Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности за 2018 год

28 декабря 2018 года

Уходящий год был отмечен широким распространением троянцев-майнеров, предназначенных для добычи криптовалют без ведома пользователей. Подобные вредоносные программы угрожали не только пользователям Microsoft Windows, но также владельцам различных устройств, работающих под управлением ОС семейства Linux. Не утратили своих позиций и энкодеры, шифрующие файлы на зараженных компьютерах и требующие выкуп за их расшифровку: в феврале и апреле специалисты «Доктор Веб» выявили двух новых представителей этого семейства, один из которых, несмотря на заверения вирусописателей, был неспособен восстановить поврежденные файлы даже в случае уплаты жертвой вознаграждения.

В конце марта 2018 года был исследован троянец Trojan.PWS.Stealer.23012, распространявшийся на сайте YouTube. Он был написан на языке Python и предназначен для хищения с зараженного устройства файлов и другой конфиденциальной информации. Проведенное аналитиками «Доктор Веб» расследование позволило выявить создателя этой вредоносной программы и нескольких ее модификаций. Благодаря еще одному расследованию был установлен злоумышленник, похищавший личную информацию у пользователей игровой платформы Steam при помощи специально созданного для этих целей троянца Trojan.PWS.Steam.13604. Деятельность другого сетевого преступника, промышлявшего в сфере криптовалют и заработавшего на обмане интернет-пользователей десятки тысяч долларов, специалисты «Доктор Веб» детально изучили в октябре.

В течение всего года проявляли активность кибермошенники, завлекавшие своих жертв на поддельные сайты и досаждавшие им массовыми почтовыми рассылками. Если в начале года сетевые жулики отправляли почтовые сообщения от имени компании Mail.Ru Group, пытаясь завладеть логинами и паролями пользователей почтового сервиса, то весной они активно рассылали письма с предложениями получить несуществующие денежные компенсации. Летом спамеры тревожили администраторов доменов, представляясь сотрудниками компании-регистратора «Региональный Сетевой Информационный Центр» (RU-CENTER). Их целью было получить деньги за продление регистрации доменных имен, принадлежащих потенциальным жертвам.

В 2018 году вирусописатели не обошли своим вниманием и пользователей мобильных устройств, работающих под управлением Google Android. Еще в январе специалисты по информационной безопасности обнаружили в каталоге Google Play зараженные игры,

которые в совокупности были скачаны более 4 500 000 раз. Чуть позже был выявлен Android-майнер, способный заразить 8% различных «умных» устройств, таких как телевизоры, телеприставки, роутеры и иные приспособления, относящиеся к миру «Интернета вещей».

В течение всего года вирусные аналитики предупреждали пользователей о распространении банковских троянцев для ОС Android, обладающих широчайшим диапазоном функциональных возможностей. Кроме того, был обнаружен целый ряд подделок под популярные Android-приложения, которые злоумышленники использовали в целях фишинга. Некоторые мобильные троянцы подписывали своих жертв на различные платные услуги, другие зарабатывали с помощью «невидимой» рекламы, третьи загружали на зараженное устройство другое вредоносное ПО.

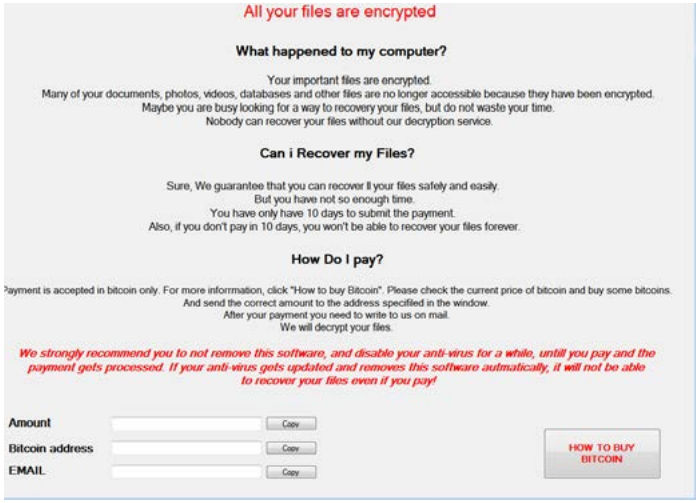
Главные тенденции года

- Распространение троянцев-майнеров, предназначенных для тайной добычи криптовалют с использованием аппаратных ресурсов зараженного компьютера
- Появление новых вредоносных программ для ОС Linux и «Интернета вещей»
- Рост числа троянцев для мобильной платформы Google Android

Наиболее интересные события 2018 года

В феврале 2018 года был обнаружен новый троянец-шифровальщик, добавленный в вирусные базы Dr.Web под именем Trojan.Encoder.24384. Эта вредоносная программа собирает информацию о запущенных на зараженном устройстве антивирусах и умеет завершать работающие приложения по заранее составленному вирусописателями списку. Троянец шифрует файлы на фиксированных, съемных и сетевых дисках, за исключением ряда служебных и системных папок.

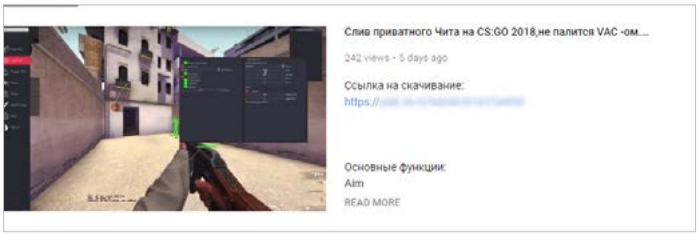
Другой энкодер, получивший известность под именем Trojan.Encoder.25129, при запуске пытался определить географическое положение жертвы по IP-адресу сетевого интерфейса ее устройства. Вирусописатели предусмотрели отмену шифрования для IP-адресов из России, Беларуси или Казахстана (а также если в настройках операционной системы установлены русский язык и российские региональные параметры), однако из-за допущенной в коде троянца ошибки это условие не соблюдалось и шифрование выполнялось в любом случае. После завершения своей вредоносной деятельности троянец показывал на экране требование выкупа.



К сожалению, упомянутая выше ошибка была не единственной в коде этого энкодера: благодаря еще одной оплошности вирусописателей расшифровать поврежденные троянцем файлы оказались не в состоянии даже его авторы. Этот факт еще раз подтверждает важность своевременного резервного копирования всех актуальных для пользователей файлов.

Наиболее интересные события 2018 года

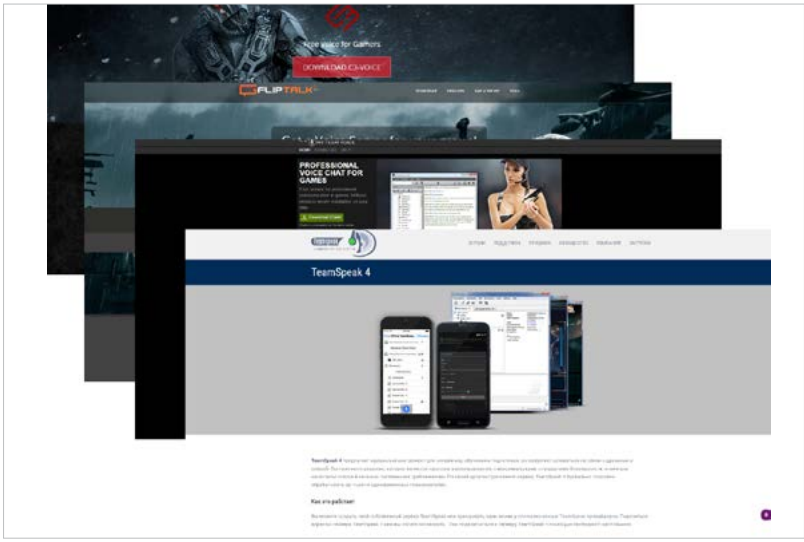
В конце марта аналитики «Доктор Веб» исследовали троянца-шпиона Trojan.PWS.Stealer.23012, написанного на Python и предназначенного для хищения конфиденциальных данных. Вредоносная программа, как и несколько ее модификаций, распространялась через сайт популярного видеохостинга YouTube с помощью ссылок в описаниях видеороликов. Ролики были посвящены использованию жульнических методов прохождения игр (так называемым «читам») с применением специальных приложений и активно рекламировались в Twitter.



Спустя месяц с небольшим наши специалисты смогли вычислить и автора этих троянцев. Вредоносная программа и ее модификации воровали сохраненные пароли и файлы cookies браузеров, основанных на Chromium, информацию из мессенджера Telegram, FTP-клиента FileZilla, изображения и офисные документы по заранее заданному списку. Одна из модификаций троянца активно рекламировалась на различных Telegram-каналах. Благодаря тому, что логины и пароли от облачных хранилищ, в которые загружались архивы с украденными файлами, были «зашиты» в тело самих троянцев, вирусные аналитики «Доктор Веб» вычислили и автора этих вредоносных программ, и всех его клиентов. Этому расследованию была посвящена опубликованная на нашем сайте статья.

Другое расследование наших аналитиков, результаты которого были обнародованы в конце мая, посвящено автору троянцев-шпионов, похищавших личные данные у пользователей игровой платформы Steam. Этот злоумышленник использовал сразу несколько способов криминального заработка: мошеннические «рулетки» (своеобразные аукционы, на которые пользователи могут выставить различные игровые предметы), где всегда выигрывают созданные мошенником программы-боты, и аренда вредоносных программ для всех желающих. Для распространения троянцев киберпреступник использовал методы социальной инженерии и поддельные сайты.

Наиболее интересные события 2018 года



О принципах работы троянцев-шпионов Trojan.PWS.Steam.13604 и Trojan.PWS.Steam.15278, а также об их создателе мы подробно рассказали в своей статье.

Летом аналитики «Доктор Веб» предупредили пользователей о появлении трояна-майнера Trojan.BtcMine.2869, который для своего распространения применял те же методы, что и нашумевший шифровальщик Trojan.Encoder.12544, известный под наименованиями Petya, Petya.A, ExPetya и WannaCry-2. Троянец проникал на компьютеры своих жертв с помощью механизма обновления программы «Компьютерный зал» для автоматизации компьютерных клубов и интернет-кафе. В период с 24 мая по 4 июля 2018 года майнер успел заразить более 2700 компьютеров.

В сентябре специалисты компании «Доктор Веб» обнаружили банковского троянца Trojan.PWS.Banker1.28321, распространявшегося под видом приложения Adobe Reader и угрожавшего клиентам бразильских кредитных организаций.

Наиболее интересные события 2018 года

При попытке открыть в браузере страницу интернет-банка ряда бразильских финансовых организаций троянец незаметно подменял ее, показывая жертве поддельную форму для ввода логина и пароля. В некоторых случаях он просил указать проверочный код авторизации из полученного от банка СМС-сообщения. Эту информацию троянец передавал злоумышленникам. Вирусные аналитики выявили более 340 уникальных образцов Trojan.PWS.Banker1.28321, а также обнаружили 129 доменов и IP-адресов принадлежащих злоумышленникам интернет-ресурсов. Более подробно об этой вредоносной программе мы рассказали в опубликованной на нашем сайте обзорной статье.

Еще одно проведенное нашими аналитиками расследование, завершившееся в середине октября, было посвящено деятельности киберпреступника, промышлявшего на рынке криптовалют. Злоумышленник использовал целый арсенал вредоносных программ, таких как стилеры Eredel, AZORult, Kpot, Kratos, N0F1L3, ACRUX, Predator The Thief, Arkei, Pony и многие другие. Для реализации своих замыслов он создал множество фишинговых сайтов, копирующих реально существующие интернет-ресурсы. Среди них — поддельная криптовалютная биржа, пул устройств для майнинга криптовалюты Dogecoin, который якобы сдается в аренду по очень выгодным ценам, и партнерская программа, предлагавшая вознаграждение за просмотр сайтов в Интернете.

Наиболее интересные события 2018 года

Еще один проект того же автора — онлайн-лотереи, призом в которых служит определенная сумма в криптовалюте Dogecoin. Лотереи устроены таким образом, что выиграть в них стороннему участнику невозможно, заработать на этом может только сам организатор розыгрыша. Среди других начинаний сетевого мошенника — партнерская программа, предлагающая выплату вознаграждения в Dogecoin за просмотр веб-страниц с рекламой (под видом необходимого для такой работы плагина с сайта киберпреступника загружается троянец), и традиционный фишинг. Более подробно обо всех этих видах мошенничества мы рассказали читателям в нашей публикации.

В ноябре была обнаружена вредоносная программа Trojan.Click3.27430, накручивавшая посещаемость веб-сайтов. Троянец маскировался под программу DynDNS, которая позволяет привязать субдомен к компьютеру, не имеющему статического IP-адреса.

Согласно информации, которую удалось собрать аналитикам «Доктор Веб», на сегодняшний день от этого троянца пострадали порядка 1400 пользователей, при этом первые случаи заражения датируются 2013 годом. Более полные сведения об этом инциденте изложены в размещенном на нашем сайте новостном материале.

Вирусная обстановка

По данным серверов статистики «Доктор Веб» в 2018 году на компьютерах чаще всего обнаруживались написанные на JavaScript вредоносные сценарии, предназначенные для встраивания постороннего содержимого в веб-страницы и добычи криптовалют, а также троянцы-шпионы и вредоносные загрузчики.

JS.Inject

Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.

JS.BtcMine

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

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.

JS.DownLoader

Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.

Вирусная обстановка

Trojan.Starter.7394

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

Trojan.Encoder.567

Представитель семейства троянцев-вымогателей, шифрующих файлы на компьютере и требующих от жертвы выкуп за расшифровку.

JS.Miner

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

VBS.BtcMine

Семейство сценариев на языке VBS, предназначенных для скрытой добычи (майнинга) криптовалют.

В анализе почтового трафика наблюдается схожая картина, однако во вложениях в сообщения электронной почты намного чаще встречаются троянцы-шпионы:

JS.DownLoader

Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.

Вирусная обстановка

JS.Inject

Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.

JS.BtcMine

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

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.

Trojan.Encoder.567

Один из представителей семейства троянцев-вымогателей, шифрующих файлы на компьютере и требующих от жертвы выкуп за расшифровку.

Trojan.DownLoader

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

Trojan.PWS.Stealer

Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.

JS.Miner

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

Троянцы-шифровальщики

По сравнению с предыдущим годом, в 2018-м число обращений в службу технической поддержки компании «Доктор Веб» от пользователей, файлы которых оказались зашифрованы троянцами-энкодерами, снизилось. Незначительный всплеск количества пострадавших от шифровальщиков отмечался в период с мая по август, минимальное количество обращений было зафиксировано в январе, максимальное — в ноябре.

Согласно статистике, чаще всего на устройства проникал энкодер Trojan.Encoder.858, вторым по количеству заражений стал Trojan.Encoder.11464, третье место занимает Trojan.Encoder.567.

Наиболее распространенные шифровальщики в 2018 году:

- Trojan.Encoder.858 — 19,83% обращений;
- Trojan.Encoder.11464 — 9,64% обращений;
- Trojan.Encoder.567 — 5,08% обращений;
- Trojan.Encoder.11539 — 4,79% обращений;
- Trojan.Encoder.25574 — 4,46% обращений.

Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

Настрой-ка Dr.Web от шифровальщиков

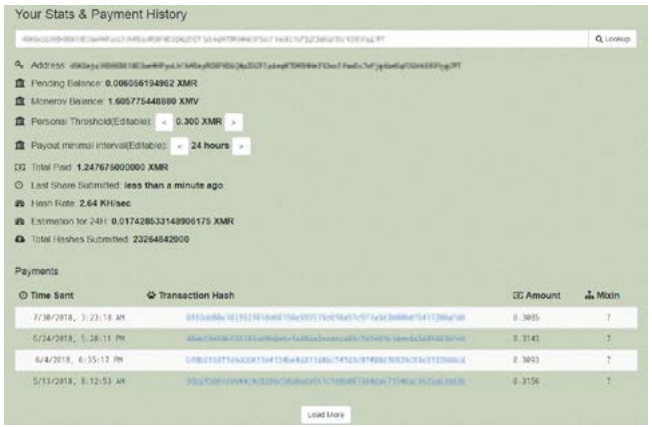
Обучающий курс

О бесплатном восстановлении

Dr.Web Rescue Pack

Вредоносные программы для Linux

Среди вредоносных программ для операционных систем семейства Linux в 2018 году чаще всего проявляли себя майнеры, предназначенные для добычи криптовалют. Первые подобные атаки на работающие под управлением Linux серверы были зафиксированы вирусными аналитиками «Доктор Веб» в начале мая 2018 года. Киберпреступники соединялись с сервером по протоколу SSH, подбирали логин и пароль методом их перебора по словарю (bruteforce) и после успешной авторизации на сервере отключали утилиту iptables, управляющую работой межсетевого экрана. Затем злоумышленники загружали на атакованный сервер утилиту-майнер и файл конфигурации для нее. Чуть позже они начали использовать для этих целей вредоносные программы. Так, в августе вирусные аналитики обнаружили троянца Linux.BtcMine.82, написанного на языке Go. Он представлял собой дроппер, который устанавливал на зараженное устройство содержащийся в нем майнер.



Исследовав сервер, с которого загружалась эта вредоносная программа, наши специалисты обнаружили там аналогичных по своим функциям троянцев для Microsoft Windows. Более подробную информацию об этом инциденте можно получить, ознакомившись с опубликованной на нашем сайте статьей.

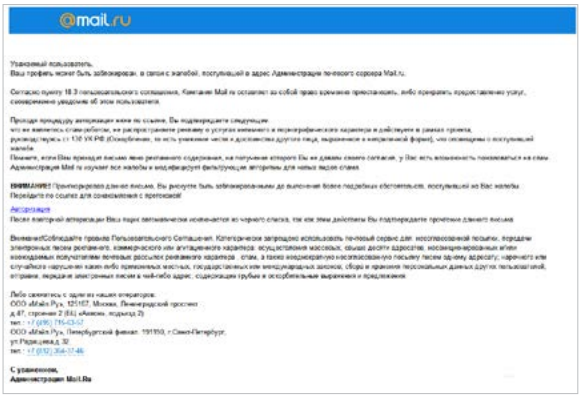
В ноябре был выявлен еще один Linux-майнер, получивший наименование Linux.BtcMine.174. Он представляет собой большой сценарий, написанный на языке командной оболочки sh и содержащий более 1000 строк кода. Этот троянец состоит из нескольких модулей и умеет отключать работающие на зараженном устройстве антивирусные программы, а также заражать другие устройства в сети. Кроме того, он скачивает и устанавливает на инфицированной машине одну из версий троянца Linux.BackDoor.Gates.9, предназначенного для выполнения поступающих от злоумышленников команд и осуществления DDoS-атак. Об этой вредоносной программе мы также рассказывали в соответствующей новостной публикации.

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. Динамика пополнения этих баз в уходящем году показана на представленной ниже диаграмме.

Сетевое мошенничество

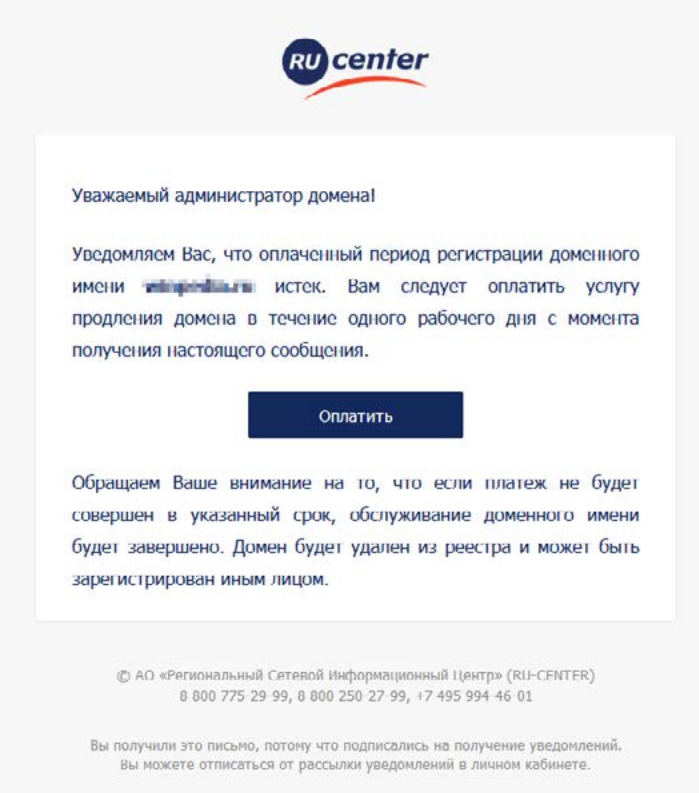
Мошенничество в Интернете — весьма распространенный вид криминального бизнеса, и в 2018 году сетевые жулики отнюдь не ушли на заслуженный отдых. Еще в самом начале марта была зафиксирована массовая рассылка фишинговых писем якобы от имени компании Mail.Ru Group. Целью злоумышленников было получение учетных данных пользователей почтового сервера Mail.Ru, для чего киберпреступники использовали поддельный веб-сайт, повторяющий своим оформлением эту популярную почтовую службу.



В мае мы рассказали нашим читателям об очередной схеме сетевого мошенничества, в которой жулики использовали обещания щедрых социальных выплат. При помощи спама и массовых СМС-рассылок жертв завлекали на специально созданные сайты, на которых сообщалось о якобы существующей возможности получить компенсацию за переплату предоставляемых населению коммунальных, медицинских услуг или услуг обязательного страхования. Для получения выплаты мошенники требовали перевести на их счет небольшую сумму. Разумеется, никаких денежных компенсаций обманутым пользователям после такой оплаты не предоставлялось.

Сетевое мошенничество

Специал исты компании «Доктор Веб» выявили более 110 подобных сайтов, созданных сетевыми мошенниками в период с февраля по май 2018 года. А в августе злоумышленники стали рассылать письма администратором доменов, зарегистрированных в компании «Региональный Сетевой Информационный Центр» (RU-CENTER). Жулики предлагали оплатить продление доменов, срок делегирования которых подходил к концу, при этом вместо официальных реквизитов RU-CENTER они предлагали сделать перевод на собственный кошелек в электронной платежной системе «Яндекс.Деньги».


RU center

Уважаемый администратор домена!

Уведомляем Вас, что оплаченный период регистрации доменного имени [redacted] истек. Вам следует оплатить услугу продления домена в течение одного рабочего дня с момента получения настоящего сообщения.

Оплатить

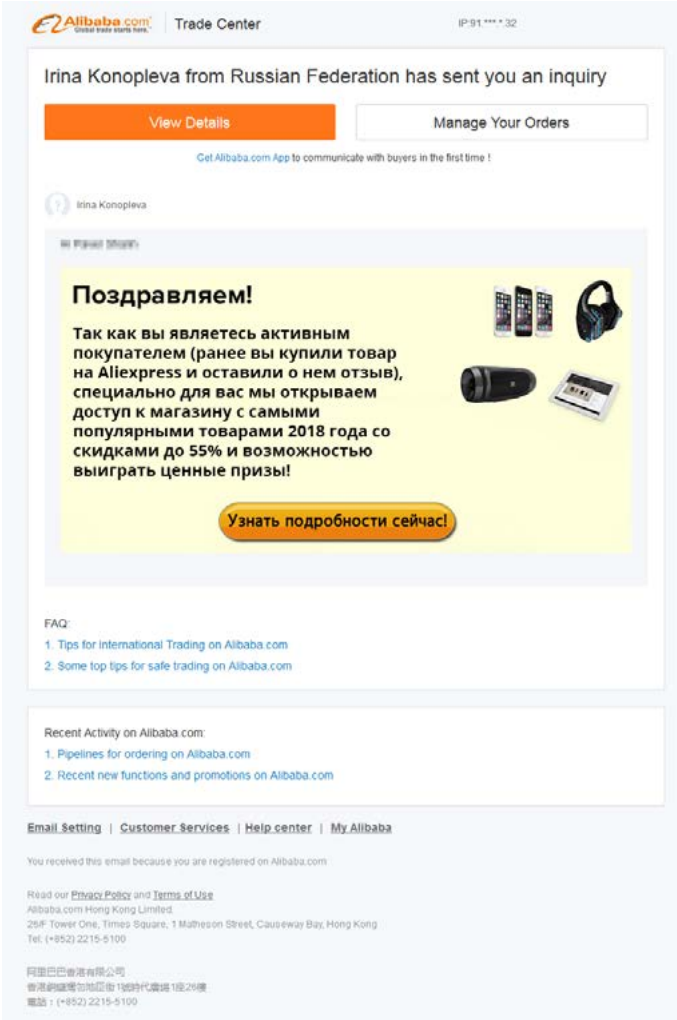
Обращаем Ваше внимание на то, что если платеж не будет совершен в указанный срок, обслуживание доменного имени будет завершено. Домен будет удален из реестра и может быть зарегистрирован иным лицом.

© АО «Региональный Сетевой Информационный Центр» (RU-CENTER)
8 800 775 29 99, 8 800 250 27 99, +7 495 994 46 01

Вы получили это письмо, потому что подписались на получение уведомлений.
Вы можете отписаться от рассылки уведомлений в личном кабинете.

Мошенники часто рассылают электронные письма от имени известных компаний — не минула эта участь и популярный интернет-магазин Aliexpress. Жулики отправляли его постоянным покупателям сообщения с предложением посетить специальный интернет-магазин с многочисленными скидками и подарками.

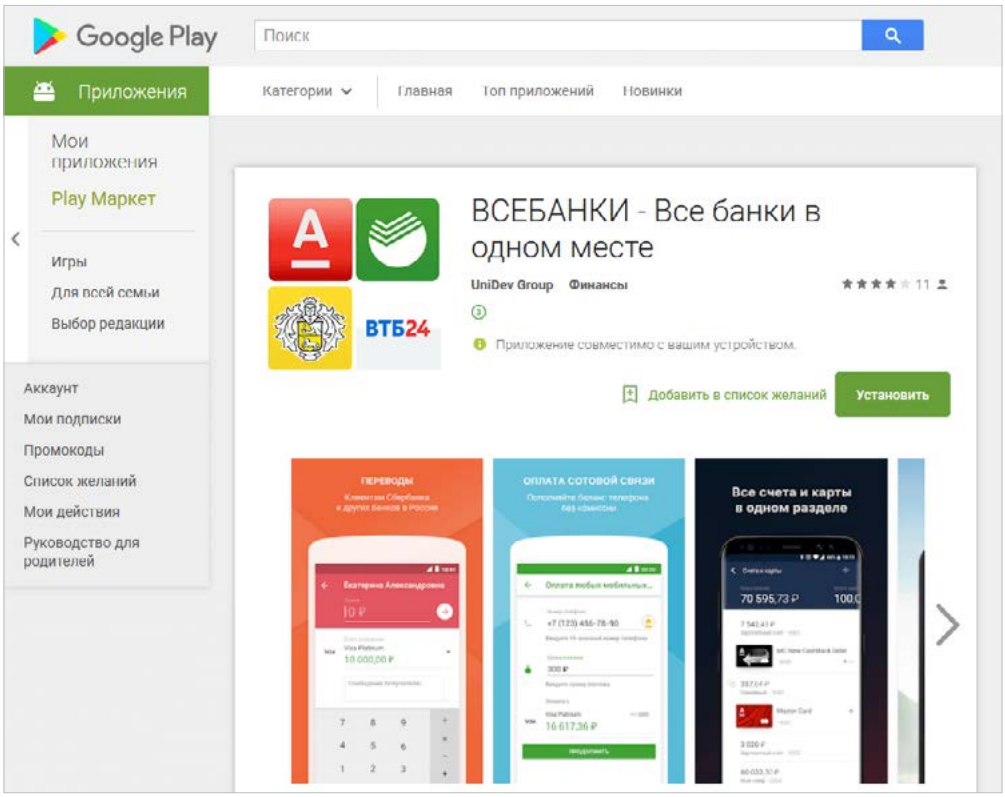
Сетевое мошенничество



В действительности «магазин» представлял собой страницу со ссылками на различные мошеннические торговые площадки, продававшие некачественные товары или товары по завышенным ценам. Вопрос о том, как злоумышленникам удалось раздобыть базу с контактами реальных покупателей Aliexpress, до сих пор остается открытым.

Для мобильных устройств

В уходящем году пользователям Android-устройств угрожало множество вредоносных программ. Среди них были банковские троянцы, с помощью которых злоумышленники пытались украсть деньги жителей России, Турции, Бразилии, Испании, Германии, Франции и других государств. Весной вирусные аналитики обнаружили троянца Android.BankBot.344.origin — он распространялся под видом универсального банковского приложения и атаковал клиентов российских кредитных организаций. Android.BankBot.344.origin запрашивал у потенциальной жертвы логин и пароль от личного кабинета в системе онлайн-банкинга, а также номер банковской карты, и передавал полученные данные злоумышленникам.



В ноябре специалисты «Доктор Веб» исследовали вредоносную программу Android.Banker.2876, предназначенную для европейских пользователей Android-устройств. Она перехватывала СМС, крала информацию о номере телефона и другие конфиденциальные сведения.

Для мобильных устройств

А уже в декабре был выявлен троянец Android.BankBot.495.origin, атаковавший бразильских пользователей. Он пытался получить доступ к специальным возможностям (Accessibility Service) ОС Android, с использованием которых считывал содержимое окон банковских приложений и самостоятельно управлял ими, нажимая на кнопки меню. Также Android.BankBot.495.origin показывал мошеннические формы поверх атакуемых программ и предлагал жертве ввести аутентификационные данные.

На протяжении всего года вирусописатели активно распространяли Android-банкеров, созданных на основе опубликованного в открытом доступе исходного кода трояна Android.BankBot.149.origin. Среди них были вредоносные программы Android.BankBot.250.origin и Android.BankBot.325.origin, не только способные красть конфиденциальную информацию, но и позволявшие злоумышленникам получать дистанционный доступ к зараженным устройствам.

Многие банкеры попадали на устройства благодаря троянцам-загрузчикам, таким как Android.DownLoader.753.origin, Android.DownLoader.768.origin и Android.DownLoader.772.origin. Киберпреступники выдавали их за полезные программы, которые на самом деле скачивали и пытались установить банковских троянцев. Подобные загрузчики использовались для распространения других вредоносных приложений – например, троянцев-шпионов Android.Spy.409.origin и Android.Spy.443.origin, а также рекламных троянцев Android.HiddenAds.710 и Android.HiddenAds.728, о которых компания «Доктор Веб» сообщала в августе.

В 2018 году владельцам Android-устройств снова угрожали троянцы семейства Android.RemoteCode, способные скачивать из Интернета и запускать произвольный код. Одного из них, получившего имя Android.RemoteCode.127.origin, вирусные аналитики обнаружили в феврале. Android.RemoteCode.127.origin загружал вспомогательные модули, которые также скачивали и запускали другие вредоносные плагины, способные выполнять различные действия. Чтобы снизить вероятность обнаружения компонентов этого трояна, злоумышленники зашифровали их и скрыли в изображениях.

Для мобильных устройств

Другой троянец этого семейства, добавленный в вирусную базу Dr.Web как Android.RemoteCode.152.origin, загружал и запускал рекламные модули. Они создавали невидимые баннеры, на которые и нажимал Android.RemoteCode.152.origin, принося киберпреступникам доход.

Для получения незаконного заработка сетевые мошенники применяли и другие вредоносные программы. Среди них были троянцы-майнеры, такие как Android.CoinMine.15. Он заражал различные устройства под управлением ОС Android — роутеры, телеприставки, медиаплееры, «умные» телевизоры и т. п. Android.CoinMine.15 распространялся как сетевой червь, проникая на оборудование с открытым портом 5555, который используется отладчиком ADB (Android Device Bridge).

Осенью специалисты «Доктор Веб» обнаружили троянца-клипера Android.Clipper.1.origin, подменявшего в буфере обмена номера электронных кошельков популярных платежных систем «Яндекс.Деньги», Qiwi и Webmoney (R и Z), а также криптовалют Bitcoin, Litecoin, Etherium, Monero, zCash, DOGE, DASH и Blackcoin. При копировании номера одного из них в буфер обмена Android.Clipper.1.origin заменял его на номер вирусописателей, из-за чего невнимательные пользователи рисковали перевести деньги злоумышленникам.

Вирусописатели активно применяли троянцев и в мошеннических кампаниях. Популярной схемой сетевых жуликов в 2018 году было обещание вознаграждения за прохождение опросов. При запуске такие троянцы показывали на экране созданные злоумышленниками веб-страницы, где потенциальным жертвам предлагалось ответить на несколько вопросов. Для получения денег от пользователей требовалась некая проверочная или иная оплата, однако после отправки средств владельцы зараженных устройств не получали ничего. Также популярностью пользовались вредоносные программы-кликеры, которые загружали сайты с рекламой и автоматически нажимали на расположенные на них объявления. Более детально об этих случаях наша компания рассказывала в соответствующей статье.

Другой тип мошенничества заключался в подписке владельцев Android-смартфонов и планшетов на дорогостоящие услуги. Троянцы, такие как Android.Click.245.origin, загружали веб-сайты, на которых жертвам предлагалось скачать различное ПО. Для этого у них запрашивались номера телефонов, на которые приходили коды подтверждения. Однако в некоторых случаях подписка происходила и вовсе автоматически. Этот тип мошенничества освещался в нашем новостном материале.

Для мобильных устройств

В уходящем году были выявлены очередные случаи заражения Android-прошивок. Об одном из них мы сообщали в марте. Вирусные аналитики обнаружили троянца Android.Triada.231 в прошивках более 40 моделей мобильных устройств. Злоумышленники встроили эту вредоносную программу в одну из системных библиотек на уровне исходного кода. Android.Triada.231 начинал работу автоматически при каждом включении зараженных смартфонов и планшетов. При старте он внедрялся в системный процесс Zygote, ответственный за запуск остальных процессов, в результате чего проникал во все из них и мог выполнять вредоносные действия без участия пользователя. Основная функция Android.Triada.231 — незаметное скачивание, установка и удаление программ.

Перспективы и вероятные тенденции

Несмотря на то, в что в 2018 году не случилось серьезных вирусных эпидемий, в будущем вполне возможны новые волны массового распространения различных угроз. По-прежнему будет расти число вредоносных сценариев, написанных на различных интерпретируемых языках. При этом подобные скрипты будут угрожать не только устройствам под управлением Microsoft Windows, но и другим платформам, прежде всего — Linux.

Будут появляться новые троянцы-майнеры, предназначенные для добычи криптовалют с использованием аппаратных ресурсов инфицированных устройств. Не ослабнет интерес злоумышленников и к «Интернету вещей»: троянцы для «умных устройств» существуют уже сейчас, но в недалеком будущем их количество наверняка вырастет.

Имеются все основания полагать, что в 2019 году вирусописатели будут создавать и распространять новых троянцев для мобильной платформы Google Android. Тенденции уходящего года показывают, что среди мобильных вредоносных программ скорее всего будут преобладать рекламные и банковские троянцы.

Также вряд ли снизится число мошеннических почтовых рассылок: сетевые жулики будут изобретать все новые и новые способы обмана интернет-пользователей. Как бы то ни было, в наступающем году определенно появятся новые угрозы информационной безопасности, а значит, очень важно обеспечить своим устройствам надежную и современную антивирусную защиту.

«Доктор Веб»: обзор вирусной активности за 2018 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