Dr.WEB®
с 1992 года

Обзор вирусной активности за 2016 год

Обзор вирусной активности за 2016 год

29 декабря 2016 года

Уходящий 2016 год оказался богатым на интересные события в сфере информационной безопасности. Прежде всего этот год запомнится значительным ростом количества обнаруженных троянцев для операционных систем семейства Linux. Объясняется это широким распространением различных бытовых устройств, работающих под управлением указанной платформы: роутеров, сетевых хранилищ, IP-камер с веб-интерфейсом и других «умных» девайсов. Пользователи зачастую подключают их к сети, не меняя заводские настройки, что и становится приманкой для злоумышленников — они взламывают такие устройства путем подбора пароля и устанавливают на них вредоносное ПО.

Весной 2016 года получил распространение первый в истории троянец-шифровальщик для компьютеров Apple, работающих под управлением операционной системы macOS (OS X). Специалисты компании «Доктор Веб» оперативно разработали методику расшифровки файлов, поврежденных этим энкодером.

Также минувший год был отмечен появлением нескольких вредоносных программ, ориентированных на популярную в России бухгалтерскую программу 1С. Среди них оказался первый в истории полноценный троянец, написанный фактически на русском языке, – вернее, на встроенном языке программирования 1С. Он запускал в инфицированной системе опасного шифровальщика. Другой нацеленный на бухгалтеров троянец был специально создан вирусописателями для похищения информации из популярных бухгалтерских приложений и почтовых клиентов. Помимо экзотического внутреннего языка 1С вирусописатели в минувшем году нередко использовали такие редкие языки программирования, как Rust и Go.

Среди угроз информационной безопасности, направленных на проведение узкоспециализированных атак, нельзя не отметить троянца, инфицировавшего компьютеры нескольких российских фирм, которые занимаются производством и продажей башенных и строительных кранов.

Обзор вирусной активности за 2016 год

В течение года было выявлено множество новых банковских троянцев, в том числе способных организовывать децентрализованные ботнеты и избирательно заражать компьютеры в различных регионах планеты.

Обнаруженные в 2016 году троянцы для мобильной платформы Google Android научились заражать системные библиотеки и запущенные на устройстве процессы. В течение прошедших 12 месяцев специалисты компании «Доктор Веб» неоднократно обнаруживали вредоносные программы в прошивках популярных мобильных телефонов и планшетов под управлением Android. Отыскивались опасные мобильные троянцы и в официальном каталоге приложений Google Play.

Главные тенденции года

- Рост количества вредоносных программ для Linux
- Появление первого шифровальщика для macOS (OS X)
- Распространение троянцев, написанных на малораспространенных языках программирования
- Появление Android-троянцев, способных заражать системные процессы и библиотеки

Наиболее интересные события 2016 года

Как и ранее, в 2016 году серьезную опасность для пользователей представляли банковские троянцы, способные похищать деньги непосредственно со счетов клиентов кредитных организаций. Среди подобных вредоносных программ встречаются как относительно простые – например, Trojan.Proxy2.102, – так и более изощренные с точки зрения архитектуры троянцы. В частности, Trojan.Gozi, способный работать на компьютерах под управлением 32- и 64-разрядных версий Windows, реализует чрезвычайно широкий набор функций. Он может фиксировать нажатия клавиш, похищать данные, которые пользователи вводят в различные экранные формы, встраивать в просматриваемые на зараженном компьютере веб-страницы постороннее содержимое (то есть выполнять веб-инжекты), предоставлять злоумышленникам удаленный доступ к рабочему столу инфицированной машины, запускать на ПК прокси-сервер SOCKS, загружать и устанавливать различные плагины, а также красть информацию, в том числе используемую для доступа к системам «банк-клиент».

37	45.173629	95.215.111.125	10.0.4.3	UDP	840 Source port: 9772 Destination port: 13888
38	45.174357	10.0.4.3	95.215.111.125	UDP	1340 Source port: 13888 Destination port: 9772
39	45.256337	95.215.111.125	10.0.4.3	UDP	860 Source port: 9772 Destination port: 13888
40	45.261248	173.177.120.102	10.0.4.3	UDP	755 Source port: 29785 Destination port: 13888
41	45.261924	10.0.4.3	173.177.120.102	UDP	315 Source port: 13888 Destination port: 29785
42	45.489461	173.177.120.102	10.0.4.3	UDP	111 Source port: 29785 Destination port: 13888
43	46.093329	10.0.4.3	142.217.75.225	UDP	881 Source port: 13888 Destination port: 31835
44	47.094204	10.0.4.3	109.90.217.159	UDP	767 Source port: 13888 Destination port: 33600
45	52.101663	10.0.4.3	198.53.206.26	UDP	641 Source port: 13888 Destination port: 63599
46	54.104842	10.0.4.3	173.177.120.102	UDP	659 Source port: 13888 Destination port: 29785
47	54.105466	10.0.4.3	173.177.120.102	UDP	831 Source port: 13888 Destination port: 29785
48	54.106034	10.0.4.3	173.177.120.102	UDP	1164 Source port: 13888 Destination port: 29785
49	54.106651	10.0.4.3	173.177.120.102	UDP	342 Source port: 13888 Destination port: 29785
50	54.107504	10.0.4.3	173.177.120.102	UDP	467 Source port: 13888 Destination port: 29785
51	54.248506	173.177.120.102	10.0.4.3	UDP	1003 Source port: 29785 Destination port: 13888
52	54.252619	173.177.120.102	10.0.4.3	UDP	933 Source port: 29785 Destination port: 13888
53	54.256380	173.177.120.102	10.0.4.3	UDP	713 Source port: 29785 Destination port: 13888
54	54.260468	173.177.120.102	10.0.4.3	UDP	953 Source port: 29785 Destination port: 13888
55	54.264843	173.177.120.102	10.0.4.3	UDP	1200 Source port: 29785 Destination port: 13888
56	55.106104	10.0.4.3	173.183.1.166	UDP	264 Source port: 13888 Destination port: 14397
57	55.106666	10.0.4.3	184.64.213.14	UDP	798 Source port: 13888 Destination port: 12294
58	55.286556	184.64.213.14	10.0.4.3	UDP	296 Source port: 12294 Destination port: 13888
59	55.287359	10.0.4.3	184.64.213.14	UDP	887 Source port: 13888 Destination port: 12294
60	55.350810	173.183.1.166	10.0.4.3	UDP	717 Source port: 14397 Destination port: 13888
61	55.351571	10.0.4.3	173.183.1.166	UDP	1123 Source port: 13888 Destination port: 14397
62	55.468797	184.64.213.14	10.0.4.3	UDP	212 Source port: 12294 Destination port: 13888
63	55.608156	173.183.1.166	10.0.4.3	UDP	1081 Source port: 14397 Destination port: 13888
64	56.107339	10.0.4.3	50.69.165.12	UDP	495 Source port: 13888 Destination port: 48090

Trojan.Gozi может объединять зараженные компьютеры в ботнеты. Для генерации имен управляющих серверов он скачивает с сервера HACA текстовый файл, содержимое которого использует в качестве словаря. Кроме того, эта вредоносная программа обладает возможностью создавать и одноранговые P2P бот-сети.

Однако к наиболее опасным банковским угрозам 2016 года следует отнести полиморфный банковский вирус Bolik – прямой наследник широко известных банкеров Zeus и Carberp, который, в отличие от них, умеет распространяться самостоятельно и заражать исполняемые файлы.

