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

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

23 декабря 2022 года

В ноябре анализ статистики детектирований антивируса Dr.Web показал снижение общего числа обнаруженных угроз на 8,58% по сравнению с октябрем. В то же время число уникальных угроз выросло на 3,27%. Наибольшую активность вновь проявили всевозможные рекламные приложения. В почтовом трафике преобладали вредоносные скрипты, трояны-загрузчики, рекламные программы и угрозы, которые для заражения атакуемых компьютеров эксплуатируют различные уязвимости.

Число обращений пользователей за расшифровкой файлов в минувшем месяце снизилось на 6,8% по сравнению с октябрем. Наиболее часто жертвы энкодеров сталкивались с троянской программой Trojan.Encoder.26996 — она стала причиной 28,24% зафиксированных инцидентов. Второй по распространенности оказалась вредоносная программа Trojan.Encoder.3953 с долей 22,19%. На третьем месте расположился Trojan.Encoder.567 — он стал виновником 2,88% выявленных случаев повреждения пользовательских файлов.

В течение ноября вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play множество новых угроз для ОС Android. Среди них — вредоносные программы, которые загружали мошеннические веб-сайты, а также троянские приложения, которые подписывали жертв на платные услуги.

ГЛАВНЫЕ ТЕНДЕНЦИИ НОЯБРЯ

- Снижение общего числа обнаруженных угроз
- Снижение числа обращений пользователей за расшифровкой файлов, пострадавших от троянов-шифровальщиков
- Вновь выявлены угрозы в каталоге Google Play

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

По данным сервиса статистики «Доктор Веб»

Угрозы прошедшего месяца:

- Adware.SweetLabs.5

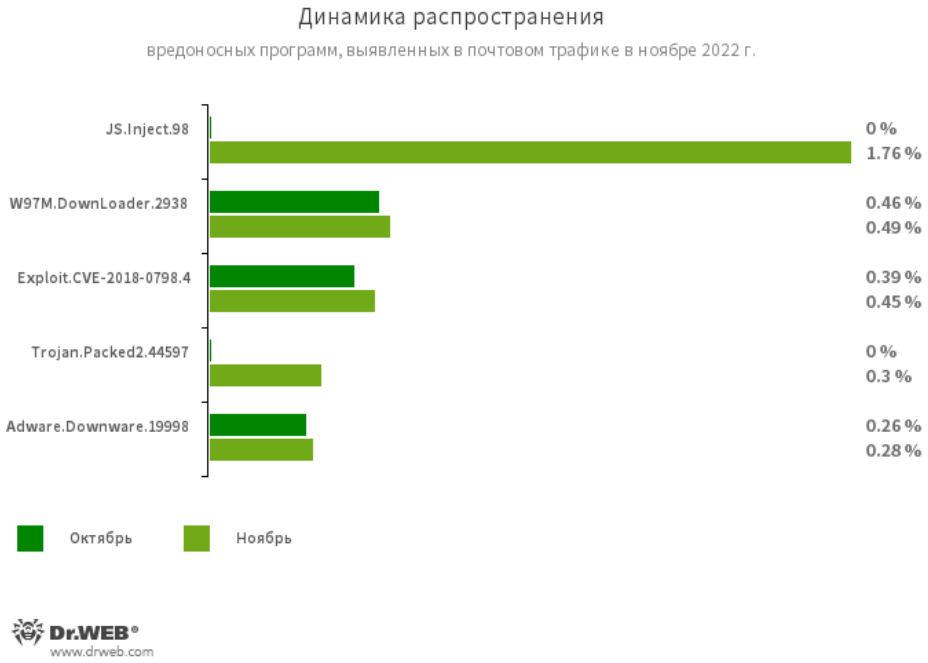
Альтернативный каталог приложений и надстройка к графическому интерфейсу Windows от создателей Adware.Opencandy.

- Adware.Downware.20091
- Adware.Downware.20088
- Adware.Downware.20261
- Adware.Downware.20272

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

«Доктор Веб»: обзор вирусной активности в ноябре 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.

- Exploit.CVE-2018-0798.4

Эксплойт для использования уязвимости в ПО Microsoft Office, позволяющий выполнить произвольный код.

- Trojan.Packed2.44597

Троянская программа-загрузчик, написанная на C#. Она загружает широкий спектр вредоносных приложений на атакуемые компьютеры, например — представителей семейств Formbook, SnakeKeylogger, AgentTesla, Redline, AsyncRAT и другие.

