«Доктор Веб»:

обзор вирусной активности
в январе 2023 года

«Доктор Веб»: обзор вирусной активности в январе 2023 года

2 марта 2023 года

Анализ статистики детектирований антивируса Dr.Web в январе 2023 года показал снижение общего числа обнаруженных угроз на 4,47% по сравнению с декабрем. В то же время число уникальных угроз, напротив, увеличилось на 4,26%. Наиболее активными оставались всевозможные рекламные приложения. В почтовом трафике чаще всего выявлялись вредоносные скрипты, а также программы, эксплуатирующие различные уязвимости.

Число обращений пользователей за расшифровкой файлов увеличилось на 5,01% по сравнению с предыдущим месяцем. Чаще всего жертвы троянов-шифровальщиков сталкивались с энкодерами Trojan.Encoder.26996, Trojan.Encoder.3953 и Trojan.Encoder.35209.

В течение января вирусная лаборатория «Доктор Веб» зафиксировала появление множества новых угроз в каталоге Google Play. Среди них были десятки мошеннических программ, а также очередные троянские приложения, подписывающие жертв на платные услуги.

ГЛАВНЫЕ ТЕНДЕНЦИИ ЯНВАРЯ

- Снижение общего числа обнаруженных угроз
- Рост количества обращений пользователей за расшифровкой файлов, пострадавших от троянов-шифровальщиков
- Появление десятков новых угроз в каталоге Google Play

«Доктор Веб»: обзор вирусной активности в январе 2023 года

По данным сервиса статистики «Доктор Веб»

Угрозы января:

Adware.Downware.20091

Adware.Downware.20280

Adware.Downware.20261

Adware.Downware.20272

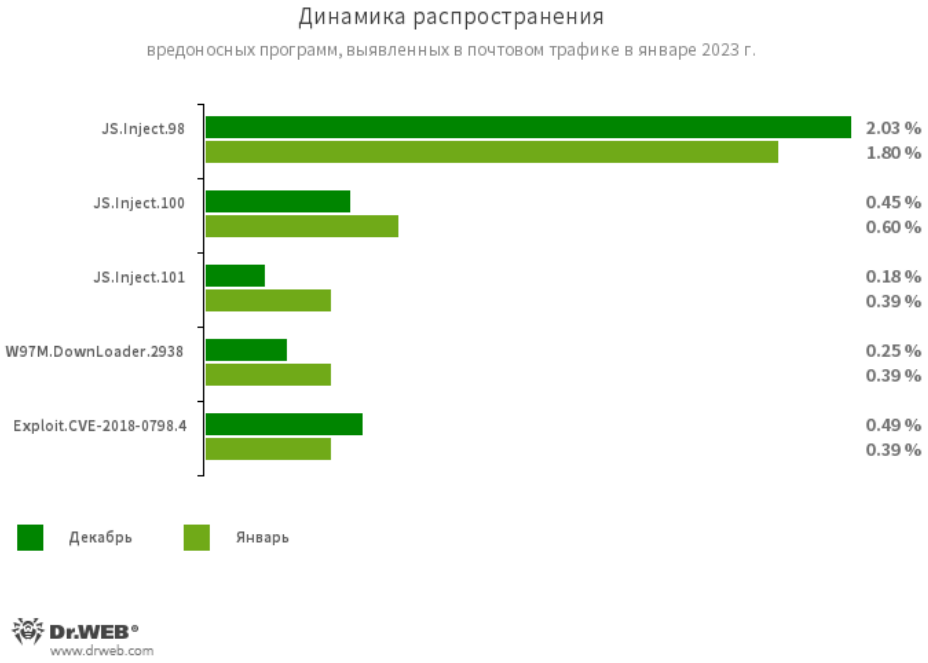
Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Trojan.BPlug.4087

Детектирование вредоносного компонента браузерного расширения WinSafe. Этот компонент представляет собой сценарий JavaScript, который открывает навязчивую рекламу в браузерах.

«Доктор Веб»: обзор вирусной активности в январе 2023 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.

W97M.DownLoader.2938

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

Exploit.CVE-2018-0798.4

Эксплойт для использования уязвимостей в ПО Microsoft Office, позволяющий выполнить произвольный код.

«Доктор Веб»: обзор вирусной активности в январе 2023 года

Шифровальщики

В январе число запросов на расшифровку файлов, поврежденных троянами-шифровальщиками, увеличилось на 5,01% по сравнению с декабрем.

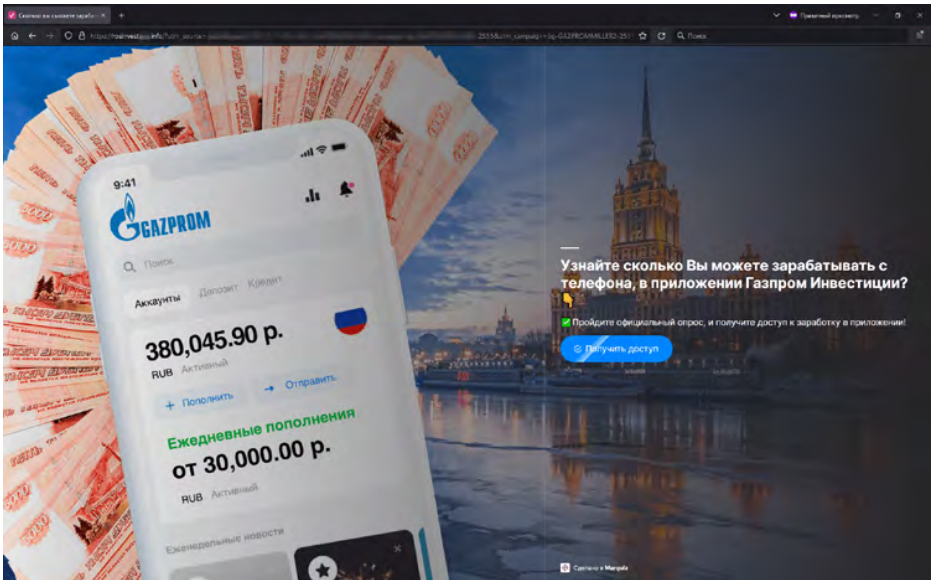
- Trojan.Encoder.26996 — 22.43%
- Trojan.Encoder.3953 — 19.39%
- Trojan.Encoder.35209 — 5.45%
- Trojan.Encoder.34027 — 4.55%
- Trojan.Encoder.35534 — 3.64%

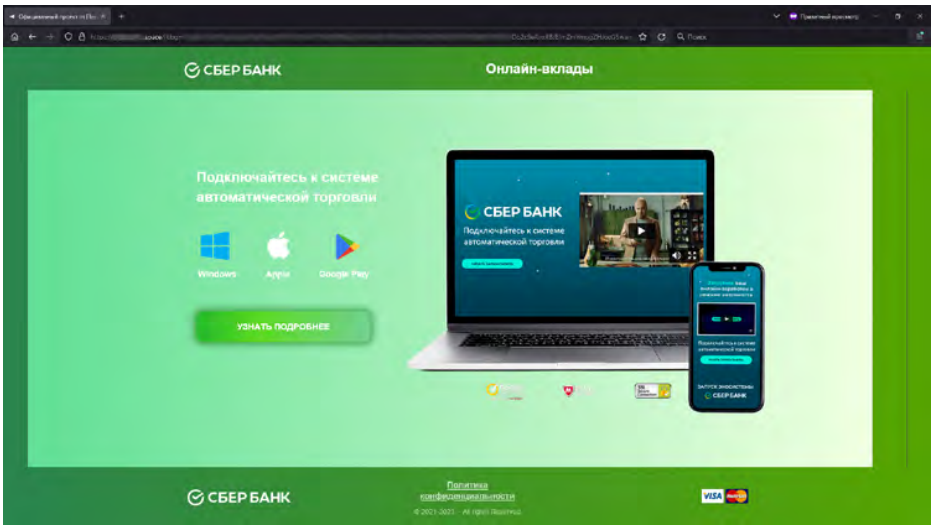
Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

«Доктор Веб»: обзор вирусной активности в январе 2023 года

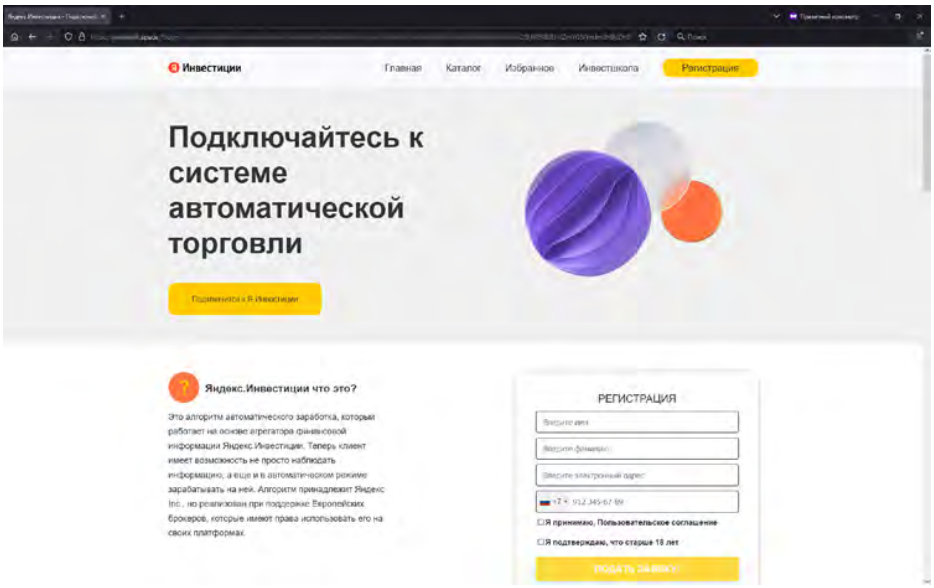
Опасные сайты

В январе 2023 года интернет-аналитики компании «Доктор Веб» отмечали очередной рост числа мошеннических сайтов, в частности — фишинговых ресурсов инвестиционной тематики. Злоумышленники предлагали потенциальным жертвам улучшить свое материальное положение через вложения в те или иные финансовые инструменты. Например, им предлагалось зарегистрировать учетную запись в определенных сервисах, которые якобы принадлежали крупным российским компаниям. На самом деле такие ресурсы были поддельными, и указанная на них персональная информация поступала мошенникам.





Опасные сайты



На скриншотах представлены примеры мошеннических веб-сайтов, имитирующих официальные сервисы крупных российских компаний. На таких сайтах потенциальным жертвам могут предлагать пройти предварительный опрос или же сразу зарегистрировать «учетную запись», указав персональные данные в специальной форме.

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 январе 2023 года вновь наблюдалась повышенная активность троянских приложений, демонстрирующих нежелательную рекламу. Кроме того, на защищаемых устройствах чаще выявлялись банковские троянские приложения, а также программы-вымогатели. Вместе с тем вирусная лаборатория компании «Доктор Веб» зафиксировала появление десятков новых угроз в каталоге Google Play. Среди них были всевозможные мошеннические программы Android.FakeApp, а также троянские приложения Android.Joker и Android.Harly, которые подписывали жертв на платные услуги.

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

- рост активности рекламных троянских программ, банковских троянов и программ-вымогателей.
- появление очередных угроз в каталоге Google Play.

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

«Доктор Веб»: обзор вирусной активности в январе 2023 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