



«Доктор Веб»: обзор вирусной активности в марте 2020 года



«Доктор Веб»: обзор вирусной активности в марте 2020 года

10 апреля 2020 года

В марте анализ данных статистики Dr.Web показал рост общего числа обнаруженных угроз на 12.51% по сравнению с февралем. Количество уникальных угроз возросло на 8.75%. Пользователям чаще всего угрожали вредоносные расширения для браузеров, нежелательные и рекламные программы. В почтовом трафике по-прежнему доминирует вредоносное ПО, использующее уязвимости документов Microsoft Office, а также банковский троян [Trojan.SpyBot.699](#).

В марте число обращений пользователей за расшифровкой файлов увеличилось на 7.63% по сравнению с февралем. Самым распространенным энкодером остается [Trojan.Encoder.26996](#), на долю которого пришлось 32.60% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ МАРТА

- Рост активности распространения вредоносного ПО
- Увеличение количества вредоносных расширений для браузеров
- Увеличение активности шифровальщиков
- Рост числа nereкомендуемых и вредоносных сайтов

Угроза месяца

В марте специалисты «Доктор Веб» [сообщили](#) о компрометации ряда сайтов — от новостных блогов до корпоративных ресурсов, — созданных на CMS WordPress. JavaScript-сценарий, встроенный в код взломанных страниц, перенаправлял посетителей на фишинговую страницу, где им предлагалось установить важное обновление безопасности для браузера Google Chrome. Загружаемый файл представляет собой установщик троянской программы, которая позволяла злоумышленникам дистанционно управлять инфицированными компьютерами и доставлять на них дополнительные вредоносные модули.

«Доктор Веб»: обзор вирусной активности в марте 2020 года

По данным серверов статистики «Доктор Веб»



Угрозы прошедшего месяца:

Trojan.BPlug.3835

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

Adware.Elemental.17

Семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают эти приложения, которые показывают рекламу, а также инсталлируют ненужное ПО.

Adware.Softobase.15

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

Adware.Ubar.13

Торрент-клиент, устанавливающий нежелательное ПО на устройство.

Adware.Downware.19722

Рекламное ПО, часто выступающее в роли промежуточного установщика пиратских программ.

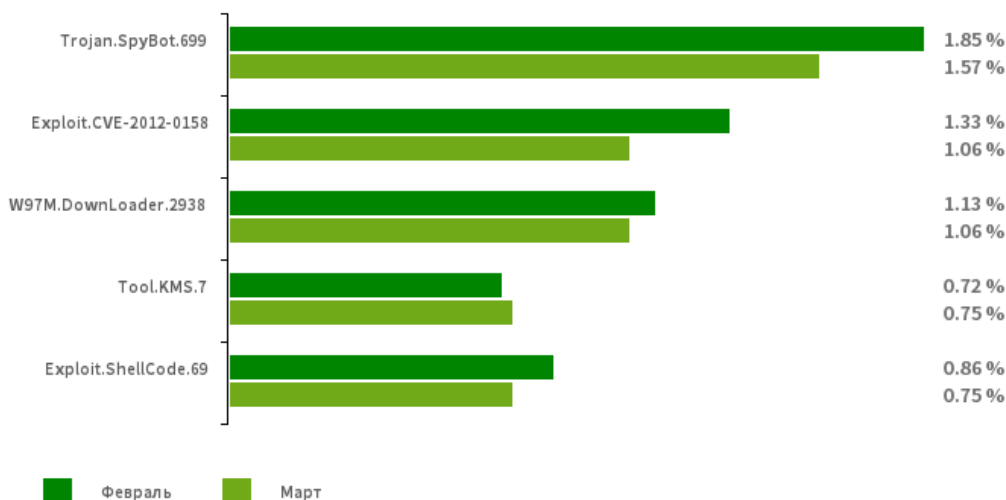
Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

«Доктор Веб»: обзор вирусной активности в марте 2020 года

Статистика вредоносных программ в почтовом трафике

Динамика распространения вредоносных программ, выявленных в почтовом трафике в марте 2020



[Trojan.SpyBot.699](#)

Многомодульный банковский троян. Позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и исполнять произвольный код.

[Exploit.CVE-2012-0158](#)

Измененный документ Microsoft Office Word, использующий уязвимость CVE-2012-0158 для выполнения вредоносного кода.

W97M.DownLoader.2938

Семейство троянов-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Tool.KMS.7

Хакерские утилиты, которые используются для активации продуктов Microsoft с поддельной лицензией.

[Exploit.ShellCode.69](#)

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

«Доктор Веб»: обзор вирусной активности в марте 2020 года

Шифровальщики

По сравнению с февралем в марте в антивирусную лабораторию «Доктор Веб» поступило на 7.63% больше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков.

Количество запросов на расшифровку, поступивших в службу технической поддержки «Доктор Веб»



- [Trojan.Encoder.26996](#) — 32.60%
- Trojan.Encoder.29750 — 9.07%
- [Trojan.Encoder.567](#) — 4.66%
- [Trojan.Encoder.11464](#) — 3.19%
- [Trojan.Encoder.11539](#) — 1.96%

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](#)

«Доктор Веб»: обзор вирусной активности в марте 2020 года

Опасные сайты

В течение марта 2020 года в базу нерекомендуемых и вредоносных сайтов был добавлен **186 881** интернет-адрес.

Февраль 2020	Март 2020	Динамика
+ 90 385	+ 186 881	+ 106.76%

[Нерекомендуемые сайты](#)

Вредоносное и нежелательное ПО для мобильных устройств

В марте антивирусные продукты Dr.Web для Android зафиксировали рост общего числа угроз на защищаемых устройствах на 21% по сравнению с февралем. В каталоге Google Play вирусные аналитики обнаружили очередные вредоносные приложения. Среди них был новый представитель уже известного семейства троянов [Android Joker](#); эти программы способны загружать и выполнять произвольный код, а также подписывать пользователей на платные сервисы. Кроме того, в прошедшем месяце была выявлена новая угроза, получившая имя [Android.Circle.1](#). По команде злоумышленников этот троян показывал рекламу и загружал веб-сайты, на которых имитировал действия пользователей.

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

- обнаружение новых угроз в каталоге Google Play;
- рост числа угроз, выявленных на защищаемых устройствах.

Более подробно о вирусной обстановке для мобильных устройств в марте читайте в нашем [обзоре](#).

«Доктор Веб»: обзор вирусной активности в марте 2020 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

[ВебиОметр](#) | [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](#)



© ООО «Доктор Веб»,
2003-2020

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)