

# «Доктор Веб»: обзор вирусной активности в сентябре 2020 года



## «Доктор Веб»: обзор вирусной активности в сентябре 2020 года

### 22 октября 2020 года

В сентябре анализ данных статистики Dr.Web показал увеличение общего числа обнаруженных угроз — на 13.88% по сравнению с августом. Количество уникальных вредоносных программ также выросло — на 19.17%. Большинство выявленных угроз по-прежнему приходится на долю рекламных программ, а также троянских загрузчиков вредоносного ПО. В почтовом трафике среди самых распространенных угроз вновь оказался опасный банковский троян [Trojan.SpyBot.699](#). Кроме того, пользователям продолжают угрожать различные модификации вредоносных HTML-документов, распространяемых в виде вложений и перенаправляющих пользователей на фишинговые сайты.

В сентябре количество обращений пользователей за расшифровкой файлов осталось на августовском уровне. Самым распространенным энкодером остается [Trojan.Encoder.26996](#), на долю которого приходится 35.71% всех инцидентов.

### ГЛАВНЫЕ ТЕНДЕНЦИИ СЕНТЯБРЯ

- Увеличение общего числа обнаруженного вредоносного ПО
- Рекламные приложения остаются в числе самых активных угроз

# «Доктор Веб»: обзор вирусной активности в сентябре 2020 года

## По данным серверов статистики «Доктор Веб»



### Угрозы прошедшего месяца:

Adware.Downware.19741

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

Adware.Softobase.15

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

Trojan.LoadMoney.4020

Семейство программ-установщиков, вместе с требуемыми приложениями инсталлирующих на компьютеры жертв всевозможные дополнительные компоненты. Некоторые модификации трояна могут собирать и передавать злоумышленникам различную информацию об атакованном компьютере.

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.SweetLabs.2

Альтернативный каталог приложений и надстройка к графическому интерфейсу Windows от создателей Adware.Opencandy.

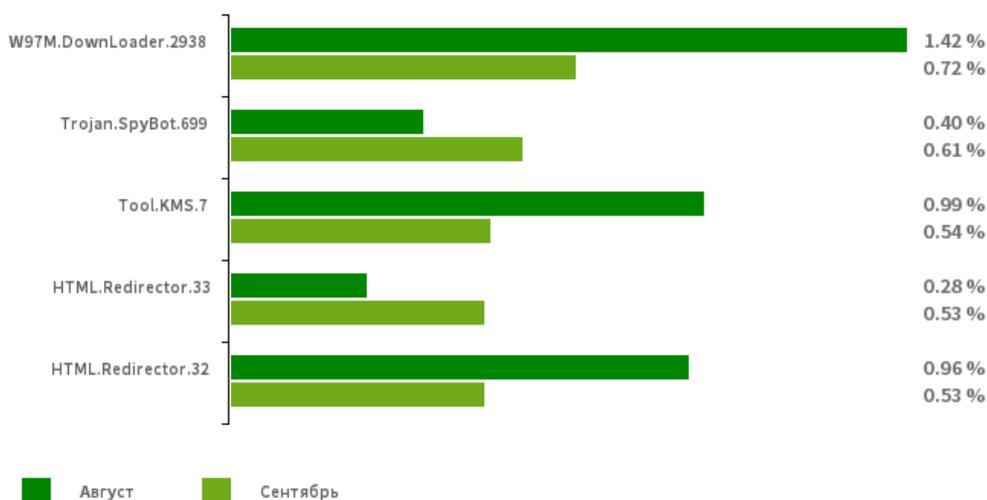
Узнайте больше

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

# «Доктор Веб»: обзор вирусной активности в сентябре 2020 года

## Статистика вредоносных программ в почтовом трафике

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



### W97M.DownLoader.2938

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

### [Trojan.SpyBot.699](#)

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

### Tool.KMS.7

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

### HTML.Redirector.33

### HTML.Redirector.32

Вредоносные HTML-документы, как правило маскирующиеся под безобидные вложения к электронным письмам. При открытии перенаправляют пользователей на фишинговые сайты или загружают полезную нагрузку на заражаемые устройства.

Узнайте больше

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

# «Доктор Веб»: обзор вирусной активности в сентябре 2020 года

## Шифровальщики

По сравнению с августом в сентябре в антивирусную лабораторию «Доктор Веб» поступило на 0.45% меньше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков.

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



- [Trojan.Encoder.26996](#) — 35.71%
- [Trojan.Encoder.567](#) — 6.59%
- Trojan.Encoder.29750 — 3.85%
- [Trojan.Encoder.18000](#) — 1.10%
- Trojan.Encoder.30356 — 1.10%

### 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 сентябре 2020 года

## Опасные сайты

В течение сентября 2020 года в базу нерекомендуемых и вредоносных сайтов было добавлено **152 270** интернет-адресов

Август 2020	Сентябрь 2020	Динамика
+ 174 501	+ 152 270	- 12.74%

[Нерекомендуемые сайты](#)

### Вредоносное и нежелательное ПО для мобильных устройств

В сентябре на Android-устройствах было выявлено на 3.75% больше угроз, чем в августе. При этом в каталоге Google Play вновь распространялись всевозможные троянские программы. В их числе оказались представители семейства [Android.Joker](#), способные выполнять произвольный код и подписывать жертв на дорогостоящие мобильные услуги. Другой угрозой стал опасный многофункциональный троян [Android.Triada.545.origin](#), который также мог выполнять произвольный код и похищал конфиденциальную информацию. Кроме того, вирусные аналитики компании «Доктор Веб» выявили очередного трояна-кликера, получившего имя [Android.Click.978](#). Он показывал рекламу, а также загружал различные веб-сайты и переходил по находившимся на них ссылкам и баннерам.

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

- увеличение общего числа угроз, обнаруженных на защищаемых Android-устройствах;
- распространение новых угроз через каталог Google Play.

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

## «Доктор Веб»: обзор вирусной активности в сентябре 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](http://www.антивирус.рф) | [www.drweb.ru](http://www.drweb.ru) | [free.drweb.ru](http://free.drweb.ru) | [www.av-desk.ru](http://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](#)