Dr.WEB®
с 1992 года

Обзор вирусной активности в марте 2017 года

Обзор вирусной активности в марте 2017 года

3 апреля 2017 года

С наступлением весны активизировались киберпреступники, промышляющие интернет-мошенничеством и распространением вредоносного ПО. Кроме того, в марте был обнаружен новый Linux-троянец, предназначенный для организации DDoS-атак. В каталоге мобильных приложений Google Play вирусные аналитики компании «Доктор Веб» выявили программу со встроенным модулем, показывавшим на экране Android-устройств назойливую рекламу, — в общей сложности это приложение скачали более 50 000 000 человек. Также в течение первого весеннего месяца базы нерекомендуемых сайтов пополнились множеством адресов потенциально опасных интернет-ресурсов.

Главные тенденции марта

- Появление нового троянца для Linux
- Обнаружение множества мошеннических веб-сайтов
- Распространение агрессивных рекламных модулей и троянцев для ОС Android

Обзор вирусной активности в марте 2017 года

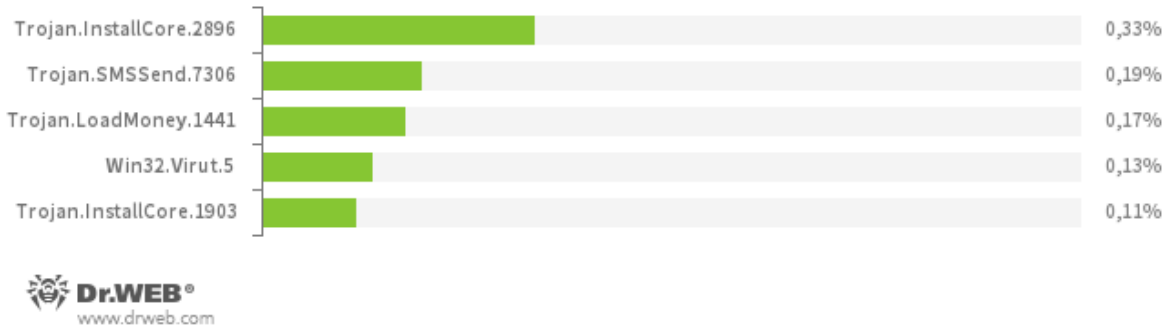
Угроза месяца

Вредоносные программы для ОС Linux обычно загружают на скомпрометированное устройство других троянцев, организуют прокси-серверы или совершают DDoS-атаки. Именно последнюю задачу и выполняет обнаруженный в марте вирусными аналитиками «Доктор Веб» троянец, получивший название Linux.DDoS.117.

Эта вредоносная программа имеет версии для аппаратных архитектур Intel x86, M68K, MIPS, MIPSEL, SPARC, SH4, Power PC и ARM. После запуска Linux.DDoS.117 ожидает соединения с Интернетом и при его появлении отсылает злоумышленникам сведения об инфицированном устройстве. Троянец может принимать поступающие команды и выполнять их с использованием командного интерпретатора sh. С помощью отдельной директивы киберпреступники передают троянцу имя атакуемого узла и данные о продолжительности DDoS-атаки. Более подробная информация о Linux.DDoS.117 содержится в техническом описании этой вредоносной программы.

По данным статистики Антивируса Dr.Web

Наиболее распространенные вредоносные программы согласно статистике Антивируса Dr.Web



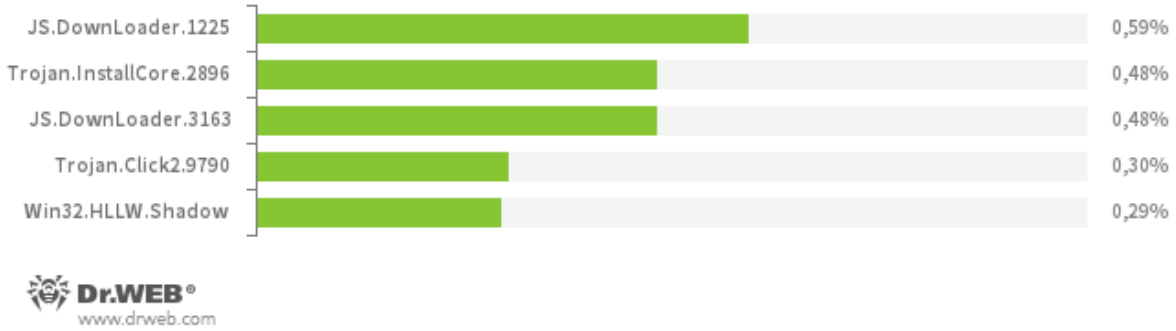
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.SMSSend.7306**
  Представитель семейства вредоносных программ, обычно реализованных в виде архива со встроенным инсталлятором. Он предлагает либо отправить платное СМС-сообщение на короткий сервисный номер для продолжения установки и, соответственно, получения доступа к содержимому архива, либо указать номер телефона и ввести полученный в ответном сообщении код, согласившись с условиями платной подписки. Основная «специализация» Trojan.SMSSend – вымогательство.

Обзор вирусной активности в марте 2017 года

- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Win32.Virut.5**
  Сложный полиморфный вирус, заражающий исполняемые файлы и содержащий функции удаленного управления инфицированным компьютером.

По данным серверов статистики «Доктор Веб»

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

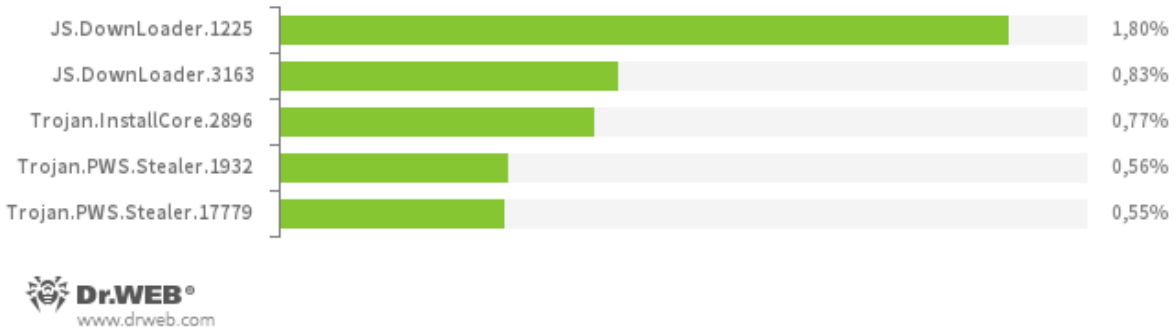


- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.Click2.9790**
  Представитель семейства вредоносных программ, предназначенных для накрутки посещаемости различных интернет-ресурсов. Такие троянцы перенаправляют запросы жертвы на определенные сайты с помощью управления поведением браузера.
- **Win32.HLLW.Shadow**
  Червь, использующий для своего распространения съемные носители и сетевые диски. Кроме того, может распространяться по сети с использованием стандартного протокола SMB. Способен загружать с управляющего сервера исполняемые файлы и запускать их.

