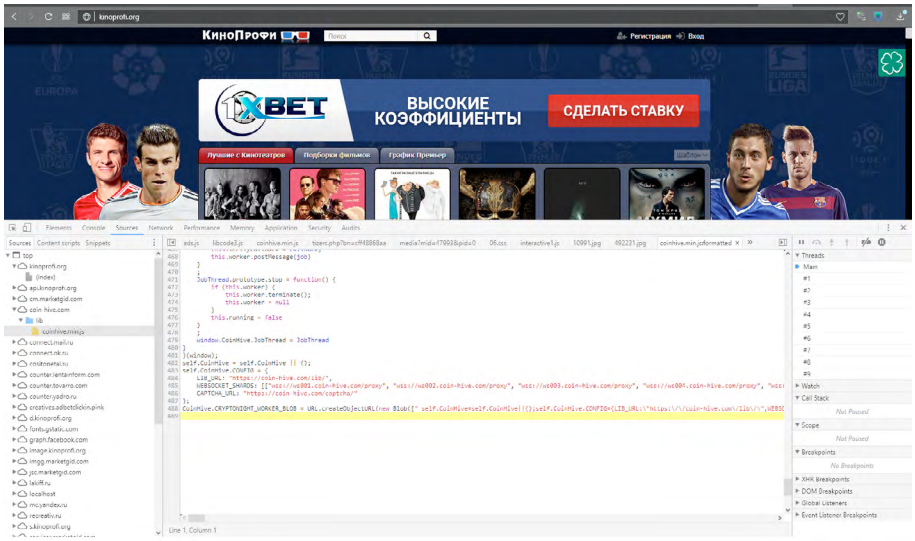
Dr.WEB®
с 1992 года

Обзор вирусной активности в сентябре 2017 года

29 сентября 2017 года

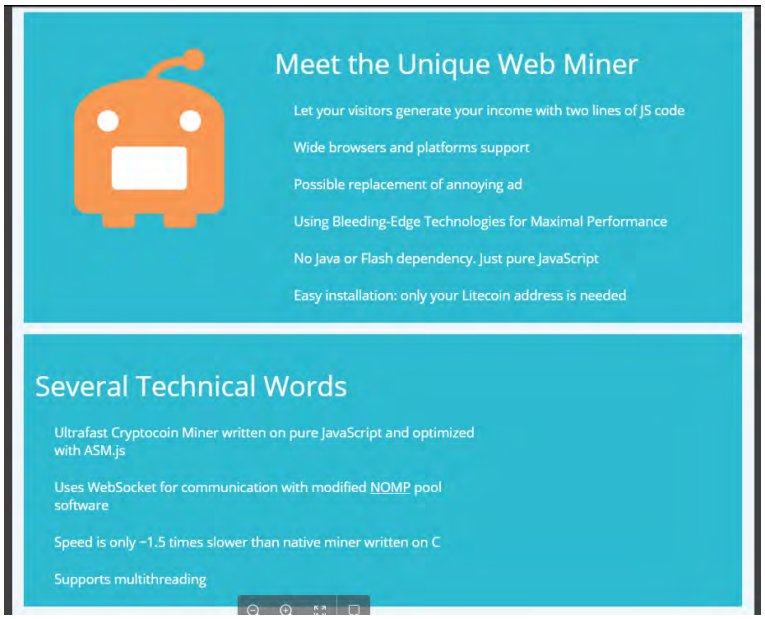
В сентябре несколько средств массовой информации сообщили о том, что киберпреступники стали активно использовать браузеры пользователей для несанкционированного майнинга (добычи) криптовалют. Наибольшей популярностью у злоумышленников пользуется криптовалюта Monero (XMR).

Майнер, добавленный в сентябре в вирусные базы Dr.Web под именем Tool.BtcMine.1046, был написан на языке JavaScript. При заходе на некоторые сайты внедренный в код разметки веб-страниц сценарий JavaScript начинал майнить криптовалюту. По сообщениям пользователей, в этот момент нагрузка на процессор компьютера достигала 100%, и возвращалась к нормальным значениям только после закрытия окна браузера. Трудно сказать, является ли этот инцидент следствием взлома сайтов или добровольного внедрения майнера в код их владельцами. В настоящий момент при попытке перехода на веб-страницы, содержащие подобный сценарий, Антивирус Dr.Web предупреждает пользователей об обнаружении потенциально опасного содержимого.



