Dr.WEB®
с 1992 года

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

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

10 августа 2020 года

В июле анализ данных статистики Dr.Web показал снижение общего числа обнаруженных угроз на 6.41% по сравнению с июнем. При этом количество уникальных угроз увеличилось на 8.58%. Рекламные программы, загрузчики и установщики вредоносного ПО продолжают лидировать по общему количеству обнаруженных угроз. В почтовом трафике на первых позициях находится многомодульный банковский троян Trojan.SpyBot.699. Кроме того, пользователям по-прежнему угрожают программы, использующие уязвимости документов Microsoft Office, а также различные модификации вредоносных HTML-документов, распространяемых в виде вложений и перенаправляющих пользователей на фишинговые сайты.

В июле статистика вновь зафиксировала снижение числа обращений пользователей за расшифровкой файлов — на 16.34% по сравнению с июнем. Самым распространенным энкодером остается Trojan.Encoder.26996, на долю которого пришлось 23.51% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ ИЮЛЯ

- Увеличение количества уникальных угроз
- Рекламные приложения остаются одними из самых активных угроз
- Снижение активности шифровальщиков

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

По данным серверов статистики «Доктор Веб»

Угрозы прошедшего месяца:

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.Downware.19741

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

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

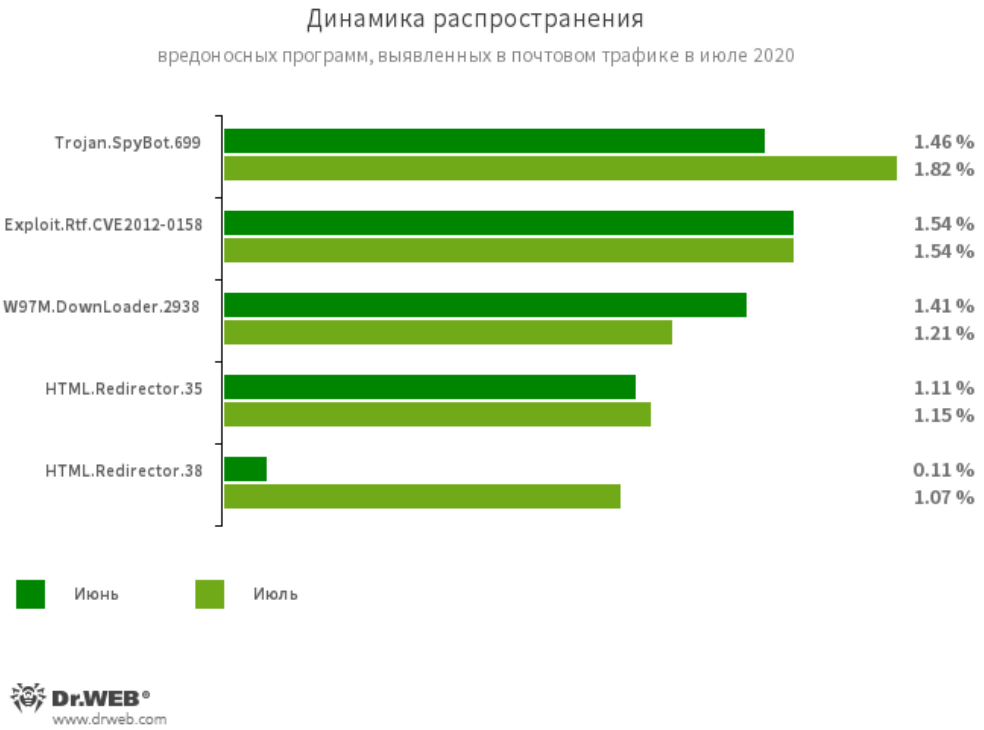
Программа-установщик, распространяющая устаревшее программное обеспечение. Меняет настройки браузера.

Trojan.BPlug.3845

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

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

Статистика вредоносных программ в почтовом трафике



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.

HTML.Redirector.32

HTML.Redirector.38

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.

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

Шифровальщики

По сравнению с июнем в июле в антивирусную лабораторию «Доктор Веб» поступило на 16.34% меньше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков.

- Trojan.Encoder.26996 — 23.51%
- Trojan.Encoder.567 — 7.93%
- Trojan.Encoder.29750 — 7.37%
- Trojan.Encoder.11464 — 2.55%
- Trojan.Encoder.30356 — 2.55%

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 июля 2020 года в базу нерекомендуемых и вредоносных сайтов было добавлено 198 467 интернет-адресов.

Июнь 2020	Июль 2020	Динамика
+ 122 679	+ 198 467	+ 61.78%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В июле общее количество угроз, обнаруженных на Android-устройствах пользователей, снизилось на 6.7%. Часть новых вредоносных программ, выявленных за прошедший месяц, вновь распространялась через каталог Google Play. Среди них оказались рекламные трояны, получившие имена Android.HiddenAds.2190 и Android.HiddenAds.2193. Они показывали пользователям надоедливые баннеры и мешали работе с устройствами. Другими угрозами стали многофункциональный троян Android.Joker.279, а также банкер Android.Banker.3259. Обе программы маскировались под приложения для работы с СМС.
Наиболее заметные события, связанные с «мобильной» безопасностью в июле:

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

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

«Доктор Веб»: обзор вирусной активности в июле 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
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