«Доктор Веб»:

обзор вирусной активности в ноябре 2023 года

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

Анализ статистики детектирований антивируса Dr.Web в ноябре 2023 года показал снижение общего числа обнаруженных угроз на 18,09% по сравнению с октябрем. Число уникальных угроз при этом также снизилось — на 13,79%. Чаще всего детектировались нежелательные рекламные программы и рекламные трояны, а также вредоносные приложения, которые распространяются в составе других угроз и затрудняют их обнаружение. В почтовом трафике преобладали фишинговые документы, вредоносные скрипты, программы, которые эксплуатируют уязвимости документов Microsoft Office, а также различные загрузчики, скачивающие другие вредоносные приложения на атакуемые компьютеры.

Число обращений пользователей за расшифровкой файлов увеличилось на 6,98% по сравнению с предыдущим месяцем. Чаще всего жертвы вредоносных программ-шифровальщиков сталкивались с Trojan.Encoder.3953 — на него пришлось 21,70% всех зафиксированных инцидентов. В 21,20% случаев пользователей атаковал Trojan.Encoder.26996, он опустился на второе место. Третьим вновь стал **Trojan.Encoder.35534** с долей 8,94%.

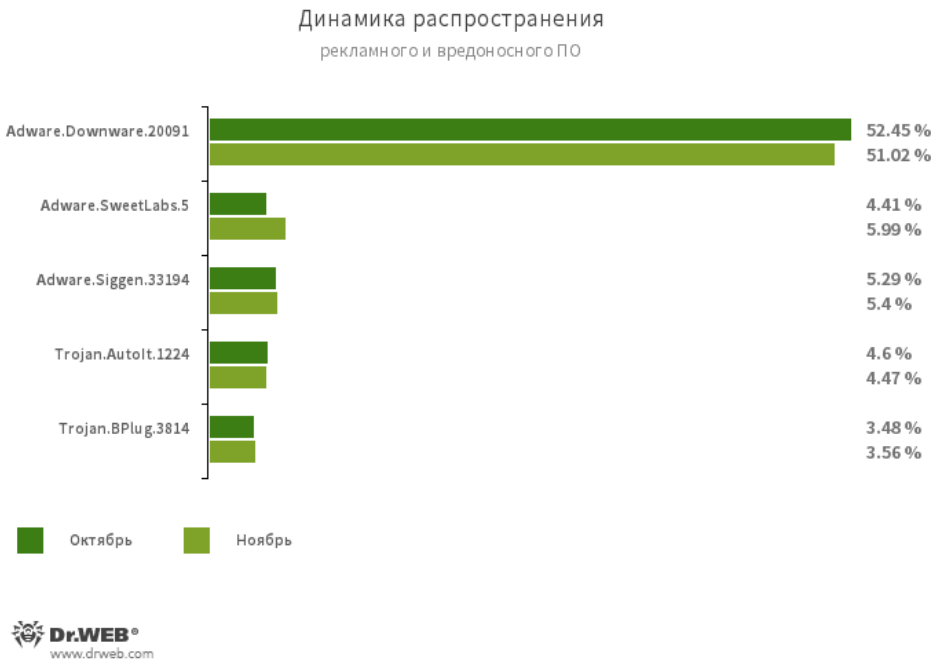
В ноябре вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play новые вредоносные приложения. Среди них — более 20 программ-подделок, которые использовались в мошеннических целях, а также троян, который подписывал владельцев Android-устройств на платные услуги.

Главные тенденции ноября

- Снижение общего числа обнаруженных угроз
- Преобладание фишинговых документов во вредоносном почтовом трафике
- Рост числа обращений пользователей за расшифровкой файлов, затронутых шифровальщиками
- Появление новых вредоносных приложений в каталоге Google Play

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

По данным сервиса статистики «Доктор Веб»



Adware.Downware.20091

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.

Adware.Siggen.33194

Детектирование созданного с использованием платформы Electron бесплатного браузера со встроенным рекламным компонентом. Этот браузер распространяется через различные сайты и загружается на компьютеры при попытке скачивания торрент-файлов.

Trojan.AutoIt.1224

Детектирование упакованной версии троянской программы Trojan.AutoIt.289, написанной на скриптовом языке AutoIt. Она распространяется в составе группы из нескольких вредоносных приложений — майнера, бэкдора и модуля для самостоятельного распространения. Trojan.AutoIt.289 выполняет различные вредоносные действия, затрудняющие обнаружение основной полезной нагрузки.

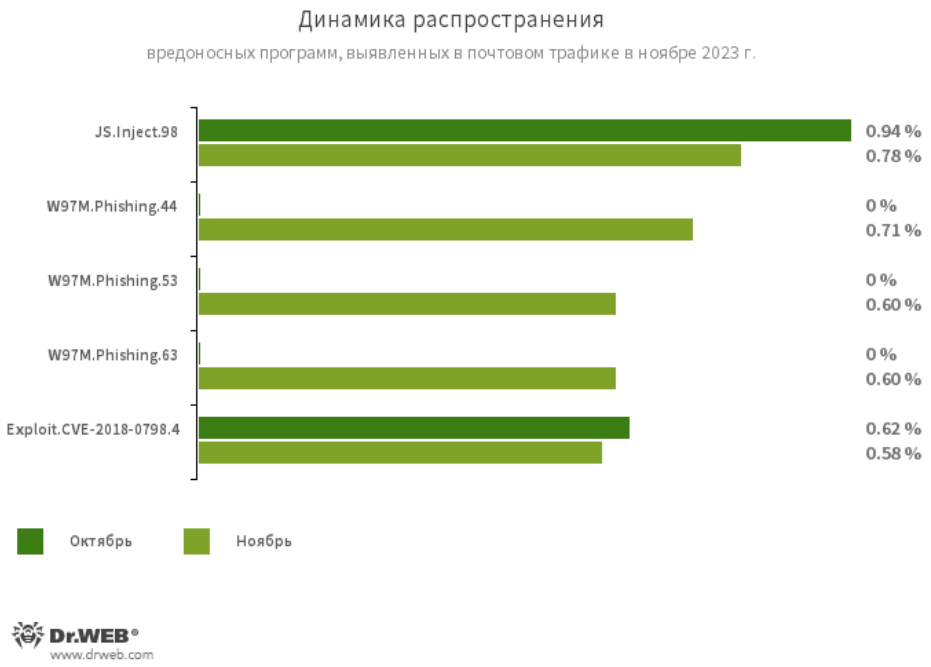
Trojan.BPlug.3814

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

«Доктор Веб»: обзор вирусной активности в ноябре 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.Phishing.44

W97M.Phishing.53

W97M.Phishing.63

Фишинговые документы Microsoft Word, которые нацелены на пользователей, желающих стать инвесторами. Они содержат ссылки, ведущие на мошеннические сайты.

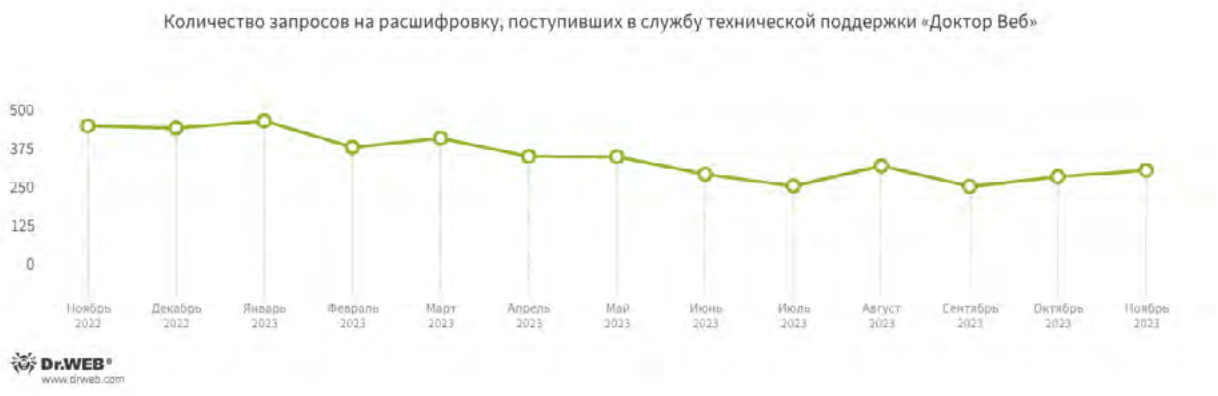
Exploit.CVE-2018-0798.4

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

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

Шифровальщики

В ноябре число запросов на расшифровку файлов, затронутых троянскими программами-шифровальщиками, увеличилось на 6,98% по сравнению с октябрем.



Наиболее распространенные энкодеры ноября:

- Trojan.Encoder.3953 — 21.70%
- Trojan.Encoder.26996 — 21.20%
- Trojan.Encoder.35534 — 8.94%
- Trojan.Encoder.37369 — 3.40%
- Trojan.Encoder.35067 — 2.98%

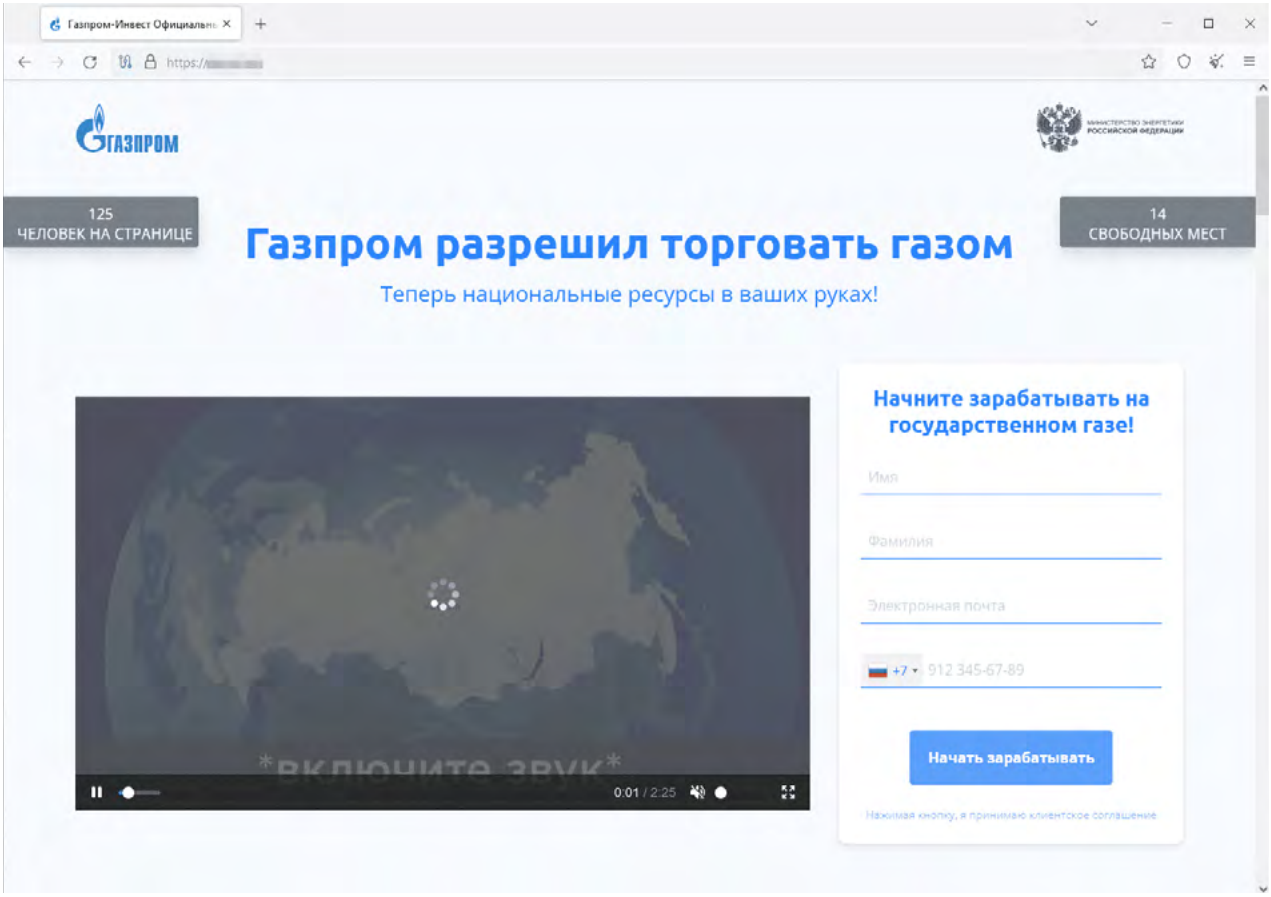
«Доктор Веб»: обзор вирусной активности в ноябре 2023 года

Опасные сайты

В ноябре 2023 года интернет-аналитики компании «Доктор Веб» не зафиксировали значимых изменений в активности кибермошенников. Злоумышленники по-прежнему пытались заманить потенциальных жертв на всевозможные сайты-подделки. Наиболее популярными среди них остаются мошеннические сайты инвестиционной тематики, а также интернет-ресурсы, предлагающие «бесплатные» лотерейные билеты и участие в «розыгрыше» призов.