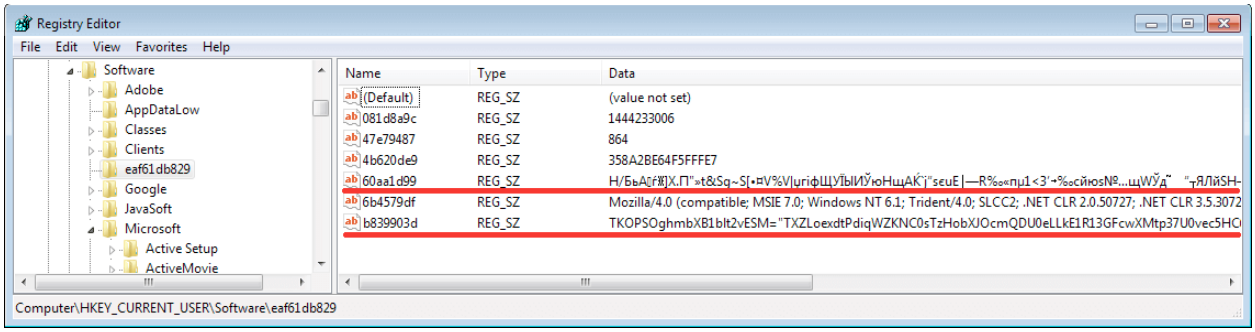
Экзотические и малораспространенные технологии для создания вредоносных программ киберпреступники используют нечасто. В качестве одного из исключений можно назвать троянца-дроппера 1C.Drop.1, написанного с использованием кириллицы на встроенном языке программирования для приложений 1С.

```
ИмяВременногоФайла = "D:\ОбновлениеБИКБанка.exe";
Попытка
    ДвоичныеДанные.Записать(ИмяВременногоФайла);
Исключение
    ИмяВременногоФайла = "C:\ОбновлениеБИКБанка.exe";
    Попытка
        ДвоичныеДанные.Записать(ИмяВременногоФайла);
    Исключение
        ИмяВременногоФайла = ПолучитьИмяВременногоФайла("exe");
        ДвоичныеДанные.Записать(ИмяВременногоФайла);
    КонецПопытки;
КонецПопытки;
ЗапуститьПриложение(ИмяВременногоФайла);
```

Этот троянец распространялся в виде вложения в почтовые сообщения, ориентированные на бухгалтеров: к письмам был прикреплен файл внешней обработки для программы «1С:Предприятие». При его открытии 1C.Drop.1 рассылал свою копию по всем обнаруженным в базе 1С электронным адресам контрагентов компании, а потом запускал на инфицированном ПК опасного троянца-шифровальщика.

Кроме того, в 2016 году вирусные аналитики «Доктор Веб» обнаружили и исследовали бэкдор Linux.BackDoor.Irc.16, написанный на языке Rust, первая стабильная версия которого появилась в 2015 году. А в октябре был выявлен энкодер Trojan.Encoder.6491, написанный на языке Go, — для него специалисты «Доктор Веб» оперативно разработали метод дешифровки. Этот язык программирования от компании Google приобретает все большую популярность в среде вирусописателей: вскоре был обнаружен еще один написанный на Go троянец — Linux.Lady.1, представляющий опасность для ОС семейства Linux. Эта вредоносная программа может атаковать другие компьютеры, а также скачивать и запускать на зараженной машине программу для добычи (майнинга) криптовалют.

К категории весьма опасных вредоносных программ можно отнести так называемых бестелесных троянцев: они не присутствуют на инфицированном компьютере в виде отдельного файла, а работают непосредственно в оперативной памяти, используя для своего хранения различные контейнеры, – например, системный реестр Windows. Одну из таких вредоносных программ аналитики «Доктор Веб» исследовали в июне 2016 года. Этот троянец, получивший название Trojan.Kovter.297, прячется в системном реестре Windows и предназначен для показа на зараженном компьютере несанкционированной рекламы.



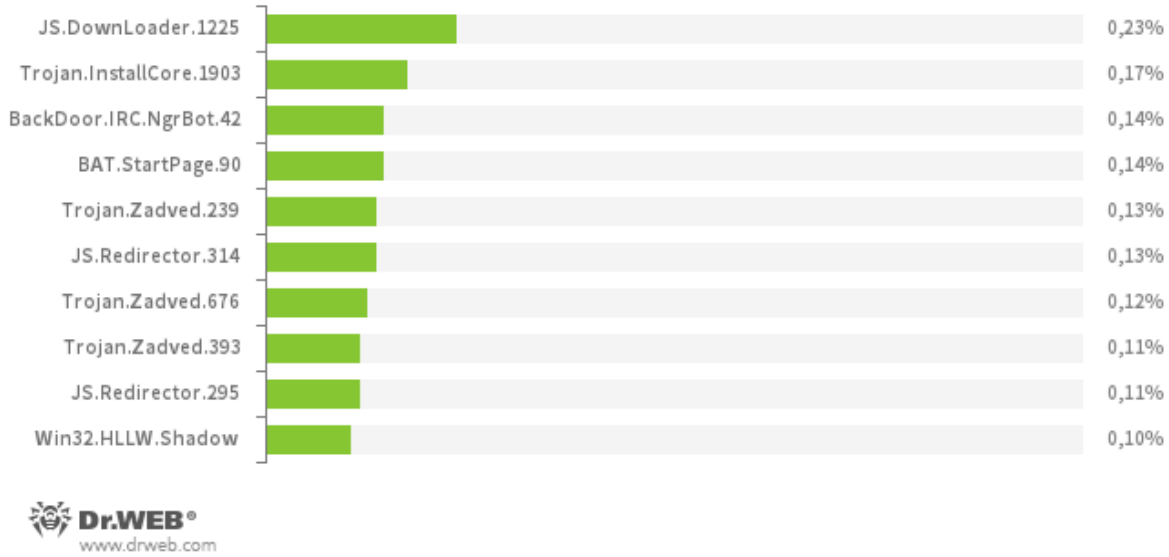
Обзор вирусной активности за 2016 год

Ну а наиболее интересной угрозой 2016 года можно назвать узкоспециализированного троянца BackDoor.Crane.1, призванного шпионить за фирмами – производителями строительных кранов. Этот бэкдор и две другие вредоносные программы, которые он загружал на зараженные машины, в течение некоторого времени похищали с инфицированных компьютеров конфиденциальную информацию. Основной целью злоумышленников были финансовые документы, договоры и деловая переписка сотрудников. Кроме того, троянцы с определенной периодичностью делали снимки экранов зараженных ПК и отправляли их на принадлежащий злоумышленникам управляющий сервер. Исследованию принципов работы этого троянца была посвящена опубликованная на сайте компании «Доктор Веб» обзорная статья.

Вирусная обстановка

Данные, собранные с использованием серверов статистики Dr.Web, показывают, что в 2016 году на компьютерах чаще всего обнаруживались скрипты и приложения, предназначенные для несанкционированной загрузки и установки вредоносных программ. Также заметную долю среди наиболее распространенных угроз составляют рекламные троянцы.

