Dr.WEB®
с 1992 года

Обзор вирусной активности в декабре 2018 года

Обзор вирусной активности в декабре 2018 года

28 декабря 2018 года

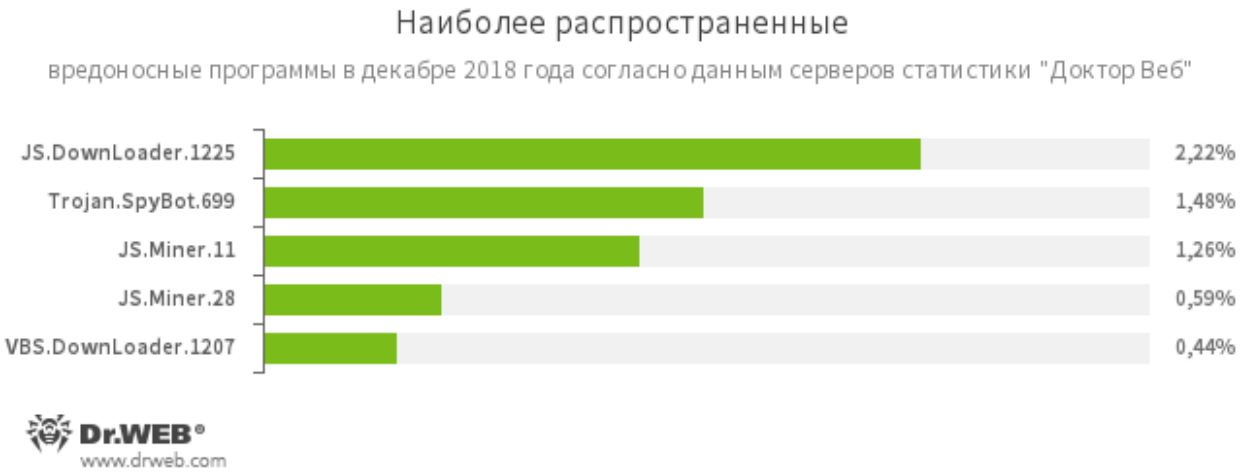
Последний месяц 2018 года не был отмечен какими-либо заметными событиями в сфере информационной безопасности. Среди обнаруживаемых на компьютерах и в почте вредоносных программ по-прежнему лидируют опасные сценарии, написанные на языке JavaScript. Значительная их часть предназначена для загрузки на инфицированное устройство другого вредоносного ПО и добычи криптовалют с использованием аппаратных ресурсов зараженного компьютера. Как и в ноябре, на жестких дисках часто обнаруживается Trojan.SpyBot.699 — многокомпонентный банковский троянец. С его помощью киберпреступники могут удаленно выполнять на компьютере различные команды и запускать другие вредоносные приложения.

Главные тенденции декабря

- Распространение вредоносных сценариев
- Появление новых троянцев для мобильной платформы Android

Обзор вирусной активности в декабре 2018 года

По данным серверов статистики «Доктор Веб»



JS.DownLoader

Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.

Trojan.SpyBot.699

Многомодульный банковский троянец. Он позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и выполнять поступающие от них команды. Троянец предназначен для хищения средств с банковских счетов.

JS.Miner

Семейство сценариев на языке JavaScript, предназначенных для скрытой добычи (майнинга) криптовалют.

VBS.DownLoader

Семейство вредоносных сценариев, написанных на языке VBS. Загружают и устанавливают на компьютер другие вредоносные программы.

Статистика вредоносных программ в почтовом трафике

JS.DownLoader

Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.

Trojan.SpyBot.699

Многомодульный банковский троянец. Он позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и выполнять поступающие от них команды. Троянец предназначен для хищения средств с банковских счетов.

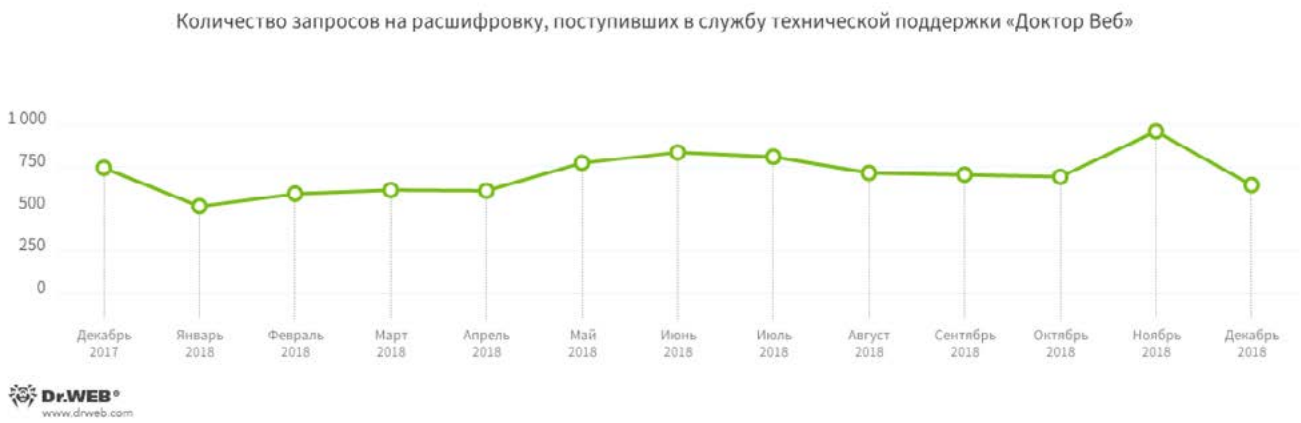
W97M.DownLoader

Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

JS.Miner

Семейство сценариев на языке JavaScript, предназначенных для скрытой добычи (майнинга) криптовалют.

Статистика вредоносных программ в почтовом трафике



В декабре в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих модификаций троянцев-шифровальщиков:

- Trojan.Encoder.858 — 22.34% обращений;
- Trojan.Encoder.11464 — 11.71% обращений;
- Trojan.Encoder.11539 — 10.17% обращений;
- **Trojan.Encoder.25574** — 5.08% обращений;
- Trojan.Encoder.567 — 4.93% обращений;
- Trojan.Encoder.5342 — 1.54% обращений.

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 декабря 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 257 197 интернет-адресов.

В течение октября 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 156 188 интернет-адресов.

Ноябрь 2018	Декабрь 2018	Динамика
+ 231 074	+ 257 197	+11.3%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В декабре специалисты «Доктор Веб» обнаружили в каталоге Google Play вредоносное приложение Android.BankBot.495.origin, предназначенное для бразильских пользователей. Оно похищало конфиденциальную банковскую информацию и могло самостоятельно управлять другими программами благодаря специальным возможностям (Accessibility Service) ОС Android. Помимо этого, в Google Play были выявлены рекламные троянцы семейств Adware.HiddenAds и **Adware.Patacore** и другие вредоносные и нежелательные приложения. Также вирусные аналитики обнаружили новую версию коммерческой шпионской программы **Program.Spyzie.1.origin**, которая позволяла злоумышленникам следить за владельцами мобильных устройств.

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

- распространение банковского троянца, атаковавшего пользователей Бразилии;
- обнаружение новой версии опасной программы, предназначенной для кибершпионажа;
- выявление в Google Play множества вредоносных и нежелательных программ.

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

Обзор вирусной активности в декабре 2018 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