«Доктор Веб»:

обзор вирусной активности
в феврале 2023 года

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

6 апреля 2023 года

Анализ статистики детектирований антивируса Dr.Web в феврале 2023 года показал рост общего числа обнаруженных угроз на 22,29% по сравнению с январем. Число уникальных угроз при этом увеличилось на 34,02%. Чаще всего детектировались всевозможные рекламные приложения и троянские программы различных семейств. В почтовом трафике наиболее часто выявлялись вредоносные скрипты и программы, эксплуатирующие уязвимости в ПО Microsoft Office. Кроме того, через сообщения электронной почты активно распространялись фишинговые HTML-файлы, которые имитировали авторизацию на известных сайтах с целью хищения аутентификационных данных.

Число обращений пользователей за расшифровкой файлов снизилось на 17,63% по сравнению с предыдущим месяцем. Наиболее часто жертв троянов-шифровальщиков атаковали энкодеры Trojan.Encoder.3953, Trojan.Encoder.26996 и Trojan.Encoder.35534.

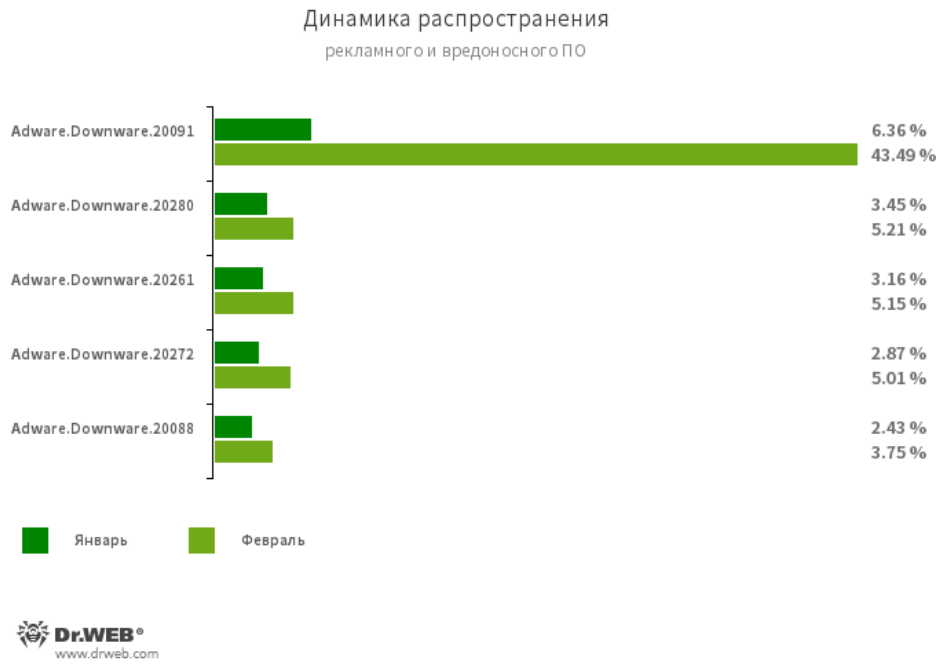
В течение февраля специалисты компании «Доктор Веб» выявили десятки новых вредоносных приложений в Google Play. Среди них — множество программ-подделок, способных загружать всевозможные мошеннические и нежелательные сайты, а также трояны, которые подписывали пользователей Android-устройств на платные услуги.

ГЛАВНЫЕ ТЕНДЕНЦИИ ФЕВРАЛЯ

- Рост общего числа обнаруженных угроз
- Снижение количества обращений пользователей за расшифровкой файлов, пострадавших от троянских программ-шифровальщиков
- Обнаружение множества новых вредоносных приложений в каталоге Google Play

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

По данным сервиса статистики «Доктор Веб»



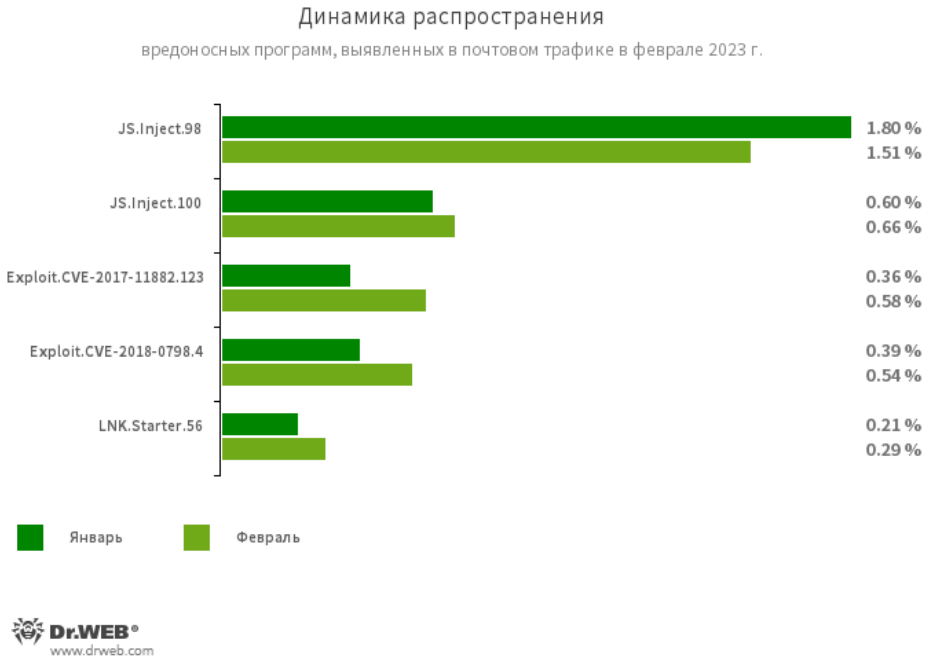
Наиболее распространенные угрозы февраля:

Adware.Downware.20091
Adware.Downware.20280
Adware.Downware.20261
Adware.Downware.20272
Adware.Downware.20088

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

«Доктор Веб»: обзор вирусной активности в феврале 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.

Exploit.CVE-2017-11882.123

Exploit.CVE-2018-0798.4

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

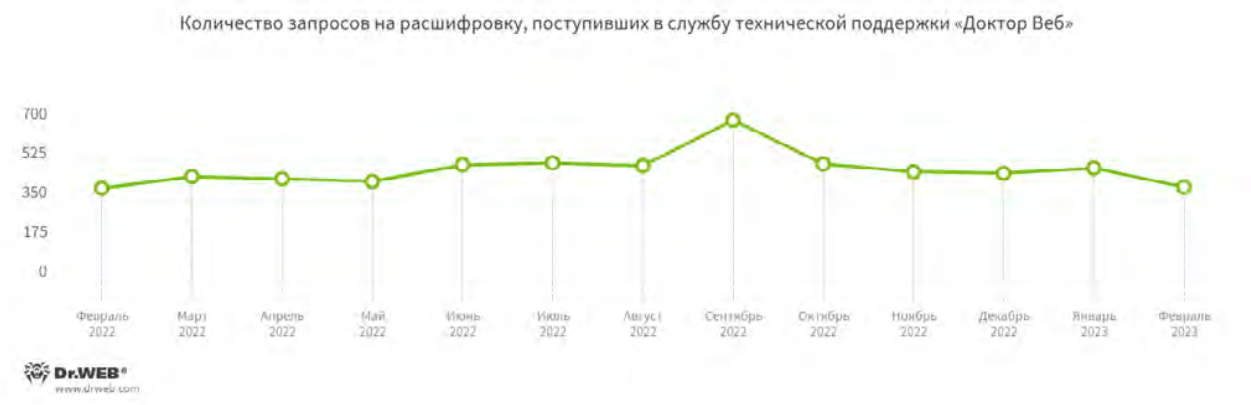
LNK.Starter.56

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 феврале 2023 года

Шифровальщики

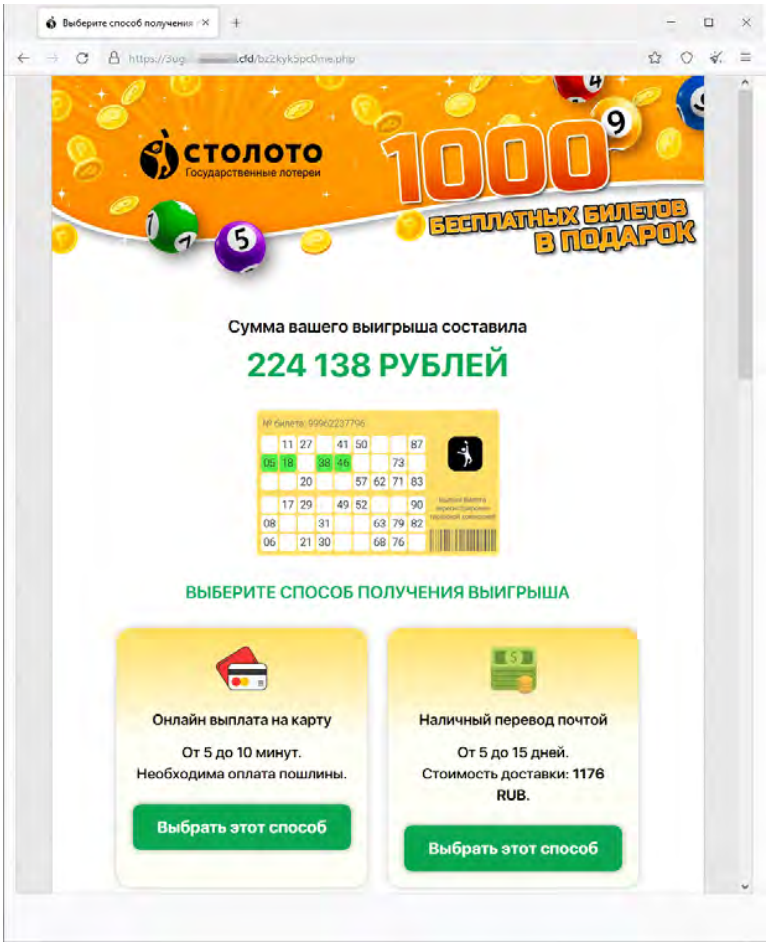
В феврале число запросов на расшифровку файлов, поврежденных троянами-шифровальщиками, снизилось на 17,63% по сравнению с январем.



- Trojan.Encoder.3953 — 23.62%
- Trojan.Encoder.26996 — 21.26%
- Trojan.Encoder.35534 — 5.51%
- Trojan.Encoder.34027 — 2.36%
- Trojan.Encoder.30356 — 1.97%

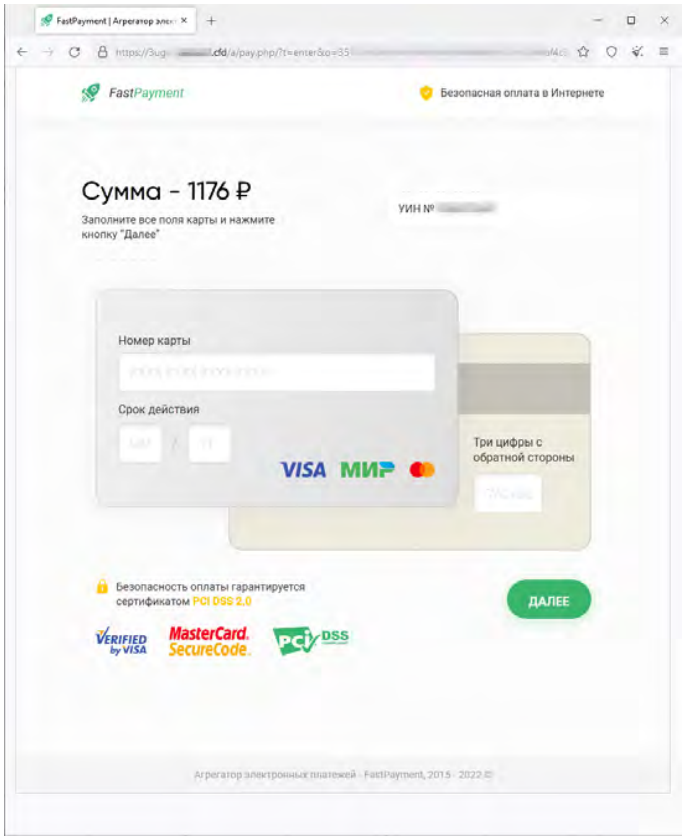
Опасные сайты

В феврале 2023 года интернет-аналитики компании «Доктор Веб» продолжили фиксировать появление мошеннических сайтов. Среди них были очередные веб-ресурсы, якобы открывающие посетителям доступ к заработку через инвестиции. Там пользователям предлагалось пройти небольшой опрос, после чего запрашивались персональные данные для регистрации учетной записи. Указываемая информация попадала к мошенникам и в дальнейшем могла использоваться в различных атаках. Кроме того, злоумышленники не оставляли попыток заманить потенциальных жертв на сайты, предлагавшие якобы бесплатные лотерейные билеты. Каждый посетитель становился «победителем» и для получения несуществующего выигрыша должен был заплатить «комиссию» или оплатить «доставку» денег.



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

Опасные сайты



На изображениях выше показаны примеры страниц одного из поддельных сайтов. Посетитель якобы выиграл в онлайн-лотерею 224 138 рублей и для «получения» приза должен заплатить некую комиссию размером 1176 рублей, предоставив данные банковской карты.

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 феврале 2023 года пользователи чаще всего вновь сталкивались с демонстрирующими надоедливую рекламу троянскими приложениями семейства Android.HiddenAds. В то же время снизилась активность банковских троянских приложений, программ-вымогателей и шпионских вредоносных программ. Вместе с тем в течение месяца специалисты «Доктор Веб» выявили в каталоге Google Play десятки новых угроз. Среди них — программы семейства Android.FakeApp, способные загружать мошеннические и другие нежелательные сайты, а также троянские приложения Android.Joker и Android.Subscription, подписывающие пользователей на платные услуги.

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

- рост активности рекламных троянских программ,
- снижение активности банковских троянских приложений и программ-вымогателей,
- обнаружение множества угроз в каталоге Google Play.

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

«Доктор Веб»: обзор вирусной активности в феврале 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