

«Доктор Веб»: обзор вирусной активности в марте 2021 года



«Доктор Веб»: обзор вирусной активности в марте 2021 года

13 апреля 2021 года

В марте анализ данных статистики Dr.Web показал увеличение общего числа обнаруженных угроз на 16.72% по сравнению с февралем. Количество уникальных угроз также выросло — на 19.49%. Рекламные программы и нежелательные приложения по-прежнему лидируют по общему количеству детектирований. В почтовом трафике на первых позициях находится разнообразное вредоносное ПО, в том числе обфусцированные троянские программы, вредоносные скрипты, а также приложения, использующие уязвимости документов Microsoft Office.

Число обращений пользователей за расшифровкой файлов увеличилось на 11.33% по сравнению с прошлым месяцем. Самым распространенным энкодером месяца оказался [Trojan.Encoder.567](#), на долю которого приходится 23.76% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ МАРТА

- Увеличение активности распространения вредоносного ПО
- Рекламные приложения остаются в числе самых активных угроз
- Рост числа запросов на расшифровку файлов, затронутых шифровальщиками

«Доктор Веб»: обзор вирусной активности в марте 2021 года

По данным серверов статистики «Доктор Веб»



Угрозы прошедшего месяца:

Adware.Downware.19894

Adware.Downware.19629

Рекламное ПО, часто выступающее в роли промежуточного установщика пиратских программ.

Adware.Softobase.15

Программа-установщик, распространяющая устаревшее программное обеспечение. Меняет настройки браузера.

Adware.SweetLabs.4

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

Adware.Elemental.17

Семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают эти приложения, которые показывают рекламу, а также инсталлируют ненужное ПО.

«Доктор Веб»: обзор вирусной активности в марте 2021 года

Статистика вредоносных программ в почтовом трафике



W97M.DownLoader.2938

Семейство троянов-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

HTML.FishForm.73

Веб-страница, распространяющаяся посредством фишинговых рассылок. Представляет собой фиктивную форму ввода учетных данных, которая имитирует авторизацию на известных сайтах. Введенные пользователем данные отправляются злоумышленнику.

JS.IFrame.811

Вредоносный скрипт, встраиваемый злоумышленниками в веб-страницы. Выполнение скрипта позволяет перенаправлять посетителей на нежелательные и опасные сайты, отображать навязчивую рекламу в браузере или отслеживать действия пользователя.

Trojan.PackedNET.576

Упакованное вредоносное ПО, написанное на VB.NET.

BackDoor.SpyBotNET.25

Бэкдор, написанный на VB.NET. Способен манипулировать файловой системой (копирование, удаление, создание директорий и т. д.), завершать процессы, делать снимки экрана.

«Доктор Веб»: обзор вирусной активности в марте 2021 года

Шифровальщики



Запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков, в марте в антивирусную лабораторию «Доктор Веб» поступило на 11.33% больше, чем в феврале.

- [Trojan.Encoder.567](#) — 23.76%
- [Trojan.Encoder.26996](#) — 17.16%
- [Trojan.Encoder.29750](#) — 3.63%
- [Trojan.Encoder.30356](#) — 1.65%
- [Trojan.Encoder.11464](#) — 1.32%

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

[Настрой-ка Dr.Web от шифровальщиков](#)

[Обучающий курс](#)

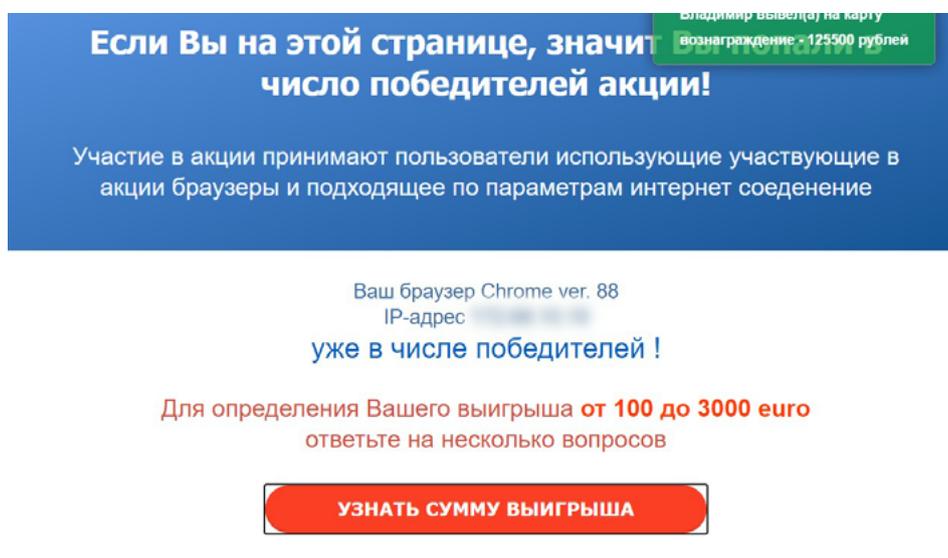
[О бесплатном восстановлении](#)

[Dr.Web Rescue Pack](#)

«Доктор Веб»: обзор вирусной активности в марте 2021 года

Опасные сайты

В течение марта 2021 года интернет-аналитики «Доктор Веб» добавили в базу не рекомендуемых и вредоносных сайтов большое количество новых мошеннических и фишинговых ресурсов. В марте злоумышленники продолжали активно распространять сайты с фальшивыми розыгрышами. Как правило, для получения несуществующего выигрыша жертве под различными предложениями предлагалось оплатить комиссию.



Владимир вывел(а) на карту вознаграждение - 125500 рублей

Если Вы на этой странице, значит Вы попали в число победителей акции!

Участие в акции принимают пользователи использующие участвующие в акции браузеры и подходящее по параметрам интернет соединение

Ваш браузер Chrome ver. 88
IP-адрес ██████████

уже в числе победителей !

Для определения Вашего выигрыша **от 100 до 3000 евро** ответьте на несколько вопросов

УЗНАТЬ СУММУ ВЫИГРЫША

Пожалуйста, после получения вознаграждения, оставьте отзыв на нашем сайте

Все эти сайты объединяли похожие визуальные элементы: разделы с отзывами, всплывающие окна с именами «победителей», имитация чата с технической поддержкой и т. п. Используя проверенные методы социальной инженерии, мошенники плавно подвели пользователей к раскрытию данных банковских карт и оплате комиссии.

[Узнайте больше о не рекомендуемых Dr.Web сайтах](#)

«Доктор Веб»: обзор вирусной активности в марте 2021 года

Вредоносное и нежелательное ПО для мобильных устройств

Вредоносное и нежелательное ПО для мобильных устройств

Среди угроз, наиболее часто встречавшихся на Android-устройствах в марте, вновь были трояны, демонстрировавшие рекламу, а также вредоносные приложения, загружавшие и выполнявшие произвольный код. Кроме того, пользователи часто сталкивались с нежелательными рекламными программами.

В каталоге Google Play вновь распространялись опасные трояны из семейства [Android.Joker](#). Их основная функция — подписка жертв на платные мобильные услуги. Вместе с тем, были выявлены и очередные мошеннические трояны [Android.FakeApp](#).

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

- появление очередных угроз в каталоге Google Play.
- активность троянов, подписывающих пользователей на платные услуги.
- распространение вредоносных приложений, применяемых в различных мошеннических схемах.

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

«Доктор Веб»: обзор вирусной активности в марте 2021 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

[ВебиОметр](#) | [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»,
2003-2021

Узнайте больше

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