



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



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

21 июля 2020 года

В июне анализ данных статистики Dr.Web показал рост общего числа обнаруженных угроз на 113.21% по сравнению с маем. При этом количество уникальных угроз снизилось на 24.1%. Большинство обнаруженных угроз по-прежнему приходится на долю рекламных программ, а также загрузчиков и установщиков вредоносного ПО. В почтовом трафике продолжает доминировать программное обеспечение, использующее уязвимости документов Microsoft Office. Кроме того, в число самых распространенных угроз входит многомодульный банковский троян [Trojan.SpyBot.699](#), а также различные модификации вредоносных HTML-документов, распространяемых в виде вложений и перенаправляющих пользователей на фишинговые сайты.

В июне статистика вновь зафиксировала снижение числа обращений пользователей за расшифровкой файлов — на 6.55% по сравнению с маем. Самым распространенным энкодером остается [Trojan.Encoder.26996](#), на долю которого пришлось 24.71% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ ИЮНЯ

- Значительное увеличение активности распространения вредоносного ПО
- Снижение количества уникальных угроз
- Рекламные приложения остаются одними из самых активных угроз
- Незначительное снижение активности шифровальщиков

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

По данным серверов статистики «Доктор Веб»



Угрозы прошедшего месяца:

Trojan.LoadMoney.4020

Семейство программ-установщиков, инсталлирующих на компьютеры жертв вместе с требуемыми приложениями 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.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.BPlug.3845

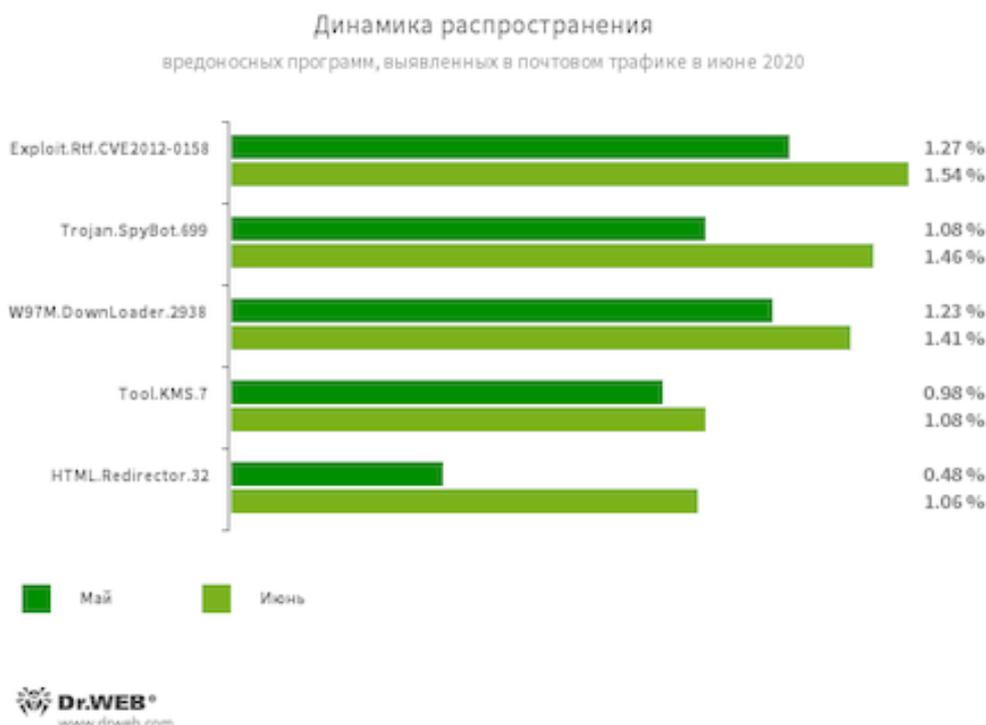
Вредоносное расширение для браузера, предназначенное для осуществления веб-инъектов в просматриваемые пользователями интернет-страницы и блокировки сторонней рекламы.

Узнайте больше

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

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

Статистика вредоносных программ в почтовом трафике



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

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

[Trojan.SpyBot.699](#)

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

[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.

[HTML.Redirector.32](#)

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

Узнайте больше

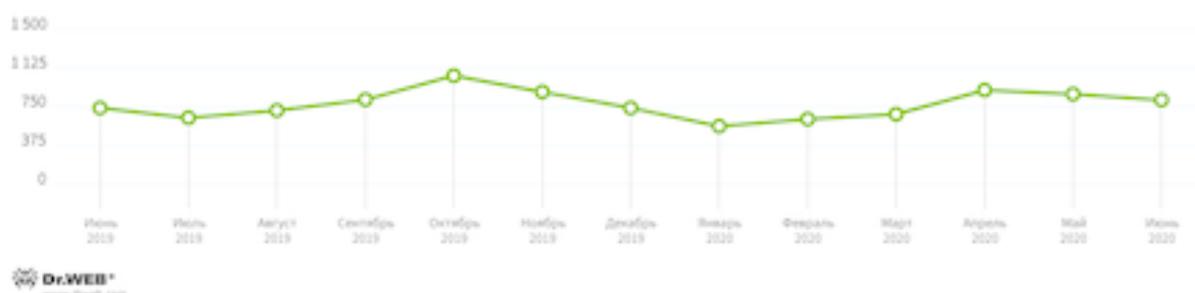
[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

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

Шифровальщики

По сравнению с маем в июне в антивирусную лабораторию «Доктор Веб» поступило на 6.55% меньше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков.

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



- [Trojan.Encoder.26996](#) — 24.71%
- Trojan.Encoder.29750 — 9.26%
- [Trojan.Encoder.567](#) — 8.31%
- Trojan.Encoder.30562 — 1.43%
- [Trojan.Encoder.858](#) — 1.19%

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 июне 2020 года

Опасные сайты

В течение июня 2020 года в базу нерекомендуемых и вредоносных сайтов было добавлено **122 679** интернет-адресов.

Май 2020	Июнь 2020	Динамика
+ 107 082	+ 122 679	+ 14.56%

[Нерекомендуемые сайты](#)

Вредоносное и нежелательное ПО для мобильных устройств

По сравнению с маем число угроз, выявленных на Android-устройствах в июне, снизилось на 17.2%. В каталоге Google Play были обнаружены новые вредоносные приложения, такие как рекламные трояны семейства [Android.HiddenAds](#) многофункциональные трояны семейства [Android.Joker](#), способные загружать и выполнять произвольный код, а также самостоятельно подписывать пользователей на платные мобильные сервисы. Среди обнаруженных угроз был и новый банковский троян, получивший имя [Android.BankBot.733.origin](#). Он загружал вспомогательный вредоносный компонент и пытался установить его при помощи функции специальных возможностей ОС Android.

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

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

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

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