Dr.WEB®
с 1992 года

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

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

9 ноября 2020 года

В октябре анализ данных статистики Dr.Web показал значительное увеличение общего числа обнаруженных угроз — на 37.80% по сравнению с сентябрем. Количество уникальных вредоносных программ при этом снизилось на 2.64%. Рекламные программы и загрузчики вредоносного ПО по-прежнему лидируют по общему количеству детектирований. В почтовом трафике на первых позициях продолжает находиться банковский троян Trojan.SpyBot.699, а также вредоносное ПО, использующее уязвимости документов Microsoft Office. Кроме того, пользователям продолжают угрожать различные модификации вредоносных HTML-документов, распространяемых в виде вложений и перенаправляющих на фишинговые сайты.

Число обращений пользователей за расшифровкой файлов продолжает держаться на одном уровне четвертый месяц. Самым распространенным энкодером остается Trojan.Encoder.26996, на долю которого приходится 26.34% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ ОКТЯБРЯ

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

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

По данным серверов статистики «Доктор Веб»

Угрозы прошедшего месяца:

Adware.Downware.19741

Рекламное ПО, часто 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 эти приложения, которые показывают рекламу, а также инсталлируют ненужное ПО.

Adware.Softobase.15

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

Trojan.LoadMoney.4020

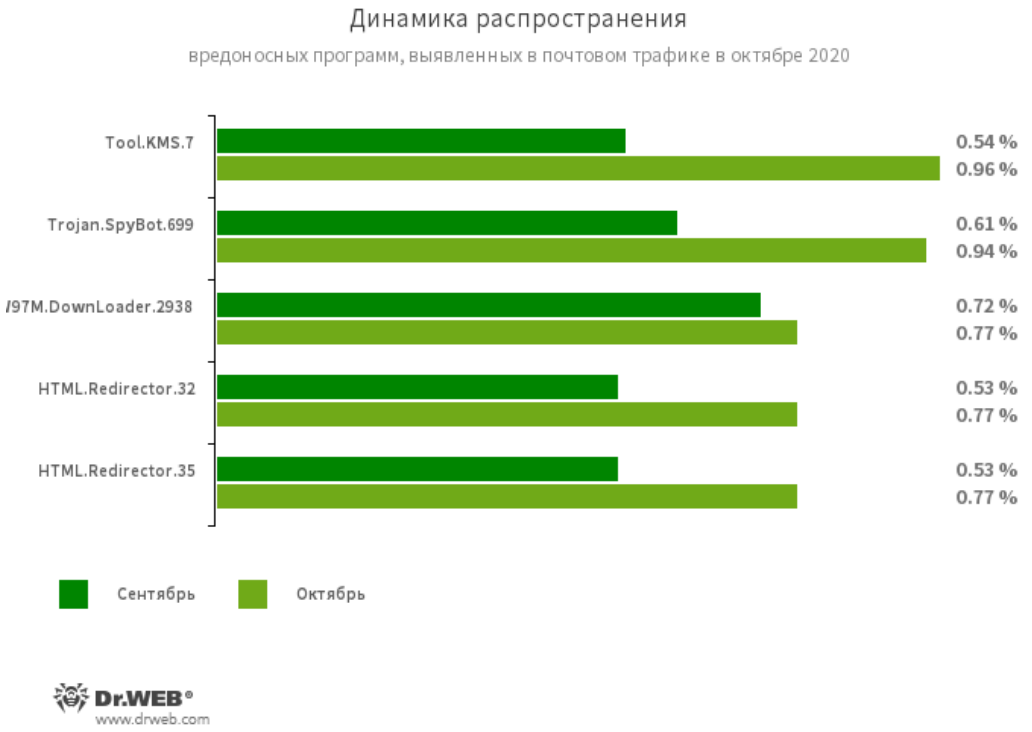
Семейство программ-установщиков, вместе с требуемыми приложениями инсталлирующих на компьютеры жертв всевозможные дополнительные компоненты. Некоторые модификации трояна могут собирать и передавать злоумышленникам различную информацию об атакованном компьютере.

Trojan.AutoIt.289

Утилита, написанная на скриптовом языке AutoIt и распространяемая в составе майнера или RAT-трояна. Выполняет различные вредоносные действия, затрудняющие обнаружение основной полезной нагрузки.

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

Статистика вредоносных программ в почтовом трафике



Tool.KMS.7

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

Trojan.SpyBot.699

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

W97M.DownLoader.2938

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

HTML.Redirector.33

HTML.Redirector.32

Вредоносные HTML-документы, как правило маскирующиеся под безобидные вложения к электронным письмам. При открытии перенаправляют пользователей на фишинговые сайты или загружают полезную нагрузку на заражаемые устройства.

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

Шифровальщики

По сравнению с прошлым месяцем в октябре в антивирусную лабораторию «Доктор Веб» поступило на 1.67% меньше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков.

- Trojan.Encoder.26996 — 26.34%
- Trojan.Encoder.567 — 9.84%
- Trojan.Encoder.29750 — 6.35%
- Trojan.Encoder.30356 — 2.54%
- Trojan.Encoder.858 — 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

Опасные сайты

В течение октября 2020 года в базу нерекомендуемых и вредоносных сайтов было добавлено 157 076 интернет-адресов

Сентябрь 2020	Октябрь 2020	Динамика
+ 152 270	+ 157 076	+ 3.16%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

Статистика детектирований угроз на Android-устройствах показала, что в минувшем октябре было выявлено на 12.36% больше угроз, чем в сентябре. При этом почти в 3 раза возросло число обнаружений потенциально опасных программ. Этот скачок произошел за счет распространения приложений, защищенных специализированным программным обфускатором, который злоумышленники могут использовать при создании троянов, усложняя их обнаружение антивирусами.

В течение октября наши специалисты выявили в каталоге Google Play множество новых вредоносных программ. Среди них были очередные трояны семейства Android.FakeApp, которые загружали мошеннические веб-сайты, а также рекламный троян, получивший имя Android.HiddenAds.2314.

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

- увеличение общего числа угроз, обнаруженных на защищаемых Android-устройствах;
- значительный рост числа выявленных потенциально опасных приложений, проникших на Android-устройства;
- распространение новых угроз через каталог Google Play.

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

«Доктор Веб»: обзор вирусной активности в октябре 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