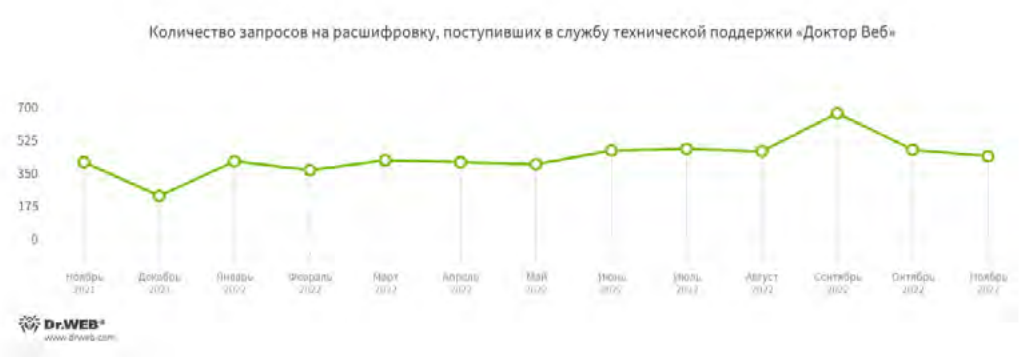
- Adware.Downware.19998

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

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

Шифровальщики

В минувшем месяце число запросов на расшифровку файлов, испорченных троянами-шифровальщиками, снизилось на 6,8% по сравнению с октябрем.



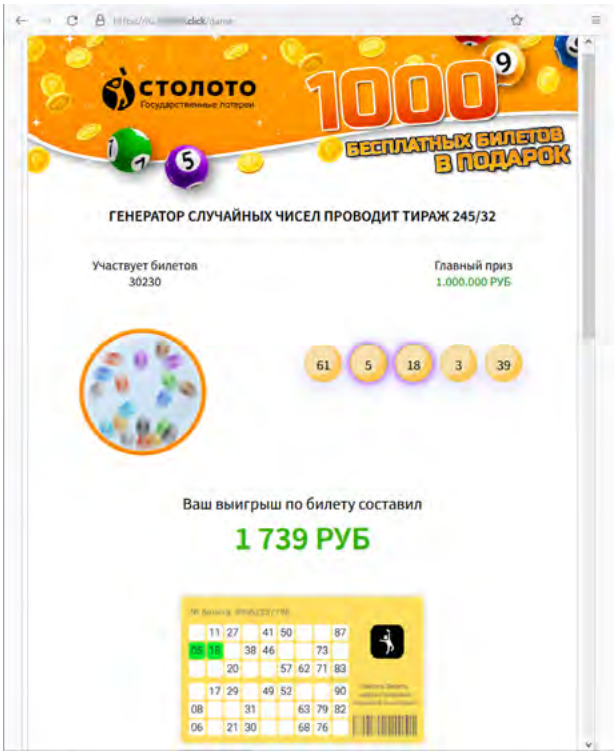
- Trojan.Encoder.26996 — 28.24%
- Trojan.Encoder.3953 — 22.19%
- Trojan.Encoder.567 — 2.88%
- Trojan.Encoder.34027 — 2.31%
- Trojan.Encoder.30356 — 1.73%

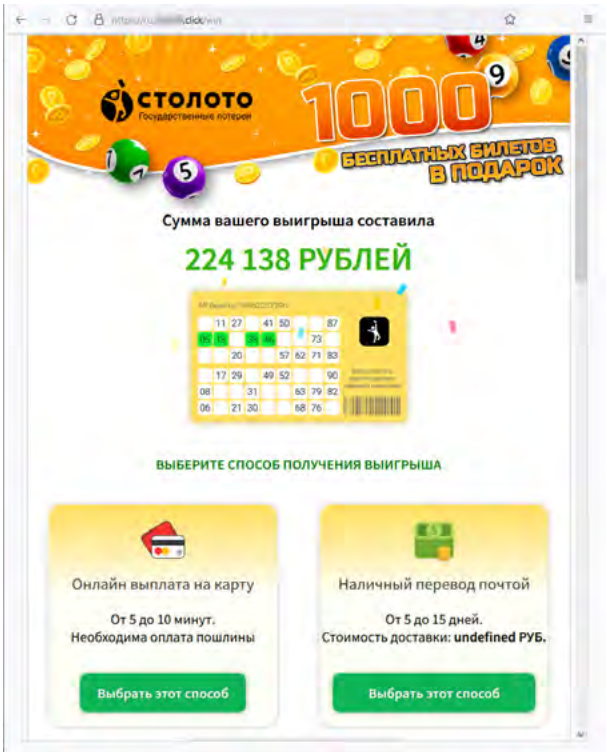
Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

Опасные сайты

В ноябре 2022 года интернет-аналитики «Доктор Веб» продолжили фиксировать фишинговые рассылки и атаки с применением различных мошеннических сайтов. Среди таких сайтов вновь были отмечены ресурсы, которые вводили пользователей в заблуждение якобы выгодными предложениями. Например, получить бесплатные лотерейные билеты или принять участие в различных акциях известных интернет-магазинов и компаний.

