Dr.WEB®
с 1992 года

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

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

16 марта 2021 года

В феврале анализ данных статистики Dr.Web показал увеличение общего числа обнаруженных угроз на 25.07% по сравнению с январем. Количество уникальных угроз при этом снизилось — на 7.57%. Большинство самых распространенных угроз по-прежнему приходится на долю рекламных программ. В почтовом трафике активнее всего распространялись различные вредоносные скрипты, а также обфусцированные модификации бэкдора Bladabindi и стилера AgentTesla. Кроме того, пользователям продолжали угрожать программы, использующие уязвимости документов Microsoft Office.

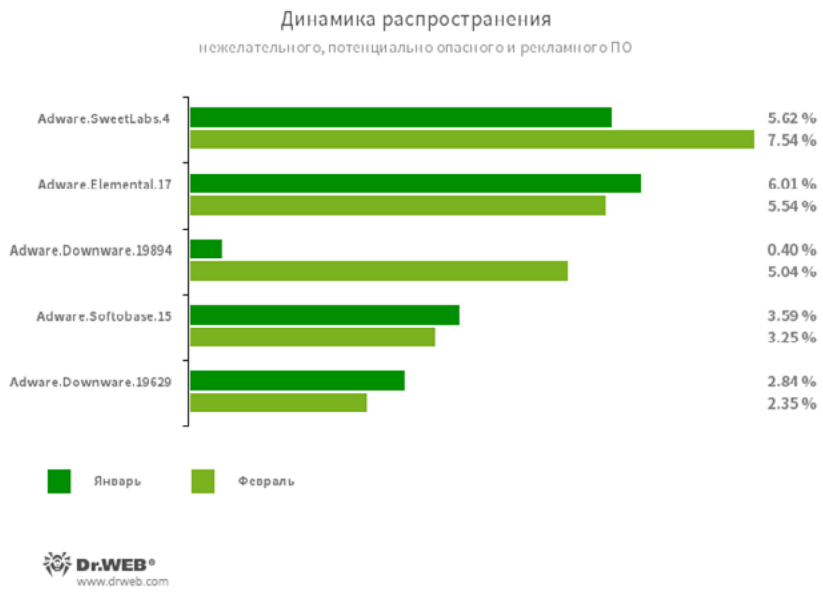
Число обращений пользователей за расшифровкой файлов снизилось на 21.27% по сравнению с январем. Самым распространенным энкодером остается Trojan.Encoder.26996, на долю которого приходится 21.45% всех инцидентов.

Главные тенденции февраля

- Увеличение активности распространения вредоносного ПО
- Рекламные приложения остаются в числе самых активных угроз
- Появление новых угроз в почтовом трафике

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

По данным серверов статистики «Доктор Веб»



Угрозы прошедшего месяца:

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.

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.

Статистика вредоносных программ в почтовом трафике

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.

W97M.DownLoader.2938

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

Trojan.Packed2.42845

Модификация бэкдора Bladabindi, обфусцированная при помощи упаковщика. Bladabindi является распространенным трояном-бэкдором с широкими возможностями для удаленного управления зараженным компьютером.

HTML.FishForm.63

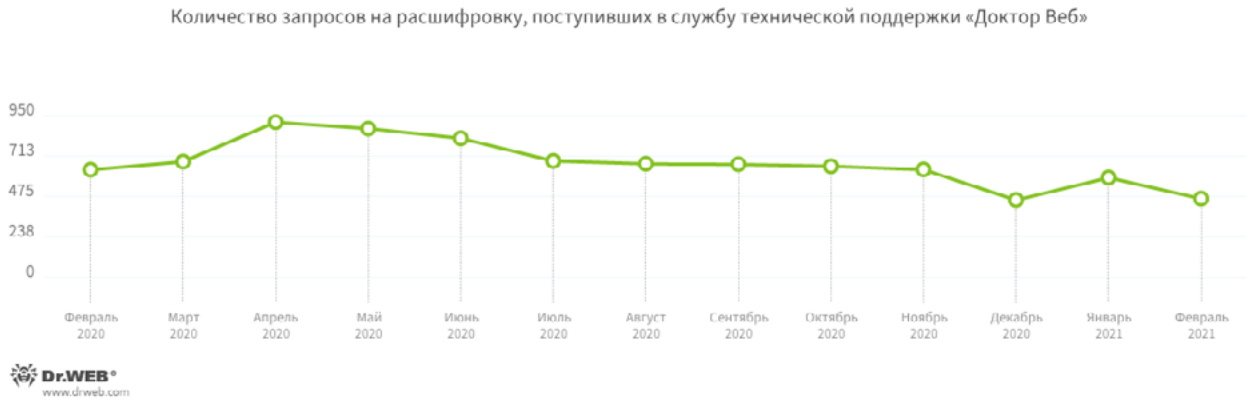
Веб-страница, распространяющаяся посредством фишинговых рассылок. Представляет собой фиктивную форму ввода учетных данных, которая имитирует авторизацию на известных сайтах. Введенные пользователем данные отправляются злоумышленнику.

Trojan.Packed2.42827

Одна из многочисленных модификаций AgentTesla, обфусцированная при помощи упаковщика.

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

Шифровальщики



Запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков, в феврале в антивирусную лабораторию «Доктор Веб» поступило на 21.27% меньше, чем в январе.

- Trojan.Encoder.26996 — 21.45%
- Trojan.Encoder.567 — 14.55%
- **Trojan.Encoder.29750** — 7.27%
- **Trojan.Encoder.30356** — 3.27%
- Trojan.Encoder.761 — 1.82%

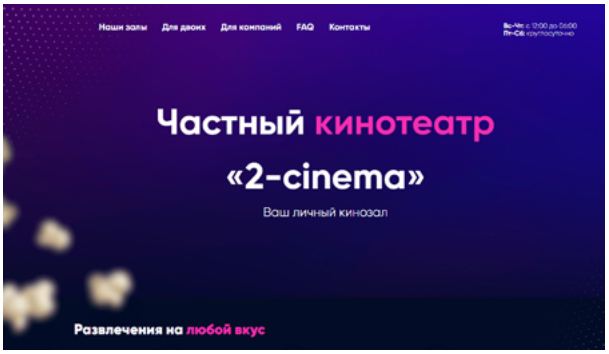
Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

Настрой-ка Dr.Web от шифровальщиков
Обучающий курс
О бесплатном восстановлении
Dr.Web Rescue Pack

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

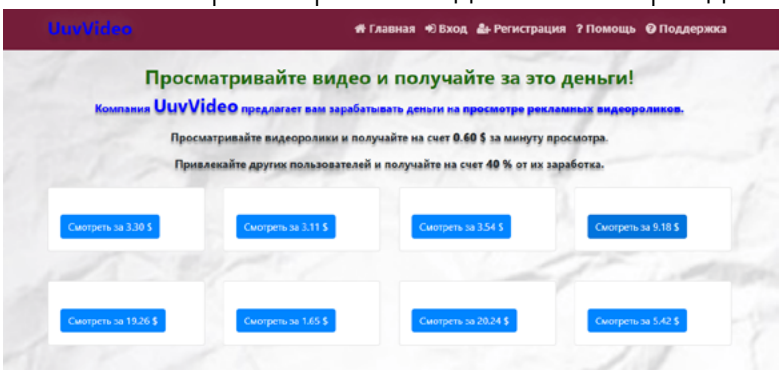
Опасные сайты

В течение февраля 2021 года интернет-аналитики «Доктор Веб» добавили в базу нерекомендуемых и вредоносных сайтов множество новых мошеннических и фишинговых ресурсов. Кроме эксплуатирования тематики с выплатами и компенсациями злоумышленники вернулись и к другим известным схемам заработка. Так, в феврале было выявлено множество ресурсов, имитирующих сайты частных кинотеатров.



Чтобы заставить потенциальную жертву приобрести билеты на сеанс на одном из таких сайтов, злоумышленники активно использовали различные методы социальной инженерии. После оплаты билетов пользователи просто теряли деньги, а данные банковских карт передавались операторам сайта. В ряде случаев после этого с жертвой связывалась «техническая поддержка» и под предлогом оформления возврата средств высылала еще одну форму для оплаты.

Кроме того, в феврале аналитики обнаружили несколько веб-сайтов, предлагающих посетителям просматривать видео за вознаграждение.



В действительности мошенники использовали эти сайты для сбора пользовательских данных, фишинга, распространения специализированного нежелательного ПО, накруток просмотров и других подобных целей. Вдобавок положенное вознаграждение от партнерских сервисов за активность пользователей получали сами злоумышленники.

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В феврале самыми распространенными Android-угрозами вновь стали троянские приложения, демонстрирующие рекламу, а также трояны, способные исполнять произвольный код и загружать различное ПО.

В течение прошедшего месяца специалисты компании «Доктор Веб» обнаружили множество угроз в каталоге Google Play. Среди них были многофункциональные трояны семейства Android.Joker, подписывающие пользователей на премиум-сервисы и выполняющие произвольный код, мошеннические трояны семейства Android.FakeApp, которые злоумышленники выдавали за полезное и безобидное ПО, рекламные трояны Android.HiddenAds, а также другие угрозы.

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

- рекламные трояны и трояны-загрузчики остаются одними из самых активных Android-угроз;
- обнаружение угроз в каталоге Google Play;
- высокая активность вредоносных приложений, применяемых в различных мошеннических схемах.

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

«Доктор Веб»: обзор вирусной активности в феврале 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
VebIQметр | 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