«Доктор Веб»:

обзор вирусной активности в сентябре 2023 года

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

Анализ статистики детектирований антивируса Dr.Web в сентябре 2023 года показал снижение общего числа обнаруженных угроз на 0,44% по сравнению с августом. Число уникальных угроз также снизилось — на 11,98%. По числу детектирований вновь лидировали рекламные троянские программы и рекламные приложения. В почтовом трафике наиболее часто выявлялись вредоносные скрипты, фишинговые документы, а также приложения, которые эксплуатируют уязвимости документов Microsoft Office.

Число обращений пользователей за расшифровкой файлов снизилось на 19,64% по сравнению с предыдущим месяцем. Самым распространенным энкодером сентября стал Trojan.Encoder.26996 — на его долю пришлось 24,64% зафиксированных инцидентов. Лидер августа, Trojan.Encoder.3953, расположился на втором месте; пользователи сталкивались с ним в 19,43% случаев. Третье место вновь заняла вредоносная программа **Trojan.Encoder.35534** с долей 5,21%.

В течение сентября в каталоге Google Play были обнаружены новые угрозы. Среди них — рекламные трояны, вредоносные программы, подписывающие пользователей на платные услуги, а также троянские приложения, которые злоумышленники используют в мошеннических целях. Кроме того, в прошлом месяце компания «Доктор Веб» опубликовала аналитические материалы о вредоносных программах Android.Pandora.2 и Android.Spy.Lydia. Первая является бэкдором, который заражает смарт-телевизоры и телевизионные приставки на базе ОС Android и по команде злоумышленников выполняет DDoS-атаки. Вторая — троянская программа-шпион, нацеленная на иранских пользователей.

Главные тенденции сентября

- Снижение общего числа обнаруженных угроз
- Снижение числа обращений пользователей за расшифровкой файлов, затронутых шифровальщиками
- Появление очередных вредоносных приложений в каталоге Google Play

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

По данным сервиса статистики «Доктор Веб»

Наиболее распространенные угрозы сентября:

Adware.Downware.20091

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

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 при попытке скачивания торрент-файлов.

Trojan.BPlug.3814

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

«Доктор Веб»: обзор вирусной активности в сентябрь 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.Phishing.33

W97M.Phishing.34

W97M.Phishing.35

Фишинговые документы Microsoft Word, которые нацелены на пользователей, желающих стать инвесторами. Они содержат ссылки, ведущие на мошеннические сайты.

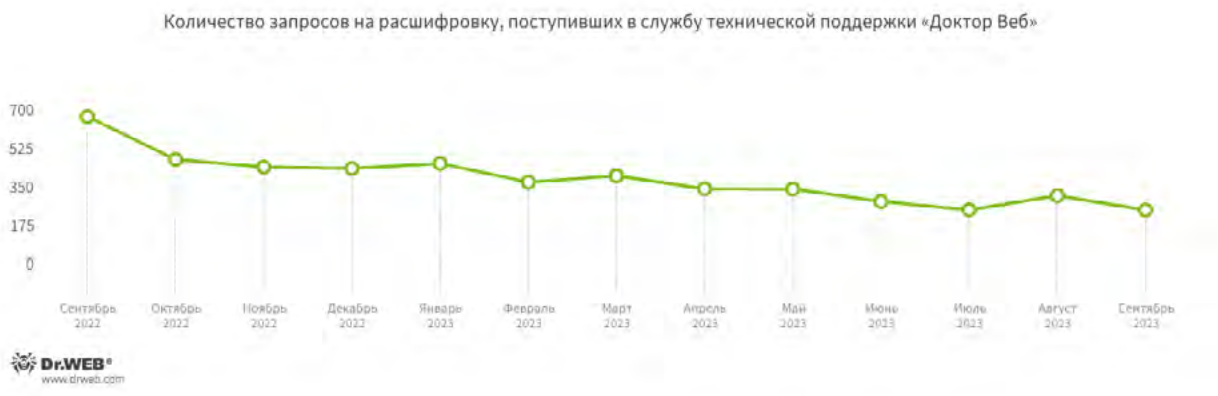
W97M.DownLoader.2938

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

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

Шифровальщики

В сентябре число запросов на расшифровку файлов, затронутых троянскими программами-шифровальщиками, снизилось на 19,64% по сравнению с августом.



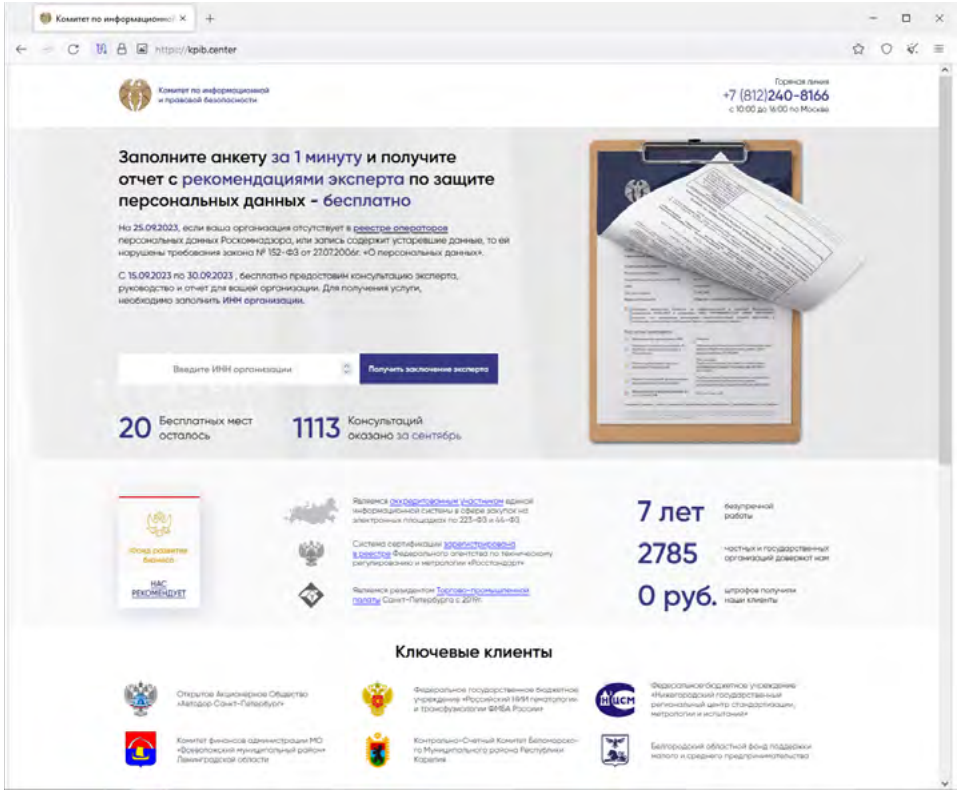
Наиболее распространенные энкодеры сентября:

- Trojan.Encoder.26996 — 24.64%
- Trojan.Encoder.3953 — 19.43%
- Trojan.Encoder.35534 — 5.21%
- Trojan.Encoder.35067 — 3.32%
- Trojan.Encoder.24383 — 2.84%

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

Опасные сайты

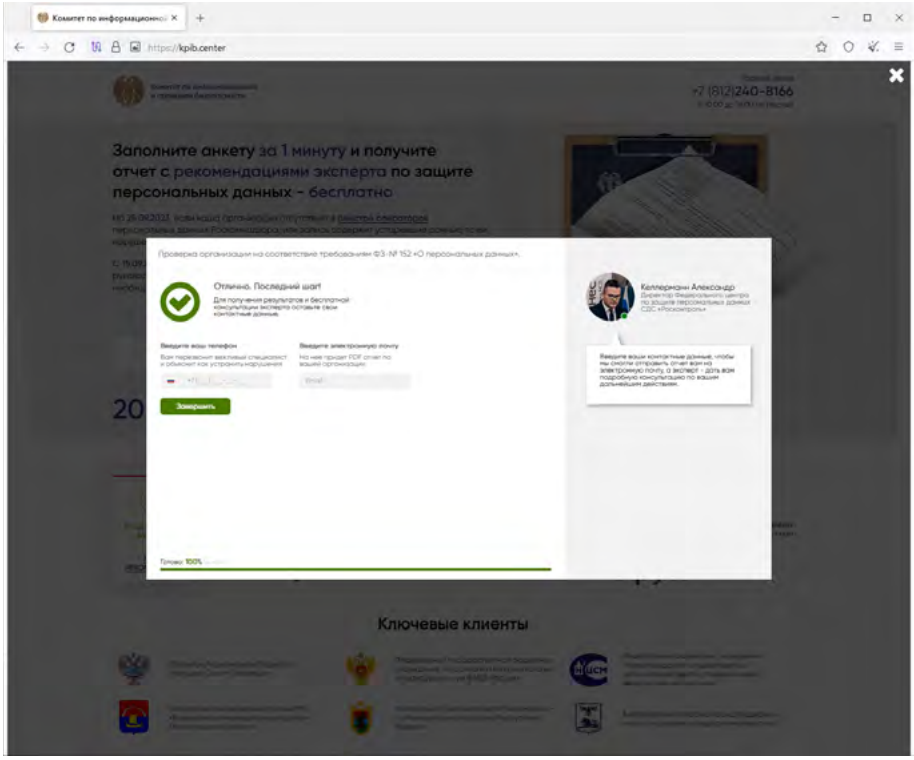
В сентябре 2023 года интернет-аналитики компании «Доктор Веб» отмечали высокую активность сетевых мошенников. Например, были зафиксированы случаи распространения нежелательных писем, отправленных якобы от имени налоговых органов. Такие письма содержали ссылку на сайт, на котором посетителям предлагалось проверить организации и предприятия на соответствие требованиям закона о персональных данных (№ 152-ФЗ «О персональных данных»). Для этого вначале требовалось пройти небольшой опрос, после чего указать персональные данные «для получения результатов и бесплатной консультации эксперта».



Скриншот выше показывает, как на одном из таких сайтов посетителям предлагается «заполнить анкету за 1 минуту и получить отчет с рекомендациями эксперта по защите персональных данных - бесплатно».

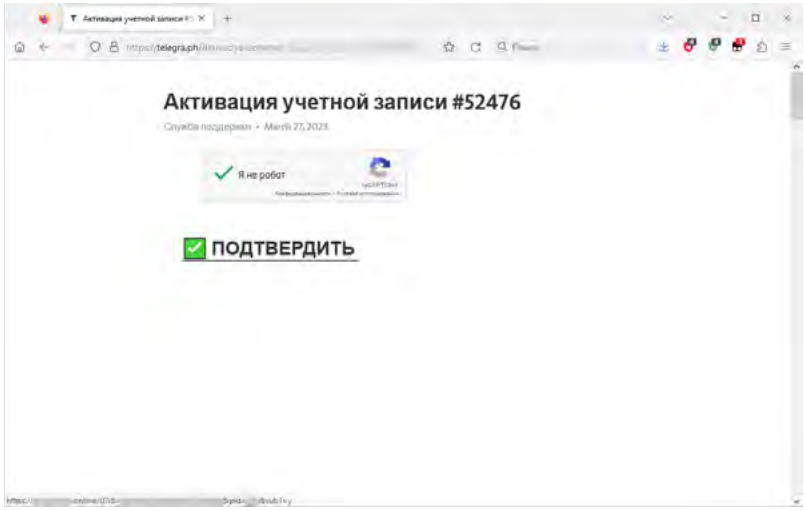
Опасные сайты

После ответа на предварительные вопросы у пользователя запрашивается номер телефона и email:

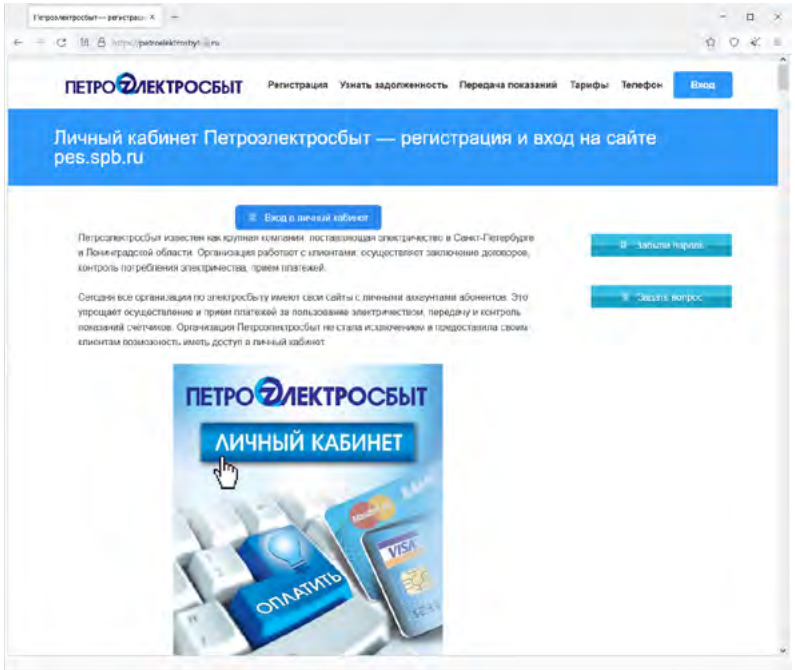


Наши специалисты также отмечали случаи распространения ссылок на фишинговые сайты через блог-платформу Telegraph. Злоумышленники публикуют в ней записи, оформленные в стиле форм подтверждения регистрации учетных записей в тех или иных онлайн-сервисах. При нажатии на элемент с текстом «ПОДТВЕРДИТЬ» потенциальные жертвы перенаправляются на фишинговые веб-ресурсы. Среди них — мошеннические сайты инвестиционной тематики.

Опасные сайты



Кроме того, были выявлены очередные поддельные сайты сервисов оплаты коммунальных услуг. С их помощью киберпреступники пытаются похитить персональные данные пользователей. На скриншоте ниже — пример сайта, который имитирует внешний вид интернет-портала одной из электроснабжающих организаций. Через него пользователи якобы могут войти в личный кабинет для оплаты счетов.



Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В сентябре 2023 года компания «Доктор Веб» опубликовала исследование троянский программы-бэкдора Android.Pandora.2, которая заражает смарт-телевизоры и приставки с Android TV. С ее помощью злоумышленники создают ботнет из инфицированных Android-устройств и выполняют DDoS-атаки.

Кроме того, наши вирусные аналитики рассказали о троянских программах Android.Spy.Lydia, которые реализуют шпионскую функциональность и нацелены на иранских пользователей.

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в сентябре владельцы Android-устройств реже сталкивались с вредоносными приложениями. В то же время возросло число детектирований рекламного ПО. При этом в течение месяца в каталоге Google Play были выявлены новые угрозы. Среди них — рекламные троянские программы Android.HiddenAds, вредоносные приложения Android.Joker, которые подписывали пользователей на платные услуги, а также используемые мошенниками трояны Android.FakeApp.

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

- снижение активности вредоносных программ,
- обнаружение новых троянских приложений в каталоге Google Play.

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

«Доктор Веб»: обзор вирусной активности в сентябрь 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

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