Dr.WEB®
с 1992 года

Обзор вирусной активности в марте 2019 года

Обзор вирусной активности в марте 2019 года

3 апреля 2019 года

В марте вирусные аналитики компании «Доктор Веб» завершили исследование трояна, угрожавшего игрокам Counter-Strike 1.6. Среди главных угроз марта наблюдается динамика по сравнению с цифрами прошлого месяца. К примеру, активность Trojan.MulDrop8.60634 снизилась почти в три раза, а число таких угроз, как Trojan.Packed.24060 и Adware.OpenCandy.243, резко возросло за последний месяц. Также в базу нерекомендуемых и вредоносных сайтов было добавлено меньше доменных имен, чем в прошлом месяце, а в техническую поддержку «Доктор Веб» поступило больше запросов на расшифровку данных.

Главные тенденции марта

- Увеличилось количество вредоносных расширений для браузеров
- Выросла активность распространения рекламного ПО и нежелательных программ
- Увеличилось число запросов на расшифровку данных

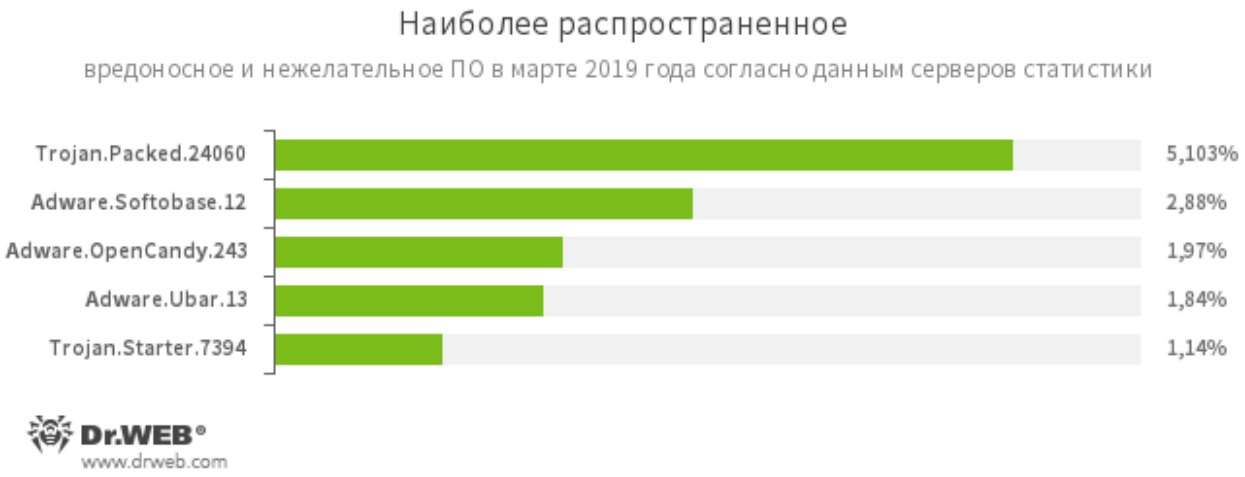
Угроза месяца

В марте аналитики «Доктор Веб» опубликовали подробное исследование трояна 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 троянцем Belonard, достигло 39% от числа всех официальных серверов, зарегистрированных в Steam. Теперь все модули трояна Belonard успешно определяются антивирусом Dr.Web и не угрожают нашим пользователям.

Подробнее о трояне

Обзор вирусной активности в марте 2019 года

По данным серверов статистики «Доктор Веб»



Угрозы этого месяца:

- Trojan.Packed.24060

Устанавливает вредоносные расширения для браузеров, перенаправляющие с результатов выдачи в поисковых системах на другие сайты.

- Adware.Softobase.12

Программа-установщик, распространяющая устаревшее программное обеспечение. Меняет настройки браузера.

- Adware.OpenCandy.243

Семейство приложений, предназначенных для установки различного ПО. Программы данного семейства используются разработчиками бесплатных приложений в целях монетизации.

- Adware.Ubar.13

Торрент-клиент, устанавливающий нежелательное ПО на устройство.

- Trojan.Starter.7394

Троянец, предназначенный для запуска другого вредоносного ПО на устройстве.

Снизилось количество угроз от:

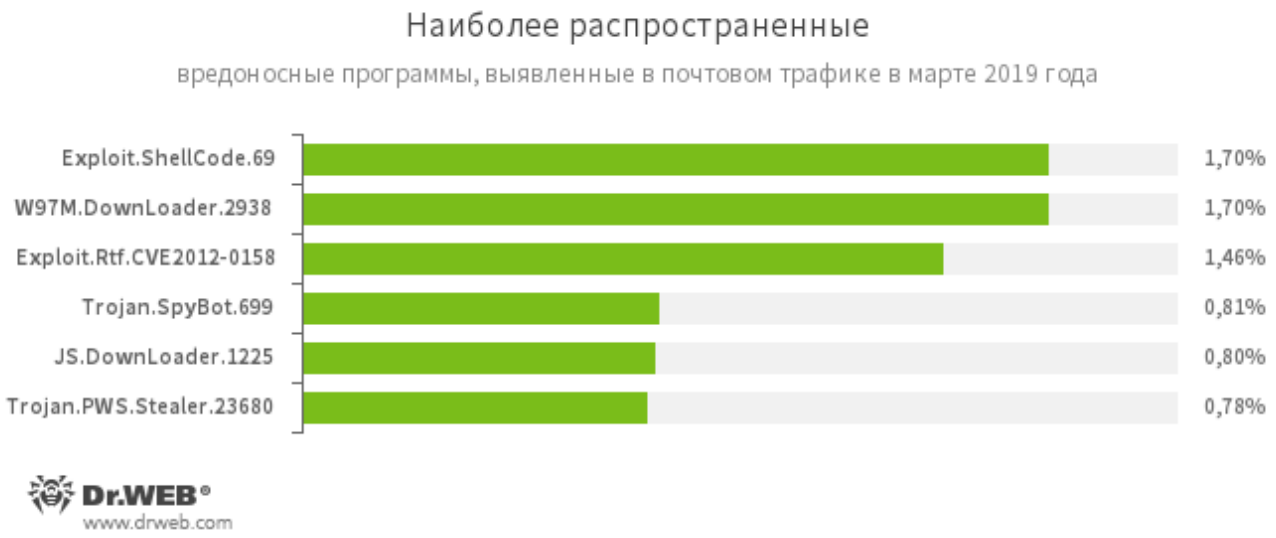
- Trojan.MulDrop8.60634

Устанавливает других троянцев в систему. Все устанавливаемые компоненты содержатся в самом теле Trojan.MulDrop.

- Adware.Downware.19283

Программа-установщик, обычно распространяется с пиратским контентом. При установке

Статистика вредоносных программ в почтовом трафике



- **Exploit.ShellCode.69**

Вредоносный документ Microsoft Office Word. Использует уязвимость CVE-2017-11882.

- **W97M.DownLoader.2938**

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

- **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

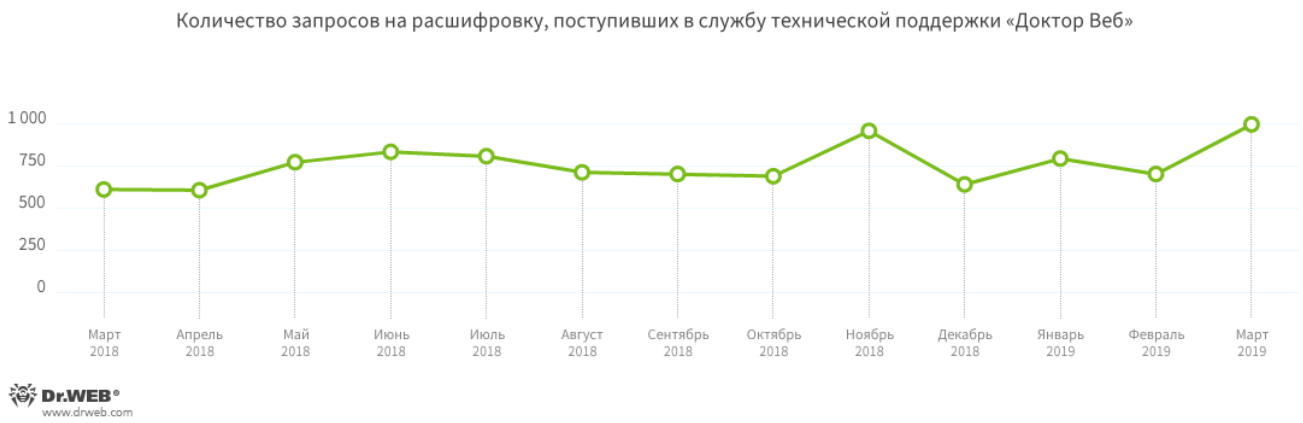
- **JS.DownLoader.1225**

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

- Trojan.PWS.Stealer.23680

Семейство троянцев, предназначенных для хищения с инфицированного компьютера паролей и другой конфиденциальной информации.

Шифровальщики



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

- Trojan.Encoder.858 — 28,39%;
- Trojan.Encoder.18000 — 9,54%;
- Trojan.Encoder.27210 — 4,25%;
- Trojan.Encoder.11464 — 4,14%;
- Trojan.Encoder.11539 — 4,14%;
- Trojan.Encoder.567 — 2,76%;
- Trojan.Archivelock — 2,34%.

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 марта 2019 года в базу нерекомендуемых и вредоносных сайтов было добавлено 288 159 интернет-адресов.

Февраль 2019	Март 2019	Динамика
+ 288 159	+ 270 227	- 6,63%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В уходящем месяце в каталоге Google Play были выявлены новые вредоносные программы. Среди них — очередные троянцы семейства Android.FakeApp, которые распространяются под видом программ для онлайн-заработка. Они загружают веб-сайты, где владельцам мобильных устройств предлагается ответить на вопросы «компаний-спонсоров». За участие в опросах злоумышленники обещают потенциальным жертвам вознаграждение. Чтобы получить его, пользователям якобы необходимо оплатить комиссию за денежный перевод или же для подтверждения своей личности. На самом деле никакого вознаграждения нет, и пользователи отправляют деньги мошенникам.

Также были обнаружены новые троянцы Android.HiddenAds. Они постоянно показывают рекламные баннеры поверх окон других программ и системного интерфейса и мешают работе с Android-устройствами.

Кроме того, злоумышленники продолжили распространять банковских троянцев. Об одном из них наша компания сообщила во второй половине марта. Вредоносная программа, известная под именем Flexnet, похищает деньги с банковских счетов и баланса мобильных телефонов пользователей.

В конце месяца вирусные аналитики раскрыли детали уязвимости популярного Android-браузера UC Browser, который способен скачивать плагины в обход серверов Google Play. Злоумышленники могли использовать эту функцию для распространения троянцев.

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

- обнаружение уязвимости в браузере UC Browser;
- распространение вредоносных программ в Google Play;
- распространение банковских троянцев.

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

Обзор вирусной активности в марте 2019 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