Dr.WEB®
с 1992 года

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

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

8 сентября 2021 года

В августе анализ данных статистики Dr.Web показал увеличение общего числа обнаруженных угроз на 16.8% по сравнению с июлем. Количество уникальных угроз увеличилось на 5.6%. Большинство детектирований по-прежнему приходится на долю рекламных программ и нежелательных приложений. В почтовом трафике чаще всего распространяется разнообразное вредоносное ПО, в том числе в виде PDF-файлов.

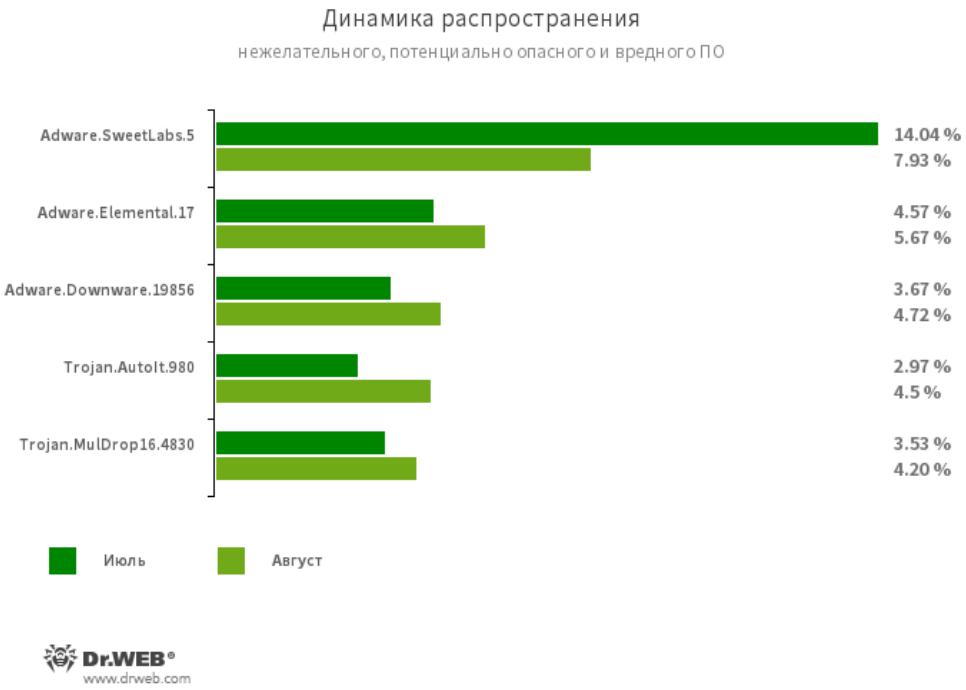
Число обращений пользователей за расшифровкой файлов увеличилось на 4.2% по сравнению с прошлым месяцем. Самым распространенным энкодером августа стал Trojan.Encoder.26996, на долю которого приходится 52.54% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ АВГУСТА

- Увеличение общего числа угроз
- Рекламные приложения по-прежнему остаются главной угрозой
- Распространение вредоносных файлов в почтовом трафике

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

По данным сервиса статистики «Доктор Веб»



Угрозы прошедшего месяца:

Adware.SweetLabs.5

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

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.Downware.19856

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Trojan.Autoit.980

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

Trojan.MulDrop16.4830

Вредоносная программа, загружающая нежелательные приложения на компьютер жертвы.

«Доктор Веб»: обзор вирусной активности в августе 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.

Trojan.PackedNET.964

Упакованное вредоносное ПО, написанное на VB.NET.

BackDoor.SpyBotNET.25

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

PDF.Phisher.267

PDF-документ, использующийся в фишинговой рассылке.

HTML.FishForm.171

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

Шифровальщики

По сравнению с июлем, в августе число запросов на расшифровку файлов, затронутых шифровальщиками, увеличилось на 4.2%.

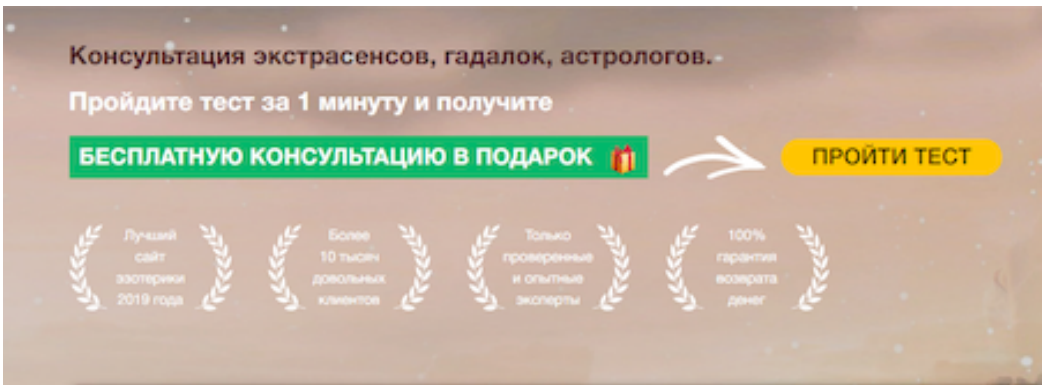
- Trojan.Encoder.26996 — 52,54%
- Trojan.Encoder.567 — 5,07%
- Trojan.Encoder.30356 — 2,13%
- Trojan.Encoder.11539 — 0,80%
- Trojan.Encoder.11432 — 0,27%

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 августе 2021 года интернет-аналитики «Доктор Веб» заметили участившееся распространение ссылок на подозрительные сайты, предлагающие онлайн-услуги экстрасенсов. Консультации «экспертов» в гадании, астрологии и экстрасенсорике стоят немалых денег, а проверить качество оказанной помощи – невозможно.



На скриншоте показана главная страница ресурса, изобилующая клише «лучший сайт», «опытные эксперты» и «гарантия возврата денег», однако в реальности это очередная мошенническая схема с липовыми гадалками, набранными по объявлениям из социальных сетей. Подобные сайты не заблокированы Роскомнадзором, но Dr.Web отправляет их в категорию нерекомендуемых для посещения.

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В августе специалисты компании «Доктор Веб» выявили в каталоге Google Play множество новых угроз. В их числе — вредоносные программы семейства Android.FakeApp, загружающие различные мошеннические сайты. Кроме того, были обнаружены очередные трояны опасного семейства Android.Joker, подписывающие жертв на платные услуги и выполняющие произвольный код. Среди найденных вредоносных программ также оказался троян, похищающий логины и пароли от учетных записей Facebook.

В течение августа антивирусные продукты Dr.Web для Android наиболее часто фиксировали на защищаемых устройствах рекламные вредоносные приложения, а также троянов, загружающих другое ПО.

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

- обнаружение новых угроз в каталоге Google Play;
- рекламные трояны и вредоносные приложения, загружающее другое ПО, остаются одними из самых активных угроз.

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

«Доктор Веб»: обзор вирусной активности в августе 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

Узнайте больше
Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека