Dr.WEB®
с 1992 года

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

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

16 сентября 2020 года

В августе анализ данных статистики Dr.Web показал значительное снижение общего числа обнаруженных угроз — на 67.16% по сравнению с июлем. Количество уникальных угроз снизилось на 9.85%. 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, пользователям угрожают различные модификации вредоносных HTML-документов, распространяемых в виде вложений и перенаправляющих пользователей на фишинговые сайты.

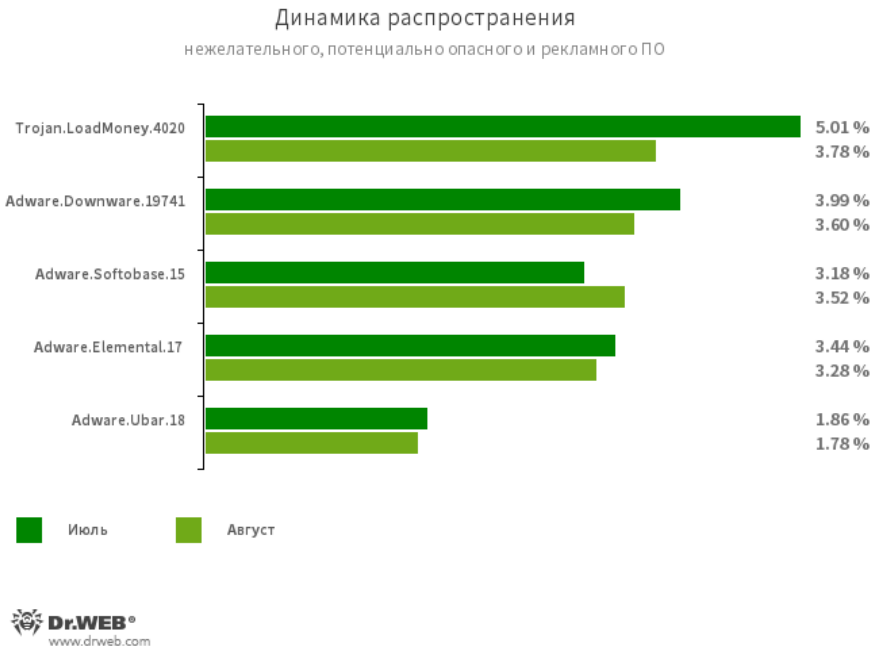
По сравнению с июлем в прошедшем месяце количество обращений пользователей за расшифровкой файлов снизилось на 2.5%. Самым распространенным энкодером остается Trojan.Encoder.26996, на долю которого по-прежнему приходится более четверти всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ АВГУСТА

- Снижение общего числа угроз
- Сокращение количества уникальных угроз

«Доктор Веб»: обзор вирусной активности в августе 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.Softobase.15

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

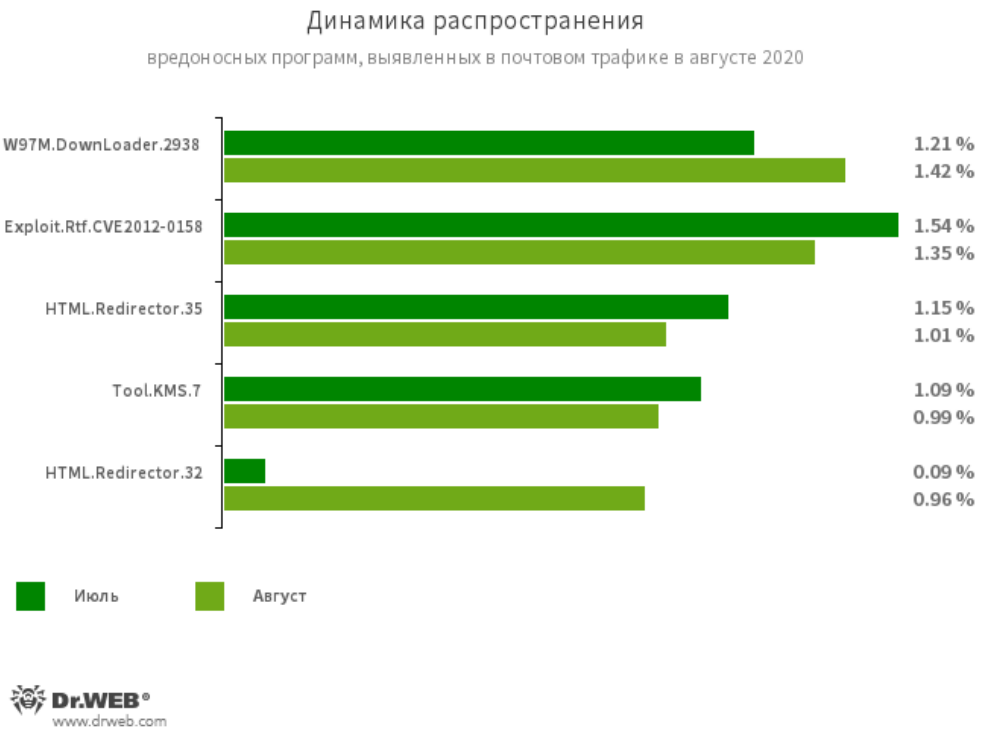
Adware.Elemental.17

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.Ubar.18

Торрент-клиент, устанавливающий нежелательное ПО на устройство.

Статистика вредоносных программ в почтовом трафике



TW97M.DownLoader.2938

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

Exploit.CVE-2012-0158

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

HTML.Redirector.35

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.

Tool.KMS.7

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

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

Шифровальщики

По сравнению с июлем в августе в антивирусную лабораторию «Доктор Веб» поступило на 2.5% меньше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков.

- Trojan.Encoder.26996 — 26.33%
- Trojan.Encoder.567 — 7.40%
- Trojan.Encoder.29750 — 5.03%
- Trojan.Encoder.30356 — 2.96%
- Trojan.Encoder.11464 — 2.07%

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 августа 2020 года в базу нерекомендуемых и вредоносных сайтов был добавлен 174 501 интернет-адрес.

Июль 2020	Август 2020	Динамика
+ 198 467	+ 174 501	- 12.08%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В августе вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play очередные угрозы. Среди них были многочисленные троянские приложения семейства Android.FakeApp, которые распространялись под видом справочников с информацией о способах получения возврата НДС и социальных выплат. На самом деле они загружали мошеннические веб-сайты, с помощью которых злоумышленники похищали у жертв персональные данные и деньги. Кроме того, был найден новый представитель опасного семейства троянов Android.Joker. Он загружал и выполнял произвольный код, а также подписывал владельцев Android-устройств на дорогостоящие услуги.

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

- рост общего числа угроз, выявленных на защищаемых Android-устройствах.
- проникновение новых угроз в каталог Google Play

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

«Доктор Веб»: обзор вирусной активности в августе 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