ЦРУ США берёт под контроль социальные сети

*В ЦРУ существует спецподразделение, неофициально называющее себя **"библиотечные ниндзя",** которое занимается мониторингом записей в социальных сетях по всему миру. Об этом сообщило агентство **Associated Press,** чьи корреспонденты побывали в секретном технопарке **ЦРУ**.*

*По данным агентства, аналитики подразделения просматривают в день до 5 млн одних только записей в **Twitter**. Кроме того они отслеживают посты в **Facebook** и других соцсетеях, а также анализируют информацию из местных телеканалов, радиостанций, газет и локальных интернет-форумов.*

ЦРУ США о РОССИИ

https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html

*Вся информация в виде отчетов затем в ежедневном режиме докладывается президенту США Бараку Обаме на внутренних брифингах в Белом доме. При этом **"библиотечные ниндзя"** фокусируются на информации из зарубежных источников, они подчеркивают, что не мониторят американские соцсети.*

*Впервые, по данным **Associated Press**, подобные группы специалистов появились в ЦРУ после теракта 11 сентября. Тогда власти говорили, что они необходимы для борьбы с терроризмом. Однако с тех пор они заметно расширили свою деятельность.*

*Всего в **"Центре открытых источников"** (это официальное название подразделения) работает несколько сотен сотрудников.*

*Самые ценные из них, по словам директора подразделения, это **"эксцентричные дерзкие хакеры, которые знают, как найти информацию, о существовании которой другие даже не догадываются".***

Глава центра сравнивает их с главной героиней криминального романа "Девушка с татуировкой дракона".

*Среди **"библиотечных ниндзя"** много лингвистов, чьи знания необходимыдля отслеживания активности в соцсетях России, Китая, Пакистана, Ирана, Ирака,Турции и других стран.*

Тактика и методы"библиотечных ниндзя".Защита домашних сетей. Смотри в разделе НАТО-ПРО.

The World Factbook Is Changing

With unrest sweeping the Middle East and economic problems in Europe, The World Factbook is trying to help readers identify the factors that may underlie these social, political, and economic changes. Accordingly, the Factbook is adding new categories of societal data, which—along with other demographic and economic entries—offer additional insight into a country's economic strength, internal stability, and impact on the environment….

Posted: Nov 18, 2011 03:12 PM
Last Updated: Nov 18, 2011 03:12 PM

Last Reviewed: Nov 18, 2011 03:12 PM

Anonymous взломали сайт "теневого ЦРУ"

*Хакеры **Anonymous** своеобразно отпраздновали Рождество: они взломали сайт компании **Stratfor**, которая занимается сбором и анализом информации о событиях в мире. Клиентами компании являются, в том*

*числе, **армия США и инвестиционный банк Goldman Sachs**. **Stratfor** также называют "теневым ЦРУ".*

О взломе серверов Stratfor хакеры объявили в своем Twitter'е. По их словам, им удалось похитить около 200 гигабайт информации, в том числе переписку сотрудников компании с ее клиентами и личные данные последних, в том числе номера банковских карт. Anonymous заявили, что в этом виноваты программисты Stratfor, которые не потрудились зашифровать личные данные клиентов.

*"#LulzXmas только начинается. Оставайтесь с нами, ребята!!! Веселье гарантировано, в противном случае мы вернем вам ваши деньги"**,** - пообещали хакеры.*

*В настоящее время **сайт Stratfor** не работает. "На сайте проходят технические работы", - сказано на его главной странице. В интервью **http://www.ap.org/ The Associated Press** , в компании подтвердили, что ее сервера были взломаны. Там добавили, что они сотрудничают с правоохранительными органами, которые пытаются найти исполнителей кибератаки.*

Одним из пострадавших клиентов "теневого ЦРУ" оказался сотрудник американского Управления внутренней безопасности. Все его личные данные были опубликованы в Интернете и он лишился денег, которые были на его банковской карте. "Почему я? Я не богатый", - пожаловался он журналистам.

Киберпреступникам, взломавшим в минувшие выходные сайт частной разведывательно-аналитической компании Strategic Forecasting в США, удалось опубликовать в открытом доступе личные данные 50 тысяч человек, сотрудничавших с компанией в разное время, сообщается в отчете компании Identity Finder, которая провела детальное исследование украденной информации. Ответственность за кибератаку взяли на себя хакеры из группы Anonymous, сообщает РИА Новости.

Среди похищенной информации эксперты обнаружили 50,3 тысячи номеров кредитных карт, срок действия почти 10 тысяч из которых не истек на момент похищения. "Это означает, что владельцы этих карт до сих пор находятся под угрозой", - сказал Аарон Тайтус, глава отдела персональной информации компании Identity Finder.

Помимо номеров карт, эксперты обнаружили 47,6 тысячи уникальных адресов электронной почты и 44,2 тысячи зашифрованных паролей от нее, примерно половину из которых, как утверждают в Identity Finder, достаточно легко расшифровать.

"Количество опубликованных паролей и вероятность их повторного нелегитимного использования значительна. Владельцы ящиков, информацию о которых распространили хакеры, должны срочно поменять пароли от них, чтобы исключить возможность атаки", - добавил Тайтус.

Кроме того эксперты обнаружили 25,6 тысячи уникальных телефонных номеров, которые также могут быть использованы хакерами в злонамеренных целях.

Strategic Forecasting, более известная по сокращенному названию Stratfor, занимается сбором и анализом информации о событиях в мире. На основании собранных данных аналитики компании составляются экономические и геополитические прогнозы.

Хакерская группировка Anonymous стала широко известна в конце прошлого года, когда они атаковали сайты организаций, которые чинили препятствия WikiLeaks. Позднее Anonymous объединились с другой известной группой LulzSec, которые "для прикола" занимались взломом правительственных сайтов США.

В серверном интерпретаторе PHP найдена опасная уязвимость

ИТ-специалисты говорят об обнаружении уязвимости в серверном интерпретаторе популярного языка веб-программирования PHP, эксплуатируя которую атакующий может внедрить злонамеренный код на сайт.

Речь идет о специальной конфигурационной директиве, предназначенной для обслуживания на выделенных и VPS-серверах. В Sucuri говорят, что им уже удалось на экспериментальном проекте внедрить злонамеренные iFrame в веб-страницы. "Мы обнаружили, что целые серверы можно

скомпрометировать, если в основной конфигурационный файл php.ini добавить директиву auto_append_file="OFF"", - *говорят в компании.*

Согласно данным руководства PHP, директива auto_append_file уточняет имя обрабатываемого файла, включаемого в парсинг до начала основной обработки кода. Эта директива является общесерверным аналогом функции PHP require (). Положение Off в ряде версий на самом деле интерпретируется как файл /tmp/Off, который хакер может создать и внедрить туда злонамеренный код, вызываемый сервером.

В компании Sucuri говорят, что в теории этой уязвимости может быть подвержено несколько десятков тысяч серверов, работающих в данный момент в интернете. "Мы уже получили отклик по данному сценарию от нескольких десятков серверов", - *говорит Девид Деде, специалист по сетевой безопасности Sucuri. По его словам, сейчас они исследовали данную уязвимость только на примере VPS и выделенных серверов, но при некоторой сноровке ее также можно применять и к серверам, обслуживающим системы разделяемого (Shared) хостинга.*

В компании Websence говорят, что им также удалось подтвердить указанную уязвимость и в теории хакеры ей могут пользоваться уже несколько месяцев, хотя крупных атак с использованием данного сценария пока не было зафиксировано.

Треть вирусов для Android распространяется через Android Market – Eset

Треть вирусов, загружаемых на устройства под управлением операционной системы Android, пользователи получают вместе с приложениями из онлайн-магазина Android Market, свидетельствуют данные исследования антивирусной компании Eset, опубликованные в четверг.

По данным компании, ОС Android пользуется наибольшей популярностью среди вирусописателей, специализирующихся на создании вредоносного кода для мобильных устройств. За последние пять месяцев доля угроз для устройств, работающих под управлением этой ОС, составила 65% от общего числа.
Еще 37% вредоносных программ попадают на устройства через SMS и MMS. Кроме того, 60% вирусов нацелено на удаленный контроль над мобильным устройством.
По оценкам Eset, в мире насчитывает более пяти миллиардов мобильных устройств, каждое четвертое из них - смартфон с возможностью выхода в интернет.

Facebook получил порцию запрещенного спама

Крупная социальная сеть Facebook на протяжении нескольких дней подвергалась массовому распространению спама. Некоторым ее пользователям в новостных разделах страницы пришлось наблюдать изображения, ссылки и видео с содержанием порнографии и насилия. Один из представителей компании Эндрю Нойес (Andrew Noyes) рассказал агентству Reuters о том, что пользователи столкнулись с распределенной спам-атакой, использующей браузерную уязвимость. Он добавил, что на данном этапе усилиями команды удалось привести к существенному сокращению объема ущерба, причиняемого такого рода атакой, и компания продолжит процесс расследования и выявления лиц, причастных к этому инциденту.

Крупная социальная сеть Facebook на протяжении нескольких дней подвергалась массовому распространению спама. Некоторым ее пользователям в новостных разделах страницы пришлось наблюдать изображения, ссылки и видео с содержанием порнографии и насилия. Один из представителей компании Эндрю Нойес (Andrew Noyes) рассказал агентству Reuters о том, что пользователи столкнулись с распределенной спам-атакой, использующей браузерную уязвимость. Он добавил, что на данном этапе усилиями команды удалось привести к существенному сокращению объема ущерба, причиняемого такого рода атакой, и

компания продолжит процесс расследования и выявления лиц, причастных к этому инциденту.

Пока не известно, кому понадобилось распространение спама и, главное, не ясен мотив, однако Эндрю Нойес объяснил механизм распространения вредного контента. Так или иначе, но виновниками отчасти оказались сами пользователи сети, которые нажимая на адресную строку браузера, цепляли вредоносное JavaScript-приложение, приводящее к неумышленному распространению вредоносного спама. По этой причине инженеры Facebook работают над устранением уязвимости браузера.
Вообще, как комментировал ситуацию Пол Фергюсон (Paul Ferguson), главный исследователь вирусных угроз из Trend Micro, Facebook и остальные сайты, использующие технологию работы Web 2.0, всегда были и будут находиться в состоянии потенциальной атаки, поскольку крупные популярные сайты не обходятся без разнообразия внешнего контента. И может показаться обычным то, что сеть Facebook просто не может обойтись без хакерских атак чуть ли не каждый день. Все потому, что сайты такого масштаба порождают соблазн сотворить что-нибудь эдакое.

Хакер предложил новый метод взлома iPhone с iOS 5.0.1

Хакер под псевдонимом pod2g предложил способ взлома Apple iPhone и iPad с самой последней версией операционной системы iOS 5.0.1, который не требует подключать устройство к компьютеру для повторения процедуры всякий раз, когда смартфон или планшет нужно перезагрузить, как это предполагалось при использовании прежних методов взлома, сообщил хакер в своем блоге.

Хакер предоставил результаты своей работы членам двух известных хакерских групп, специализирующихся на взломе мобильной техники Apple,

iPhone Dev Team и Chronic Dev Team. Те в свою очередь создали программы, которые предназначены для всех желающих.

Процедура взлома, именуемая JailBreak, позволяет открыть доступ к файловой системе устройства и устанавливать приложения, полученные из источников, отличных от официального интернет-магазина Apple App Store. В частности, на iPhone, подвергнутом JailBreak, можно установить пиратский софт.

Хакер отмечает, что с помощью предложенного им метода доступен взлом любых устройств, которые совместимы с iOS 5, кроме iPad 2 и iPhone 4S. По словам pod2g, теперь он переключится на работу по взлому именно этих устройств.

Apple выпустила финальную версию iOS 5 в октябре, а ее первое обновление iOS 5.0.1 появилось спустя примерно месяц. Средства для их взлома стали доступны практически сразу, однако пользователю требовалось повторять процедуру каждый раз при перезагрузке устройства (так называемый привязанный JailBreak). Новый способ лишен этого недостатка.

В следующем обновлении мобильной платформы iOS компания Apple может закрыть уязвимости в защите системы, который обнаружил и использовал pod2g.

В середине 2010 года в американский закон об авторских правах в цифровую эпоху (DMCA - Digital Millennium Copyright Act) были внесены изменения, которые узаконили взлом телефонов, в том числе и iPhone, для установки любого программного обеспечения. Аналогичным образом было легализовано и устранение привязки телефона к сети определенного оператора мобильной связи.

В Москве соберутся хакеры со всего мира

Компания Positive Technologies сообщила о завершении отборочных этапов конкурсов по взлому и защите информации CTF Quals и CTF Afterparty, проходивших в рамках форума Positive Hack Days. В результате сильнейшие мировые хакерские команды встретятся в Москве 30 и 31 мая 2012 года.

В общей сложности, в борьбе за выход в финал приняли участие свыше 200 человек из 27 стран мира. Самую большую активность проявили российские, американские и французские хакеры. Также среди участников присутствовали специалисты из Японии, Нидерландов, Южной Кореи, Туниса, Германии, Швейцарии, Кении, Канады, Перу, Великобритании, Швеции, Ливана, Австралии и Испании.

http://phdays.ru/

Positive Hack Days - *мероприятие, посвященное практическим вопросам информационной безопасности. В программу форума входят доклады ведущих специалистов российского IT-рынка, мастер-классы, деловые семинары, различные конкурсы по защите и взлому информационных ресурсов.*

В 2011 году Positive Hack Days посетило свыше 500 человек, среди которых были специалисты из России, Европы, США и Азии, представители ведущих российских и зарубежных IT-компаний, независимые эксперты. Форум получил широкий отклик в профессиональной среде и был признан "самым интересным событием года" в сфере информационной безопасности.

Используемая литература в разделе: http://tvernedra.ru/content/prousa.html

Хакеры Ниндзя.Искусство войны тактика, маскировка, шпионаж, взлом, методы, проникновение. 12.2011 ХИТ!!!!!

Опубликовано: 31 декабря 2011 года.

http://www.tvernedra.ru/