Dr.WEB

«Доктор Веб»: обзор вирусной активности в августе 2022 года

«Доктор Веб»: обзор вирусной активности в августе 2022 года

15 сентября 2022 года

В августе анализ данных статистики антивируса Dr.Web показал рост общего числа обнаруженных угроз на 10,72% по сравнению с июлем. Количество уникальных угроз также увеличилось — на 8,59%. Наиболее часто пользователи сталкивались со всевозможными рекламными приложениями. В почтовом трафике преобладали вредоносные скрипты, троянские программы, загружающие другие вредоносные приложения, а также фишинговые веб-страницы, предназначенные для кражи аутентификационных данных. Кроме того, злоумышленники продолжили распространять в почтовых вложениях программы, использующие уязвимости документов Microsoft Office.

В минувшем месяце число обращений пользователей за расшифровкой файлов снизилось на 2,57%. При этом лидером среди энкодеров в очередной раз стал Trojan.Encoder.26996 — на его долю пришлось 32,24% всех инцидентов.

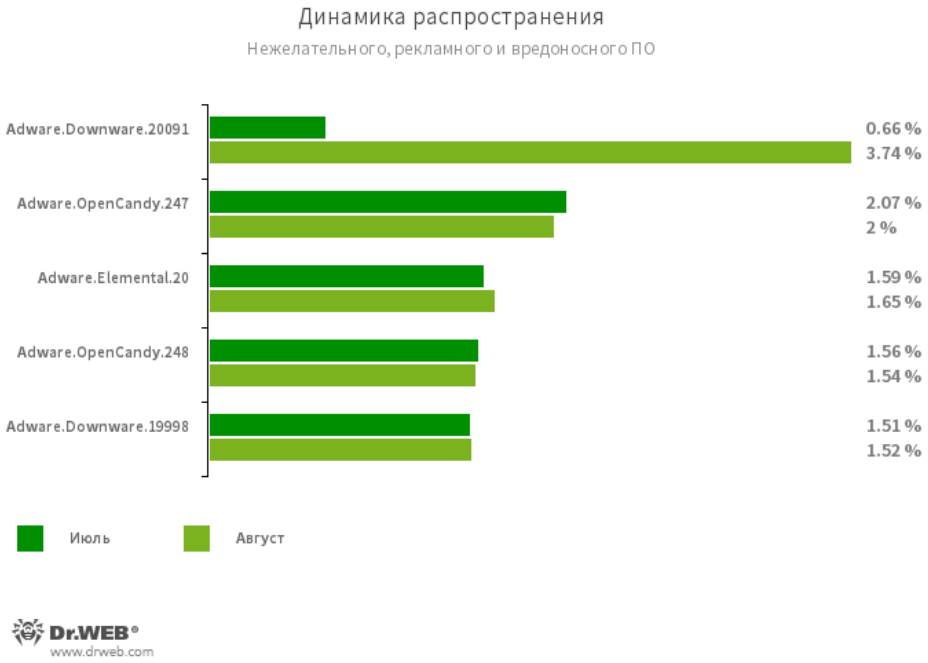
Среди угроз для мобильных устройств высокая активность вновь наблюдалась со стороны троянских приложений и программ, предназначенных для демонстрации нежелательной рекламы.

ГЛАВНЫЕ ТЕНДЕНЦИИ АВГУСТА

- Рост общего числа обнаруженных угроз
- Рекламные приложения остаются одними из наиболее распространенных угроз
- Снижение числа обращений пользователей за расшифровкой файлов, пострадавших от троянов-шифровальщиков.

«Доктор Веб»: обзор вирусной активности в августе 2022 года

По данным сервиса статистики «Доктор Веб»



Угрозы прошедшего месяца:

Adware.Downware.20091

Adware.Downware.19998

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Adware.OpenCandy.247

Adware.OpenCandy.248

Семейство приложений, предназначенных для установки на компьютер различного дополнительного рекламного ПО.

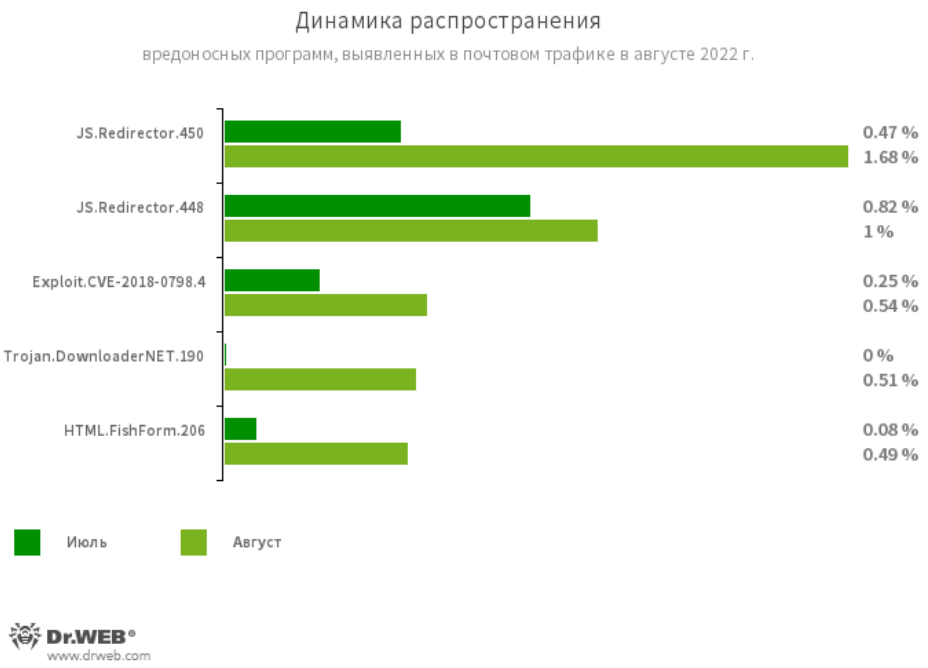
Adware.Elemental.20

Семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают эти приложения, которые показывают рекламу, а также устанавливают ненужное ПО.

«Доктор Веб»: обзор вирусной активности в августе 2022 года

Статистика вредоносных программ в почтовом трафике

.



JS.Redirector.448

JS.Redirector.450

Вредоносные сценарии на языке JavaScript, размещаемые в коде веб-страниц. Предназначены для перенаправления пользователей на фишинговые или рекламные сайты.

Exploit.CVE-2018-0798.4

Эксплойт, предназначенный для эксплуатации уязвимости в ПО Microsoft Office и позволяющий выполнить произвольный код.

Trojan.DownloaderNET.190

Троянская программа, предназначенная для загрузки других вредоносных приложений на целевые компьютеры.

HTML.FishForm.206

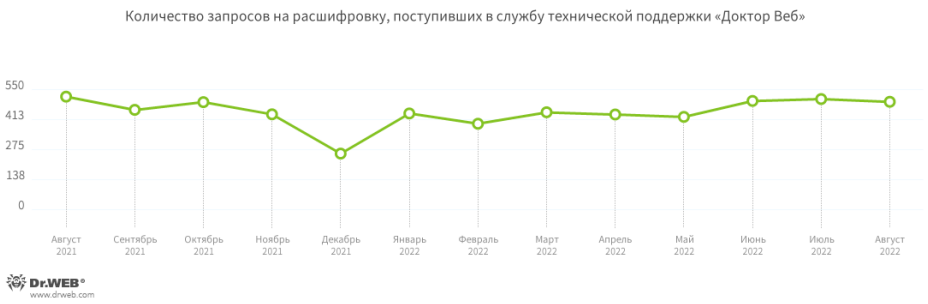
Веб-страница, распространяющаяся посредством фишинговых рассылок. Представляет собой фиктивную форму ввода учетных данных, которая имитирует авторизацию на известных сайтах. Введенные пользователем данные отправляются злоумышленникам.

«Доктор Веб»: обзор вирусной активности в августе 2022 года

Шифровальщики

.

В августе число запросов на расшифровку файлов, затронутых троянами-шифровальщиками, снизилось на 2,57% по сравнению с июлем.



- Trojan.Encoder.26996 — 32.24%
- Trojan.Encoder.3953 — 12.17%
- Trojan.Encoder.30356 — 3.95%
- Trojan.Encoder.567 — 2.96%
- Trojan.Encoder.11539 — 1.97%

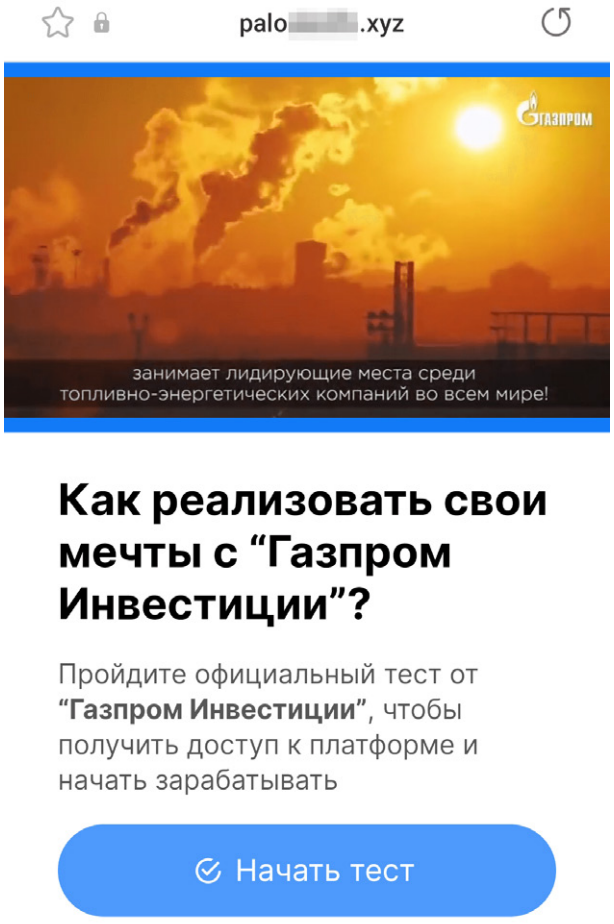
Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

Настрой-ка Dr.Web от шифровальщиков
Обучающий курс
О бесплатном восстановлении
Dr.Web Rescue Pack

Опасные сайты

В августе сохранялась высокая активность интернет-мошенников. Например, они вновь заманивали потенциальных жертв на псевдоинвестиционные сайты, якобы имеющие отношение к крупным российским компаниям финансового и нефтегазового сектора. На таких ресурсах пользователям в качестве «билета» в мир инвестиций может предлагаться пройти простой опрос, зарегистрировать учетную запись, предоставив персональную информацию, и ждать звонка «менеджера». Если пользователи поверят в обещанное, то сами передадут неизвестной стороне свои данные. При этом им могут начать поступать нежелательные звонки как от мошенников, притворяющихся сотрудниками банка, так и представителей компаний, рекламирующих собственные услуги.

Пример одного из таких сайтов. Вначале посетителям предлагается пройти тест, ответы на вопросы которого на самом деле никак не влияют на итоговый результат. После этого якобы открывается эксклюзивный доступ к инвестиционной платформе крупного российского банка. В конце требуется оставить свои контактные данные — имя и фамилию, номер мобильного телефона и адрес электронной почты. Указав данные, пользователи видят сообщение об успешной регистрации и информацию о том, что с ними в ближайшее время свяжется «эксперт».



Опасные сайты

Вы успешно зарегистрировались

Наш эксперт свяжется с Вами в течение дня!

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В августе наблюдался рост активности троянов и программ, созданных для демонстрации нежелательной рекламы на Android-устройствах. Также возросла активность специализированных программных платформ, позволяющих запускать Android-приложения без их установки. Вместе с тем продолжилось снижение активности трояна Android.Spy.4498, похищающего информацию из уведомлений от других приложений.

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

- рост активности вредоносных и других программ, предназначенных для показа нежелательной рекламы;
- снижение активности трояна-шпиона Android.Spy.4498.

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

«Доктор Веб»: обзор вирусной активности в августе 2022 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