Dr.WEB®
с 1992 года

Обзор вирусной активности в апреле 2017 года

Обзор вирусной активности в апреле 2017 года

28 апреля 2017 года

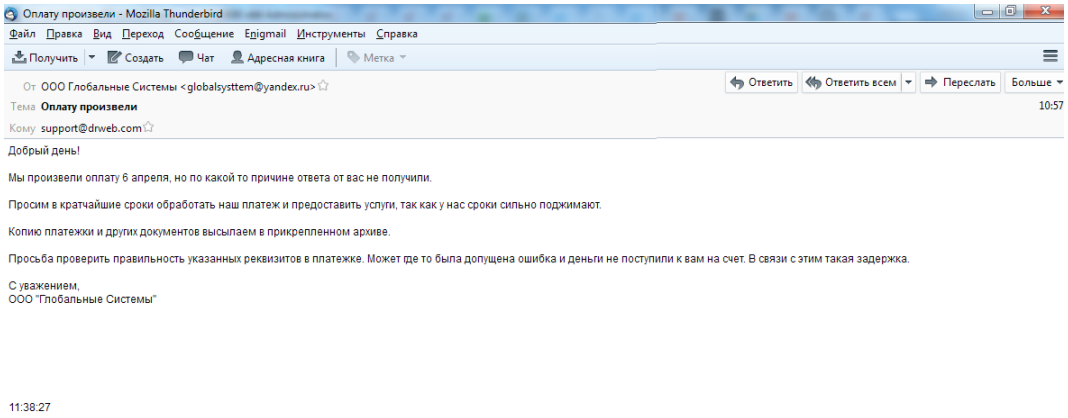
В апреле произошло много событий, связанных с информационной безопасностью. В начале месяца киберпреступники организовали вредоносную рассылку, с помощью которой распространялся многокомпонентный троянец. Он предназначен для кражи с инфицированного компьютера конфиденциальной информации. В середине апреля специалисты «Доктор Веб» исследовали мошенническую схему, в которой злоумышленники использовали для обмана пользователей вредоносную программу. В конце месяца была выявлена уязвимость в офисном ПО Microsoft Office и зафиксировано распространение троянца, ворующего с инфицированного компьютера пароли.

Главные тенденции апреля

- Распространение вредоносной рассылки с многокомпонентным троянцем
- Обнаружение уязвимости в Microsoft Office
- Распространение троянских программ для Windows

Угроза месяца

Многофункциональный троянец, получивший наименование Trojan.MulDrop7.24844, распространялся в виде заархивированного вложения в сообщении электронной почты.

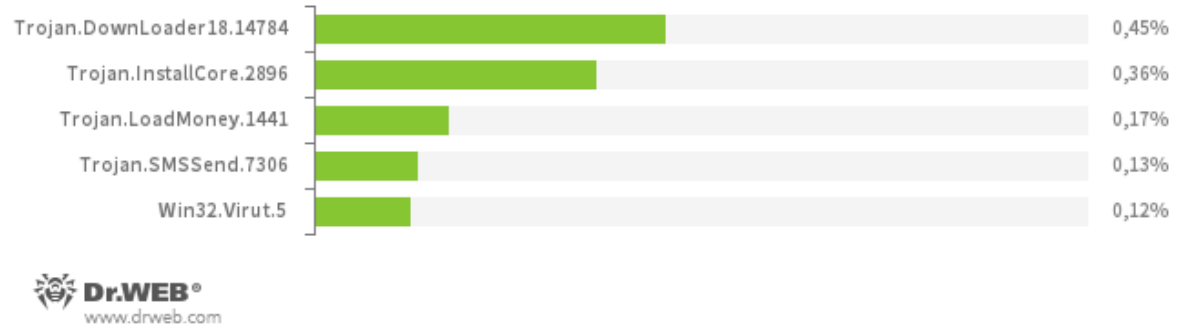


В архиве содержится упакованный контейнер, который создан с использованием возможностей языка Autoit. Один из компонентов, который Trojan.MulDrop7.24844 запускает на зараженном компьютере, — приложение для удаленного администрирования, детектируемое Антивирусом Dr.Web как Program.RemoteAdmin.753. Кроме него троянец сохраняет на диск два других приложения, которые являются 32- и 64-разрядной версиями утилиты Mimikatz. Она предназначена для перехвата паролей открытых сессий в Windows. Trojan.MulDrop7.24844 активирует кейлоггер, записывающий в файл информацию о нажатых пользователем клавишах, а также выполняет ряд других функций, определяемых заданным при его запуске параметром. Троянец открывает злоумышленникам удаленный доступ по протоколу RDP (Remote Desktop Protocol), вследствие чего те могут управлять инфицированным компьютером. Подробнее об этой вредоносной программе рассказано в опубликованной на сайте компании «Доктор Веб» статье.

Обзор вирусной активности в апреле 2017 года

По данным статистики Антивируса Dr.Web

Наиболее распространенные вредоносные программы согласно статистике Антивируса Dr.Web

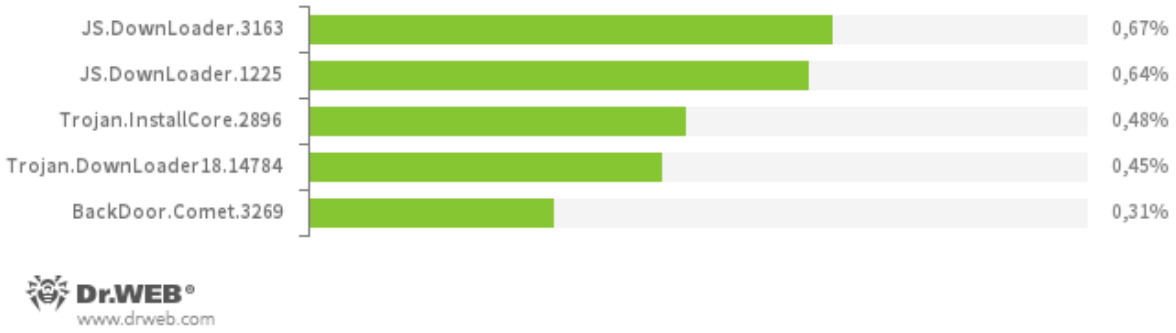


- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.SMSSend.7306**
  Представитель семейства вредоносных программ, реализованных в виде архива со встроенным инсталлятором. Он предлагает либо отправить платное СМС-сообщение на короткий сервисный номер для продолжения установки и получения доступа к содержимому архива, либо указать номер телефона и ввести полученный в ответном сообщении код, согласившись с условиями платной подписки. Основная «специализация» Trojan.SMSSend – вымогательство.
- **Win32.Virut.5**
  Сложный полиморфный вирус, заражающий исполняемые файлы и содержащий функции удаленного управления инфицированным компьютером.

Обзор вирусной активности в апреле 2017 года

По данным серверов статистики «Доктор Веб»

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

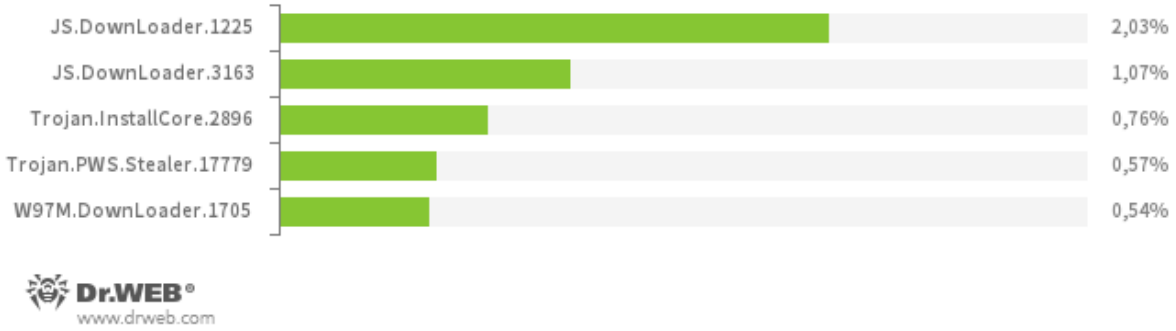


- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **BackDoor.Comet.3269**
  Представитель семейства вредоносных программ, выполняющих на зараженном устройстве поступающие от злоумышленников команды и предоставляющих к нему несанкционированный доступ.

Обзор вирусной активности в апреле 2017 года

Статистика вредоносных программ в почтовом трафике

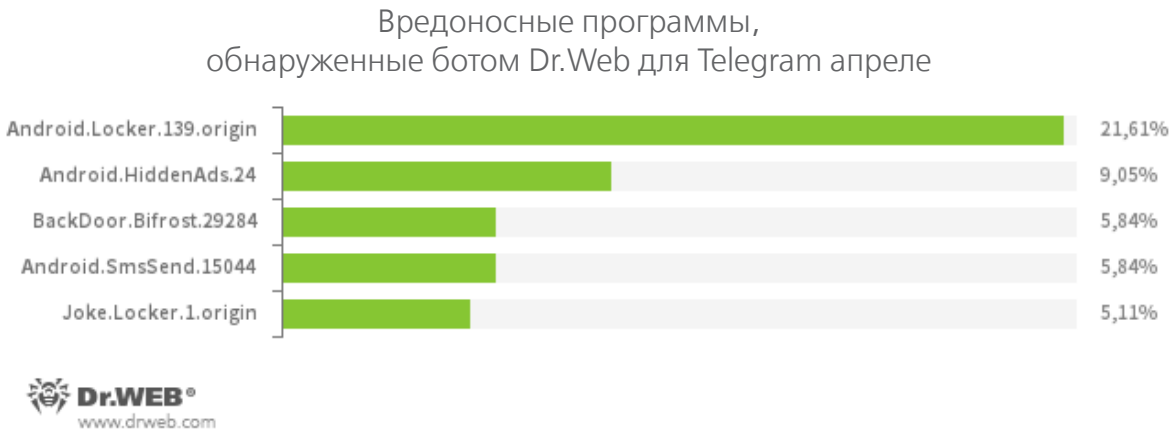
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в апреле 2017 года



- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Обзор вирусной активности в апреле 2017 года

По данным бота Dr.Web для Telegram



- **Android.Locker.139.origin**
  Представитель семейства Android-троянцев, предназначенных для вымогательства. Он показывает навязчивое сообщение якобы о нарушении закона и о последовавшей в связи с этим блокировке мобильного устройства, для снятия которой пользователю предлагается заплатить определенную сумму.
- **Android.HiddenAds.24**
  Троянец, предназначенный для показа навязчивой рекламы.
- **BackDoor.Bifrost.29284**
  Представитель семейства троянцев-бэкдоров, способных выполнять на зараженной машине поступающие от злоумышленников команды.
- **Android.SmsSend.15044**
  Представитель семейства вредоносных программ, предназначенных для отправки СМС-сообщений с повышенной тарификацией и подписки пользователей на различные платные контент-услуги и сервисы.
- **Joke.Locker.1.origin**
  Программа-шутка для ОС Android, блокирующая экран мобильного устройства и выводящая на него изображение «синего экрана смерти» ОС Windows (BSOD, Blue Screen of Death).

