Dr.WEB®
с 1992 года

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

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

16 декабря 2020 года

В ноябре анализ данных статистики Dr.Web показал незначительное уменьшение общего числа обнаруженных угроз — на 1.75% по сравнению с октябрем. Количество уникальных угроз при этом увеличилось на 5.26%. Чаще всего пользователей атаковали программы для показа рекламы, а также троянские загрузчики и установщики. В почтовом трафике на первых позициях находится разнообразное вредоносное ПО, в том числе бэкдор, написанный на .NET, банковский троян Trojan.SpyBot.699, а также программы, использующие уязвимости документов Microsoft Office.

Число обращений пользователей за расшифровкой файлов снизилось на 3.08% по сравнению с октябрем. Самым распространенным энкодером остается Trojan.Encoder.26996, на долю которого приходится 36.68% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ НОЯБРЯ

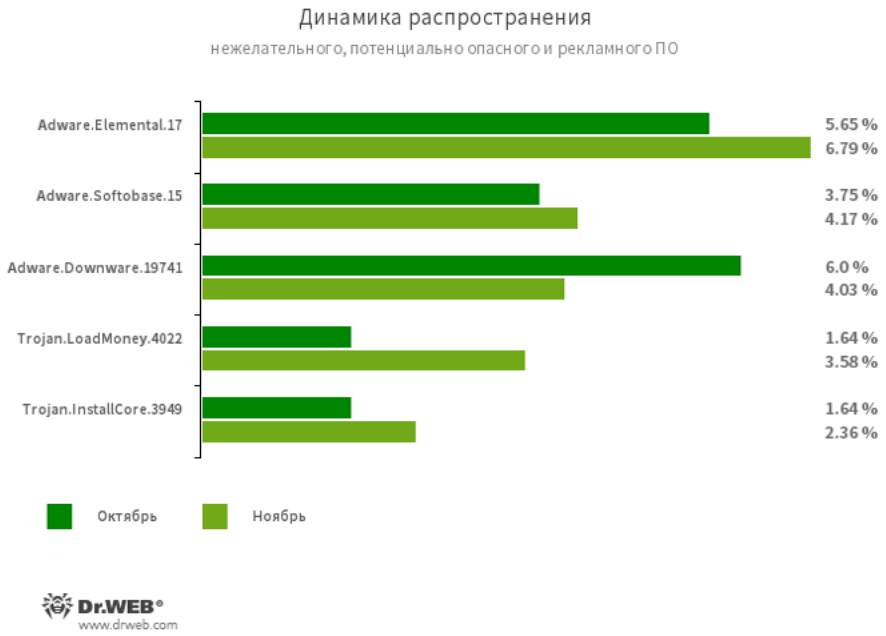
- Увеличение общего числа обнаруженного вредоносного ПО
- Рекламные приложения остаются в числе самых активных угроз

Угроза месяца

В ноябре вирусные аналитики компании «Доктор Веб» зафиксировали рассылку фишинговых писем корпоративным пользователям. Злоумышленники использовали метод социальной инженерии, чтобы заставить потенциальных жертв открыть вредоносные вложения. Письма содержали троянские программы, обеспечивающие скрытую установку и запуск утилиты Remote Utilities, компоненты которой также находились в составе вложения. В случае заражения компьютеры сотрудников оказывались доступны для удаленного управления без каких-либо визуальных признаков работы программы.

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

По данным серверов статистики «Доктор Веб»



Угрозы прошедшего месяца:

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.

Trojan.LoadMoney.4022

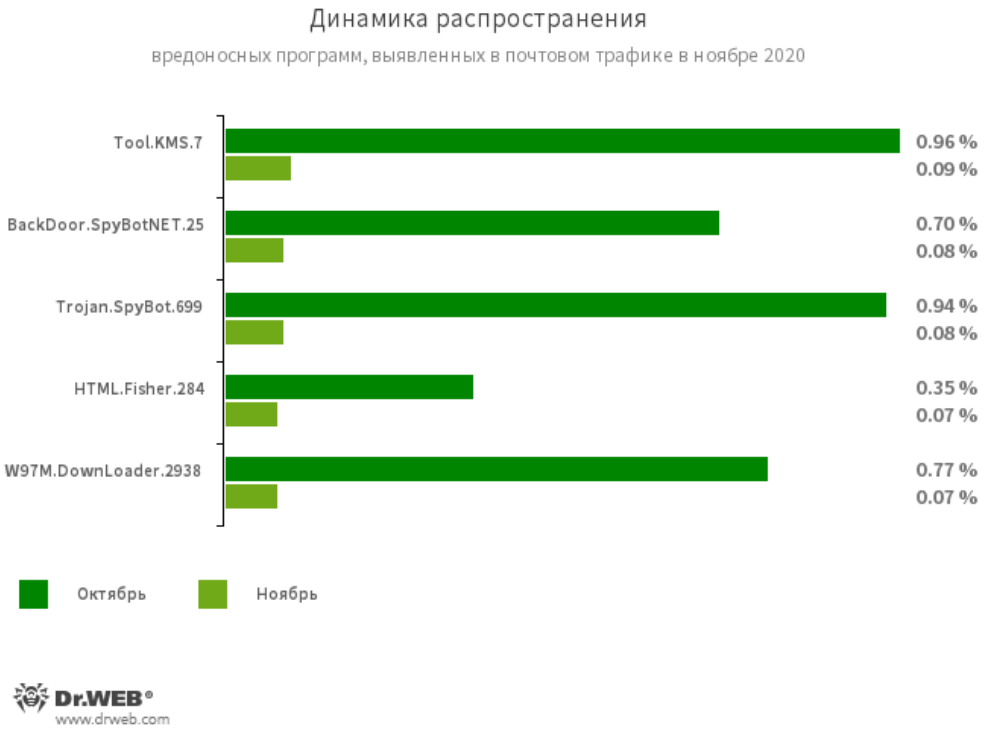
Семейство программ-установщиков, вместе с нужными приложениями инсталлирующих на компьютеры жертв всевозможные дополнительные компоненты. Некоторые модификации трояна могут собирать и передавать злоумышленникам различную информацию об атакованном компьютере.

Trojan.InstallCore.3949

Семейство обфусцированных установщиков рекламного и нежелательного ПО, использующее недобросовестные методы распространения.

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

Статистика вредоносных программ в почтовом трафике



Tool.KMS.7

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

BackDoor.SpyBotNET.25

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

Trojan.SpyBot.699

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

HTML.Fisher.284

Фишинговая HTML-страница с формой ввода логина и пароля от почты.

W97M.DownLoader.2938

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

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

Шифровальщики

По сравнению с прошлым месяцем, в ноябре запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков, в антивирусную лабораторию «Доктор Веб» поступило на 3.08% меньше.

- Trojan.Encoder.26996 — 36.68%
- Trojan.Encoder.567 — 10.03%
- Trojan.Encoder.29750 — 4.49%
- Trojan.Encoder.11464 — 1.85%
- Trojan.Encoder.30356 — 1.85%

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

Опасные сайты

В течение ноября 2020 года в базу нерекомендуемых и вредоносных сайтов было добавлено 154 606 интернет-адресов.

Октябрь 2020	Ноябрь 2020	Динамика
+ 157 076	+ 154 606	- 1.57%

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 ноябре на защищаемых устройствах было выявлено на 5.14% меньше угроз по сравнению с октябрем.

В каталоге Google Play по-прежнему появляются различные вредоносные приложения. Так, в прошедшем месяце вирусные аналитики «Доктор Веб» обнаружили в нем очередных троянов. Среди них были представители семейства Android.Joker, способные выполнять произвольный код и подписывать пользователей на дорогостоящие мобильные услуги, а также многофункциональный троян Android.Mixi.44.origin.

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

- снижение общего числа угроз, обнаруженных на защищаемых Android-устройствах;
- обнаружение новых троянов 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 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