Dr.WEB®
с 1992 года

Обзор вирусной активности в сентябре 2019 года

Обзор вирусной активности в сентябре 2019 года

9 октября 2019 года

По сравнению с прошлым месяцем в сентябре статистика серверов Dr.Web зафиксировала увеличение общего числа угроз на 19.96%. В то же время доля уникальных угроз снизилась на 50.45%. Чаще всего пользователей атаковали программы для показа рекламы, а также загрузчики и установщики ПО. В почтовом трафике вновь преобладали угрозы, которые для заражения устройств используют уязвимости документов Microsoft Office.

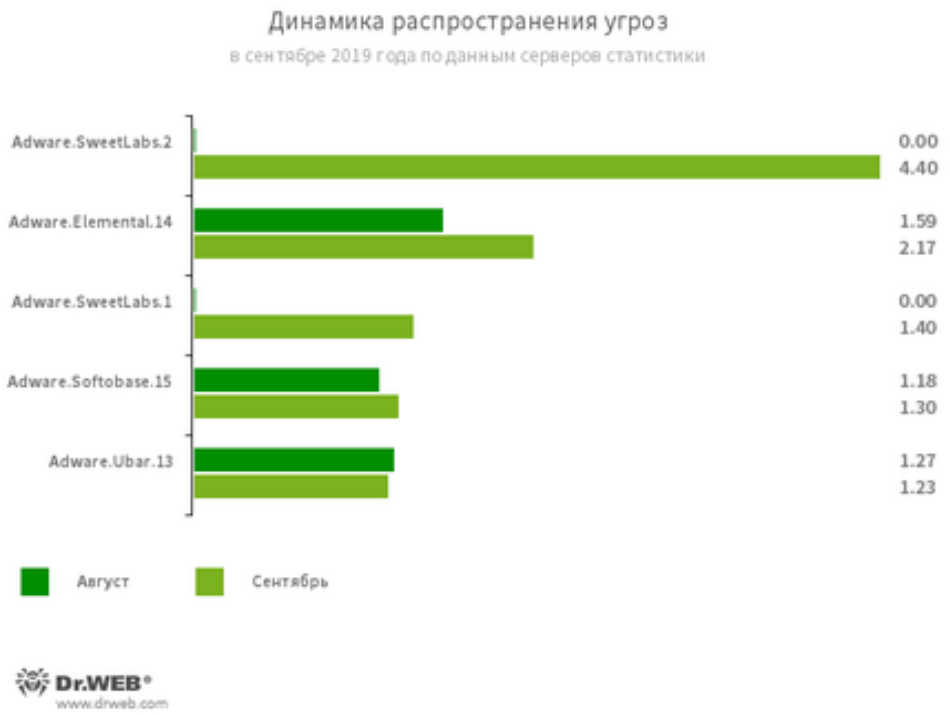
Выросло число обращений пользователей на расшифровку файлов, пострадавших от троянцев-шифровальщиков. При этом самым активным энкодером стал Trojan.Encoder.858 — на его долю пришлось 16.60% всех инцидентов. Кроме того, в базу нерекомендуемых и вредоносных сайтов было внесено почти вдвое больше интернет-адресов, чем в августе.

Главные тенденции сентября

- Рост числа пользователей, пострадавших от шифровальщиков
- Рекламные троянцы и рекламное ПО остаются одними из самых активных угроз

Обзор вирусной активности в сентябре 2019 года

По данным серверов статистики «Доктор Веб»



Наиболее распространенные угрозы сентября:

Adware.SweetLabs.1

Adware.SweetLabs.2

Альтернативный каталог приложений и надстройка к графическому интерфейсу Windows от создателей Adware.Opencandy.

Adware.Elemental.14

Детектирование рекламных программ, которые путем подмены ссылок загружаются с файлообменных сервисов при попытке скачать с них те или иные файлы. Вместо ожидаемых файлов жертвы получают эти приложения, которые показывают рекламу, а также инсталлируют ненужное ПО.

