Dr.WEB

«Доктор Веб»:

обзор вирусной активности в августе 2023 года

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

Анализ статистики детектирований антивируса Dr.Web в августе 2023 года показал рост общего числа обнаруженных угроз на 4,05% по сравнению с июлем. Число уникальных угроз при этом увеличилось на 3,35%. Чаще всего пользователи сталкивались с рекламными программами. В почтовом трафике преобладали вредоносные скрипты, фишинговые документы и приложения, эксплуатирующие уязвимости документов Microsoft Office.

Число обращений пользователей за расшифровкой файлов возросло на 23,99% по сравнению с предыдущим месяцем. Самым распространенным энкодером стал Trojan.Encoder.3953 с долей 20,80% от общего числа зафиксированных инцидентов. Лидер июля, Trojan.Encoder.26996, опустился на второе место — он атаковал пользователей в 17,26% случаев. На третьем месте расположился **Trojan.Encoder.35534** с долей 8,85%.

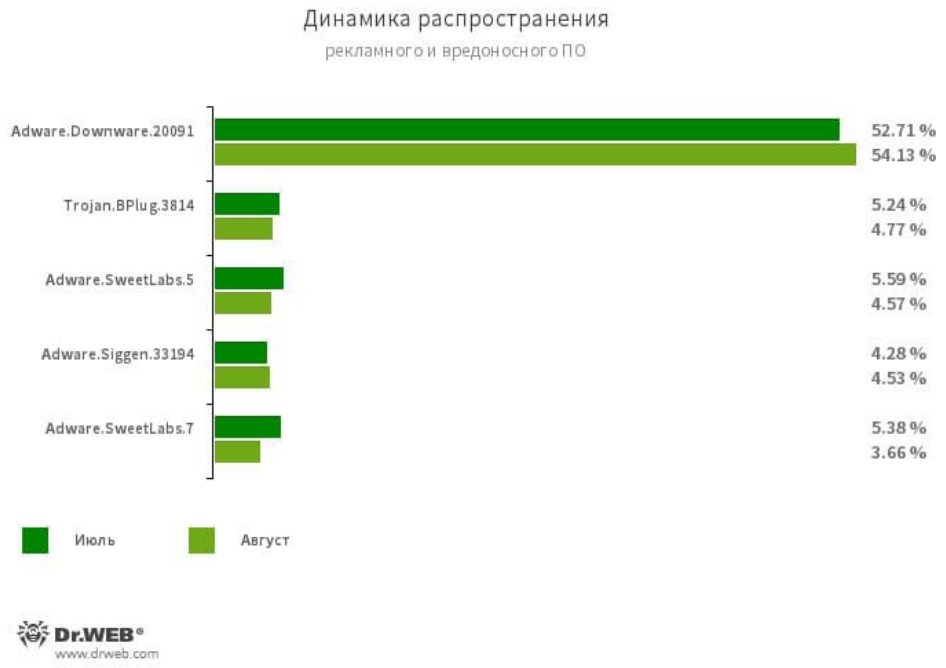
В августе в каталоге Google Play была выявлена троянская программа Android.HiddenAds.3766 — она демонстрировала нежелательную рекламу.

Главные тенденции августа

- Увеличение общего числа обнаруженных угроз
- Рост числа обращений пользователей за расшифровкой файлов, затронутых шифровальщиками
- Появление новой вредоносной программы в каталоге Google Play

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

По данным сервиса статистики «Доктор Веб»



Наиболее распространенные угрозы августа:

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 открывает навязчивую рекламу в браузерах.

