Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности в декабре 2020 года

«Доктор Веб»: обзор вирусной активности в декабре 2020 года

28 декабря 2020 года

В декабре анализ данных статистики Dr.Web показал уменьшение общего числа обнаруженных угроз на 11.49% по сравнению с ноябрем. Количество уникальных угроз также снизилось — на 24.51%. По общему количеству детектирований лидируют рекламные программы и вредоносные расширения для браузеров. В почтовом трафике на первых позициях находится разнообразное вредоносное ПО, в том числе банковский троян Trojan.SpyBot.699, обфусцированный стилер, написанный на VB.NET, а также программы, использующие уязвимости документов Microsoft Office.

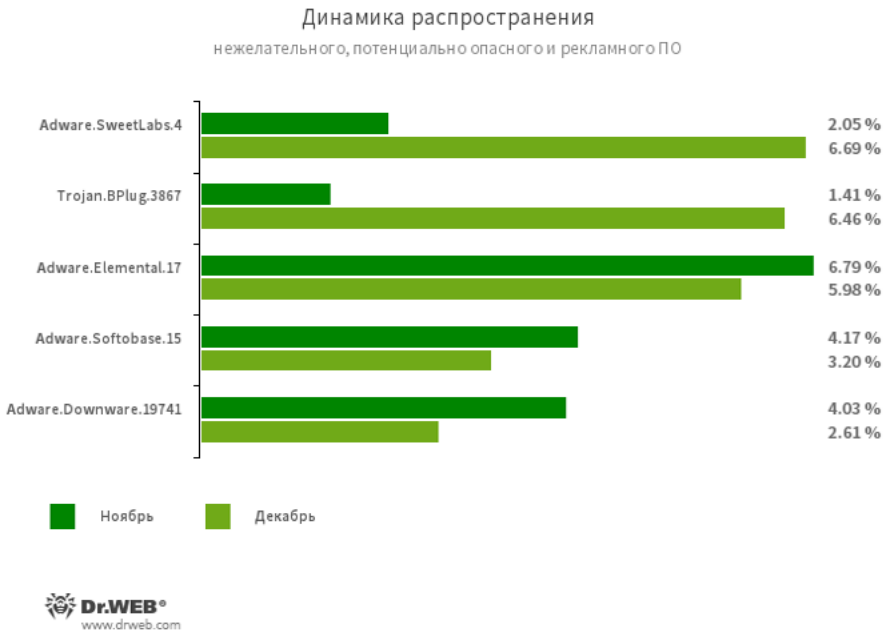
Число обращений пользователей за расшифровкой файлов снизилось на 31.54% по сравнению с ноябрем. Самым распространенным энкодером остается Trojan.Encoder.26996, на долю которого приходится 37.14% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ ДЕКАБРЯ

- Снижение активности распространения вредоносного ПО
- Рекламные приложения остаются в числе самых активных угроз
- Снижение количества уникальных угроз в почтовом трафике

«Доктор Веб»: обзор вирусной активности в декабре 2020 года

По данным серверов статистики «Доктор Веб»



Угрозы прошедшего месяца:

Adware.SweetLabs.4

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

Trojan.BPlug.3867

Вредоносное расширение для браузера, предназначенное для веб-инжектов в просматриваемые пользователями интернет-страницы и блокировки сторонней рекламы.

Adware.Elemental.17

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

Adware.Softobase.15

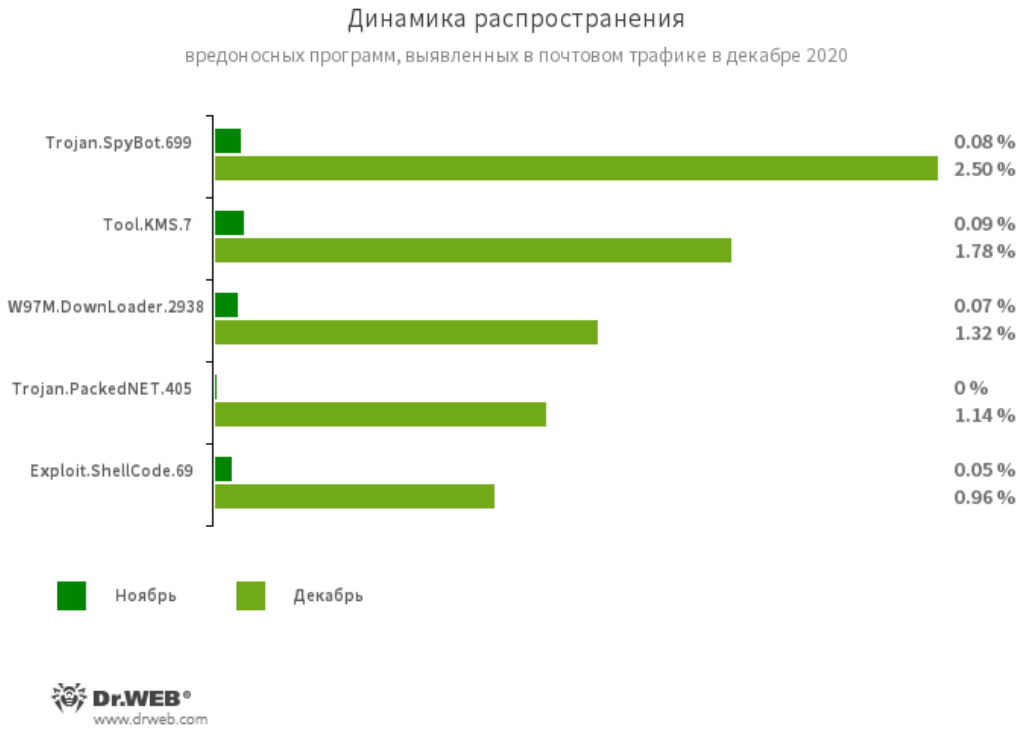
Программа-установщик, распространяющая устаревшее программное обеспечение. Меняет настройки браузера.

Adware.Downware.19741

Рекламное ПО, часто выступающее в роли промежуточного установщика пиратских программ.

«Доктор Веб»: обзор вирусной активности в декабре 2020 года

Статистика вредоносных программ в почтовом трафике



Trojan.SpyBot.699

Многомодульный банковский троян. Позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и исполнять произвольный код.

Tool.KMS.7

Хакерские утилиты, которые используются для активации продуктов Microsoft с поддельной лицензией.

W97M.DownLoader.2938

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

Trojan.PackedNET.405

Обфусцированная версия стилера, написанного на VB.NET. Имеет функциональность кейлоггера и используется для кражи конфиденциальной информации.

Exploit.ShellCode.69

Вредоносный документ Microsoft Office Word. Использует уязвимость CVE-2017-11882.

«Доктор Веб»: обзор вирусной активности в декабре 2020 года

Шифровальщики

Запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков, в декабре в антивирусную лабораторию «Доктор Веб» поступило на 28.41% меньше, чем в ноябре..

- Trojan.Encoder.26996 — 37.14%
- Trojan.Encoder.567 — 20.00%
- Trojan.Encoder.29750 — 3.17%
- Trojan.Encoder.11549 — 1.27%
- Trojan.Encoder.30356 — 1.27%

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 декабре 2020 года

Опасные сайты

В течение декабря 2020 года в базу нерекомендуемых и вредоносных сайтов было добавлено 105 840 интернет-адресов.

Ноябрь 2020	Декабрь 2020	Динамика
+ 154 606	+ 105 840	- 31.54%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

Согласно статистике детектирований, полученной антивирусными продуктами Dr.Web для Android, в декабре на защищаемых Android-устройствах было выявлено на 25,34% меньше угроз по сравнению с ноябрем. При этом наиболее часто пользователи сталкивались с рекламными троянами, а также вредоносными приложениями, загружающими другое ПО и выполняющими произвольный код.

Очередная угроза была обнаружена в каталоге Google Play. Это оказался троян Android.Joker.477, который скрывался в приложении с коллекцией изображений. Он подписывал жертв на дорогостоящие мобильные сервисы и мог загружать и выполнять произвольный код.

Кроме того, в декабре пользователей Android-устройств атаковали различные банковские трояны.

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

- снижение общего числа угроз, выявленных на защищаемых Android-устройствах;
- обнаружение новой вредоносной программы в каталоге Google Play.

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

«Доктор Веб»: обзор вирусной активности в декабре 2020 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
ВебIQметр | Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125040, 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