Dr.WEB®
с 1992 года

Обзор вирусной активности в августе 2019 года

Обзор вирусной активности в августе 2019 года

9 сентября 2019 года

В августе статистика серверов Dr.Web зафиксировала снижение роста общего числа обнаруженных угроз на 21.28% по сравнению с июлем. При этом количество уникальных угроз уменьшилось незначительно – на 2.82%. В почтовом трафике на первых позициях находится вредоносное ПО, использующее уязвимости документов Microsoft Office, а также троянцы-загрузчики. Продолжает тенденцию прошлого месяца и статистика по вредоносному и нежелательному ПО: большинство обнаруженных угроз приходится на долю рекламных программ.

Главные тенденции августа

- Снижение активности распространения вредоносного ПО
- Рост числа нерекомендуемых и вредоносных сайтов
- Повышение активности шифровальщиков
-

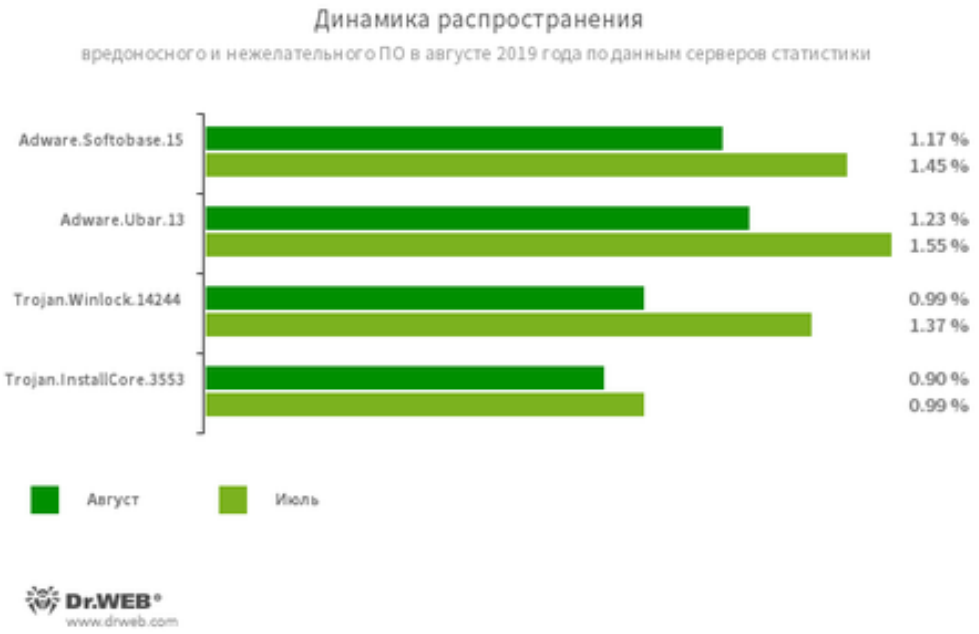
Угроза месяца

В августе специалисты вирусной лаборатории «Доктор Веб» обнаружили, что хакеры используют копии сайтов популярных сервисов для распространения опасного банковского троянца. Один из таких ресурсов копирует известный VPN-сервис, а другие замаскированы под сайты корпоративных офисных программ.

Подробнее об угрозе

Обзор вирусной активности в августе 2019 года

По данным серверов статистики «Доктор Веб»



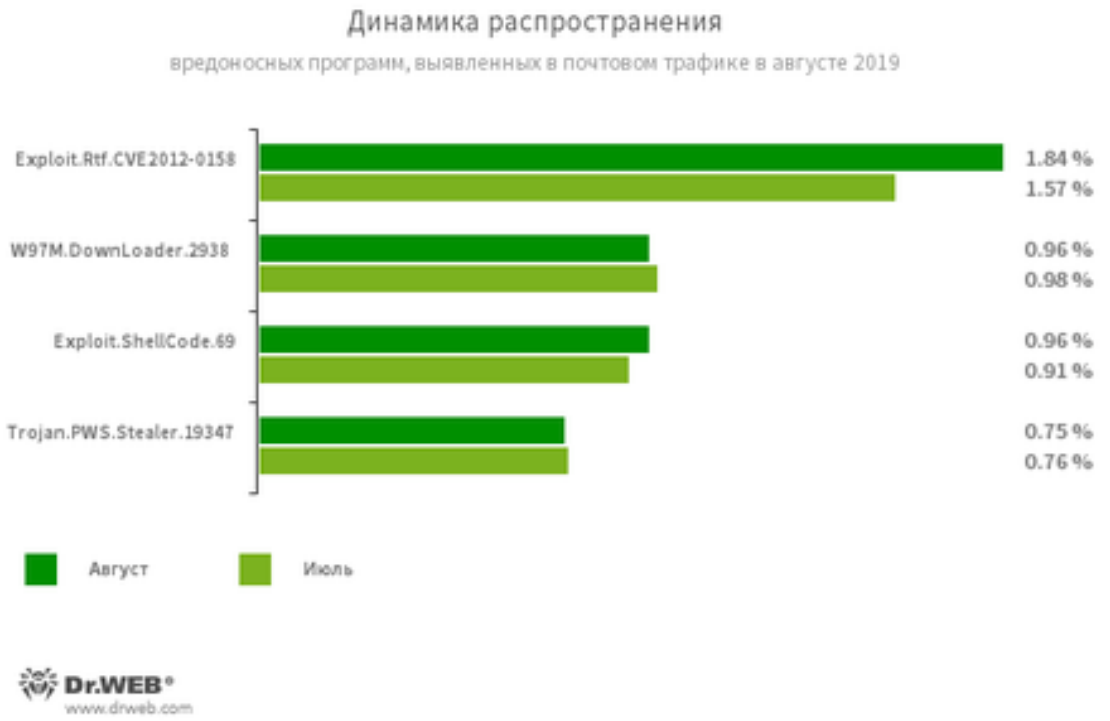
Adware.Softobase.15
Программа-установщик, распространяющая устаревшее программное обеспечение. Меняет настройки браузера.

Adware.Ubar.13
Торрент-клиент, устанавливающий нежелательное ПО на устройство.

Trojan.Winlock.14244
Блокирует или ограничивает доступ пользователя к операционной системе и её основным функциям. Для разблокировки системы требует перечислить деньги на счет разработчиков троянца.

Trojan.InstallCore.3553
Еще один известный установщик рекламного ПО. Показывает рекламу и устанавливает дополнительные программы без согласия пользователя.

Статистика вредоносных программ в почтовом трафике



Exploit.Rtf.CVE2012-0158
Измененный документ Microsoft Office Word, использующий уязвимость CVE2012-0158 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.

Trojan.PWS.Stealer.19347
Семейство троянцев, предназначенных для хищения с инфицированного компьютера паролей и другой конфиденциальной информации

Шифровальщики

- Trojan.Encoder.858 — 17.73%
- Trojan.Encoder.11464 — 7.09%
- Trojan.Encoder.18000 — 4.96%
- Trojan.Encoder.28004 — 4.26%
- Trojan.Encoder.11539 — 2.60%
- Trojan.Encoder.25574 — 1.18%
- Trojan.Encoder.567 — 1.65%

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 2019 года в базу нерекомендуемых и вредоносных сайтов был добавлен 204 551 интернет-адрес.

Июль 2019	Август 2019	Динамика
+ 123 251	+ 204 551	+ 65.96%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В августе специалисты «Доктор Веб» обнаружили в Google Play сразу несколько новых вредоносных программ. В начале месяца в вирусную базу Dr.Web была добавлена запись для детектирования троянца Android.Click.312.origin, который по команде сервера переходил по ссылкам и загружал различные веб-сайты. Кроме того, вирусные аналитики выявили новых рекламных троянцев Android.HiddenAds, а также загрузчика Android.DownLoader.915.origin — он мог скачивать другие вредоносные приложения.

В конце месяца специалисты «Доктор Веб» обнаружили очередного банковского троянца, который атаковал пользователей из Бразилии. Вредоносная программа, получившая имя Android.Banker.346.origin, использовала специальные возможности (Accessibility Service) ОС Android и могла перехватывать СМС-сообщения.

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

- распространение вредоносных программ через каталог Google Play;
- появление новых нежелательных рекламных модулей.

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

Обзор вирусной активности в августе 2019 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