Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности в ноябре 2021 года

«Доктор Веб»: обзор вирусной активности в ноябре 2021 года

9 декабря 2021 года

В ноябре анализ данных статистики Dr.Web показал уменьшение общего числа обнаруженных угроз на 24.36% по сравнению с октябрем. Количество уникальных угроз уменьшилось на 7.66%. Большинство детектирований по-прежнему приходится на долю рекламных программ и нежелательных приложений. В почтовом трафике чаще всего распространялось разнообразное вредоносное ПО, в том числе загружающее нежелательные приложения на компьютер жертвы.

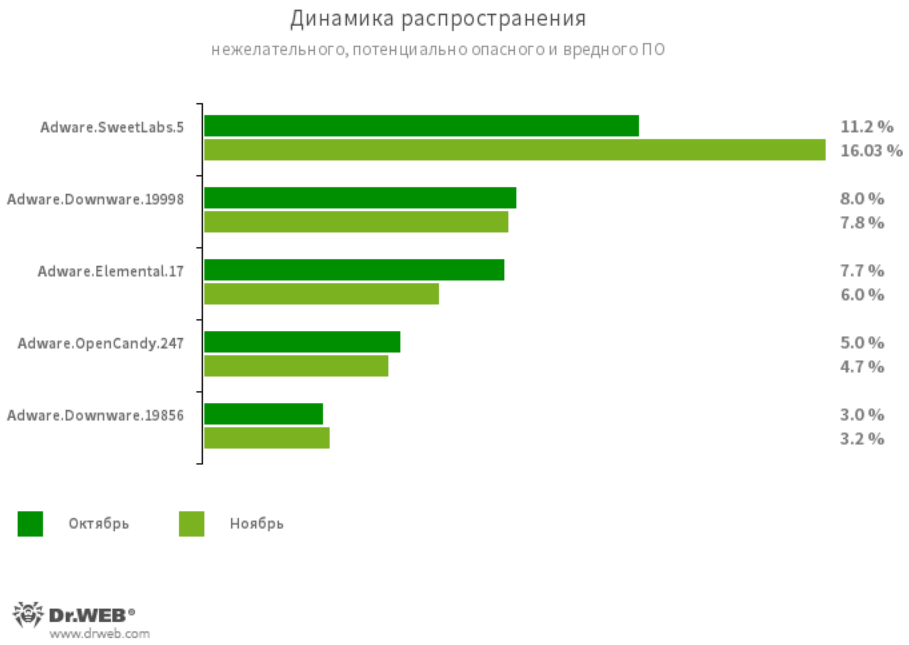
Число обращений пользователей за расшифровкой файлов уменьшилось на 11.4% по сравнению с октябрем. Самым распространенным энкодером месяца стал Trojan.Encoder.26996, на долю которого пришлось 32.93% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ НОЯБРЯ

- Существенное уменьшение общего числа угроз
- Рекламные приложения по-прежнему остаются главной угрозой
- Снижение количества обращений за расшифровкой файлов

«Доктор Веб»: обзор вирусной активности в ноябре 2021 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.19998

Adware.Downware.19856

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Adware.Elemental.17

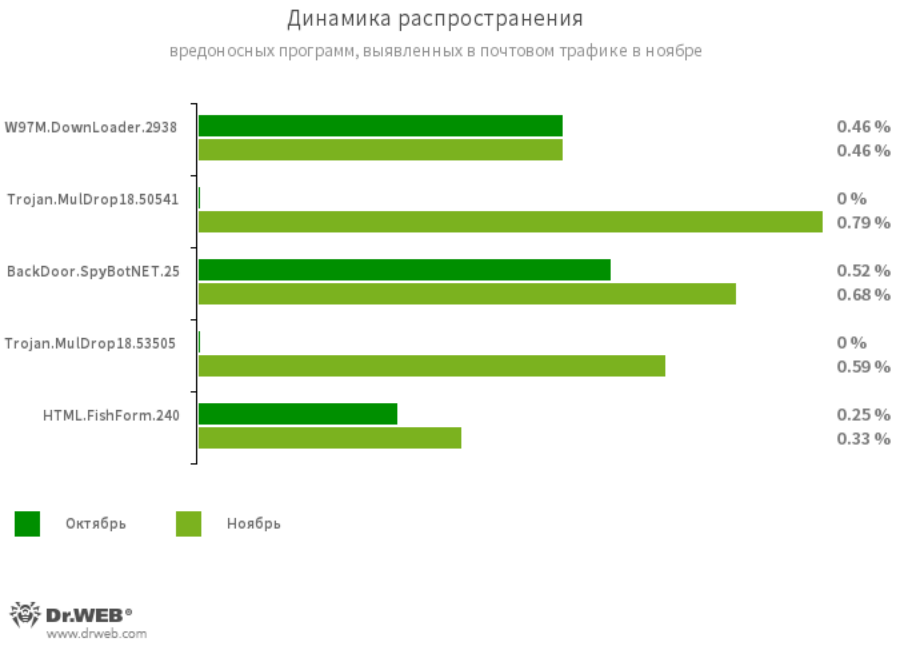
Семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают приложения с рекламой, а также инсталлируют ненужное ПО.

Adware.OpenCandy.247

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

«Доктор Веб»: обзор вирусной активности в ноябре 2021 года

Статистика вредоносных программ в почтовом трафике



W97M.DownLoader.2938

Семейство троянов-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Trojan.MulDrop18.50541

Trojan.MulDrop18.53505

Вредоносная программа, загружающая нежелательные приложения на компьютер жертвы.

BackDoor.SpyBotNET.25

Бэкдор, написанный на VB.NET. Способен манипулировать файловой системой (копирование, удаление, создание директорий и т. д.), завершать процессы, делать снимки экрана.

HTML.FishForm.240

Веб-страница, распространяющаяся в фишинговых рассылках. Представляет собой фиктивную форму ввода учетных данных, которая имитирует авторизацию на известных сайтах.

Шифровальщики

По сравнению с октябрем, в ноябре число запросов на расшифровку файлов, затронутых шифровальщиками, уменьшилось на 7.66%.

- Trojan.Encoder.26996 — 32.93%
- Trojan.Encoder.567 — 10.77%
- Trojan.Encoder.3953 — 4.31%
- Trojan.Encoder.11539 — 3.38%
- **Trojan.Encoder.30356** — 2.77%

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

Настрой-ка Dr.Web от шифровальщиков

Обучающий курс

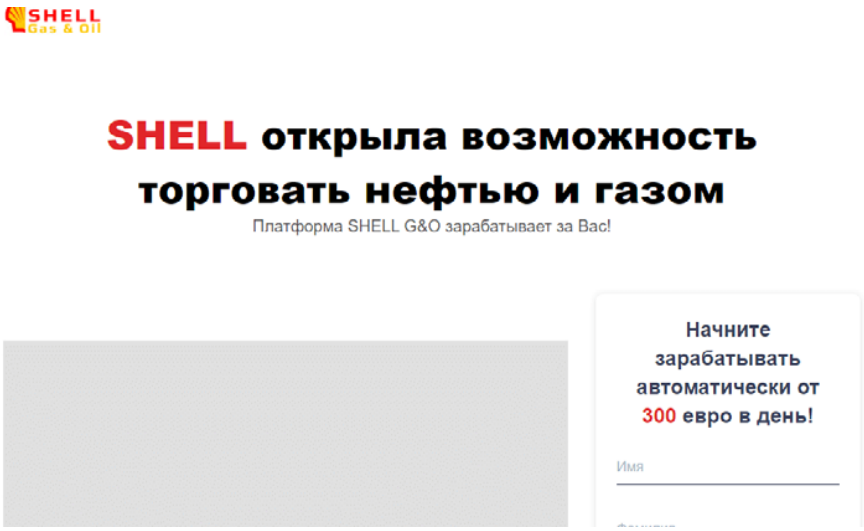
О бесплатном восстановлении

Dr.Web Rescue Pack

В ноябре 2021 года интернет-аналитики «Доктор Веб» заметили увеличение числа сайтов, ма-

Опасные сайты

скирующихся под веб-ресурсы крупнейших нефтяных компаний мира. Мошенники предлагают любому желающему инвестировать в нефтяные продукты и зарабатывать от 300 евро в день.



На скриншоте изображена фишинговая страница Shell, на которой злоумышленники призывают инвестировать вместе с известной компанией.

Узнайте больше о нерекомендуемых Dr.Web сайтах

В ноябре компания «Доктор Веб» опубликовала исследование, направленное на поиск потенци-

Вредоносное и нежелательное ПО для мобильных устройств

альных уязвимостей в детских смарт-часах. Результаты данного исследования показали, что уровень их безопасности неудовлетворителен. В частности, на некоторых моделях таких устройств могут быть предустановлены троянские приложения.

В течение прошедшего месяца наши вирусные аналитики выявили новые угрозы в каталогах Google Play и AppGallery, среди которых были трояны-шпионы и трояны, подписывающие жертв на платные услуги. При этом антивирусные продукты Dr.Web для Android чаще всего детектировали рекламных троянов, а также вредоносные программы, способные выполнять произвольный код и загружать другое ПО.

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

- высокая активность рекламных троянов;
- появление новых вредоносных приложений в каталоге Google Play;
- появление нового трояна в каталоге AppGallery.

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

«Доктор Веб»: обзор вирусной активности в ноябре 2021 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