На скриншотах ниже показан пример мошеннического сайта, где по заранее заготовленному сценарию имитируется розыгрыш лотереи и сообщается о выигрыше. Для «получения» денег потенциальной жертве предлагается оплатить пошлину или комиссию. Если пользователь поверит и согласится на оплату, его деньги уйдут мошенникам. Кроме того, он рискует раскрыть данные своей банковской карты.

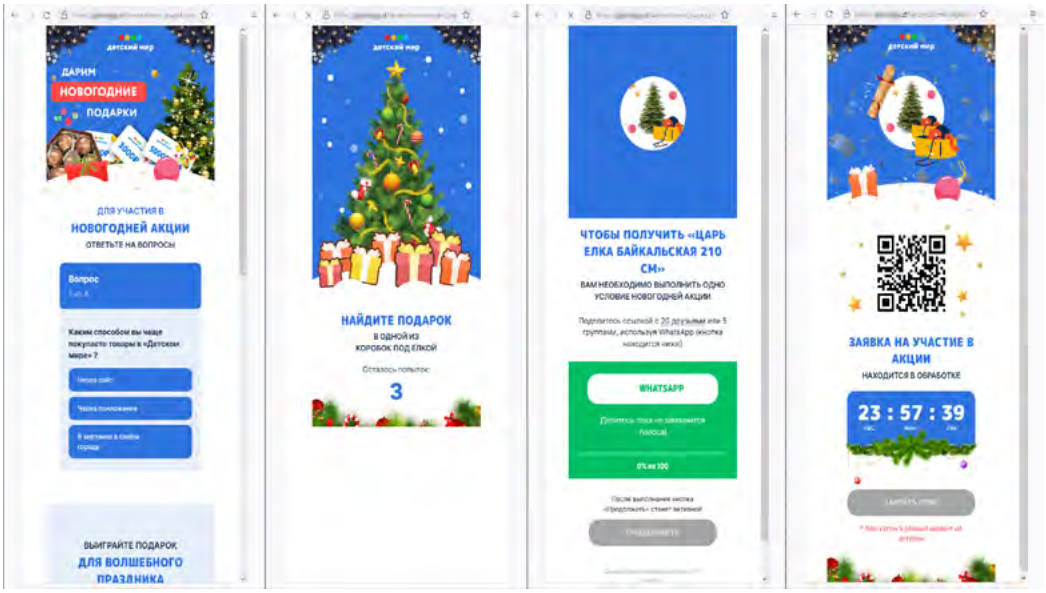




На следующем изображении — поддельный сайт крупного российского ритейлера, где потенциальной жертве мошенников предлагается принять участие в новогодней акции с перспективой получить подарок. Вначале пользователь должен пройти опрос, а затем — поучаствовать в мини-игре и угадать, в какой из коробок находится приз. Как и в предыдущем случае, факт выигрыша здесь заранее предопределен. Для «получения» подарка пользователь должен поделиться предоставленной ему ссылкой с определенным числом контактов или групп в мес-

Опасные сайты

сенджере WhatsApp. При этом подвох заключается в том, что такая ссылка будет вести не на текущий, как могла бы предположить жертва, а на какой-либо другой сайт. В том числе это может быть сайт с фишингом или рекламой, либо веб-ресурс, распространяющий вредоносные приложения. После того как введенный в заблуждение пользователь распространит ссылку на сомнительный сайт среди большого числа своих контактов, он увидит сообщение с ложной информацией о том, что его заявка на участие в акции якобы находится в обработке.



Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

Согласно данным статистики детектирований антивируса Dr.Web для Android, в ноябре возросла активность банковских, а также рекламных троянских приложений. В то же время пользователи реже сталкивались с программами, содержащими нежелательные рекламные модули.

В течение месяца наши вирусные аналитики выявили в каталоге Google Play десятки новых вредоносных приложений. Среди них — множество программ-подделок из семейства Android.FakeApp, которые злоумышленники используют в различных мошеннических схемах, а также троянские программы Android.Joker и Android.Subscription, подписывающие жертв на платные услуги.

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

- рост активности банковских и рекламных троянских программ;
- появление новых угроз в каталоге Google Play.

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

«Доктор Веб»: обзор вирусной активности в ноябре 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