



**«Доктор Веб»:
обзор вирусной активности
в декабре 2023 года**

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

Анализ статистики детектирований антивируса Dr.Web в декабре 2023 года показал рост общего числа обнаруженных угроз на 40,87% по сравнению с ноябрем. Число уникальных угроз также увеличилось — на 24,55%. По количеству детектирований вновь лидировали рекламные троянские и нежелательные приложения, а также вредоносные программы, которые распространяются в составе других угроз и затрудняют их обнаружение. В почтовом трафике чаще всего выявлялись фишинговые документы различных форматов.

Число обращений пользователей за расшифровкой файлов снизилось на 27,95% по сравнению с предыдущим месяцем. Чаще всего жертвы троянских программ-шифровальщиков сталкивались с [Trojan.Encoder.26996](#), [Trojan.Encoder.3953](#) и [Trojan.Encoder.37369](#), на долю которых пришлось 21,76%, 20,73% и 4,14% зафиксированных инцидентов соответственно.

В декабре специалисты компании «Доктор Веб» обнаружили в каталоге Google Play очередные вредоносные программы. Кроме того, были выявлены новые сайты, через которые злоумышленники распространяли поддельные приложения криптокошельков для ОС Android и iOS.

Главные тенденции декабря

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

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

По данным сервиса статистики «Доктор Веб»



Adware.Downware.20091

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

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.Autolt.1224

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

Adware.SweetLabs.5

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

Trojan.BPlug.3814

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

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

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

Статистика вредоносных программ в почтовом трафике



W97M.Phishing.44

W97M.Phishing.88

W97M.Phishing.85

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

PDF.Phisher.642

PDF-документы, используемые в фишинговых email-рассылках.

JS.Inject

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

Узнайте больше

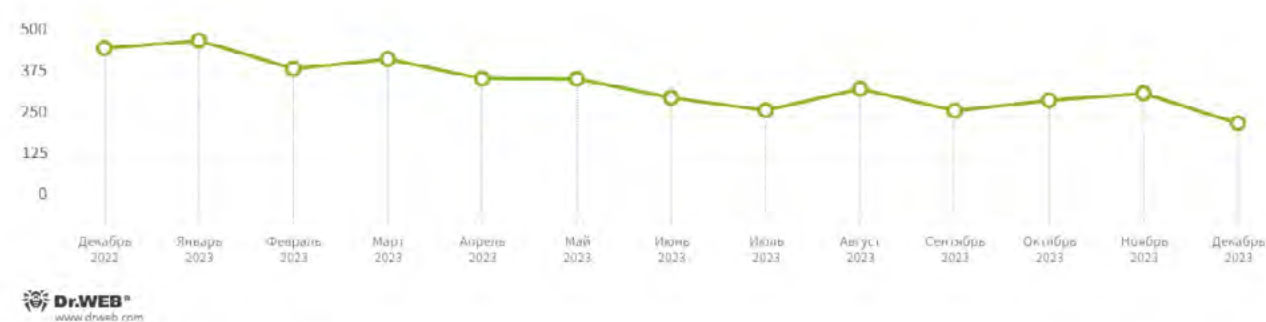
[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

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

Шифровальщики

В декабре 2023 года число запросов на расшифровку файлов, затронутых троянскими программами-шифровальщиками, снизилось на 27,95% по сравнению с ноябрем.

Количество запросов на расшифровку, поступивших в службу технической поддержки «Доктор Веб»



Наиболее распространенные энкодеры ноября:

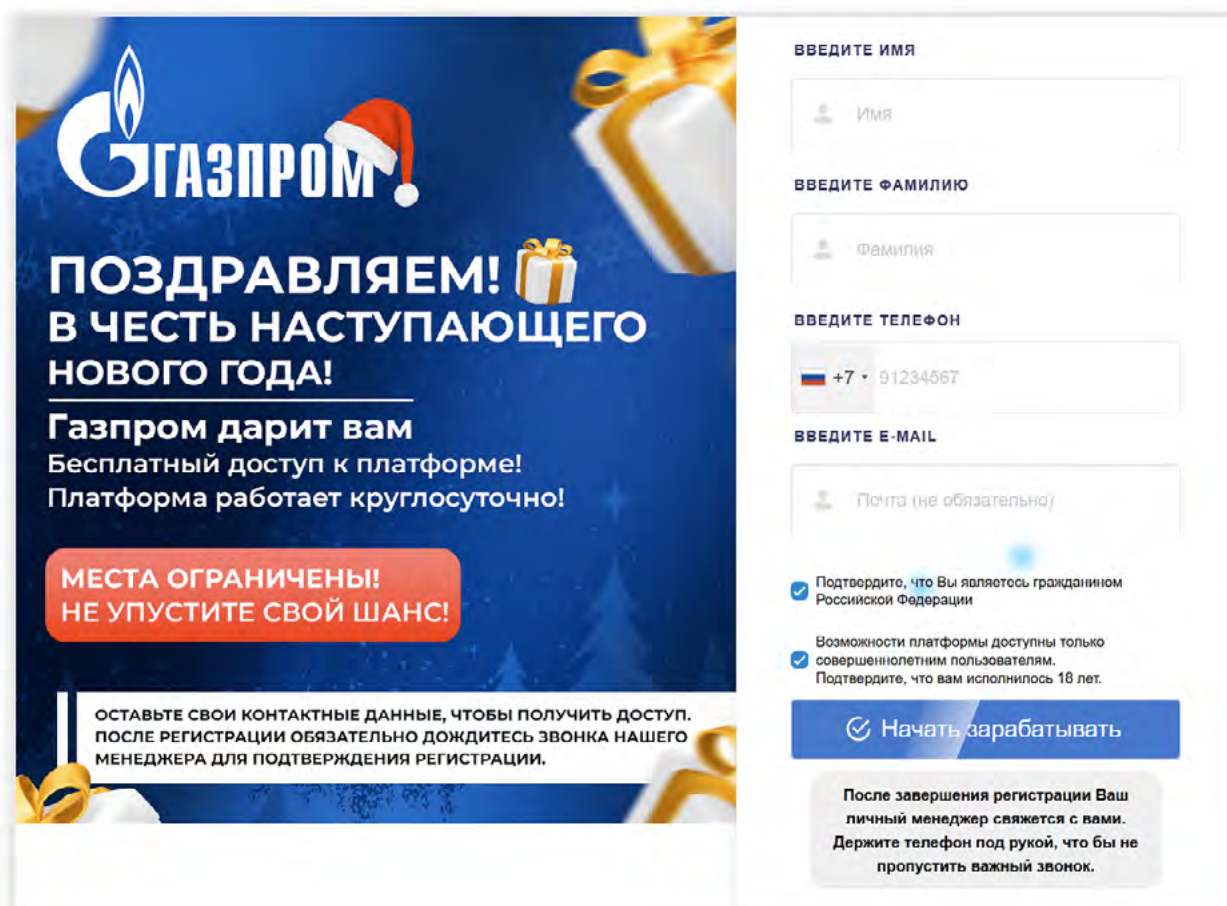
- Trojan.Encoder.26996 — 21.76%
- Trojan.Encoder.3953 — 20.73%
- Trojan.Encoder.37369 — 4.14%
- Trojan.Encoder.34790 — 3.63%
- Trojan.Encoder.30356 — 3.11%

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

Опасные сайты

В декабре 2023 года интернет-аналитики компании «Доктор Веб» продолжили выявлять мошеннические сайты инвестиционной тематики, якобы имеющие отношение к нефтегазовым компаниям, банкам и другим организациям. Посетителям таких сайтов предлагается указать персональные данные для регистрации учетной записи и получения доступа к тем или иным финансовым сервисам.

В период новогодних праздников злоумышленники соответствующим образом скорректировали эту схему обмана: они привлекали потенциальных жертв «подарками» и «специальными условиями». Например, на одном из мошеннических сайтов посетителям «в честь наступающего нового года» предлагался бесплатный доступ к некой инвестиционной платформе:



ГАЗПРОМ

ПОЗДРАВЛЯЕМ! В ЧЕСТЬ НАСТУПАЮЩЕГО НОВОГО ГОДА!

Газпром дарит вам
Бесплатный доступ к платформе!
Платформа работает круглосуточно!

**МЕСТА ОГРАНИЧЕНЫ!
НЕ УПУСТИТЕ СВОЙ ШАНС!**

ОСТАВЬТЕ СВОИ КОНТАКТНЫЕ ДАННЫЕ, ЧТОБЫ ПОЛУЧИТЬ ДОСТУП.
ПОСЛЕ РЕГИСТРАЦИИ ОБЯЗАТЕЛЬНО ДОЖДИТЕСЬ ЗВОНКА НАШЕГО
МЕНЕДЖЕРА ДЛЯ ПОДТВЕРЖДЕНИЯ РЕГИСТРАЦИИ.

ВВЕДИТЕ ИМЯ

Имя

ВВЕДИТЕ ФАМИЛИЮ

Фамилия

ВВЕДИТЕ ТЕЛЕФОН

+7 • 91234567

ВВЕДИТЕ E-MAIL

Почта (не обязательно)

Подтвердите, что Вы являетесь гражданином Российской Федерации

Возможности платформы доступны только совершеннолетним пользователям.
Подтвердите, что вам исполнилось 18 лет.

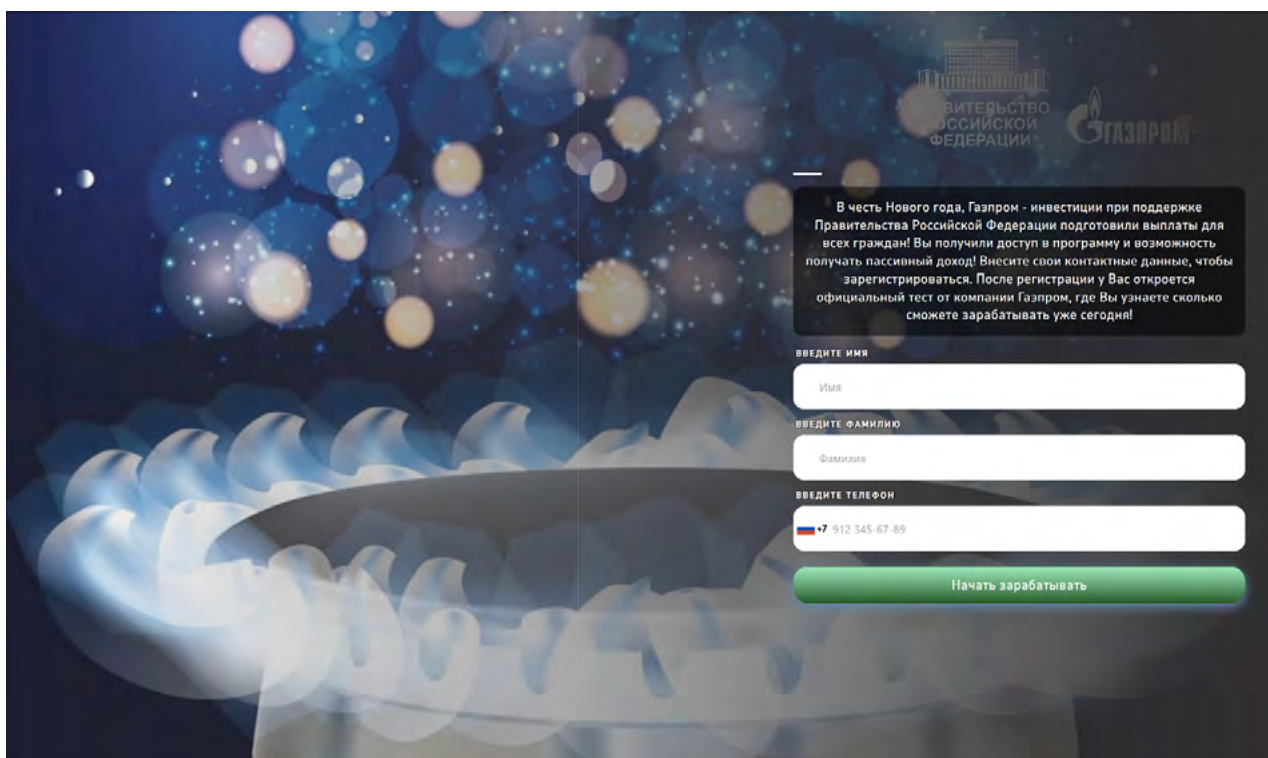
Начать зарабатывать

После завершения регистрации Ваш личный менеджер свяжется с вами.
Держите телефон под рукой, что бы не пропустить важный звонок.

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

Опасные сайты

А на другом сайте — якобы при поддержке правительства Российской Федерации и одной крупной нефтегазовой компании — всех граждан «ждали» социальные выплаты:



Узнайте больше о нерекомендуемых Dr.Web сайтах

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

Вредоносное и нежелательное ПО для мобильных устройств

Согласно данным статистики детектирования Dr.Web для мобильных устройств Android, в декабре пользователей чаще всего атаковали рекламные троянские программы [Android.HiddenAds](#). В то же время активность этих вредоносных приложений снизилась по сравнению с предыдущим месяцем. Также снизилось число атак банковских троянов и вредоносных программ-шпионов.

В течение декабря вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play очередные программы-подделки из семейства [Android.FakeApp](#). Кроме того, наши специалисты обнаружили новые сайты, которые злоумышленники используют для распространения поддельных приложений криптокошельков для устройств на базе ОС Android и iOS.

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

- снижение активности рекламных троянских программ [Android.HiddenAds](#),
- снижение активности банковских троянов и шпионских троянских приложений,
- обнаружение новых вредоносных программ в каталоге Google Play,
- обнаружение новых сайтов, через которые распространяются поддельные приложения криптокошельков.

Более подробно о вирусной обстановке для мобильных устройств в декабре читайте в нашем [обзоре](#).

[Узнайте больше с Dr.Web](#)

«Доктор Веб»: обзор вирусной активности в декабре 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](#)



© ООО «Доктор Веб»,
2003

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)