В первом случае пользователям предлагается стать инвесторами, для чего они должны указать свои персональные данные. Во втором — участие в так называемых бесплатных лотереях и онлайн-конкурсах для всех пользователей всегда заканчиваются выигрышем, для получения которого якобы необходимо оплатить комиссию.

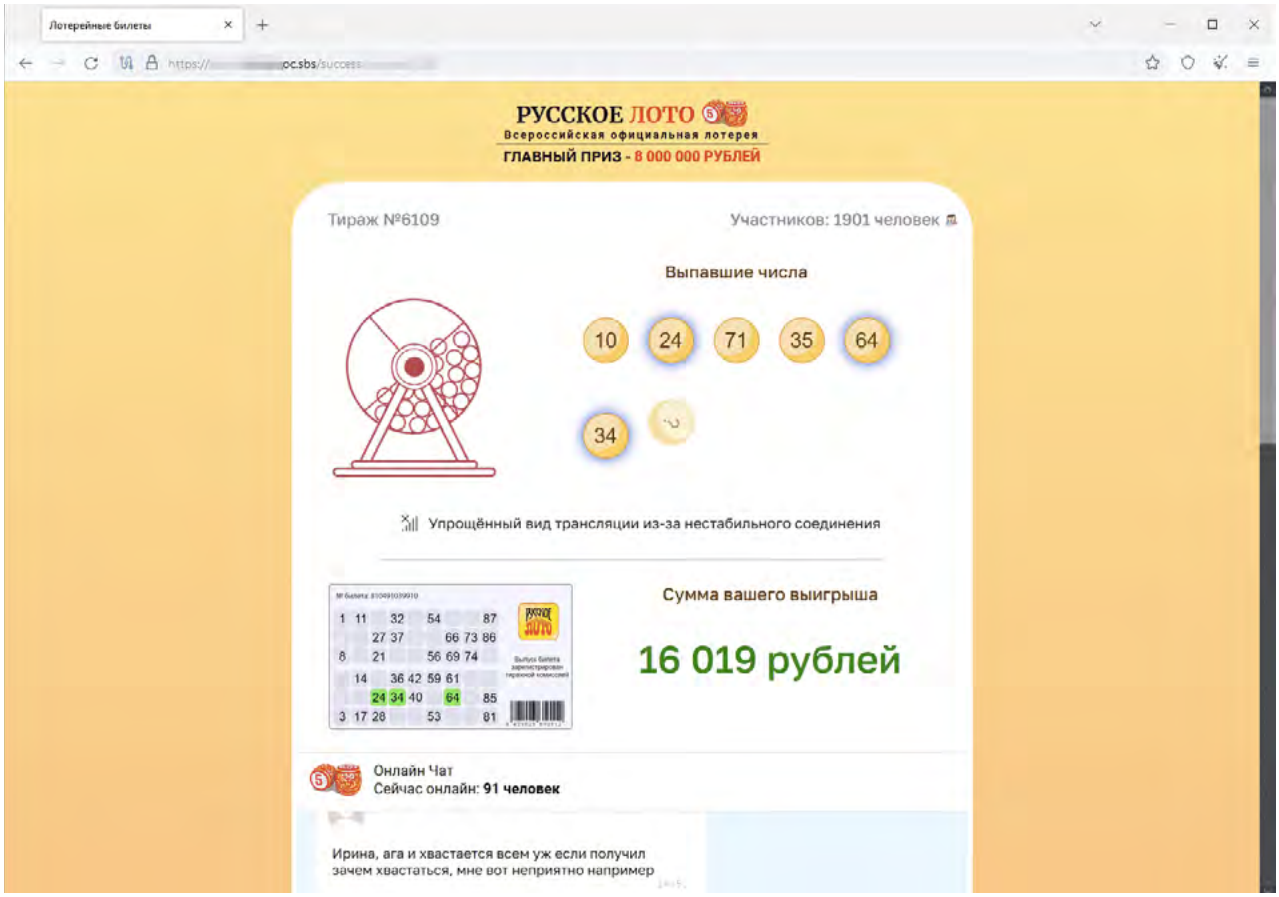
Пример фишингового сайта, где посетителю предлагается стать инвестором:



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

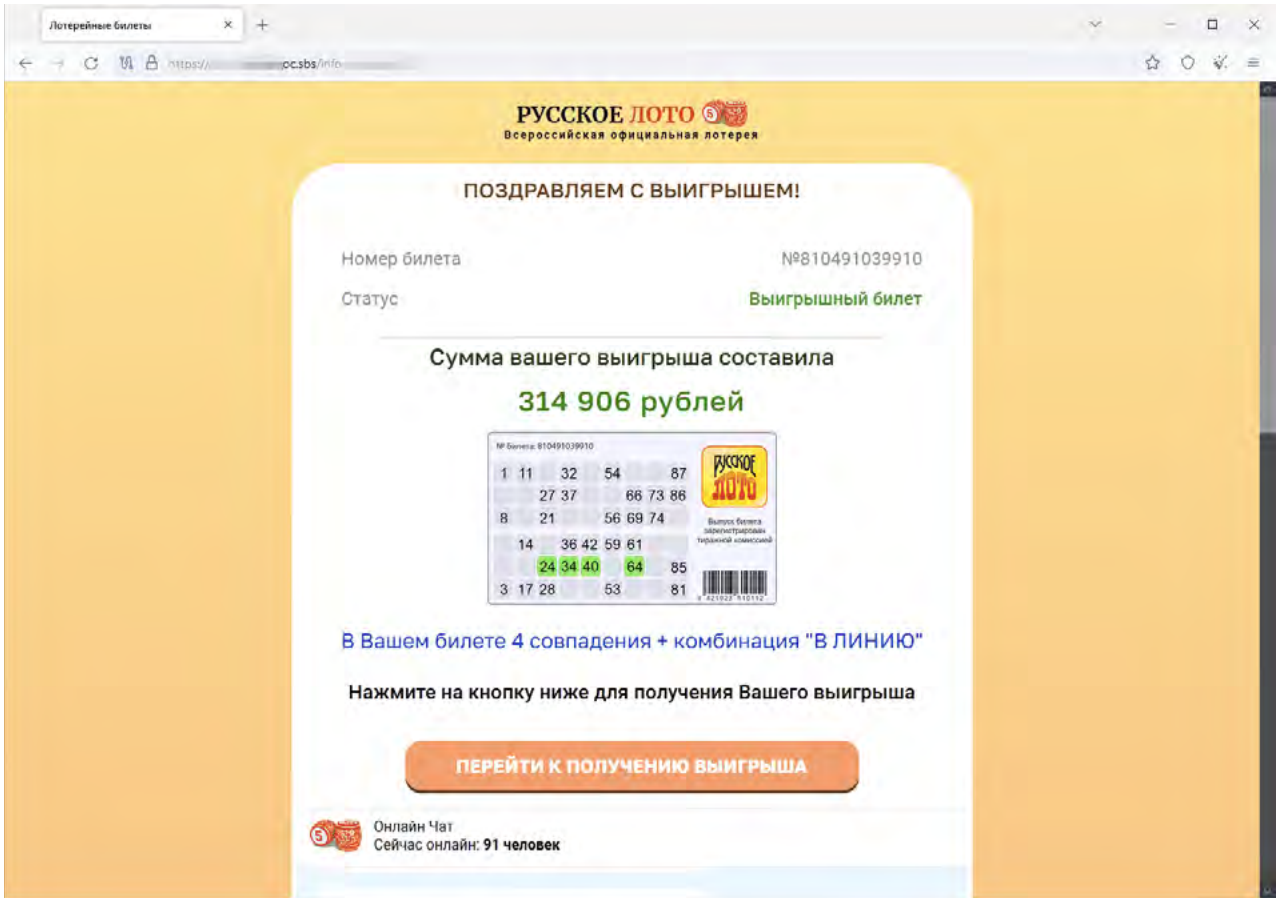
Опасные сайты

Пример мошеннического сайта, на котором имитируется розыгрыш лотереи:



Опасные сайты

Пользователь якобы выиграл 314 906 рублей и может приступить к получению выигрыша:



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 ноябре на защищаемых устройствах реже обнаруживались рекламные троянские программы Android.HiddenAds и Android.MobiDash. Кроме того, пользователи реже сталкивались с банковскими троянами и вредоносными программами-шпионами.

В минувшем месяце специалисты компании «Доктор Веб» выявили в каталоге Google Play множество новых вредоносных приложений из семейства Android.FakeApp, которые злоумышленники применяли в различных мошеннических схемах. Кроме того, был обнаружен троян Android.Subscription.21 — он подписывал пользователей на платные услуги.

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

- снижение активности рекламных троянских программ,
- снижение активности банковских троянов и шпионских троянских приложений,
- появление новых вредоносных приложений в каталоге Google Play.

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

«Доктор Веб»: обзор вирусной активности в ноябре 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