Dr.WEB®
с 1992 года

Обзор вирусной активности в марте 2018 года

Обзор вирусной активности в марте 2018 года

3 апреля 2018 года

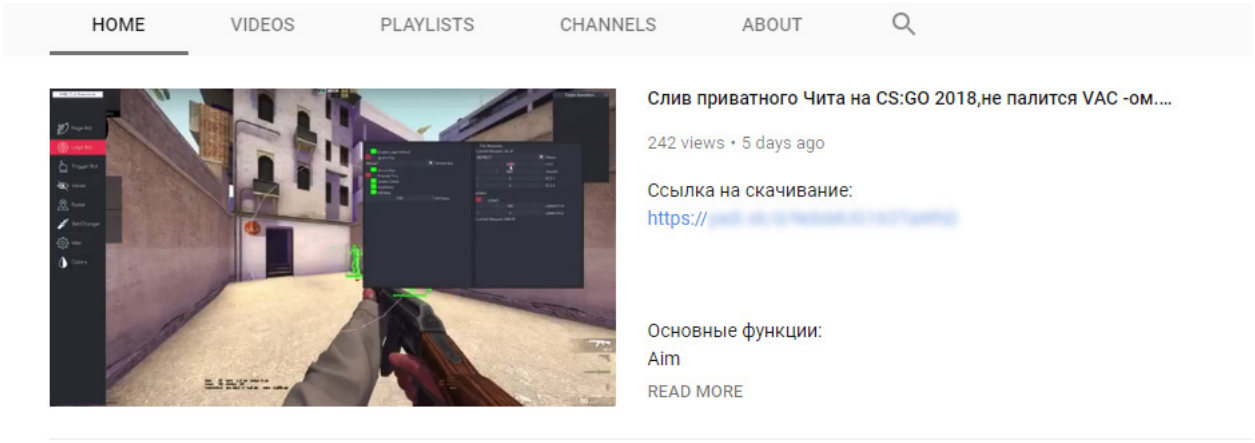
В минувшем марте специалисты «Доктор Веб» выявили и исследовали множество новых вредоносных программ. В начале месяца была зафиксирована массовая фишинговая рассылка якобы от имени компании Mail.Ru. Также аналитики изучили несколько новых троянцев, относящихся к обширному семейству вредоносных программ Trojan.LoadMoney. Во второй половине месяца был обнаружен опасный троянец Trojan.PWS.Stealer.23012, похищающий с зараженного устройства файлы и другую конфиденциальную информацию. Наконец, в марте вирусные аналитики выявили целый ряд вредоносных программ для мобильной платформы Google Android.

Главные тенденции марта

- Массовая рассылка фишинговых сообщений по электронной почте
- Распространение новых представителей семейства Trojan.LoadMoney
- Появление опасного троянца, похищающего конфиденциальную информацию

Угроза месяца

Распространение вредоносной программы Trojan.PWS.Stealer.23012 началось 11 марта 2018 года. Ссылки на троянца вирусописатели размещали в комментариях к видео на популярном интернет-ресурсе YouTube. Многие из таких роликов посвящены использованию жульнических методов прохождения игр (так называемым «читам») с применением специальных приложений. Киберпреступники пытаются выдать троянца за такие программы и другие полезные утилиты.



Троянец собирает на инфицированном компьютере файлы Cookies, а также сохраненные логины и пароли из нескольких популярных браузеров, делает снимок экрана и копирует файлы с Рабочего стола Windows. Похищенная информация вместе с данными о расположении зараженного устройства отправляется на сервер злоумышленников. Более подробно о принципах работы Trojan.PWS.Stealer.23012 рассказано в опубликованной на нашем сайте статье.

Обзор вирусной активности в марте 2018 года

По данным статистики Антивируса Dr.Web

Trojan.Starter.7394

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

Trojan.Inject

Семейство вредоносных программ, встраивающих вредоносный код в процессы других программ.

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.

Trojan.Moneyinst.520

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

Trojan.Encoder.11432

Сетевой червь, запускающий на компьютере жертвы опасного троянца-шифровальщика. Известен также под именем WannaCry.

Обзор вирусной активности в марте 2018 года

По данным серверов статистики «Доктор Веб»

BackDoor.Meterpreter.56

Представитель семейства вредоносных программ, позволяющих злоумышленникам удаленно управлять зараженным компьютером и отдавать ему различные команды.

JS.Inject

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

BackDoor.IRC.Bot.4771

Представитель семейства вредоносных программ, позволяющих злоумышленникам удаленно управлять зараженным компьютером и отдавать ему различные команды. Управление этим троянцем осуществляется с использованием протокола обмена текстовыми сообщениями IRC (Internet Relay Chat).

Trojan.Encoder.11432

Сетевой червь, запускающий на компьютере жертвы опасного троянца-шифровальщика. Известен также под именем WannaCry.

JS.DownLoader

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

Статистика вредоносных программ в почтовом трафике

JS.Inject

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

Trojan.Encoder.24788

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

Java.Jrat.58

Вредоносная программа для удаленного управления компьютером (Remote Access Tools, RAT), написанная на языке Java.

Trojan.PWS.Stealer

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

Шифровальщики

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

- Trojan.Encoder.858 — 15.38% обращений;
- Trojan.Encoder.11464 — 7.26% обращений;
- Trojan.Encoder.11539 — 6.62% обращений;
- **Trojan.Encoder.24249** — 5.77% обращений;
- Trojan.Encoder.567 — 3.63% обращений;
- Trojan.Encoder.2667 — 2.35% обращений.

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

Настрой-ка Dr.Web от шифровальщиков

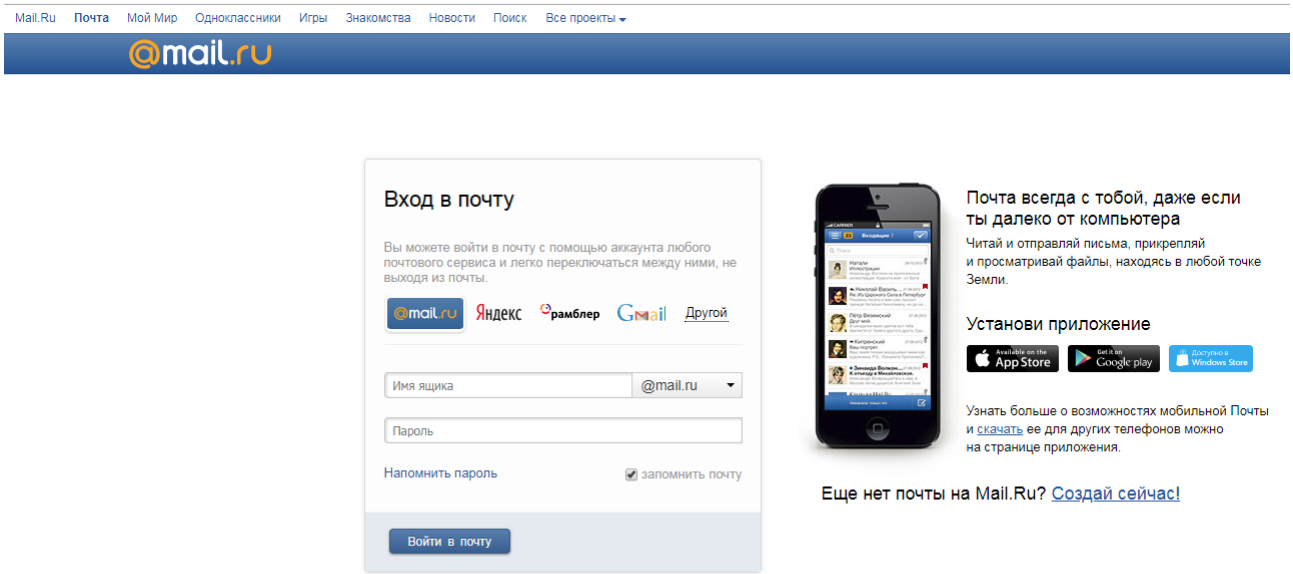
Обучающий курс

О бесплатном восстановлении

Dr.Web Rescue Pack

Опасные сайты

В начале марта компания «Доктор Веб» сообщила о массовой рассылке по электронной почте фишинговых писем якобы от имени компании Mail.Ru. В этих посланиях злоумышленники предупреждали получателей о блокировке их учетных записей на сервере Mail.Ru и предлагали пройти повторную авторизацию. Ссылка в письме вела на поддельный сайт Mail.Ru, а введенная пользователем информация незамедлительно передавалась злоумышленникам.



Адрес поддельного сайта был добавлен в базы Офисного и Родительского контроля Dr.Web.

В течение марта 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 624 474 интернет-адреса.

Февраль 2018	Март 2018	Динамика
+ 1 174 380	+ 624 474	- 46.8%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Другие события в сфере информационной безопасности

Троянцы семейства Trojan.LoadMoney, скачивающие на зараженный компьютер другие вредоносные программы, известны с 2013 года. В марте вирусные аналитики «Доктор Веб» исследовали несколько новых представителей этого семейства. Вирусописатели не реализовали в коде вредоносных программ никаких визуальных эффектов, так что эти троянцы не проявляют себя в зараженной системе и обнаружить их вредоносную деятельность непросто. Более подробно об исследованных вредоносных программах семейства Trojan.LoadMoney рассказано в нашей обзорной статье.

Вредоносное и нежелательное ПО для мобильных устройств

В марте вирусные аналитики «Доктор Веб» опубликовали результаты исследования троянца Android.Triada.231, которого вирусописатели внедрили в прошивку более 40 моделей Android-смартфонов. Android.Triada.231 заражает процессы всех приложений и может незаметно выполнять различные вредоносные действия. В течение прошедшего месяца в каталоге Google Play было выявлено множество новых троянцев, среди которых – представители семейства Android.Click, способные загружать и показывать любые веб-страницы, а также Android-банкер Android.BankBot.344.origin. Кроме того, специалисты компании «Доктор Веб» обнаружили новых банковских троянцев, созданных на основе исходного кода вредоносного приложения Android.BankBot.149.origin. Один из них получил имя Android.BankBot.325.origin. Этот банкер показывал фишинговые окна, использовался для кибершпионажа и предоставлял злоумышленникам дистанционный доступ к зараженным устройствам.

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

- обнаружение троянца в десятках моделей Android-смартфонов;
- появление новых банковских троянцев;
- обнаружение вредоносных программ в каталоге Google Play.

Обзор вирусной активности в марте 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 | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах