Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности за 2019 год

«Доктор Веб»: обзор вирусной активности за 2019 год

Главное

3 февраля 2020 года

В 2019 году одними из самых распространенных угроз стали троянцы и вредоносные скрипты, предназначенные для незаметной добычи криптовалют. Кроме того, серьезную опасность представляли троянцы, похищавшие пароли и другую конфиденциальную информацию. На протяжении всего года пользователей атаковали банковские троянцы, в том числе Win32.Bolik.2. Вирусные аналитики «Доктор Веб» зафиксировали его распространение в начале весны, а также летом. Эта вредоносная программа обладает свойствами полиморфного файлового вируса и способна заражать другие приложения. Win32.Bolik.2 выполнял веб-инжекты, перехватывал сетевой трафик и нажатия на клавиатуре, а также крал информацию из систем «банк-клиент».

Также весной наши специалисты обнаружили несколько уязвимостей в Steam-клиенте популярной игры Counter Strike 1.6, которые эксплуатировал троянец Belonard. Он объединял зараженные компьютеры в ботнет и превращал их в прокси-серверы.

В почтовом трафике преобладали угрозы, которые загружали на атакуемые компьютеры других троянцев и выполняли произвольный код. Кроме того, в сообщениях электронной почты злоумышленники распространяли майнеров, шпионов и банковских троянцев.

Несмотря на то, что большая часть выявленных вредоносных программ предназначалась для пользователей ОС Windows, владельцы компьютеров под управлением macOS также были в зоне риска. Одной из угроз для них стал бэкдор Mac.BackDoor.Siggen.20, с помощью которого злоумышленники могли загружать и выполнять на зараженных устройствах произвольный код.

Пользователям мобильных устройств на базе ОС Android угрожали рекламные троянцы, шпионское ПО, банкеры и всевозможные загрузчики, которые скачивали другие вредоносные приложения и выполняли произвольный код.

Главные тенденции года

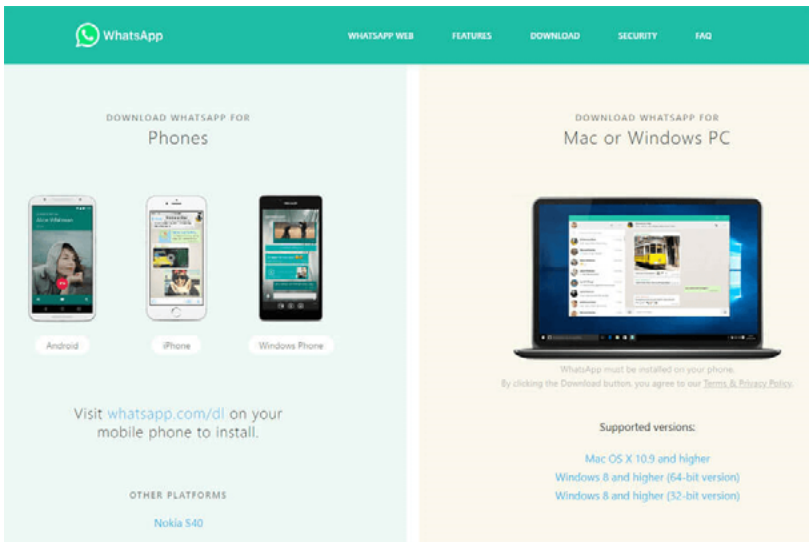
- Распространение троянцев-майнеров для тайной добычи криптовалют
- Повышение активности шифровальщиков
- Появление новых угроз для macOS
- Активное распространение вредоносных программ Для ОС Android в каталоге Google Play

Наиболее интересные события 2019 года

В январе аналитики «Доктор Веб» обнаружили троянца в программе для отслеживания курса криптовалют. Вредоносная программа распространялась вместе с утилитой и устанавливала на зараженные устройства других троянцев. Используя эти программы, хакеры получали возможность красть личные данные пользователей, в том числе пароли от кошельков криптовалют.

В марте аналитики «Доктор Веб» опубликовали подробное исследование троянца Belonard, использующего уязвимости нулевого дня в Steam-клиенте игры Counter-Strike 1.6. Попав на компьютер жертвы, троянец менял файлы клиента и создавал игровые прокси-серверы для заражения других пользователей. Количество вредоносных серверов CS 1.6, созданных Belonard, достигло 39% от числа всех официальных серверов, зарегистрированных в Steam. Теперь все модули Trojan.Belonard успешно определяются антивирусом Dr.Web и не угрожают нашим пользователям.

В мае специалисты «Доктор Веб» сообщили о новой угрозе для операционной системы macOS – Mac.BackDoor.Siggen.20. Это ПО позволяет загружать и исполнять на устройстве пользователя любой код на языке Python. Сайты, распространяющие это вредоносное ПО, также заражают компьютеры под управлением ОС Windows шпионским троянцем BackDoor.Wirenet.517 (NetWire). Последний является давно известным RAT-троянцем, с помощью которого хакеры могут удаленно управлять компьютером жертвы, включая использование камеры и микрофона на устройстве. Кроме того, распространяемый RAT-троянец имеет действительную цифровую подпись.



В июне в вирусной лаборатории «Доктор Веб» был изучен образец редкого Node.js-троянца — Trojan.MonsterInstall. Запустившись на устройстве жертвы, он загружает и устанавливает необходимые для своей работы модули, собирает информацию о си-

Наиболее интересные события 2019 года

стеме и отправляет ее на сервер разработчика. После получения ответа от сервера он устанавливается в автозагрузку и начинает добычу (майнинг) криптовалюты TurtleCoin. Разработчики этого вредоносного ПО используют для распространения собственные ресурсы с читами к популярным играм, а также заражают файлы на других подобных сайтах.

Вирусная обстановка

По данным серверов статистики «Доктор Веб», в 2019 году на компьютерах чаще всего обнаруживались троянцы и скрипты, выполняющие майнинг криптовалют на устройствах без ведома пользователей. Кроме того, активными были троянцы, которые устанавливали различное вредоносное ПО.

Trojan.MulDrop9.2530

Троянец-дроппер, распространяющий и устанавливающий вредоносное ПО.

Trojan.Starter.7394

Представитель семейства троянцев, основное назначение которых — запуск в инфицированной системе исполняемого файла с определенным набором вредоносных функций.

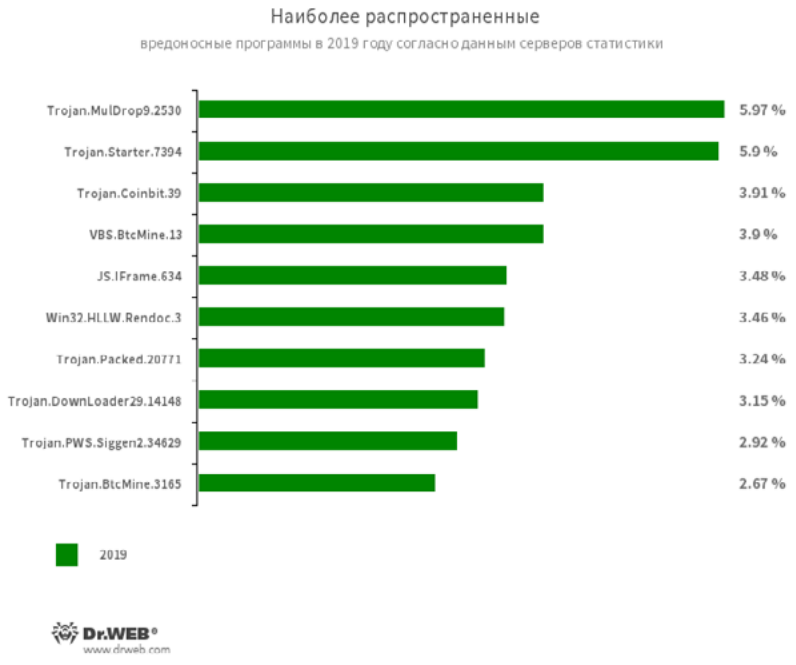
Trojan.Coinbit.39

Trojan.BtcMine.3165

Троянцы, занимающиеся незаметной добычей (майнингом) криптовалют с использованием вычислительных ресурсов зараженных устройств.

Вирусная обстановка

VBS.BtcMine.13
Вредоносный сценарий на языке VBS, выполняющий скрытую добычу (майнинг) криптовалют.
JS.IFrame.634
Скрипт, который злоумышленники внедряют в html-страницы. При открытии таких страниц скрипт выполняет перенаправление на различные вредоносные и нежелательные сайты.
Win32.HLLW.Rendoc.3
Сетевой червь, распространяющийся в том числе через съемные носители информации.
Trojan.Packed.20771
Семейство вредоносных приложений, защищенных программным упаковщиком.
Trojan.DownLoader29.14148
Троянец, предназначенный для загрузки другого вредоносного ПО.
Trojan.PWS.Siggen2.34629
Представитель семейства троянцев, похищающих пароли.
В почтовом трафике преобладали троянцы, загружавшие и устанавливавшие на атакуемые устройства другое вредоносное ПО. Кроме того, по каналам электронной почты злоумышленники распространяли программы-вымогатели, майнеры, банковских троянцев и шпионов, похищавших конфиденциальные данные.



Вирусная обстановка

JS.DownLoader.1225
Представитель семейства вредоносных сценариев, написанных на языке JavaScript. Они загружают и устанавливают на компьютер другие вредоносные программы.

Exploit.Rtf.CVE2012-0158
Измененный документ Microsoft Office Word, использующий уязвимость CVE2012-0158 для выполнения вредоносного кода.

Trojan.SpyBot.699
Многомодульный банковский троянец. Он позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и выполнять поступающие от них команды. Троянец предназначен для хищения средств с банковских счетов.

Exploit.ShellCode.69
Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.

W97M.DownLoader.2938
Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

JS.Miner.11
Семейство сценариев на языке JavaScript, предназначенных для скрытой добычи (майнинга) криптовалют.

Trojan.PWS.Siggen2.10310

Trojan.PWS.Stealer.19347
Представители семейств троянцев, похищающих логины и пароли.

Trojan.Nanocore.23
Троянец, с помощью которого злоумышленники подключаются к зараженным компьютерам и управляют ими.

Trojan.Encoder.26375
Вредоносная программа, которая шифрует файлы и требует выкуп за их расшифровку.

Троянцы-шифровальщики

По сравнению с 2018 годом, за последние 12 месяцев число обращений в службу технической поддержки компании «Доктор Веб» от пользователей, файлы которых оказались зашифрованы троянцами-энкодерами, выросло на 19,52%. Динамика регистрации таких запросов в 2019 году показана на графике:

Наиболее распространенные шифровальщики в 2019 году:

- Trojan.Encoder.858 — 20.18% обращений;
- Trojan.Encoder.18000 — 5.70% обращений;
- Trojan.Encoder.11464 — 5.59% обращений;
- Trojan.Encoder.26996 — 5.15% обращений;
- Trojan.Encoder.567 — 4.20% обращений.

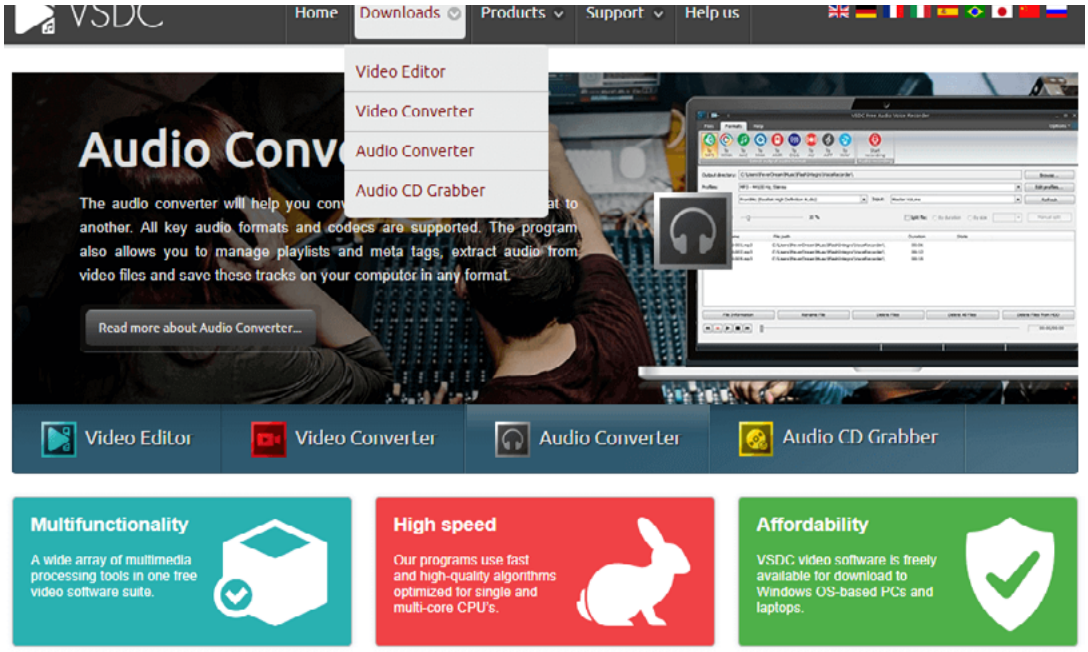
Опасные и нерекомендуемые сайты

Базы Родительского (Офисного) контроля и веб-антивируса SpIDer Gate регулярно пополняются новыми адресами нерекомендуемых и потенциально опасных сайтов. Среди них — мошеннические и фишинговые ресурсы, а также страницы, с которых распространяется вредоносное ПО. Наибольшее число таких ресурсов было зафиксировано в первом квартале, а наименьшее — в третьем. Динамика пополнения баз нерекомендуемых и опасных сайтов в прошлом году показана на диаграмме ниже.

Сетевое мошенничество

В апреле специалисты компании «Доктор Веб» предупредили пользователей о компрометации официального сайта популярного ПО для обработки видео и звука. Хакеры заменили ссылку на скачивание, и вместе с редактором пользователи загружали опасного банковского трояна Win32.Bolik.2. Он предназначен для выполнения веб-инжектов, перехвата трафика, кейлоггинга (регистрации нажатий на клавиатуре) и похищения информации из систем «банк-клиент» различных кредитных организаций.

Позднее хакеры заменили Win32.Bolik.2 на другое вредоносное ПО – один из вариантов шпиона Trojan.PWS.Stealer (KPOT Stealer). Этот троянец крадет информацию из браузеров, аккаунта Microsoft, различных мессенджеров и других программ.



В августе специалисты вирусной лаборатории «Доктор Веб» обнаружили, что в середине лета злоумышленники несколько изменили тактику и для распространения Win32.Bolik.2 начали использовать копии сайтов популярных сервисов. Один из таких ресурсов копировал известный VPN-сервис, а другие были замаскированы под сайты корпоративных офисных программ.

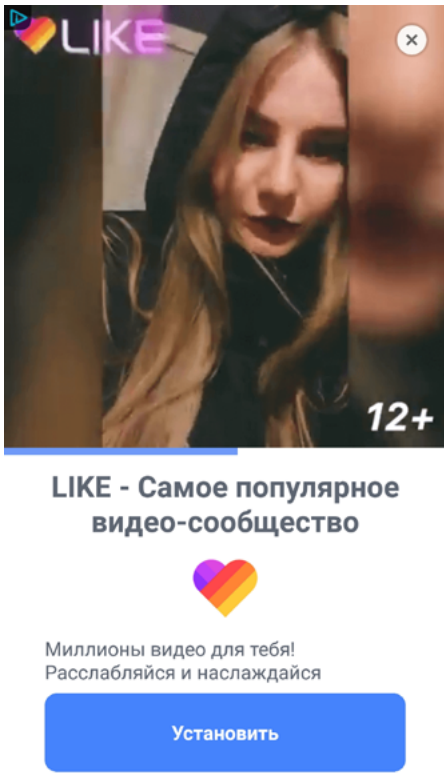
Для мобильных устройств

Пользователям мобильных устройств прошедший год запомнился, прежде всего, активностью троянцев и нежелательных программ, основной задачей которых был показ рекламы. В их числе – многочисленные троянцы семейства Android.HiddenAds.