Наиболее распространенные вредоносные программы в 2016 году
согласно данным серверов статистики Dr.Web

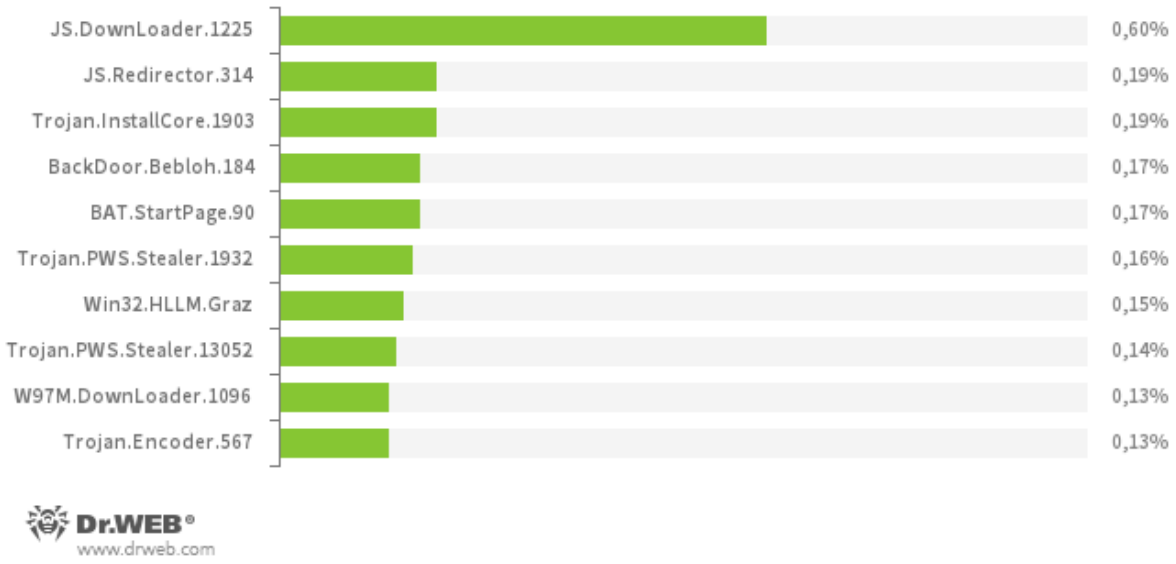


- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **BackDoor.IRC.NgrBot.42**
  Довольно распространенный троянец, известный специалистам по информационной безопасности еще с 2011 года. Вредоносные программы этого семейства способны выполнять на инфицированном компьютере поступающие от злоумышленников команды, а управление ими киберпреступники осуществляют с использованием протокола обмена текстовыми сообщениями IRC (Internet Relay Chat).
- **BAT.StartPage.90**
  Вредоносный сценарий, позволяющий подменять стартовую страницу в настройках браузера.
- **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.Redirector**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Автоматически перенаправляют пользователей браузеров на другие веб-страницы.
- **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 и запускать исполняемые файлы.

Статистика угроз, обнаруженных в 2016 году в почтовом трафике, демонстрирует схожую картину: чаще всего по каналам электронной почты злоумышленники рассылали вредоносные сценарии-загрузчики и рекламных троянцев. Среди опасных вложений в сообщения электронной почты также встречаются троянцы-шпионы, шифровальщики, бэкдоры, и программы для подмены стартовой страницы в браузерах. Десять наиболее распространенных вредоносных приложений согласно данным почтового Антивируса Dr.Web представлено на следующей гистограмме.

Обзор вирусной активности за 2016 год

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в 2016 году



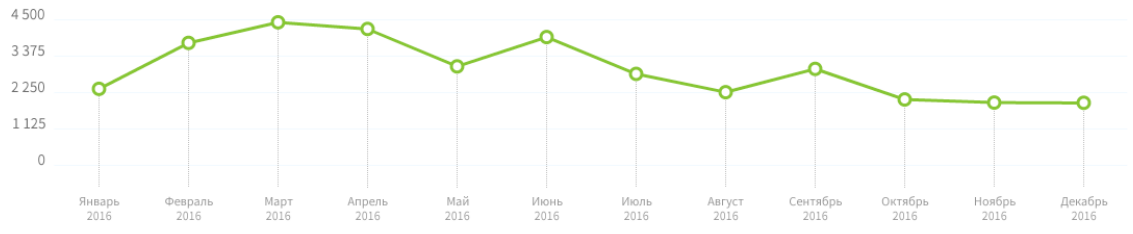
- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **JS.Redirector**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Автоматически перенаправляют пользователей браузеров на другие веб-страницы.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **BackDoor.Bebloh.184**
  Один из представителей троянцев-бэкдоров, способных встраиваться в процессы других приложений и выполнять поступающие от злоумышленников команды.
- **BAT.StartPage.90**
  Вредоносный сценарий, позволяющий подменять стартовую страницу в настройках браузера.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.
- **Win32.HLLM.Graz**
  Почтовый червь массовой рассылки. Отслеживает трафик на определенных портах и разбирает передаваемые данные в соответствии с протоколами для извлечения паролей. Эта информация используется для дальнейшего распространения червя.

- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.
- **Trojan.Encoder.567**
  Энкодер, шифрующий файлы на компьютере и требующий у жертвы выкуп за расшифровку. Может зашифровывать файлы следующих типов: .jpg, .jpeg, .doc, .docx, .xls, xlsx, .dbf, .1cd, .psd, .dwg, .xml, .zip, .rar, .db3, .pdf, .rtf, .7z, .kwm, .arj, .xlsm, .key, .cer, .accdb, .odt, .ppt, .mdb, .dt, .gsf, .ppsx, .pptx.

Троянцы-шифровальщики

В 2016 году, как и раньше, троянцы-шифровальщики представляли серьезную опасность для пользователей. За минувшие 12 месяцев в службу технической поддержки компании «Доктор Веб» обратилось в общей сложности более 34 000 жертв, пострадавших от действия энкодеров. Пик обращений пришелся на февраль и первые два весенних месяца, единичный всплеск отмечался в июле, а к концу года активность троянцев-шифровальщиков понемногу снижалась, о чем свидетельствует представленный ниже график.

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



По итогам года наиболее часто файлы пользователей шифровал троянец Trojan.Encoder.858, на втором месте по «популярности» — Trojan.Encoder.761, третье место со значительным отставанием занимает Trojan.Encoder.3953.

Наиболее распространенные шифровальщики в 2016 году:

- **Trojan.Encoder.858** — 23,00% обращений;
- **Trojan.Encoder.761** — 17,44% обращений;
- **Trojan.Encoder.3953** — 4,76% обращений;
- **Trojan.Encoder.567** — 4,58% обращений;
- **Trojan.Encoder.3976** — 4,26% обращений.

Обзор вирусной активности за 2016 год

В уходящем году шифровальщики угрожали не только пользователям Microsoft Windows: еще в январе был обнаружен новый энкодер для Linux, получивший наименование Linux.Encoder.3. Он присваивал зашифрованным файлам расширение .encrypted и был способен запоминать дату создания и изменения исходного файла, а затем подменять ее значениями, которые были установлены до шифрования.

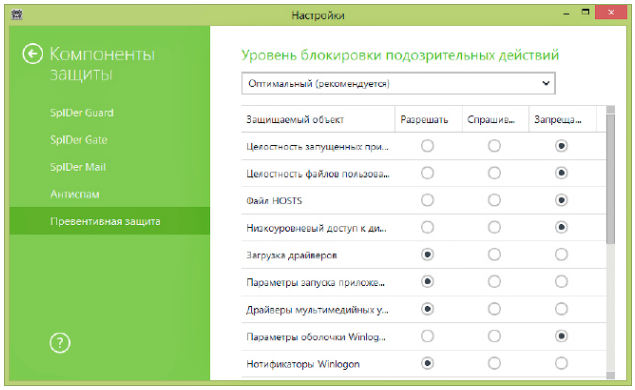
А уже в марте стало известно о распространении первого троянца-шифровальщика, ориентированного на компьютеры Apple, – Mac.Trojan.KeRanger.2. Впервые этот энкодер обнаружили в инфицированном обновлении популярного торрент-клиента для macOS (OS X), распространявшегося в виде дистрибутива в формате DMG. Программа была подписана действующим сертификатом разработчика приложений, благодаря чему могла обойти встроенную систему защиты ОС от Apple.

В обоих упомянутых случаях специалисты компании «Доктор Веб» оперативно разработали метод расшифровки файлов, поврежденных этими вредоносными программами.

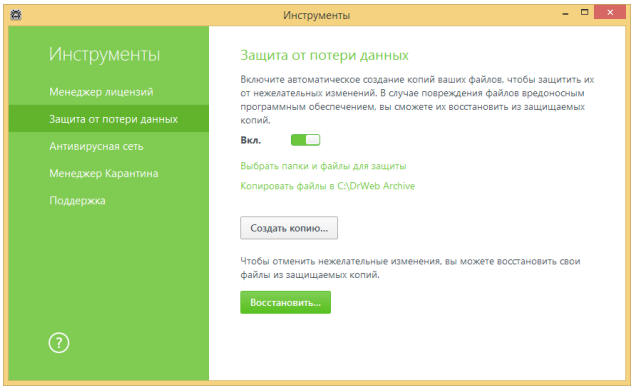
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



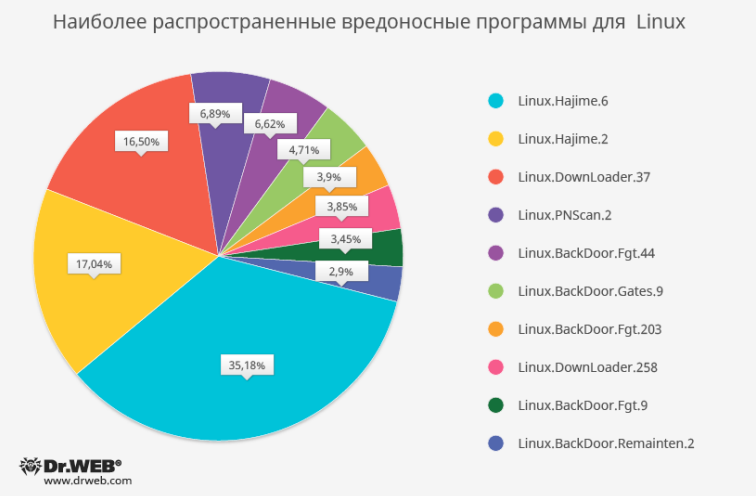
Подробней Смотрите видео о настройке

Вредоносные программы для Linux

Одной из наиболее ярких тенденций 2016 года можно назвать распространение большого количества вредоносных программ для Linux, нацеленных на так называемый «Интернет вещей», — различные управляемые устройства, подключенные к сети. Среди них — роутеры, сетевые хранилища, телевизионные приставки, IP-камеры и иные «умные» девайсы. Основной причиной, оправдывающей интерес злоумышленников к таким устройствам, является невнимательность самих пользователей, которые редко меняют установленные по умолчанию заводские настройки. В результате для киберпреступников не составляет труда получить несанкционированный доступ к ним с использованием стандартных логинов и паролей, а затем — загрузить вредоносное ПО.

Как правило, вирусописатели устанавливают на скомпрометированные Linux-устройства три типа вредоносных программ. Это троянцы для организации DDoS-атак, приложения, позволяющие запустить в системе прокси-сервер (он используется злоумышленниками для анонимности), а также троянцы и скрипты, предназначенные для загрузки на устройство других приложений. Для соединения с атакуемыми девайсами киберпреступники используют протоколы SSH и Telnet.

С начала осени 2016 года специалисты компании «Доктор Веб» начали отслеживать активность подобных Linux-угроз при помощи специально сконфигурированных сетевых узлов-ловушек, так называемых «ханипотов» (от англ. honeypot, «горшочек с медом»). Месяц от месяца количество совершаемых на такие узлы атак непрерывно росло: если в октябре было выявлено 40 756 подобных инцидентов, то в ноябре зафиксировано уже 389 285 атак. Изменилось и их соотношение: если в октябре 35 423 атаки осуществлялись по протоколу SSH и 5 333 — по протоколу Telnet, то в ноябре ситуация оказалось прямо противоположной: 79 447 раз злоумышленники получали несанкционированный доступ к устройствам по протоколу SSH, и 309 838 — посредством Telnet. Столь резкая смена приоритетов может объясняться ростом популярности троянца Linux.Mirai, исходные коды которого попали в свободный доступ. Эта вредоносная программа известна вирусным аналитикам еще с мая 2016 года. Она предназначена для организации DDoS-атак и способна работать на устройствах с архитектурой x86, ARM, MIPS, SPARC, SH-4 и M68K. Для атаки на уязвимые девайсы Linux.Mirai использует протокол Telnet. Пропорциональное соотношение вредоносных программ, которые киберпреступники загружали на атакованные устройства в течение трех осенних месяцев 2016 года, показано на следующей диаграмме:

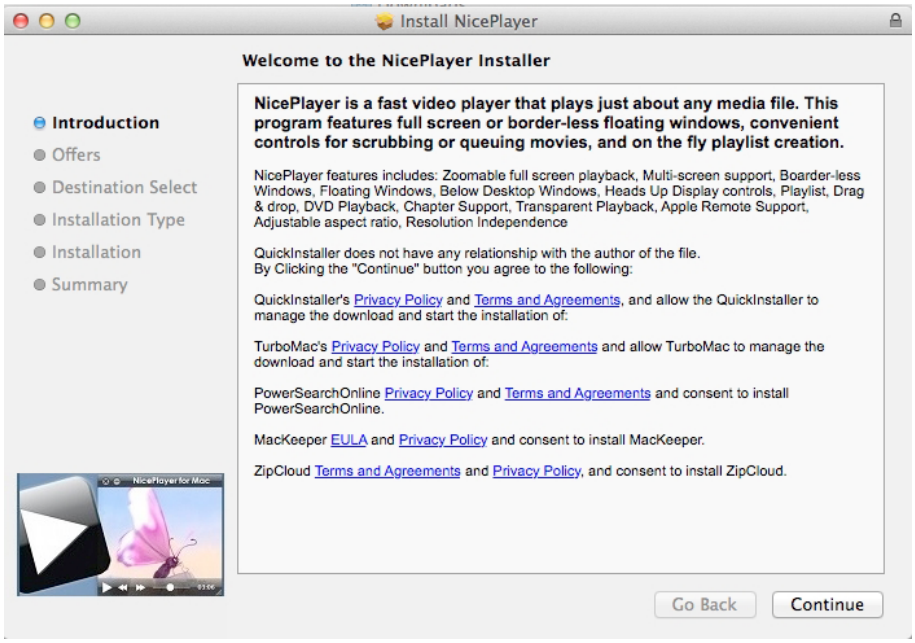


- **Linux.Hajime**
  Семейство сетевых червей для Linux, распространяются с использованием протокола Telnet. После успешной авторизации путем подбора пароля плагин-инфектор сохраняет на устройство хранящийся в нем загрузчик для архитектур MIPS/ARM, написанный на ассемблере. С компьютера, с которого осуществлялась атака, тот загружает основной модуль троянца, который включает устройство в децентрализованный P2P-ботнет.
- **Linux.DownLoader**
  Семейство вредоносных программ и сценариев (скриптов) для ОС Linux, предназначенных для загрузки и установки в скомпрометированной системе других вредоносных приложений.
- **Linux.PNScan.2**
  Сетевой червь, предназначенный для заражения роутеров, работающих под управлением ОС семейства Linux. Червь решает следующие задачи: самостоятельное инфицирование устройств, открытие портов 9000 и 1337, обслуживание запросов по этим портам и организация связи с управляющим сервером.
- **Linux.BackDoor.Fgt**
  Семейство вредоносных программ для ОС Linux, предназначенных для DDoS-атак. Существуют версии троянцев для различных дистрибутивов Linux, в том числе встраиваемых систем для архитектур MIPS и SPARC.
- **Linux.BackDoor.Gates**
  Семейство Linux-троянцев, которые сочетают функции бэкдора и DDoS-бота. Троянцы способны выполнять поступающие команды, а также осуществлять DDoS-атаки.
- **Linux.BackDoor.Remaiten**
  Семейство вредоносных программ для Linux, предназначенных для осуществления DDoS-атак. Троянец умеет взламывать устройства по протоколу Telnet методом перебора паролей, в случае успеха сохраняет на устройство загрузчик, написанный на языке Ассемблер. Этот загрузчик предназначен для скачивания и установки на атакуемое устройство других вредоносных приложений.

Помимо упомянутых выше вредоносных программ для «Интернета вещей» в 2016 году вирусные аналитики «Доктор Веб» исследовали и другие угрозы для Linux. Так, еще в январе специалисты обнаружили троянца Linux.Ekoms.1, способного делать снимки экрана на инфицированной машине, и многофункциональный бэкдор Linux.BackDoor.Xunpes.1. Вскоре было зафиксировано распространение хакерской утилиты, заражающей пользователей Linux опасным троянцем, затем — троянца Linux.Rex.1, способного объединять зараженные компьютеры в ботнеты, и бэкдора, получившего наименование Linux.BackDoor.FakeFile.1. Эта вредоносная программа может выполнять на зараженной Linux-машине поступающие от киберпреступников команды.

Вредоносные программы для macOS

Помимо уже упоминавшегося ранее троянца-энкодера для macOS, в 2016 году было выявлено не так много новых вредоносных программ для компьютеров Apple. Среди них — семейство троянцев Mac.Trojan.VSearch, предназначенных для показа на зараженном компьютере нежелательной рекламы.

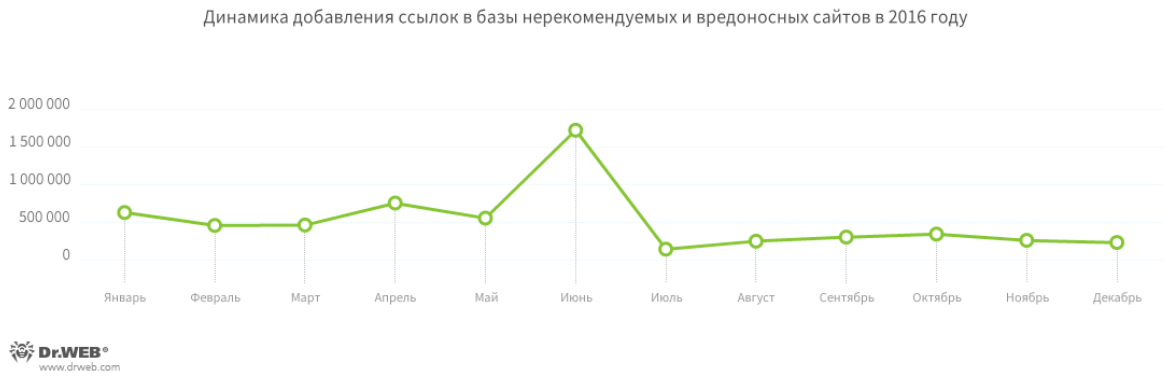


Эти троянцы распространяются под видом различных утилит – например, проигрывателя Nice Player, который пользователь может скачать с веб-сайтов, предлагающих бесплатное ПО. Один из представителей семейства, Mac.Trojan.VSearch.2, устанавливает на «маке» несколько нежелательных приложений, среди которых — троянец Mac.Trojan.VSearch.4. Он выкачивает с управляющего сервера специальный скрипт, подменяющий в настройках браузера поисковую систему по умолчанию. Затем вредоносный сценарий устанавливает поисковый плагин для браузеров Safari, Google Chrome и Mozilla Firefox и загружает троянца Mac.Trojan.VSearch.7. В свою очередь, Mac.Trojan.VSearch.7 создает в операционной системе нового «невидимого» пользователя и запускает специальный прокси-сервер, с помощью которого встраивает во все открываемые в окне браузера веб-страницы сценарий на языке JavaScript, показывающий рекламные баннеры. Помимо этого вредоносный скрипт собирает пользовательские запросы к нескольким популярным поисковым системам.

Специалистам компании «Доктор Веб» удалось установить, что в общей сложности на принадлежащие киберпреступникам серверы за время их существования поступило 1 735 730 запросов на загрузку вредоносных программ этого семейства. Кроме того, было зафиксировано 478 099 уникальных IP-адресов обращавшихся к этим серверам компьютеров.

Опасные и нерекомендуемые сайты

В Интернете действует множество опасных сайтов, посещение которых может нанести вред компьютеру или даже самому пользователю: среди них — фишинговые и мошеннические интернет-ресурсы, а также сайты, замеченные в распространении вредоносного ПО. Для защиты от подобных веб-страниц в составе Антивируса Dr.Web имеются модули SplDer Gate и Родительский контроль, в базы которых ежедневно добавляются новые ссылки на вредоносные и нерекомендуемые сайты. Динамика пополнения этих баз в 2016 году показана на следующей диаграмме.

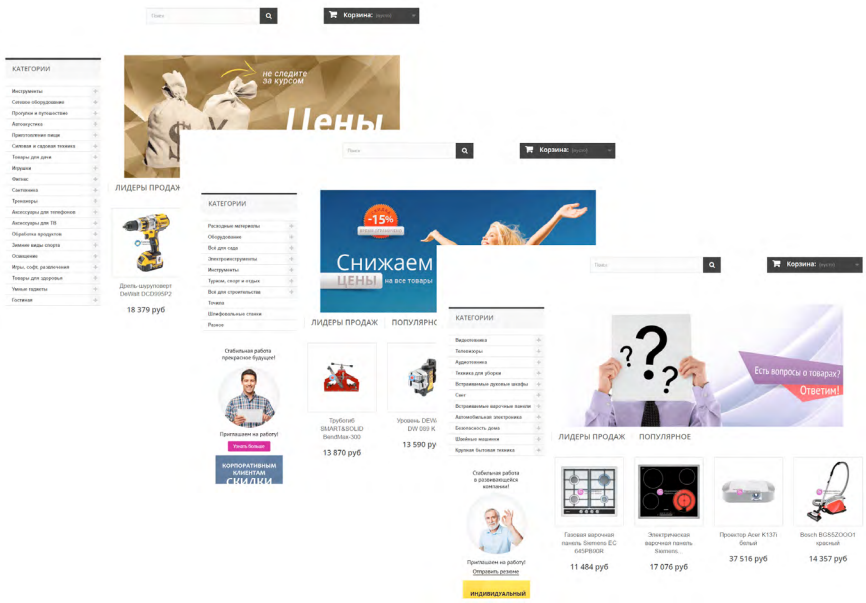


Нерекомендуемые сайты

Сетевое мошенничество

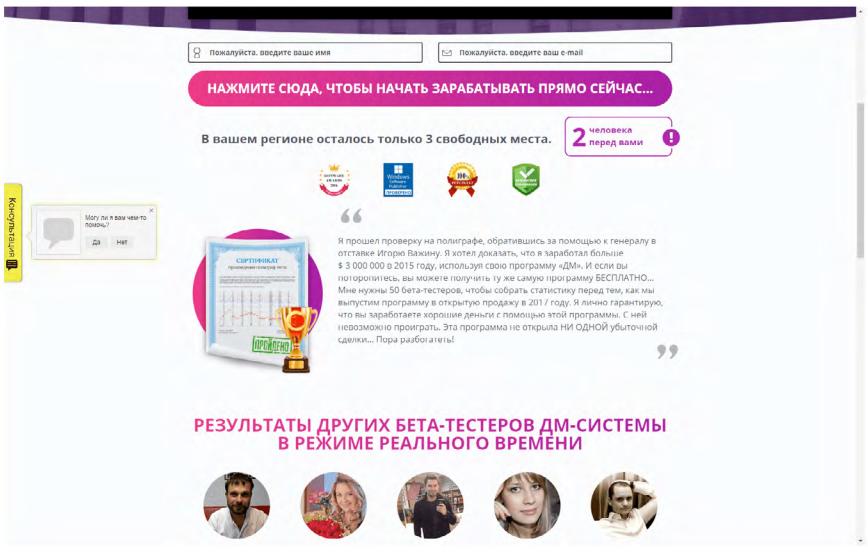
Как и в прошлые годы, в 2016-м в Интернете проявляли активность сетевые мошенники, пытающиеся нажиться на доверчивых пользователях. Еще в апреле компания «Доктор Веб» рассказывала о поддельных интернет-магазинах, беззастенчиво обманывающих своих покупателей.

Обзор вирусной активности за 2016 год



Подобные магазины обещают организовать доставку выбранного товара в любой регион России на условиях стопроцентной предоплаты. Оплатив покупку (как правило, на несколько десятков тысяч рублей), жертва ожидает подтверждения отправки своего заказа, однако спустя некоторое время сайт интернет-магазина неожиданно исчезает, отосланные на контактный адрес электронной почты письма возвращаются, а телефонный номер мошенников замолкает навсегда. И уже через несколько дней в точности такой же магазин с аналогичным ассортиментом товаров появляется в Интернете по другому адресу и с другим названием. В опубликованной на сайте компании обзорной статье специалисты «Доктор Веб» рассказали о том, по каким признакам можно отличить поддельный интернет-магазин от настоящего.

Еще одним популярным способом сетевого мошенничества в 2016 году воспользовались создатели сайта «Детектор Миллионера», о котором мы рассказывали в минувшем октябре.



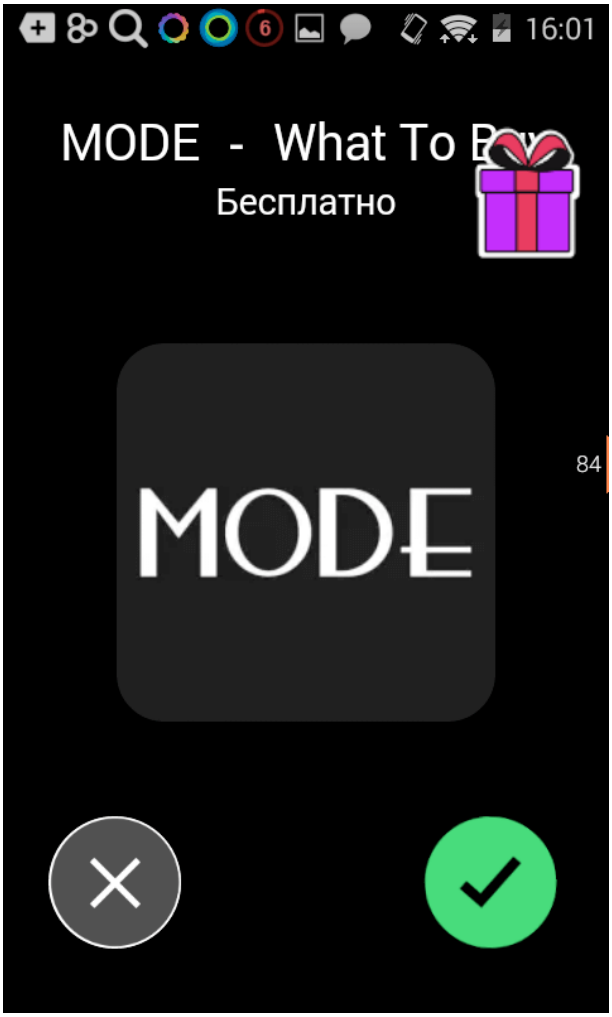
Этот ресурс и многие подобные ему являются разновидностью системы бинарных опционов — жульнической схемы, известной как минимум с 2014 года. Вне всяких сомнений сетевые мошенники будут и в дальнейшем совершенствовать используемые ими незаконные способы заработка, поэтому пользователям Интернета не стоит терять бдительности.

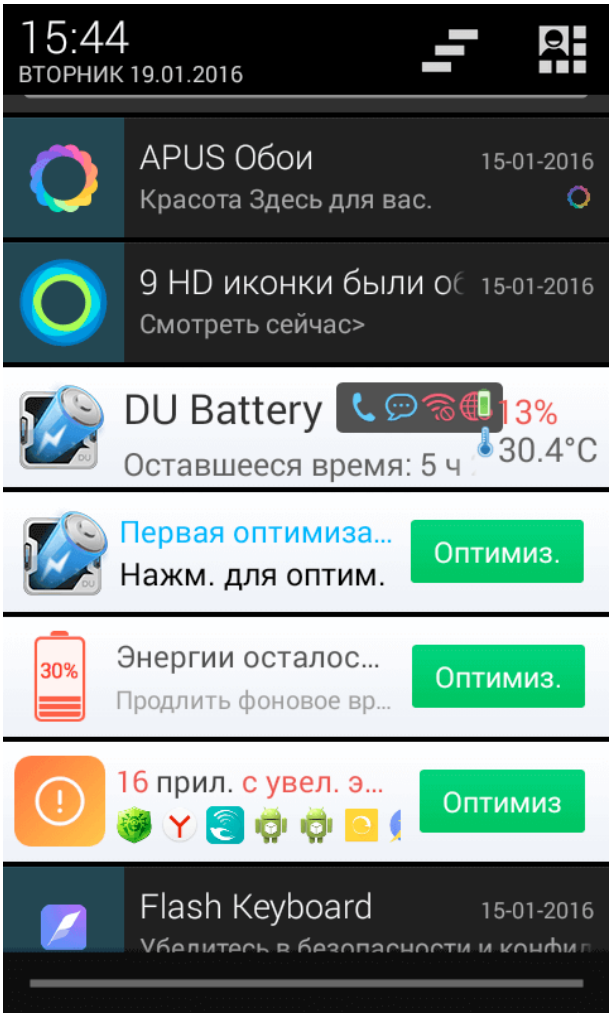
Для мобильных устройств

В 2016 году киберпреступники вновь не оставили без внимания владельцев мобильных устройств. В течение прошедших 12 месяцев было выявлено множество вредоносных и нежелательных программ, предназначенных для работы на смартфонах и планшетах. Как и прежде, основной интерес для вирусописателей представляли Android-устройства, однако не обошлось и без появления угроз для платформы iOS.

Главной целью злоумышленников, атакующих Android-смартфоны и планшеты, остается получение незаконной прибыли. И для этого в арсенале вирусописателей имеется сразу несколько инструментов. Один из них — троянцы, которые устанавливают ненужные приложения и показывают рекламу. В 2015 году наблюдалась тенденция распространения таких вредоносных программ, при этом многие из них пытались с использованием эксплойтов получить root-доступ, чтобы устанавливать ПО незаметно. В 2016 году эта тенденция сохранилась, однако вирусописатели пошли еще дальше и нашли несколько новых нестандартных решений. Так, в начале года вирусные аналитики «Доктор Веб» обнаружили троянцев семейства Android.Loki, которые внедрялись в процессы программ (в том числе системных) и могли незаметно устанавливать и удалять любые приложения. Уже в конце года появилась новая версия одного из этих вредоносных приложений, которая научилась заражать не только процессы, но и системные библиотеки. В результате этот троянец также получал root-привилегии и скрытно выполнял установку программ.

Некоторые злоумышленники внедряют троянцев-установщиков и рекламных троянцев непосредственно в прошивку мобильных устройств, причем в большинстве случаев производители зараженных смартфонов и планшетов сами не подозревают о том, что поставляют на рынок зараженные девайсы. В 2016 году было выявлено сразу несколько таких случаев. Например, в январе компания «Доктор Веб» сообщала о троянце Android.Cooee.1, обнаруженном в прошивке одного из популярных смартфонов.





Android.Cooee.1 был встроен в созданную вирусописателями графическую оболочку и представлял собой рекламный модуль. Этот троянец показывал рекламу, а также незаметно загружал и запускал различные приложения, среди которых были и вредоносные.

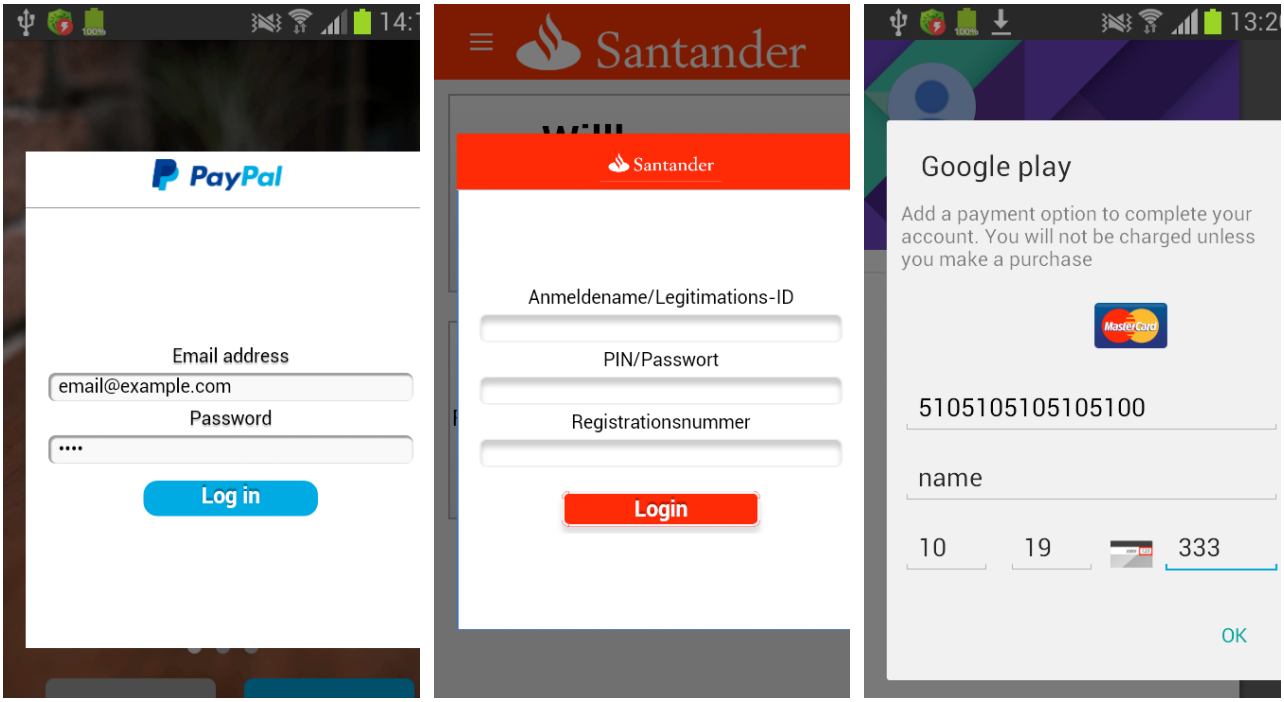
В марте был обнаружен троянец Android.Gmobi.1, которого киберпреступники предустановили на нескольких десятках моделей мобильных устройств, а в ноябре стало известно о появлении аналогичного троянца, который получил имя Android.Spy.332.origin. Обе эти вредоносные программы располагались в системном каталоге зараженных смартфонов и планшетов. Они незаметно для пользователей скачивали и устанавливали программы, а также выполняли другие нежелательные действия.

Вместе с откровенно троянскими приложениями очень часто для распространения ненужных программ и показа рекламы вирусописатели используют рекламные модули, которые условно не являются вредоносными. В 2016 году среди всех потенциально опасных программ, выявленных на смартфонах и планшетах, такие модули были в лидерах по числу обнаружений антивирусными продуктами Dr.Web для Android.

Обзор вирусной активности за 2016 год

Другим распространенным источником незаконного заработка, который злоумышленники продолжают активно использовать, остаются банковские троянцы. По сравнению с прошлым годом, в 2016 году антивирусные продукты Dr.Web для Android обнаружили на 138% больше проникновений этих вредоносных программ на Android-устройства.

Одним из таких троянцев стал Android.SmsSpy.88.origin, который известен вирусным аналитикам еще с 2014 года. Авторы этого банкера постоянно его совершенствуют и теперь используют при атаках на клиентов кредитных организаций по всему миру. Android.SmsSpy.88.origin отслеживает запуск десятков банковских приложений. После того как одно из них начинает работать, троянец показывает поверх его окна поддельную форму аутентификации, запрашивая логин и пароль от учетной записи сервиса мобильного банкинга. Фактически Android.SmsSpy.88.origin может атаковать клиентов любого банка — вирусописателям достаточно лишь создать нужную мошенническую форму и загрузить ее на управляющий сервер.



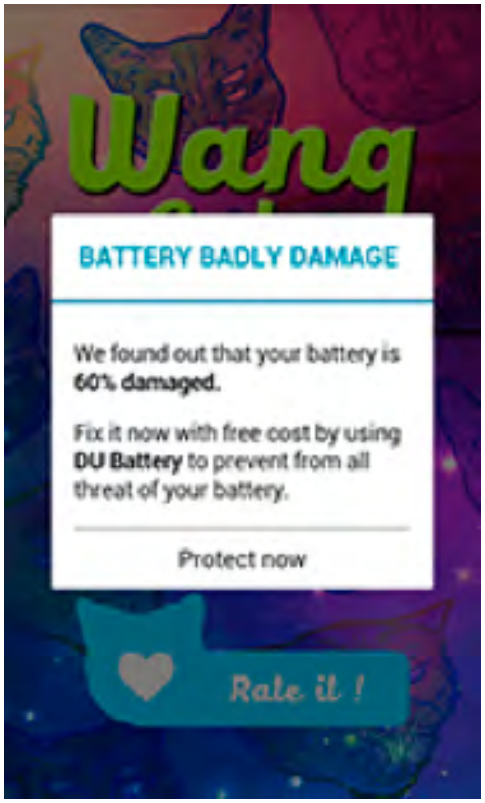
Вирусные аналитики Dr.Web установили, что с начала 2016 года этот троянец заразил порядка 40 000 мобильных устройств, а жертвами банкера стали жители более 200 стран. Подробнее об этом опасном банковском троянце рассказано в соответствующем материале.

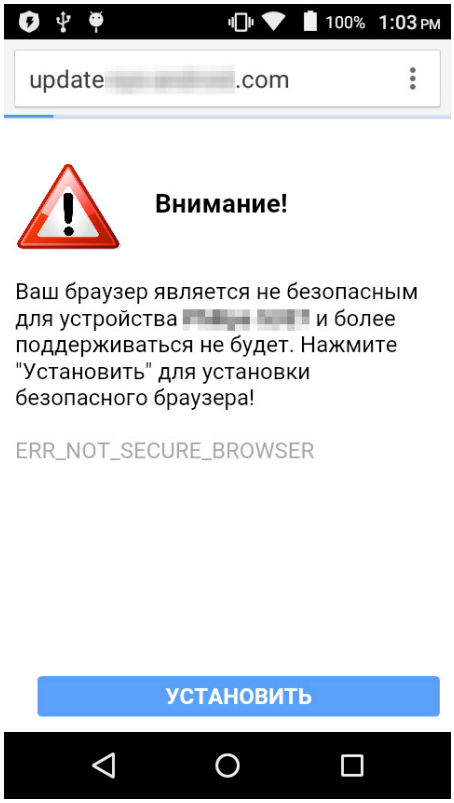
Еще один Android-банкер, который был выявлен в 2016 году, получил имя Android.BankBot.104.origin. После заражения мобильного устройства он проверял баланс доступных банковских счетов и при наличии там денег незаметно переводил средства злоумышленникам.

Обзор вирусной активности за 2016 год

Троянцы-вымогатели семейства Android.Locker по прежнему представляют серьезную угрозу для владельцев Android-смартфонов и планшетов. Они блокируют мобильные устройства и требуют выкуп за разблокировку. А особо опасные представители этого семейства могут зашифровать все доступные файлы — фотографии, документы, видеоролики, музыку и т. п. При этом сумма выкупа часто превышает несколько сотен долларов США. В 2016 году вирусописатели продолжили атаковать пользователей при помощи таких вредоносных приложений, однако пик их распространения пришелся на начало года. В течение 12 месяцев антивирусные продукты Dr.Web для Android обнаруживали вымогателей на мобильных устройствах более 540 000 раз.

В течение 2016 года в официальном каталоге приложений Google Play было найдено множество троянцев. Так, в марте вирусные аналитики «Доктор Веб» выявили вредоносную программу Android.Spy.277.origin, которая показывала рекламу и пугала пользователя тем, что аккумулятор его мобильного устройства поврежден. При этом для его восстановления тут же предлагалось установить некое приложение. Похожий троянец, обнаруженный в апреле, получил имя Android.Click.95. После запуска он проверял, установлено ли на зараженном устройстве одно из приложений, которое он должен был рекламировать. Если эта программа не находилась, троянец загружал мошеннический веб-сайт, на котором пользователя либо ждало тревожное сообщение о повреждении аккумулятора, либо говорилось, что текущая версия браузера небезопасна. В обоих случаях для решения «проблемы» все так же предлагалось установить ту или иную программу, которая владельцу устройства была вовсе не нужна.





В июне в каталоге Google Play был обнаружен троянец Android.PWS.Vk.3, который позволял прослушивать музыку из социальной сети «ВКонтакте», для чего запрашивал логин и пароль от учетной записи. Вредоносная программа действительно имела заявленную функцию, однако полученные конфиденциальные данные она незаметно для пользователя передавала на сервер злоумышленников. В этом же месяце компания «Доктор Веб» сообщила о троянце Android.Valeriy.1.origin, которого вирусописатели также распространяли через Google Play. Эта вредоносная программа показывала всплывающие окна, в которых пользователям предлагалось ввести номер мобильного телефона для загрузки той или иной программы. После того как владелец зараженного устройства указывал свой телефон, ему приходило СМС с информацией о подписке на дорогостоящий сервис, однако Android.Valeriy.1.origin отслеживал такие сообщения и скрывал их. Кроме того, он мог нажимать на рекламные баннеры и переходить по ссылкам, а также скачивал ненужные программы, среди которых встречались даже другие троянцы.

В июле в каталоге Google Play была найдена вредоносная программа Android.Spy.305.origin, основная задача которой заключалась в показе рекламы. Другой троянец, проникший в официальный каталог приложений ОС Android, был обнаружен в сентябре. Он получил имя Android.SockBot.1. Этот троянец превращал зараженное устройство в прокси-сервер и позволял вирусописателям анонимно соединяться с удаленными устройствами, подключенными к сети. Кроме того, с его помощью киберпреступники могли перенаправлять сетевой трафик, похищать конфиденциальную информацию и организовывать DDoS-атаки на различные интернет-серверы. А в сентябре вирусные аналитики «Доктор Веб» выявили в Google Play троянца, добавленного в вирусную базу как Android.MulDrop.924. Часть функционала этого вредоносного приложения находилась во вспомогательных модулях, которые были зашифрованы и спрятаны внутри PNG-изображения, расположенного в каталоге ресурсов Android.MulDrop.924. Один из этих компонентов содержал несколько рекламных плагинов, а также троянца-загрузчика Android.DownLoader.451.origin, который незаметно для пользователя скачивал игры и приложения и предлагал установить их. Кроме того, этот загрузчик показывал навязчивую рекламу в панели уведомлений мобильного устройства.

В 2016 году не остались без внимания вирусописателей и пользователи мобильных устройств под управлением iOS. В феврале в вирусную базу Dr.Web была добавлена потенциально опасная программа Program.IPhoneOS.Unwanted.ZergHelper, которая распространялась через каталог App Store. С ее помощью владельцы мобильных устройств могли скачать различные приложения, включая взломанные версии платного ПО, а также программы, не прошедшие предварительную проверку в компании Apple. Кроме того, она могла загружать свои обновления в обход каталога App Store, а также запрашивала идентификатор Apple ID и пароль пользователя. В марте был обнаружен троянец IPhoneOS.AceDeciever.6, который также запрашивал у владельцев iOS-смартфонов и планшетов идентификатор Apple ID и пароль. IPhoneOS.AceDeciever.6 автоматически устанавливался на мобильные устройства после того, как они при помощи USB-кабеля подключались к компьютерам под управлением Windows с установленным на нем приложением с именем 爱思助手. Эта программа позиционировалась как аналог утилиты iTunes и была добавлена в вирусную базу как троянец Trojan.AceDeciever.2.

Перспективы и вероятные тенденции

Анализ киберкриминальной обстановки, сложившейся в 2016 году, позволяет сделать некоторые прогнозы относительно развития ситуации в сфере информационной безопасности в году наступающем. В первую очередь ожидается рост количества вредоносных программ для устройств, работающих под управлением ОС семейства Linux — то есть, для «Интернета вещей». Исходя из имеющихся в распоряжении вирусных аналитиков данных можно предположить, что будет увеличиваться как число атак на уязвимые устройства с использованием протоколов Telnet и SSH, так и ассортимент используемых злоумышленниками вредоносных программ. Будут расти и их функциональные возможности. Логическим продолжением этой тенденции может стать рост интенсивности DDoS-атак на различные сетевые узлы и IT-инфраструктуру отдельных интернет-сервисов.

По-прежнему высокую опасность для пользователей представляют троянцы-шифровальщики, уже сегодня угрожающие не только владельцам устройств под управлением ОС Windows, но также успешно освоившие Linux, Android и macOS. Можно предположить, что используемые ими алгоритмы шифрования будут усложняться, а количество энкодеров наиболее распространенных семейств — расти.

В качестве третьей наиболее вероятной тенденции наступающего 2017 года можно назвать ожидаемый рост числа разновидностей и общего количества вредоносных программ для мобильной платформы Google Android, и в первую очередь — банковских троянцев. Ни для кого не секрет, что приложения банк-клиент для смартфонов и планшетов весьма удобны и пользуются высокой популярностью среди владельцев таких устройств. Этим они и привлекают многочисленных злоумышленников, стремящихся получить прибыль любыми незаконными способами. Несмотря на усилия разработчика Android, корпорации Google, эта система все еще остается уязвимой для многочисленных троянцев.

Будут совершенствоваться способы доставки опасного ПО. Уже сейчас хорошо заметен рост количества почтовых рассылок, использующих для установки различных троянцев вредоносные сценарии, написанные на различных скриптовых языках, в частности JavaScript. Среди вложений в электронных письмах нередко встречаются файлы, использующие известные уязвимости в офисных приложениях. Нет никаких оснований сомневаться в том, что ассортимент используемых киберпреступниками методов заражения компьютеров пользователей вредоносными программами будет расширяться и в наступающем году.

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