Обзор вирусной активности в апреле 2017 года

Трояны-шифровальщики

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

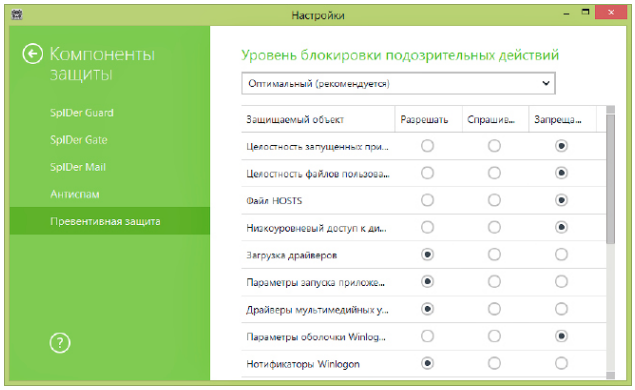
В апреле в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих модификаций троянцев-шифровальщиков:

- **Trojan.Encoder.858** — 33.57% обращений;
- **Trojan.Encoder.3953** — 8.97% обращений;
- **Trojan.Encoder.567** — 3.80% обращений;
- **Trojan.Encoder.10144** — 3.59% обращений;
- **Trojan.Encoder.761** — 2.58% обращений.

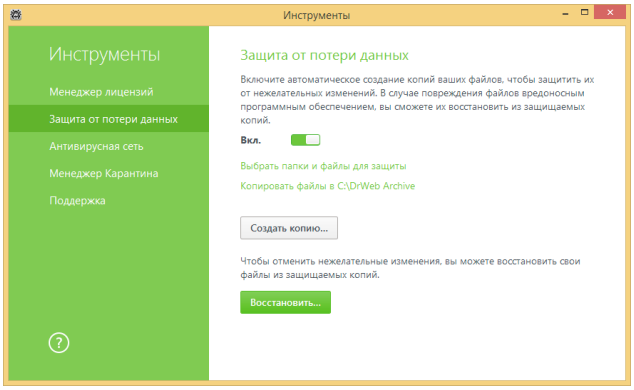
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



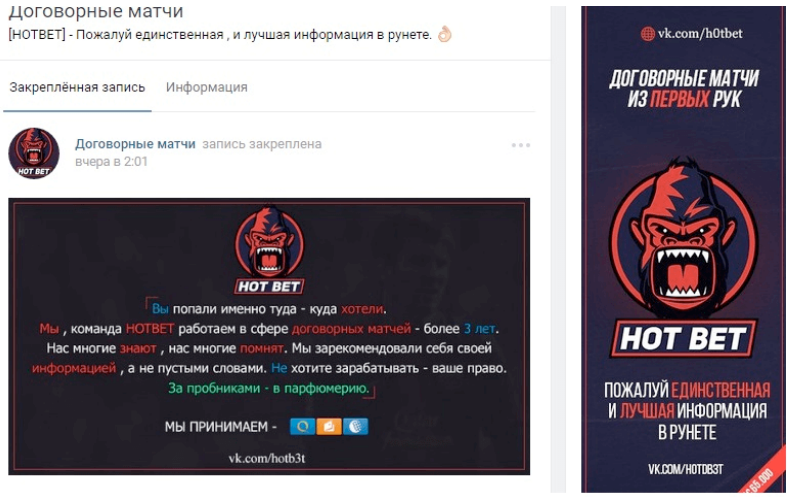
Подробней Смотрите видео о настройке

Опасные сайты

В течение апреля 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 568 903 интернет-адреса.

Март 2017	Апрель 2017	Динамика
+ 223 173	+ 568 903	+ 154.91%

В середине апреля компания «Доктор Веб» рассказала о мошеннической схеме, которую с некоторых пор используют сетевые жулики, промышляющие «договорными матчами».



Обычно мошенники продают доверчивым пользователям недостоверную информацию об исходе предстоящих спортивных состязаний, с использованием которой можно делать якобы гарантированно выигрышные ставки в букмекерских конторах. Теперь киберпреступники предлагают потенциальной жертве скачать защищенный паролем самораспаковывающийся RAR-архив, якобы содержащий текстовый файл с результатами того или иного матча. Пароль для архива жулики высылают после завершения состязания – так потенциальная жертва может убедиться в качестве прогноза. Однако вместо архива она получает написанную злоумышленниками программу, полностью имитирующую интерфейс и поведение SFX-архива, созданного с помощью приложения 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.

