Аналитика, обзоры, рекомендации.

user And LINUX

{ Secure Shell }

UA Linux http://ualinux.com

Хакеры опубликовали 16 ГБ секретных данных Bank of America

Читайте в этом номере:

- Хакеры опубликовали 16 ГБ секретных данных Bank of America.

- Выявлена вредоносная программа, которая особо «поработала» в Украине.

- $10 млн в неделю: как работают российские хакеры.

- ЛК: Хакеры используют web-серверы для проведения DDoS-атак

- На крючке у хакеров. Хакеры разоряют счета украинцев.

- Win32/Spy.Ranbyus нацелен на модификацию Java-кода систем удаленного банкинга Украины.

- МВД отчиталось о борьбе с киберпреступностью

И многое другое.

Эксперт в области безопасности.

UA Linux open source ■ open future

Хакеры из Anonymous опубликовали 16 ГБ данных, украденных с сервера Bank of America, крупнейшего банка США. Группировка внутри Anonymous, осуществившая утечку данных, называет себя Par:AnoIA. Данные были опубликованы на одноименном сайте.

Хакеры утверждают, что Bank of America нанимал охранные фирмы, чтобы следить за гражданами США. Это следует из опубликованных ими секретных данных банка.

Bank of America нанял фирму TEKSystems, чтобы отслеживать поведение пользователей, ассоциирующихся с группировкой Anonymous, в соцсетях. Эта информация составляла большую часть данных, утекших с сервера банка. Еще 4,8 ГБ данных содержали подробную информацию о карьере и зарплате сотен тысяч менеджеров корпораций по всему миру. Папка, содержавшая эту информацию, была озаглавлена «Bloomberg», а записи в ней помечены словом «reuterscompanycontent» (содержание компании Reuters), что может указывать на то, что к сбору пользовательских данных причастны новостные агентства Bloomberg и Reuters.

Также на сервере хранилась программа OneCalais, анализирующая тексты новостей и блогпостов в Интернете.

Хакеры получили доступ к данным с незащищенного сервера, находящегося в Тель-Авиве. Для этого им даже не пришлось взламывать систему безопасности, сообщает ruformator.ru.

Источник: http://k-z.com.ua

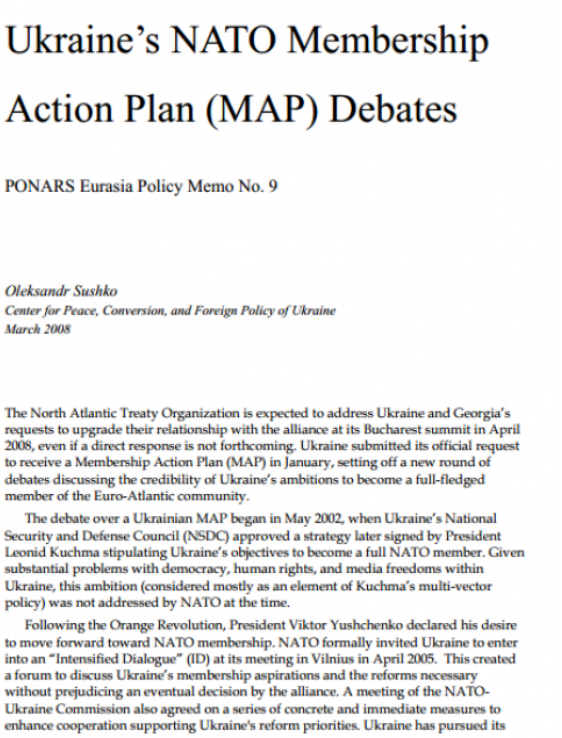
And User Linux

Выявлена вредоносная программа, которая особо «поработала» в Украине.

Обнаружен вирус, загрузчик которого написан на Ассемблере, который работал против правительственных учреждений. Украина – одна самых из наиболее пострадавших стран.

Выявлена масштабная кибератака с применением сочетания сложных вредоносных кодов на устаревших языках программирования и новых технологий использования уязвимостей в Adobe Reader. Созданный специально для этих атак бэкдор MiniDuke написан на Ассемблере и чрезвычайно мал – всего 20 Кб, Целью атаки стало получение информации геополитического характера. Об этом говорится в отчёте «Лаборатории Касперского».

Вредоносная программа MiniDuke распространялась при помощи недавно обнаруженного эксплойта для Adobe Reader (CVE-2013-6040). Среди жертв трояна оказались госучреждения Украины, Бельгии, Португалии, Румынии, Чехии и Ирландии. Кроме того, от действий киберпреступников пострадали ряд исследовательских учреждений в разных странах.



Ukraine's NATO Membership Action Plan (MAP) Debates

PONARS Eurasia Policy Memo No. 9

Oleksandr Sushko
Center for Peace, Conversion, and Foreign Policy of Ukraine
March 2008

The North Atlantic Treaty Organization is expected to address Ukraine and Georgia's requests to upgrade their relationship with the alliance at its Bucharest summit in April 2008, even if a direct response is not forthcoming. Ukraine submitted its official request to receive a Membership Action Plan (MAP) in January, setting off a new round of debates discussing the credibility of Ukraine's ambitions to become a full-fledged member of the Euro-Atlantic community.

The debate over a Ukrainian MAP began in May 2002, when Ukraine's National Security and Defense Council (NSDC) approved a strategy later signed by President Leonid Kuchma stipulating Ukraine's objectives to become a full NATO member. Given substantial problems with democracy, human rights, and media freedoms within Ukraine, this ambition (considered mostly as an element of Kuchma's multi-vector policy) was not addressed by NATO at the time.

Following the Orange Revolution, President Viktor Yushchenko declared his desire to move forward toward NATO membership. NATO formally invited Ukraine to enter into an "Intensified Dialogue" (ID) at its meeting in Vilnius in April 2005. This created a forum to discuss Ukraine's membership aspirations and the reforms necessary without prejudicing an eventual decision by the alliance. A meeting of the NATO-Ukraine Commission also agreed on a series of concrete and immediate measures to enhance cooperation supporting Ukraine's reform priorities. Ukraine has pursued its

В ходе исследования специалисты пришли к следующим выводам:

- Авторы MiniDuke до сих пор продолжают свою активность, последний раз они модифицировали вредоносную программу 20 февраля 2013 года. Для проникновения в системы жертв киберпреступники рассылали вредоносные PDF-документы.

- При заражении системы на диск жертвы попадал небольшой загрузчик, размером всего 20 Кб. Он уникален для каждой системы и содержит бэкдор, написанный на Ассемблере.

- Если атакуемая система соответствует заданным требованиям, вредоносная программа будет использовать Twitter для поиска специальных твитов от заранее созданных акаунтов

- Как только заражённая система устанавливает соединение с сервером управления, она начинает получать зашифрованные бэкдоры через GIF-файлы, которые маскируются под картинки на компьютере жертвы.

- Бэкдор выходит на связь с двумя

серверами – в Панаме и Турции – для того чтобы получить инструкции от кибер-преступников.

Источник: http://www.imena.ua

$10 млн в неделю: как работают российские хакеры

Хакерские группировки в России зарабатывают, по оценкам некоторых экспертов, до $10 миллионов в неделю. Их деятельность наносит серьезный ущерб бизнесу и даже приводит к банкротству отдельных компаний. Среди кибер-преступников есть не только профессиональные технические специалисты, но и предприимчивые «менеджеры», которые просто покупают готовые технологии и нанимают исполнителей.

Специалисты по кибербезопасности рассказали «Газете.Ru», как и сколько зарабатывают российские криминальные хакерские группы.

Давно ни у кого не вызывает удивления, что в громких хакерских аферах часто прослеживается российский след. Так, 10 ноября в Эстонии были арестованы 6 кибер-преступников российского происхождения, а седьмого члена группы, гражданина России, ищут до сих пор. По данным ФБР, группа заразила 4 млн компьютеров по всему миру, построив рекламную мошенническую систему, перенаправляющую пользователей на нужные сайты через поисковые запросы.

За накрутку трафика платили владельцы рекламируемых сайтов, которым нужен был рост посещаемости. С 2007 по 2011 год хакеры предположительно заработали таким образом $14 млн. Таких криминальных бизнес-моделей, которые совсем неочевидны обывателям, но приносят огромные деньги преступникам, существует немало.

Данный случай – не единственный пример совместных российско-эстонских преступных проектов. В деле Евгения Аникина, хакера из Новосибирска, который в 2008 году похитил у американского подразделения Royal Bank of Scottland $10 млн, тоже был замешан эстонский подельник. Сам Аникин уже получил 5 лет условно, а его компаньон все еще находится под следствием.

Среди именно российских кибер-ОПГ наиболее известной считается криминальная группировка, работавшая под собственным брендом Russian Business Network (RBN), занимавшаяся различными типами компьютерных преступлений, в частности, созданием так называемых «абузоустойчивых сетей» для размещения в них детской порнографии, фишинговых сайтов, вредоносного ПО и т.п. (Абузоусточивый хостинг – хостинг, где можно размещать любой, в том числе и нелегальный контент – ред.). По данным компании Group-IB, сейчас RBN распалась, а ее участники работают в нескольких ОПГ под другими именами.

Как сообщил «Газете. Ru» генеральный директор Group-IB Илья Сачков, IT-криминалисты компании Group-IB участвовали в «показательном» расследовании в отношении 18-летнего россиянина, который создал ботнет (сеть зараженных компьютеров) и сдавал его в аренду другим злоумышленникам для организации DDoS-атак и рассылки спама. За полтора года он заработал $1 млн 733 тыс. Эксперты собрали доказательную базу по этому делу, но арестовать преступника правоохранительные органы не успели – юный хакер выехал за границу и скрылся.

По словам Сачкова, сейчас эта сумма уже не кажется впечатляющей, особенно по сравнению с заработками преступных групп, специализирующихся на мошенничестве в системах электронного банкинга.

«Подобные группы в России зарабатывают миллионы долларов ежемесячно. Зафиксированные нами рекорды — $24 и $26 миллионов за полтора месяца. Речь идет о двух разных группировках, которые заработали эти суммы в беспрецедентно короткие сроки», – говорит Сачков.

Генеральный директор Group-IB под-

черкнул, что деньги воруются именно у российских компаний, в основном представляющих средний и малый бизнес. Многие из них в итоге оказываются на грани банкротства или вообще не могут продолжать коммерческую деятельность. Таким образом, злоумышленники не просто нарушают законы и воруют деньги, они наносят прямой ущерб экономике страны. На данный момент хищение денег со счетов юридических лиц — самое популярное и самое прибыльное киберпреступление в России. Обороты мошенничества с использованием реквизитов банковских карт частных пользователей и поддельных сайтов в десятки, а то и в сотни раз меньше.

«Преступникам даже не требуется профильных знаний в области информационных технологий, необязательно быть «продвинутым хакером», – продолжает Сачков. – Достаточно иметь общие представления о преступных схемах и сумму в районе $8 тысяч.

Благодаря такому первоначальному капиталу злоумышленник сможет найти на внутреннем рынке киберпреступности тех, кто выполнит большую часть технических работ - такой своеобразный криминальный аутсорсинг».

О кибер-кражах на десятки миллионов долларов даже не в месяц, а в неделю предупреждает и антивирусная компания ESET. Директор Центра вирусных исследований и аналитики Александр Матросов сообщил «Газете.Ru», что самой опасной вредоносной программой, которая работает с системами ДБО (дистанционного банковского обслуживания), стал новый троян Carberp - технологически сложная и дорогостоящая разработка, еще более опасная, чем известные банковские трояны Zeus и SpyEye. Carberp появился примерно 2 года назад и с тех пор вирусописатели создают для него обновления, пик активности вируса аналитики наблюдают в 2011 году.

Россия сегодня является абсолютным лидером по количеству инцидентов с использованием Carberp (72% от общего количества инцидентов в различных странах), а доход преступников, по словам эксперта, составляет $10 млн в неделю.

Причем оператором трояна, по данным Матросова, выступает крупная российская преступная группировка.

В ESET утверждают, что пострадавшими от этого вредоносного ПО стали клиенты практически всех крупнейших российских банков – причем не только коммерческие компании, но и государственные структуры.

Эксперты компании сообщают, что в новой версии трояна Carberp используется специальный загрузочный функционал, который позволяет обходить защитные системы и загружать в IT-инфраструктуру компаний вредоносные файлы и запускать нужные процессы. Стоимость подобного дополнения к троянской программе на «черном» рынке составляет несколько десятков тысяч долларов. Это в несколько раз больше, чем цены на аналогичные трояны предыдущего поколения. Carberp также эксплуатирует 4 уязвимости в операционных системах Microsoft Windows, что позволяет ему красть финансовые средства даже с компьютеров корпоративной сети, где есть доступ к ДБО. Также троян Carberp объединяет зараженные ПК в ботнет - сейчас в этой сети насчитывается уже несколько сотен тысяч компьютеров.

«Несмотря на то, что сейчас основной целью Carberp являются клиенты российских банков, ситуация может быстро измениться, так как технологических препятствий для атак на банки в других странах у этой преступной группы нет, – говорит Матросов. – И скорее всего злоумышленники в ближайшем будущем начнут искать партнеров по атакам в других странах».

Компания «Лаборатория Касперского» в оценках ущерба от действий преступных групп в сфере онлайн-банкинга более осторожна. В интервью «Газете.Ru» главный антивирусный эксперт компании

Александр Гостев предположил, что в России потери в результате действий злоумышленников в системах ДБО составляют десятки миллионов рублей ежемесячно.

Несмотря на популярность «банковских» преступлений, большая доля доходов приходится и на другие направления, например на рынок нежелательных рассылок (спама). По данным компании Symantec, в прошлом году оборот только российского рынка спама составил более 25 млрд. рублей, а доля России в мировом рынке спама – порядка 3%.

«Криминальный кибер-рынок опасен прежде всего своим масштабом. По всему миру работают миллиарды бот-инфицированых компьютеров, рассылающих спам и распространяющих вирусы, основная масса из которых находится в США и Китае, а раскрытие отдельных группировок приоткрывает лишь малую часть криминального рынка», – сообщил «Газете.Ru» ведущий технический консультант Symantec в России Олег Шабуров.

Сказать, в какой стране сосредоточено наибольшее количество кибер-криминала и где хакеры зарабатывают больше всего, конечно, очень сложно. С одной стороны, важную роль играет распространение широкополосного доступа и количество пользователей интернета в той или иной стране. Россия, кстати, по этому показателю недавно вышла на первое место в Европе, так что у России есть шанс стать «чемпионом» и в этой области. С другой стороны, некоторые эксперты по компьютерной безопасности считают, что большая часть инфицированных компьютеров, а также крупнейшие хостинг-провайдеры, замеченные в размещении вредоносного ПО, находятся в настоящий момент на территории США.

Источник: http://www.obzor.lt

ЛК: Хакеры используют web-серверы для проведения DDoS-атак

Злоумышленники осуществляют поиск серверов с неустраненными уязвимостями и встраивают в них средства для осуществления DDoS-атак.

Специалисты из «ЛК» сообщают, что в настоящее время организовывающие DdoS-атаки мошенники все чаще используют простые в управлении web-серверы вместо ботнетов. Об этом сообщают РИА Новости.

В связи с таким развитием событий, количество DDoS-атак увеличивается, и они становятся более усовершенствованными. Отказ от использования ботнетов был спровоцирован тем, что обеспечивать их постоянную работу – очень тяжелая задача, так как мошенникам сложно поддерживать работоспособность нужного количества зараженных ПК онлайн. Именно поэтому хакеры разрабатывают новые способы проведения атак.

В частности, злоумышленники осуществляют поиск серверов с неустраненными уязвимостями, встраивают в них средства для осуществления DDoS-атак и впоследствии выполняют все поступающие к ним заказы. Несколько серверов намного производительнее, чем рабочие станции, и их проще активировать.

Генеральный директор компании Highload Lab Александр Лямин отмечает, что использование серверов в DDoS-атаках стало возможно в связи с появлением новых инструментов анонимизации, которые затрудняют определение местоположение серверов, распространяющих вредоносный трафик. Злоумышленники территориально распределяют инфраструктуру для осуществления атак так, чтобы их было максимально трудно прекратить через обращение к провайдеру или датацентру, в котором расположен атакующий сервер.

Эксперты отмечают, что зачастую DDoS-атаки являются методом нанесения убытков конкурентам, так как недоступность банков, интернет-магазинов и других финансовых учреждений подрывает их репутацию, в результате чего они теряют клиентов.

Источник: http://www.securitylab.ru

На крючке у хакеров

Хакеры разоряют счета украинцев

Хакеры разоряют счета украинцев: достаточно одного неосторожного платежа в интернет-магазине либо социальной сети, и на карточке физлица не останется ни копейки

Карточные расчеты в Украине становятся все более опасными. Еще год-два назад владельцам пластика советовали обходить стороной банкоматы с накладками мошенников и по возможности не "светить" реквизиты карточек под видеокамерами во время расчетов в магазинах. Теперь же держателям рекомендуют несколько раз подумать, прежде чем рассчитаться в интернете: в системе интернет-банкинга или просто на сайте торгово-розничных сетей (интернет-магазинов, кинотеатров, транспортных компаний и пр.). Новая опасность для наших карт — хакеры. Они беспощадно грабят как личные счета рядовых граждан, так и "кубышки" предприятий.

Сеть — рай для мошенников

Разгул карточной преступности на прошлой неделе был подтвержден статистикой правоохранительных органов и Нацбанка. По информации чиновников, за 2012 г. общее количество мошеннических операций с платежными картами в нашей стране выросло сразу на 47% и с 35 до 57 увеличилось количество банков, со счетов которых пропадали средства. Как и прежде, по числу несанкционированных списаний со счетов лидировали физлица (ежедневно от населения поступает до 50 жалоб, со счетов за прошлый год пропало 11,4 млн грн.), а по объемам потерь — компании. Как сообщили "ДС" в МВД, за прошлый год правоохранители возбудили 139 уголовных дел на предмет списаний мошенниками при помощи систем "Клиент-Банк" 116 млн грн. Не менее активно исчезали деньги со счетов предприятий и в нынешнем году: зафиксировано 23 факта пропажи средств на общую сумму 12,5 млн грн.

Население, банкиры и даже силовики оказались не готовы к активизации финансового криминалитета, а главное, — к смене его приоритетов. До 2012 г. мошенники собирали информацию о карточных счетах украинцев главным образом в торговых точках (считывали данные с POS-терминалов во время платежа) и банкоматах, на которые устанавливались накладки, считывающие данные с пластика. Но в прошлом году они по-новому открыли для себя Всемирную паутину: компьютерные гении не только продолжали взламывать системы интернет-банкинга, но и стали писать специальные вирусы, считывающие с ПК банковских клиентов информацию о карточных счетах.

"Чаще всего использовался вирус типа back-door, позволяющий злоумышленникам на удалении контролировать компьютеры жертв. Как правило, между их заражением и проведением несанкционированной транзакции преступники в течение нескольких недель отслеживали состояние счетов и анализировали технические особенности соединения компьютеров клиентов с серверами банков (лог-файлы)", — рассказал "ДС" начальник управления по борьбе с киберпреступностью МВД Украины Максим Литвинов.

Собственно, именно технологическая революция, перевернувшая весь мир в 2012 г., и стала главной причиной стремительного роста финансовой преступности в нашей стране. "Прошлый год знаменовался активным использованием современных информационных технологий для компрометации платежных карт: я имею в виду и создание новых вирусов, и взломы больших компаний по приему платежей и

торговых точек", — отметил в беседе с "ДС" ведущий эксперт управления безопасности ОТП Банка Алексей Немченко.

Профессиональный уровень жуликов стремительно повышался, а клиенты банков оставались такими же беспечными, как и прежде: продолжали, например, по первому требованию передавать мошенникам, представившимся по телефону либо электронной почте работниками банков, информацию о карточных счетах. Да и компьютеры физлиц и предприятий оставались совершенно беззащитными перед атаками мошенников: большинство отечественных пользователей ПК до сих пор не пользуются не только лицензированными антивирусными программами, но даже базовым лицензионным программным обеспечением.

Не всегда перед хакерами могли устоять и финансовые учреждения: либо из-за виртуозного искусства преступников, либо из-за устаревших программ, которые не спешили менять финансово немотивированные банки. "В нашей стране отсутствует ответственность банков за предоставление небезопасного сервиса с потерями выше определенного уровня. А также отсутствуют требования к безопасности систем дистанционного банковского обслуживания", — признал начальник департамента безопасности информационных систем УкрСиббанка BNP Paribas Group Андрей Моршнев.

Усугублялась ситуация еще и более активным проникновением в банковские структуры криминала. Хакеры вступали с финансистами в преступные сговоры и ускоряли передвижение и вывод со счетов украденных денег. "В ходе расследований мы нередко сталкивались с подозрительными операциями по оперативной выдаче значительных сумм наличности. Это создавало предпосылки для преступлений и указывало на возможную заинтересованность работников банков в реализации преступного умысла", — заметил "ДС" Максим Литвинов.

Деньги вернут VIP-клиентам и застрахованным

Обычно жулики собирали информацию о картах физлиц (номер карты и код CVV, который нужен для покупок в интернете) тремя способами. Реже прибегали к классическому: обзванивание физлиц под видом банковских работников с просьбой уточнить данные карты. Хотя обыватели до сих пор покупаются на эти нехитрые трюки. Куда чаще жулики демонстрировали свои хакерские таланты: создавали вредоносные программы, собирающие сведения о карточных счетах физлиц непосредственно на их компьютерах, после чего вирусы запускали в интернет.

"Те попадали на порталы, не имеющие четко построенной защиты от мошенничества: созданные для оплат компьютерных игр, программного обеспечения (чаще всего пиратского происхождения). А то и вовсе на фишинговые сайты: это ресурсы, выдающие себя за другие порталы, создаются с целью хищения логинов, паролей и другой конфиденциальной информации", — рассказал "ДС" начальник управления безопасности карточного бизнеса департамента банковской безопасности банка Надра Вячеслав Федотенко.

Нередко вредоносные программы подхватывались компьютерами пользователей с разного рода интернет-форумов и социальных сетей. Хакеры не гнушались и банального взлома карточных данных, правда, прибегали к этому крайне редко: проникали в ноутбуки физлиц в публичных зонах Wi-Fi и считывали при помощи спецпрограммы нужные данные.

Как ни старались финучреждения защитить свои системы интернет-банкинга, им так и не удалось выстроить идеальный барьер против хакеров-разрушителей. Поэтому они также служили для

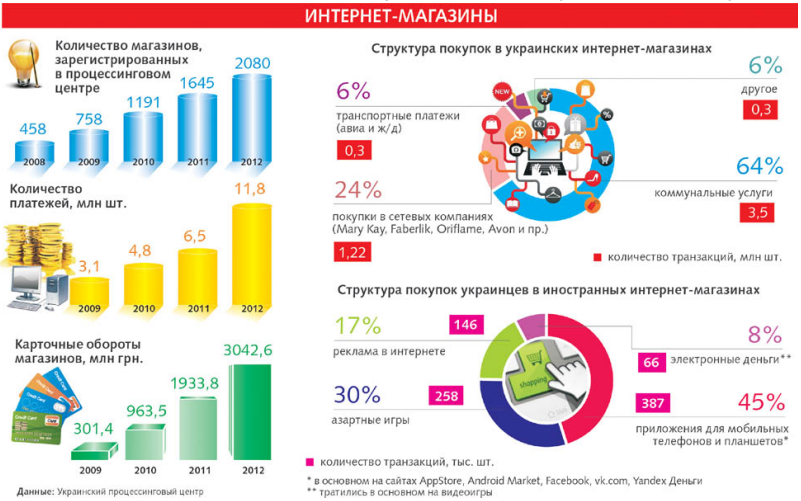
злых гениев источниками информации о карточных счетах населения. "Системы защиты конфиденциальных сведений финучреждений остаются уязвимыми. На это указывает статистика краж средств со счетов клиентов Укрсоцбанка и УкрСиббанка", — сказал "ДС" г-н Литвинов. Некоторое утешение лишь в том, что количество попыток взломов удаленных систем банкинга, по оценкам финансистов, в 2012 г. было зафиксировано на 10–15% меньше, чем в 2011 г.

Следующая плохая новость: у мошенников заметно выросли аппетиты. Если в 2011 г. с карты физлица до ее блокирования банком (после обращения клиента) успевали похитить от 300 до 500 грн., то в 2012 г. — уже порядка 700–1000 грн. Вернуть же эти средства удавалось далеко не всегда и только после проведения расследования, которое обычно длится до 30 дней. Как правило, банк соглашается компенсировать потери клиентов лишь в некоторых случаях: если в ходе расследования (службы безопасности финучреждения и МВД) будет доказана вина финансистов или сайта, на котором до кражи денег осуществлялись платежи. То есть выяснится, что утечка информации о картах произошла из-за оборудования или действий их сотрудников.

"В случаях, когда явно виноват банк, он выплачивает компенсацию. Если ошибся клиент (например, сам выдал данные карты мошеннику), скорее всего, финучреждение не заплатит. Хотя бывают и исключения: в некоторых банках существуют программы лояльности, в рамках которых они возмещают клиентам потери в любом случае. Но обычно это касается лишь VIP-клиентов", — рассказал "ДС" координатор комитета Независимой ассоциации банков Украины по вопросам банковской инфраструктуры и платежных систем Владимир Еременко.

Также стопроцентную возможность вернуть себе украденные средства имеют застрахованные держатели пластика. Но платить им будет уже не банк, а страховая компания в рамках страховой суммы. "По желанию клиентов, в некоторых тарифных планах мы предлагаем воспользоваться возможностью оформить страховой полис от мошенничества. Плата за такую опцию колеблется в среднем от 40 до 150 грн. в год в зависимости от типа карты, размера кредитного лимита и страхового покрытия (обычно оно не превышает 30 тыс. грн.)", — сообщил "ДС" заместитель начальника управления платежных карт Банка "Национальный кредит" Денис Мельник.

В ближайшее время финансисты не обещают менять правила компенсаций для обобранных мошенниками клиентов. Чтобы не попадаться на удочку жуликов, советуют следовать нескольким правилам. Главное — ни в коем случае не сообщать данные карт третьим лицам. Кроме того, желательно установить лимиты на операции, sms-информирование о каждой транзакции, не пользоваться системами интернет-банкинга и платежными функциями на других сайтах в публич-



ных зонах Wi-Fi. А также выпустить к стандартной карте дополнительную — для платежей в интернете (класса Virtuon), и только по ней совершать транзакции в Сети.

Охота по-крупному

Украинские компании мошенники грабят практически так же, как и население. Сначала пытаются выудить информацию у малоопытных и беспечных бухгалтеров: раздобыв у банка базу данных e-mail адресов корпоративных клиентов, жулик рассылает по ней письма с просьбой ответить на некоторые вопросы (например, ПИН-код, номер карты, одноразовый пароль и т. д.). Получив информацию, преступник действует мгновенно — со счетов компании начинают исчезать средства.

Второй способ получить информацию о счете сводится к написанию хакером специального вируса под отдельно взятую систему "Клиент-Банк" (нельзя написать универсальную программу, которая будет взламывать все системы подряд). Он либо откроет злоумышленнику удаленный доступ к компьютеру предприятия в онлайн-режиме, либо просто перехватит для хакера пароль и ключ, открывающие доступ к "Клиент-Банку".

Компании теряют на атаках злых гениев куда большие суммы, чем физлица. "Суммы, на которые посягают преступники, в 2012 г. колебались от 30 тыс. до 30 млн грн.", — сообщил "ДС" Максим Литвинов. Утешает лишь то, что раскрываемость корпоративных краж у правоохранителей довольно высока: за прошлый год милиция совместно с банками и Госфинмониторингом смогла компенсировать 54% убытков юрлиц в 74 случаях из 139 зафиксированных. Обычно отследить средства удавалось после того, как они начинали стихийно переводиться со счета на счет в разных банках.

В то же время розыск пропавших денег по корсчетам и поимка преступников — единственный реальный шанс для компаний вернуть свои средства. Такие потери банки практически не компенсируют. Возмещение может состояться лишь в том случае, если будет доказан сговор банковского работника с жуликами и вина финучреждения будет очевидна.

Руководителям компаний, желающих защититься от хакеров, сегодня дают несколько советов. В первую очередь стандартные: ограничивать число сотрудников, ответственных за осуществление операций в "Клиент-Банке", и компьютеров, используемых для этого. "Также мы предлагаем клиентам для хранения электронных ключей специальные токены, которые защищают ключи от несанкционированного копирования при входе в "Клиент-Банк". И советуем клиентам прописывать свои IP-адреса, с которых будет возможен вход в систему или использовать одноразовые пароли для подтверждения операций через sms-сообщения", — объяснил "ДС" начальник сектора мониторинга и опротестования транзакций АО "Эрсте Банк" Игорь Попов.

В случае применения всех этих рекомендаций вероятность хищений сводится к минимуму. У жуликов останется лишь один способ получить деньги компании — физически вторгнуться в офис предприятия и быстро "зачистить" его счета. По слухам, в Украине были и такие случаи, однако они заканчивались поимками преступников.

Карточный облом

Карточные расчеты банки активно пропагандируют последние лет десять. Чего только не делают: и разбрасывают бесплатный пластик по почтовым ящикам украинцев, и дают им скидки на покупаемые картой товары, и насчитывают за покупки денежные бонусы на счет. Главная же заповедь финансистов: на карточном счете деньгам куда безопаснее, чем в кошельке. Если карманный вор утащит

портмоне, то наличные пропадут навсегда, а "пластиковые" средства находятся под замком у банка, и до них злодею не добраться. Но совершенно неожиданно для многих выяснилось, что все это миф.

Преступники научились оперативно взламывать защиту финансистов и ловко грабить счета населения, которое живет вчерашним днем и призрачной надеждой, что банки надежно оберегают их накопления. Гражданам, которые, не вникая, подмахивали карточные договоры с банками, не вчитываясь в правила пользования карточкой, и в голову не приходит, что под видом банкиров им могут позвонить жулики, выведать номер карты с кодом и в считанные минуты оставить без копейки. А потому и попадаются они на избитые уловки мошенников, количество которых в последнее время растет стремительными темпами.

Причем все чаще среди них встречаются не только примитивные махинаторы, подсматривающие карточные пароли в магазинах, но и настоящие гении. Они могут облапошить даже самого искушенного карточного пользователя: при помощи вируса, запущенного в компьютер физлица, собрать всю информацию о карте, и, пока тот безмятежно спит (и не видит банковские sms-сообщения о расчетах), за одну ночь разграбить весь его банковский счет. А дальше — тупик. Глухим к просьбам вернуть деньги может оказаться и банк, который использует любую возможность экономить — не компенсировать потери, и правоохранители. В самом лучшем случае удается возврат около половины украденного.

Перед картодержателем разведут руками — технический прогресс открывает перед хакерами бесконечные возможности. В такой ситуации невольно задумаешься: готов ли ты нести на своем кошельке издержки высоких технологий и покупаться на россказни финансистов о безопасном размещении у них своих кровных.

Наказание для шопоголиков

Главная опасность при расчетах картами в интернет-магазинах — это все тот же пресловутый фишинг. Только здесь, чтобы попасться на удочку мошенников, вовсе не обязательно выдавать жуликам данные карты по телефону, достаточно лишь войти на неблагонадежный сайт и попытаться там что-то купить. Для этого, собственно, их и создают: чтобы выведывать данные о счетах. Внешне они выглядят весьма благопристойно и делают покупателям очень выгодные предложения (товары на этих порталах могут быть чуть ли не на 20–30% дешевле, чем в среднем по рынку). А иногда даже напоминают своим дизайном известные интернет-магазины. Все делается для того, чтобы покупатель не заподозрил подвоха и попытался приобрести товар — вбил реквизиты своей карты. Это все, что нужно владельцам портала, чтобы начать разграбление карточного счета физлица.

Сведения о счетах получают и накапливают в своих базах данные только "фишинговые" сайты. Все нормально действующие порталы работают через процессинговые центры, и данные о картах даже "не видят".

"Они применяют международную технологию 3-D Secure. Происходит взаимообмен между тремя сторонами: банком, выпустившим карту, банком-эквайером (обслуживающим конкретный магазин) и процессинговым центром. Сам же интернет-магазин лишь получает от банка-эмитента ответ, если транзакция невозможна (например, нет денег на счете) или же положительный отчет о зачислении денег", — объяснил "ДС" председатель правления Украинского процессингового центра Антон Романчук. Такая система передачи данных практически сводит к нулю возможность кражи банковской информации в интернет-магазинах.

Чтобы максимально себя обезопасить, населению советуют пользоваться новыми технологиями: подписывать каждую проплату кодом и sms-сообщением.

"Платежные карты могут быть защищены протоколом 3-D Secure на стороне эмитента карточки. В таком случае при каждой операции в интернете, помимо стандартных данных (номер карты, имя владельца, CVV-2 кода и даты окончания срока действия карты), от плательщика

требуется ввести одноразовый пароль, который высылается ему на номер мобильного телефона с помощью sms-сообщения. Это полностью исключает опасность потери денег клиентом, так как даже если его информация о карте попадет в руки мошенникам, они не смогут ничего оплатить без пароля", — заверил г-н Романчук. Еще один совет специалистов: входить на сайты магазинов только при помощи защищенного соединения — адрес сайта должен начинаться с https://.

МНЕНИЕ ЭКСПЕРТА

Ростислав Кравец, старший партнер адвокатской компании "Кравец, Новак и Партнеры"

У банка можно отсудить не только сумму похищенных с карточки денег, но и пеню

Банки обязаны компенсировать клиентам украденные с карточного счета средства, даже если платежи подтверждались кодом CVV. И отказы это сделать незаконны. В любой платежной системе деньги перечисляются не сразу, а блокируются на счете на некоторое время, и если клиент своевременно обращается в банк с заявлением, то вернуть их довольно легко.

Основным документом, регулирующим деятельность платежных систем в нашей стране, устанавливающим понятия и общий порядок проведения перевода средств в пределах Украины, а также ответственность субъектов перевода, является закон "О платежных системах и переводе средств в Украине". Взаимоотношения между банком и клиентом подпадают под действие Гражданского кодекса, а также Закона "О защите прав потребителей".

Крайне сложно доказать вину банка и отсудить у него компенсацию похищенных жуликами средств, если владелец счета сам сообщил злоумышленникам данные карты либо поздно уведомил банк о возможной пропаже пластика. Если же вина финучреждения будет доказана, то в зависимости от обстоятельств можно требовать от банка не только возврата потерянных средств, но еще и пеню: по 0,1% в день от суммы, которую клиент не смог перечислить при помощи карты, но не более 10% суммы.

К общему же размеру ущерба можно причислить не только размер похищенных со счета средств, но и дополнительные затраты на возмещение этих потерь. Скажем, комиссию, уплаченную при отправке перевода Western Union клиенту, оставшемуся без копейки на карточном счете.

Источник:
"Деловая столица"
http://www.depo.ua

Win32/Spy.Ranbyus нацелен на модификацию Java-кода систем удаленного банкинга Украины

Недавно мы обнаружили новую модификацию банковского трояна Win32/Spy.Ranbyus, который уже был предметом исследования наших аналитиков. Одна из его модификаций упоминалась Александром Матросовым в сообщении, посвященном эксплуатированию смарт-карт в банковских троянах. Описываемая там модификация обладает интересным функционалом, так как показывает возможность обхода операций аутентификации при осуществлении платежных транзакций с помощью устройств смарт-карт. В той же модификации был обнаружен код поиска активных смарт-карт или их ридеров, после нахождения которых бот отсылал информацию о них в командный центр C&C с описанием типа найденных устройств.

Аналитики ESET внимательно отслеживали последние модификации семейства этого трояна и выяснили, что Ranbyus начал специализироваться на модификации Java-кода в одной из самых популярных систем удаленного банкинга (remote banking systems) на Украине, а именно, BIFIT iBank 2. На момент нашего анализа, статистика ESET Virus Radar показывала, что на Украине зафиксировано наибольшее количество инфекций Ranbyus.

Отличительной особенностью этого банковского трояна является то, что он не обладает механизмом web-инжектов, обычно применяемых в угрозах подобного рода (как, например, известный Zeus), и вместо этого реализует атаку на специфическое банковское/платежное ПО, т. е. ПО, используемое при осуществлении различного рода платежей и других банковских операций. Win32/Spy.Ranbyus собирает информацию о зараженной системе (активные процессы, версию ОС и т. д.) и отправляет ее на командный сервер (C&C). Основной функционал по краже денег основан на наборе различных форм-грабберов, нацеленных на специальное платежное ПО. Например, грабберы для ПО, разработанного под Java-платформу выглядят так:

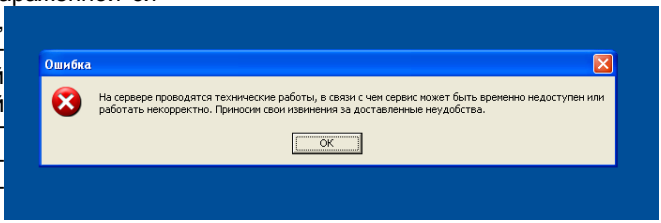
```
int __usercall inject_javaw<eax>(int a1<ebx>)
{
  int v1; // eax@3
  char v3; // [sp+0h] [bp-10h]@1

  init(&v3);
  create_process_mutex(&v3);
  if ( get_config_value_96() )
    get_import(&v3);
  delete_iBank_files();
  check_BIFIT_keys(a1);
  mem_alloc();
  init_java_hooks(&v3);
  init_javaw_grabber();
  init_java_javaw_browser_grabber();
  v1 = get_imports_table();
  (*(v1 + kernel32_Sleep))(0xFFFFFFFFu);
  exit_process(&v3);
  return 0;
}
```

Код внедрения Java-граббера.

Наш коллега Александр Матросов уже описывал схожий функционал о Java-патчинге в другом семействе банковских вредоносных программ — Carberp. Carberp обладает специальным функционалом по модификации виртуальной Java-машины (Java Virtual Machine, JVM) и отслеживания активности ПО для осуществления платежей. Ranbyus использует другой подход, он модифицирует Java-код только для определенного приложения, не прибегая к модификации JVM. Например, Ranbyus может модифицировать расположение форм, чтобы скрыть информацию о поддельных транзакциях, реализованных через троян.

В дополнении к этому, Win32/Spy.Ranbyus может блокировать действия ПО системы удаленного банкинга и показывать такое сообщение на русском языке.



Ranbyus нацелен только на Украинские и Российские банки и мы не наблюдали подобные атаки в других регионах. Панель управляющего центра ботнета выглядит таким образом:

Киберпреступная группа Carberp является лидером на преступном рынке в России и уже обеспечила себе безопасное присутствие в 20-ке наиболее активных угроз в России за весь год. В то же время, Ranbyus занимает лидирующую позицию среди других банковских вредоносных программ на Украине.

```
removeNodeFromParent•
(Ljavax/swing/tree/MutableTreeNode;)V•
getText•
getUserObject•
getChild•
(Ljava/lang/Object;I)Ljava/lang/Object;•
getChildCount•
(Ljava/lang/Object;)I•
getRoot•
getModel•
()Ljavax/swing/tree/TreeModel;•
class com.bifit.swing.tree.XTree•
getComponent•
(I)Ljava/awt/Component;•
()Ljava/lang/Object;•
getComponentCount•
()I•
javax/swing/text/JTextComponent•
javax/swing/JLabel•
prepareRenderer•
(Ljavax/swing/table/TableCellRenderer;II)Ljava/awt/Component;•
getCellRenderer•
(II)Ljavax/swing/table/TableCellRenderer;•
getContentPane•
()Ljava/awt/Container;•
SUM•
(I)Ljava/lang/String;•
%.02f•
repaint•
setText•
(Ljava/lang/String;)V•
class javax.swing.JLabel•
fireTableDataChanged•
(I)Ljava/lang/Object;•
getRowCount•
getColumnCount•
()Ljavax/swing/table/TableModel;•
class com.bifit.swing.table.Table•
```

Методы Java, отслеживаемые Ranbyus.

Источник:
Блог компании ESET NOD32
http://habrahabr.ru

Anonymous взломали сайт Национальной ассоциации Федеральных агентов США

Активисты хакерской группировки Anonymous взломали официальный сайт Национальной ассоциации Федеральных агентов США (National Association of Federal Agents). По имеющейся информации, сайт federalagents.org был взломан Anonymous в рамках операции OpLastResort.

Хакеры "обезобразили" главную страницу сайта (фактически заменив её).

Судя по всему, данная акция также является частью начатой ранее операции #FFF.

В минувший четверг Anonymous взяли на себя ответственность за сбой в работе сайта FedCenter.gov, но до сих пор нет никаких сведений, подтверждающих, что DDoS-атака на FedCenter.gov является частью OpLastResort.

Немногим ранее, в рамках операции OpLastResort, активисты Anonymous взломали сайты инвестиционной компании George K. Baum and Company и Госдепартамента США.

OpLastResort началась вскоре после самоубийства Аарона Шварца (Aaron Swartz), интернет-бизнесмена и политического активиста, выступавшего за свободу информации в сети Интернет. Как известно, федеральные власти США обвинили Шварца во взломе сети Массачусетского технологического института (MIT) и краже более чем 4 млн. статей.

Источник: http://www.anti-malware.ru

Новый магазин взломанных Paypal-аккаунтов

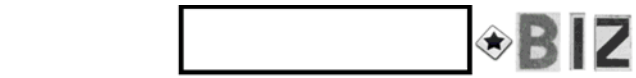
Специалист по безопасности Данчо Данчев из компании Webroot сообщил об открытии интернет-магазина аккаунтов Paypal, доступ к которым осуществляется через прокси-сервер Socks5, то есть через чей-то другой заражённый компьютер.

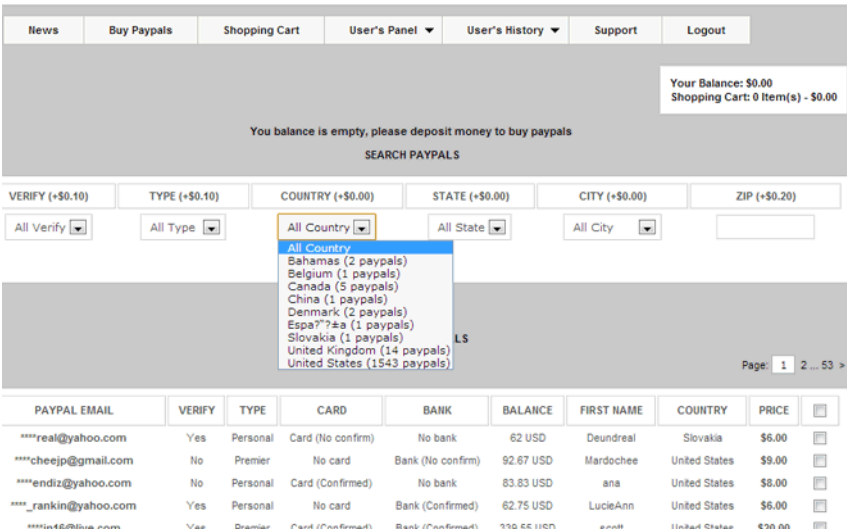
Покупателю предлагают на выбор список жертв. Для каждого указан текущий баланс, место жительства владельца, тип аккаунта и его стоимость.

Аккаунты с минимальным балансом продаются обычно по 3 доллара, аккаунты с балансом в сотни долларов продаются по 15-20 долларов. Очевидно, злоумышленники боятся заниматься обналичкой самостоятельно, потому что это очень рискованное занятие. Они предпочитают просто продать аккаунты, практически наверняка сохранив анонимность.

В данный момент на продажу выставлено более 1500 взломанных аккаунтов, абсолютное большинство из которых принадлежит гражданам США.

Источник: http://www.xakep.ru





Вслед за Apple и Facebook хакеры атаковали Microsoft.

Пока в США пытаются выяснить, откуда родом хакеры, обвиняют во всем китайцев, те продолжают спокойно свою работу. Кто на этот раз стал жертвой неизвестных и таинственных хакеров, какую информацию им удалось украсть на этот раз выясняли эксперты отдела новости США издания для инвесторов «Биржевой Лидер».

Со слов представителей Microsoft стало известно, что определенное количество персональных компьютеров корпорации заражены были вредоносной программой. Когда конкретно предпринята была кибератака, информации нет. В то же самое время, работники Microsoft заверили, что указаний на какое-то повреждение или же хищение информации клиентов фирмы не было, пишут РИА новости.

СМИ отмечают и тот факт, что софтверная корпорация Microsoft сразу после предприятия Apple, а также социальной сети Facebook накануне сообщила о "недавней" кибератаке на свои персональные компьютеры, сообщило ночью агентство Рейтер.

Также со слов представителей Microsoft, определенное число личных компьютеров предприятия заражены были вредоносной программой. Когда конкретно предпринята была кибератака, информации пока нети. В то же самое время, в Microsoft уверены, что нет причин для особого беспокойства, так как не замечено каких-либо повреждений или хищений информации пользователей фирмы.

Такого рода кибератаки для Microsoft и иных фирм, которым приходится бороться с настойчивыми и решительными злоумышленниками, неудивительны, — говорит представитель руководства фирмы Microsoft Мэтт Томлинсон.

Как сообщали ранее эксперты «Биржевого Лидера», в конце минувшего месяца — начале текущего о моментах, связанных с несанкционированным доступом к своим внутренним серверам заявил целый ряд американских фирм, СМИ, учреждений, таких как издание New York Times, Wall Street Journal и Washington Post, предприятие Apple, социальные сети Twitter (подр. «Кибератака на Twitter – похищены данные четверти миллиона пользователей»)и Facebook, а также несколько ведомств и министерств. В кибератаках СМИ США обвинили хакеров из Китая. Правительство Китая назвали обвинения совершенно безосновательными (подр. «Хакеры атаковали внутреннюю сеть Apple. Подозревают китайцев» и «Bloomberg: Атаку на Apple, Facebook и Twitter совершили из Восточной Европы»).

Ранее агентство Ассошиэйтед Пресс со ссылкой на собственные источники сообщило, что правительство США рассмотрит возможность введения торговых санкций против Китая, если подтвердится, что кибератаки на американские предприятия и учреждения осуществляются при официальной поддержке Пекина.

Источник: http://www.anti-malware.ru

2013 год станет годом DDoS-атак

Аналитическая компания Gartner утверждает, что в 2013 году количество и качество DDoS-атак существенно возрастет.

По мнению экспертов компании по анализу сетевой безопасности, DDoS-атаки на приложения составят 25% всех Кибератак в 2013 году. Кроме того, их сложность и комплексность неустанно будут расти.

В частности, под наибольшей угрозой окажутся финансовые организации и компании, занимающиеся интернет-торговлей, выяснила Gartner в ходе своего исследования. Вредоносное программное обеспечение будет блокировать приложения жертв, и даже останавливать работу процессора устройства.

Помимо этого, аналитики установили,

что мощность DDoS-атак возрасла в несколько десятков раз. В частности, во второй половине 2012 года DDoS-атаки на ряд американских банков имели мощность до 70 Гб в секунду. В то же время, годом ранее сила атак не превышала 5 Гб в секунду. Впрочем, даже этого показателя было достаточно, чтобы полностью парализовать работу, скажем, банковского сайта. В будущем же мощность нападений будет только расти.

Наиболее популярной целью DDoS-атак становится отвлечение внимания сотрудников службы информационной безопасности компании-жертвы, в то время, как основной удар приходится на счета клиентов или архивы данных. А самым уязвимым звеном в системе информационной безопасности по-прежнему остается человеческий фактор.

Источник: http://www.imena.ua

Check Point опубликовала отчет по безопасности-2013

Компания Check Point, опубликовала обширное исследование «Отчет по безопасности-2013», раскрывающее наиболее серьезные риски, с которыми в настоящее время сталкиваются организации во всем мире. В нем освещаются основные угрозы безопасности, веб-приложения, работа с которыми может подвергнуть рискам корпоративные сети, а также случаи утечки данных из-за непреднамеренных действий сотрудников.

В ходе развертывания начавшейся в 2012 году между хакерами и ИТ-специалистами «гонки вооружений» стало ясно, что многие серьезные угрозы оставались скрытыми от сетевых администраторов. Эти угрозы связаны с тем, что злоумышленники постоянно придумывают все новые и новые способы кибервзлома, а также с беспечным поведением в интернете собственных сотрудников, которые, сами того не желая, делают корпоративные сети уязвимыми. Прежде, чем приступить к разработке эффективного плана защиты безопасности, организации должны изучить и полностью понять процессы, происходящие в их сетях.

Основанный на данных почти 900 компаний, Отчет по безопасности-2013 компании Check Point проливает свет на то, что скрывается в корпоративных сетях, и на те риски, которым организации подвергаются ежедневно:

Скрытые угрозы безопасности

В этом году интенсивность кибератак в любых проявлениях, от криминального ПО до социально-политического хактивизма, только возрастет, и это касается всех организаций, от крупных до самых малых. Результаты исследования показали, что корпоративные сети 63% организаций подвергались атакам ботов, а более половины – воздействию вредоносного ПО не реже одного раза в день. В Отчете приводится перечень опаснейших угроз, включая широко известные ботнеты, перечень вредоносных программ (по странам), самые распространенные слабые места в системах (по хпроизводителям), статистика случаев атак типа внедрения SQL-кода (по странам), а также другие данные, полученные в ходе исследования.

Небезопасные веб-приложения 2.0

Стремительное распространение приложений веб 2.0 раскрыло перед хакерами беспрецедентные возможности проникновения в корпоративные сети. Исследование показало, что 91% организаций используют потенциально небезопасные приложения. Эти приложения всесторонне освещаются в Отчете, включая частоту и области применения анонимайзеров, P2P-приложений, ресурсов и программ для хранения и совместного использования файлов и наиболее популярных социальных сетей, каждое из которых может открыть лазейку к корпоративным сетям.

Утечка данных

Сегодня корпоративная информация стала доступнее и мобильнее, чем когда-

либо, а это чревато потерей или утечкой данных. Более чем в половине исследуемых организаций был хотя бы один случай потенциальной потери данных. В Отчете описываются различные группы данных, наиболее подверженных риску потери и утечки, включая информацию о платежных картах. В нем также перечислены отрасли, наиболее подверженные этим рискам утечки.

«Наше исследование выявило многочисленные слабые места и угрозы безопасности сетей, о которых большинство организаций не имело представления, — говорит Амнон Бар-Лев (Amnon Bar-Lev), президент компании Check Point Software Technologies. — Осведомленность о них поможет ИТ-специалистам создать план защиты компаний от непрерывного потока постоянно меняющихся угроз, ведущих к утечке данных: от ботнетов до использования сотрудниками веб-приложений, например анонимайзеров».

«Отчет по безопасности-2013 компании Check Point — это призыв к действию, позволяющий оценить серьезность и масштабы существующих и грядущих угроз, — говорит Альберто Досаль (Alberto Dosal), председатель совета директоров Compuquip Technologies, одного из крупнейших в Южной Флориде поставщиков универсальных ИТ-услуг. — Это поистине впечатляющее и полное руководство для любого менеджера высшего звена».

Источник: http://www.anti-malware.ru

В Киеве задержали мошенников, воровавших деньги с благотворительных счетов

В ходе совместной операции службы безопасности “ПриватБанка” и сотрудников управления борьбы с киберпреступностью ГУ МВД в Киевской области был задержан организатор мошеннической группы, которая на протяжении нескольких месяцев обманным путём получала доступ к благотворительным счетам граждан.

Под предлогом перевода крупной суммы денег преступники получали от владельцев карт секретные данные и пароли банков, с помощью которых снимали средства через Интернет. Как сообщили в банке, задержанному 35-летнему К. предъявлено обвинения по фактам мошеннических действий с банковскими счетами 20 граждан Украины, большая часть которых использовалось для сбора денег на лечение тяжелобольных детей.

“Слаженные действия банкиров и милиции помогли задержать преступника с поличным, сегодня он находится под арестом, а остальные члены преступной группы в розыске, – говорит руководитель Службы безопасности ПриватБанка Станислав Крижановский”.

По предварительным данным, ущерб от деятельности преступников составил свыше 100 тысяч гривень.

Напоминаем, что нельзя сообщать посторонним секретные данные своих карт или счетов. Если к Вам обратились с просьбой продиктовать ПИН-код или CVV, сразу обратитесь в банк, это сигнал что Вы могли стать целью мошенников. Кроме того, если у вас случайно перестал работать мобильный – срочно обратитесь к оператору, а также сообщите в банк и временно заблокируйте карты.

Источник: http://www.imena.ua

МВД отчиталось о борьбе с киберпреступностью

Милицейские борцы с киберпреступностью отчитались о текущей ситуации в сфере онлайн-мошенничеств и интернет-преступлений.

С начала 2013 года сотрудники Управления борьбы с киберпреступностью (УБК) МВД Украины выявили 23 факта несанкционированного списания денег с банковских счетов юрлиц на более 12,5 млн грн. Совместно с Госфинмониторингом и банкирами потерпевшим удалось вернуть почти 9,2 млн грн. Об этом заявил руководитель управления Максим Литвинов.

Также он рассказал про похищение с карточных счетов средств, предназначенных на лечение тяжелобольных детей. Участники преступной группы искали в СМИ объявления. Получив необходимые данные, звонили родителям больных детей и под предлогом желания перечислить определенную сумму денег, просили сообщить данные их карточного счета, в том числе и код банковской карты. Далее, манипулируя средствами, которые находились на счету, злоумышленники переводили наличные денежные средства потерпевшего на собственный счет. Пока известно, что таким образом было украдено почти 100 тыс. грн. Интернет-мошенника выявили сотрудники УБК киевской областной милиции, говорится в сообщении МВД Украины.

Максим Литвинов отметил, что треть преступлений, совершаемых с помощью сети интернет, связаны с распространением порнографии. В настоящее время открыто 148 уголовных производств, связанных с созданием, сбытом и распространением порнопродукции, в том числе детской порнографии в Интернете. Подозреваемыми по этим делам проходят 22 человека, под стражей содержатся 2 человека. Изъяты 154 единицы компьютерной техники и других предметов, которые использовались преступниками, а также деньги и матценности на общую сумму более 200 тыс. грн.

По его словам, раскрывать онлайн-мошенничества достаточно сложно, поскольку злоумышленники легко уничтожают свои следы. «Сейчас обсуждаем вопросы технического обеспечения службы – нам нужен хотя бы такой же арсенал техсредств, которыми пользуются интернет – мошенники», – добавил Максим Литвинов.

Источник: http://www.imena.ua

Компания Panda выпустила новую версию бесплатного антивируса

Аналитика, обзоры, рекомендации.

Компания Panda Security выпустила обновление для своего продукта Panda Cloud Antivirus Free 2.1.1, бесплатного «облачного» антивируса для операционной системы Windows. Ключевым нововведением, представленным в новой версии, яв-

ляется расширенная совместимость продукта с Windows 8.

Антивирусный движок, лежащий в основе Panda Cloud Antivirus, использует все преимущества современных технологий облачных вычислений. Благодаря этой особенности продукт способен эффективно обнаруживать большинство современных угроз и удалять их с вашего ПК. Стоит отдельно отметить, что антивирус прекрасно справляется в выявлением малоизученных и совсем новых разновидностей вредоносных программ. Успешное прохождение сертификации на совместимость с новой ОС от Microsoft в первую очередь означает, что Panda Cloud Antivirus теперь гарантирует защиту в режиме реального времени приложений, приобретенных в Интернет-магазине Windows Store, передает soft.mail.ru.

Новая версия может похвастаться усовершенствованными механизмами эвристического анализа, а также обеспечит более эффективную защиту от вредоносных программ, использующих уязвимости в установленном ПО, таком как Java, Adobe и Microsoft Office. Пользователям также предстоит оценить возросшую производительность продукта, слегка модифицированный интерфейс и большое количество устраненных ошибое и недочетов. В том числе разработчики устранили «баг», препятствующий открытию консоли управления при определенных условиях.

Panda Cloud Antivirus Free 2.1.1 работает под управлением операционной системы Windows XP и более поздних версий. Копию продукта можно загрузить с сайта разработчика — http://www.cloudantivirus.com/en.

Напомним, что предлагаемый антивирус также доступен в виде коммерческой версии Panda Cloud Antivirus Pro. Пользователи, заплатившие 29,95 долларов, получат в свое распоряжение универсальный межсетевой экран и набор дополнительных защитных механизмов.

Источник: http://www.securelist.com

Криминалистический подход к анализу временных атрибутов файлов в операционной системе семейства Microsoft Windows и файловой системе NTFS

Матвеева Веста Сергеевна
ведущий специалист по компьютерной криминалистике, компания Group-ib

Согласно данным Википедии, типичным персонажем детективного жанра является преступник, который «совершает преступление, заметает следы, пытается противодействовать следствию». Ничего сверхнового из Википедии не узнаешь, но! надо отметить, что немыслимо, чтобы человек, нарушивший закон или совершивший иное общественно опасное деяние не пытался себя спасти путем запутывания следствия или сокрытия следов (исключения, конечно, бывают).

В виртуальном пространстве все немного сложнее в этом плане. До появления реальных случаев расследования компьютерных преступлений и набирающего обороты такого направления в коммерческой области, как: проведение исследований и судебных экспертиз, злоумышленники оставляли множество следов после своей активности во «взломанной» системе. На сегодняшний день техник противодействия криминалистическому исследованию компьютерной информации становится все больше. Об одной из них и пойдет речь в настоящей статье, а также будет приоткрыта завеса тайн компьютерных криминалистов.

Подмена временных атрибутов файлов. Это делают как вручную, переводя системные часы, так и с помощью специальных программ, которых существует достаточное количество. Но интересно то, что эти же функциональные возможности также прописывают у ряда вредоносных программ с целью ввести в заблуждение пользователя и отнести файл скорее к системному, чем к подозрительному. Таким образом, при просмотре свойств файла в ОС будут отображаться подмененные сведения. Но не все так просто с точки зрения криминалистики. Для распознания факта подмены используются особенности файловой системы. Все сведения, которые изложены ниже, справедливы для ОС Microsoft Windows и файловой системы NTFS, как для самого часто встречаемого сочетания ОС и файловой системы.

В файловой системе NTFS временные атрибуты файлов содержатся в файловой записи для каждого файла в главной файловой таблице (далее – MFT). И как ни странно у файла их ровно 8!, а не 3 как мы привыкли. За временные атрибуты отвечает две структуры ***$STANDARD_INFORMATION*** и ***$FILE_NAME***, каждая из которых содержит: дату и время создания файла, последнего изменения файла, последнего доступа к файлу, а также дату и время последнего изменения сведений в файловой записи. На рисунке 1 приведена файловая запись, содержимое которой отображается с помощью ПО «AccessData FTK Imager»:

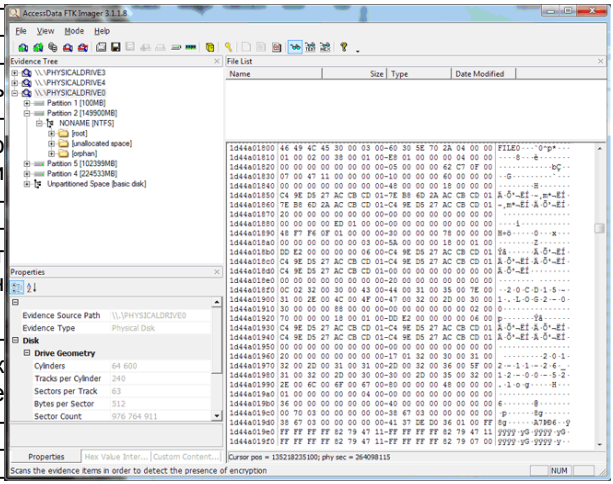


Рисунок 1

Если не вдаваться в подробности смещений упомянутых структур, то их легко распознать по содержимому. Время в данных структурах имеет формат ОС Microsoft Windows, записи которого выглядят так:

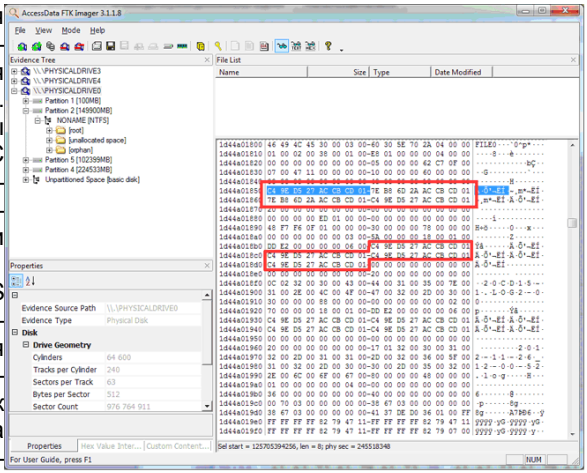


Рисунок 2

Для преобразования временной метки, которая указана в файловой записи, можно использовать специализирован-

ное средство «DCode Date»:

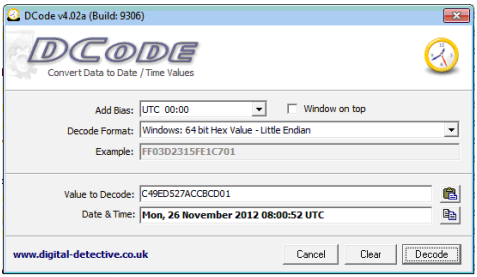


Рисунок 3

или преобразовывать ее вручную.

Однако можно получать доступ ко всем восьми атрибутам с помощью автоматизированных средств анализа: The Sleuth Kit (TSK) по команде «istat»:

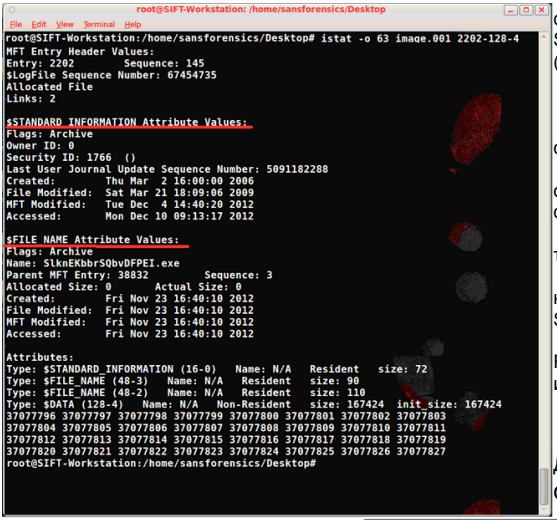


Рисунок 4

или в графическом интерфейсе с помощью ПО «Autopsy Browser».

Ну, а теперь к главному. Правильная оценка временных атрибутов из структур ***$STANDARD_INFORMATION*** и ***$FILE_NAME*** дает криминалисту возможность правильно восстановить хронологию событий, что очень важно при исследовании.

Для начала необходимо представлять, при каких действиях с файлами меняются его атрибуты. Для этого на ОС Microsoft Windows XP и 7 для архитектур процессора x86 и x64 проведена серия тестов, результаты которых сведены в таблицах для текстовых и исполняемых файлов.

Где названия столбцов обозначают следующее:

Rename – переименование файла;
Local Move – перемещение файла в пределах одной файловой системы;
Volume move – перемещение между файловыми системами;
Copy – копирование файла;
Create – создание файла;
Delete – удаление файла;
Open – открытие файла;
Properties – просмотр свойств файла;
Attributes – изменение атрибутов файла;
Modify – изменение файла;

по строкам записаны временные атрибуты файлов, содержащиеся в структурах STANDARD_INFORMATION (SI) и FILE_NAME (FN)

x – изменение атрибута файла;
x(PE) – изменение атрибута только для файлов PE-формата;
x(day) – изменение атрибута производится один раз в день при первом обращении к файлу;
x(?) – замечены случаи изменения атрибута, которые происходят не каждый раз;
(SI) – все сведения в структуре FILE_NAME копируются из предыдущей структуры STANDARD_INFORMATION;
(created) – все атрибуты в структуре FILE_NAME совпадают с датой создания файла из структуры STANDARD_INFORMATION.

В результате подобных тестов с другими форматами файлов и ОС обнаружены незначительные от-

FN	Rename	Local Move	Volume move	Copy	Create	Delete	Open	Properties	Attributes	Modify
Modification	x	x	x	x	x	x				
Accessed	x	x	x	x	x	x				
MFT modified	x	x	x	x	x	x				
Create	x	x	x	x	x	x				
	(SI)		(created)	(created)		(SI)				

SI	Rename	Local Move	Volume move	Copy	Create	Delete	Open	Properties	Attributes	Modify
Modification					x					x
Accessed	x	x	x	x	x	x	x (PE) x(day)	x (PE)	x	x
MFT modified	x	x	x(PE)	x(PE)	x	x	x (PE)	x (PE)	x	x
Create			x	x	x					

Таблица – Windows 7

FN	Rename	Local Move	Volume move	Copy	Create	Delete	Open	Properties	Attributes	Modify
Modification	x	x	x	x	x	x				
Accessed	x	x	x	x	x	x				
MFT modified	x	x	x	x	x	x				
Create	x	x	x	x	x	x				
	(SI)	(SI)	(created)	(created)		(SI)				

SI	Rename	Local Move	Volume move	Copy	Create	Delete	Open	Properties	Attributes	Modify
Modification					x					x
Accessed	x	x	x	x	x	x(?)	x(day)	x(PE)	x	x
MFT modified	x	x		x	x	x			x	x
Create			x	x	x					

личия от приведенных в таблицах.Как видно, данные в структуре ***$FILE_NAME*** создаются в момент создания файла и представляют собой копию даты создания и изменяются при переименовании, локальном перемещении, перемещении между файловыми системами, копировании и удалении файла. Следовательно, сведения в этой структуре не могут превосходить временные атрибуты из структуры ***$STANDARD_INFORMATION***. Но это актуально именно для времени создания и изменения файла. Время последнего доступа к файлу и атрибут MFT modified могут измениться только в структуре ***$STANDARD_INFORMATION***. Поэтому время последнего доступа к файлу следует определять по структуре ***$STANDARD_INFORMATION***. В ОС Microsoft Windows Vista и 7 по умолчанию время последнего доступа не изменяется для экономии ресурсов системы. Указанная опция регулируется значением ключа реестра:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\FileSystem

NtfsDisableLastAccessUpdate = 1 (дата и время последнего доступа к файлу не изменяются при доступе к файлу) = 0 (дата и время последнего доступа к файлу изменяются при доступе к файлу)

В таблицах приведены результаты испытаний с опцией изменения даты последнего доступа при обращении к файлу.

Атрибут MFT modified изменяется, когда хотя быть один атрибут файловой записи меняется. Но в силу времени разрешения (time resolution) файловой системы NTFS, которое составляет до 1 часа, сведения о последнем доступе к файлу сначала сохраняются в оперативную память, а затем записываются в файловую запись. Следовательно, небольшие расхождения в этих атрибутах могут быть. Но, стоит отметить, что при изменении атрибута Accessed атрибут MFT modified меняется не всегда.

В связи с описанными оговорками разберем подход криминалиста при проведении исследования НЖМД, который был задействован при совершении мошеннической операции в системе интернет-банкинга на стороне клиента.

Ниже, на рисунке 5 приведены временные атрибуты вредоносной программы семейства «Trojan.Carberp». Такие программы часто встречаются в подобных инцидентах, так как позволяют производить скрытое от пользователя копирование данных, необходимых для аутентификации в системах дистанционного банковского обслуживания. Такие программы имеют функциональную возможность изменять временные атрибуты, отображаемые пользователю, на идентичные для системных файлов.

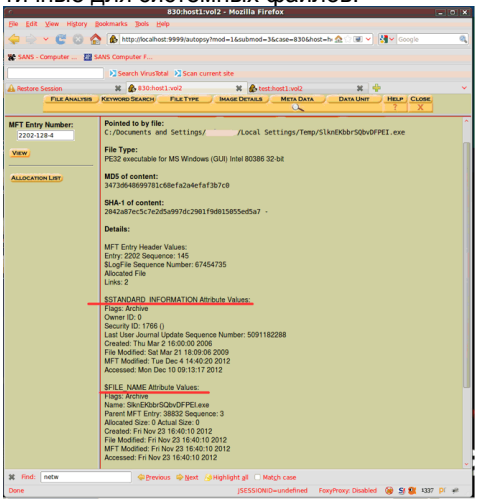


Рисунок 5

При восстановлении хронологии событий очень важным аспектом является правильное определение времени загрузки вредоносной программы. Попробуем применить полученные в данной статье сведения для определения временных атрибутов файла «SlknEKbbrSQbvDFPEI.exe».Так как атрибуты в структуре ***$FILE_NAME*** не могут превосходить атрибуты в структуре ***$STANDARD_INFORMATION***, то датой создания файла признается: 23.11.2012 г. 16:40:10. Оригинальная дата изменения файла при этом неизвестна, так как в структуре ***$STANDARD_INFORMATION*** она подменена, а в ***$FILE_NAME*** – является копией даты и времени создания файла, которая была сохранена в файловую запись при создании файла. Дата и время последнего доступа определяется из структуры ***$STANDARD_INFORMATION*** – 10.12.2012 г. 09:13:17. Сведения в файло-

вой записи изменялись последний раз 04.12.2012 г. 14:40:20 в соответствии с атрибутом MFT modified, который не изменялся при доступе к файлу.

Таким образом, в следствие ручного анализа можно выявить верные временные атрибуты файла, что является достаточно трудоемким занятием, если количество файлов большое. Поэтому ниже приводится псевдокод, который позволяет автоматизировать процесс определения временных атрибутов файла, принимая на вход данные структур ***$STANDARD_INFORMATION*** и ***$FILE_NAME*** (дата и время последнего изменения файла при подмене атрибутов берется из структуры ***$FILE_NAME***):

```
SI=null; // структура $STANDARD_INFORMATION
FN=null; // структура $FILE_NAME
Result=null; // структура реальных атрибутов

SI=receive_standard_information(file);
FN=receive_file_name(file);
If (SI!=0 and FN!=null)
{
Result.Created = FN.Created
If (SI.Modified < FN.Modified)
{
If (FN.Modified == SI.Created)
{
Result.Modified = SI.Modified
writeline ("The file was copied")
}
else Result.Modified = FN.Modified
}
else Result.Modified = SI.Modified
If (SI.Accessed < FN.Accessed) Result.Accessed =
FN.Accessed
else
{
Result.Accessed = SI.Accessed
}
If (SI.MFT_modified < FN.MFT_modified)
Result.MFT_modified = FN.MFT_modified
Else Result.MFT_modified = SI.MFT_modified

If (Result.Created > Result.Modified) writeline ("The
file was copied to the OS")
}
```

Тонкостей в определении временных атрибутов файлов очень много. Но главное, что хотелось донести в этой статье, является идея о том, что по временным атрибутам файла можно восстановить даже действия, которые были произведены с файлами, что и помогает компьютерным криминалистам при проведении исследований и судебных экспертиз.

Источник: http://www.xakep.ru

Raspberry Pi автоматически собирает парольные хэши в локальной сети

В журнале «Хакер» неоднократно публиковались обзоры устройства типа AutoPwn, которые автоматически перехватывают трафик и собирают пароли в локальной сети. Достаточно принести такое устройств в офис и незаметно воткнуть где-нибудь в свободную розетку.

Был всего лишь вопрос времени, когда автоматический сборщик паролей сделают на основе миниатюрного компьютера Raspberry Pi. Вполне логичный выбор, учитывая популярность и дешевизну компьютера за 25-35 долларов.

Один из хакеров соорудил устройство, которое автоматически осуществляет атаку по протоколу Web Proxy Auto-Discovery Protocol (WPAD) на сервис NBNS (Netbios Name Service). Это позволяет подделать ответы NBNS на запросы, рассылаемые с каждого Windows-компьютера в локальной сети. После подделки ответа мы можем запустить модуль Metasploit и поднять несколько фальшивых сервисов, к которым могут подключиться наши Windows-компьютеры, ищущие соединения. При попытке подключения к сервису в локальной сети каждый Windows-компьютер автоматически постарается аутентифицироваться и пришлёт свои учётные данные в хэшированном виде. Это могут старые простенькие хэши LM, они ломаются в считанные минуты, или более сложные хэши NTLMv2, которые тоже можно брутфорсить.

Если вы не знакомы с концепцией, подробнее о концепции сбора паролей в локальной сети с помощью спуфинга NBNS см. http://www.packetstan.com.

Цель была сделать устройство, которое автоматически осуществляет атаку, описанную в упомянутой статье. То есть мы делаем на основе Raspberry Pi автоматический сборщик парольных хэшей — он подключается в локальную сеть, поднимает фальшивые сервисы и ждёт, когда все компьютеры под Windows попытаются в них авторизоваться.

Для запуска Ruby и Metasploit на Raspberry Pi можно поставить дистрибутив Raspbian или Raspberry-Pwn.

Источник: http://www.xakep.ru

Facebook и Twitter стали главными целями интернет-мошенников

Компания GFI Software недавно выпустила отчет VIPRE за январь 2013 года. Исследование в основном сосредоточено на кибер-атаках, которые портят жизнь пользователям популярных социальных сетей Twitter, Facebook или LinkedIn. В основном, как показывают данные, нападения производятся с целью одурачить пользователей и вытянуть из них деньги.

Среди наиболее интересных афер, которые распространялись по Facebook в январе 2013, специалисты называют ту, во время которой пользователям рассылалось сообщение, оповещающее о том их учетные записи «нарушают определенные правила поведения в Facebook». После этого жертв просили передать свою информацию в Facebook, включая логин и некоторые личные данные.

На Twitter также развернулась одна неприятная афера. Злоумышленники рассылали прямые сообщения, которые уведомляли пользователей в том, что о них распространяли неприятные сообщения. Те, кто клацали на ссылку, ведущую к сообщениям, попадали на фальшивую страницу Twitter, где их просили вновь зайти на сайт. Дальше злоумышленники шли по накатанной схеме и выуживали из клиентов личные данные.

Что касается вредоносного программного обеспечения, то тут доминирует троян Win32.Generic!BT (24,87%). За ним следует Sirefef (3,25%). Плагин для браузера GamePlayLabs и некоторые рекламные программы вроде Yontoo, Wajam и Wajam (fs) также были освещены в январском отчете, попав в десятку самых распространенных угроз.

«С проникновением крупнейших социальных сетей в наши жизни, их ценность для киберпреступников значительно повышается. Они начинают искать новые способы замаскировать свои нападения», – говорит Кристофер Бойд – старший аналитик по сетевым угрозам в GFI¸ – «*Сосредоточив свои усилия на этих сайтах, преступники повышают шансы обмануть большее количество пользователей. Они заставляют жертв скачивать вредоносное программное обеспечение на компьютеры и на мобильные устройства. Через взломанные учетные записи, злоумышленники получают возможность захватить еще большее количество жертв*».

Detection	Type	Percent
Trojan.Win32.Generic	Trojan	35.1
Yontoo (v)	Adware	2.23
FraudTool.Win32.FakeRean	Rogue Security Program	1.62
INF.Autorun (v)	Trojan	1.28
Trojan.Win32.FakeAV.mqa (v)	Trojan	1.21
Trojan.Win32.Ramnit.c (v)	Trojan	0.94
Exploit.PDF-JS.Gen (v)	Exploit	0.86
GameVance (fs)	Adware	0.82
Pinball Corporation. (v)	Adware	0.79
Trojan.Win32.Jpgiframe (v)	Trojan	0.77

Самые распространенные угрозы в январе 2013 года.

Ознакомиться с подробностями отчета VIPRE за январь 2013 года можно на официальной странице компании.

Источник: http://www.anti-malware.ru

Аналитика, обзоры, рекомендации.

user And LINUX

{ Secure Shell }

Тут может быть Ваша информация!

Заявите о себе!

И про Вас узнают Все...

{
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.