Аналитика, обзоры, рекомендации.

user And LINUX

{ Secure Shell }

UA Linux http://ualinux.com

## Злоумышленники перенаправляют посетителей блога Seagate на вредоносный сайт

### Читайте в этом номере:



Несколько недель назад эксперты Sophos выявили очередную кампанию по распространению вредоносных программ. Организовавшие данную кампанию киберпреступники использовали модули Apache, позволяющие производить внедрение iFrame, перенаправляя посетителей «модифицированных» таким образом сайтов на вредоносные вебсайты, инфицированные BlackHole.

Исследователи утверждают, что одной из жертв злоумышленников стал блог Seagate (smb.media.seagate.com).

Специалисты Sophos связались с представителями компании Seagate, сообщив им о выявленной проблеме ещё в феврале текущего года, но, по имеющейся информации, компания так и не смогла удалить вредоносный iFrame, идентифицированный Sophos как Mal/Iframe-AL.


Эксперты утверждают, что Seagate далеко не единственная жертва Mal/Iframe-AL, столкнувшаяся с подобной проблемой, так как этот вредонос достаточно сложно выявить.

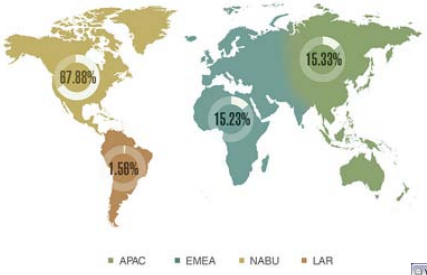
**Источник:**http://www.anti-malware.ru


# User And Linux

# Эксперты Trend Micro исследовали бот-сеть Asprox

Специалисты Trend Micro исследовали бот-сеть Asprox. Известно, что посредством данной бот-сети злоумышленники осуществляли рассылку спама. Киберпреступники рассылали фальшивые электронные письма от имени различных компаний, таких как DHL, FedEx и почтовая служба США.Эксперты отмечают, что с момента своего появления в 2007 году, Asprox генерировала весьма существенную долю мирового спама. Несмотря на то, что за прошедшие годы информации об Asprox было не так уж много, известно, что хозяева бот-сети усовершенствовали её, сделав ещё более эффективной.

Например, известно, что на данный момент Asprox имеет модульную структуру, что позволяет операторам бот-сети, при необходимости, расширять её функциональность.




Кроме того, известно, что посредством Asprox злоумышленники распространяют модуль, крадущий информацию с инфицированных компьютеров. Данный модуль позволяет своим хозяевам «собирать» с инфицированных систем логины и пароли к аккаунтам. Например, электронной почты, сайтов и FTP-серверов.

Чтобы заставить жертв открыть инфицированные файлы или вредоносные ссылки, содержащиеся в письме, злоумышленники используют множество шаблонов писем на разных языках.

Для обхода спам-фильтров Asprox использует скомпрометированные email-аккаунты.

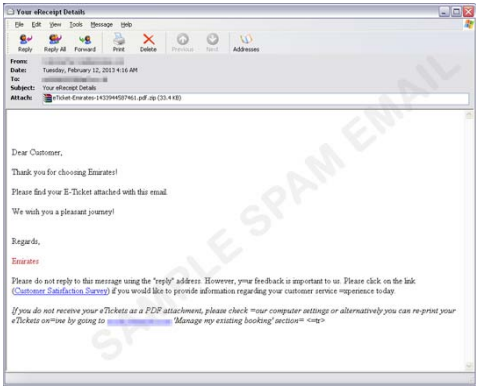
**Источник:** http://www.anti-malware.ru

## Бот-сеть Andromeda вновь напомнила о себе

Специалисты Trend Micro предупреждают о возобновлении активности бот-сети Andromeda, впервые обнаруженной ещё в 2011 году. Известно, что хозяева бот-сети обновили вредоносную программу, распространяемую посредством Andromeda, до версии 2.60. Наибольшая активность Andromeda зарегистрирована в Австралии, Турции и Германии.

Известно, что Andromeda распространяет вредоносную программу BKDR_ANDROM.DA, рассылая электронные письма (спам), содержащие инфицированные файлы или вредоносные ссылки. Переходя по этим ссылкам, жертвы злоумышленников попадают на сайты, инфицированные набором эксплойтов BlackHole.

Попадая на компьютер жертвы, компоненты BlackHole могут выполнять различные функции, например, клавиатурного шпиона (keylogger), а также устанавливать руткиты и загружать дополнительные вредоносные элементы, такие как печально известный троян ZeuS.



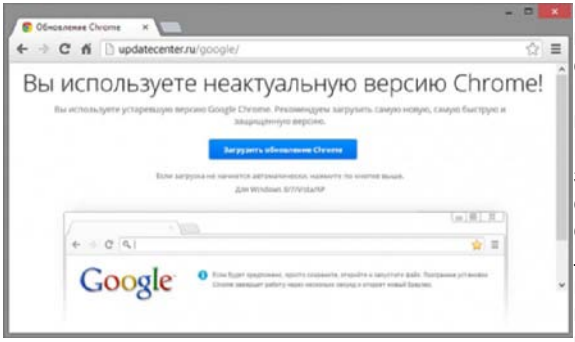

Цена самого вредоноса - до $500 (384 евро). Дополнительные модули продаются отдельно.

**Источник:** http://www.anti-malware.ru

## В Сети появились фальшивые обновления для браузеров с вредоносным ПО.

Русскоязычный сегмент Сети захлестнула волна фальшивых обновлений браузеров. Под их видом киберпреступники устанавливают на компьютеры пользователей вредоносное программное обеспечение.

Многочисленные отзывы русскоязычного сегмента Сети и данные сервиса Яндекс.Блоги указывают на то, что в Рунете активизировались мошенники, занимающиеся распространением вредоносного программного обеспечения под видом обновлений для популярных браузеров.




Распространение вредоносного софта ведется с помощью стилевого оформления, схожего с официальными экранами обновления браузеров Internet Explorer, Firefox, Chrome, Safari и Opera. Для максимальной убедительности преступники имитируют реальный процесс инсталляции обновлений, вводя тем самым в заблуждение невнимательных интернет-пользователей. Предупреждаем, что такое «обновление» на самом деле устанавливает на компьюютер вредоносное программное обеспечение.

Специалисты по безопасности уже призвали пользователей повысить внимание и тестировать антивирусами любой контент, загружаемый из Сети. В частности, эксперты по безопасности из Group-IB создали сайт, позволяющий протестировать любую страничку на предмет надежности.

В данный момент «лечения» для фальшивых обновлений еще не найдено.

**Источник:** http://www.imena.ua

## Программа помощи жертвам хакеров начинает работу.

Google запустил информационную кампанию, из которой пользователи смогут узнать, что делать, если их сайт взломали хакеры, почему это произошло, с какой целью были использованы вредоносные программы и как очистить свой сайт от вирусов. Об этом сообщается на специальной странице Google, посвященной новой инициативе.

Информационная программа «Помощь для взломанных сайтов» включает в себя десятки статей и видео, которые научат владельцев веб-страниц избегать вирусов, а также возвращать контроль над уже взломанным сайтом, пишет Tasstelecom.ru.

«Каждый день злоумышленники угрожают тысячам веб-сайтов. Вирусы часто невидимы для пользователей, но при этом они остаются опасными для любого, кто просматривает страницу – в том числе, для владельцев контента, – отмечает Google. – Например, без ведома владельца хакер может заразить его сайт с помощью вредоносного кода, запоминающего комбинации клавиш, которые используют посетители на своих домашних компьютерах, осуществляя таким образом кражи учетных данных для онлайн-платежей».

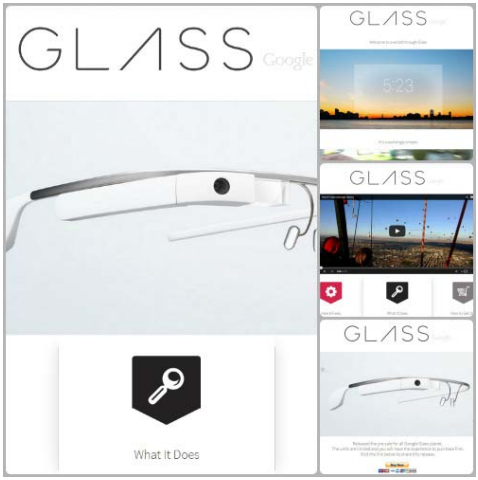
Серия включает в себя ответы на вопросы о том, почему киберпреступники взламывают интернет-сайты, предоставляет справочную информацию о спаме и вредоносных программах, рассказывает о способах очистки и поддержания зараженных сайтов.

**Источник:** http://www.anti-malware.ru

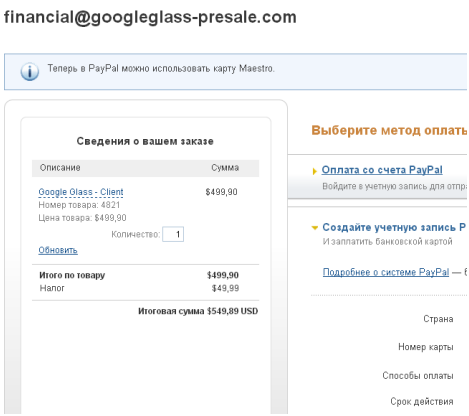
## Мошенники принимают предзаказы на Google Glass.

В интернете уже появились сайты, где вовсю идёт приём предварительных заказов на очки Google Glass. Естественно, эти магазины не имеют никакого отношения к компании Google, а принадлежат мошенникам, хотя дизайн сделан весьма

профессионально.




Очевидно, что спрос на техническую новинку настолько велик, что люди готовы заплатить деньги непонятно кому даже до официальной премьеры гаджета.




Домен googleglass-presale.com зарегистрирован на какого-то парня из Бразилии.

**Источник:** http://www.xakep.ru

## “Советские” хакеры выложили в Сеть личные данные американских политиков.

Спецслужбы США расследуют факт грандиозной утечки информации об американских политиках и знаменитостях. Неизвестные хакеры выложили в Сеть их личные данные.

Неизвестные хакеры создали сайт, на котором выложили личные данные целого ряда высокопоставленных американских политиков и информацию о знаменитостях. В частности, на всеобщее обозрение была выставлена информация о бывшем госсекретаре США Хилари Клинтон (Hillary Clinton) и певице Бритни Спирс (Britney Spears).

Среди других лиц, упомянутых на сайте, фигурируют вице-президент США Джозеф Байден (Joseph Biden), глава Федерального бюро расследований Роберт Мюллер (Robert Mueller), актеры Мел Гибсон (Mel Gibson), Арнольд Шварценеггер (Arnold Schwarzenegger), Эштон Катчер (Ashton Kutcher), певица Бейонсе (Beyonce Knowles) и другие известные люди.

Агенты ФБР уже подтвердили, что знают об инциденте, но пока что не уточнили, будут ли его расследовать. В свою очередь, Секретная Служба США, занимающаяся обеспечением безопасности первых лиц страны уже начала собственное расследование утечки. Параллельно с ними к расследованию приступила полиция Лос-Анджелеса – среди данных, опубликованных на сайте, оказались номер социального страхования и отчет о кредитных операциях одного из руководителей правоохранительных органов города.

Интересно, что сайт находится на домене SU, зарегистрированном еще в 1991 году для Советского Союза, и продолжающего использоваться до сих пор.

**Источник:** http://www.imena.ua

## Trend Micro: бойтесь не китайских хакеров, а русских.

Технический директор антивирусной компании Trend Micro Раймунд Генес говорит, что опасения бизнеса в связи в участившимися атаками, спонсируемыми государствами, в реальности блекнут с масштабами хищений, совершаемых хакерами из России и стран СНГ. По его словам, подавляющему большинству частных пользователей и компаний мало-

го и среднего бизнеса не следует опасаться так называемых "госхакеров", а вот хакеров из России и стран СНГ стоит.

"Когда я вижу большую шумиху вокруг отчетов, наподобие тех, что был недавно опубликован компанией Mandiant, обличающий китайских хакеров, то в большинстве случаев соглашаюсь, что китайцы действительно занимаются корпоративным шпионажем. Но вы думаете, что американцы не занимаются? Или русские?",- говорит Генес. "Лично меня больше тревожит активность русских хакеров. Они занимаются киберпреступностью очень давно, задолго до того, как китайцы сели за компьютеры. Этих опасных ребят частенько нанимают для совершения разных грабежей. Все наши последние данные однозначно говорят о том, что наиболее сложные атаки исходят из России".

Некоторое время назад компания Mandiant опубликовала статистический отчет, в котором говорилось, что несколько сложных APT-атак (Advanced Persistent Thread) ведут в китайскую армию. Отчет вызвал публичный обмен обвинениями между Вашингтоном и Пекином. Генес отметил, что в последнее время все больше специалистов по ИТ-безопасности начинают спекулировать термином APT.

"Я ненавижу термин APT. На прошлой неделе я был в RSA и там все кому не лень твердили о том, что APT повсюду. Тот факт, что подобные атаки вызывают большой интерес, невозможно оспорить, но не следует преувеличивать масштабы подобных атак. Многие коды, изначально созданные для APT-атак, потерпели провал - Stuxnet, Red October и другие, все они были созданы для удара по конкретным целям, но распространились слишком широко и не выполнили своих задач. Код хорош тогда, когда вы его не видите", - полагает он.

CTO Trend Micro говорит, что многие киберпреступники используют модифицированные коды для атак, а их довольно легко детектировать. В то же время, оригинальная платформа вредоноса зачастую создается в "русском подполье", а уже потом растекается по всему миру. Генес говорит, что на сегодня практически все ИТ-специалисты согласны с тем, что от таргетированных атак невозможно полностью защититься. "Если кто-то на протяжении нескольких лет пытается влезть в вашу сеть, рано или поздно он это сделает и неважно будет ли это сделано по электронной почте, через USB-накопитель или как-то еще", - уверен специалист.

Еще одним моментом, вызывающим опасение топ-менеджера антивирусной компании, является растущая доступность очень мощных инфраструктурных решений для все возрастающего числа хакеров.

"Раньше клиенты платили нам за то, чтобы мы защитили их ресурсы от атак. Сейчас - чтобы мы помогли минимизировать ущерб от атак и найти следы атаковавших злоумышленников", - признает Генес.

По его словам, еще одной животрепещущей проблемой для бизнеса является отсутствие единых норм и требований по ИТ-безопасности. Генес говорит, что сейчас Евросоюз движется в этом направлении, но до завершения этого пути еще далеко.

**Источник:** http://www.cybersecurity.ru

## Хакеры получили доступ к серверу Yahoo.

Хакеры опубликовали более 453 000 пользовательских регистрационных данных, похищенных из одного из сервисов компании Yahoo. В сообщении хакеров говорится, что данные были получены в виде открытого текста, что говорит о слабой системе защиты. Дамп данных был размещен на одном из публичных сайтов группой хакеров, именующих себя D33Ds Company.

В данных D33Ds Company говорится, что они получили доступ к одному из поддоменов Yahoo и при помощи методики SQL-инъекции получили расширенный доступ к системе, где хранятся пользовательские данные. Технически, при помощи полученных данных хакеры могли бы использовать бек-энд серверы Yahoo для выдачи большого объема пользовательской информации.

В подтверждении своих слов хакеры опубликовали не только 453 492 аккаунта

Yahoo, но и более 2700 других записей из баз данных, а также 298 MySQL-переменных, которые можно использовать для дальнейшей незаконной работы во взломанной системе.

"Мы надеемся, что лица, ответственные за управление системами безопасности этого домена, примут соответствующие меры. Там есть множество пробелов в системе безопасности, которые можно эксплуатировать в незаконных целях", - говорится в сообщении хакеров.

По неофициальным данным, хакерам удалось получить доступ к Yahoo Voice и серверу на домене dbb1.ac.bf1.yahoo.com

Обновление от 17:00 мск: в пресс-службе компании в Лондоне подтвердили факт компрометации приблизительно полумиллиона аккаунтов пользователей, сообщив, что Yahoo начала расследование по данному факту.

**Источник:** http://www.cybersecurity.ru

## Спуфинг трафика со смартфонов создаёт фальшивые дорожные пробки.

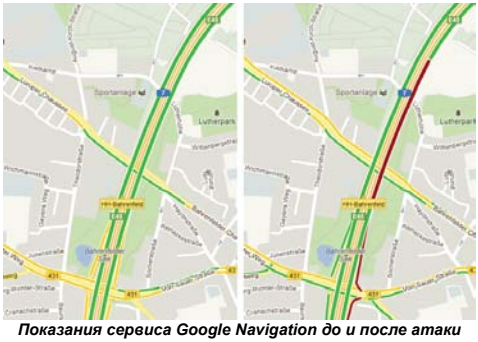
На конференции BlackHat Europe 2013 в Амстердаме выступил немецкий хакер Тобиас Джеске (Tobias Jeske) с очень интересным докладом о спуфинге трафика навигационных сервисов.

В этом докладе интересна сама идея, которая проста и эффективна. По словам Джеске, в наши дни очень многие автолюбители полагаются на информацию о пробках, которую получают из веб-сервисов вроде Google Navigation и Waze. Сюда можно добавить «Яндекс.Пробки», о котором Джеске не знает, но в России этот сервис очень популярен. Если водитель видит на навигаторе, что впереди по дороге пробка, то он выберет альтернативный маршрут.

Информация о пробках собирается со смартфонов самих автолюбителей. Вышеупомянутые Google Navigation и Waze получают информацию о скорости перемещения мобильных телефонов на каждом участке дороге — и делают вывод, на каком участке движение затруднено.

Джеске показал, каким образом можно обмануть навигационный сервис и создать видимость пробки там, где её нет. И наоборот, можно «спрятать» пробку от навигационной системы. Искажение показаний осуществляется просто. Злоумышленник должен записать трафик, который передают смартфоны во время пробки, а впоследствии может заново воспроизвести его, поменяв метки времени и куки. Хакер уже провёл эксперимент и успешно подделал трафик в Google Navigation и Waze.

В случае масштабного применения подобной техники можно парализовать движение во всём городе, говорит Джеске.



*Показания сервиса Google Navigation до и после атаки*

**Источник:** http://www.xakep.ru

## На соревнованиях хакеров в Ванкувере сломали Windows-браузеры.

На конференции CanSecWest, проходящей в качестве конференции по безопасности, прошли соревнования хакеров

В 1-й день уже были сломаны все основные браузеры для системы Windows, кроме того, Java, Adobe Flash и Adobe Reader. Вскрывать браузер Safari в этом году не пытался никто.

За взлом Internet Explorer 10 в 8-й версии Windows и Chrome 25 в Windows 7 выплатили по 100 тыс. дол. За взлом Java причитался приз всего в 20 тыс. дол, так как платформа слабо защищена.

Главный же призовой фонд в размере 3 млн долл., который учредила Google за нахождение дыр в операционке Chrome OS, оказался невостребованным.

Кстати, операционку от Google было так сложно сломать потому, что накануне

конкурса разработчики выпустили патч, который залатал 10 новых дыр. За обнаружение 6 из них ранее были выплачены компенсации от 1 до 2 тыс. дол.

Хакерские соревнования Pwn2Own были придуманы американской компанией Tipping Point. Они проводятся каждый год в рамках конференции по компьютерной безопасности в Ванкувере с 2007 года.

Цель соревнований — взломать популярные приложения за счет уязвимостей. Google собиралась добавить к ним аналогичный конкурс Pwnium, только он должен был касаться операционных систем. Компания даже хотела выступать в качестве спонсора, но потом правила конкурса изменились, и участникам было разрешено не разглашать все аспекты уязвимостей - и компания передумала, пишет newsru.com

**Источник:** http://telegraf.com.ua

## Хакеры взломали билборды, разместив рекламу популярного торрент-трекера.

Двое компьютерных взломщиков разместили на видео-билбордах в сербском Белграде промо торрент-трекера The Pirate Bay. Ролик с описанием взлома был размещен на YouTube.

Инициаторами взлома оказались два сербских студента, которые изучают компьютерные технологии. На видео показано, как они дистанционно входят в систему управления билбордами и размещают на них символ The Pirate Bay, пишет korrespondent.net


Хакеры также добавили к логотипу текст: "Сначала вас не замечают, потом над вами смеются, потом с вами борются. А потом вы побеждаете". Более того, перед этим студенты некоторе время играли в компьютерную игру 1978 года Space Invaders, пользуясь билбордами как дисплеями.

Как подчеркнули студенты, это мероприятие не имело преступных намерений, поскольку они не "ломали" систему защиты билбордов, а лишь использовали открытую уязвимость. Они также отметили, что связались с владельцем рекламных щитов и уведомили его об уязвимости и о способах ее поправить.

Также хакеры отметили, что никоим образом не связаны с группировкой Anonymous. Из их слов вытекает, что акция не имела политического характера и ее первоначальной целью не была реклама торрент-портала The Pirate Bay. Так, студенты стремились привлечь внимание на то, как во всех hitech-системах легкомысленно относятся к вопросам безопасности.

Отметим, что цитата, помещенная взломщиками на экранах, используется поклонниками "ненасильственного сопротивления", которые приписывают ее Махатме Ганди. Тем не менее, свидетельств того, что Ганди действительно так говорил, не сохранилось.

Добавим, что The Pirate Bay - сервис, который размещает торрент-файлы, основанный в Швеции в 2003 году. На всем протяжении своей работы сайт сталкивался с обвинениями в пиратстве и множеством исков от правообладателей.

Ранее сообщалось, что пользователи сети выяснили, что популярный торрент-портал The Pirate Bay не переносил свои серверы в Северную Корею, вопреки заявлениям в официальном блоге.

**Источник:** http://e-news.com.ua

# «Доктор Веб»: анализ вирусной активности в феврале 2013 года

**Вирусная обстановка**

Согласно статистике, собранной с использованием лечащей утилиты Dr.Web CureIt!, наиболее распространенной угрозой в последний месяц зимы как и прежде стали троянцы семейства ***Trojan.Mayachok***, при этом чаще всего на компьютерах пользователей обнаруживалась модификация - ***Trojan.Mayachok.18566***. Не менее часто лечащая утилита фиксировала наличие платных архивов, детектируемых антивирусным ПО Dr.Web как ***Trojan.SMSSend***, при этом абсолютным лидером среди них является ***Trojan.SMSSend.2363***.

Такие архивы злоумышленниками используются по стандартной модели — они обычно маскируются под программу установки какого-либо приложения и требуют после своего запуска отправить платное СМС-сообщение или принуждают пользователя подписаться на ту или иную «услугу». Архив, как правило, не содержит заявленного ПО и, кроме того, нередко содействует распространению других, более опасных вредоносных программ. Также достаточно велико количество заражений троянскими программами:

***BackDoor.IRC.NgrBot.42,***
***Trojan.Click2.47013,***
***Win32.HLLP.Neshta.***

Сведения об угрозах, обнаруженных с использованием лечащей утилиты Dr.Web CureIt! в феврале, представлены в следующей таблице:

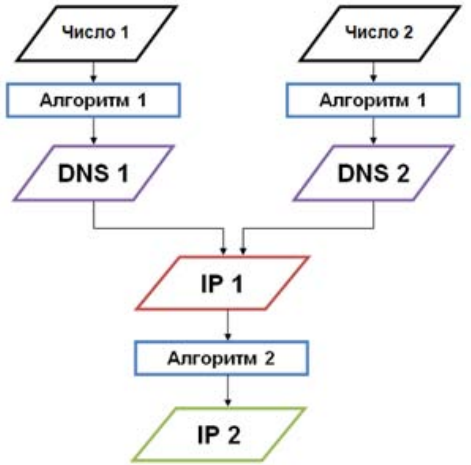
| Угроза | % |
|---|---|
| Trojan.MayachokMEM.4 | 2,00 |
| Trojan.SMSSend.2363 | 1,38 |
| Trojan.Mayachok.18566 | 1,20 |
| BackDoor.IRC.NgrBot.42 | 1,14 |
| Trojan.Click2.47013 | 0,79 |
| Win32.HLLP.Neshta | 0,78 |
| Win32.HLLW.Phorpiex.54 | 0,69 |
| Win32.Sector.22 | 0,65 |
| Trojan.Mayachok.18579 | 0,61 |
| Trojan.Hosts.6814 | 0,59 |
| Trojan.Hosts.6815 | 0,59 |
| Trojan.Hosts.6838 | 0,55 |
| BackDoor.Butirat.245 | 0,54 |
| Trojan.Hosts.6809 | 0,52 |
| Win32.HLLW.Gavir.ini | 0,51 |
| Exploit.CVE2012-1723.13 | 0,51 |
| Trojan.Mayachok.18397 | 0,47 |

**Угроза месяца: Linux.Sshdkit**

Наиболее интересной угрозой, обнаруженной в феврале специалистами компании «Доктор Веб», можно назвать троянскую программу ***Linux.Sshdkit***, заражающую серверы под управлением операционной системы Linux. Троянец представляет собой динамическую библиотеку, при этом существуют ее разновидности как для 32-разрядных, так и для 64-разрядных версий дистрибутивов Linux. После успешной установки в систему троянец встраивается в процесс sshd, перехватывая функции аутентификации. После установки сессии и успешного ввода пользователем логина и пароля они отправляются на принадлежащий злоумышленникам удаленный сервер. IP-адрес управляющего центра «зашит» в теле троянской программы, однако адрес командного сервера каждые два дня генерируется заново. Для этого ***Linux.Sshdkit*** применяет весьма своеобразный механизм выбора имени командного сервера.

***Linux.Sshdkit*** генерирует по специальному алгоритму два DNS-имени, и если оба они ссылаются на один и тот же IP-адрес, то этот адрес преобразуется в другой IP, на который троянец и передает похищенную информацию. Используе-

мый данной вредоносной программой алгоритм генерации адреса командного сервера показан на иллюстрации ниже.



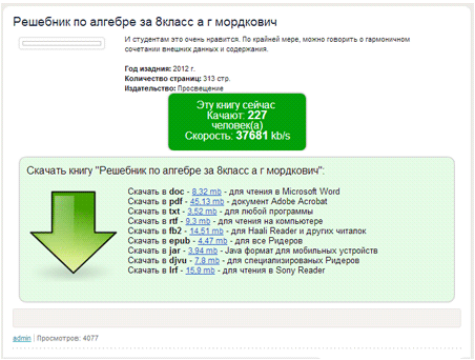

Специалистам компании «Доктор Веб» удалось перехватить несколько управляющих серверов ***Linux.Sshdkit***. На начало марта к перехваченным управляющим центрам обратилось 476 инфицированных серверов, однако многие из них принадлежат хостинг-провайдерам и поддерживают работу значительного числа веб-сайтов, к которым злоумышленники получили доступ. Больше всего инфицированных серверов, а именно 132, находится на территории США, второе место с показателем 37 случаев заражения заняла Украина, на третьем месте расположились Нидерланды. Общие статистические данные, полученные специалистами «Доктор Веб» с использованием перехваченных управляющих центров ***Linux.Sshdkit***, приведены в следующей таблице:

| Страна | Кол-во инфицированых серверов | % |
|---|---|---|
| США | 132 | 27,7 |
| Украина | 37 | 7,8 |
| Нидерланды | 29 | 6,1 |
| Таиланд | 23 | 4,8 |
| Турция | 22 | 4,6 |
| Германия | 19 | 4,0 |
| Индия | 19 | 4,0 |
| Великобритания | 17 | 3,6 |
| Италия | 17 | 3,6 |
| Франция | 15 | 3,2 |
| Индонезия | 12 | 2,5 |
| Австралия | 10 | 2,1 |
| Россия | 10 | 2,1 |
| Канада | 10 | 2,1 |
| Аргентина | 10 | 2,1 |
| Бразилия | 10 | 2,1 |
| Южная Корея | 7 | 1,5 |
| Вьетнам | 7 | 1,5 |
| Чили | 6 | 1,3 |
| Испания | 6 | 1,3 |
| Китай | 5 | 1,1 |
| Румыния | 5 | 1,1 |
| Мексика | 5 | 1,1 |
| Южная Африка | 4 | 0,8 |
| Другие страны | 39 | 7,9 |

**Распространение Trojan.Hosts и взломы веб-сайтов**

В конце февраля — начале марта 2013 года был зафиксирован очередной всплеск атак на веб-сайты с целью распространения вредоносного ПО. Используя украденные данные для доступа к ресурсам по протоколу FTP, злоумышленники подменяли файл .htaccess и внедряли собственный скрипт-обработчик. В результате посетители взломанного веб-сайта подвергались опасности заражения различными троянскими программами. В частности, с использованием этого метода были зафиксированы факты распространения троянцев семейства ***Trojan.Hosts*** — данные вредоносные программы модифицируют один из файлов (%systemroot %/system32/drivers/hosts), в результате чего браузер автоматически перенаправ-

ляет жертву на специально созданную злоумышленниками веб-страницу. Наглядным примером активной деятельности злоумышленников являются сайты, размещающие решенные домашние задания для учащихся средних общеобразовательных учреждений. Попав на такую страницу, пользователь перенаправлялся на зараженный интернет-ресурс, с которого на его компьютер загружался троянец ***Trojan.Hosts*** и другие опасные приложения.




### Угрозы для Android

Февраль 2013 года оказался весьма неспокойным с точки зрения угроз для мобильной платформы Android. Так, в начале февраля вирусные базы Dr.Web пополнились записью для троянца ***Android.Claco.1.origin***, который распространялся в каталоге Google Play под видом утилиты для оптимизации скорости работы операционной системы. Запускаясь на мобильном устройстве, этот троянец мог выполнить отправку СМС-сообщений по команде злоумышленников, открыть произвольный URL в браузере, а также загрузить персональную информацию пользователя (такую как содержимое карты памяти, СМС-сообщения, фотографии и контакты из телефонной книги) на удаленный сервер. Однако главной особенностью ***Android.Claco.1.origin*** являлось то, что с его помощью могли быть инфицированы компьютеры под управлением Windows: подключаясь к удаленному серверу, троянец мог загружать с него другие вредоносные файлы и помещать их на карту памяти мобильного устройства. Среди этих объектов присутствовал исполняемый файл и файл autorun.inf, который осуществлял автоматический запуск соответствующей ему вредоносной программы при подключении инфицированной карты памяти к Windows-компьютеру. Стоит отметить, что, начиная с Windows Vista, функция автозапуска имеет статус отключенной по умолчанию, поэтому для многих пользователей Windows угроза со стороны ***Android.Claco.1.origin*** была незначительной.

Другой заметной вредоносной программой в феврале стал троянец ***Android.Claco.1.origin***, который распространялся злоумышленниками на популярных китайских веб-сайтах в модифицированных ими приложениях. ***Android.Claco.1.origin*** способен выполнять отправку СМС-сообщений в соответствии с принимаемой командой от удаленного сервера, совершать звонки, открывать произвольный URL, загружать на сервер персональную информацию владельца мобильного устройства (например, содержимое телефонной книги, историю звонков, координаты пользователя), а также выполнять некоторые другие функции.

Кроме того, в течение месяца в вирусные базы Dr.Web вносились записи для новых представителей семейства СМС-троянцев ***Android.SmsSend***.

### Другие угрозы февраля

В конце долгой зимы заметно активизировались сетевые мошенники, в частности, промышляющие в поисках жертв на сайтах знакомств. Как правило, мошенники представляются эмигрантами либо иностранцами с русскими корнями — именно этим они объясняют хороший уровень владения русским языком. Завоевав доверие жертвы в процессе переписки, злоумышленник сообщает ей, что намерен отправить своей «избраннице» какой-либо дорогой подарок: электронный планшет, смартфон или ювелирное украшение. Злоумышленники завлекают потенциальных жертв на поддельный сайт курьерской службы, где им предла-

гается оплатить доставку посылки. Естественно, в случае оплаты «курьерская служба», как и сам щедрый поклонник, исчезают в неизвестном направлении. Подробнее об этом способе мошенничества рассказано в нашем информационном материале.

В начале февраля были зафиксированы случаи распространения вредоносных программ с использованием встроенного приложения социальной сети Facebook — этому инциденту посвящена статья, опубликованная на сайте news.drweb.com.

Наконец, в середине месяца специалистами компании «Доктор Веб» был обнаружен забавный троянец-винлок. О том, чем эта вредоносная программа насмешила вирусных аналитиков, можно узнать из нашей публикации.

**Вредоносные файлы, обнаруженные в почтовом трафике в феврале**

| 01.02.2013 00:00 - 28.02.2013 11:00 | | |
|---|---|---|
| 1 | BackDoor.Andromeda.22 | 1.18% |
| 2 | JS.Redirector.185 | 1.12% |
| 3 | Win32.HLLM.MyDoom.54464 | 0.53% |
| 4 | Win32.HLLM.MyDoom.33808 | 0.39% |
| 5 | Trojan.Necurs.97 | 0.39% |
| 6 | Trojan.PWS.Panda.786 | 0.39% |
| 7 | Trojan.DownLoad3.20933 | 0.39% |
| 8 | Trojan.PWS.Stealer.1932 | 0.39% |
| 9 | Trojan.Oficla.zip | 0.37% |
| 10 | Tool.PassView.525 | 0.33% |
| 11 | Trojan.Packed.2820 | 0.31% |
| 12 | SCRIPT.Virus | 0.29% |
| 13 | Trojan.PWS.Panda.655 | 0.29% |
| 14 | BackDoor.Tordev.8 | 0.29% |
| 15 | Win32.HLLM.Beagle | 0.27% |
| 16 | Trojan.Packed.196 | 0.27% |
| 17 | Trojan.PWS.Stealer.2155 | 0.26% |
| 18 | BackDoor.Andromeda.150 | 0.26% |
| 19 | Trojan.KeyLogger.16674 | 0.24% |
| 20 | Win32.HLLM.Graz | 0.24% |

**Вредоносные файлы, обнаруженные в феврале на компьютерах пользователей**

| 01.02.2013 00:00 - 28.02.2013 11:00 | | |
|---|---|---|
| 1 | Trojan.Fraudster.245 | 0.77% |
| 2 | SCRIPT.Virus | 0.70% |
| 3 | Tool.Unwanted.JS.SMSFraud.26 | 0.63% |
| 4 | Adware.Downware.915 | 0.61% |
| 5 | JS.IFrame.387 | 0.52% |
| 6 | Adware.Downware.179 | 0.49% |
| 7 | Tool.Unwanted.JS.SMSFraud.10 | 0.42% |
| 8 | Trojan.Fraudster.394 | 0.36% |
| 9 | Adware.Webalta.11 | 0.36% |
| 10 | Tool.Skymonk.11 | 0.33% |
| 11 | Trojan.Fraudster.407 | 0.32% |
| 12 | Win32.HLLW.Shadow | 0.31% |
| 13 | Tool.Skymonk.12 | 0.30% |
| 14 | JS.Redirector.175 | 0.30% |
| 15 | Adware.Downware.910 | 0.29% |
| 16 | Adware.InstallCore.53 | 0.29% |
| 17 | Win32.HLLW.Autoruner1.33556 | 0.29% |
| 18 | Adware.Downware.774 | 0.29% |
| 19 | Win32.HLLW.Autoruner.59834 | 0.29% |
| 20 | JS.Redirector.179 | 0.27% |

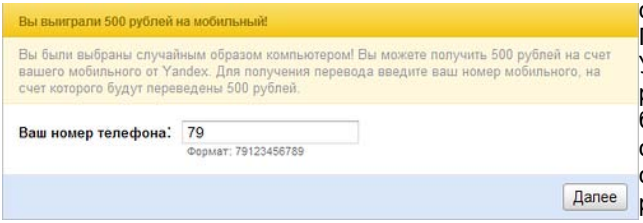
**Источник:** http://news.drweb.com

## Google, Mail.Ru, Яндекс и ВКонтакте предупредили о мошенничестве в сети.

Компании Google, Group-IB, Mail.Ru Group, ВКонтакте, «Доктор Веб», «Лаборатория Касперского» и «Яндекс» опубликовали совместное заявление о распространении нового типа мошенничества.

В последнее время пользователи интернета все чаще сталкиваются с объявлениями, в которых их просят ввести номер мобильного и потом — код активации из SMS. Чтобы выманить у человека но-

мер, злоумышленники используют самые разные объявления: «Вы выиграли приз», «Ваш аккаунт заблокирован». Такие сообщения часто размещают на страницах, которые выглядят, как популярные ресурсы (Яндекс, Одноклассники, ВКонтакте и т.д.). Если пользователь вводит номер мобильного телефона и код подтверждения, он, не сознавая того, подключает платную SMS-подписку, за которую с его счета каждый день списывают деньги.




***Сообщение мошенников***

Компании официально напомнили, что не имеют отношения к объявлениям такого рода. Это уловка злоумышленников, которые пытаются заработать на доверчивости пользователей.

Кроме того, Google, Group-IB, Mail.Ru Group, ВКонтакте, «Доктор Веб», «Лаборатория Касперского» и «Яндекс» объединили усилия, чтобы обезопасить пользователей от нового вида мошенничества. Они передают друг другу данные об обнаруженных угрозах, чтобы антивирусные компании могли оперативно блокировать мошеннические веб-страницы, а интернет-компании – предупреждать пользователей об опасности при попытке перехода на такие ресурсы. Операторам сотовой связи передаются данные о коротких номерах, на которые злоумышленники обманом подписывают пользователей.

**Источник:** http://protv.ua

## В Одессе милиция задержала иностранца, который похищал деньги из банкоматов.

В Одессе милиция задержала иностранного гражданина, который похищал деньги через электронные устройства по считыванию данных с банковских карточек.

Как сообщили УНИАН в отделе по связям с общественностью Главного управления МВД Украины в Одесской области, работники управления по борьбе с киберпреступностью ГУМВД Украины в Одесской области получили оперативную информацию с установленного на банкомате одного из ведущих банков Украины электронного устройства для видеофиксации ввода ПИН-кода и считывания персональной информации с магнитной полосы банковской карты клиента.

С поличным был задержан 26-летний иностранец - житель одного из государств Евросоюза, у которого изъяты самодельные устройства для считывания информации с платежных карт.

По месту его временного проживания выявлены и изъяты самодельные устройства для считывания информации клиентов банков, компьютерная техника, заготовки под банковские карты, микросхемы, USB-провода, паяльник и множество деталей для изготовления так называемых накладок, для получения информации о настоящих банковских карточках.

По данному факту следственным отделом Приморского районного отдела милиции ОГУ ГУМВД Украины в Одесской области открыто уголовное производство по ст.200 «Незаконные действия с документами и перевод, платежными карточками и другими средствами доступа к банковским счетам, оборудованием для их изготовления» и по ч.1 ст.361 УК Украины «Несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), систем и

компьютерных сетей».

Как сообщал УНИАН, в феврале в Одессе был задержан 38-летний иностранец, который при помощи считывающих устройств снимал деньги с чужих банковских счетов.

**Источник:** http://vchaspik.ua

## Взлом TLS и SSL через уязвимость в шифре RC4

На этой неделе в Сингапуре прошла криптографическая конференция Fast Software Encryption. Главным событием стало выступление Дэна Бернстейна (Dan Bernstein), профессора университета Иллинойса, который представил новую технику для вскрытия протоколов Transport Layer Security (TLS) и Secure Sockets Layer (SSL), если в них используется шифр RC4.

Шифр RC4, созданный в 1987 году, до сих пор широко используется и считается одним из самых популярных и рекомендуемых шифров. Слабости RC4 давно и хорошо известны, но до практических реализаций атаки на TLS дело пока что не доходило, хотя AES и Triple DES уже скомпрометированы в атаках BEAST и Lucky 13. Теперь дошло дело до RC4, впервые опубликован реальный и доступный способ такой атаки.

RC4 (Rivest Cipher 4) — популярный потоковый шифр, созданный легендарным криптографом Роном Ривестом (Ron Rivest), широко применяется в SSL, TLS и алгоритме безопасности беспроводных сетей WEP. Алгоритм RC4, как и любой потоковый шифр, строится на основе параметризованного ключом генератора псевдослучайных битов с равномерным распределением. Длина ключа может составлять от 40 до 256 бит. Основные преимущества шифра — высокая скорость работы и переменный размер ключа.

Уязвимость RC4 связана с недостаточной случайностью потока битов, которым скремблируется сообщение. Прогоняя через него одно сообщение много раз, удалось выявить достаточное количество повторяющихся паттернов для восстановления исходного сообщения.

Для атаки нужно прогнать через шифр гигантский объём данных. В текущей реализации взлом TLS занимает до 32 часов, но злоумышленник может использовать различные способы для оптимизации процесса. Например, это может быть баннер на сайте с большой посещаемостью или фрагмент кода, который добавляют каждому пользователю на уровне маршрутизатора.

**Источник:** http://www.xakep.ru

## ENISA призывает Европу уделить больше внимания борьбе с кибератаками

Европейское агентство по сетевой и информационной безопасности (ENISA) опубликовало доклад под названием: “Кибератаки – новая грань старых вооружений”, в котором рассматриваются последние целевые (направленные) кибератаки против различных организаций Европы.В докладе содержится детальный анализ крупных кампаний, например, Красный Октябрь (Red October) и MiniDuke. И раскрываются некоторые общие методы проведения кибератак, используемые хакерами; целевая рассылка вредоносных электронных писем (направленный фишинг) и использование уязвимостей, содержащихся в программном обеспечении.

Кроме того, в рамках доклада, ENISA даёт организациям общие рекомендации, в частности, принять меры, позволяющие минимизировать количество успешных кибератак и/или их последствия; обеспечить безопасность электронной почты; выявлять и своевременно устранять уязвимости в программном обеспечении.

Эксперты ENISA заявляют, что на сегодняшний день следует уделять особое внимание именно разработке и внедрению мер, и технологий, позволяющих предотвращать кибератаки.

**Источник:** http://www.anti-malware.ru

## Новый Android-вредонос Perkele перехватывает короткие сообщения.

Обнаружена новая вирусная программа, перехватывающая входящие sms-сообщения при пользовании мобильными устройствами под управлением ОС Android. Независимый эксперт по компьютерной безопасности Брайен Кребс нашел на одном из интернет-форумов выставленную на продажу программу, пересылающую тексты входящих sms организаторам вирусной атаки, «сливая» конфиденциальную информацию пользователя – например, данные для интернет-банкинга.

Часть банковских учреждений во многих странах используют двухуровневую аутентификацию – клиенту для подтверждения платежа нужно вводить не только пароль, но еще и особый sms-код.

Вирус Perkele (название программы переводится как финское нецензурное ругательство) действует совместно с другой вредоносной программой, которая устанавливает вирус и подменяет инструкции на платежной веб-странице – в результате пользователя просят установить на телефон «специальную защищенную программу для Android», под видом которой и скрывается Perkele.

Анализируя данные за прошлый год, эксперты по антивирусной безопасности сходятся во мнении: лидером по количеству атак остаётся ОС Android. Учитывая возможности мобильных Android-устройств и увеличение числа их пользователей, многие специалисты прогнозируют дальнейший рост популярности данной ОС у киберпреступников.

Финский антивирусный вендор F-Secure на днях опубликовал отчет, согласно которому в 2012 году открытая операционная система Android показала стремительный рост не только по популярности, но и по количеству выпускаемого вредоносного ПО. В 2012 году Android стала целью для 79% выпускаемого вредоносного программного обеспечения. Годом ранее этот показатель составлял 65%.

Только в четвертом квартале на долю Android пришлось 96 абсолютно новых вирусных семейств, а с учетом вариантов вредоносных кодов, количество новых угроз идет на сотни. F-Secure отмечает, что в последнем квартале 2012 года самыми популярными Android-вредоносами стали разнообразные коды, выполняющие те или иные операции с SMS-сообщениями и премиальными SMS-номерами. Из 96 новых семейств 21 было ориентировано на тайную отправку коротких сообщений на короткие номера.

Также набирают популярность среди вирусописателей и сравнительно новые SMS-вредоносы, которые сами создают короткие сообщения и используют методы социальной инженерии, чтобы ввести пользователей в заблуждение и тем или иным способом вынудить его совершить платеж на счет мошенников. Также достаточно популярными являются вредоносные коды, ворующие мобильные банковские реквизиты и передающие их в фоновом режиме мошенникам.

Чтобы как-то снизить опасность, F-Secure рекомендует пользователям регулярно обновлять свои Android-устройства, а также регулярно обновлять антивирусное ПО и сканировать систему на предмет наличия вредоносных кодов в смартфоне.

**Источник:** http://cybersecurity.ru

## Появился новый вирус для MAC, который обходит защиту GATEKEEPER.

Новый вирус уже успел заразить компьютеры сотрудников Apple, Facebook, Twitter, а также ряда других, в том числе и правительственных, американских организаций.

Хотим вам сообщить об обнаружении нового вредоносного программного обеспечения, ориентированного на Mac. Новый вирус уже успел заразить компьютеры сотрудников Apple, Facebook, Twitter, а также ряда других, в том числе и правительственных, американских организаций.

Назвали этот вирус Pintsized.A. Он

представляет собой новый класс компьютерных угроз, использующих ранее неизвестную уязвимость во встроенном в Mac OS X средстве безопасности Gatekeeper.

Новый вирус успешно маскируется под программное обеспечение CUPS, применяемое в Linux и Mac для управления печатью документов. При этом, внимательный Mac-пользователь может обратить внимание, что псевдо-CUPS пытается установиться в папку, которая не имеет никакого отношения к легитимному CUPS.

Pintsized.A открывает сетевой канал для общения с удаленным командным сервером, контролируемым злоумышленниками. Для введения в заблуждение троян использует модифицированную версию утилиты OpenSSH, причем сам шифрует свои данные при помощи SSH, что усложняет его обнаружение.

Известно, что сейчас большая часть копий Pintsized.A обращается к серверу по адресу corp-aapl.com. В Intego говорят, что сетевые инженеры Facebook выявили подозрительный трафик в отношении данного ресурса со стороны внутренней сети компании. Похожая ситуация была в Twitter и Apple.

**Источник:** http://newstech.in.ua

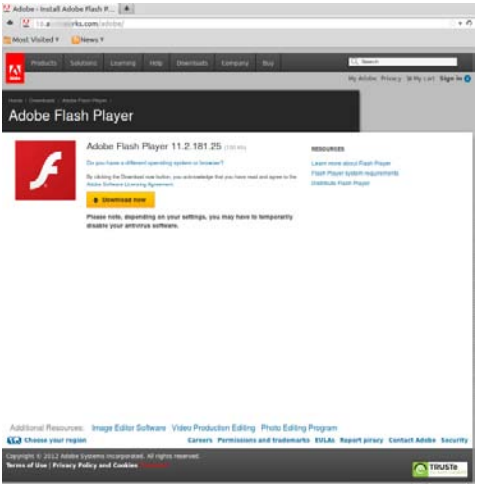
## Хакеры создали фальшивую страницу обновления Adobe Flash.

Злоумышленникам удалось создать достаточно правдоподобную копию официального сайта обновления Adobe Flash. Основная цель – добиться установки вредоносной программы.

В интернете зафиксирована новая вредоносная кампания, использующая для обмана пользователей поддельные сайты обновления Adobe Flash. Их компьютеры заражаются вредоносной программой-вымогателем и программой-автокликом, которая ходит по рекламным ссылкам от имени пользователя, сообщает антивирусная компания Symantec.

Широкое распространение среди пользователей и достаточно частая необходимость обновления Adobe Flash сделали этот продукт объектом повышенного внимания кибер-преступников. Применяя методы социальной инженерии, злоумышленники заманивают пользователей на поддельные страницы обновления Adobe Flash, с которых вместо очередного обновления ни о чем не подозревающий пользователь устанавливает на свой компьютер вредоносную программу.

В качестве одного из ярких примеров специалисты антивирусной компании указывают сайт, выдающий себя за страницу обновления Adobe Flash Player: http://16.a[REMOVED]rks.com/adobe/.




*Поддельная страница обновления Adobe Flash*

Злоумышленникам удалось создать достаточно правдоподобную копию официального сайта, однако все же был допущен ряд недочетов: большая часть ссылок ведет назад на атакующий домен, и абсолютно все ссылки на странице – кроме ссылки на само вредоносное содержимое – к корневому каталогу сайта, что приводит к ошибке 404 (страница не найдена).

Основная цель злоумышленников – добиться установки вредоносной программы, и для увеличения шансов они предлагают на выбор пользователю два варианта. Первый вариант представляет собой всплывающее окно, предлагающее пользователю скачать файл под названием "flash_player_updater.exe". Вторая опция – кнопка "Download Now", после нажатия на которую начинает скачиваться файл "update_flash_player.exe". Оба файла идентифицируются Downloader.Ponik.

Выяснилось, что помимо кражи паролей эти вредоносные программы выискивают в системе учетные записи удаленного доступа по FTP/telnet/SSH, а также отслеживают учетные записи почты по протоколам SMTP, IMAP и POP3.

**Источник:** http://zn.ua

## Исламисты вывели из строя сайт банка JP Morgan Chase.

Хакерская атака палестинской группировки «Изз ад-Дин аль-Кассам» на несколько часов вывела из строя сайт банка JP Morgan Chase.

Сайт был недоступен в течение полутора часов с двух часов ночи по московскому времени. Все это время пользователям выводилось сообщение «Наш сайт временно недоступен, но наши мобильные приложения работают». Работа ресурса была восстановлена, однако вплоть до утра по московскому времени сайт работал с перебоями.

По данным американского телеканала NBC, ответственность за взлом взяла группа хакеров «Изз ад-Дин аль-Кассам». Атака стала ответом на отказ властей США и компании Google удалять ролик «Невинность мусульман» с видеохостинга YouTube.

Бригада «Изз ад-Дин аль-Кассам» является военным крылом палестинского террористического движения ХАМАС. В сентябре 2012 года хакерская группа этой бригады запустила «операцию Ababиль», во время которой атаковала сайты крупнейших банков США и сайт нью-йоркской фондовой биржы. Причиной атаки хакеры также называли оскорбление, нанесенное им фильмом «Невинность мусульман».

В январе 2013 года хакеры начали вторую волну атак. Их особенностью стало то, что запросы, парализующие работу сайтов, исходили не с персональных компьютеров, а с зараженных веб-сайтов. На всех этих сайтах использовалась система управления содержимым Joomla, уязвимостью в которой и воспользовались хакеры.

Эксперты отмечали высокий технический уровень атак. Как считают некоторые специалисты, за атаками может стоять Иран, и, по сообщениям источников, того же мнения придерживается правительство США. В то же время хакеры «Изз ад-Дин аль-Кассам» отвергли обвинения в том, что за атаками стоит какое-либо государство.

**Источник:** http://lenta.ru

## Троянец-шифровальщик атаковал Испанию и Францию.

Trojan.ArchiveLock. Модификация этой вредоносной программы, получившая название Trojan.ArchiveLock.20, заражает всё большее количество компьютеров во Франции и Испании.

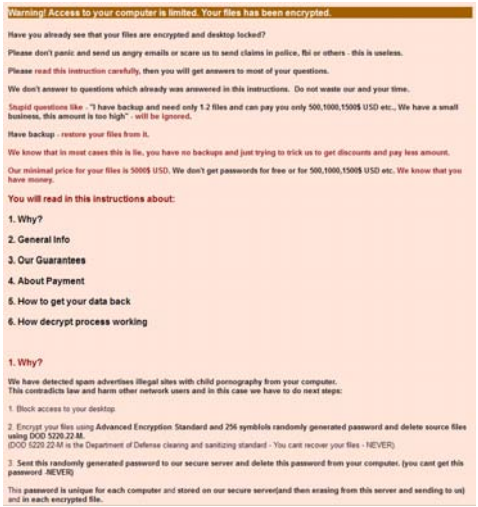
В августе прошлого года компания «Доктор Веб» сообщала о троянце-шифровальщике Trojan.ArchiveLock. Эта вредоносная программа использует для шифрования файлов стандартный архиватор WinRAR. В целях распространения угрозы злоумышленники применяют метод перебора паролей для доступа к компьютеру жертвы по протоколу RDP. Подключившись к атакуемой рабочей станции, киберпреступники запускают на ней троянца. Получив управление, Trojan.ArchiveLock.20 размещает в одной из системных папок приложение-шифровальщик.

Затем Trojan.ArchiveLock.20 создает список подлежащих шифрованию файлов, после чего очищает Корзину и удаляет хранящиеся на компьютере резервные копии данных. С использованием консольного приложения WinRAR шифровальщик помещает пользовательские файлы по заранее составленному списку в защищенные паролем самораспаковывающиеся архивы, а исходные данные уничтожает с помощью специальной утилиты – восстановление удаленных файлов после этого становится просто невозможным.

Пароль, которым защищаются архивы, может иметь длину более 50

символов. Затем Trojan.ArchiveLock.20 демонстрирует на экране инфицированного компьютера сообщение с требованием заплатить 5000 USD за пароль, необходимый для извлечения файлов из архива, предлагая обращаться за «технической поддержкой» по одному из следующих адресов электронной почты:

- sec777999@gmail.com,
- sec222555@gmail.com,
- sec333888@gmail.com,
- sec333888@gmail.com,
- ausec222999@gmail.com,
- sec777999@gmail.com,
- casec222777@gmail.com,
- auidhelp@gmail.com,
- sec777999@gmail.com,
- sec222555@gmail.com,
- sec333888@gmail.com,
- ausec222999@gmail.com,
- casec222777@gmail.com,
- auidhelp@gmail.com,
- usidhelp2@gmail.com,
- frsechelp@gmail.com,
- spainsec1@gmail.com,
- spainsec2@gmail.com.


Warning! Access to your computer is limited. Your files has been encrypted.

Have you already see that your files are encrypted and desktop locked?

Please don't panic and send us angry emails or scare us to send claims in police, fbi or others - this is useless.

Please read this instruction carefully, then you will get answers to most of your questions.

We don't answer to questions which already was answered in this instructions. Do not waste our and your time.

Stupid questions like - "I have backup and need only 1-2 files and can pay you only 500,1000,1500$ USD etc., We have a small business, this amount is too high" - will be ignored.

Have backup - restore your files from it.

We know that in most cases this is lie, you have no backups and just trying to trick us to get discounts and pay less amount.

Our minimal price for your files is 5000$ USD. We don't get passwords for free or for 500,1000,1500$ USD etc. We know that you have money.

You will read in this instructions about:

1. Why?

2. General Info

3. Our Guarantees

4. About Payment

5. How to get your data back

6. How decrypt process working

1. Why?

We have detected spam advertises illegal sites with child pornography from your computer.
This contradicts law and harm other network users and in this case we have to do next steps:

1. Block access to your desktop.

2. Encrypt your files using Advanced Encryption Standard and 256 symbols randomly generated password and delete source files using DOD 5220.22-M.
(DOD 5220.22-M is the Department of Defense clearing and sanitizing standard - You cant recover your files - NEVER)

3. Sent this randomly generated password to our secure server and delete this password from your computer. (you cant get this password -NEVER)

This password is unique for each computer and stored on our secure server(and then erasing from this server and sending to us) and in each encrypted file.

В настоящее время от действия троянца пострадало значительное количество пользователей в Испании и Франции: только за истекшие 48 часов в службу технической поддержки «Доктор Веб» обратились десятки жертв Trojan.ArchiveLock.20, и подобные запросы продолжают поступать. Несмотря на то, что в демонстрируемом на экране инфицированного компьютера сообщении злоумышленники говорят о невозможности подобрать пароль к архивам, из-за особенностей применяемого хеширования sha1 во многих случаях расшифровка и восстановление файлов возможны, о чем компания «Доктор Веб» сообщала еще в августе 2012 года.

Пострадавшим от Trojan.ArchiveLock.20 пользователям специалисты «Доктор Веб» рекомендуют ни в коем случае не удалять никакие файлы с жесткого диска инфицированного компьютера и не переустанавливать операционную систему. Для расшифровки заархивированных троянцем файлов можно обратиться в компанию «Доктор Веб», создав тикет в категории «Запрос на лечение». Данная услуга предоставляется бесплатно.

**Источник:** http://news.drweb.com

## Украденный телефон выложил в сеть фото своего похитителя.

Высокие технологии встали на пути мелкого преступника. Незадачливого воришку мобильного телефона удалось найти и арестовать после того, как украденный им телефон выложил в Интернет фотографию своего похитителя.

Буквально на днях жительница Нью-Йорка, чье имя не разглашается в интересах следствия, стала жертвой воришки, который похитил ее мобильный телефон. Однако похититель был задержан уже на следующий день, сообщает cellular-news.

Как выяснилось, смартфон был настроен таким образом, что автоматически публиковал все отснятые фотографии в социальную сеть Facebook, на страницу настоящей владелицы телефона. Похититель не стал проверять настройки, и несколько раз сфотографировал себя – при этом на одной из фотографии он запечатлен курящим марихуану.

Пострадавшая немедленно предоставила фотографию вора полиции, которые быстро установили его личность, и задержали недоумевающего преступника прямо в собственной квартире. Любопытно, что против незадачливого преступника выдвинуто несколько обвинений – в краже чужой собственности и в незаконном хранении и употреблении наркотических веществ, что серьезно повлияет на срок тюремного заключения.

**Источник:** http://www.imena.ua

## Новая угроза – хакеры шпионят за девушками через web-камеры.

Новый подвид хакеров – так называемые RAT'еры – стали настоящим бичом американских девушек. Молодые дарования развлекаются тем, что шпионят за прекрасной половиной человечества через web-камеры.

RAT'еры – хакеры, которые подглядывают за девушками посредством инструментов Remote Administration Tools (RAT) стали новой большой проблемой для интернет-пользовательниц США. Способ подглядывания, созданный для развлечения уже стал популярным у более серьезных людей, нежели малолетние «подглядыватели» и активно приобретает популярность у людей, занимающихся промышленным шпионажем и разведкой.

На многочисленных подпольных форумах хакеры активно распространяют ссылки на программное обеспечения для «развлекательного шпионажа», и охотно делятся опытом. Особой популярностью пользуются программы DarkComet или Mighty Mouse – причем в последней есть даже специальное меню для подобных «шуток». В подтверждение своего успеха каждый участник форума публикует фотографии и видеоролики, иллюстрирующие то, что он умудрился сотворить с компьютером жертвы.

Помимо обычного шпионажа, RAT'еры любят «прикалываться» над пользователем, скрывая кнопку пуск или индикатор часов в Windows, открывая и закрывая крышку DVD-привода и размещая на рабочем столе пользователя сообщения от якобы одержимого бесами компьютера.

Принимая во внимание, что для осуществления подобной «шутки» требуются минимальные технические навыки, большого вреда RAT'еры нанести не могут. Тем не менее, предостерегаем читателей от скачивания подозрительных программ, и тщательной фильтрации людей, которым вы даете доступ к своему компьютеру.

**Источник:** http://www.imena.ua

## Киберпреступники заводят в соцсетях странички от имени известных брендов.

До Украины добралось новое мошенничество – аферисты создают в социальных сетях фальшивые страницы именитых компаний, предлагая всем, кто отметит ее кнопкой «like» дорогие подарки. Таким образом, мошенники недобросовестно увеличивают количество подпис-

чиков.

Суть мошенничества заключается в следующем – в популярной социальной сети, типа Facebook заводят страницу известного бренда или компании. На ней размещается «официальное уведомление» о «конкурсе». Каждый человек, который подпишется на страницу и поставит ей «like» получает шанс выиграть дорогостоящие товары от указанного бренда, сообщает Waffles At Noon. В частности, разыгрываются дорогие наушники от Beats Electronics и iPad Mini от Apple. Само время розыгрыша призов отстоит от текущей даты примерно на месяц.

Чтобы избежать подозрений пользователей в том, что бренды предлагают слишком уж дорогие подарки, мошенники уточняют, что все разыгрываемые наушники не могут быть проданы из-за нарушения целостности упаковки.

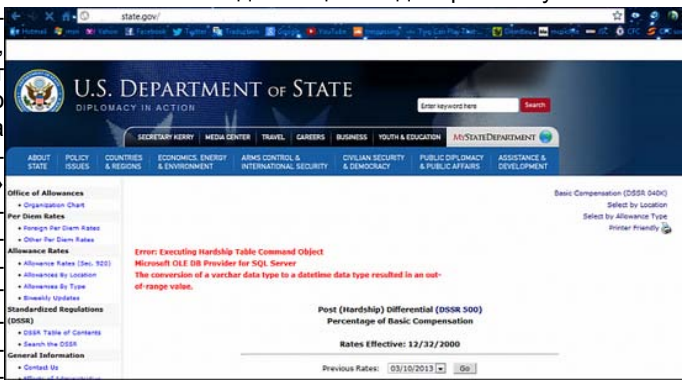
Представители вышеупомянутых компаний уже обратились с официальным запросом к руководству соцсети Facebook с сообщением о том, что они не проводят никаких конкурсов и розыгрышей. Кроме того, корпорации уже разослали соответствующие уведомления другим крупнейшим социальным сетям.

Эксперты уже высказали предположение, что данные страницы являются частью какой-то крупной мошеннической схемы по недобросовестному увеличению подписчиков на странице. Возможно, после набора подписчиков страница будет продана и переименована.

**Источник:** http://www.imena.ua

## Tunisian Cyber Army взломала сайты Пентагона и Госдепартамента США.

Tunisian Cyber Army совместно с активистами Al Qaida Electronic Army начала операцию OpBlackSummer. По данным компании illSecure, активисты Tunisian Cyber Army выявили и использовали уязвимости, позволяющие осуществить внедрение SQL–кода на двух доменах, принадлежащих Госдепартаменту США.




По словам хакеров, им удалось получить доступ к конфиденциальной информации, а также IP-адресам правительственных компьютеров и серверов. Кроме того, члены Tunisian Cyber Army выявили и, по некоторым данным, использовали XSS-уязвимость на одном из сайтов Пентагона, принадлежащем Национальной Гвардии сухопутных войск.

По информации HackRead, хакеры планируют использовать выявленные уязвимости в ходе операции «Черное лето» (OpBlackSummer). Данную операцию Tunisian Cyber Army планирует провести совместно с китайскими хакерами. Следует отметить, что это далеко не первый случай, когда хакеры выявляют и используют уязвимости в системах защиты сайтов Госдепартамента США. Известно, что в феврале текущего года, в рамках операции OpLastResort, активисты хакерской группировки Anonymous выкрали учетные данные сотен пользователей из баз данных сайта state.gov.

**Источник:** http://www.anti-malware.ru

## Хакерские группировки готовят совместный удар по Израилю.

Активисты нескольких хакерских группировок объявили о начале совместной операции, направленной против израильских сайтов. По имеющейся информации, в рамках данной операции член хакерской группировки Muslim Liberation Army, известный под ником Hitcher, взломал и

обезобразил 54 израильских сайта.По данным HackRead, таким образом хакер выразил протест против «незаконной оккупации палестинских территорий». На взломанных сайтах Hitcher разместил текст следующего содержания: «Мы разгневаны нынешним положением палестинского народа и фактом незаконной оккупации сионистами палестинских территорий. Данная атака - наш ответ на беззакония, творимые Израилем в отношении палестинского народа.

Muslim Liberation Army далеко не еденственная хакерская группировка, целью которой становятся сайты, принадлежащие израильтянам. По информации The Hackers Post, 7 апреля текущего года сразу несколько хакерских группировок начнут крупную совместную антиизраильскую операцию. Известно, что кроме Muslim Liberation Army в операции примут участие активисты хакерских группировок AnonGhost, Mauritania HaCker Team, Ajax Team, the Muslim Liberation Army, Moroccan Hackerz, Gaza Hacker Team, Gaza Security Team, Anonymous Syria, ZHC, The Hacker Army, X-BLACKERZ INC, Devil Zone Team, Moroccan Hackers и Algerian Hackers.

По словам хакеров, таким образом они хотят заявить о своей солидарности с народом Палестины.

**Источник:** http://www.anti-malware.ru

## Большинство преступлений в Нью-Йорке совершается с привлечением хакеров

Согласно статистическим данным, представленным на симпозиуме в Pace Universityокружным прокурором Манхеттена Сайрусом Венсом (Cyrus Vance), на сегодняшний день большая часть преступлений в Нью-Йорке совершается с привлечением хакеров и/или при помощи компьютерных технологий. По словам Венса, большая часть уголовных дел, расследуемых на данный момент полицией Манхеттена, открываются по факту кражи личных данных и других противоправных действий, совершаемых киберпреступниками. Сайрус Венс отметил, что на сегодняшний день практически все преступления в финансовой сфере и даже убийства совершаются при помощи компьютерных технологий.

Помимо высокопрофессиональных хакеров из стран бывшего СССР, важность и перспективность освоения и использования кибертехнологий начинают понимать и представители организованной преступности США. В свою очередь, президент Pace University Стивен Фридман **(**Stephen Friedman) заявил, что успех в борьбе с подобного рода преступлениями можно обеспечить лишь наладив тесное сотрудничество в данной сфере между бизнес-структурами и государством.

**Источник:** http://www.anti-malware.ru

## Открылся сервис VPN-взаимопомощи

Выпускник японского вуза Дайу Нобори (Daiyuu Nobori) в качестве дипломной работы сделал сервис VPN Gate, где можно предоставить свой компьютер для помощи нуждающимся в защищённом соединении или просто воспользоваться бесплатным VPN. Как говорит автор, целью проекта было помочь пользователям в странах, где действует государственная цензура интернет-трафика.

Сложно сказать, в чём преимущество VPN Gate перед Tor. Этот сервис может быть удобнее и быстрее, если здесь больше рилеев и софт проще установить. Правда, в VPN Gate список рилеев тоже находится в открытом доступе. В любом случае, VPN Gate вполне имеет право на существование как альтернатива Tor.

VPN Gate так же бесплатен и открыт для всех желающих, как и Tor. С момента запуска в пятницу всего за пять дней сервисом воспользовались 77 тыс. пользователей, сгенерировав около четырёх терабайт трафика, так что спрос на бесплатные VPN явно присутствует.

Каждый пользователь может предоставить свой компьютер или компьютер своей компании для передачи чужого трафика. Для этого нужно установить open source программу SoftEther VPN Server, а затем активировать настройки VPN Gate Setting.

**Источник:** http://www.xakep.ru

**Аналитика, обзоры, рекомендации.**

# user And LINUX

# { Secure Shell }




{
Адрес журнала в интернете:
http://ualinux.com/index.php/journal

Обсуждение журнала на форуме:
http://ualinux.com/index.php/forum
}

{
Адрес редакции:

Украина, 03040, г.Киев, а/я 56
email: journal@ualinux.com
}

Тип издания: электронный/печатный
Тираж: *более 15 000 копий.

*указано суммарное количество прошлого выпуска журнала с первичных источников, а также загрузок с других известных ftp, http и torrent серверов.