информации об этом ВПО. Злоумышленники пользуются всеми доступными средствами:

- дорабатывают PoC буткитов, как это произошло, например, с буткитом Stoned, трансформировавшемся в буткит для атак Whistler;
- ищут разработчиков, которые смогут создать буткит с нуля;
- покупают готовые решения.

Мы проанализировали 58 телеграм-каналов и десять наиболее популярных русскоязычных и англоязычных форумов в дарквебе, где представлены предложения о продаже и запросы о покупке буткитов, а также объявления о поиске разработчиков вредоносов.

Средняя стоимость буткита в аренду составляет 4900 долл. США. Для сравнения: взять руткит в аренду можно за 100–200 долл. США.

За 10 тыс. долл. США можно приобрести исходный код для буткита, а за 2000 долл. США — получить образ для запуска. За разработку буткита, ориентированного на заражение MBR, злоумышленники готовы заплатить 3–5 тыс. долл. США. Максимальная цена, которую готовы заплатить за готовый буткит для прошивки UEFI, составляет 2 млн долл. США.

Рисунок 4. Объявление о продаже буткита для атаки на банкоматы

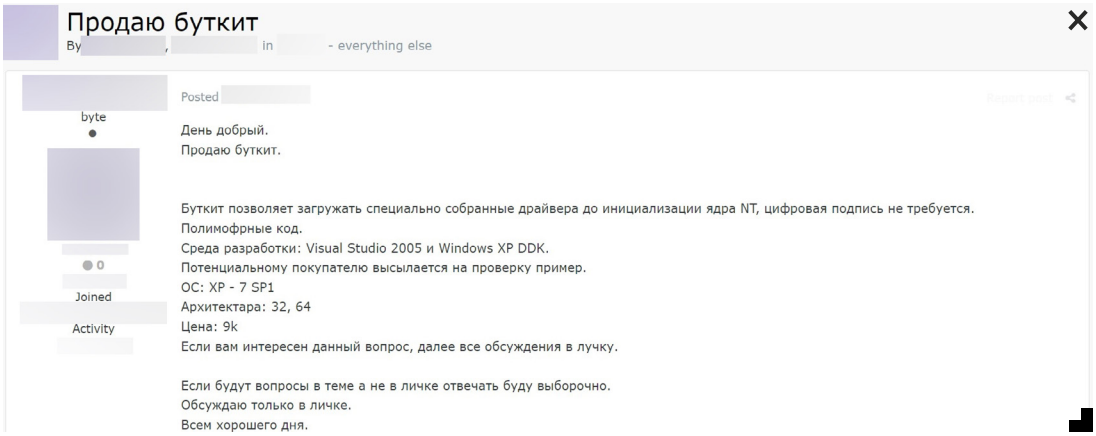

Рисунок 5. Объявление о продаже буткита

В телеграм-каналах мы встречали сообщения, в которых авторы прикрепляли архивы с исходным кодом для PoC буткитов и буткитов, встречающихся в реальных атаках, то есть злоумышленники могут собрать себе готовый буткит или использовать фрагменты готового кода при разработке собственного вредоноса.

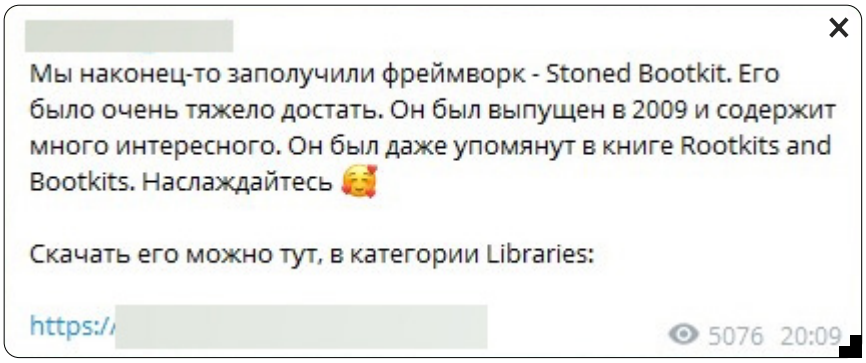

Рисунок 6. Пост со ссылкой на исходный код Stoned Bootkit

Рисунок 7. Пост с архивом, содержащим исходный код для буткита Espector

Как не допустить заражения буткитом

На наш взгляд, исследования прошивок приведут к обнаружению новых уязвимостей, а сами буткиты будут становиться с каждым годом все популярнее. Лучше всего не допустить инфицирования системы буткитом, и в качестве превентивных мер мы советуем:

- отслеживать потенциально опасные операции в системе — получение прямого доступа к жесткому диску, установку драйвера, чтение прошивки;
- включить режим Secure Boot для UEFI, так как если драйверы для буткита не будут иметь цифровой подписи, то этот режим препятствует их запуску и, соответственно, заражения системы не произойдет;
- не производить загрузку ОС с использованием недоверенных носителей;
- при обновлении версии ОС и прошивки проверять, не появлялась ли информация о компрометации вендоров (чтобы не стать жертвой атаки supply chain).

Также не забывайте о важности обнаружения и противодействия загрузчикам и установщикам вредоносного ПО на ранней стадии, используйте современные антивирусные средства и песочницы, позволяющие проанализировать потенциальное поведение файла в системе до его непосредственного исполнения.

Для того чтобы обнаружить факт заражения, необходимо контролировать целостность загрузочных записей и прошивок.

Узнать больше о том, как работает буткит, можно в исследовании экспертов PT Expert Security Center.

ptsecurity.com
pr@ptsecurity.com