Dr.WEB®
с 1992 года

Обзор вирусной активности в июле 2019 года

Обзор вирусной активности в июле 2019 года

5 августа 2019 года

В июле статистика серверов Dr.Web зафиксировала снижение роста общего числа обнаруженных угроз на 54.21% по сравнению с июнем. При этом количество уникальных угроз выросло почти в два раза. В почтовом трафике на первых позициях находится вредоносное ПО, использующее уязвимости документов Microsoft Office. Рекламные программы и установщики по-прежнему лидируют по общему количеству обнаруженных угроз. Среди шифровальщиков в июле лидировал Trojan.Encoder.858, на которого пришлось 21.15% всех поступивших в поддержку «Доктор Веб» запросов на расшифровку данных.

Аналитики компании «Доктор Веб» подготовили обзорное исследование, в котором представлены распространенные угрозы для умных устройств и Интернета вещей (IoT) в целом. Обзор наших специалистов основывается на статистических данных, собираемых с 2016 года с зараженных устройств, и призван привлечь внимание к проблеме безопасности в сфере IoT.

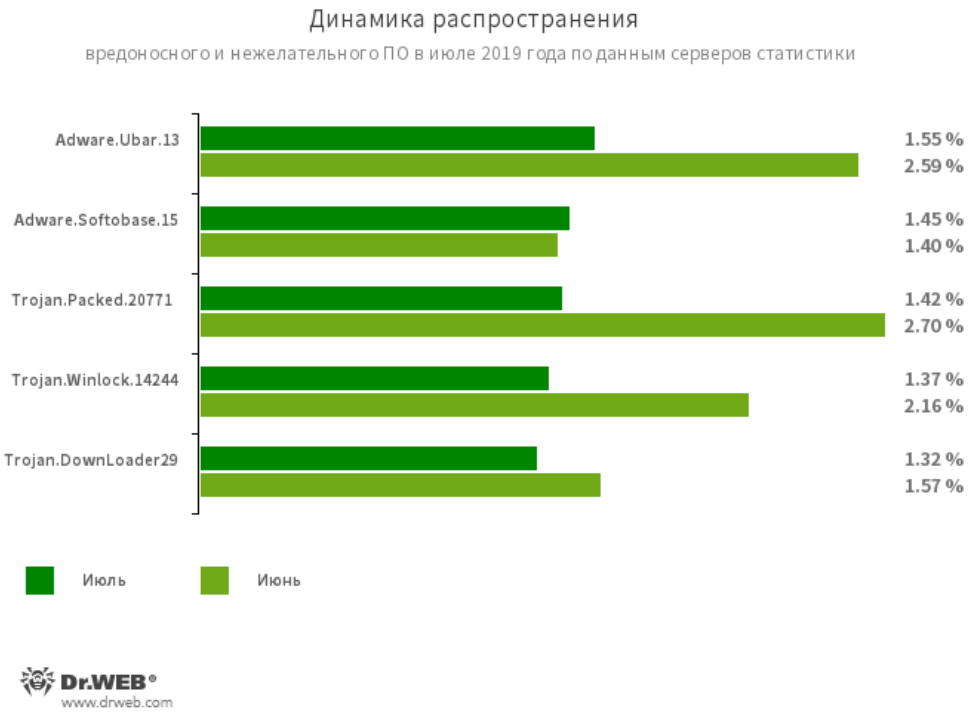
Читать исследование

Главные тенденции июля

- Повышение активности распространения уникального вредоносного ПО
- Снижение активности шифровальщиков

Обзор вирусной активности в июле 2019 года

По данным серверов статистики «Доктор Веб»



Угрозы этого месяца:

- Adware.Ubar.13

Торрент-клиент, устанавливающий нежелательное ПО на устройство.

- Adware.Softobase.15

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

- Trojan.Packed.20771

Устанавливает вредоносные расширения для браузеров, перенаправляющие с результатов выдачи в поисковых системах на другие сайты.

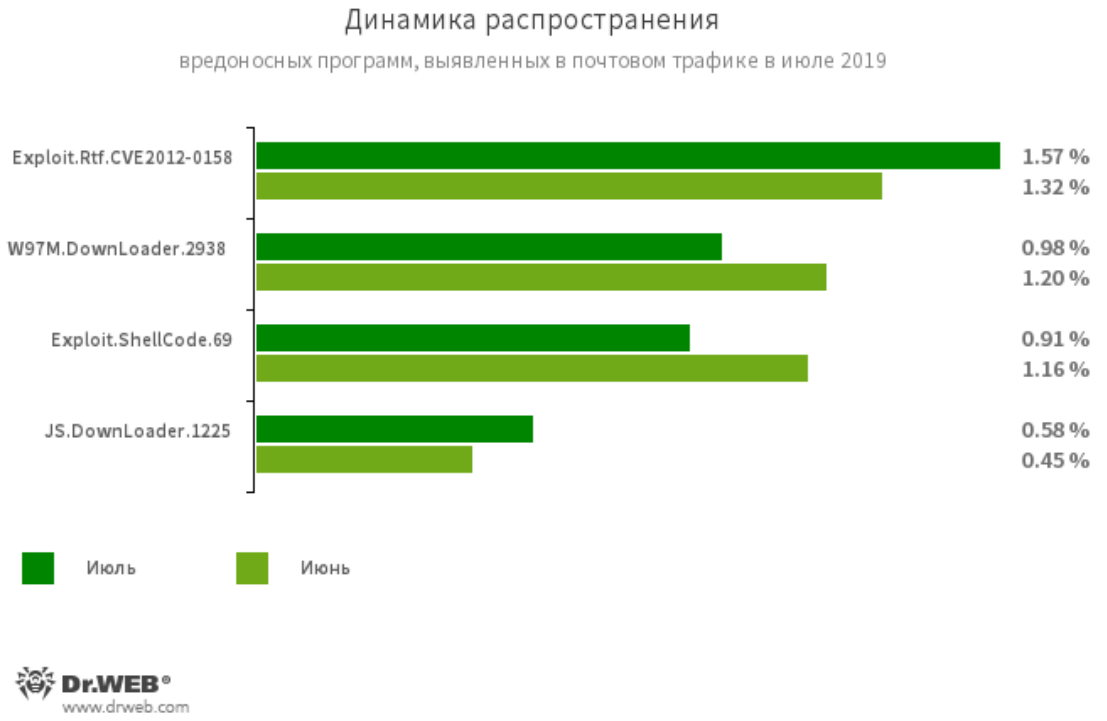
- Trojan.Winlock.14244

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

- Trojan.DownLoader29.14148

Загружает и выполняет вредоносные программы без согласия пользователя.

Статистика вредоносных программ в почтовом трафике



- **Exploit.Rtf.CVE2012-0158**

Измененный документ Microsoft Office Word, использующий для выполнения вредоносного кода уязвимость CVE2012-0158.

- **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.

- **JS.DownLoader.1225**

Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.

Шифровальщики

В июле в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих троянцев-шифровальщиков:

- Trojan.Encoder.858 — 21.15%
- Trojan.Encoder.567 — 9.45%
- Trojan.Encoder.11464 — 8.01%
- Trojan.Encoder.25574 — 4.93%
- Trojan.Encoder.18000 — 3.90%
- Trojan.Encoder.11539 — 3.08%
- Trojan.Encoder.28004 — 1.85%

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 2019 года в базу нерекомендуемых и вредоносных сайтов был добавлен 123 251 интернет-адрес.

Июнь 2019	Июль 2019	Динамика
+ 151 162	+ 123 251	-18.46%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В середине июля компания «Доктор Веб» сообщила о появлении в Google Play опасного троянца Android.Backdoor.736.origin, с помощью которого злоумышленники дистанционно управляли зараженными Android-устройствами. Этот бэкдор мог устанавливать приложения, крал конфиденциальные данные и выполнял другие вредоносные действия по команде вирусописателей.

Среди выявленных угроз были новые троянцы семейства Android.HiddenAds, которые скрывали свои значки с главного экрана и показывали рекламу. Кроме того, аналитики «Доктор Веб» обнаружили несколько программ со встроенным рекламным модулем Adware.HiddenAds.9.origin. Тот отображал баннеры даже если эти приложения были закрыты.

Также вирусная база Dr.Web пополнилась записями для детектирования нескольких троянцев семейства Android.Spy, которые использовались для кибершпионажа

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

- обнаружение опасного бэкдора, выполнявшего команды злоумышленников;
- появление новых вредоносных программ в Google Play;
- распространение троянцев, предназначенных для кибершпионажа.

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

Обзор вирусной активности в июле 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