Программа была добавлена в вирусные базы Dr.Web под именем Trojan.Fraudster.2986, а адреса распространяющих ее веб-страниц – в базы нерекомендуемых сайтов.

Узнайте больше о нерекомендуемых Dr.Web сайтах

Другие события в сфере информационной безопасности

В конце апреля было зафиксировано распространение вредоносной программы Trojan.DownLoader23.60762, предназначенной для хищения паролей из популярных браузеров и несанкционированного скачивания различных файлов. На зараженном компьютере троянец встраивается в процессы браузеров и перехватывает функции, отвечающие за работу с сетью. Он может выполнять следующие команды:

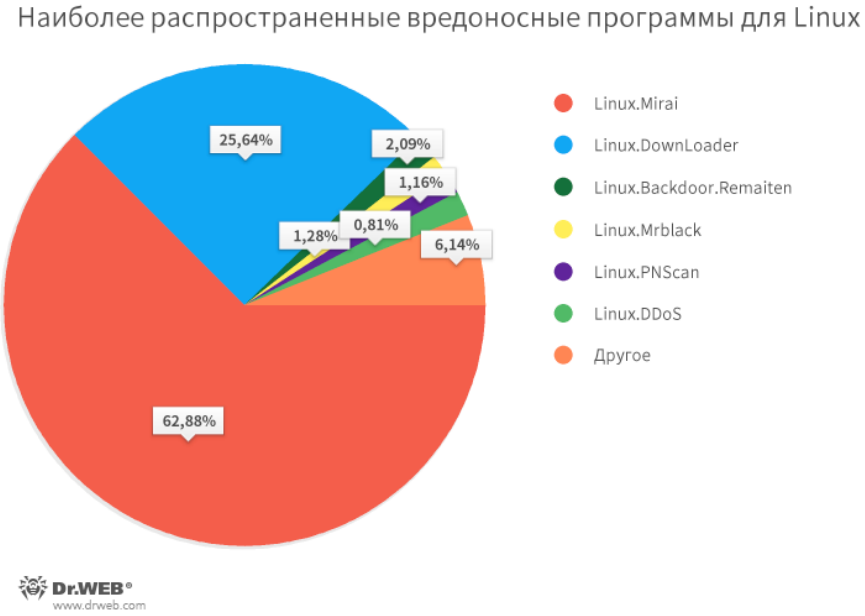
- запустить файл из временной папки на диске зараженного компьютера;
- встроиться в работающий процесс;
- скачать указанный файл;
- запустить указанный исполняемый файл;
- сохранить и передать злоумышленникам базу данных SQLite, используемую Google Chrome;
- сменить управляющий сервер на указанный;
- удалить файлы cookies;
- перезагрузить операционную систему;
- выключить компьютер.

Подробнее об этой вредоносной программе рассказано в опубликованном на нашем сайте материале.

Также в апреле была выявлена уязвимость в текстовом редакторе Word, входящем в состав пакета Microsoft Office. Злоумышленники создали для этой уязвимости эксплойт Exploit.Ole2link.1. Эксплойт реализован в виде документа Microsoft Word, имеющего расширение .docx. При попытке открытия этого документа происходит загрузка другого файла с именем doc.doc, который содержит встроенный HTA-сценарий, детектируемый Dr.Web под именем PowerShell.DownLoader.72. Этот HTA-сценарий, написанный с использованием синтаксиса Windows Script, вызывает командный интерпретатор PowerShell. В нем обрабатывается другой вредоносный скрипт, скачивающий на атакуемый компьютер исполняемый файл. Более полная информация об этой уязвимости изложена в соответствующей обзорной статье.

Вредоносные программы для Linux

В течение минувшего месяца специалисты компании «Доктор Веб» выявили 1 317 388 атак на различные Linux-устройства, из них 147 401 осуществлялась по протоколу SSH и 1 169 987— по протоколу Telnet. Пропорциональное соотношение вредоносных программ, которые киберпреступники загружали на атакованные устройства, показано на следующей диаграмме:



- **Linux.Mirai**
  Троянец для ОС Linux, предназначенный для организации DDoS-атак. Может отключать предотвращающий зависание операционной системы сторожевой таймер watchdog (чтобы исключить перезагрузку устройства).
- **Linux.DownLoader**
  Семейство вредоносных программ и скриптов для Linux, предназначенных для загрузки и установки на атакуемое устройство других вредоносных программ.
- **Linux.BackDoor.Remaiten**
  Семейство вредоносных программ для Linux, предназначенных для осуществления DDoS-атак. Троянцы этого семейства умеют взламывать устройства по протоколу Telnet методом перебора паролей, в случае успеха сохраняют на устройство загрузчик, написанный на языке Ассемблер. Этот загрузчик предназначен для скачивания и установки на атакуемое устройство других вредоносных приложений.

- **Linux.Mrblack**
  Троянская программа, предназначенная для выполнения DDoS-атак, ориентирована на работу с дистрибутивами Linux для процессоров ARM. Троянец имеет встроенный обработчик команд, позволяющий выполнять директивы, получаемые от удаленного управляющего сервера.
- **Linux.DDoS**
  Семейство вредоносных программ для Linux-устройств. Предназначены для организации DDoS-атак.
- **Linux.PNScan**
  Семейство сетевых червей, предназначенных 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.

В апреле вирусные аналитики компании «Доктор Веб» исследовали обновленную версию вредоносной программы семейства Linux.UbntFM, которая получила название Linux.UbntFM.2. Этот троянец разработан вирусописателями для операционных систем семейства Linux, в том числе Air OS, которую производит и устанавливает на свои устройства Ubiquiti Networks. Он реализован в виде скриптов bash, распространяющихся в архиве tgz.

Linux.UbntFM.2 создает на инфицированном устройстве новые учетные записи, а также может скачивать и запускать произвольные файлы. Кроме того, троянец умеет атаковать удаленные устройства с использованием уязвимости в веб-интерфейсе Air OS, позволяющей загрузить произвольный файл по произвольному пути без выполнения авторизации. Если троянцу не удалось установить протокол (или на атакуемом устройстве не установлена Air OS), он может попытаться подобрать учетные данные для SSH-соединения по словарю с использованием логинов «root», «admin», «ubnt» и паролей, хранящихся в файле «passlst». Подробнее о принципах работы этой вредоносной программы рассказано в техническом описании.

Кроме того, в апреле была обнаружена новая версия троянца семейства Fgt — Linux.BackDoor.Fgt.645. От предшественников эту модификацию вредоносной программы отличает ограниченный набор функций (среди них остался только модуль подбора паролей для взлома удаленных узлов и дроппер), также новая версия получила возможность отправлять запрос на скачивание и запуск sh-сценария.

Вредоносное и нежелательное ПО для мобильных устройств

В апреле в вирусную базу Dr.Web был добавлен новый троянец-шпион, получивший имя Android.Chrysaor.1.origin. Вирусописатели могли использовать его для таргетированных атак, чтобы украсть конфиденциальную информацию у пользователей мобильных устройств под управлением ОС Android. Также в прошедшем месяце в каталоге Google Play было выявлено сразу несколько новых банковских троянцев. Один из них получил имя Android.BankBot.179.origin. Он распространялся под видом программ для просмотра онлайн-видео, которые в действительности выполняли заявленную функцию. Другой Android-банкер, выявленный в Google Play, был добавлен в вирусную базу как Android.BankBot.180.origin. Этот троянец представлял собой программу-фонарик.

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

- обнаружение Android-троянца, предназначенного для кибершпионажа;
- проникновение в каталог Google Play банковских троянцев, которые похищали конфиденциальную информацию пользователей Android и крали у них деньги.

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

Обзор вирусной активности в апреле 2017 года

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

Полезные ресурсы
ВебIQметр | Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах