Dr.WEB

«Доктор Веб»:
обзор вирусной активности в феврале 2024 года

«Доктор Веб»: обзор вирусной активности в феврале 2024 года

Анализ статистики детектирований антивируса Dr.Web в феврале 2024 года показал рост общего числа обнаруженных угроз на 1,26% по сравнению с январем. При этом число уникальных угроз снизилось на 0,78%. Лидирующие позиции по количеству детектирований вновь заняли различные рекламные трояны и нежелательные рекламные программы. Кроме того, высокую активность сохранили вредоносные приложения, которые распространяются в составе других угроз и затрудняют их обнаружение. В почтовом трафике чаще всего выявлялись вредоносные скрипты, фишинговые документы, а также программы, которые эксплуатируют уязвимости документов Microsoft Office.

Число обращений пользователей за расшифровкой файлов снизилось на 7,02% по сравнению с предыдущим месяцем. Наиболее часто виновниками атак становились трояны-шифровальщики Trojan.Encoder.3953 (18,27% инцидентов), **Trojan.Encoder.37369** (9,14% инцидентов) и Trojan.Encoder.26996 (8,12% инцидентов).

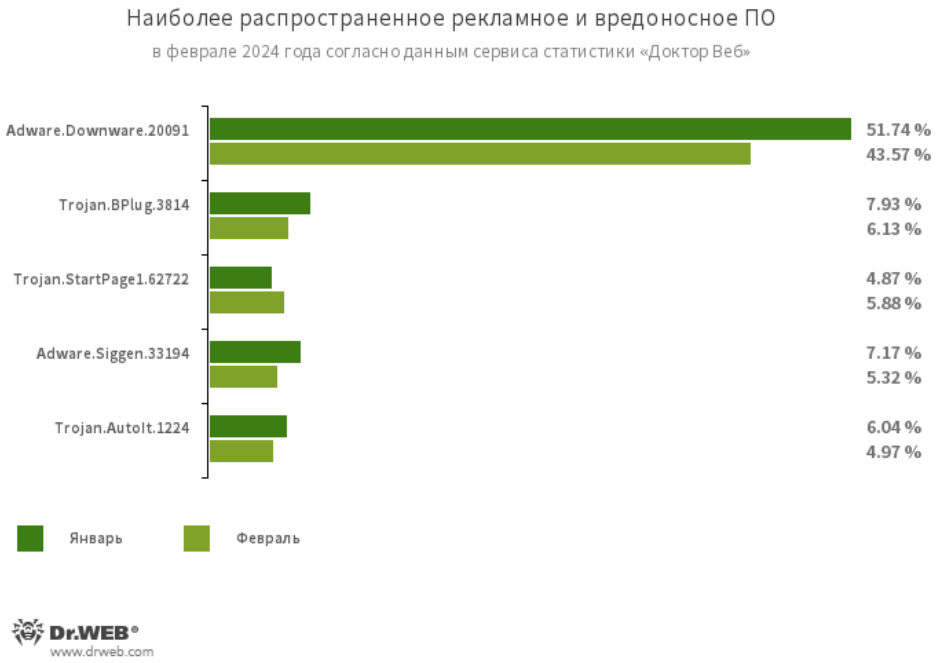
На Android-устройствах наиболее часто вновь детектировались рекламные трояны семейства Android.HiddenAds, активность которых значительно возросла.

Главные тенденции февраля

- Рост общего числа обнаруженных угроз
- Преобладание вредоносных скриптов и фишинговых документов во вредоносном почтовом трафике
- Снижение числа обращений пользователей за расшифровкой файлов, затронутых шифровальщиками
- Рост числа детектирований рекламных троянских приложений Android.HiddenAds на защищаемых устройствах

«Доктор Веб»: обзор вирусной активности в феврале 2024 года

По данным сервиса статистики «Доктор Веб»



Adware.Downware.20091

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Trojan.BPlug.3814

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

Trojan.StartPage1.62722

Вредоносная программа, подменяющая стартовую страницу в настройках браузера.