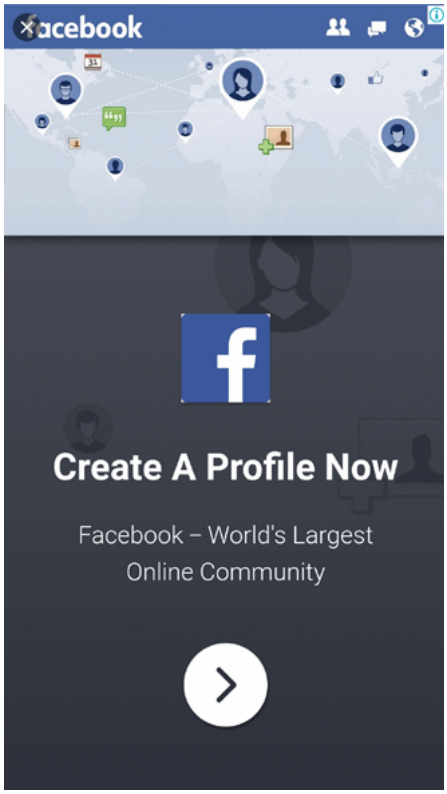
Например, только в феврале вирусные аналитики «Доктор Веб» обнаружили в Google Play около 40 различных модификаций этих вредоносных приложений, которые установили более 10 000 000 пользователей. А в течение всего года наши специалисты выявили сотни таких троянцев. В общей сложности на их долю пришлось 22,27% всех угроз, детектируемых на Android-устройствах.

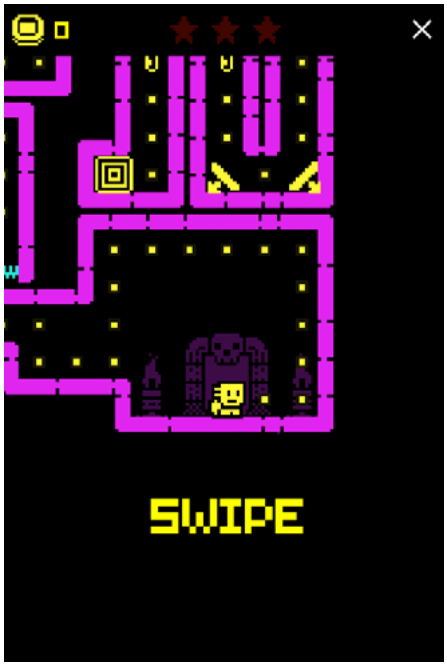
Злоумышленники распространяют их под видом полезных программ и даже рекламируют через социальные сети и популярные онлайн-сервисы с многомиллионными аудиториями (например, Instagram и YouTube). Пользователи полагают, что устанавливают безобидные приложения, поэтому троянцы легко проникают на множество устройств.

После установки и запуска троянцы Android.HiddenAds скрывают свои значки из списка программ на главном экране и начинают показывать надоедливую рекламу — баннеры, окна с анимацией и видеороликами. Такая реклама перекрывает окна других приложений и интерфейс операционной системы, мешая нормальной работе с Android-устройствами.

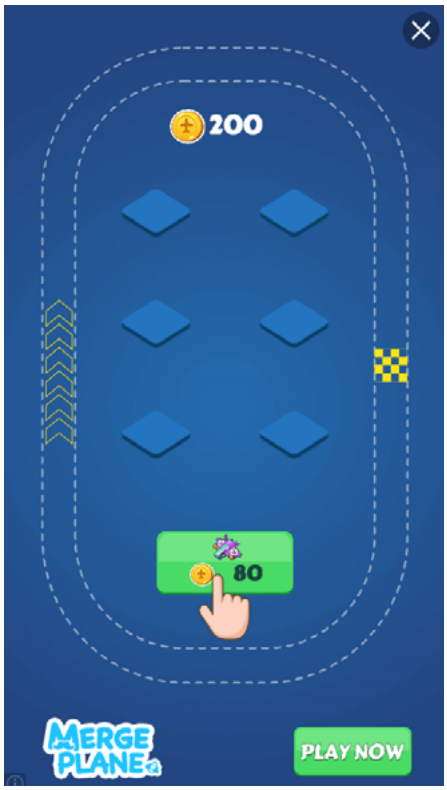


Для мобильных устройств





Для мобильных устройств



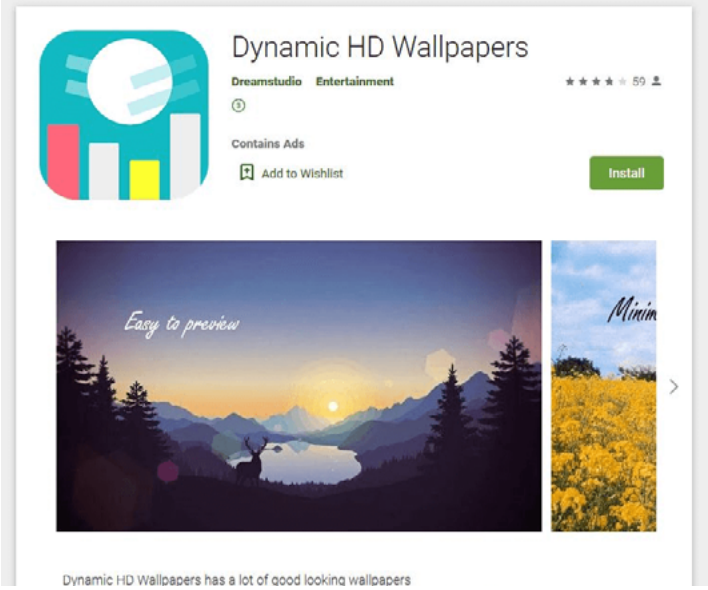
Уже весной наши вирусные аналитики обнаружили троянца Android.InfectionAds.1, эксплуатировавшего критические уязвимости ОС Android. Он заражал другие программы и мог устанавливать приложения без разрешения пользователей. Основной функцией Android.InfectionAds.1 был показ рекламы и подмена рекламных идентификаторов в заражаемых приложениях, в результате чего доход от рекламы поступал вирусописателям, а не разработчикам затронутых программ.

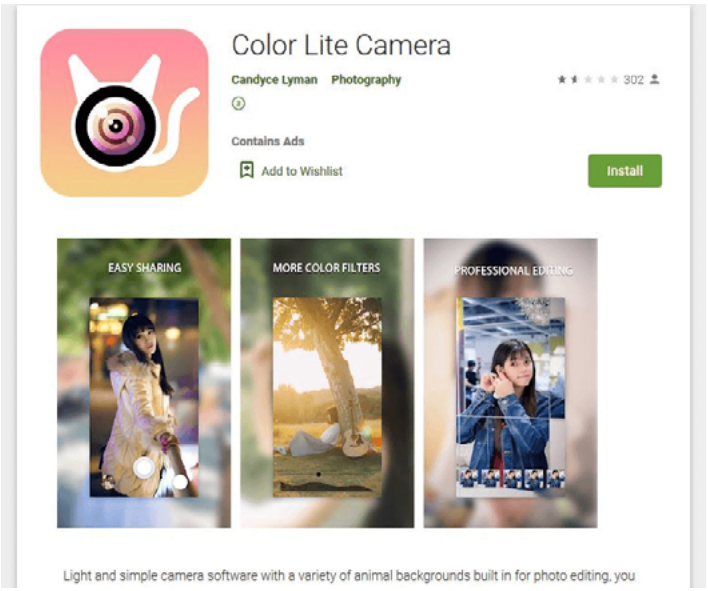
Кроме того, заработок от показа рекламы получали и создатели нежелательных рекламных модулей (Adware), которые многие разработчики сознательно, а иногда и по незнанию встраивают в приложения для их монетизации. Среди угроз, обнаруженных на Android-устройствах, доля таких модулей составила 14,49%.

Как и в прошлые годы, опасность для пользователей представляли различные троянцы-загрузчики и вредоносные программы, которые скачивают других троянцев и приложения, а также способны выполнять произвольный код. К таким угрозам относятся, например, представители семейств Android.DownLoader, Android.Triada и Android.RemoteCode. В 2019 году эти троянцы были одними из самых распространенных угроз, обнаруживаемых на Android-устройствах.

Для мобильных устройств

В течение года было выявлено множество новых троянцев-кликеров, которые выполняют автоматические переходы по ссылкам, загружают веб-страницы с рекламой и подписывают пользователей на платные мобильные услуги. Среди таких вредоносных программ, найденных нашими специалистами, были Android.Click.312.origin, Android.Click.322.origin, Android.Click.323.origin и Android.Click.324.origin. Эти и другие подобные троянцы распространяются под видом безобидных и полезных приложений — фоторедакторов, сборников обоев рабочего стола игр и т. п.





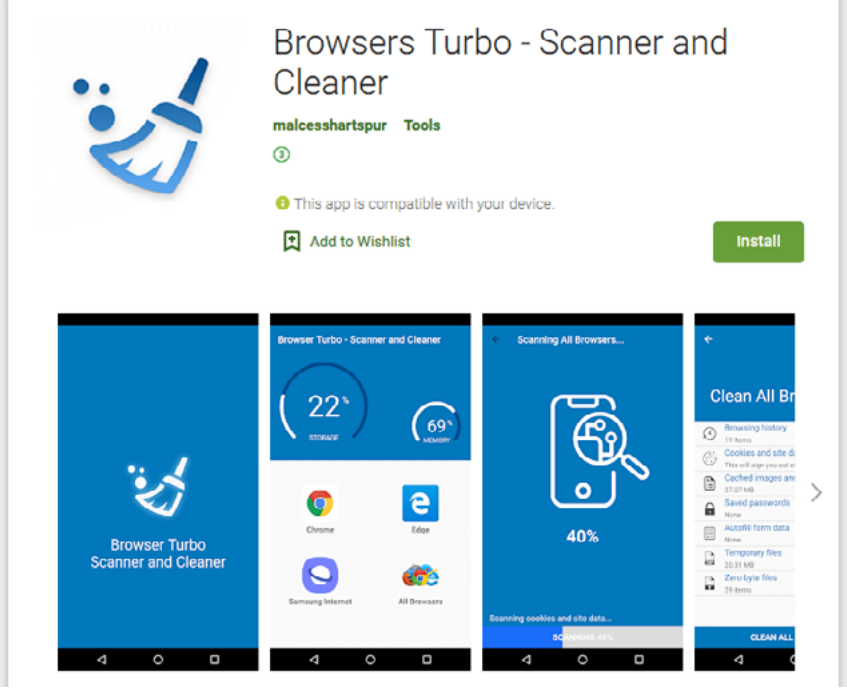
Для мобильных устройств

В 2019 году серьезную опасность для владельцев Android-устройств вновь представляли банковские троянцы, которые атаковали пользователей по всему миру. Например, в августе и октябре вирусные аналитики «Доктор Веб» обнаружили очередные модификации опасного троянца Android.BankBot.495.origin, нацеленного на клиентов бразильских кредитных организаций. Это вредоносное приложение использует специальные возможности ОС Android (Accessibility Service), предназначенные для людей с ограниченными возможностями. С помощью этих функций банкер похищает конфиденциальные данные, после чего злоумышленники получают доступ к счетам жертв.

Кроме того, продолжились атаки троянца Flexnet, который относится к семейству Android.ZBot. По современным меркам эта вредоносная программа имеет скромный набор функций, которых, однако, хватает для успешной кражи денег со счетов пользователей. С помощью этого банкера киберпреступники переводят деньги жертв на свои карты, счета мобильных телефонов и оплачивают различные услуги.

Прошедший год показал, что актуальной остается проблема кибершпионажа и утечек секретных данных. В июне наши специалисты выявили в Google Play опасного бэкдора Android.Backdoor.736.origin, известного также как PWNDROID1. А уже позднее, в ноябре, была найдена его новая модификация. Этот троянец позволял злоумышленникам дистанционно управлять зараженными Android-устройствами и выполнять на них различные действия — перехватывать СМС-сообщения, следить за телефонными звонками и местоположением устройств, выполнять прослушивание окружения, передавать файлы пользователей на сервер и даже загружать и устанавливать другие программы.

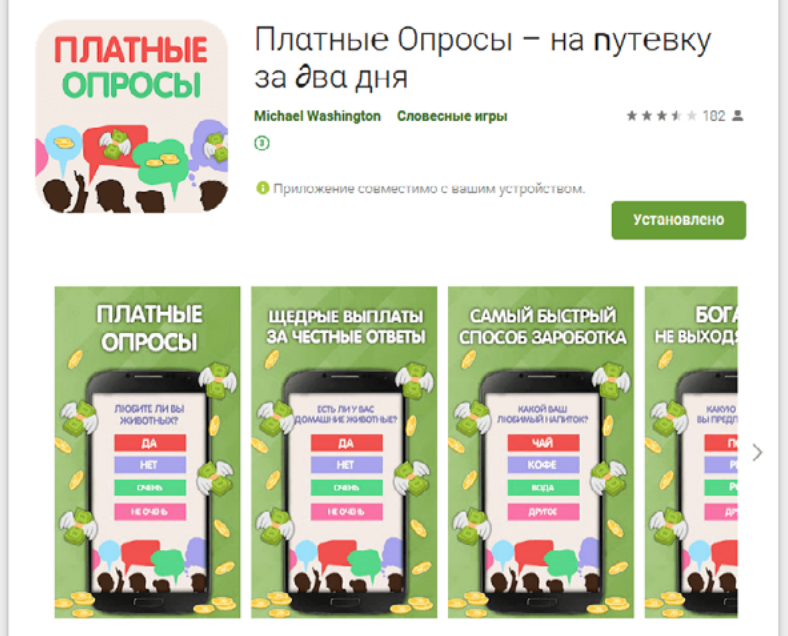
Для мобильных устройств

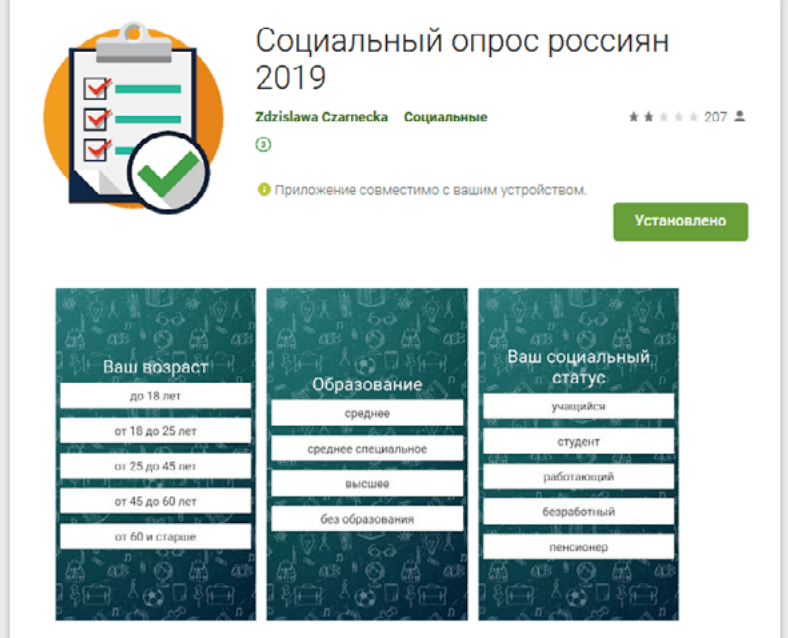


Кроме того, в 2019 году было выявлено новое ПО для наблюдения за пользователями. Такие приложения часто позиционируются как средства обеспечения безопасности детей и других членов семьи, контроля работников и т. п. Они не являются вредоносными, но могут быть использованы в незаконных целях.

Также пользователям устройств под управлением ОС Android стоило опасаться мошенников. Например, вновь получили распространение троянские программы семейства Android.FakeApp, загружавшие веб-сайты с поддельными опросами. За участие в них потенциальным жертвам предлагалось денежное вознаграждение. Чтобы получить его, пользователи якобы должны были оплатить комиссию или подтвердить свою личность, переведя на счет мошенников определенную сумму. Однако в итоге никакого вознаграждения жертвы не получали и теряли деньги.

Для мобильных устройств





Перспективы и вероятные тенденции

В конце 2018 года пользователи сталкивались с множеством информационных угроз, и одним из основных рисков для них были потеря денег и кибершпионаж. По нашему прогнозу, эта тенденция должна была сохраниться и в 2019 году, что оказалось верным.

В наступившем году киберпреступники продолжат использовать вредоносные приложения для своего незаконного обогащения. В связи с этим стоит ожидать роста активности троянцев-майнеров, банковских и рекламных троянцев, а также шпионского ПО, которое будет собирать ценные сведения о пользователях. Кроме того, вероятно появление новых мошеннических схем, а также фишинг-кампаний и спам-рассылок.

При этом под прицелом вновь окажутся не только пользователи Windows: владельцы устройств под управлением macOS, Android, Linux и других платформ останутся под пристальным вниманием вирусописателей и сетевых мошенников. Эволюция вредоносных программ и изобретательность киберпреступников не стоят на месте, поэтому пользователям необходимо соблюдать правила информационной безопасности и применять надежные антивирусные средства.

«Доктор Веб»: обзор вирусной активности за 2019 год

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

Полезные ресурсы
ВебIQметр | Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах