Dr.WEB®
с 1992 года

Обзор вирусной активности в декабре 2017 года

Обзор вирусной активности в декабре 2017 года

29 декабря 2017 года

Последний месяц уходящего года запомнится специалистам по информационной безопасности появлением нового бэкдора для компьютеров и устройств, работающих под управлением Microsoft Windows. Также в декабре вирусные аналитики «Доктор Веб» установили, что злоумышленники стали взламывать веб-сайты с использованием Linux-троянца Linux.ProxyM. Кроме того, в течение месяца вирусные базы Dr.Web пополнились записями для новых вредоносных программ, ориентированных на мобильную платформу Android.

Главные тенденции декабря

- Появление нового бэкдора для Linux
- Взломы сайтов с использованием Linux-троянца
- Распространение вредоносных программ для Android

Обзор вирусной активности в декабре 2017 года

Угроза месяца

В декабре вирусные аналитики исследовали очередного представителя семейства троянцев Anunak, способных выполнять на зараженном компьютере команды злоумышленников. Новый бэкдор рассчитан на работу в 64-разрядных версиях Windows и получил наименование BackDoor.Anunak.142. Троянец может выполнять на зараженном компьютере следующие действия:

- скачивание файлов с заданного удаленного сервера;
- загрузка файлов на удаленный сервер;
- запуск файла на инфицированном устройстве;
- выполнение команд в консоли cmd.exe;
- перенаправление трафика между портами;
- загрузка и установка собственных модулей.

Подробнее об этой вредоносной программе рассказано в новостном материале, опубликованном на нашем сайте.

По данным статистики Антивируса Dr.Web

Наиболее распространенные вредоносные программы согласно статистике Антивируса Dr.Web

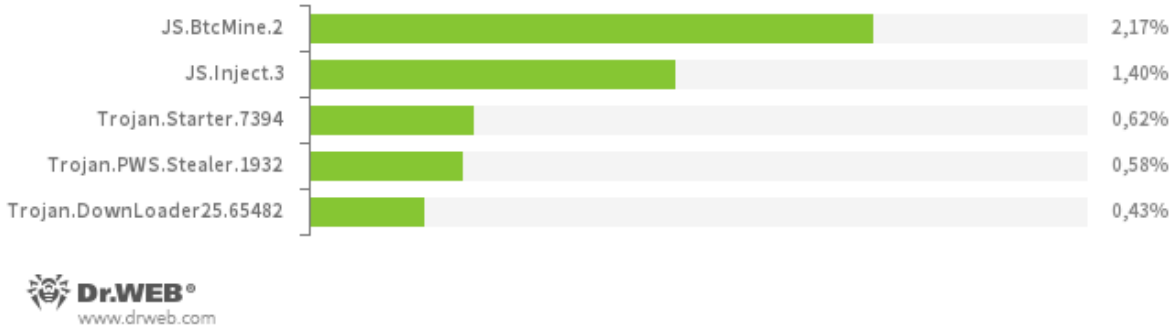
- **Trojan.Starter.7394**
  Представитель семейства троянцев, основное назначение которых — запуск в инфицированной системе исполняемого файла с определенным набором вредоносных функций.
- **Trojan.Encoder.11432**
  Червь-шифровальщик, также известный под именем WannaCry.

Обзор вирусной активности в декабре 2017 года

- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.
- **JS.BtcMine.2**
  Сценарий на языке JavaScript, предназначенный для скрытой добычи (майнинга) криптовалют.
- **Trojan.BPlug**
  Это надстройки (плагины) для популярных браузеров, демонстрирующие назойливую рекламу при просмотре веб-страниц.

По данным серверов статистики «Доктор Веб»

Наиболее распространенные вредоносные программы в декабре 2017 года согласно данным серверов статистики Dr.Web



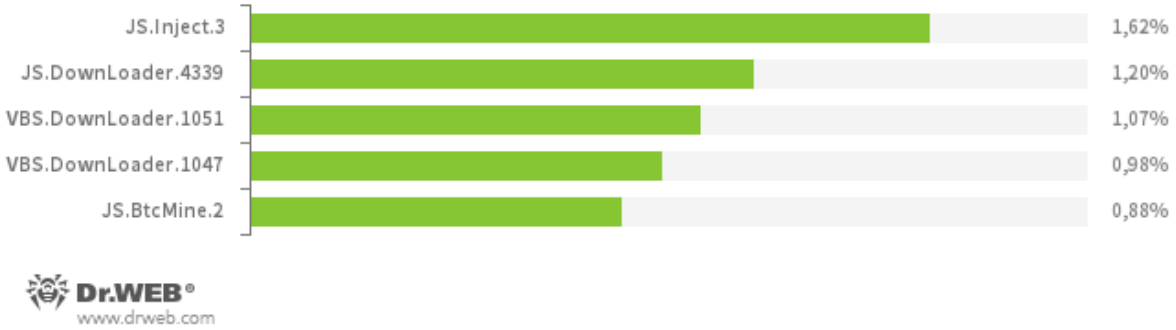
- **JS.BtcMine.2**
  Сценарий на языке JavaScript, предназначенный для скрытой добычи (майнинга) криптовалют.
- **JS.Inject**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **Trojan.Inject**
  Семейство вредоносных программ, встраивающих вредоносный код в процессы других программ.
- **Trojan.Starter.7394**
  Представитель семейства троянцев, основное назначение которых — запуск в инфицированной системе исполняемого файла с определенным набором вредоносных функций.

Обзор вирусной активности в декабре 2017 года

- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.

Статистика вредоносных программ в почтовом трафике

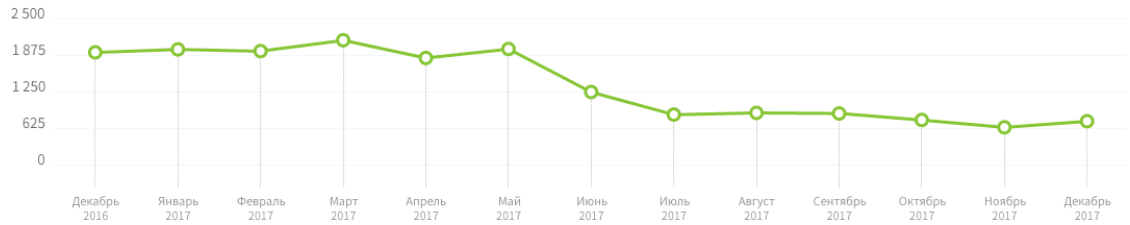
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в декабре 2017 года



- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **JS.Inject**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **VBS.DownLoader**
  Семейство вредоносных файлов, написанных на языке сценариев VBScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **JS.BtcMine.2**
  Сценарий на языке JavaScript, предназначенный для скрытой добычи (майнинга) криптовалют.

Шифровальщики

Количество запросов на расшифровку, поступивших
в службу технической поддержки «Доктор Веб»



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

- **Trojan.Encoder.3953** — 17,88% обращений;
- **Trojan.Encoder.858** — 27,29% обращений;
- **Trojan.Encoder.11539** — 12,55% обращений;
- **Trojan.Encoder.3953** — 4,09% обращений;
- **Trojan.Encoder.11464** — 3,41% обращений;
- **Trojan.Encoder.2667** — 2,59% обращений;
- **Trojan.Encoder.567** — 2,05% обращений.

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

Этого функционала нет в лицензии Антивирус Dr.Web для Windows
Настрой-ка Dr.Web от шифровальщиков
Обучающий курс
О бесплатном восстановлении

Dr.Web Rescue Pack

Обзор вирусной активности в декабре 2017 года

Опасные сайты

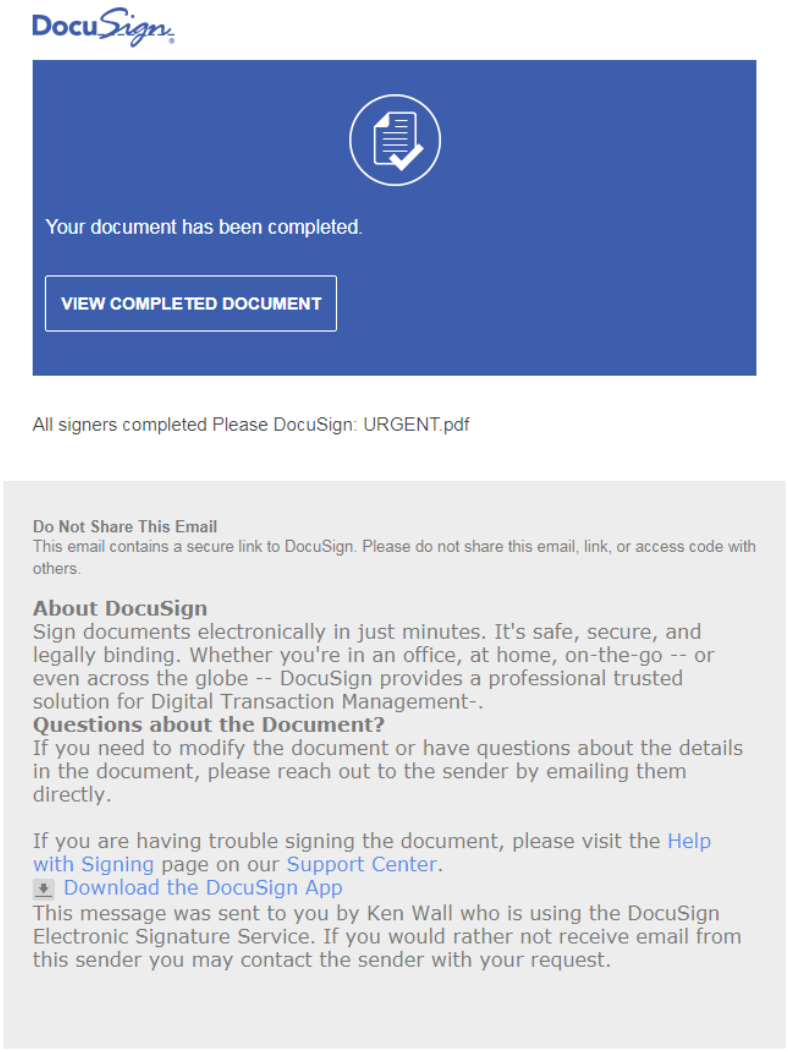
В течение декабря 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 241 274 интернет-адреса

ноябрь 2017	декабрь 2017	Динамика
+331 895	+241 274	-27,3%

Нерекомендуемые сайты

Вредоносные программы для ОС Linux

Троянец Linux.ProxyM известен вирусным аналитикам еще с мая 2017 года. Это довольно-таки простая вредоносная программа, запускающая на инфицированном устройстве SOCKS-прокси-сервер. С ее помощью злоумышленники рассылали до 400 спам-сообщений с каждого зараженного узла, а вскоре стали распространять фишинговые письма, в частности от имени сервиса DocuSign, позволяющего работать с электронными документами. Таким образом киберпреступники собирали учетные данные его пользователей.



В декабре, используя для анонимности реализованный в троянце прокси-сервер, злоумышленники стали предпринимать многочисленные попытки взлома веб-сайтов. Для этого использовались SQL-инъекции (внедрение в запрос к базе данных сайта вредоносного SQL-кода), XSS (Cross-Site Scripting) – метод атаки, заключающийся в добавлении в страницу вредоносного сценария, который выполняется на компьютере при открытии этой страницы, и Local File Inclusion (LFI) – метод атаки, позволяющий злоумышленникам удаленно читать файлы на атакуемом сервере с помощью специально сформированных команд. Подробности об этом инциденте рассказаны в опубликованном нами новостном материале.

Вредоносное и нежелательное ПО для мобильных устройств

В декабре в каталоге Google Play были выявлены банковские троянцы Android.BankBot.243.origin и Android.BankBot.255.origin, которые похищали логины и пароли для доступа к учетным записям клиентов кредитных организаций. Кроме того, похожий троянец распространялся и вне официального каталога ПО мобильной платформы Android. Он получил имя Android.Packed.15893. Также в декабре в вирусную базу Dr.Web был добавлена вредоносная программа Android.Spy.410.origin, которая шпионила за итальянскими пользователями.

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

- распространение новых банковских троянцев;
- обнаружение вредоносной программы-шпиона, кравшей конфиденциальную информацию.

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

Обзор вирусной активности в декабре 2017 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 | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах