Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности за 2021 год

«Доктор Веб»: обзор вирусной активности за 2021 год

21 января 2022 года

Среди самых популярных угроз в 2021 году фигурировали многочисленные вредоносные программы. Среди них были трояны-дропперы, предназначенные для распространения вредоносного ПО, а также множественные модификации троянов-загрузчиков — они загружают и запускают на компьютере жертвы исполняемые файлы с различной полезной нагрузкой. Помимо этого, злоумышленники активно распространяли бэкдоры.

Среди почтовых угроз самыми популярными оказались стилеры, различные модификации бэкдоров, написанные на VB.NET. Кроме того, злоумышленники активно распространяли PDF-файлы с вредоносной нагрузкой, трояны-загрузчики, а также веб-страницы, представляющие собой форму ввода учетных данных, которая имитирует авторизацию на известных сайтах. Часть распространяемых в почте угроз пришлась на программы, эксплуатирующие различные уязвимости документов Microsoft Office.

В 2021 году вирусная лаборатория «Доктор Веб» опубликовала несколько расследований. Одним из них стало исследование Spyder — модульного бэкдора для целевых атак. Наши специалисты зафиксировали, что хакерская группировка Winnti использовала этот образец для атак на предприятия в Центральной Азии.

Также в прошедшем году аналитики «Доктор Веб» расследовали целевые атаки на российские НИИ. В ходе расследования специалистам нашей компании удалось раскрыть несанкционированное присутствие APT-группы, деятельность которой оставалась незамеченной почти 3 года.

Однако вирусописатели традиционно не ограничивали себя платформой Windows. Атакам регулярно подвергались владельцы устройств на базе ОС Android. Злоумышленники активно распространяли трояны в каталоге Google Play, при этом мы обнаружили первые трояны и в AppGallery. Самыми популярными угрозами для мобильных устройств оказались различные шпионские и банковские трояны, а также загрузчики вредоносного ПО и трояны, способные выполнять произвольный код.

ГЛАВНЫЕ ТЕНДЕНЦИИ ГОДА

- Активное распространение ВПО для Android, в том числе в официальных каталогах
- Рост числа инцидентов с троянами-вымогателями
- Рост числа мошеннических сайтов
- Распространение сетевого мошенничества

Наиболее интересные события 2021 года

В марте специалисты «Доктор Веб» выпустили масштабное исследование модульного бэкдора, предназначенного для целевых атак. В нашу вирусную лабораторию обратились телекоммуникационная компания из Центральной Азии. Оказалось, что сеть была скомпрометирована хакерской группировкой Winnti. Рассмотренный образец бэкдора для целевых атак BackDoor.Spyder.1 оказался примечателен тем, что его код не выполняет прямых вредоносных функций. Среди основных задач трояна — скрытое функционирование в зараженной системе и установление связи с управляющим сервером с последующим ожиданием команд операторов.

Спустя месяц специалисты «Доктор Веб» опубликовали ещё одно исследование. За помощью обратился российский научно-исследовательский институт — сотрудники заметили некоторые технические проблемы, которые свидетельствовали о наличии вредоносного ПО на сервере локальной сети. Вирусные аналитики выяснили, что НИИ подвергся целевой атаке с использованием нескольких бэкдоров, включая BackDoor.Skeye и BackDoor.DNSep. Примечательно, что впервые сеть была скомпрометирована ещё в 2017 году и с тех пор несколько раз подвергалась атакам, судя по имеющимся данным — сразу несколькими хакерскими группировками.

Летом компания «Доктор Веб» рассказывала о появлении критических уязвимостей диспетчера очереди печати ОС Windows. Уязвимость затрагивала все популярные версии операционной системы. С помощью эксплойтов злоумышленники использовали в своих целях компьютеры жертв. Например, загружали вредоносные трояны-шифровальщики, требующие выкуп за расшифровку поврежденных файлов. Уязвимости CVE-2021-34527 и CVE-2021-1675 получили название PrintNightmare. Для каждой из них вскоре появились официальные патчи от разработчика операционной системы.

Начало осени запомнилось массовым введением QR-кодов, подтверждающих факт вакцинации, в связи с чем активизировались мошенники. Например, злоумышленники часто подделывали сайт портала Госуслуг. Фишинговые сайты предназначались для кражи учетных данных, впоследствии используемых для несанкционированных действий от лица жертв. Количество выявленных фишинговых сайтов резко увеличилось почти на 30%. В дни наибольшей активности мошенников база веб-антивируса Dr.Web SpIDer Gate пополнялась сотнями фейковых сайтов.

Эксплуатация коронавирусной повестки продолжилась и в декабре. Злоумышленники предлагали скачать генератор QR-кодов о вакцинации. На деле же пользователь, который загружал вредоносную программу, получал сразу несколько троянов. Загруженный архив содержал исполняемый файл, который дополнительно доставлял на компьютер жертвы майнер и клипер.

Также в прошедшем году пользователям угрожали уязвимости библиотеки логирования Log4j 2. Наиболее критическая из них — Log4Shell (CVE-2021-44228) основана на том, что при логировании библиотекой Log4j 2 сообщений, сформированных особым образом, происходит обращение к контролируемому злоумышленниками серверу с последующим выполнением кода. Через уязвимости киберпреступники распространяли майнеры, бэкдоры, а также DDoS-трояны. Продукты Dr.Web успешно детектируют полезную нагрузку вредоносного ПО, проникающего на устройства через уязвимости.

Вирусная обстановка

Анализ статистики Dr.Web показал, что в 2021 году пользователей чаще всего атаковали трояны-загрузчики, которые устанавливали вредоносные программы. Помимо этого, на протяжении всего года пользователям угрожали различные бэкдоры и трояны, предназначенные для скрытого майнинга.

Trojan.BPlug.3867

Вредоносное расширение для браузера, предназначенное для осуществления веб-инжектов в просматриваемые пользователями интернет-страницы и блокировки сторонней рекламы.

Trojan.AutoIt.289

Trojan.AutoIt.961

Утилита, написанная на скриптовом языке AutoIt и распространяемая в составе майнера или RAT-трояна. Выполняет различные вредоносные действия, затрудняющие обнаружение основной полезной нагрузки.

Tool.BtcMine.2449

Вредоносная программа для скрытого майнинга на устройстве.

BackDoor.RMS.178

BackDoor.RMS.82

Бэкдор для удаленного управления компьютером.

Trojan.DownLoader35.65029

Троян для загрузки вредоносного ПО на компьютер жертвы.

Trojan.MulDrop9.2530

Trojan.MulDrop15.62039

Дроппер, распространяющий и устанавливающий другое вредоносное ПО.

JS.DownLoader.5684

Троян, написанный на языке JavaScript, предназначенный для загрузки вредоносных программ.

В почтовом трафике в 2021 году чаще всего распространяли различные бэкдоры, трояны-банкеры и другое вредоносное ПО, использующее уязвимости офисных документов. Кроме того, злоумышленники отправляли в фишинговых рассылках фиктивные формы ввода данных и вредоносные PDF-файлы.

Вирусная обстановка

W97M.DownLoader.2938
Семейство троянов-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.
BackDoor.SpyBotNET.25
Бэкдор, написанный на .NET. Способен манипулировать файловой системой (копирование, удаление, создание директорий и т. д.), завершать процессы, делать снимки экрана.
JS.IFrame.811
Скрипт, который злоумышленники внедряют в html-страницы. При открытии таких страниц скрипт выполняет перенаправление на различные вредоносные и нежелательные сайты.
Trojan.SpyBot.699
Многомодульный банковский троян. Позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и исполнять произвольный код.
Win32.HLLW.Rendoc.3
Сетевой червь, распространяющийся в том числе через съемные носители информации.
JS.Redirector.407
Вредоносный сценарий на языке JavaScript, размещаемый в коде веб-страниц. Предназначен для перенаправления пользователей на фишинговые или рекламные сайты.
PDF.Phisher.313
PDF-документ, использующийся в фишинговой рассылке.
Exploit.ShellCode.69
Вредоносный документ Microsoft Office Word. Использует уязвимость CVE-2017-11882.
HTML.FishForm.209
Веб-страница, распространяющаяся посредством фишинговых рассылок. Представляет собой фиктивную форму ввода учетных данных, которая имитирует авторизацию на известных сайтах. Введенные пользователем данные отправляются злоумышленнику.
JS.Siggen5.40409
Вредоносный сценарий, написанный на языке JavaScript.

Шифровальщики

По сравнению с 2020, в 2021 году число запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков, в антивирусную лабораторию «Доктор Веб» поступило на 26,6% меньше. Динамика регистрации таких запросов в 2021 году показана на графике:

Наиболее распространенные шифровальщики в 2021 году:

Trojan.Encoder.26996

Шифровальщик, известный как STOP Ransomware. Пытается получить приватный ключ с сервера, а в случае неудачи пользуется зашитым. Один из немногих троянов-вымогателей, который шифрует данные поточным алгоритмом Salsa20.

Trojan.Encoder.567

Шифровальщик, написанный на Delphi. История развития трояна насчитывает множество версий с использованием различных алгоритмов шифрования. Как правило, распространяется в виде вложений к электронным письмам.

Trojan.Encoder.29750

Шифровальщик из семейства Limbo/Lazarus. Несет в себе зашитый авторский ключ, применяемый в случае отсутствия связи с управляющим сервером и возможности выгрузить приватную часть сгенерированного ключа.

Trojan.Encoder.30356

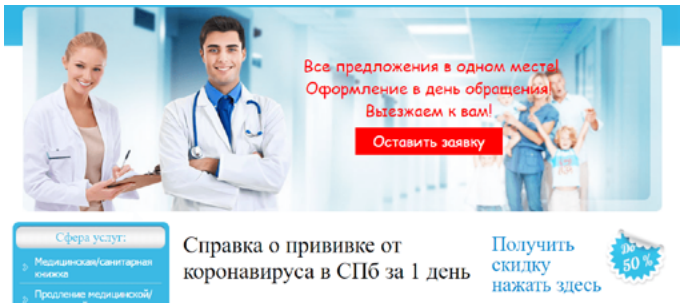
Шифровальщик, написанный на Delphi и известный как Zeppelin Ransomware. Для шифрования файлов использует симметричный алгоритм AES-256, а для защиты закрытого ключа — ассиметричный RSA-2048.

Trojan.Encoder.11539

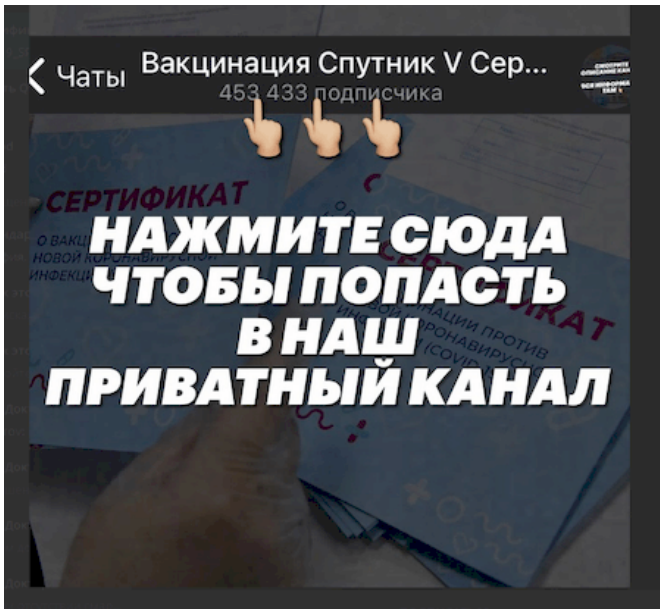
Шифровальщик, имеющий множество модификаций, которые отличаются разным набором алгоритмов шифрования. Как правило, распространяется в виде вложений к электронным письмам и для шифрования файлов использует алгоритм AES-256 в режиме CBC.

Сетевое мошенничество

В течение 2021 года интернет-аналитики «Доктор Веб» обнаружили множество опасных сайтов, большинство из которых оказались связаны с тематикой QR-кодов. В мае были обнаружены страницы, позволяющие купить любые поддельные документы, в том числе и справки о прививке от коронавируса. Мошенники тщательно пытались замаскировать нелегальную деятельность, публикуя на сайте разоблачающие других жуликов статьи.



С тех пор злоумышленники не отпускали тему коронавируса, каждый месяц создавая сайты и прочие ресурсы, где можно купить или сгенерировать QR-код. Летом специалисты «Доктор Веб» обнаружили приватные чаты: они кишат предложениями приобрести QR-код и подтверждают «безопасность» процедуры якобы восторженными отзывами тех, кто уже купил сертификат о вакцинации.



Также на волне коронавирусной тематики злоумышленники распространяют фейковые генераторы QR-кодов. Следует помнить, что сертификат о вакцинации нельзя сгенерировать каким-то особым образом, — он генерируется только из ссылки на конкретную страницу портала Госуслуг или информационной системы субъекта федерации, касающуюся факта иммунизации гражданина.

Для мобильных устройств

Согласно статистике детектирований антивирусными продуктами Dr.Web для Android, в 2021 году пользователи ОС Android чаще всего сталкивались с троянами семейства Android.HiddenAds, демонстрировавшими всевозможную рекламу. На их долю пришлось более 83% всех вредоносных приложений, обнаруженных на защищаемых устройствах. Широкое распространение получили трояны, основная функция которых — загрузка других программ, а также скачивание и запуск произвольного кода. По сравнению с 2020 годом, на 43% возросла активность банковских троянов.

Среди нежелательных приложений самыми активными оказались программы семейства Program.FakeAntiVirus, имитировавшие работу антивирусов. Они предлагали пользователям приобрести их полные версии — якобы для лечения выявленных заражений. Также на Android-устройствах встречалось различное ПО, позволяющее следить за их владельцами.

Более чем на 53% выросло число обнаруженных потенциально опасных утилит Tool.SilentInstaller, позволяющих запускать Android-приложения без их установки. Такие инструменты могут использоваться не только в безобидных целях, но и при распространении троянов. Всевозможные рекламные модули и рекламные программы также детектировались довольно часто — их доля превысила 10% от всех выявленных угроз.

В течение года вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play множество угроз. Среди них — приложения-подделки семейства Android.FakeApp, которые злоумышленники используют в различных мошеннических схемах, и трояны Android.Joker, способные загружать и исполнять произвольный код, а также автоматически подписывать пользователей на платные мобильные сервисы. Также здесь встречались рекламные трояны, рекламные приложения и банковские трояны. Кроме того, злоумышленники распространяли вредоносные программы семейства Android.PWS.Facebook, похищавшие необходимые для взлома учетных записей Facebook данные.

Минувший год был отмечен тем, что в каталоге приложений AppGallery для Android-устройств компании Huawei были найдены первые троянские приложения. Ими стали уже знакомые трояны семейства Android.Joker, а также вредоносный модуль Android.Cynos.7.origin, который собирал информацию о мобильных номерах пользователей и демонстрировал рекламу.

Среди угроз, выявленных нашими специалистами в 2021 году, был троян Android.Triada.4912. Злоумышленники встроили его в одну из версий приложения APKPure — клиентского ПО одноименного альтернативного каталога Android-программ. Он загружал различные веб-сайты, а также скачивал другие вредоносные модули и разнообразные приложения. Кроме того, вирусные аналитики «Доктор Веб» обнаружили новое семейство модульных банковских троянов Android.BankBot.Coper. Они перехватывают и отправляют СМС-сообщения, выполняют USSD-запросы, блокируют и разблокируют экран, демонстрируют push-уведомления и фишинговые окна, способны удалять программы, перехватывать вводимую на клавиатуре информацию и выполнять другие вредоносные действия.

Также в минувшем году компания «Доктор Веб» проанализировала популярные в России модели детских смарт-часов на предмет возможных уязвимостей в них. Как показало исследование, безопасность подобных устройств находится на неудовлетворительном уровне. Например, на одной из моделей были предустановленные троянские приложения.

Перспективы и вероятные тенденции

В первую очередь, прошедший год показал, насколько оперативно злоумышленники подстраиваются под ту или иную актуальную тематику. Следует ожидать ещё более хитрых мошеннических схем, связанных с ковидом или другими важными темами грядущего года.

Помимо этого, останутся активными рекламные трояны, всевозможные шифровальщики и другое вредоносное ПО. Корпорациям и компаниям в новом году следует уделять повышенное внимание информационной защите. Как показывает практика, пренебрежение правилами цифровой безопасности многократно увеличивает риски компрометации корпоративной сети. 2021 год запомнился большим количеством «громких» инцидентов с трояна-вымогателями, распространяющимся по модели Ransomware as a Service (RaaS). И эта тенденция продолжит набирать обороты.

Также стоит быть внимательными пользователям устройств, управляемых ОС Android. Ожидается увеличение количества угроз в официальных каталогах приложений.

«Доктор Веб»: обзор вирусной активности за 2021 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
Центр противодействия кибер-мошенничеству

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

Контакты
Центральный офис
125124 Россия, Москва, 3-я Ямского поля улица, д.2, к.12а
www.антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах