Dr.WEB

«Доктор Веб»:

обзор вирусной активности в декабре 2022 года

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

27 января 2023 года

Анализ статистики детектирований антивируса Dr.Web в декабре показал рост общего числа обнаруженных угроз на 14,02% по сравнению с ноябрем. Число уникальных угроз при этом также увеличилось — на 2,2%. Наиболее активными по-прежнему остаются рекламные приложения. В почтовом трафике чаще всего встречались вредоносные скрипты, ПО для эксплуатации различных уязвимостей, а также рекламные программы.

Число обращений пользователей за расшифровкой файлов снизилось на 1,5% по сравнению с предыдущим месяцем. Наиболее часто жертвы энкодеров сталкивались с такими троянскими программами как Trojan.Encoder.3953, Trojan.Encoder.26996 и Trojan.Encoder.34027.

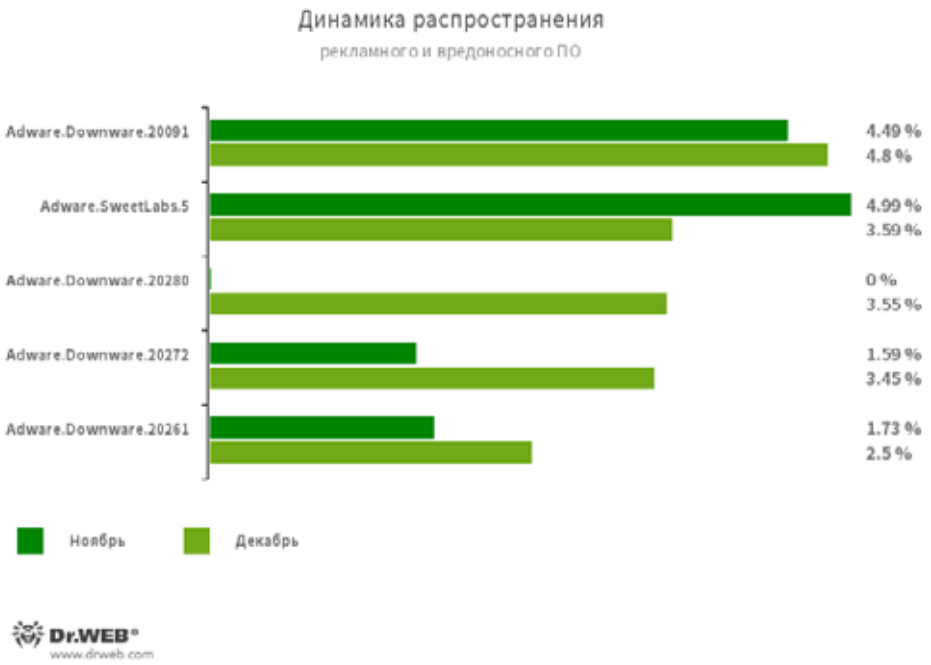
Кроме того, в декабре вирусные аналитики компании «Доктор Веб» вновь выявили многочисленные угрозы в каталоге Google Play. Среди них были как троянские, так и нежелательные приложения.

ГЛАВНЫЕ ТЕНДЕНЦИИ ДЕКАБРЯ

- Рост общего числа обнаруженных угроз
- Снижение количества обращений пользователей за расшифровкой файлов, пострадавших от троянов-шифровальщиков
- Обнаружение множества угроз в каталоге Google Play.

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

По данным сервиса статистики «Доктор Веб»



Угрозы прошедшего месяца:

Adware.Downware.20091

Adware.Downware.20261

Adware.Downware.20272

Adware.Downware.20280

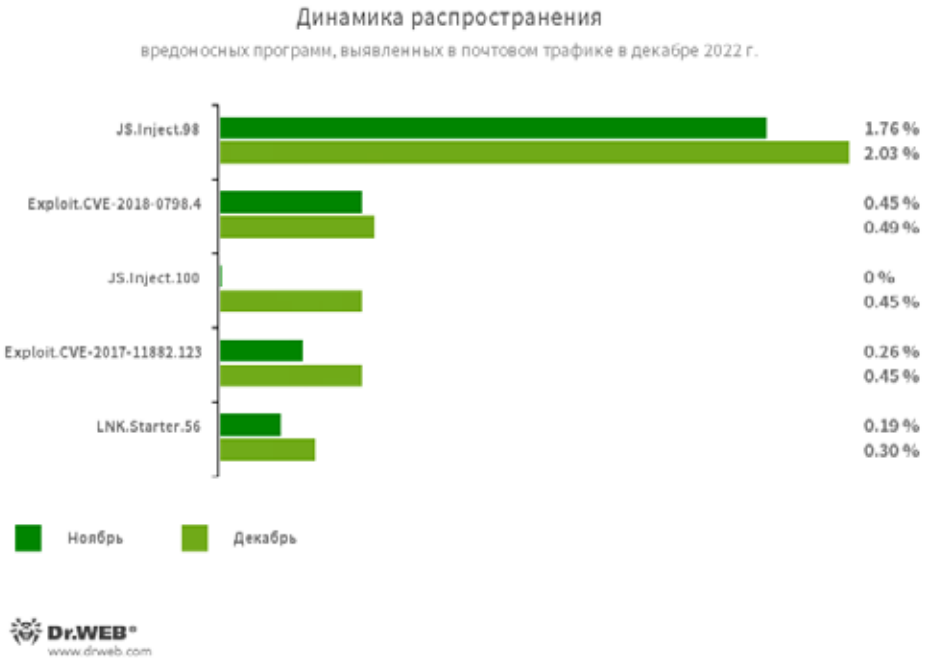
Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Adware.SweetLabs.5

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

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

Статистика вредоносных программ в почтовом трафике



JS.Inject

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

Exploit.CVE-2018-0798.4

Exploit.CVE-2017-11882.123

Эксплойты для использования уязвимостей в ПО Microsoft Office, позволяющие выполнить произвольный код.

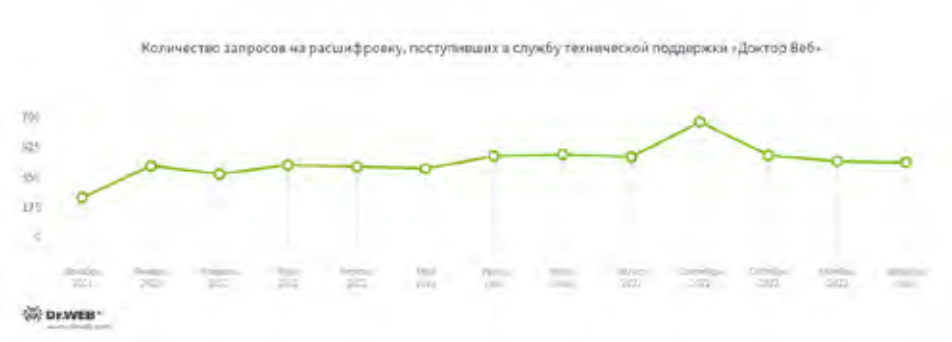
LNK.Starter.56

Детектирование специальным образом сформированного ярлыка, который распространяется через съемные накопители и для введения пользователей в заблуждение имеет значок диска. При его открытии происходит запуск вредоносных VBS-скриптов из скрытого каталога, расположенного на том же носителе, что и сам ярлык.

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

Шифровальщики

В минувшем месяце число запросов на расшифровку файлов, поврежденных троянами-шифровальщиками, снизилось на 1,5% по сравнению с ноябрем.

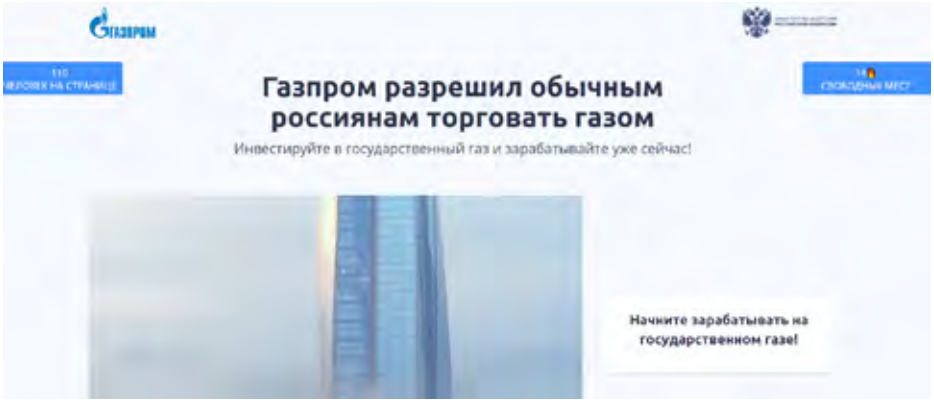


- Trojan.Encoder.3953 — 22.98%
- Trojan.Encoder.26996 — 18.12%
- Trojan.Encoder.34027 — 6.80%
- Trojan.Encoder.30356 — 1.94%
- Trojan.Encoder.35209 — 1.94%

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

Опасные сайты

В прошлом месяце интернет-аналитики «Доктор Веб» вновь наблюдали рост числа сайтов, которые маскировались под веб-ресурсы крупных российских нефтегазовых и других компаний. На них потенциальным жертвам предлагается выгодно вложить деньги в те или иные проекты.



На скриншоте изображен пример одного из таких сайтов. Мошенники предлагают пользователям торговать газом, при этом на странице расположены ложные счетчики посещения и количества оставшихся для регистрации свободных мест. Второй счетчик показывает, что мест якобы практически не осталось. Этот прием применяется для того, чтобы жертвы совершили так называемую спонтанную или импульсную покупку — согласились с предложением под влиянием эмоций. Чтобы «начать» торговлю, от посетителей сайта требуется указать персональные данные.

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в заключительном месяце 2022 года возросла активность рекламных троянских приложений, а также шпионских программ. При этом в течение декабря в каталоге Google Play вновь было выявлено множество новых угроз. Среди них — опасные трояны Android.Joker, которые подписывали жертв на платные услуги, программы-подделки Android.FakeApp, применяемые в различных мошеннических схемах, а также нежелательное ПО.

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

- рост активности рекламных троянских программ и шпионских приложений;
- появление очередных угроз в каталоге Google Play.

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

«Доктор Веб»: обзор вирусной активности в декабре 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