Вскоре в вирусные базы был добавлен еще один похожий инструмент, получивший наименование Tool.BtcMine.1048. Этот майнер также был написан на JavaScript. Возможно, он был задуман как

альтернатива заработку за счет размещения рекламы, однако использовался без явного согласия посетителей сайтов. Иными словами, указанная технология может применяться как легально, так и в целях криминального заработка. Подобные сценарии могут встраиваться в код сайта не только его владельцами, но и внедряться туда с помощью недобросовестных рекламодателей или в результате взлома. Кроме того, функция добычи криптовалюты может быть реализована и в плагинах, которые пользователи самостоятельно устанавливают в своих браузерах.



Также в сентябре специалисты по информационной безопасности обнаружили уязвимости в стеке протоколов Bluetooth, а аналитики «Доктор Веб» выяснили, что киберпреступники используют «Интернет вещей» для массовой рассылки спама.

Главные тенденции сентября

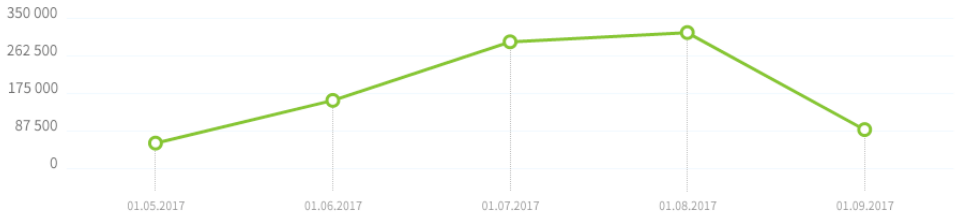
- Появление программ-майнеров, написанных на языке JavaScript
- Использование злоумышленниками «Интернета вещей» для рассылки спама
- Обнаружение опасных уязвимостей в протоколе Bluetooth

Обзор вирусной активности в сентябре 2017 года

Угроза месяца

Компания «Доктор Веб» уже рассказывала о вредоносной программе Linux.ProxyM, которая запускает на инфицированном Linux-устройстве SOCKS-прокси-сервер. Существуют сборки этого троянца для устройств с архитектурой x86, MIPS, MIPSEL, PowerPC, ARM, Superh, Motorola 68000 и SPARC, то есть он может работать на многих «умных» устройствах, таких как роутеры, телевизионные приставки и т. д. Вирусные аналитики установили, что киберпреступники рассылают с помощью зараженных этим троянцем устройств спам, рекламирующий ресурсы для взрослых. Ежесуточно каждое зараженное Linux.ProxyM устройство рассылает порядка 400 писем. Активность этого ботнета показана на следующем графике:

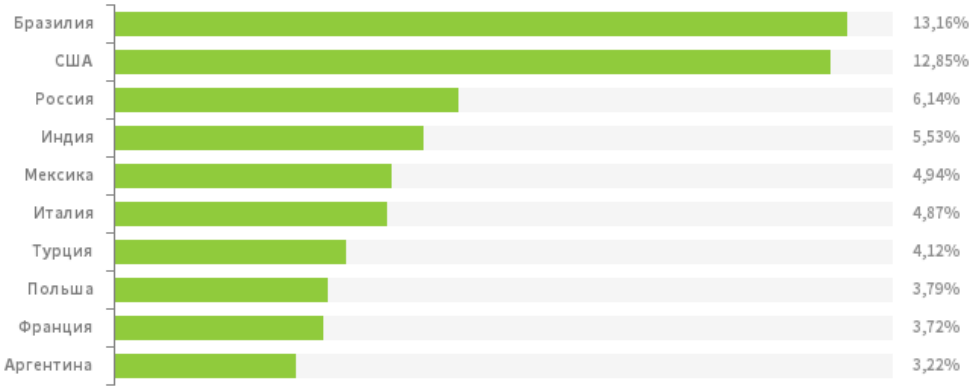
Количество атак с использованием Linux.ProxyM



Dr.WEB®
www.drweb.com

Больше всего зараженных так устройств, с которых выполняются атаки, расположено в Бразилии. На втором месте по этому показателю – США, на третьем – Россия.

Распределение источников атак
Linux.ProxyM по странам

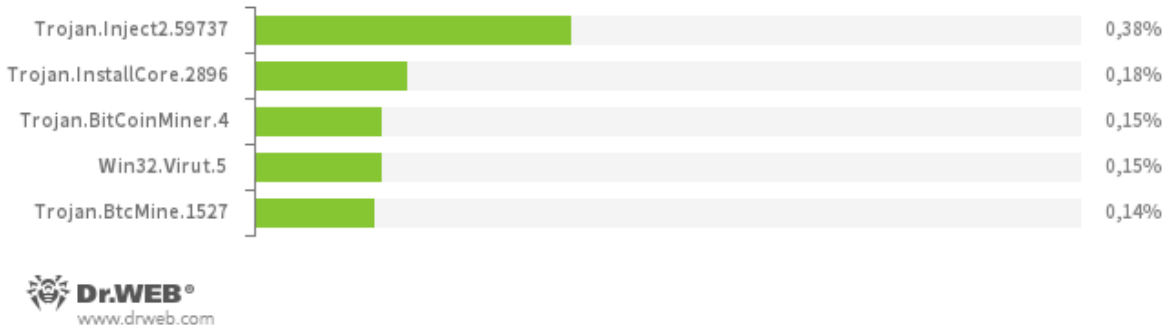


Dr.WEB®
www.drweb.com

Обзор вирусной активности в сентябре 2017 года

По данным статистики Антивируса Dr.Web

Наиболее распространенные вредоносные программы согласно статистике Антивируса Dr.Web

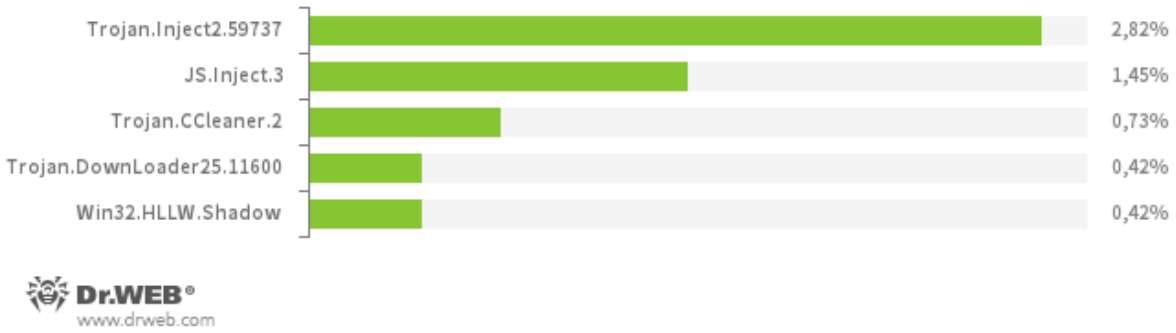


- **Trojan.Inject**
  Семейство вредоносных программ, встраивающих вредоносный код в процессы других программ.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.BitCoinMiner.4**
  Представитель семейства вредоносных программ, предназначенных для скрытой добычи (майнинга) криптовалюты BitCoin.
- **Win32.Virut.5**
  Полиморфный вирус, заражающий исполняемые файлы. Содержит функции управления инфицированными компьютерами с использованием IRC-канала.
- **Trojan.BtcMine**
  Семейство вредоносных программ, которые втайне от пользователя применяют вычислительные ресурсы зараженного компьютера для добычи (майнинга) различных криптовалют – например, Bitcoin.

Обзор вирусной активности в сентябре 2017 года

По данным серверов статистики «Доктор Веб»

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

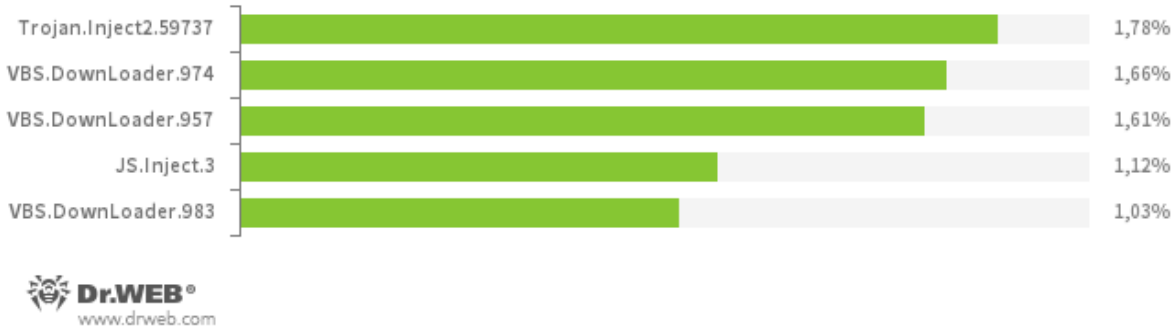


- **Trojan.Inject**
  Семейство вредоносных программ, встраивающих вредоносный код в процессы других приложений.
- **JS.Inject.3**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **Trojan.CCleaner.2**
  Вредоносная программа, обнаруженная в приложении CCleaner для оптимизации операционных систем Microsoft Windows.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **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 сентябре 2017 года

Статистика вредоносных программ в почтовом трафике

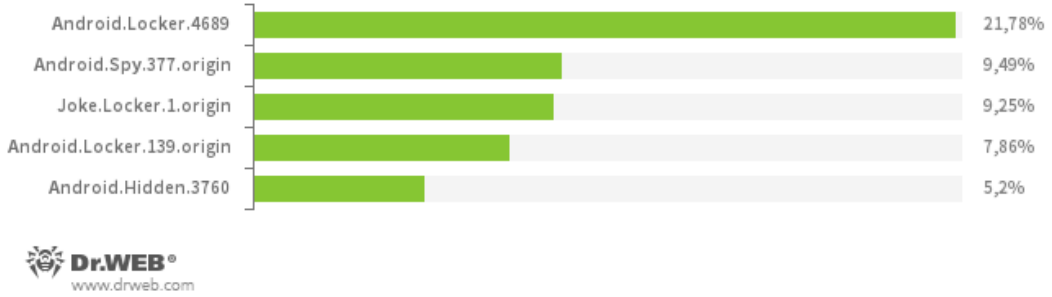
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в сентябре 2017 года



- **Trojan.Inject**
  Семейство троянцев, встраивающих вредоносный код в процессы других программ.
- **VBS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке VBScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **JS.Inject.3**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.

По данным бота Dr.Web для Telegram

Наиболее распространенные вредоносные программы, обнаруженные ботом Dr.Web для Telegram



Обзор вирусной активности в сентябре 2017 года

- **Android.Locker**
  Семейство Android-троянцев, предназначенных для вымогательства. Они показывают 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.Spy.337.origin**
  Представитель семейства троянцев для ОС Android, способных похищать конфиденциальную информацию, в том числе пользовательские пароли.
- **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.Hidden**
  Семейство Android-троянцев, способных скрывать свой значок в списке приложений инфицированного устройства.

Шифровальщики

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

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

- **Trojan.Encoder.858** — 23,49% обращений;
- **Trojan.Encoder.13671** — 5,33% обращений;
- **Trojan.Encoder.11464** — 3,89% обращений;
- **Trojan.Encoder.761** — 2,74% обращений;
- **Trojan.Encoder.5342** — 2,02% обращений;
- **Trojan.Encoder.567** — 2,00% обращений.

Обзор вирусной активности в сентябре 2017 года

Dr.Web Security Space 11.0 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

Опасные сайты

В течение сентября 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 298 324 интернет-адреса.

Август 2017	Сентябрь 2017	Динамика
+ 275 399	+ 298 324	+8.32%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В сентябре появилась информация о выявленной группе опасных уязвимостей BlueBorne в реализации протокола Bluetooth. Им подвержены различные устройства, включая Android-смартфоны и планшеты. Эти уязвимости позволяют получить полный контроль над атакуемыми устройствами, выполнять на них произвольный код и похищать конфиденциальную информацию. Помимо этого в прошедшем месяце в каталоге Google Play был обнаружен троянец Android.BankBot.234.origin, предназначенный для кражи сведений о банковских картах.

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

- появление подробностей об обнаруженных ранее уязвимостях в стеке протокола Bluetooth;
- выявление в каталоге Google Play банковского троянца.

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

Обзор вирусной активности в сентябре 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