Обзор вирусной активности в марте 2017 года

Статистика вредоносных программ в почтовом трафике

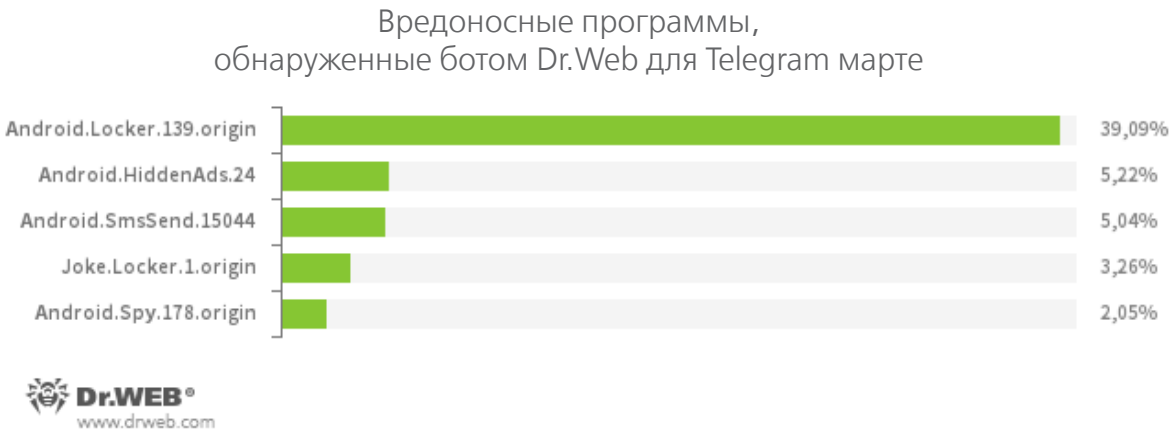
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в марте 2017 года



- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.

Обзор вирусной активности в марте 2017 года

По данным бота Dr.Web для Telegram



- **Android.Locker.139.origin**
  Представитель семейства Android-троянцев, предназначенных для вымогательства. Он показывает навязчивое сообщение якобы о нарушении закона и о последовавшей в связи с этим блокировке мобильного устройства, для снятия которой пользователю предлагается заплатить определенную сумму.
- **Android.HiddenAds.24**
  Троянец, предназначенный для показа навязчивой рекламы.
- **Android.SmsSend.15044**
  Представитель семейства вредоносных программ, предназначенных для отправки СМС-сообщений с повышенной тарификацией и подписки пользователей на различные платные контент-услуги и сервисы.
- **Joke.Locker.1.origin**
  Программа-шутка для ОС Android, блокирующая экран мобильного устройства и выводящая на него изображение «синего экрана смерти» ОС Windows (BSOD, Blue Screen of Death).
- **Android.Spy.178.origin**
  Представитель семейства троянцев для ОС Windows, способных похищать конфиденциальную информацию, в том числе пользовательские пароли.

Троянцы-шифровальщики

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

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

- **Trojan.Encoder.858** — 26.71% обращений;
- **Trojan.Encoder.3953** — 5.89% обращений;
- **Trojan.Encoder.10144** — 2.83% обращений;
- **Trojan.Encoder.761** — 2.60% обращений;
- **Trojan.Encoder.567** — 2.09% обращений.

В начале марта один из пользователей форума bleepingcomputer.com опубликовал ссылку на список приватных ключей, используемых троянцем-шифровальщиком Dharma. Согласно номенклатуре «Доктор Веб», он имеет обозначение Trojan.Encoder.3953. Это уже второй случай утечки приватных ключей для данного энкодера. Зашифрованные этим троянцем файлы получают суффикс с контактным адресом электронной почты злоумышленников и расширением .xtbl, .CrySiS, .crypted, .crypt или .lock. Благодаря утечке ключей специалисты «Доктор Веб» уже 2 марта разработали методику расшифровки файлов, поврежденных Trojan.Encoder.3953.

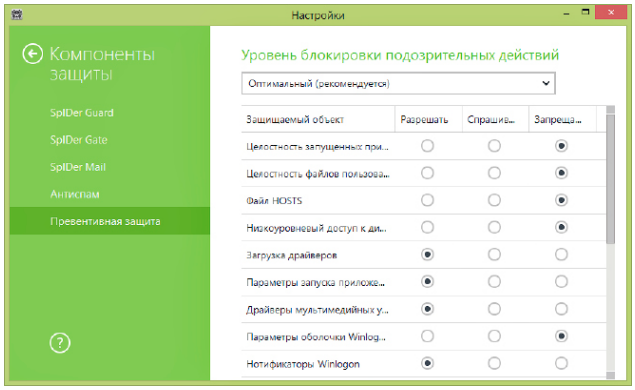
Кроме того, в марте вирусные аналитики «Доктор Веб» создали алгоритм расшифровки данных, зашифрованных троянцем Trojan.Encoder.10465. Вредоносная программа написана на языке Delphi и присваивает зашифрованным файлам расширение .crptxxx. Подробная информация об этом шифровальщике, а также рекомендации для пострадавших от него изложены в опубликованной нами статье.

Обзор вирусной активности в марте 2017 года

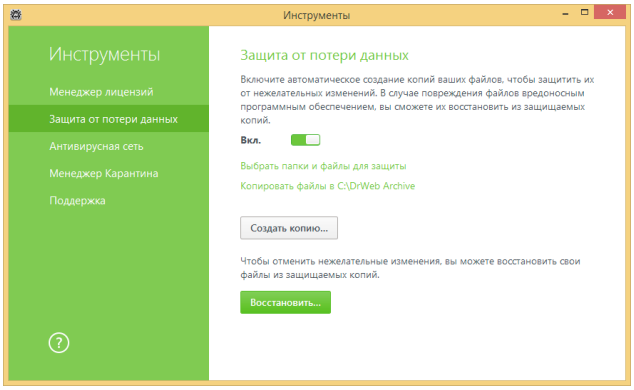
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



Подробней Смотрите видео о настройке

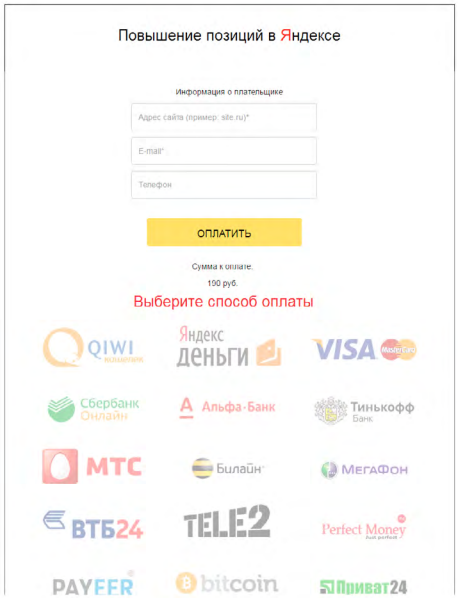
Опасные сайты

В течение марта 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 223 173 интернет-адреса.

Февраль 2017	Март 2017	Динамика
+ 134 063	+ 223 173	+ 66,46%

В марте специалисты «Доктор Веб» выявили более 500 мошеннических веб-страниц, ориентированных на владельцев и администраторов интернет-сайтов. Многие из них получили электронное письмо якобы от компании «Яндекс» с предложением улучшить позиции принадлежащего им сайта в результатах поиска. Оно содержало ссылку на страничку с формой для оплаты предложенной услуги.

Обзор вирусной активности в марте 2017 года



Это предложение оказалось обычным мошенничеством: после внесения платежа жертва не получала обещанного. Киберпреступники создали более 500 таких страничек, разместив их на нескольких арендованных площадках в Интернете. Подробности этого инцидента изложены в новостной статье, опубликованной на сайте компании «Доктор Веб».

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В марте вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play новый рекламный модуль, получивший имя Adware.Cootek.1.origin. Он был встроен в программу TouchPal, представляющую собой экранную клавиатуру. После установки этого приложения Adware.Cootek.1.origin показывал навязчивую рекламу нескольких типов: например, создавал неудаляемые виджеты и встраивал баннеры в экран блокировки. Кроме того, он демонстрировал рекламу после разблокирования мобильного устройства.

Наиболее заметное событие, связанное с «мобильной» безопасностью в марте:

- обнаружение в каталоге Google Play приложения со встроенным в него программным модулем, который показывал агрессивную рекламу.

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

Обзор вирусной активности в марте 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
125124, 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