Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности в сентябре 2021 года

«Доктор Веб»: обзор вирусной активности в сентябре 2021 года

15 октября 2021 года

В сентябре анализ данных статистики Dr.Web показал увеличение общего числа обнаруженных угроз на 58.1% по сравнению с августом. Количество уникальных угроз уменьшилось на 12.2%. Большинство детектирований по-прежнему приходится на долю рекламных программ и нежелательных приложений. В почтовом трафике чаще всего распространялось разнообразное вредоносное ПО, в том числе бэкдоры, позволяющие проводить манипуляции с файловой системой.

Число обращений пользователей за расшифровкой файлов уменьшилось на 11.8% по сравнению с августом. Самым распространенным энкодером месяца стал Trojan.Encoder.26996, на долю которого пришлось 43.79% всех инцидентов.

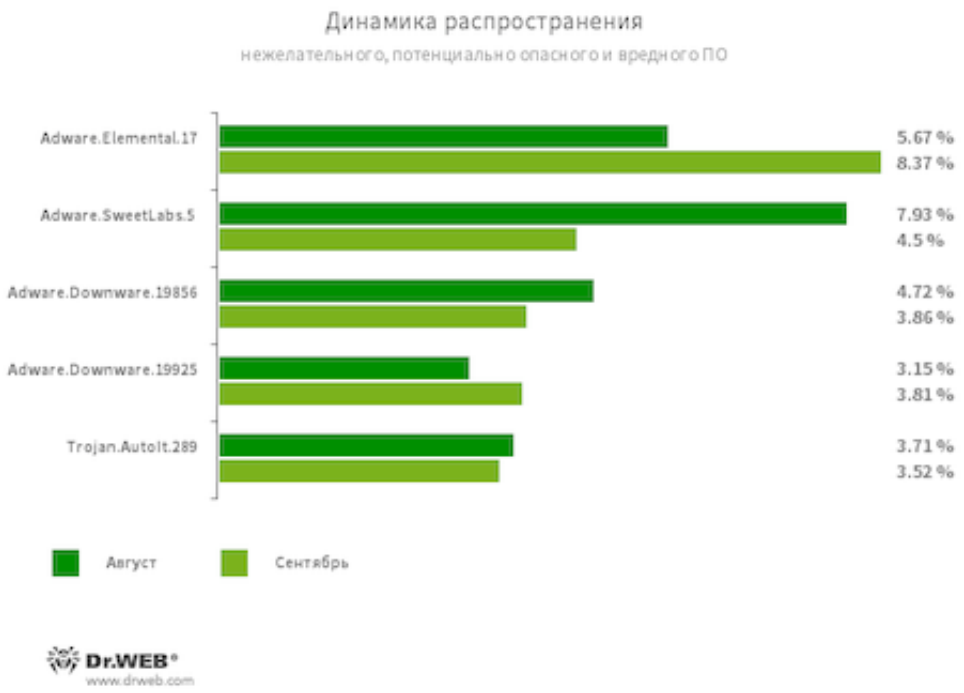
ГЛАВНЫЕ ТЕНДЕНЦИИ СЕНТЯБРЯ

- Существенное увеличение общего числа угроз
- Рекламные приложения по-прежнему остаются главной угрозой
- Распространение вредоносных загрузчиков в почтовом трафике

«Доктор Веб»: обзор вирусной активности в сентябре 2021 года

По данным сервиса статистики «Доктор Веб»

Угрозы прошедшего месяца:



Adware.Elemental.17

Семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают приложения с рекламой, а также инсталлируют ненужное ПО.

Adware.SweetLabs.5

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

Adware.Downware.19856

Adware.Downware.19925

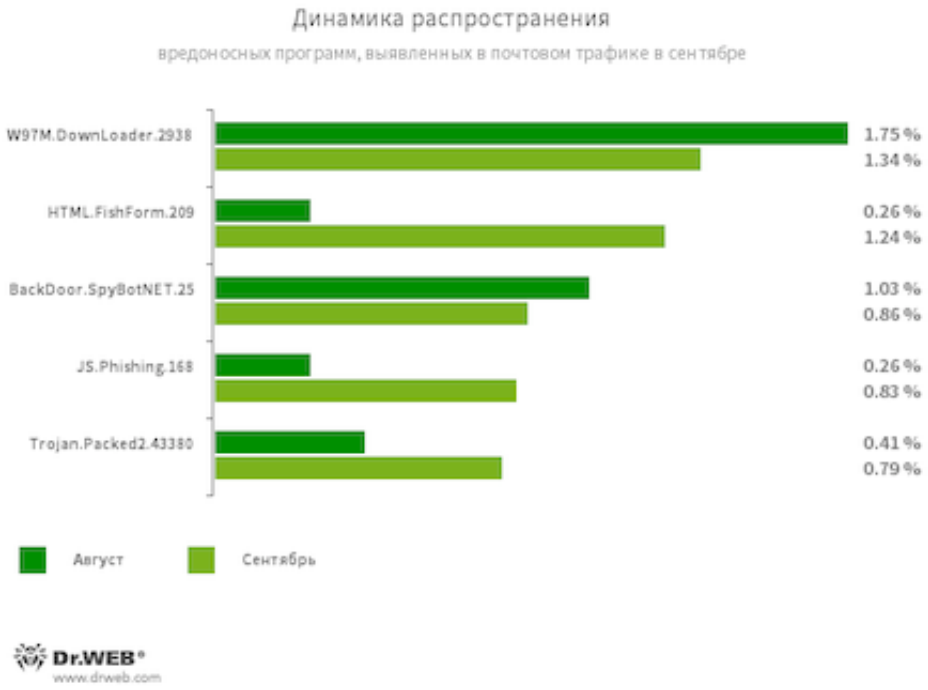
Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Trojan.AutoIt.289

Утилита, написанная на скриптовом языке AutoIt и распространяемая в составе майнера или RAT-трояна. Выполняет различные вредоносные действия, затрудняющие обнаружение основной полезной нагрузки.

«Доктор Веб»: обзор вирусной активности в сентябре 2021 года

Статистика вредоносных программ в почтовом трафике



W97M.DownLoader.2938

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

HTML.FishForm.209

Веб-страница, распространяющаяся посредством фишинговых рассылок. Представляет собой фиктивную форму ввода учетных данных, которая имитирует авторизацию на известных сайтах. Введенные пользователем данные отправляются злоумышленнику.

BackDoor.SpyBotNET.25

Бэкдор, написанный на .NET. Способен манипулировать файловой системой (копирование, удаление, создание директорий и т. д.), завершать процессы и делать снимки экрана.

JS.Phishing.168

Вредоносный сценарий на языке JavaScript, формирующий фишинговую веб-страницу.

Trojan.Packed2.43380

Модификация бэкдора Bladabindi, обфусцированная при помощи упаковщика. Bladabindi – распространенный бэкдор с широкими возможностями для удаленного управления зараженным компьютером.

«Доктор Веб»: обзор вирусной активности в сентябре 2021 года

Шифровальщики

По сравнению с августом, в сентябре число запросов на расшифровку файлов, затронутых шифровальщиками, уменьшилось на 11.8%.

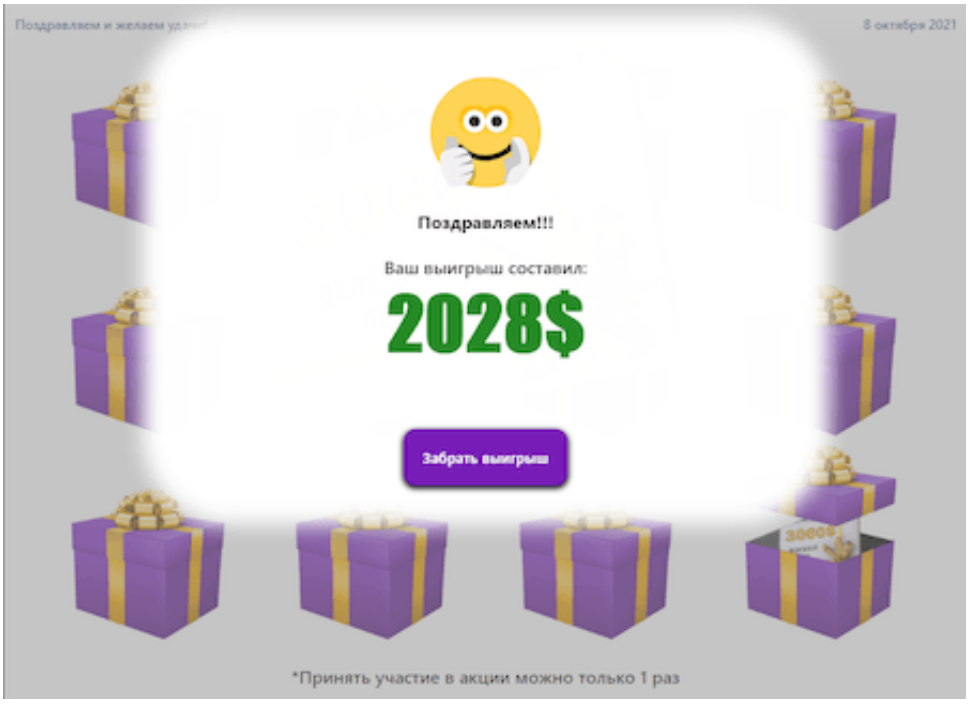
- Trojan.Encoder.26996 — 43.79%
- Trojan.Encoder.567 — 15,86%
- Trojan.Encoder.30356 — 3,45%
- Trojan.Encoder.11539 — 1,03%
- Trojan.Encoder.761 — 1,03%

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 сентябре 2021 года интернет-аналитики «Доктор Веб» заметили увеличение числа сайтов с «выигрышами». Любому случайному посетителю предлагается выбрать 3 случайных подарочных коробки, в одной из которых обязательно будут деньги.



На скриншоте изображена страница, где пользователю предлагается забрать выигрыш. Однако для этого требуется ввести номер банковской карты и другие персональные данные. Далее со «счастливчиком» связываются операторы чата, главная цель которых – выманить у жертвы как можно больше средств. Отправить мошенникам деньги призывают под разными предлогами: комиссия, информационные услуги или даже «налог».

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В сентябре пользователям Android-устройств чаще всего угрожали рекламные трояны, а также вредоносные программы, загружающие другие приложения и выполняющие произвольный код. При этом наши специалисты обнаружили в каталоге Google Play множество новых троянов семейства Android.FakeApp, которые использовались в различных мошеннических схемах.

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

- обнаружение множества новых угроз в каталоге Google Play;
- сохранение активности троянов, предназначенных для загрузки других приложений и выполнения произвольного кода.

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

«Доктор Веб»: обзор вирусной активности в сентябре 2021 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
Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125124 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