Adware.SweetLabs.5

Adware.SweetLabs.7

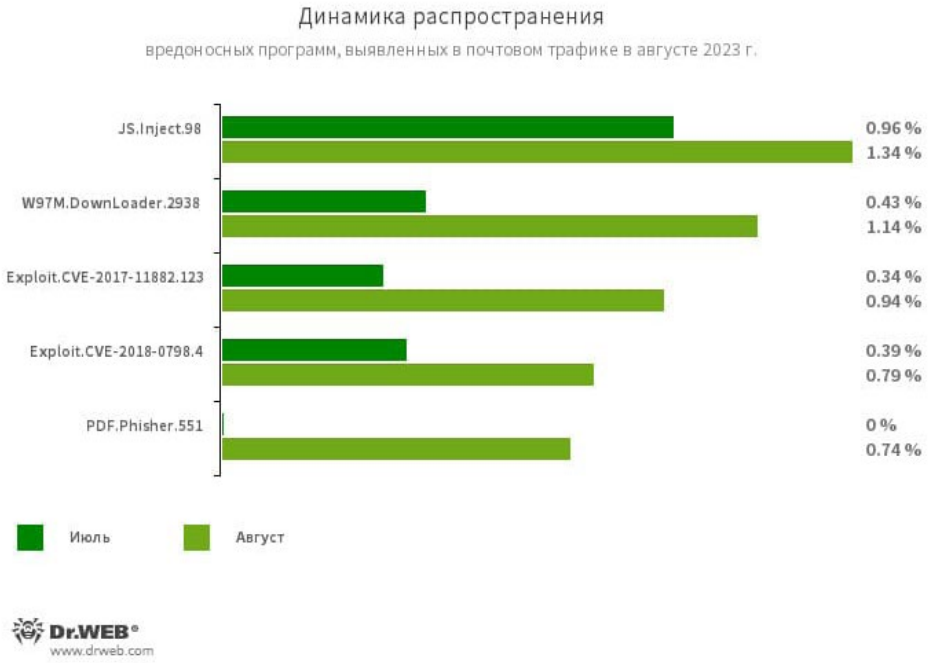
Альтернативный каталог приложений и надстройка к графическому интерфейсу Windows от создателей Adware.Opencandy.

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 пользователей при попытке скачать торрент-файлы.

«Доктор Веб»: обзор вирусной активности в августе 2023 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.

W97M.DownLoader.2938

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

Exploit.CVE-2017-11882.123

Exploit.CVE-2018-0798.4

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

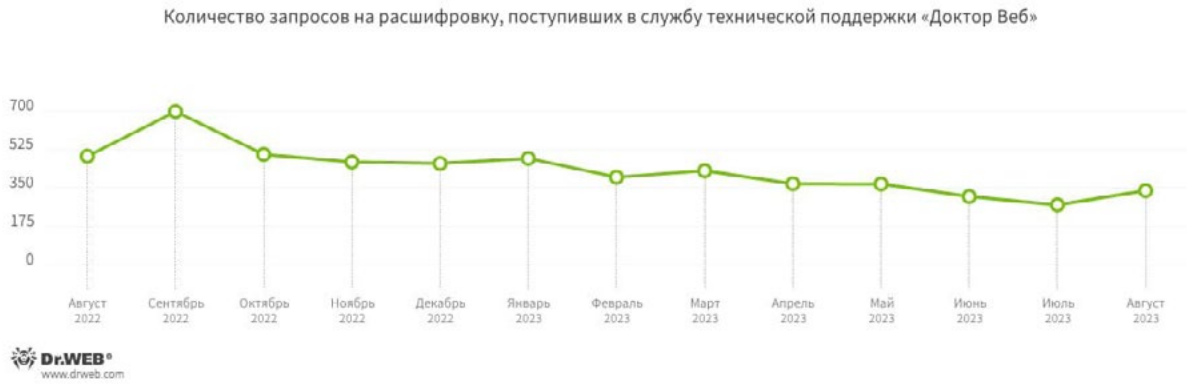
PDF.Phisher.551

PDF-документы, используемые в фишинговых email-рассылках.

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

Шифровальщики

В августе число запросов на расшифровку файлов, затронутых троянскими программами-шифровальщиками, увеличилось на 23,99% по сравнению с июлем.



Наиболее распространенные энкодеры августа:

- Trojan.Encoder.3953 — 20.80%
- Trojan.Encoder.26996 — 17.26%
- Trojan.Encoder.35534 — 8.85%
- Trojan.Encoder.29750 — 2.65%
- Trojan.Encoder.30356 — 2.65%

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

Опасные сайты

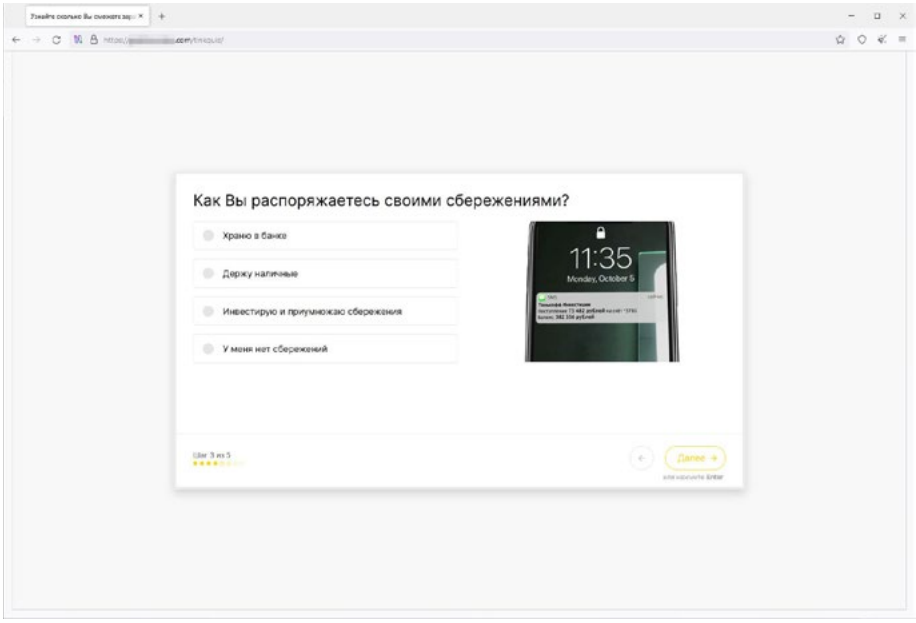
В августе 2023 года интернет-аналитики компании «Доктор Веб» выявили очередные мошеннические сайты, на которых пользователи якобы могли восстановить или приобрести новые дипломы, паспорта и другие официальные документы. Попытки воспользоваться подобными «услугами» могут привести к утечке персональных данных, потере денег и проблемам с правоохранительными органами. Пример такого сайта представлен на скриншоте ниже:

Кроме того, злоумышленники продолжили заманивать пользователей на фишинговые сайты, якобы имеющие отношение к банкам и различным инвестиционным сервисам. На таких ресурсах посетителям предлагается получить доступ к «инвестиционным продуктам». Для этого от них требуется пройти короткий опрос и указать персональные данные для регистрации учетной записи. В случае согласия пользователи фактически передают информацию о себе в чужие руки и могут стать жертвами мошенников. Те, например, могут притвориться сотрудниками финансовых организаций и предложить «выгодно» вложить деньги. На следующих скриншотах показан пример одного из таких сайтов.

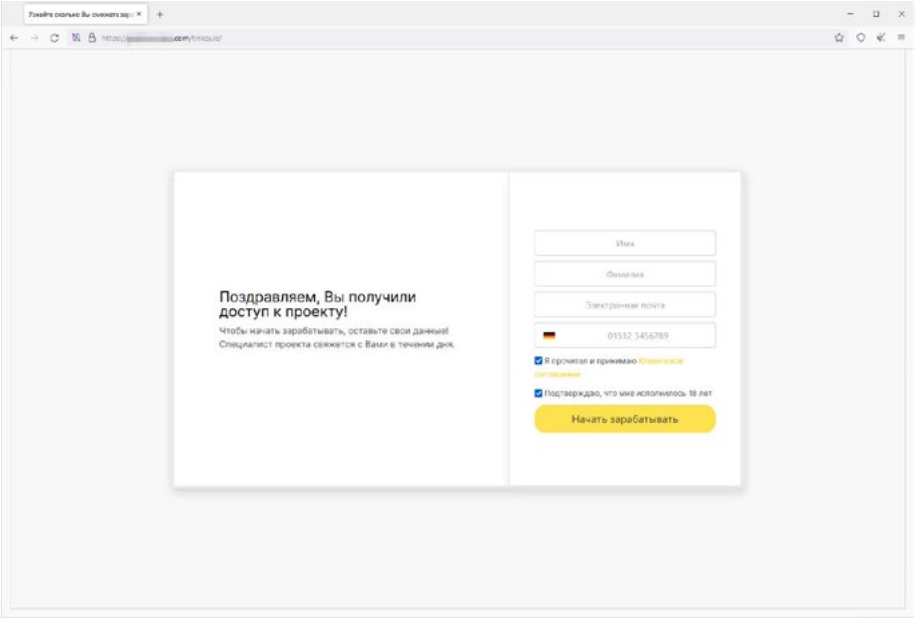
«Доктор Веб»: обзор вирусной активности в августе 2023 года

Опасные сайты

Предварительный опрос:

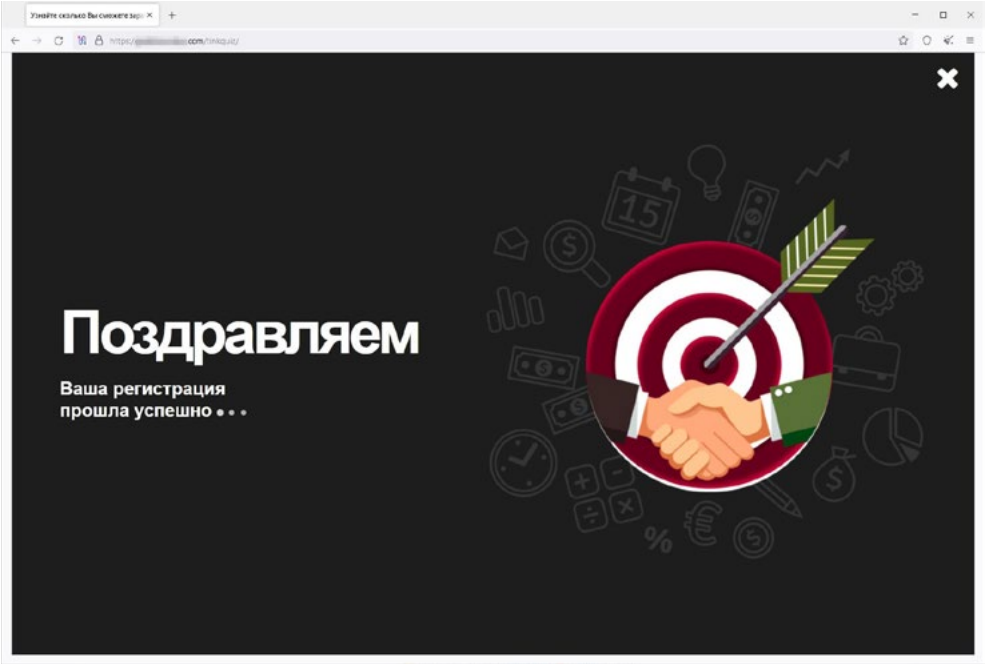


Форма для ввода персональных данных — имени и фамилии, электронной почты и номера телефона:



Вредоносное и нежелательное ПО для мобильных устройств

После того как пользователь подтверждает ввод персональной информации и нажимает кнопку «Начать зарабатывать», сайт сообщает об успешной регистрации:



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 августе 2023 года значительно возросла активность рекламных троянских программ семейства Android.MobiDash. В то же время пользователи реже сталкивались с рекламными троянскими программами семейства Android.HiddenAds.

По сравнению с июлем снизилась активность программ-вымогателей и шпионских троянских приложений. При этом возросло число атак банковских троянов.

Также в минувшем месяце в каталоге Google Play была выявлена новая вредоносная программа.

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

- значительный рост активности рекламных троянских программ семейства Android.MobiDash,
- снижение активности рекламных троянских программ семейства Android.HiddenAds,
- снижение активности программ-вымогателей и шпионских троянских приложений,
- рост числа атак Android-банкеров.

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

«Доктор Веб»: обзор вирусной активности в августе 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