Dr.WEB

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

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

31 августа 2022 года

В июле анализ данных статистики антивируса Dr.Web показал снижение общего числа обнаруженных угроз на 11,04% по сравнению с июнем. При этом количество уникальных угроз увеличилось на 16,74%. Чаще всего пользователям угрожали различные рекламные приложения. В почтовом трафике вновь преобладали вредоносные скрипты, а также программы, использующие уязвимости документов Microsoft Office.

В предыдущем месяце число обращений пользователей за расшифровкой файлов выросло на 1,81%. Лидерство среди энкодеров по-прежнему удерживает Trojan.Encoder.26996, на долю которого пришлось 28,65% всех инцидентов.

Наиболее распространенными угрозами для Android-устройств вновь стали рекламные троянские программы Android.HiddenAds, а также троян Android.Spy.4498, который похищает информацию из уведомлений от других приложений. Кроме того, вирусные аналитики компании «Доктор Веб» выявили вредоносные программы в прошивке нескольких моделей смартфонов. Обнаруженные угрозы использовались для атаки на мессенджеры WhatsApp и WhatsApp Business.

ГЛАВНЫЕ ТЕНДЕНЦИИ ИЮЛЯ

- Снижение общего числа обнаруженных угроз
- Сохранение высокой активности рекламных приложений
- Рост числа обращений пользователей за расшифровкой файлов, пострадавших от троянов-шифровальщиков.

«Доктор Веб»: обзор вирусной активности в июле 2022 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.OpenCandy.247
- Adware.OpenCandy.248

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

- Adware.Elemental.20

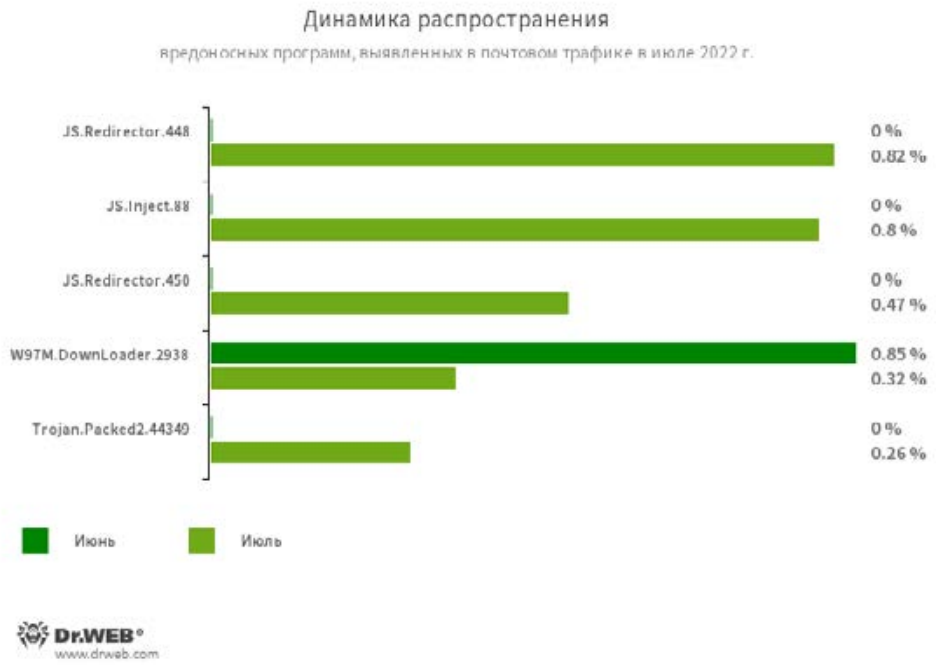
Семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают эти приложения, которые показывают рекламу, а также устанавливают ненужное ПО.

- Adware.Downware.19998

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

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

Статистика вредоносных программ в почтовом трафике



- Redirector.448
- JS.Redirector.450

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

- JS.Inject

Семейство вредоносных сценариев, написанных на языке JavaScript. Они встраивают вредоносный скрипт в HTML-код веб-страниц.

- Trojan.Packed2.44349

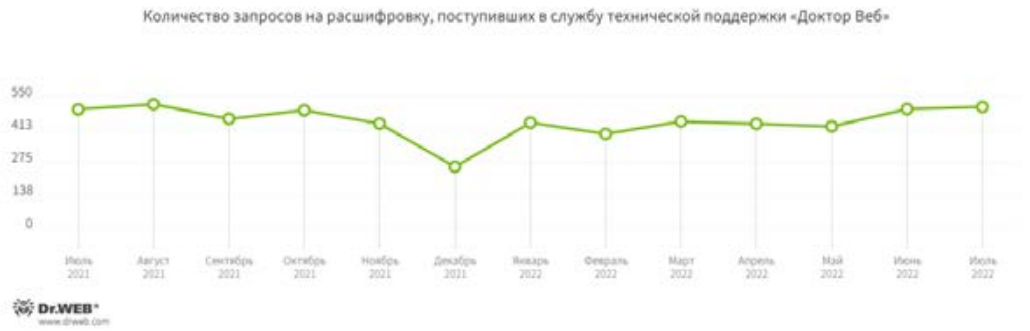
Детектирование вредоносных приложений, защищенных программным упаковщиком.

- W97M.DownLoader.2938

Семейство троянов-загрузчиков, использующих уязвимости документов Microsoft Office. Они предназначены для загрузки других вредоносных программ на атакуемый компьютер.

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

Шифровальщики



В июле число запросов на расшифровку файлов, затронутых троянами-шифровальщиками, выросло на 1,81% по сравнению с июнем.

- Trojan.Encoder.26996 — 28.65%
- Trojan.Encoder.3953 — 12.20%
- Trojan.Encoder.567 — 5.67%
- Trojan.Encoder.30356 — 3.35%
- Trojan.Encoder.11539 — 3.05%

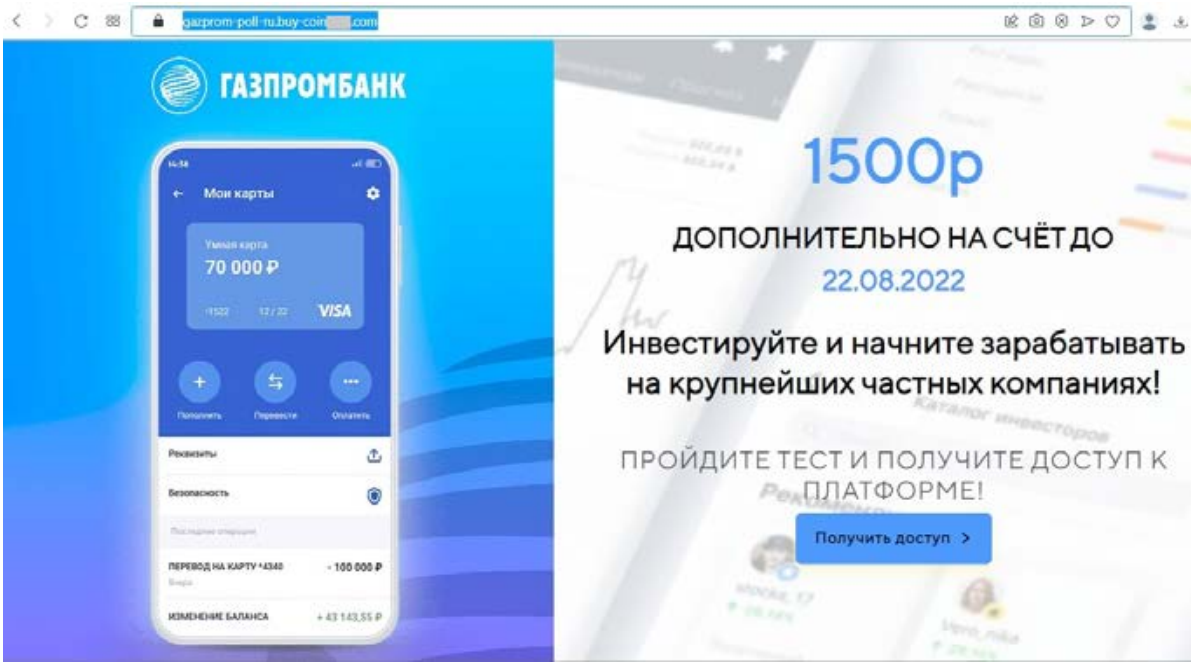
Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

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

Опасные сайты

В прошлом месяце интернет-аналитики компании «Доктор Веб» вновь наблюдали высокую активность киберпреступников, которые массово распространяли фишинговые письма со ссылками на мошеннические сайты. Популярностью среди злоумышленников по-прежнему пользуются подделки сайтов известных банков, онлайн-магазинов, нефтегазовых, транспортных и других компаний. На них потенциальным жертвам традиционно предлагается, например, стать инвесторами или получить оплату за доставленный покупателю товар. Главная цель мошенников остается неизменной — им нужна конфиденциальная информация пользователей, включая данные банковских карт, а также их деньги.

Пример мошеннического сайта, якобы принадлежащего крупной российской кредитной организации. На нем указано, что пользователи после прохождения «теста» якобы смогут получить доступ к специализированной инвестиционной платформе.



Пример поддельного сайта транспортной компании. На нем для каждого посетителя генерируется уникальная страница с персональной информацией и ссылкой, при переходе по которой якобы станет возможно получить оплату за доставленный товар.

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

Опасные сайты

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В июле наиболее распространенной Android-угрозой, выявленной на защищаемых устройствах, вновь стала троянская программа Android.Spy.4498, похищающая информацию из уведомлений от других приложений. Тем не менее, ее активность продолжает постепенно снижаться. В то же время в прошлом месяце наблюдался рост активности одной из ее модификаций, Android.Spy.4837. Одними из самых распространенных Android-угроз по-прежнему остаются троянские программы, демонстрирующие рекламу.

В прошлом месяце наши специалисты обнаружили атаку на пользователей мессенджеров WhatsApp и WhatsApp Business. В ней были задействованы вредоносные приложения, заражающие прошивку ряда моделей Android-смартфонов.

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

- снижение активности трояна-шпиона Android.Spy.4498;
- рекламные трояны остаются одними из самых распространенных Android-угроз;
- выявлена атака на пользователей мессенджеров WhatsApp и WhatsApp Business.

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

«Доктор Веб»: обзор вирусной активности в июле 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