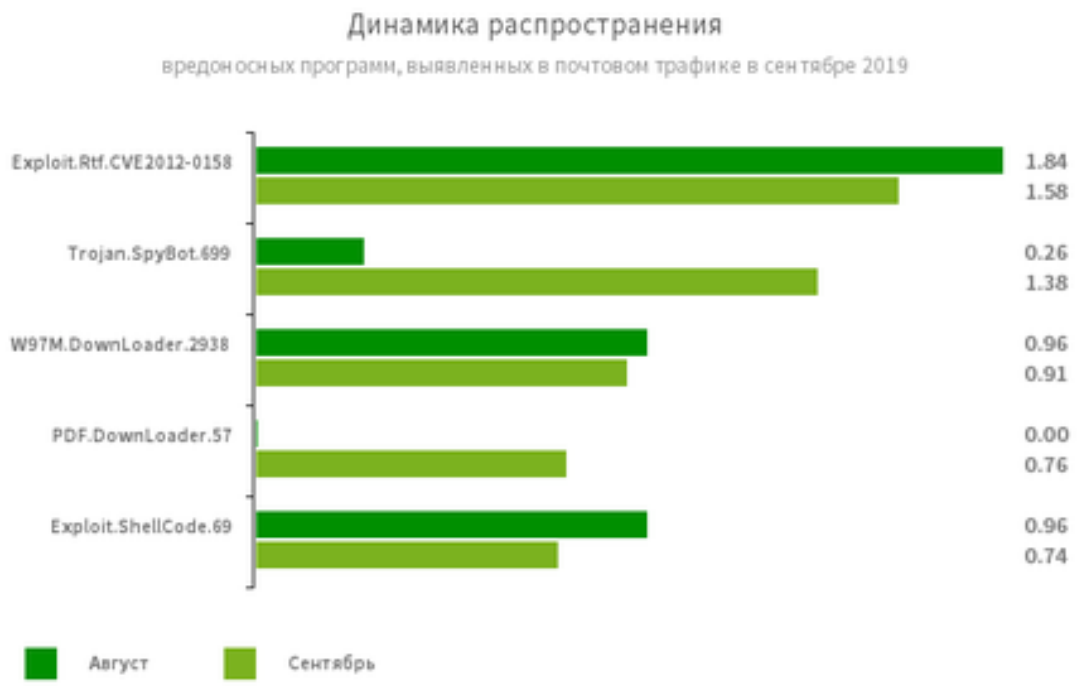
Adware.Softobase.15

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

Adware.Ubar.13

Торрент-клиент, устанавливающий нежелательное ПО на устройство.

Статистика вредоносных программ в почтовом трафике



Exploit.Rtf.CVE2012-0158

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

Trojan.SpyBot.699

Троянец-шпион, способный перехватывать вводимые на клавиатуре символы (кейлоггер).

W97M.DownLoader.2938

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

PDF.DownLoader.57 (новая угроза)

Представитель семейства троянцев-загрузчиков, которые распространяются в специально сформированных документах формата PDF.

Exploit.ShellCode.69

Вредоносный документ Microsoft Office Word. Использует уязвимость CVE-2017-11882.

Шифровальщики

По сравнению с августом в сентябре в службу технической поддержки компании «Доктор Веб» поступило на 14.59% больше запросов на расшифровку файлов от пользователей, пострадавших от троянцев-шифровальщиков.

Чаще всего обращения были связаны со следующими энкодерами:

- Trojan.Encoder.858 — 16.60%
- Trojan.Encoder.11464 — 6.93%
- Trojan.Encoder.11539 — 5.04%
- Trojan.Encoder.25574 — 2.94%
- Trojan.Encoder.10700 — 2.52%
- Trojan.Encoder.567 — 1.89%
- Trojan.Encoder.24383 — 1.47%

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 сентября 2019 года в базу нерекомендуемых и вредоносных сайтов было добавлено 238 637 интернет-адресов.

Август 2019	Сентябрь 2019	Динамика
+ 204 551	+ 238 637	+ 16.66%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В течение сентября в каталоге Google Play было выявлено множество вредоносных программ. В начале месяца вирусные аналитики «Доктор Веб» обнаружили банковского троянца Android.Banker.347.origin, который атаковал пользователей из Бразилии. Он перехватывал СМС-сообщения с одноразовыми кодами и мог загружать мошеннические веб-сайты по команде злоумышленников. Другой банкер, найденный в конце месяца, получил имя Android.Banker.352.origin. Он крал данные авторизации пользователей криптовалютной биржи YoBit.

Среди распространявшихся через Google Play угроз были троянцы-загрузчики Android.DownLoader.920.origin и Android.DownLoader.921.origin, которые скачивали другие вредоносные приложения. Кроме того, вирусные аналитики зафиксировали рекламных троянцев Android.HiddenAds. Помимо них, наши специалисты обнаружили несколько модификаций троянцев семейства Android.Joker. Они подписывали пользователей на дорогостоящие услуги, могли перехватывать СМС и передавали злоумышленникам данные из телефонной книги зараженных устройств. Также эти троянцы скачивали, а потом запускали вспомогательные модули и были способны исполнять произвольный код.

Кроме того, вирусные аналитики выявили новые версии потенциально опасных программ, предназначенных для кибершпионажа.

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

- распространение вредоносных программ через каталог Google Play;
- обнаружение новых версий ПО для кибершпионажа.

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

Обзор вирусной активности в сентябре 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