Adware.Siggen.33194

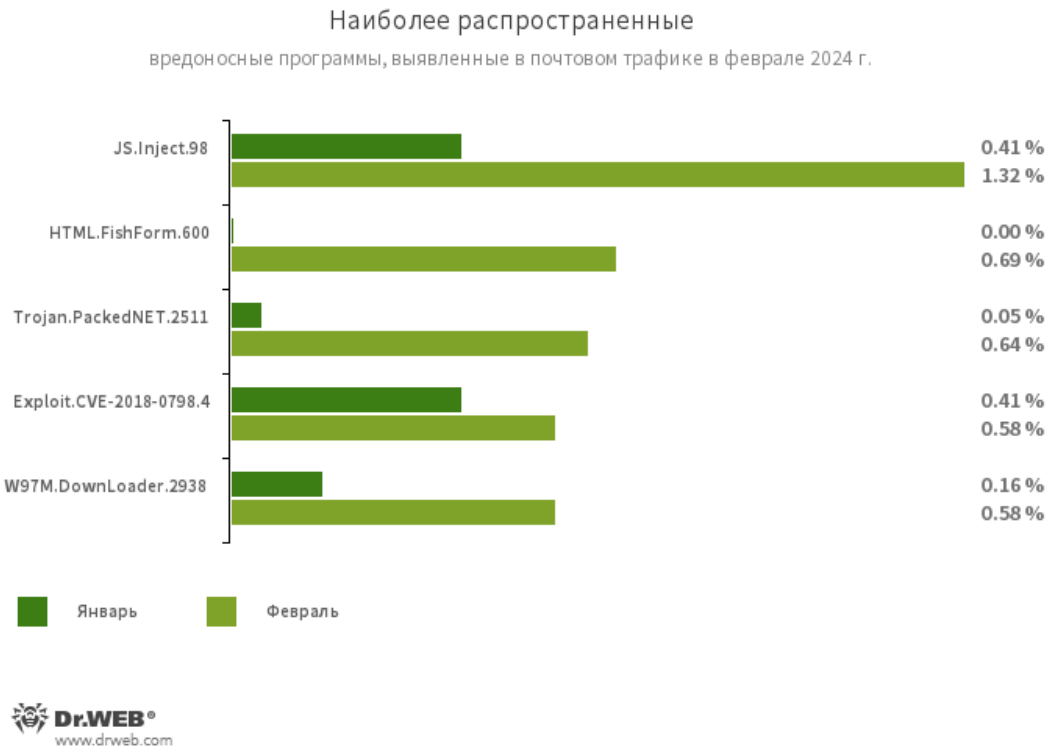
Детектирование созданного с использованием платформы Electron бесплатного браузера со встроенным рекламным компонентом. Этот браузер распространяется через различные сайты и загружается на компьютеры при попытке скачивания торрент-файлов.

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.

«Доктор Веб»: обзор вирусной активности в феврале 2024 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.

HTML.FishForm.365

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

Trojan.PackedNET.2511

Вредоносное ПО, написанное на VB.NET и защищенное программным упаковщиком.

Exploit.CVE-2018-0798.4

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

W97M.DownLoader.2938

Семейство троянов-загрузчиков, использующих уязвимости документов Microsoft Office. Они предназначены для загрузки других вредоносных программ на атакуемый компьютер.

«Доктор Веб»: обзор вирусной активности в феврале 2024 года

Шифровальщики

В феврале 2024 года число запросов на расшифровку файлов, затронутых троянскими программами-шифровальщиками, снизилось на 7,02% по сравнению с январем.

Наиболее распространенные энкодеры февраля:

- Trojan.Encoder.3953 — 18.27%
- **Trojan.Encoder.35534** — 9.14%
- Trojan.Encoder.26996 — 8.12%
- Trojan.Encoder.29750 — 0.51%
- **Trojan.Encoder.37400** — 0.51%

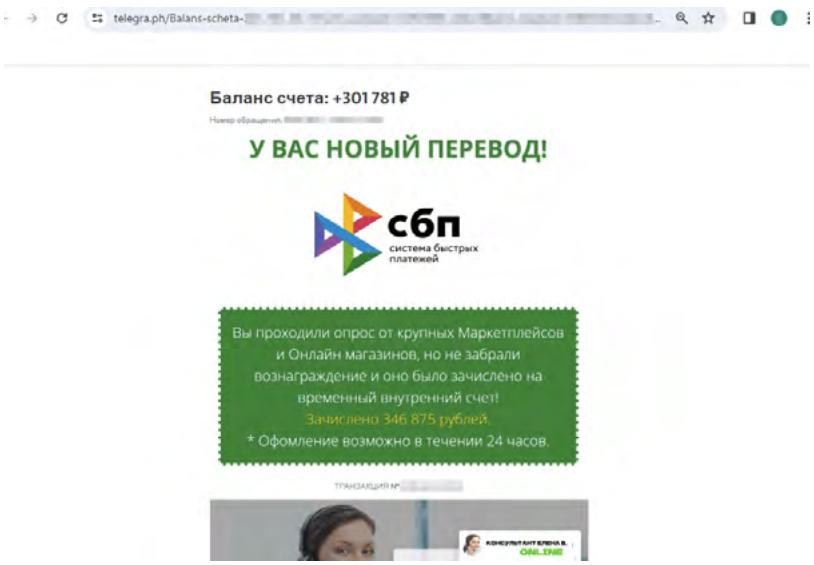
Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

«Доктор Веб»: обзор вирусной активности в феврале 2024 года

Опасные сайты

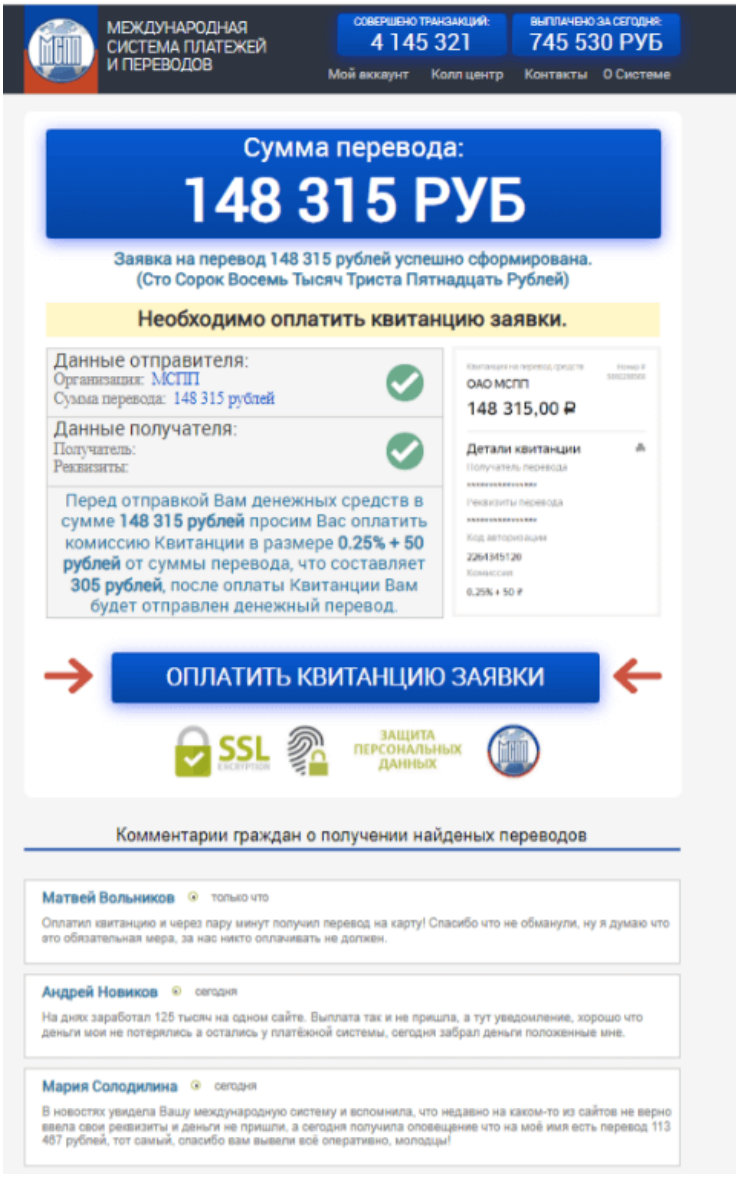
В феврале 2024 года интернет-аналитики компании «Доктор Веб» продолжили выявлять нежелательные сайты различной тематики. Так, популярностью среди злоумышленников стали пользоваться сайты, информирующие потенциальных жертв о доступности для них неких денежных переводов. Для «получения» этих средств пользователи должны заплатить «комиссию» за межбанковский перевод. Ссылки на подобные сайты распространяются в том числе через блог-платформу Telegraph.

Ниже представлен пример такой публикации. Потенциальным жертвам предлагается в течение 24 часов «забрать» вознаграждение, якобы полученное после участия в опросе интернет-магазинов:



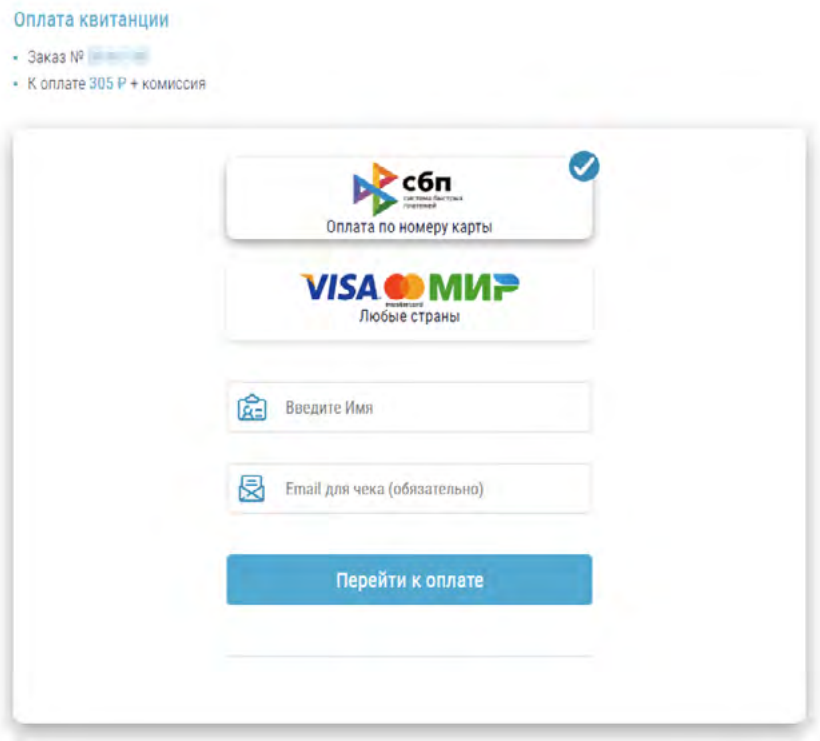
Опасные сайты

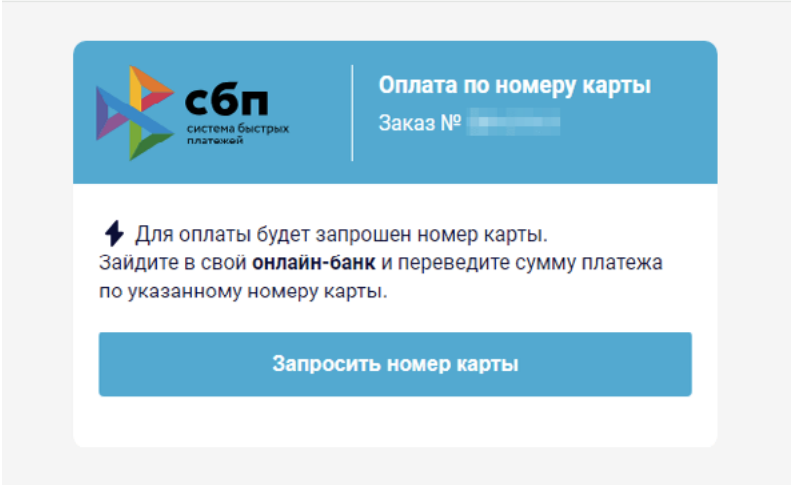
При нажатии на ссылку «ОФОРМИТЬ ВЫПЛАТУ» пользователь перенаправляется на мошеннический сайт некой «Международной Системы Платежей и Переводов», где ему якобы доступно получение обещанной выплаты:

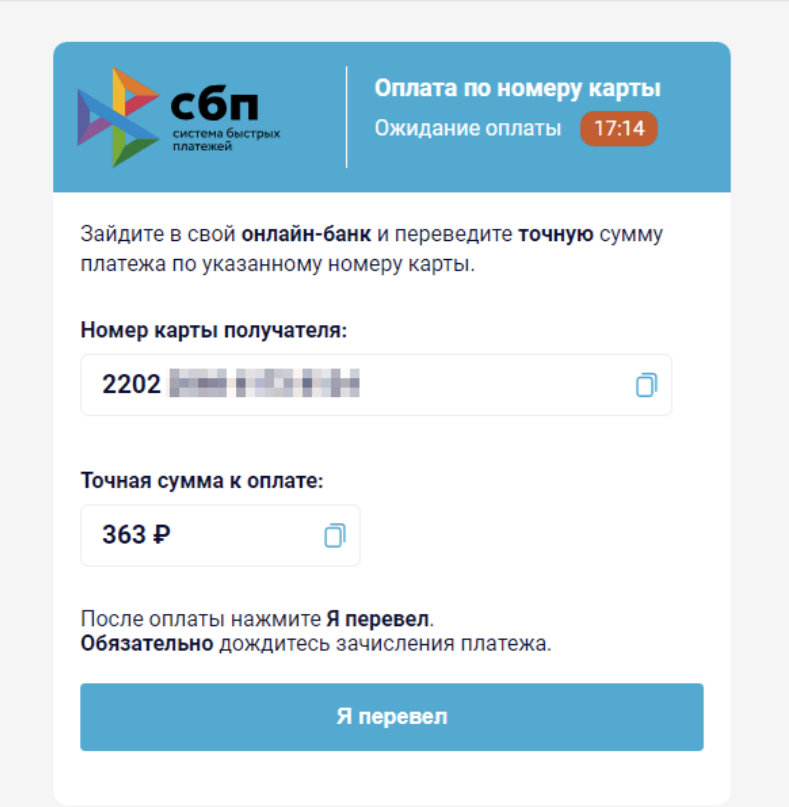


Для «получения» денег пользователь вначале должен указать персональные данные — имя и адрес электронной почты, а затем заплатить «комиссию» через Систему быстрых платежей (СБП) за «перевод» ему несуществующего вознаграждения. При этом в качестве способа оплаты «комиссии» мошенники указывают перевод денег по номеру банковской карты через

онлайн-банк, в то время как СБП предусматривает переводы только по номеру мобильного телефона. В данном случае злоумышленники могут целенаправленно спекулировать на набирающем в России популярность способе перевода денег в расчете на низкую финансовую грамотность пользователей. Если жертва согласится заплатить «комиссию», она переведет собственные деньги на подконтрольную мошенникам банковскую карту. В то же время нельзя исключать, что в попытке украсть у пользователей деньги злоумышленники в будущем действительно станут использовать СБП.







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 феврале 2024 года на защищаемых устройствах наиболее часто вновь выявлялись троянские программы Android.HiddenAds, демонстрирующие нежелательную рекламу. Их активность по сравнению с январем возросла на 73,26%. При этом рекламные троянские программы другого семейства, Android.MobiDash, атаковали пользователей на 58,85% реже.

Число детектирований шпионских троянов Android.Spy снизилось на 27,33%, а банковских троянов — на 18,77%. В то же время вредоносные программы-вымогатели Android.Locker выявлялись на 29,85% чаще.

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

- значительный рост активности рекламных троянских программ Android.HiddenAds,
- снижение числа атак банковских троянов и шпионских троянских приложений,
- рост числа атак вредоносных программ-вымогателей.

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

«Доктор Веб»: обзор вирусной активности в феврале 2024 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
«Доктор Веб» в других странах

Узнайте больше
Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека