Dr.WEB®
с 1992 года

Обзор вирусной активности в январе 2018 года

Обзор вирусной активности в январе 2018 года

31 января 2018 года

Начало 2018 года ознаменовалось обнаружением в каталоге Google Play нескольких игр для ОС Android со встроенным троянцем, скачивавшим и запускавшим на инфицированных устройствах вредоносные модули. Также вирусные аналитики исследовали несколько троянцев-майнеров, заражавших серверы под управлением Windows. Все они использовали уязвимость в программном обеспечении Cleverence Mobile SMARTS Server.

Главные тенденции января

- Появление в каталоге Google Play опасного троянца для Android
- Распространение новых версий троянцев-майнеров, заражающих Windows-серверы

Угроза месяца

Cleverence Mobile SMARTS Server — это комплекс приложений для автоматизации магазинов, складов, различных учреждений и производств. Уязвимость нулевого дня в этих программах аналитики «Доктор Веб» обнаружили еще в июле 2017 года и сообщили о ней разработчикам ПО. Вскоре те выпустили обновление безопасности для своего программного продукта. Однако далеко не все администраторы установили это обновление, что позволило злоумышленникам продолжить взломы уязвимых серверов. Для этого киберпреступники отправляют на уязвимый сервер специальный запрос, в результате чего происходит выполнение содержащейся в нем команды. Затем взломщики создают в системе нового пользователя с административными привилегиями и получают от его имени несанкционированный доступ к серверу по протоколу RDP. В некоторых случаях с помощью утилиты Process Hacker киберпреступники завершают процессы работающих на сервере антивирусов. Получив доступ к системе, они устанавливают в ней троянца-майнера.

Используемый взломщиками майнер непрерывно совершенствуется. Изначально они устанавливали несколько модификаций троянца, добавленных в вирусную базу Dr.Web под именами Trojan.BtcMine.1324, Trojan.BtcMine.1369 и Trojan.BtcMine.1404. Позже этот список пополнили Trojan.BtcMine.2024, Trojan.BtcMine.2025, Trojan.BtcMine.2033, а самой актуальной версией майнера на текущий момент является Trojan.BtcMine.1978.

Этот троянец запускается в качестве критически важного системного процесса, при попытке завершить который Windows аварийно прекращает работу и демонстрирует «синий экран смерти» (BSOD). После старта майнер пытается остановить процессы и удались службы нескольких антивирусов. Киберпреступники используют Trojan.BtcMine.1978 для добычи криптовалют Monero (XMR) и Aeon. Специалисты компании «Доктор Веб» рекомендуют установить все выпущенные разработчиками обновления безопасности Cleverence Mobile SMARTS Server, а более подробную информацию об этом инциденте можно найти в опубликованной на нашем сайте обзорной статье.

Обзор вирусной активности в январе 2018 года

По данным статистики Антивируса Dr.Web

Trojan.Moneyinst.520

Вредоносная программа, устанавливающая на компьютер жертвы различное ПО, в том числе других троянцев.

Trojan.Starter.7394

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

Trojan.BPlug

Это надстройки (плагины) для популярных браузеров, демонстрирующие назойливую рекламу при просмотре веб-страниц.

Trojan.DownLoad

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

Trojan.Zadved

Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.

Обзор вирусной активности в январе 2018 года

По данным серверов статистики «Доктор Веб»

JS.BtcMine.7, JS.BtcMine.2

Сценарий на языке JavaScript, предназначенный для скрытой добычи (майнинга) криптовалют.

JS.Inject

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

JS.DownLoader

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

Trojan.PWS.Stealer

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

Статистика вредоносных программ в почтовом трафике

JS.BtcMine.7

Сценарий на языке JavaScript, предназначенный для скрытой добычи (майнинга) криптовалют.

JS.Inject

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

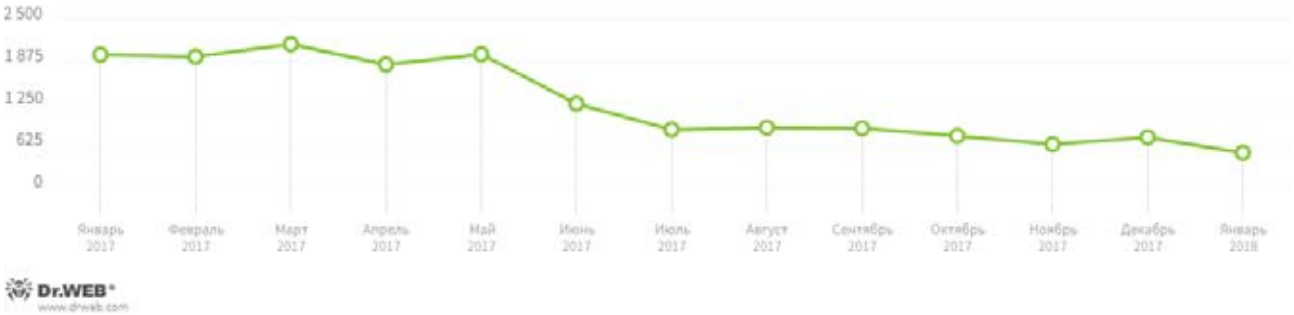
Trojan.Encoder.24348

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

Trojan.PWS.Stealer

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

Шифровальщики



В январе в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих модификаций троянцев-шифровальщиков:

- Trojan.Encoder.858 — 22,12% обращений;
- Trojan.Encoder.567 — 7,83% обращений;
- Trojan.Encoder.11539 — 6,45% обращений;
- Trojan.Encoder.2267 — 3,46% обращений;
- Trojan.Encoder.761 — 3,23% обращений;
- Trojan.Encoder.3953 — 3,20% 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

Опасные сайты

В течение января 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 309 933 интернет-адреса.

Декабрь 2017	Январь 2018	Динамика
+ 241 274	+ 309 933	+28.4%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В январе вирусные аналитики компании «Доктор Веб» обнаружили троянца Android.RemoteCode.127.origin, встроенного во множество доступных в каталоге Google Play Android-игр. Он незаметно загружал и запускал вредоносные модули, которые могли выполнять разнообразные действия. Помимо этого, в уходящем месяце пользователям угрожал банковский троянец Android.BankBot.250.origin, который крал логины и пароли для доступа к учетным записям онлайн-банкинга. Кроме того, в январе специалисты по информационной безопасности выявили вредоносную программу-майнер, получившую имя Android.CoinMine.8. Этот троянец использовал мощности зараженных смартфонов и планшетов для добычи криптовалюты Monero. В этом же месяце в вирусную базу Dr.Web было добавлено несколько записей для детектирования Android-шпионов, которых злоумышленники использовали для слежки. Одним из них был Android.Spy.422.origin. Другие вредоносные приложения являлись новыми модификациями троянца Android.Spy.410.origin, распространявшегося еще в декабре 2017 года.

Наиболее заметные события, связанные с «мобильной» безопасностью в январе:

- обнаружение в Google Play нового троянца;
- распространение нового Android-майнера, использовавшего зараженные мобильные устройства для добычи криптовалюты;
- выявление новых троянцев-шпионов.

Более подробно о вирусной обстановке для мобильных устройств в январе читайте в нашем обзоре.

Обзор вирусной активности в январе 2018 года

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 | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах