



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



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

11 февраля 2020 года

В январе статистика серверов Dr.Web зарегистрировала рост общего числа обнаруженных угроз на 0.53% по сравнению с декабрем. При этом количество уникальных угроз снизилось на 5.06%. Статистика по вредоносному и нежелательному ПО показывает преобладание вредоносных расширений для браузеров, нежелательных и рекламных программ. В почтовом трафике по-прежнему доминирует вредоносное ПО, использующее уязвимости документов Microsoft Office. Вместе с тем двукратно возросло количество обнаружений банковского трояна [Trojan.SpyBot.699](#).

В январе продолжила снижаться активность шифровальщиков — число обращений пользователей за расшифровкой файлов снизилось на 24.02% по сравнению с декабрем. Самым распространенным энкодером остается [Trojan.Encoder.26996](#), на долю которого пришлось 18.48% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ ЯНВАРЯ

- Увеличение количества вредоносных расширений для браузеров
- Рекламные трояны и рекламное ПО остаются одними из самых активных угроз
- Увеличение количества обнаруженных угроз в почтовом трафике
- Снижение активности шифровальщиков

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

По данным серверов статистики «Доктор Веб»



Угрозы прошедшего месяца:

Trojan.BPlug.3814

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

Adware.Elemental.14

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.19627

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

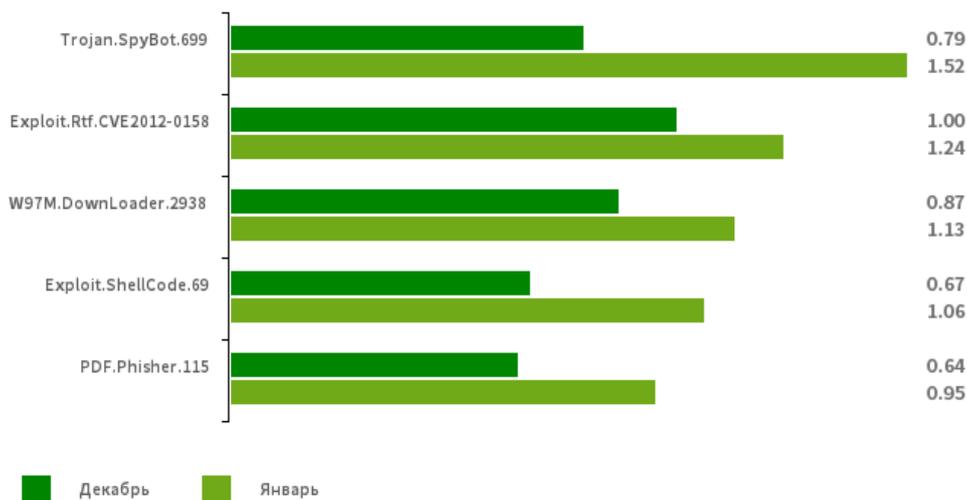
Узнайте больше

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

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

Статистика вредоносных программ в почтовом трафике

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



[Trojan.SpyBot.699](#)

Многомодульный банковский троянец. Он 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 троянцев-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

[Exploit.ShellCode.69](#)

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

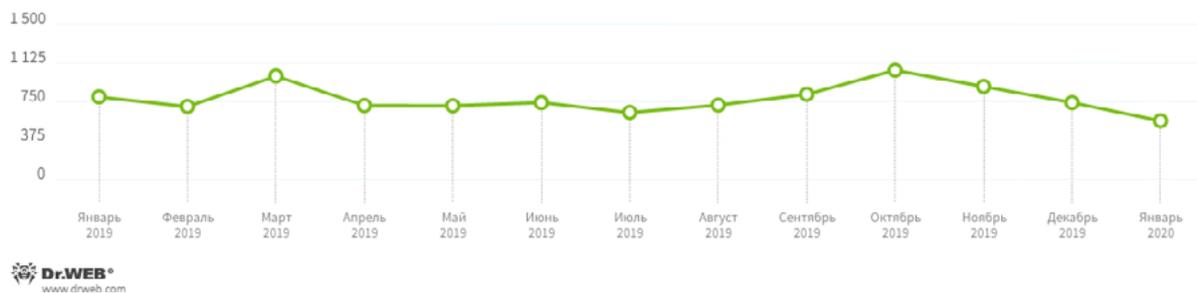
[PDF.Phisher.115](#)

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

Шифровальщики

По сравнению с декабрем в январе в антивирусную лабораторию «Доктор Веб» поступило на 24.02% меньше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков.

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



- [Trojan.Encoder.26996](#) — 18.48%
- [Trojan.Encoder.567](#) — 10.38%
- Trojan.Encoder.29750 — 4.81%
- [Trojan.Encoder.858](#) — 3.54%
- [Trojan.Encoder.11464](#) — 2.78%

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 январе 2020 года

Опасные сайты

В течение января 2020 года в базу нерекомендуемых и вредоносных сайтов было добавлено **97 166** интернет-адресов.

Декабрь 2019	Январь 2020	Динамика
+ 162 535	+ 97 166	- 40.22%

[Нерекомендуемые сайты](#)

Вредоносное и нежелательное ПО для мобильных устройств

По сравнению с декабрем на Android-устройствах количество обнаруженных угроз снизилось почти на 13%. При этом программы, предназначенные для слежения за пользователями, а также трояны, загружающие и запускающие другие вредоносные приложения, по-прежнему остаются активными.

В течение января вирусные аналитики «Доктор Веб» выявили в Google Play несколько новых модификаций троянов семейства [Android Joker](#), которые подписывают пользователей на премиум-сервисы и загружают дополнительные вредоносные компоненты. Злоумышленники распространяли этих троянов под видом безобидного ПО — игр, фотокамер, сборников изображений и других подобных программ.

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

- появление новых угроз в каталоге Google Play;
- снижение числа угроз, обнаруженных на защищаемых устройствах.

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

«Доктор Веб»: обзор вирусной активности в январе 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](#)