Dr.WEB®
с 1992 года

Обзор вирусной активности в июне 2015 года

Обзор вирусной активности в июне 2015 года

30 июня 2015 года

В июне 2015 года произошло сразу несколько весьма любопытных событий в сфере информационной безопасности. Так, специалисты компании «Доктор Веб» зафиксировали факты взлома злоумышленниками ряда веб-сайтов, среди которых оказался и портал Всероссийского центра изучения общественного мнения (ВЦИОМ). Также в течение первого летнего месяца получили распространение новые вредоносные программы для ОС Windows, Mac OS X и Android.

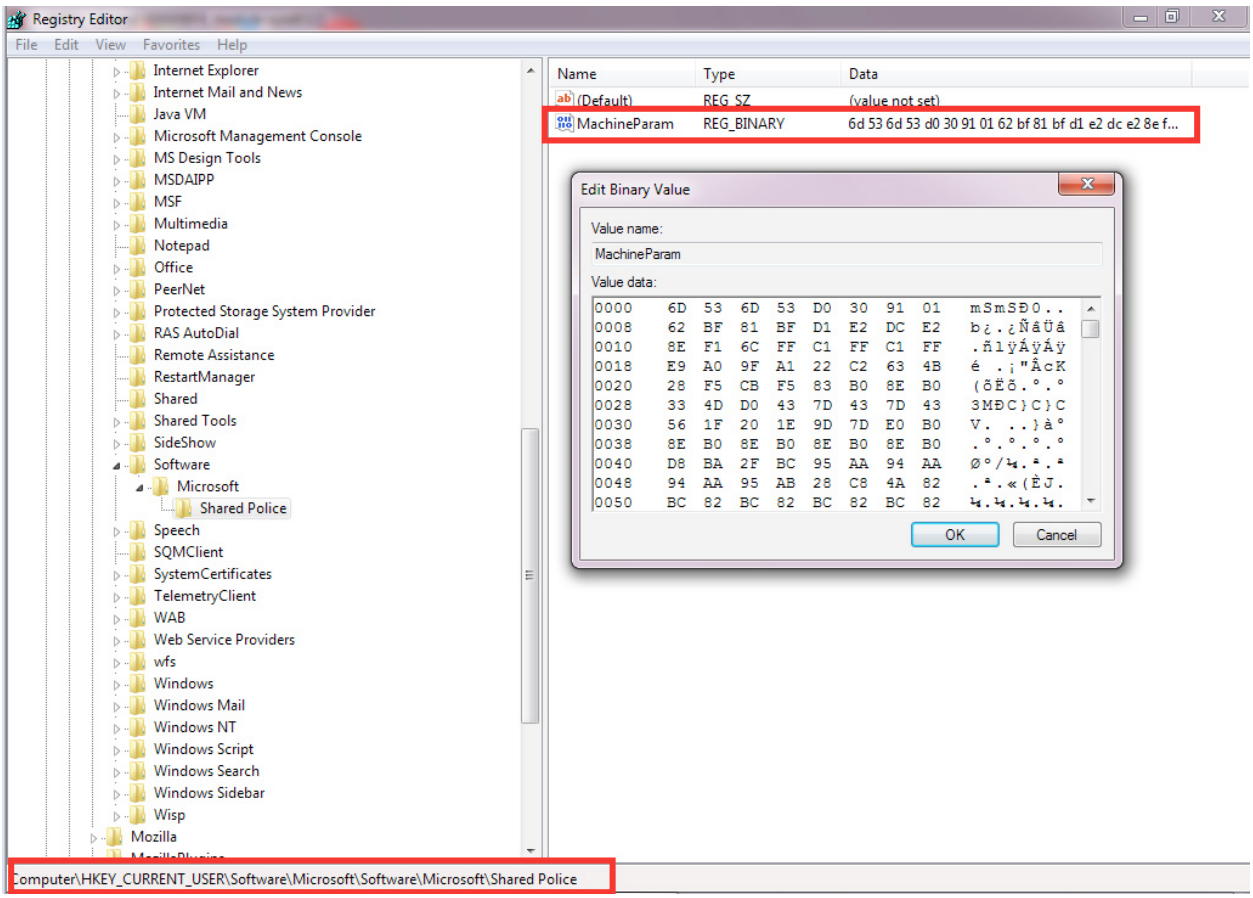
Главные тенденции июня

- Участившиеся случаи взлома злоумышленниками различных веб-сайтов
- Увеличение числа распространяющихся в Интернете установщиков нежелательных приложений для платформы Mac OS X
- Появление новых вредоносных программ для ОС Windows и мобильной платформы Google Android

Обзор вирусной активности в июне 2015 года

Угроза месяца

В начале июня 2015 года вирусные аналитики компании «Доктор Веб» выявили новую троянскую программу Trojan.Proxy.27552, предназначенную для массовой рассылки спама. Этот троянец примечателен тем, что еще на начальном этапе своей работы из-за заложенной в него создателями ошибки может «обрушить» операционную систему, вызвав появление «синего экрана смерти» (BSOD). Другая интересная особенность Trojan.Proxy.27552 заключается в том, что он хранит список адресов своих управляющих серверов в системном реестре Windows.

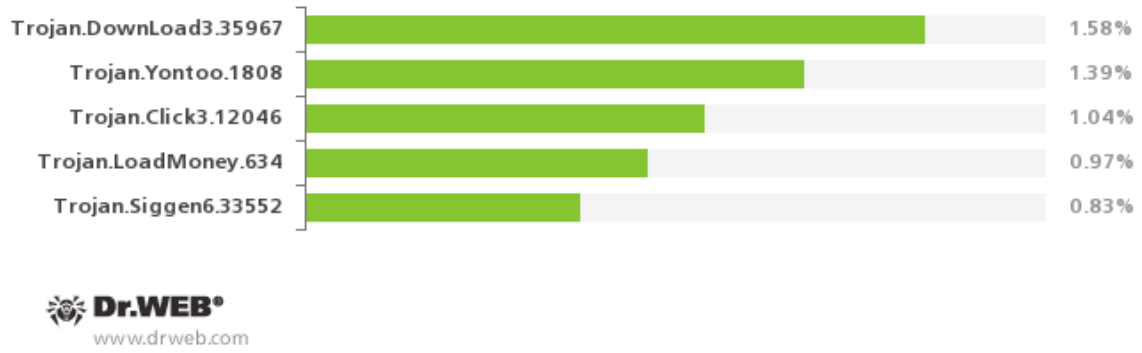


Основное предназначение Trojan.Proxy.27552 – рассылка почтового спама совместно с удаленным спам-сервером. Любопытно, что ссылки в этих письмах ведут в основном на веб-страницы, расположенные на взломанных сайтах. Более подробная информация об этой вредоносной программе изложена в опубликованной на сайте компании «Доктор Веб» статье.

Обзор вирусной активности в июне 2015 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

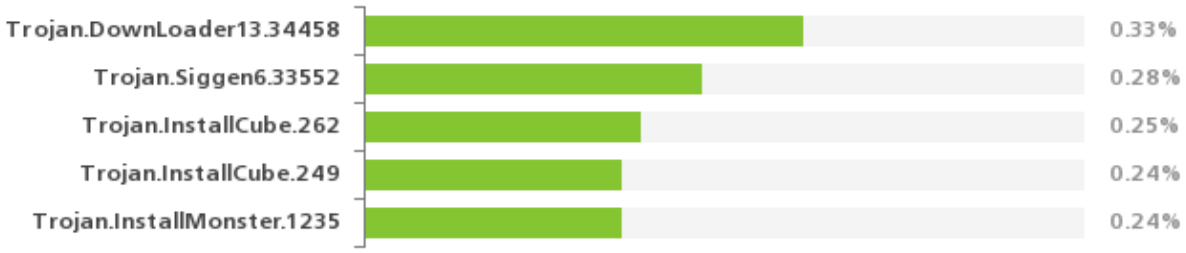


- **Trojan.DownLoader13.34458**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **Trojan.Yontoo**
  Семейство надстроек для популярных браузеров, назначение которых заключается в демонстрации пользователю рекламы при просмотре веб-страниц.
- **Trojan.Click**
  Семейство вредоносных программ, предназначенных для накрутки посещаемости различных интернет-ресурсов путем перенаправления запросов жертвы на определенные сайты с помощью управления поведением браузера.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.

Обзор вирусной активности в июне 2015 года

По данным серверов статистики «Доктор Веб»

Наиболее распространенные вредоносные программы в июне 2015 года
согласно данным серверов статистики Dr.Web

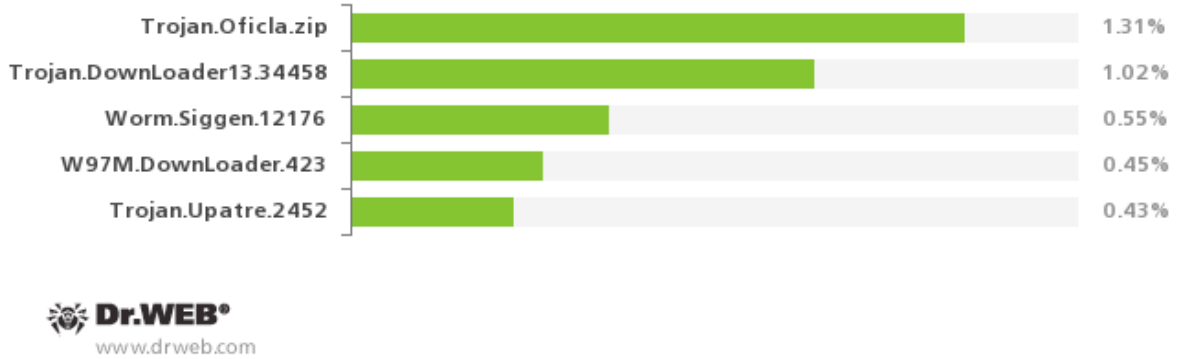


Dr.WEB®
www.drweb.com

- **Trojan.DownLoader13.34458**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.
- **Trojan.InstallCube**
  Семейство программ-загрузчиков, инсталлирующих на компьютер пользователя различные ненужные и нежелательные приложения.
- **Trojan.Installmonster**
  Семейство вредоносных программ, созданных с использованием партнерской программы installmonster. Данные приложения устанавливают на компьютер жертвы различное нежелательное ПО.

Статистика вредоносных программ в почтовом трафике

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в июне 2015 года

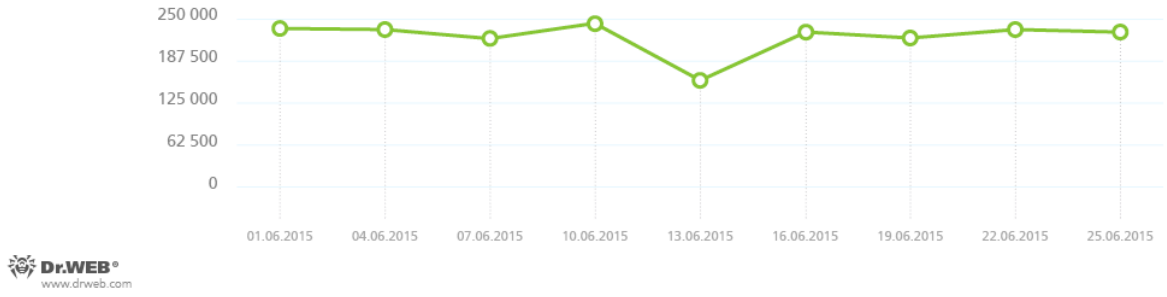


- **Trojan.Oficla**
  Семейство троянцев, распространяющихся преимущественно по каналам электронной почты. При заражении компьютера они скрывают свою вредоносную активность. В дальнейшем Trojan.Oficla включает компьютер в бот-сеть и позволяет злоумышленникам загружать на него другое вредоносное ПО. После заражения системы владельцы бот-сети, формируемой Trojan.Oficla, получают возможность контролировать компьютер жертвы. В частности, они могут загружать, устанавливать и использовать на нем практически любое вредоносное ПО.
- **Trojan.DownLoader13.34458**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **Worm.Siggen.12176**
  Вредоносная программа-червь, распространяющаяся преимущественно в виде вложений в сообщения электронной почты.
- **W97M.DownLoader.423**
  Представитель семейства вредоносных программ, распространяющихся преимущественно по электронной почте в документах Microsoft Word. Предназначен для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.Upatre**
  Семейство троянцев-загрузчиков, предназначенных для скачивания на инфицированный компьютер и скрытной установки других вредоносных приложений.

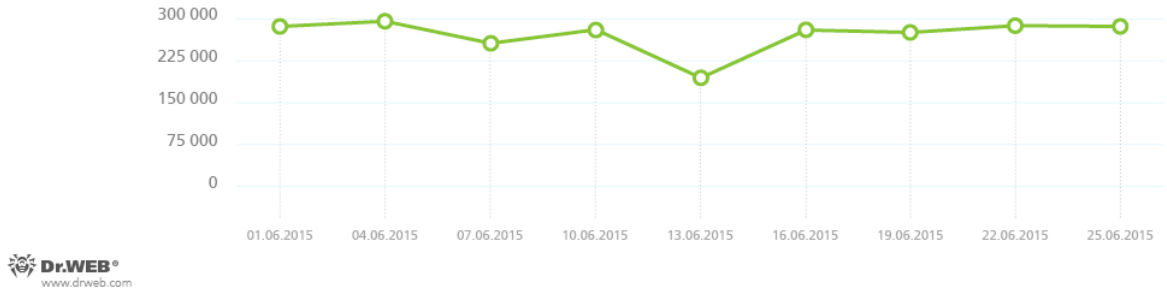
Ботнеты

Вирусные аналитики компании «Доктор Веб» продолжают внимательно следить за активностью бот-сетей, представляющих угрозу современным пользователям. Так, среднесуточная активность двух наблюдаемых специалистами подсетей Win32.Rmnet.12 представлена на следующих диаграммах:

Активность ботнета Win32.Rmnet.12 в июне 2015 года (1 подсеть)



Активность ботнета Win32.Rmnet.12 в июне 2015 года (2 подсеть)



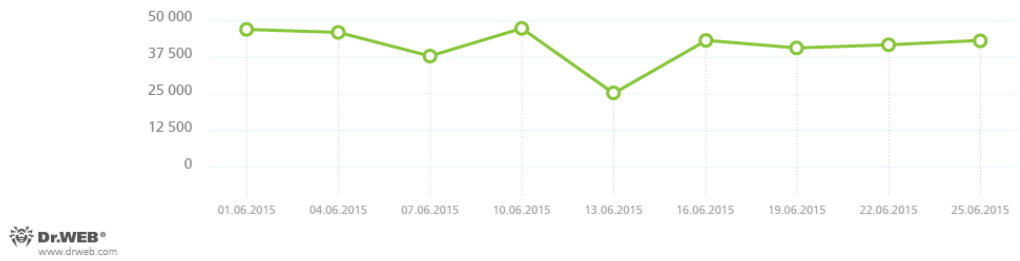
Rmnet — это семейство файловых вирусов, распространяющихся без участия пользователя, способных встраивать в просматриваемые пользователям веб-страницы постороннее содержимое (это теоретически позволяет киберпреступникам получать доступ к банковской информации жертвы), а также красть файлы cookies и пароли от наиболее популярных FTP-клиентов и выполнять различные команды, поступающие от злоумышленников.

Обзор вирусной активности в июне 2015 года

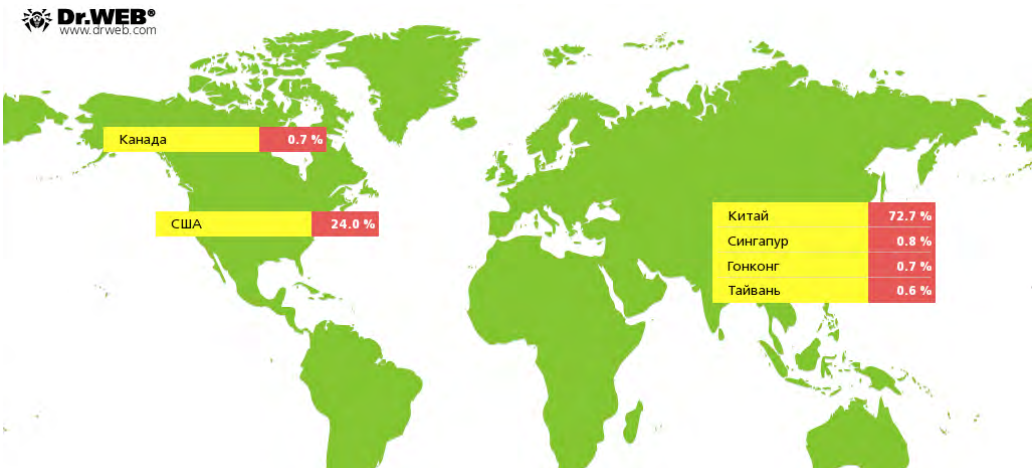
По-прежнему продолжает функционировать бот-сеть, состоящая из компьютеров, зараженных файловым вирусом Win32.Sector. Данная вредоносная программа обладает следующими деструктивными функциями:

- загрузка из P2P-сети и запуск на зараженной машине различных исполняемых файлов;
- встраивание в запущенные на инфицированном компьютере процессы;
- возможность останавливать работу некоторых антивирусных программ и блокировать доступ к сайтам их разработчиков;
- инфицирование файловых объектов на локальных дисках и сменных носителях (где в процессе заражения создает файл автозапуска autorun.inf), а также файлов, хранящиеся в общедоступных сетевых папках.

Активность ботнета Win32.Sector в июне 2015 года



Значительно сократилось по сравнению с предыдущим месяцем число зафиксированных в июне 2015 года атак на различные веб-сайты, осуществляемых злоумышленниками с использованием трояна Linux.BackDoor.Gates.5. В июне число уникальных IP-адресов, на которые осуществлялись атаки, снизилось на 76,6% и составило 1284. Также изменились и цели проводимых злоумышленниками атак: первое место по количеству атакованных интернет-ресурсов теперь занимает Канада, а вторую и третью позицию поделили Китай и США:



Обзор вирусной активности в июне 2015 года

Троянцы-шифровальщики

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

Май 2015	Июнь 2015	Динамика
1200	1417	+ 18%

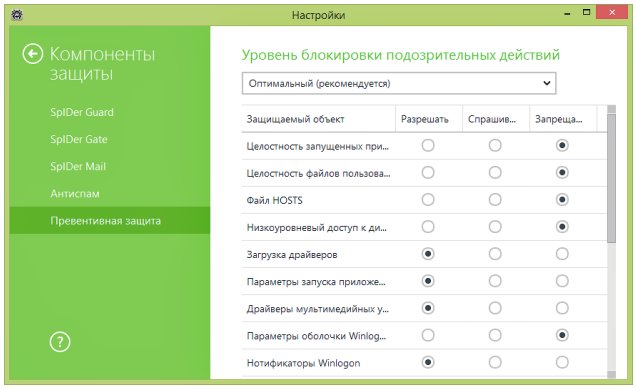
Наиболее распространенные шифровальщики в июне 2015 года:

- Trojan.Encoder.858
- Trojan.Encoder.567
- BAT.Encoder

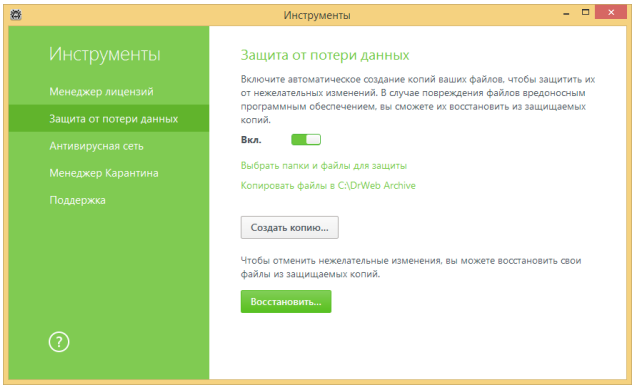
Dr.Web Security Space 10.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери

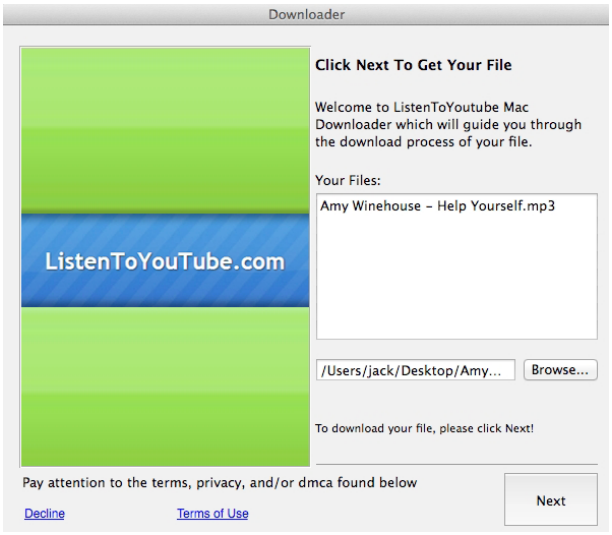


Подробней Смотрите видео о настройке

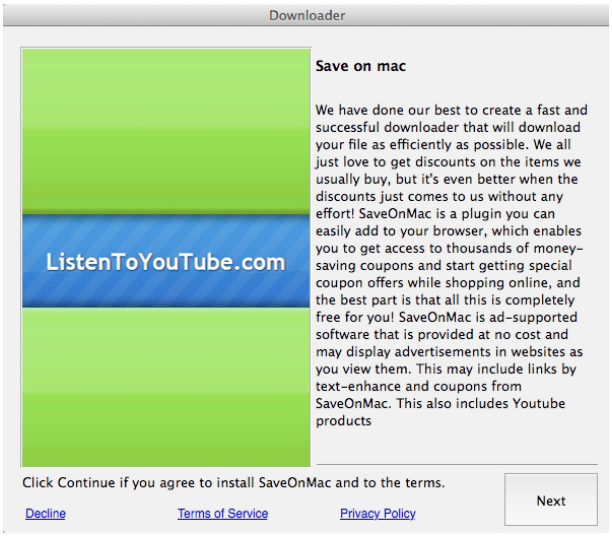
Угрозы для Mac OS X

Среди всех вредоносных программ, угрожающих пользователям операционной системы Mac OS X, значительное количество составляют рекламные троянцы и установщики различных нежелательных приложений. С каждым днем таких программ становится все больше и больше — так, в конце июня очередное подобное приложение было добавлено в вирусные базы под именем Adware.Mac.MacInst.1.

Установщик Adware.Mac.MacInst.1 после своего запуска демонстрирует на экране компьютера диалоговое окно, где сначала отображается информация о запрошенном пользователем файле, который пользователь изначально и собирался скачать.



После нажатия на кнопку «Next» установщик демонстрирует партнерское предложение, подразумевающее, что помимо требуемого файла программа установит и некоторые дополнительные компоненты.



Еще одна опасная программа для Linux получила наименование Linux.Iframe.4 — она представляет собой вредоносный плагин для веб-сервера Apache, который встраивает в передаваемые пользователям html-страницы объект Iframe, а тот, в свою очередь,

Обзор вирусной активности в июне 2015 года

Среди них — программа, детектируемая антивирусом Dr.Web как Trojan.VIndinstaller.3. Это приложение, в свою очередь, устанавливает на компьютер вредоносные надстройки для браузеров Safari, Firefox и Chrome, детектируемые как троянцы семейства Trojan.Crossrider. Более подробную информацию об этом инциденте можно получить, ознакомившись с опубликованной на нашем сайте обзорной статьей.

Узнайте подробности о вредоносных программах для Mac OS X!

Посмотрите видео о том, как вредоносные программы проникают на «маки»

Опасные сайты

Среди прочих опасных и нежелательных интернет-ресурсов, распространяющих вредоносное ПО, в июне 2015 года в базы Dr.Web были временно добавлены ссылки на ряд страниц сайта Всероссийского центра изучения общественного мнения (ВЦИОМ), который был взломан киберпреступниками. Взлому подверглась как русскоязычная (wciom.ru), так и англоязычная (wciom.com) версии официального веб-сайта ВЦИОМ. Злоумышленники создали на скомпрометированном сервере специальный раздел, в котором размещались веб-страницы с заголовками, пользующимися высокой популярностью согласно статистике поисковых систем. Все эти страницы содержали ссылку на скачивание файла, детектируемого антивирусным ПО Dr.Web как один из представителей семейства Trojan.DownLoader. С помощью данного загрузчика злоумышленники устанавливали на компьютер жертвы программу-майнер, предназначенную для добычи различных криптовалют, а также иной нежелательный софт. Судя по собранным киберпреступниками данным статистики, количество потенциальных жертв злоумышленников исчисляется десятками тысяч.

Обзор вирусной активности в июне 2015 года

Период отчета: 14.06.2015 14:45:18 - 16.06.2015 18:53:37 Отчет создан в Вт Июн 16, 2015 - 18:58:19

Сводка

Сводка

Хиты	
Всего хитов	155 503
Хиты посетителей	155 207
Хиты роботов	296
Хитов в день	51 834
Хитов на посетителя	7,24
Кэшированные запросы	793
Ошибочные запросы	5 396
Просмотры страниц	
Всего просмотров страниц	76 982
Просмотров страниц в день	25 660
Просмотров страниц на посетителя	3,59
Посетители	
Всего посетителей	21 429
Посетителей в день	7 143
Всего уникальных IP-адресов	12 436
Трафик	
Всего трафик	465,01 МБ
Трафик посетителей	464,76 МБ
Трафик роботов	248,42 КБ
Трафик в день	155,00 МБ
Трафик на хит	3,06 КБ
Трафик на посетителя	22,21 КБ

Подробности о взломе сайта ВЦИОМ можно узнать в опубликованной компанией «Доктор Веб» информационной статье

В течение июня 2015 года в базу нерекомендуемых и вредоносных сайтов было добавлено 978 982 интернет-адреса.

Май 2015	Июнь 2015	Динамика
+ 221 346	+ 978 982	+ 342,28 %

Обзор вирусной активности в июне 2015 года

Вредоносное и нежелательное ПО для Android

В июне специалисты «Доктор Веб» выявили большое число различных вредоносных и нежелательных программ для ОС Android, а также зафиксировали новые атаки злоумышленников на пользователей Android-смартфонов и планшетов. Наиболее заметные тенденции, связанные с вредоносными Android-приложениями в прошедшем месяце:

- использование злоумышленниками разнообразных банковских троянцев для кражи денег у пользователей ОС Android;
- появление новых Android-вымогателей;
- применение вирусописателями троянцев-загрузчиков для распространения вредоносного ПО среди владельцев мобильных Android-устройств;
- рост числа СМС-троянцев.

Более подробно о вирусной обстановке в «мобильном» сегменте по состоянию на июнь читайте в специально подготовленном обзоре.

Узнайте больше с Dr.Web

Обзор вирусной активности в июне 2015 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