Dr.WEB®
с 1992 года

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

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

28 января 2022 года

В декабре анализ данных статистики Dr.Web показал увеличение общего числа обнаруженных угроз на 34% по сравнению с ноябрем. Количество уникальных угроз уменьшилось на 15%. Большинство детектирований по-прежнему приходится на долю рекламных программ и нежелательных приложений. В почтовом трафике чаще всего распространялось разнообразное вредоносное ПО, в том числе различные бэкдоры.

Число обращений пользователей за расшифровкой файлов уменьшилось на 41,3% по сравнению с прошлым месяцем. Самым распространенным энкодером декабря стал Trojan.Encoder.26996, на долю которого приходится почти треть всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ ДЕКАБРЯ

- Существенное увеличение общего числа угроз
- Рекламные приложения по-прежнему остаются главной угрозой

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

По данным сервиса статистики «Доктор Веб»

Угрозы прошедшего месяца:

Adware.SweetLabs.5

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

Adware.Downware.19998

Adware.Downware.19985

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Adware.Elemental.17

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

Adware.OpenCandy.247

Семейство приложений, предназначенных для установки на компьютер различного дополнительного рекламного ПО.

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

Статистика вредоносных программ в почтовом

W97M.DownLoader.2938

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

BackDoor.SpyBotNET.25

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

Trojan.DownLoader34.24881

Загрузчик вредоносного ПО.

HTML.FishForm.209

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

BackDoor.RatNET.2

Бэкдор, который считывает хранящиеся в браузере пароли.

По сравнению с ноябрем, в декабре число запросов на расшифровку файлов, затронутых шифровальщиками, уменьшилось на 41,3%.

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

Шифровальщики

- Trojan.Encoder.26996 — 29,3%
- Trojan.Encoder.567 — 16.16%
- Trojan.Encoder.3953 — 11.62%
- Trojan.Encoder.11539 — 1.52%
- Trojan.Encoder.28501 — 1.52%

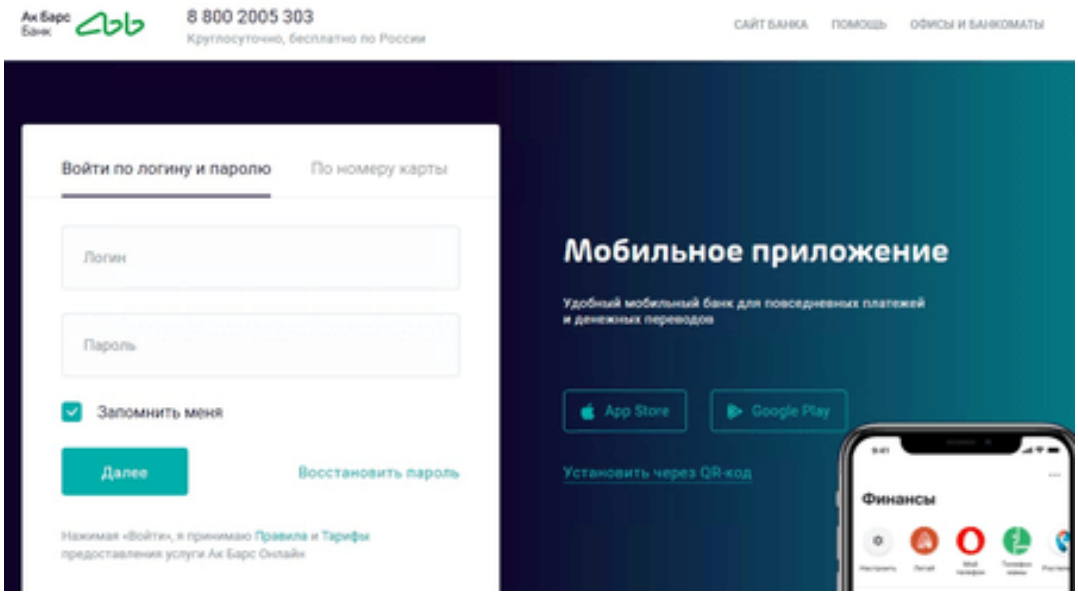
Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

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

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

Опасные сайты

В декабре 2021 года интернет-аналитики «Доктор Веб» заметили увеличение числа сайтов, маскирующихся под веб-ресурсы российских региональных банков. Мошенники создают страницы, максимально похожие на те, что использует банк. Жертве предлагается ввести реальные логин и пароль, а также установить «удобное мобильное приложение».



На скриншоте изображена главная страница фишингового сайта, сделанного по мотивам официального веб-сайта Ак Барс Банка.

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных

В декабре 2021 года антивирусные продукты Dr.Web для Android наиболее часто выявляли на защищаемых устройствах рекламных троянов, а также вредоносные приложения, загружающие другое ПО и выполняющие произвольный код. В то же время в каталоге Google Play были найдены новые угрозы. Среди них — очередные программы-подделки, которые злоумышленники использовали в различных мошеннических схемах, и трояны, подписывавшие жертв на платные мобильные услуги.

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

- Рекламные трояны остаются одними из наиболее активных Android-угроз;
- Появление новых вредоносных приложений в каталоге Google Play.

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

«Доктор Веб»: обзор вирусной активности в декабре 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
Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125124 Россия, Москва, 3-я Ямского поля улица, д.2, к.12а
www.антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах