«Доктор Веб»: обзор вирусной активности в сентябре 2022 года

«Доктор Веб»: обзор вирусной активности в сентябре 2022 года

31 октября 2022 года

В сентябре анализ статистики детектирований антивируса Dr.Web показал снижение общего числа обнаруженных угроз на 9,29% по сравнению с августом. Одновременно с этим уменьшилось и количество уникальных угроз — на 38,95%. Как и ранее, пользователи чаще всего сталкивались с рекламными приложениями. В почтовом трафике наибольшее распространение получили вредоносные скрипты, а также применяемые в фишинг-атаках вредоносные PDF-файлы. Кроме того, злоумышленники не оставляли попыток заразить компьютеры пользователей при помощи рассылки приложений, использующих уязвимости документов Microsoft Office.

В минувшем месяце число обращений пользователей за расшифровкой файлов выросло на 41,26%. Самым распространенным энкодером сентября стал Trojan.Encoder.3953 с долей 25,83% от общего числа зафиксированных инцидентов, в то время как многомесячный лидер Trojan.Encoder.26996 опустился на второе место.

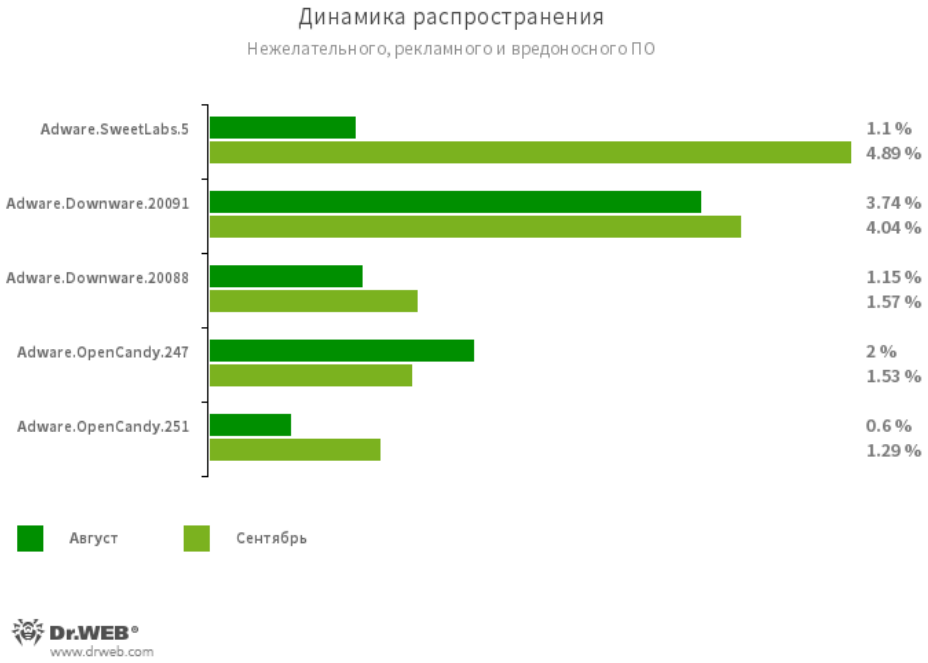
Вирусные аналитики компании «Доктор Веб» выявили новые угрозы в каталоге Google Play. Среди них — троянские программы-подделки семейства Android.FakeApp, которые злоумышленники используют в различных мошеннических схемах, а также рекламные приложения.

ГЛАВНЫЕ ТЕНДЕНЦИИ СЕНТЯБРЯ

- Снижение общего числа обнаруженных угроз
- Значительный рост числа обращений пользователей за расшифровкой файлов, пострадавших от троянов-шифровальщиков
- Активное распространение вредоносных PDF-документов через сообщения электронной почты
- Появление новых угроз в Google Play

«Доктор Веб»: обзор вирусной активности в сентябре 2022 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.20091
- Adware.Downware.20088

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Adware.OpenCandy.247
Adware.OpenCandy.251

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

«Доктор Веб»: обзор вирусной активности в сентябре 2022 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.

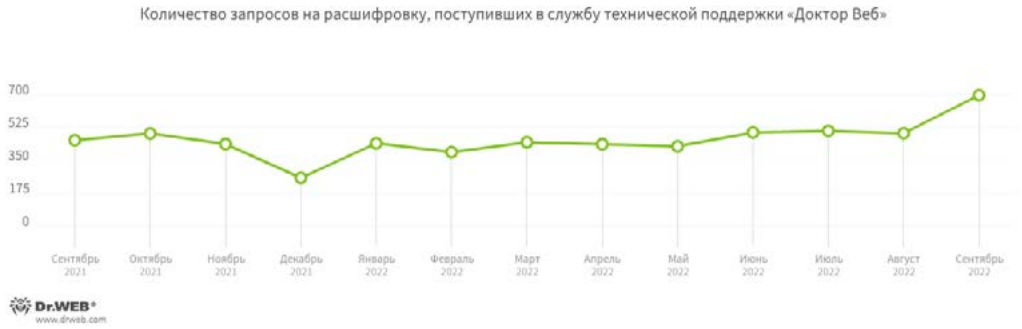
- PDF.Fisher.367
- PDF.Fisher.371
- PDF.Fisher.366

PDF-документы, используемые в фишинговых email-рассылках.

«Доктор Веб»: обзор вирусной активности в сентябре 2022 года

Шифровальщики

В сентябре число запросов на расшифровку файлов, затронутых троянами-шифровальщиками, увеличилось на 41,26% по сравнению с августом.



- Trojan.Encoder.3953 — 25.83%
- Trojan.Encoder.26996 — 23.94%
- Trojan.Encoder.11539 — 2.61%
- Trojan.Encoder.567 — 2.37%
- Trojan.Encoder.35209 — 1.90%

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

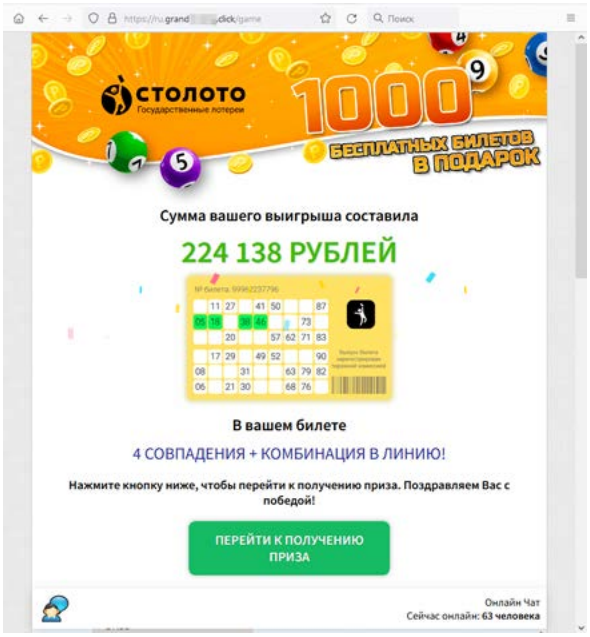
Настрой-ка Dr.Web от шифровальщиков
Обучающий курс
О бесплатном восстановлении
Dr.Web Rescue Pack

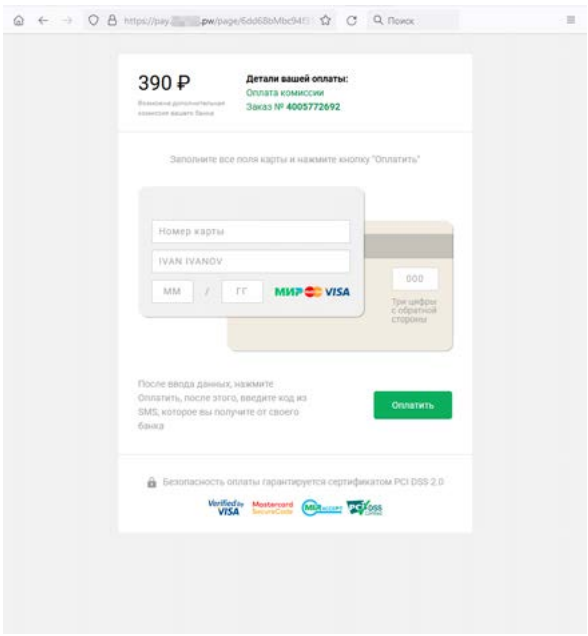
«Доктор Веб»: обзор вирусной активности в сентябре 2022 года

Опасные сайты

В сентябре 2022 года интернет-аналитики компании «Доктор Веб» вновь фиксировали массовое распространение спам-писем со ссылками на мошеннические сайты. Среди них — сайты, на которых российские пользователи якобы могли получить бесплатные лотерейные билеты. На самом деле никаких билетов не предоставлялось, и злоумышленники вводили в заблуждение потенциальных жертв, имитируя розыгрыш призов. При этом каждому посетителю сообщалось, что он победитель. Для «получения» приза от пользователей требовалось указать данные банковской карты и заплатить «комиссию» за перевод.

Ниже представлены примеры двух сайтов — на одном имитируется розыгрыш лотереи и сообщается о выигрыше, а на другом якобы осуществляется оплата комиссии за перевод выигрыша на банковскую карту жертвы:

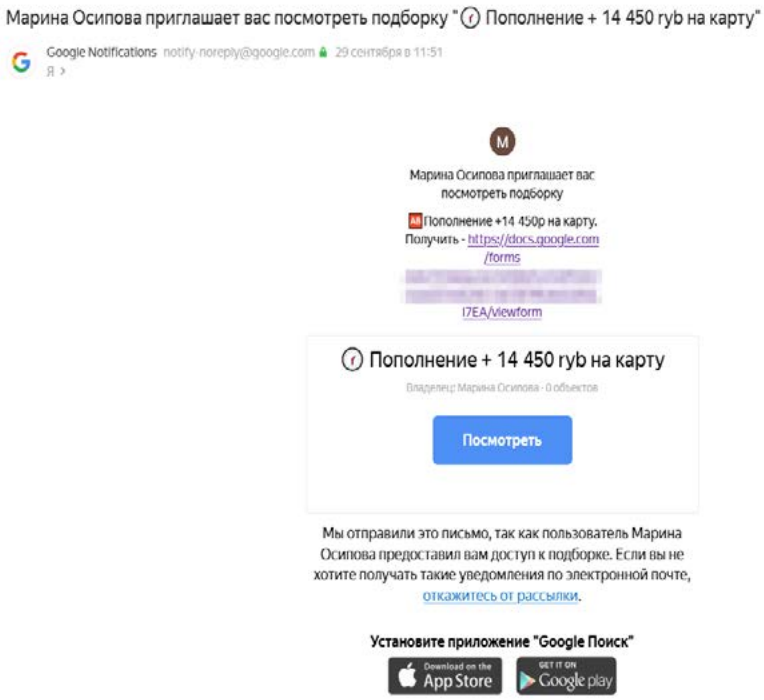




На других сайтах пользователям предлагалось стать участниками различных инвестиционных платформ, якобы аффилированных с известными финансовыми и нефтегазовыми компаниями. Для этого требовалось пройти опрос и зарегистрировать учетную запись, указав имя и фамилию, адрес электронной почты и номер телефона. После «регистрации» жертвы такого обмана обычно перенаправляются на различные веб-сайты, в том числе — нежелательные. Кроме того, киберпреступники в дальнейшем могут использовать предоставляемые данные для проведения фишинг-атак или организации мошеннических телефонных звонков.

Опасные сайты

Пример фишингового письма, в котором говорится о возможности безвозмездного получения денег на банковскую карту. Для этого потенциальной жертве предлагается перейти по ссылке. При переходе по ней загружается мошеннический сайт с информацией о «легком заработке» и рекламой другого мошеннического интернет-ресурса, якобы имеющего отношение к крупному российскому банку.



Вредоносное и нежелательное ПО для мобильных устройств

В минувшем месяце наблюдался рост активности банковских троянских приложений, атакующих владельцев Android-устройств. При этом несколько снизилась активность вредоносных программ, предназначенных для демонстрации нежелательной рекламы. В то же время отмечалось очередное снижение активности троянской программы-шпиона Android.Spy.4498, которая похищает информацию из уведомлений от других приложений.

В течение сентября специалисты вирусной лаборатории «Доктор Веб» выявили новые угрозы в каталоге Google Play. Среди них — очередные вредоносные программы семейства Android.FakeApp, которые злоумышленники используют в различных мошеннических схемах, а также программы с нежелательными рекламными модулями.

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

- рост активности банковских троянских приложений;
- незначительное снижение активности рекламных троянских программ;
- продолжилось снижение активности трояна-шпиона Android.Spy.4498;
- появление новых угроз в каталоге Google Play.

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

«Доктор Веб»: обзор вирусной активности в сентябре 2022 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