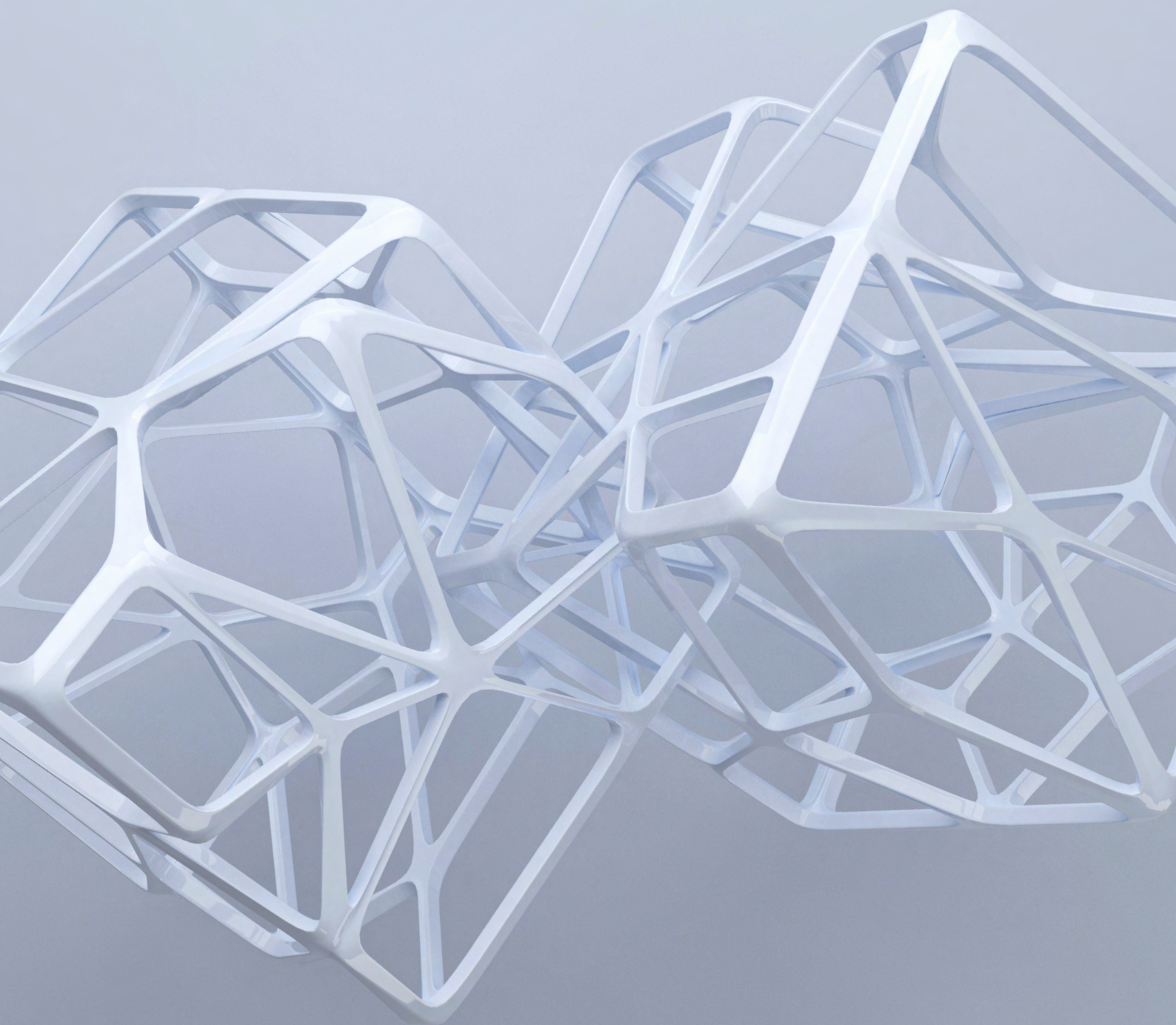


Руткиты: эволюция и способы обнаружения



Содержание

Введение	3
Что такое руткит	4
Эволюция руткитов	5
Кто стоит за атаками	9
Что предлагает дарквеб	11
Способы обнаружения	14
Будущее руткитов	15

Введение

В исследовании мы расскажем, как развивались руткиты, кем и для чего используются сейчас, как их обнаружить, и спрогнозируем их будущее



На прочтение:
15 минут

Руткиты встречаются в арсенале злоумышленников не так часто, как другие типы вредоносного ПО. К примеру, по данным компании Bitdefender, руткиты составляют менее 1% от общего числа выявляемых вредоносных программ. Однако все случаи обнаружения связаны с громкими атаками. Среди них, например, кибершпионская кампания APT-группировки Strider (они же ProjectSauron, или G0041), в рамках которой злоумышленники распространяли руткит Remsec. Группировка собирала информацию об используемых методах шифрования: в атаках на госучреждения злоумышленники похищали ключи шифрования, файлы конфигурации, собирали IP-адреса серверов инфраструктуры ключей шифрования. Киберпреступники были нацелены на организации на территории России, Бельгии, Китая, Ирана, Швеции и Руанды.

Хотя из-за высокой сложности разработки руткиты используются не так часто, они несут в себе угрозу, поскольку скрывают вредоносную активность на устройствах и препятствуют своевременному обнаружению факта компрометации. Руткиты все еще успешно используются в атаках, несмотря на внедрение средств защиты от них в современных ОС. При подготовке этого исследования мы проанализировали 16 наиболее известных семейств руткитов, обнаруженных экспертами за последние 10 лет. Мы расскажем, как развивались руткиты, кем и для чего используются сейчас, как их обнаружить, и дадим прогноз относительно того, будут ли злоумышленники использовать их в будущем.

Что такое руткит

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

Зачастую руткиты входят в состав многофункционального вредоносного ПО, которое обладает дополнительными возможностями, к примеру предоставляет злоумышленникам удаленный доступ к скомпрометированным узлам, перехватывает сетевой трафик, шпионит за пользователями, считывает нажатия клавиш, похищает сведения для аутентификации или использует ресурсы жертвы для майнинга криптовалюты и проведения DDoS-атак. Задачей руткита становится маскировка этой нелегитимной активности.

Виды руткитов по уровню получаемых привилегий:

- **Руткиты, работающие в режиме ядра.** Такие руткиты имеют те же привилегии, что и операционная система. Они разработаны в виде драйверов устройств или загружаемых модулей. Такие руткиты сложно разрабатывать, потому что любые ошибки в исходном коде могут повлиять на стабильность системы, что поспособствует обнаружению вредоноса. Этих руткитов в нашей выборке оказалось 38%.
- **Руткиты, работающие в режиме пользователя.** Эти руткиты чаще используются в массовых атаках. Это обусловлено тем, что их проще разрабатывать в сравнении с руткитами, работающими в режиме ядра. Руткиты в режиме пользователя работают с теми же привилегиями, что и большинство приложений. Они могут перехватывать системные вызовы и подменять значения, возвращаемые API. Доля таких руткитов составила 31%.

Некоторые руткиты, например Necurs, Flame и DirtyMoe, разработаны так, чтобы совмещать оба режима работы. Они составили 31% в выборке.

Переход на руткиты режима пользователя — одна из тенденций среди разработчиков руткитов. Например, исследователи Sophos обнаружили, что разработчики руткита ZeroAccess полностью перешли на использование этого режима. На наш взгляд, такие действия могут быть обусловлены следующими причинами:

- Как мы уже писали выше, руткит режима ядра сложно разрабатывать и незаметно внедрять в систему жертвы; злоумышленники могут не обладать достаточным уровнем компетенций, чтобы использовать его в своих атаках, поэтому выбирают более простой вариант.
- На разработку или модификацию такого руткита уходит много времени, а у злоумышленников оно может быть ограничено, например если нужно как можно быстрее воспользоваться уязвимостью на периметре компании, пока ее не заметили и не установили обновления безопасности или пока ей не воспользовалась другая группировка. Злоумышленники действуют быстро: с момента публикации эксплойта до первых попыток эксплуатации уязвимости может пройти менее суток, а если у группировки нет надежного готового к использованию инструмента, этого времени явно недостаточно для его разработки.

- Если в исходном коде руткита режима ядра есть ошибки, в работе ОС могут произойти непоправимые изменения, которые выдадут злоумышленников и сорвут атаку.
- Нецелесообразно усложнять атаку, если есть уверенность в том, что система защиты неэффективна. Если найдена точка входа в компанию, если разведка показала, что периметр слабо защищен, значит, в системе безопасности есть существенные недостатки, поэтому использовать руткит уровня ядра, на разработку которого нужно потратить много сил и который может наделать шума, нерационально.

Если руткиты, особенно уровня ядра, настолько сложны в разработке, то кто и почему продолжает их использовать? Ответ лежит на поверхности: это те группировки, для которых результат атаки превосходит все усилия, потраченные на ее организацию, группировки, обладающие достаточной технической квалификацией и финансовыми возможностями. Среди них есть как АРТ-группировки, которые добывают информацию или производят разрушительные действия в инфраструктуре в интересах заказчиков, не считаясь с затратами, так и финансово мотивированные преступники, которые похищают крупные суммы, покрывая расходы на подготовку.

Эволюция руткитов



Хронологию появления
руткитов с 2011 года
см. на [стр. 8](#)

Изначально руткиты использовались в атаках на Unix-системы для получения максимальных привилегий и выполнения команд от имени пользователя root — отсюда и их название. Но уже в 1999 году появился первый руткит, ориентированный на операционную систему Windows, — NTRootkit. Позднее появились и руткиты, которые можно было использовать в атаках на macOS.

Наиболее известный случай применения руткита в атаках — кампания 2010 года по распространению вредоносной программы Stuxnet. С помощью Stuxnet злоумышленники скрытно осуществляли сбор данных, а также загружали на скомпрометированные узлы исполняемые файлы. В ходе расследования была выявлена причастность разведывательных служб США и Израиля к созданию этого вредоносного ПО, а главной целью такой коллаборации была приостановка развития ядерной системы Ирана и физическое разрушение инфраструктуры.

В последнее десятилетие чаще всего потребность в использовании руткитов возникает у киберпреступников, нацеленных на получение данных. В рамках одной из кибершпионских кампаний на Ближнем Востоке злоумышленники использовали руткит Flame, который помогал им отслеживать сетевой трафик жертв, осуществлял функции кейлоггера, а также делал скриншоты экрана.



Интересный факт

В исходном коде драйвера руткита DirtyMoe специалисты компании Avast выявили множество ошибок, что может свидетельствовать о заимствовании фрагментов кода из интернета. Модули вредоноса написаны на языке Delphi, из-за чего могут быть легко обнаружены анти-вирусными средствами, поэтому разработчики DirtyMoe воспользовались VMProtect для обфускации исходного кода.

С помощью руткитов можно не только незаметно добыть необходимую информацию и получить удаленный доступ. Злоумышленники применяют их и для извлечения прямой финансовой выгоды, например для сокрытия модулей-майнеров, как в случае с руткитом DirtyMoe. По данным компании Avast, в 2021 году киберпреступники, распространяющие этот руткит, заразили более 100 000 компьютеров, хотя еще в 2020 году число жертв не превышало 10 000. К такому резкому скачку количества жертв привело добавление нового модуля, облегчающего распространение на компьютерах с Windows. Модуль выполнял сканирование интернета на предмет компьютеров с открытым SMB-портом, а затем подбирал учетные данные для удаленного доступа.

Есть случаи непреднамеренного создания руткитов, например, как это произошло в 2016 году с разработчиками игры Street Fighter V компании Capcom. Компания выпустила обновление, которое отключало защиту от выполнения стороннего кода на уровне ядра (SMEP) и, таким образом, позволяло злоумышленникам получить удаленный доступ к компьютерам игроков. Внимательные пользователи прервали установку этого обновления из-за того, что в процессе установки запрашивались привилегии уровня системы.

Руткит Moriya использовался в целевой кибершпионской кампании TunnelSnake как минимум с 2018 года. В списке жертв, среди прочих, две дипломатические организации в Юго-Восточной Азии и Африке. Основная цель вредоноса — обеспечить злоумышленникам удаленный доступ в IT-инфраструктуру жертв, а также сделать возможными загрузку и запуск деструктивного кода. Руткит ориентирован на объекты под управлением Windows и совмещает режим пользователя и ядра. В качестве первоначального вектора проникновения злоумышленники воспользовались уязвимостями на доступных из интернета серверах, предположительно уязвимостью CVE-2017-7269. Разработчики руткита предусмотрели механизм обхода проверки обязательной подписи драйверов и модуля PatchGuard. Последний при попытке проникновения в ядро системы вызывает BSoD (Blue Screen of Death). Для этого они использовали драйвер для виртуальной машины VirtualBox. Кроме того, руткит не иницирует соединение с управляющим сервером, что способствует его сокрытию.

Руткит Remsec (Cremes) — модульное вредоносное ПО, используемое группировкой Strider (ProjectSauron, G0041) с целью кибершпионажа. Злоумышленников интересует информация о программном обеспечении для защиты трафика с помощью криптографических методов. Они тщательно выбирают жертв, в числе которых государственные учреждения, научно-исследовательские центры, телекоммуникационные компании. Для проникновения в инфраструктуру используются уязвимости нулевого дня. Руткит Remsec работает в режиме ядра и ориентирован на Windows, а его модули позволяют злоумышленникам получить удаленный доступ, загрузить вредоносное ПО, прослушать сетевой трафик, а также зафиксировать нажатия клавиш на клавиатуре и передать полученные данные на сервер атакующих.



Раньше задача руткитов заключалась в том, чтобы получить максимальные привилегии в системе (либо привилегии администратора, либо системы). Сейчас они больше нацелены на то, чтобы не допустить обнаружения вредоносной активности средствами защиты.

Большая часть модулей написана на языке Lua. Исследователи ESET выявили, что для внедрения руткита использовались легитимные драйверы режима ядра антивирусных продуктов. Примечательно, что Remsec не перехватывает API-вызовы или системные операции для сокрытия своей активности в системе, — вместо этого разработчикам вредоноса требовалось лишь выполнение своего кода с повышенными привилегиями.

На борьбу с руткитами выходят не только разработчики средств защиты, но и производители ОС: например, массовый переход на Windows 10 сказался на уже существующих руткитах. В этой версии ОС предусмотрен целый комплекс мер по противодействию руткитам, более подробно об этом мы рассказываем в разделе «Что предлагает дарквеб». Однако злоумышленники тоже не стоят на месте и, к примеру, в относительно новом рутките Moriya уже предусмотрены механизмы обхода встроенных в ОС средств защиты — проверки обязательной подписи драйверов и модуля PatchGuard. К разработке руткитов привлекаются высококвалифицированные специалисты, разбирающиеся в устройстве ОС, а также обладающие знаниями и опытом в реверс-инжиниринге и программировании. Методами реверс-инжиниринга разработчики вредоносов выявляют особенности функционирования ОС, которые позволяют внедрить руткит. Несмотря на все сложности, связанные с их созданием, регулярно появляются новые руткиты.

Из всего вышесказанного следует, что руткиты несут огромную опасность, потому что:

- они предоставляют злоумышленникам повышенные привилегии в системе;
- значительно затрудняют детектирование вредоносной активности;
- их сложно обнаружить и удалить;
- их присутствие чаще всего свидетельствует о целенаправленной атаке хорошо подготовленной кибергруппировки, а значит за то время, пока атака остается незамеченной, инфраструктура компании может находиться под полным контролем злоумышленников.

В большинстве случаев атака приводит не только к компрометации данных, но и к реальному финансовому ущербу, который очень сложно оценить по нескольким причинам:

- последствия атаки с участием высококвалифицированных злоумышленников могут проявляться на протяжении долгого времени, особенно если злоумышленники находились в сети компании годами;
- требуется подсчитать все затраты на устранение последствий атаки, а в некоторых случаях руткит невозможно удалить и приходится обновлять аппаратную часть IT-инфраструктуры;
- если атака была направлена на получение данных, необходимо оценить в денежном эквиваленте украденные данные и ущерб, который понесла компания из-за утечки.



ptsecurity.com

РУТКИТЫ

ХРОНОЛОГИЯ ПОЯВЛЕНИЯ

2011	2012	2013	2014	2015
<div>ZeroAccess </div> <div><ul style="list-style-type: none">Поддерживает запуск майнера или кликера после зараженияМожет быть использован для атак на GSM-станции</div> <div>Hikit </div> <div><ul style="list-style-type: none">Используется APT AxiomПредоставляет удаленный доступ к скомпрометированным узламНаправлен на сбор данных</div> <div>Ebury </div> <div><ul style="list-style-type: none">Используется APT WindigoКрадет учетные данные для OpenSSHПредоставляет удаленный доступ к скомпрометированным узлам</div>	<div>Flame </div> <div><ul style="list-style-type: none">Используется APT Equation GroupПерехватывает сетевой трафикСтирает следы активности злоумышленника на зараженной машинеМожет записывать звук и делать скриншоты, а также передавать полученные данные, в том числе по Bluetooth</div> <div>Necurs </div> <div><ul style="list-style-type: none">Может загружать вымогатели и банковские трояны, был замечен в кампании по распространению DridexОтключает средства защитыИспользует алгоритмы генерации доменов (DGA)Содержит модуль для спам-рассылок, модули для проведения других атак и модуль для перенаправления трафика</div> <div>Regin </div> <div><ul style="list-style-type: none">Использует APT Equation GroupМожет заражать контроллеры GSM-станцийСодержит набор инструментов для шпионажаПредоставляет удаленный доступ к скомпрометированным узлам</div>	<div>Careto </div> <div><ul style="list-style-type: none">Используется APT MaskИмеет два модуля: руткит и буткитИсходный код вредоноса подписан цифровым сертификатомСобирает файлы конфигурации VPN, RDP и ключи SSHПозволяет злоумышленникам запускать свои команды</div>	<div>Kronos </div> <div><ul style="list-style-type: none">Осуществляет сбор данных для доступа в интернет-банкингСочетает в себе функции банковского трояна и загрузчикаРаспространяется в рамках фишинговых кампаний</div>	<div>Shedun </div> <div><ul style="list-style-type: none">Используется группировкой YingmobИмитирует популярные приложенияМожет применяться для загрузки дополнительного ВПО, в том числе рекламного ПО</div> <div>Umbreon </div> <div><ul style="list-style-type: none">Устанавливает бэкдор EspreonСоздает локальных пользователей для доступа к зараженной системеПерехватывает вызовы функции libc, чтобы скрыть наличие нового пользователя в файле /etc/passwd</div>
2016	2017	2018	2019	2020
<div>Remsec (Cremes) </div> <div><ul style="list-style-type: none">Используется APT StriderПрименяется в кибершпионских кампанияхПредоставляет удаленный доступ к скомпрометированным узлам, а также позволяет загружать дополнительное ПОСодержит модуль для перехвата сетевого трафика и нажатий клавиш на клавиатуре</div>	<div>DirtyMoe </div> <div><ul style="list-style-type: none">Распространяется подобно червю, объединяя жертв в ботнетИспользует вычислительные ресурсы жертв для проведения DDoS-атак и майнинга криптовалюты</div>	<div>Moriya </div> <div><ul style="list-style-type: none">Используется предположительно APT1Скрывает связь с сервером управленияПредоставляет удаленный доступ к скомпрометированным узлам</div>	<div>Skidmap </div> <div><ul style="list-style-type: none">Загружает модуль для майнинга криптовалютыПоказывает поддельные данные о загрузке процессора</div> <div>Scranos </div> <div><ul style="list-style-type: none">Внедряет рекламное ПО на скомпрометированных узлахПохищает учетные данные из браузераРаспространяет рекламное ПО для мобильных устройств через взломанные аккаунты в социальных сетях</div>	<div>Drovorub </div> <div><ul style="list-style-type: none">Используется APT28Обеспечивает канал связи с командным серверомОбладает возможностью перехвата и перенаправления сетевого трафикаИзменяет правила на межсетевом экране</div>

Ориентация руткитов на ОС



Unix



IOS



Android



Windows

Тип атаки



Целевые атаки



Массовые атаки

Кто стоит за атаками

56%

исследованных
руткитов применялись
в целенаправленных
атаках

Учитывая весь спектр возможностей и сложности, связанные с разработкой руткитов, чаще всего их используют АРТ-группировки. Основной мотив злоумышленников такого уровня — получение данных, кибершпионаж. Например, Equation Group активно использовала руткит Flame в своих кибершпионских кампаниях на Ближнем Востоке. К слову, среди всех исследованных нами семейств руткитов в 77% случаев злоумышленники, распространяющие их, преследовали мотив получения данных. Примерно в трети случаев (31%) преступники стремились извлечь финансовую выгоду, как, например, Yingmob и TA505. Их атаки носили массовый характер и не были привязаны к конкретным отраслям, при этом Yingmob были нацелены на частных лиц. Самый редкий мотив — использование инфраструктуры компании-жертвы для проведения последующих атак. Он был отмечен лишь в 15% атак с использованием руткитов.

В качестве основного способа распространения руткитов (85% случаев) злоумышленники используют методы социальной инженерии, такие как рассылка фишинговых сообщений, создание поддельных сайтов и приложений, имитирующих легитимные. Например, злоумышленники, распространяющие руткит Scranos, были ориентированы на частных лиц, поэтому в качестве способов распространения выбрали взломанное ПО и фишинговые рассылки. Особую активность вредонос проявил в 2019 году. Жертвы этой кампании были обнаружены на территории Китая, Индии, Румынии, Франции, Италии, Бразилии и Индонезии. Мотивы, которые преследуют киберпреступники, — финансовая выгода и получение данных. Прежде всего их интересовали файлы куки и учетные данные для доступа в интернет-банкинг и аутентификации в социальных сетях и на других интересующих преступников ресурсах. Вредонос не только предоставлял злоумышленникам удаленный доступ и возможность сбора данных, но и внедрял загрузчик в легитимный процесс svchost.exe. Чаще всего злоумышленники дополнительно загружали рекламное ПО, поэтому для того, чтобы определить, были ли вы заражены этим вредоносом, проанализируйте свою активность в социальных сетях Facebook и на видеохостинге YouTube. Если вы обнаружите действия, которые были инициированы не вами, это признак того, что кто-то контролирует вашу учетную запись, и вам стоит проверить систему на предмет вредоносного ПО. Еще один интересный момент: Scranos перезаписывает себя на диск перед выключением компьютера и создает ключ в реестре для автозагрузки.

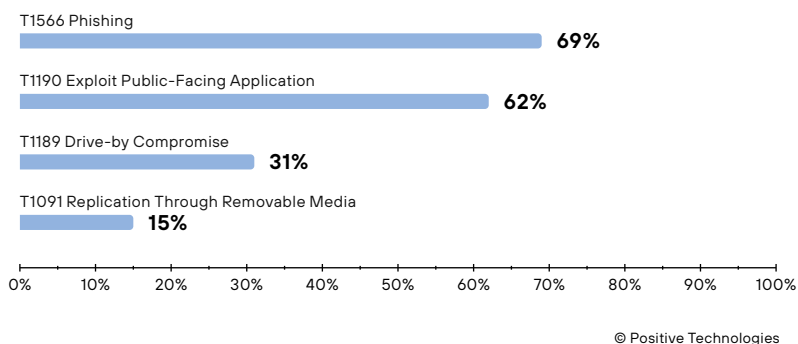
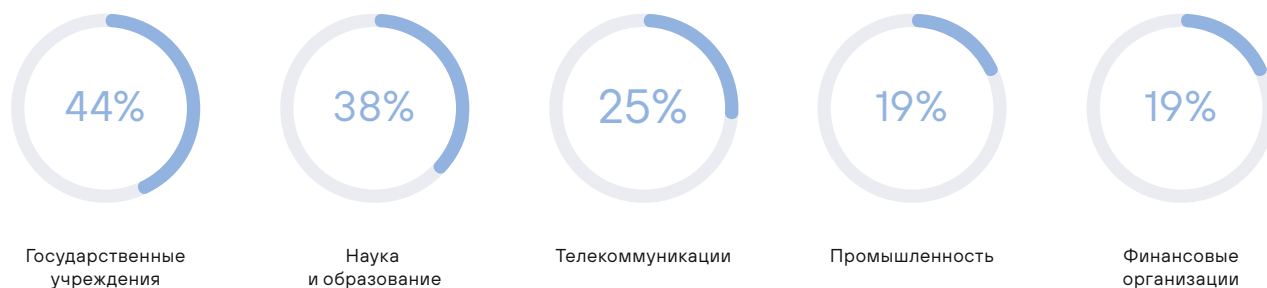


Рисунок 1. Методы распространения руткитов по классификации MITRE ATT&CK (доли руткитов)

Пятерка самых атакуемых отраслей (доля руткитов)

© Positive Technologies

Анализ семейств руткитов показал, что в 44% случаев злоумышленники, используя эти вредоносы, атаковали госучреждения; чуть реже в качестве целей атак встречались учреждения науки и образования. Прежде всего это связано с основным мотивом, преследуемым преступниками, ведь информация, которая обрабатывается в организациях из этих отраслей, представляет большую ценность для злоумышленников.



В атаках на финансовые организации применялось 19% руткитов. Один из примеров руткитов, ориентированных на банки, — [Kronos](#). Его жертвами стали банки на территории Великобритании и Индии.

Более половины руткитов (56%) используется и в атаках на частных лиц. Преимущественно это целенаправленные атаки в отношении высокопоставленных чиновников, дипломатов, сотрудников организаций, представляющих интерес для злоумышленников, то есть атаки в рамках кампаний по кибершпионажу.

Что предлагает дарквеб

Эксперт Билл Демиркапи на конференции по ИБ Defcon в 2020 году пошутил, что написать качественный руткит для Windows очень просто: для этого достаточно программировать на языке C или C++ и собирать проекты, уметь разрабатывать эксплойты, заниматься обратной разработкой и иметь глубокие познания в архитектуре устройств на платформе Windows. Для успешной атаки необходимо всего лишь найти и использовать в своих деструктивных целях уязвимый драйвер, затем незаметно внедрить и установить сам руткит.

Разработка руткита — сложный процесс, однако в сети много информации на эту тему, особенно в дарквебе. Помимо справочных данных, там можно найти как уже готовые варианты вредоносов «для любого кошелька», так и разработчиков, которые допишут код или соберут проект, а сами разработчики могут найти клиентов-работодателей.

Мы проанализировали десять наиболее популярных русскоязычных и англоязычных форумов в дарквебе, где представлены предложения о продаже и запросы о покупке руткитов, а также объявления о поиске разработчиков вредоносов. В основном в объявлениях о продаже фигурируют пользовательские руткиты. Стоимость готового руткита варьируется от 45 до 100 000 долл. США и зависит от режима работы, целевой ОС, условий использования и дополнительных функций.

К примеру, за 100–200 долл. США покупатель получает руткит во временное пользование, то есть может использовать его, например, не более месяца.

Средняя стоимость
руткита в дарквебе —

2800
долл. США

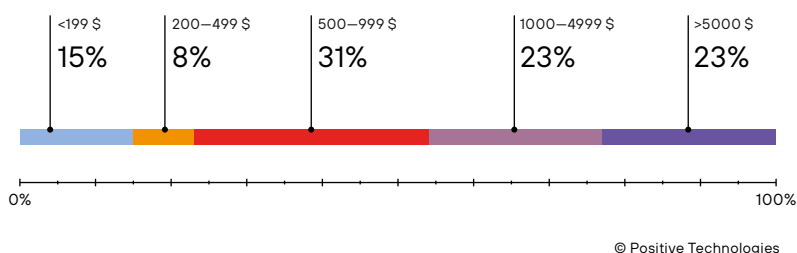


Рисунок 2. Соотношение стоимостей руткитов в продаже

Руткиты без ограничений по времени использования стоят дороже: например, в 2014 году руткит Kronos, который осуществляет сбор данных для доступа в интернет-банкинг, был продан за 7000 долл. США. Такие руткиты чаще всего используются в целевых атаках АРТ-группировок.

В некоторых случаях разработчики вредоноса предлагают доработку руткита под нужды заказчика и оказывают сервисное сопровождение.

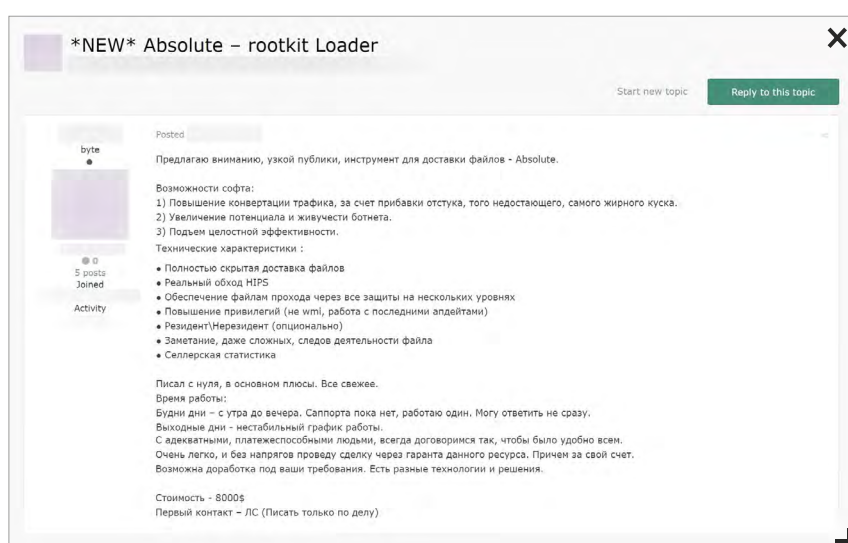


Рисунок 3. Объявление о продаже руткита на форуме в дарквебе

В объявлениях о покупке руткита в основном запрашивают наличие следующих функций: предоставление удаленного доступа, сокрытие файлов, процессов и сетевой активности.

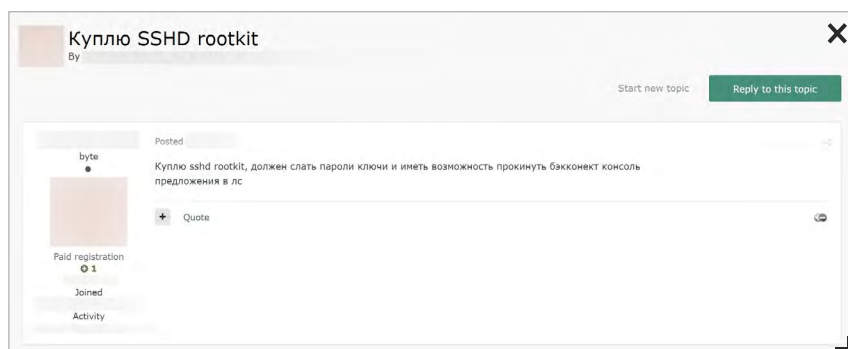
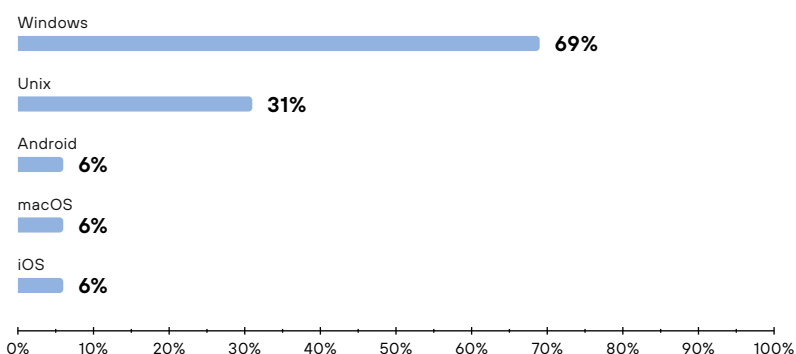


Рисунок 4. Объявление о покупке руткита в дарквебе

В 67% случаев в объявлении фигурировало требование о том, что руткит должен быть заточен под Windows, и в реальных атаках также чаще всего встречаются руткиты, ориентированные на Windows: в исследованных нами семействах их доля составила 69%. Отметим, что некоторые руткиты поддерживают сразу несколько ОС.



© Positive Technologies

Рисунок 5. Доля руткитов, ориентированных на определенные ОС, среди исследованной выборки

В 2006 году разработчики Windows, оценив ущерб от руткитов и степень их распространенности, добавили в новую версию Windows Vista компонент Kernel Patch Protection (KPP). Этот модуль обязал поставщиков аппаратного и программного обеспечения проставлять цифровую подпись для своих драйверов. Позже у злоумышленников получилось обойти эту проверку, поэтому в Windows 10 был предусмотрен ряд функций, которые направлены на предотвращение запуска руткитов за счет проверки драйверов, целостности компонентов, настройки надежных загрузчиков, а также записи и оценки процесса загрузки. Тем не менее эти нововведения также не гарантируют защиту.

Способы обнаружения

Для обнаружения руткита в системе прибегают к сигнатурному и поведенческому анализу системы, а также проверке ее целостности. Согласно данным Европейского агентства по сетевой и информационной безопасности (ENISA), в большинстве случаев руткит можно удалить, только переустановив скомпрометированную систему.

Чтобы обнаружить руткит, можно:

- осуществлять проверку целостности системы;
- анализировать сетевой трафик на предмет аномалий;
- воспользоваться сканером руткитов;
- использовать средства для обнаружения вредоносной активности на конечных узлах, которые помогут обнаружить руткит еще на этапе его установки;
- использовать решения класса песочница (sandbox) для обнаружения руткита на этапе установки и в процессе работы.

Песочница поможет выявить руткит на этапе его установки в системе, так как в это время злоумышленник выполняет ряд вредоносных или как минимум подозрительных действий. Песочницы, работающие без агентов, не препятствуют загрузке руткита, а встроенные анализаторы оповещают о сторонней потенциально опасной нагрузке. Так как вредоносный процесс проходит без прерывания, а проверки на наличие средств защиты не обнаруживают песочницу в таком исполнении, у злоумышленника не возникает подозрений, что его уже обнаружили. К слову, эксперты PT ESC в октябре 2021 года выпустят подробное исследование, в котором можно будет ознакомиться подробнее со всеми техниками детектирования руткитов с помощью песочницы.

Для того чтобы свести к минимуму возможность заражения руткитом, следует отслеживать и своевременно устанавливать обновления безопасности, устанавливать программы только из доверенных источников и проверять цифровые подписи и сертификаты перед установкой, а также регулярно обновлять сигнатуры антивирусных средств, ведь они способны обнаружить большую часть «старых» руткитов.

Будущее руткитов

Мы считаем, что в ближайшее время руткиты не пропадут из инструментов киберпреступников. Специалисты PT ESC отмечают появление новых версий руткитов, чей механизм работы отличается от уже известных вредоносов, и это свидетельствует о том, что злоумышленники не стоят на месте и придумывают новые техники обхода защиты. Преимущества, которые дает использование руткитов — выполнение кода в привилегированном режиме, возможность скрываться от средств защиты и незаметно находиться в сети длительное время, — слишком важны для преступников, чтобы отказаться от такого инструмента. Вместе с тем руткиты продолжают использовать преимущественно высококвалифицированные группировки, обладающие навыками для разработки подобного инструмента, а также группировки, обладающие достаточными финансовыми ресурсами для покупки руткитов на теневом рынке. Это означает, что главная опасность руткитов будет заключаться в сокрытии сложных целенаправленных атак вплоть до непосредственного осуществления недопустимых для организации событий.



ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности. Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «[Новости](#)» на сайте [ptsecurity.com](#).