UA Linux
http://ualinux.com
Аналитика, обзоры, рекомендации.

user And LINUX
{ Secure Shell }

Читайте в этом номере:

Итоги проекта «Доктор Веб» по борьбе с банковскими троянцами

Компания «Доктор Веб» подводит итоги просветительского проекта по борьбе с банковскими троянцами. За три недели с момента запуска проект посетили более 820 тысяч пользователей.

Огромный интерес проявили как представители малого, среднего и крупного бизнеса, так и простые пользователи, заботящиеся о сохранности собственных денежных средств. Оказалось, что многие знают, насколько коварны вредоносные программы, но не все представляют, с помощью каких ресурсов они распространяются.

В рамках проекта участникам предлагалось пройти краткий тест, состоящий из пяти вопросов об угрозах со стороны новых банковских троянцев. Каждый вопрос сопровождался информационной справкой. Интересно, что самым легким для участников оказался вопрос о времени, которое необходимо известному троянцу Trojan.Carberp для похищения паролей и денежных средств со счета жертвы. Правильный ответ — 1–3 минуты — дали почти все пользователи, а именно 84%.

Вторым по числу правильных ответов — 78% — оказался вопрос о виновниках того, что новые вирусы не всегда сразу обнаруживаются антивирусными программами. И в этом действительно виноваты вирусописатели. Ведь каждый час появляются тысячи вирусов, так что антивирус не может знать их все: ежесуточно в антивирусную лабораторию «Доктор Веб» поступает в среднем не менее 60 тысяч образцов вредоносных программ, а в ноябре 2012 года был поставлен своеобразный «рекорд» — за 24 часа на анализ поступило более 300 тысяч файлов. Большинство участников, а именно 72%, знают и о максимальном сроке наказания для компьютерных мошенников за хищение денежных средств — до 10 лет.

Главным и самым печальным итогом стала статистика верных ответов на один из важнейших вопросов: при посещении каких сайтов можно чаще всего заразиться вредоносным ПО. 66% участников ответили неверно на этот вопрос, основываясь на господствующем в обществе ошибочном мнении: главная площадка для вредоносных программ — порнографические сайты. На самом же деле чаще всего источниками вредоносного ПО являются сайты, посвященные технологиям и телекоммуникациям, а также бизнес-порталы. Сайты для взрослых занимают только третье место в списке вредоносных ресурсов. Неудивительно, что количество зараженных ПК только растет, ведь, по данным статистики сканирований лечащей утилиты Dr.Web CureIt!, приблизительно 60% домашних компьютеров не имеют никакой защиты.

Источник: http://www.chip.ua

В Испании пойманы кибермошенники из РФ, Украины и Грузии

Испанские власти вместе с европейским полицейским ведомством (Европол) раскрыли сеть киберпреступников, получавших миллионные прибыли благодаря рассылке вирусов-вымогателей на десятки тысяч компьютеров по всему миру.

По подозрению в причастности к кибергруппировке испанские власти арестовали 11 человек, включая шестерых граждан России, двух граждан Украины и двух выходцев из Грузии.

Главой кибергруппировки, по данным Европола, вероятно являлся 27-летний россиянин, который отвечал за "создание, развитие и международное распространение различных версий вируса-вымогателя". Он был арестован в ОАЭ и в настоящее время ждет экстрадицию в Испанию.

Как сообщает европейское полицейское ведомство, предполагаемые преступники заражали компьютеры вирусом, который затем обвинял пользователей в просмотре нелегального контента, в частности, детской порнографии. После этого адресатам сообщений говорилось, что они должны уплатить штраф, прежде чем смогут вновь воспользоваться своим компьютером.

Фальшивые полицейские

В официальном заявлении Европола говорится: "Маскируя вредоносное программное обеспечение под сообщения от правоохранительных органов, киберпреступники убеждали своих жертв заплатить штраф в размере 100 евро (130 долларов) двумя способами оплаты на выбор через виртуальные анонимные шлюзы в качестве наказания за предполагаемое нарушение".

Сообщения незадачливому пользователю приходили якобы от имени Европола или местной полиции.

Получив деньги, киберпреступники продолжали незаметно красть информацию с компьютера жертвы.

"С момента обнаружения вируса в мае 2011 года в одной лишь Испании было зафиксировано более 1200 подобных случаев, при том что число жертв [киберпреступников] может быть выше", - говорится в заявлении европейской полиции.

Следователи из новой структуры Европола - Европейского центра по борьбе с киберпреступностью - заявили, что сеть киберпреступников заразила вредоносной программой "десятки тысяч" компьютеров по всему миру.

По оценкам Европола, прибыль кибергруппировки может составлять около миллиона евро в год.

Предполагаемые преступники получали деньги разными способами, включая использование электронных пиринговых платежных систем, подобных Bitcoin.

Они также подозреваются в использовании испанских банкоматов для снятия средств со взломанных кредитных карт. В частности, около 26 тысяч евро были сняты с одной из подобных карт незадолго до ареста подозреваемых.

Источник: http://www.bbc.co.uk

Никогда не кидай веб-дизайнера!

По адресу fitnesssf.com сейчас можно наблюдать забавную картину. Вместо нового сайта компании FitnessSF там опубликовано обращение к клиентам от имени некоего Фрэнка Джонена.

Фрэнк Джонен — простой американский дизайнер, и его грубо кинули с оплатой за сайт. Он сделал то, что мечтают сделать многие фрилансеры с сайтом заказчика, который ведёт себе нечестно.

На «взломанном» сайте дизайнер просит прощения у всех за вызванные неудобства — и подробно объясняет ситуацию. Естественно, симпатии публики на стороне «кинутого» фрилансера. История уже вызвала широкий резонанс в прессе, а компания FitnessSF вынуждена оправдываться, почему она не заплатила Фрэнку.

Источник: http://www.xakep.ru

UA Linux
open source open future
Эксперт в области безопасности.

The Pirate Bay угрожает засудить антипиратский сайт за воровство своего дизайна

Финская антипиратская организация CIAPC прославилась на весь мир в ноябре прошлого года, когда у 9-летней девочки конфисковали ноутбук с Вини-Пухом — ноутбук был уликой по иску за скачивание нелицензионной музыки из интернета. Девочка нашла через Google последний альбом своей любимой певицы Кису и скачала mp3-файлы через торрент-трекер The Pirate Bay. История закончилась благополучно: ноутбук девочке вернули, но осадок остался.

Сейчас финская антипиратская группа CIAPC опять заявила о себе. Она запустила сайтPiraattilahti.fi (The Pirate Bay на финском языке), на котором полностью скопировала дизайн и HTML-код оригинального сайта The Pirate Bay, с одним отличием. Вместо логотипа с плывущим по волнам парусником они изобразили тонущий корабль.

Владельцы торрент-трекера The Pirate Bay отреагировали на этот инцидент со свойственным им сарказмом: «Мы возмущены таким поведением. Люди должны понимать, что можно делать, а что нельзя. Кража таких материалов в интернете представляет угрозу для экономики всего мира», — сказал представитель сайта The Pirate Bay в интервью изданию Torrent Freak. Он добавил, что в таких условиях они могут подать судебный иск против нарушителя, которому грозит штраф до 5000 евро за нарушение пользовательского соглашения и возмещение дополнительных расходов, таких как расходы на трафик и т.д.

Источник: http://www.xakep.ru

Вы работаете в области информационной безопасности.

Это место для Вас!

UA Linux
http://ualinux.com
Эксперт в области безопасности.

«Медовые ловушки» в интернете

«Медовой ловушкой» в профессиональной среде разведчиков называется использование сексуально привлекательной девушки или молодого человека, для того чтобы добыть у вражеского агента требуемую информацию или шантажировать его в интересах спецслужб.

Жизнь рядового пользователя, конечно, не похожа на полную загадок и опасностей жизнь резидента, однако и ему следует быть внимательным. Многочисленные мошенники, брачные аферисты и прочие сомнительные личности используют в своих неблаговидных целях стремление человека найти свою пару. Такого рода злоумышленники давно уже облюбовали интернет — они расставляют свои сети на веб-страницах, в рекламных объявлениях и даже забрасывают их прямо в почтовые ящики. Так что виртуальные «медовые ловушки» не редкость и на просторах Всемирной паутины, а поддавшись минутному увлечению, можно не только заразить компьютер вредоносной программой, но и потерять деньги…

Приятное знакомство?

Сайты знакомств давно заняли свою нишу во Всемирной паутине. Количество пользователей, зарегистрированных на самых крупных ресурсах такого рода (match.com, badoo.com mamba.ru, loveplanet.ru), исчисляется миллионами. Конечно, такая популярность интернет-знакомств не могла не привлечь внимания злоумышленников.

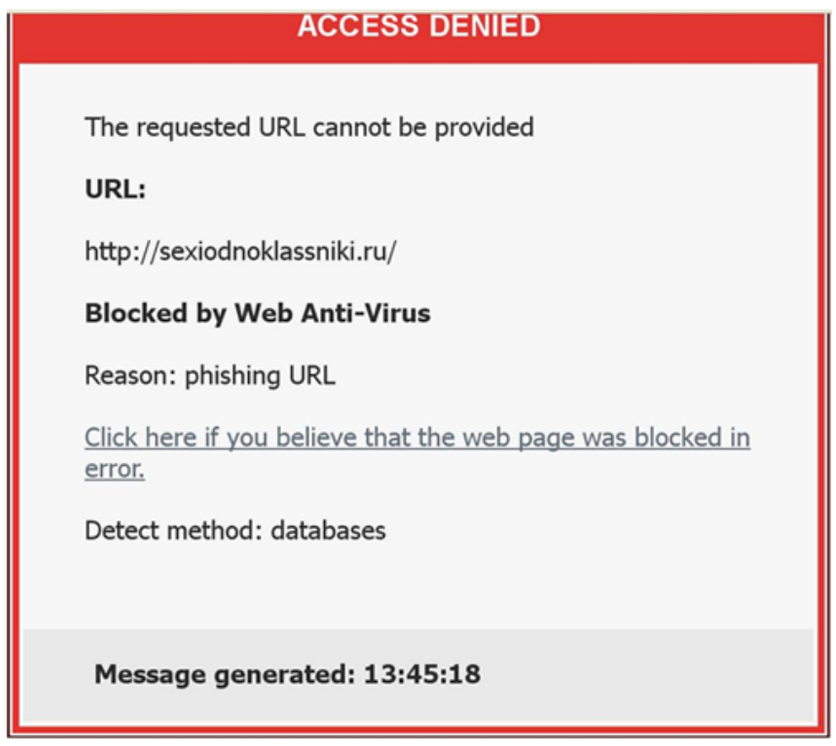
Спамовые письма, в которых предлагается «познакомиться с приятной молодой девушкой» или просто «встретиться на одну ночь», стали попадать в наши ловушки довольно часто. Разумеется, никакого отношения к крупным порталам знакомств они не имеют. Если приличные ресурсы, заботясь о своей репутации, регулярно проверяют своих пользователей, то в спаме, наоборот, подчеркивается, что регистрация на рекламируемых сайтах не обязательна. Пройдя по ссылке из такого письма, пользователь рискует нанести урон своему компьютеру – вместо фотографий прекрасной незнакомки, на компьютер, как правило, начинает подгружаться вредоносное ПО.

Вот одно из писем с рекламой сайта знакомств:

From: Лаура
Subject: Интим Mamba – сладкие знакомства!
Поиск новых знакомств с целью дружбы и серьезных отношений, а также попутчиков. Возможность назначать свидания. Онлайн-игры, приложения для общения и флирта, рейтинг фотографий. Регистрируйтесь, начинайте знакомиться и получать удовольствие от общения» Кто-то ждем именно Вас прямо сейчас! Это место, где осуществятся Ваши желания!
{LINK} *******.5ballov.ru***

Ссылка в этом письме вела на зараженную веб-страницу:

Еще одна опасность – фишинговые атаки. Так, например, в последнее время пользователи Рунета получали письма с приглашением посетить сайты «для взрослых», якобы созданные специально для пользователей социальной сети odnoklassniki.ru (их название нередко пародировало название этой сети: odnopostelniki, odnokrovatniki).



Чтобы зайти на такой сайт, пользователю надо было воспользоваться своим логином и паролем к сети Одноклассники. Все такие сайты оказались фишинговыми - мошенники использовали их как приманку, чтобы заполучить аккаунты пользователей популярного социального ресурса.

Кроме того, в ряде случаев посетителю сайта знакомств при регистрации предлагается указывать номер телефона, а это чревато для пользователя потоком спама, на этот раз мобильного.

Дело техники

Мошенничество на поддельных сайтах знакомств может сводиться не только к виртуальной опасности, связанной с фишингом или распространением вредоносного ПО. Пострадать могут и финансы излишне доверчивого пользователя.

Охота за кошельком пользователя зачастую идет на веб-страницах, имитирующих стартовые страницы сайтов знакомств. Для регистрации на таком «сайте» или подтверждения своего возраста (старше 18 лет) пользователю нужно отправить SMS сообщение на короткий номер. Отправив платное SMS, любитель или любительница приключений расстается с определенной суммой – от 10 до 350 рублей. Однако после этого никакого доступа к контенту не предоставляется – контента просто нет.

Такие веб-ресурсы, как правило, недолговечны – через несколько недель или даже дней мошеннические страницы, имитирующие стартовые страницы сайтов знакомств, исчезают, или их содержание меняется на типичную спамерскую рекламу (виагра и т.п.).

Мобильный телефон достаточно часто оказывается союзником «медовых» мошенников, порой в ход идут достаточно хитрые приемы. Сравнительно недавно на форумах в интернете стали распространяться сообщения одураченных посетителей сайта знакомств. Они пробовали общаться с авторами анкет с помощью системы мгновенного обмена сообщениями на этом веб-ресурсе, но через некоторое время обнаруживали, что вместо привлекательной девушки им отвечает робот. Вся соль в том, что для отправки каждого сообщения требовалось передать SMS на короткий номер. Таким способом мошенникам за недолгое время удавалось вытянуть из каждого посетителя немалую сумму.

All you need is spam

В любом случае доходы мошеннических сайтов знакомств напрямую зависят от количества пользователей, поэтому борьба за посещаемость ведется любыми средствами. Основным инструментом в этом случае является спам.

Обычно распространители непрошеной рекламы, продвигающие такие веб-ресурсы, используют самые элементарные приемы. Значительное количество «мусорных» писем – это сообщения из двух-трех фраз, снабженные ссылкой на сайт знакомств. Во многих случаях тексты сообщений составляются автоматическими средствами по готовым шаблонам из типовых фраз, что заметно, если просмотреть несколько сообщений подряд. Форматирование – самое простое, графических элементов нет, текст – примитивен и пестрит ошибками: «Бесплатно зарегестрировавшись…», «…заполните не большую анкету». Все, что нужно автору письма, – заманить доверчивого получателя на нужный веб-ресурс, а остальное уже дело техники.

Подобные сообщения широко распространены в спаме почти на всех языках мира. А поскольку качество текстов сообщений оставляет желать лучшего, спамеры компенсируют его количеством: объемы таких рассылок без преувеличения огромны. Расчет недобросовестных рекламщиков прост: хоть кто-нибудь, да клюнет.

Не брезгуют спамеры и более прозаическими заработками: рекламой притонов под видом «саун», рассылкой анкет проституток и т. д.

Сразить наповал

Самая колоритная разновидность спамерских писем, не утратившая своей популярности умошенников за многие годы, – так называемый «нигерийский спам».

В случае романтической разновидности нигерийских писем, помимо массовых спам-рассылок мошенники могут отыскивать потенциальную жертву и среди тех, кто зарегистрировался на сайте знакомств.

Девушка, от имени которой пользователю приходит письмо, как правило, проживает в далекой африканской стране, охваченной беспорядками. В случае если пользователь зарегистрирован на сайте знакомств, практически из первого же письма становится понятно, что девушка без ума в него влюблена. Если письмо распространяется в ходе массовой рассылки, чувства у девушки вспыхивают в ходе переписки, что следует из второго или третьего письма.

Вот одно из спамовых писем, которое в январе было разослано на адреса десятков тысяч пользователей:

Subject: Hello my dearest Friend in mind with hope you are good healthy?

Hello my dearest Friend in mind with hope you are good healthy?
How are you today and your work with hope all is well?
Praise the day. I am very happy to meet you today I know this mail will find you in good health and also surprised, but I believe God has his own way to bring people together considering the fact, we have not know each other in person or even have seeing before, forgive my indignation if this mail comes to you as a surprise and may offend your personality for contacting you without your prior of consent, my name is Nadine Konan Soro, it's my pleasure to contact you today for a serious relationship, I saw your profile today from your Country data base dueling my browsing in the Internet I become interested in you,
I would like us to know ourselves more better I believe we can become a good Friend I like you for being my friend and I also seek advice from you that will help me, My dear, please write back to me so I'll tell you more about myself also send you my picture, Please do not let a humble heart that is lonely and looking for your reply, because friendship is a foundation to build other relatives, Remember that religion does not matter what matter is understanding and sincere matters a lot in life, I believe it's a day human beings use to know each other let makes the world a global village, I will be expecting to hear from you, I wish you happy near year and prosperous new year of the 2013 and prosperity
Have a great new year and remain blessed,
Yours sincere Friend Nadine,

Возлюбленная по переписке может сообщать своему будущему жениху трогательные подробности из своей жизни. Верность невесты гарантируется письмами пастора и адвоката.

Также довольно быстро выясняется, что красавица — еще и наследница миллионного состояния, и она готова отдать все вместе с рукой и сердцем. Чтобы вывести из страны невесту и ее деньги, от будущего мужа требуется лишь определенная сумма на оплату адвокатских услуг. Она может исчисляться тысячами долларов, но все это ни в какое сравнение не идет с миллионами, которые в скором времени должны будут оказаться на банковском счете жениха. Получив деньги, фальшивые красавица, пастор, адвокат и миллионы исчезают.

Такая тактика обычно предполагает длительную переписку, так как мало кто согласится добровольно и по первому же движению сердца расстаться с деньгами. На первые письма претендентов на руку и сердце африканской красавицы отвечают роботы, как только становится понятно, что у мошенников есть шанс поживиться, они сами включаются в переписку. Обработка потенциальной жертвы может идти долго, и здесь важен индивидуальный подход и понимание психологии.

В зависимости от подготовленности преступников, наравне с приемами социальной инженерии в ход могут пойти и попытки получить несанкционированный доступ непосредственно к счету пользователя. Работа мошенниками ведется кропотливая, но она себя оправдывает: куш, который сорвут злоумышленники, достаточно велик по сравнению с доходами от обычного интернет-мошенничества.

Не отстают от своих «коллег» и мошенники, рассылающие письма от имени «русских невест». Такие письма нацелены, в основном, на пользователей стран Западной Европы и США.

Subject: hello

Hey.

I just saw your profile on a dating site. You're an interesting man. And of course I liked you. I'm looking for a good, good and good guy for friendship and possible serious relationship.

I send you my picture. Now do you see what I look like, and I hope that I'm your type.

Reply to my email, if I am interested you.

And do not forget to send me your photos.

В отличие от «нигерийских» невест, «россиянки» — девушки бедные, но гордые, и все надежды возлагают на будущего богатого супруга. Деньги им, как выяснится в ходе переписки, понадобятся, чтобы купить билет на самолет и встретиться, наконец, с мужчиной своей мечты. Ну и от подарков от женихов милые тургеневские барышни тоже не отказываются.

Подчас в голове не укладывается, как разумный человек по собственной воле может оказаться втянутым в такую нелепую историю. Однако, по данным СМИ, количество жертв мошеннических «невест» не убывает, причем для «жениха» такое приключение может закончиться трагично. Два года назад едва ли не весь интернет обошла история гражданина США, который покончил с собой, не дождавшись встречи со своей виртуальной обольстительницей. По непроверенным данным, злоумышленники сообщили ему о том, что его невеста сама совершила самоубийство – но перед этим они сумели получить от него ряд денежных переводов на общую сумму около 50 000 долларов.

Соблюдайте технику безопасности!

Интернет дает прекрасные возможности для общения. Однако, это не самое безопасное виртуальное пространство, в том числе для поиска романтических отношений.

Мы рассказали лишь о малой части многочисленных «медовых ловушек», расставленных в интернете. Чтобы избежать разочарований, соблюдайте основные принципы безопасности:

1. Не посещайте непроверенные сайты знакомств, особенно если они рекламируются в спаме.
2. Не открывайте письма от неизвестных отправителей.
3. Не отвечайте на письма, если они вызывают у вас хоть малейшее подозрение.
4. Не доверяйте излишне щедрым и сомнительным предложениям, даже если эти предложения вам делает прекрасная девушка/мужественный красавец.
5. И последнее, но важное: пользуйтесь надежными средствами для защиты вашего компьютера!

В заключение нам остается только пожелать нашим читателям не попадаться на удочку фальшивых обольстительниц/обольстителей, найти и сберечь свою настоящую любовь.

Источник: http://www.securelist.com

Facebook: где, как и зачем торгуют чужими аккаунтами

В московском представительстве компании Digital Sky Technologies, контролирующей более 5% Facebook, заявили, что "пока воздержатся от комментариев" относительно сообщений о продаже неким хакером логинов и паролей к полутора миллионам аккаунтов пользователей этой социальной сети.

В последние дни в интернете появились сообщения о том, что хакер с ником "Kirllos" предлагает на продажу 1,5 млн аккаунтов пользователей Facebook.

Компания iDefense Labs, входящая в группу VeriSign и занимающаяся обеспечением информационной безопасности, первой обнаружила подобное предложение о продаже и распространила об этом официальное сообщение.

Профайлы с десятью "друзьями" и меньше предлагались за 25 долларов за тысячу аккаунтов, с большим количеством друзей - за 45 долларов. Самый первый пост этого хакера с предложением продать сто тысяч аккаунтов социальной сети датируется 1 февраля 2010 года.

Директор iDefense Labs по информационной безопасности Рик Ховард в интервью bbcrussian.com не исключил, что этот хакер - российского происхождения, поскольку его пост написан на русском языке.

По словам Ховарда, Facebook запросила у iDefense Labs обнаруженную информацию.

Сама Facebook до настоящего момента не ответила на запрос bbcrussian.com о комментарии.

Побочный продукт

Главный редактор журнала "Хакер" Никита Кислицин сомневается, что была взломана сама сеть Facebook.

"Эти данные собраны с большого числа компьютеров, например, в интернет-кафе", - считает он.

Как объясняет Кислицин, хакерские программы считывают все логины и пароли, использованные на взломанном компьютере для авторизации на разных сайтах.

Главный интерес для мошенников представляет финансовая информация, "а побочный продукт - это почтовые аккаунты, социальные сети, все, что под спам используется, вот этот побочный продукт хакер и пытался продать", - пояснил эксперт в интервью Би-би-си.

Facebook - популярный сервис, отмечает Кислицин, и на многих компьютерах можно найти следы авторизации на сайт этой сети.

"1,5 миллиона аккаунтов - это полтора миллиона зараженных компьютеров", - резюмирует он.

Проверить "реальность" аккаунтов, тем более такого большого количества, очень сложно.

"Специфика этого черного рынка такая, что когда люди сомневаются, то есть ряд путей, как обезопасить себя от разных проблем. Например, "гарант" - сервис, когда в сделку вступает третий человек. Он получает сначала часть денег и перепроверяет качество товара, и если качество хорошее, то он передает его покупателю, а деньги - продавцу за вычетом своей комиссии. Вот этот третий человек, - обычно какой-то человек, пользующийся авторитетом в этом сообществе", - объясняет эксперт схему торговли конфиденциальной информацией.

Закрытые продажи

Никита Кислицин называет продажу полутора миллионов аккаунтов через открытый форум "немного странной".

Обычно такие предложения появляются на закрытых хакерских форумах, которые нельзя найти при помощи поиска в Google.

"Работает это в виде закрытого форума с несколькими тысячами участников, с некоей рейтинговой системой каждого участника, по которой можно оценивать и формировать свой уровень доверия к этому участнику, - говорит редактор журнала. - На этом форуме идут обсуждения и осуществляются сделки покупки - продажи товаров и услуг [черного рынка]: начиная от украденных персональных данных и заканчивая какими-нибудь услугами программиста...".

Как отмечают в журнале "Хакер", форумы - явление глобальное.

Обычно сообщения на таких форумах публикуются на двух языках - по основному языку можно предположить, из какого региона основатель ресурса.

Как используют чужой аккаунт

Компания iDefense распространила ранее официальное заявление, в котором также отмечается, что интернет-мошенники все больше "интернационализируются" и все чаще обращаются к международным социальным сетям.

Как отмечает Рик Ховард из iDefense, атаки на социальные сети явление не новое, но ранее они были ограничены каким-то одним регионом, как в случае с сетью "В контакте", популярной в России, Белоруссии и на Украине.

В 2009 году пароли 130 тысяч пользователей "В Контакте" оказались в свободном доступе в интернете.

В заявлении iDefense говорится, что персональная информация, собранная через социальные сети, может быть использована для различных мошеннических операций - например, незаконных денежных переводов и открытия банковских счетов, для рассылки вирусов, спама, оформления фальшивых паспортов, водительских прав и в других преступных целях.

Никита Кислицин из журнала "Хакер" согласен, что пользователи социальных сетей все чаще становятся объектами мошенничества: "Спам по имейлу уже не такой эффективный. А вот спам внутри социальных сетей очень эффективный, потому что он рассылается от имени конкретного человека конкретным друзьям, и уровень доверия этим сообщениям значительно выше. Он очень эффективный и его можно монетизировать".

По мнению Кислицина, основное применение похищенных логина и пароля от аккаунта, например, Facebook, это спам - "по друзьям, рассылка в статусе или приватные сообщения с ссылкой на зараженный сайт, который установит "Троян".

Эксперт приводит распространенный в России вариант спам-рассылки: "Привет, я знаю, что ты рассылаешь спам, вот тебе ссылка на прикольный антивирус, который тебе вылечит все твои вирусы" - и ссылка на поддельный антивирус, который потребует оплату через смс".

"В России все через смс делается, - констатирует Кислицин. - Предложат скачать этот новый "антивирус", он скажет, что у него обнаружено 36 страшных вирусов и что ему надо оплатить смс-кой, чтобы вылечить их".

В США и Европе срабатывают другие схемы обмана - в основном связанные с электронным переводом денег.

Ответственность пользователя

По мнению экспертов, атаке подвержены любые интернет-сервисы - как социальные сети, так, например, и почтовые.

И популярность этих атак кроется в действиях самих пользователей, которые нажимают на сомнительные ссылки.

Главный редактор журнала "Хакер" считает, что сами сети в такой ситуации могут сделать немного.

"Со стороны администраторов сети сложно отличить, украден этот пароль или нет, - объясняет Кислицин. - Они тут слабо могут помочь пользователям. Только сами пользователи могут увидеть, что по друзьям рассылается какая-то ерунда - поменяют пароль, установят антивирус, найдут эту злую программу, удалят ее и решат проблему".

На сайте Facebook для тех, кто подозревает, что их аккаунт был взломан, предлагается пройти стандартную процедуру замены пароля.

Как заключают эксперты по информационной безопасности, основными причинами уязвимости пользователей остаются недостаточность их компьютерных знаний, с одной стороны, и постоянно растущая компетентность кибер-мошенников - с другой.

Источник: http://www.bbc.co.uk

UA Linux
open source ■ open future
Эксперт в области безопасности.

UA Linux
http://ualinux.com
Эксперт в области безопасности.

«Доктор Веб»: сетевые мошенники ищут жертв через сайты знакомств

Представляясь иностранцами с русскими корнями, мошенники ищут на сайтах знакомств одиноких женщин, которым в процессе общения предлагают отправить по почте дорогой подарок (планшет, смартфон или ювелирное украшение). Для этого мошенник предлагает воспользоваться услугами частной курьерской службы, за которой скрывается подставной сайт, где жертва и теряет деньги, оплатив доставку столь ценного подарка.

Эта схема, успешно применяемая сетевыми мошенниками вот уже более года, в последнее время все больше набирает популярность, судя по росту числа пострадавших. Для реализации своего преступного замысла злоумышленники регистрируются на различных сайтах знакомств и выбирают себе потенциальную жертву из числа одиноких женщин. 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. Однако поскольку презент представляет большую ценность, отправитель не рискует отсылать отправление обычной почтой, вместо этого он предпочитает воспользоваться услугами частной курьерской службы.

Через некоторое время потенциальной жертве приходит электронное сообщение со ссылкой на сайт транспортной компании, также содержащее логин и пароль для доступа в «личный кабинет». После успешной авторизации пользовательнице демонстрируется веб-страница с номером почтового отправления, указанием его веса и имени получателя. Однако в этот момент выясняется пикантная подробность: отправитель не оплатил стоимость доставки посылки до получателя. Эту сумму, составляющую обычно от нескольких сотен рублей до нескольких сотен долларов, злоумышленники и предлагают выплатить жертве. Вполне естественно, что вскоре после оплаты «курьерская служба», как и сам щедрый поклонник, исчезают в неизвестном направлении.

Существует и более изощренный вариант аналогичного мошенничества. Злоумышленник представляется американским офицером, служащим в одной из «горячих точек» — например, в Афганистане или Сирии. Нередко киберпреступники используют в своих целях имена и фотографии настоящих военнослужащих армии США, взятые из открытых источников, как правило, социальных сетей. После непродолжительного периода романтического общения — переписки и даже телефонных звонков — «горячий поклонник» сообщает своей избраннице, что вскоре ему предстоит отпуск или через некоторое время подходит срок окончания контракта, поэтому он готов встретиться с ней. Еще одна приятная новость: в ходе военных действий этот офицер сумел раздобыть те или иные материальные ценности, например, ювелирные украшения, антиквариат, драгоценности, и готов переправить их своей возлюбленной. Ценности он планирует отослать дипломатической почтой, которая, как известно, не подлежит таможенному декларированию и досмотру, или через знакомого — сотрудника одной из международных организаций. Только вот для того, чтобы вывезти эти богатства из страны, нужно заплатить посреднику. Совсем немного: тысячу-другую долларов. В качестве альтернативного сценария аферисты нередко используют такой прием: отправление якобы задержали на таможне в какой-то далекой стране, и чтобы оно достигло адресата, нужно заплатить некую сумму в качестве «взятки».

Киберпреступники, промышляющие подобными аферами на сайтах знакомств, называются «скамерами», и описанные выше ситуации являются весьма распространенными способами мошенничества «на доверии». Специалисты компании «Доктор Веб» призывают пользователей относиться к виртуальным знакомым с определенной долей осторожности и ни в коем случае не оплачивать услуги по доставке каких-либо подарков или посылок. Если вы в силу обстоятельств стали жертвой сетевых аферистов, обязательно напишите заявление о факте мошенничества в территориальный отдел полиции.

Источник: http://news.drweb.com

Украине грозят санкции за злостное нарушение авторских прав

Украина признана главной пиратской страной в мире. Международный альянс интеллектуальной собственности в своем ежегодном отчете назвал ее приоритетной страной.

Украина признана главной пиратской страной в мире. Международный альянс интеллектуальной собственности в своем ежегодном отчете назвал ее приоритетной страной, которую Торговая палата США должна включить в список государств, где систематически нарушаются авторские права, пишет Коммерсантъ-Украина в статье Программное ужесточение.

Издание поясняет, что в ближайшее время стране угрожает исключение из программы поддержки развивающихся стран, что лишит украинских предпринимателей права на беспошлинный ввоз товаров в США.

Напомним, что в пятницу, 8 февраля, Международный альянс интеллектуальной собственности (IIPA), объединяющий семь крупнейших ассоциаций американских производителей контента, присвоил Украине статус приоритетной страны для введения санкций.

Газета указывает на тот факт, что ни одно государство не получало этот статус с 2006 года, и его присвоение означает, что распространение пиратского контента в стране приобрело масштабы, наносящие правообладателям значительные убытки.

По мнению IIPA, Украина – ключевой экспортер цифрового пиратского контента в Европе и СНГ. Более того, согласно расследованию альянса, нелицензионное программное обеспечением в нашей стране используют даже госорганы, среди которых Министерство внутренних дел, Государственная налоговая служба и прокуратура.

Кроме того, альянс признал украинское правительство крупнейшим потребителем нелегального программного обеспечения в стране. В качестве подтверждения приводится такой факт: в бюджете на 2013 год на закупку ПО для госучреждений отведено 100 млн грн, что составляет 10-20% от необходимой суммы, если ПО будет лицензионным.

Более того, правительство уже заявило о планах сокращения даже этого бюджета, отмечает Коммерсантъ-Украина.

Примечательно, что больше всего в IIPA недовольны сайтом ex.ua, который, по их мнению, ответственен за распространение половины всего нелегального контента в Украине. При этом, как убедился альянс в прошлом году, государство не может справиться с ситуацией.

«Для американской ассоциации непонятно, как такое возможно: ex.ua, который ежегодно попадает во все списки крупнейших пиратских сайтов, не просто признан невиновным, но в его защиту выступил народный депутат – сын действующего президента», – поясняет управляющий партнер юридической компании Jurimex Юрий Крайняк.

Однако, как пишет газета, теперь на основании рекомендаций IIPA и консультаций с правообладателями Торговая палата США сформирует так называемый отчет 301. Попавшие в него страны исключаются из Общей системы привилегий (GSP) – программы американского правительства по поддержке экономического роста развивающихся стран, в рамках которой в США беспошлинно ввозится 3,4 тыс. видов товаров из 140 стран.

Как указывают в IIPA, благодаря GSP за 11 месяцев 2012 года украинская продукция на $70 млн была ввезена в США беспошлинно. При получение статуса приоритетной страны делает перспективу применения санкций практически решенным вопросом, считают эксперты.

Источник: http://vlasti.net

Тут может быть Ваша информация!

Заявите о себе!

И про Вас узнают Все...

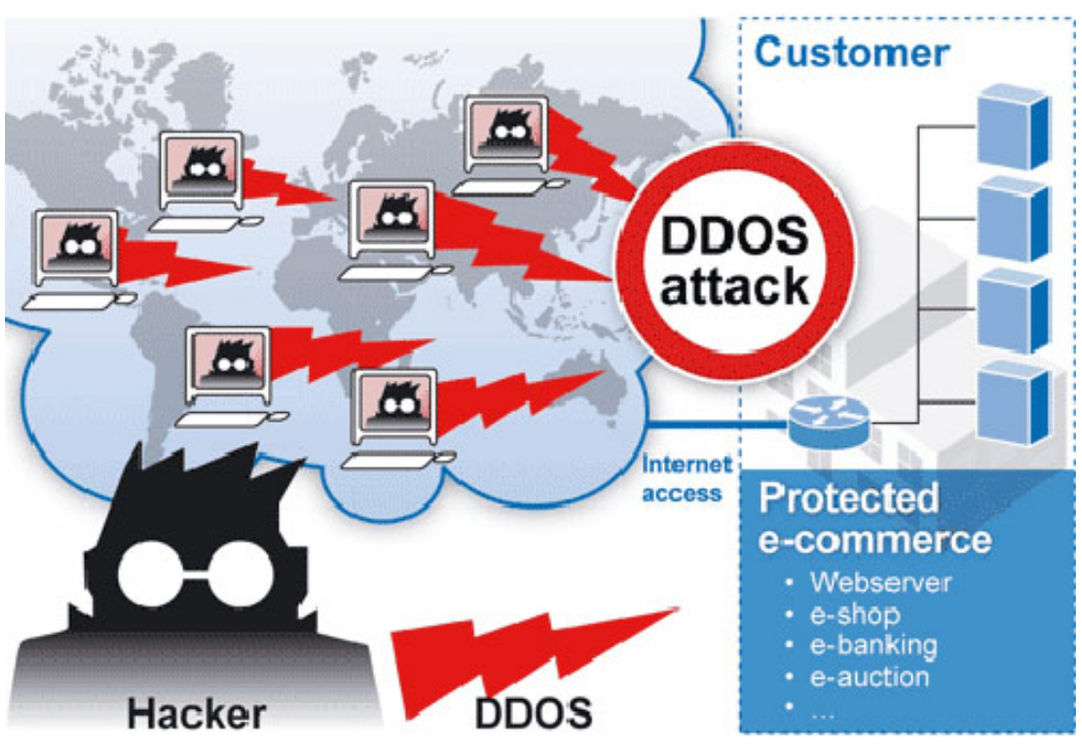
UA Linux
http://ualinux.com
Эксперт в области безопасности.

Как уберечься от DDoS-атак

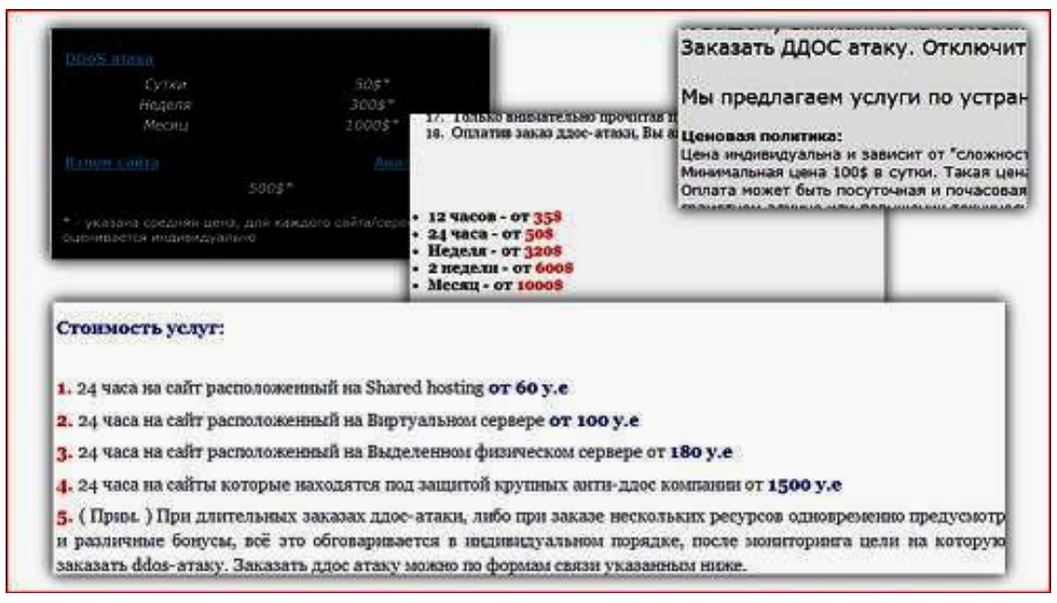
Верного способа защиты от DDoS-атак пока нет. Их жертвами становились такие гиганты, как MasterCard и Visa, Twitter и eBay. Среди украинских «пострадавших» наибольший резонанс вызвали DDoS-атаки «Укртелекома», МВД и официального сайта президента.

Мощь и популярность DDoS-атак предельно ясна – сегодня это один из самых доступных способов «it-мести».

Из Википедии: «Если атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). В некоторых случаях к фактической DDoS-атаке приводит непреднамеренное действие, например, размещение на популярном интернет-ресурсе ссылки на сайт, размещённый на не очень производительном сервере (слэшдот-эффект). Большой наплыв пользователей приводит к превышению допустимой нагрузки на сервер и, следовательно, отказу в обслуживании части из них».



По словам руководителя отдела корпоративных продаж компании ITBiz, Владимира Гука, заказать DDoS-атаку легко, достаточно ввести нужные слова в поисковик и остается выбрать понравившийся вариант. Средняя стоимость такого «удовольствия» от 5 до 100 у.е. Самые изощренные обойдутся заказчику максимум в 1500 у.е. При нехитрой математике можно легко убедиться, что эти затраты ничто по сравнению с материальными и репутационными потерями атакуемой стороны.



Не стоит упускать из вида и тот факт, что современные DDoS-атаки направлены не просто на то, чтобы сделать недоступным сайт, их основной вектор сместился в направлении недоступности как отдельных приложений, так и центров обработки данных в целом.


Прибыль банков Украины на 01.10.2012 года

№	Банк	Прибыль (после налогообложения)
1	ПРИВАТБАНК	
2	ВТБ БАНК	
3	ОЩАДБАНК	
4	ІНГ БАНК УКРАЇНА	
5	СІТІБАНК	
6	СБЕРБАНК РОСІЇ	
7	УКРГАЗБАНК	
8	КІБ КРЕДІ АГРІКОЛЬ	
9	ПЕРШИЙ УКР.МІЖНА БАНК	
10	РАЙФФАЙЗЕН БАНК	
	ИТОГО	

Прибыль банков Украины на 01.10.2012 года

№	Банк	Прибыль (после налогообложения)
11	УКРЕКСІМБАНК	
12	ПІВДЕННИЙ	
13	ЕКСПРЕС-БАНК	
14	УКРАЇНСЬКИЙ ПРОФЕ БАНК	
15	КРЕДІ АГРІКОЛЬ БАНК	
16	ФОЛЬКСБАНК	
17	УКРСОЦБАНК	
18	ДОЙЧЕ БАНК ДБУ	
19	УНІКРЕДИТ БАНК	
20	ДЕЛЬТА БАНК	
	ИТОГО	

Прибыль банков Украины на 01.10.2012 года

№	Банк	Прибыль (после налогообложения)
21	АЛЬФА-БАНК	30 892 000
22	КЛІРИНГОВИЙ ДІМ	23 540000
23	АСТРА БАНК	21 135 000
24	ІНДУСТРІАЛБАНК	20 634 000
25	УКРБІЗНЕСБАНК	19 656 000
26	КЛАСИКБАНК	22 958 000
27	ПОЛТАВА - БАНК	18 983 000
28	ПРОКРЕДИТ БАНК	15 676 000
29	ТАСКОМБАНК	19 649 000
30	ВСЕУКРАЇНСЬКИЙ БАНК РОЗВИТКУ	16 035 000
	ИТОГО	209 158 000

Среднедневная прибыль банка из 3-й десятки составляет **110 000 грн.**

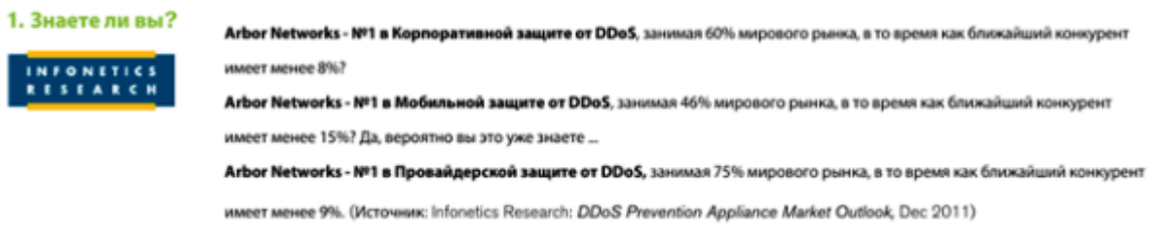
Источник: forinsurer.com по материалам НБУ

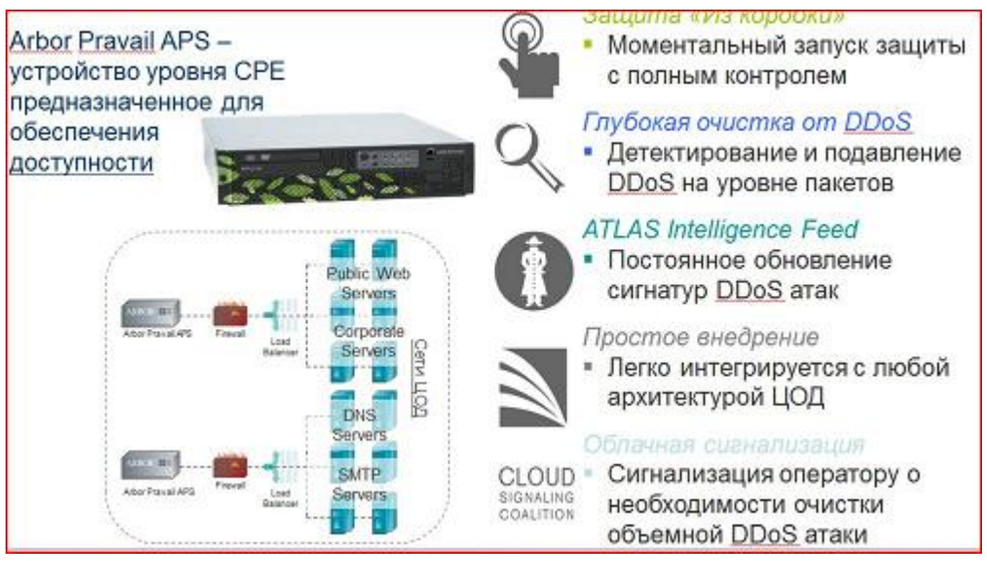
«Сколько стоит день работы (простоя) банка? – подсчитывает Владимир Гук. – Если мы возьмем наши банки, то среднестатистический банк из третьего десятка рейтинга НБУ зарабатывает порядка 110 тысяч гривен чистой прибыли. Максимальная цена DDoS-атак – 12 тысяч гривен».

Сегодня основные методы борьбы с DDoS-атаками – это межсетевые экраны (firewall) и системы предотвращения вторжений (IPS). Механизмы этих способов далеки от совершенства, а значит, безопасность и защита данных находятся под вопросом. Принцип их работы можно объяснить на примере обычного турникета, где его пропускной способностью является количество человек в определенный промежуток времени, и пропустить больше, чем, к примеру, 2 человека за 1 секунду он не сможет физически, и уведомит об этом администратора сети только по факту «перегрузки». Исходя из этого, DDoS-атаку можно представить как целенаправленное переполнение огромным количеством сессий («человек») всех возможных ресурсов защитного устройства или приложения.

Механизмы атак эволюционируют, и сейчас DDoS-атаки становятся сложнее. Они направлены не столько на нарушение доступности сайта, приложения или оборудования, их используют больше как прикрытие для кражи данных, финансовых махинаций и поддержку других хакерских воздействий. Поэтому полагаться сегодня только на указанные средства защиты достаточно рискованно.

На украинском рынке появилось новое средство по борьбе с DDoS-атаками – Arbor Pravail APS, которое активно используется не только по всему миру, а уже в России и Украине. Принцип работы данного устройства кардинально отличается от существующих способов борьбы с DDoS-атаками.





«Решение, которое предлагает компания Arbor, защищает от DDoS-атак не «по примеру пропуска через турникет», после чего идет обрезка опасного трафика, а технологически на другом уровне, где посессионный пропуск отсутствует, и возможность перенагрузки исключена. Принцип защиты построен так, что Arbor Pravail APS сначала пропускает трафик через себя, анализирует его и обрезает опасный, в результате чего сервер получает уже очищенный и безопасный трафик, и продолжает нормально функционировать, - рассказывает Владимир Гук. – Конечно, идеальных систем не бывает, и мы иногда сталкиваемся с, так называемыми, false-срабатываниями, когда урезается трафик, который не несет угрозы. Тем не менее, эффективность данной системы достаточно высока и, по уровню информационной безопасности, не имеет равных.

Чем это устройство интересно? Во-первых, оно простое в обслуживании, не требует особых настроек и готово выполнять свои защитные функции прямо «из коробки». Во-вторых, свою мощь оно продемонстрировало как по всему миру, так и в Украине. Например, во время последних парламентских выборов сайты Президента и Центральной Избирательной Комиссии защищались с помощью данного оборудования, которое предоставила для тестирования компания «ITBiz». DDoS-атаки были, оборудование со своей задачей справилось, атаки предотвратило и обеспечило безопасность. Обещанную «медаль» нам пока не дали, но виртуально она уже есть».

Источник: http://internetua.com

Тут может быть Ваша информация!

Заявите о себе!

И про Вас узнают Все...

UA Linux
http://ualinux.com
Эксперт в области безопасности.

Facebook столкнулась с промышленным шпионажем

Представители социальной сети Facebook в пятницу заявили, что компьютеры нескольких инженеров компании, связанных с разработкой ключевых технологий Facebook, были атакованы при помощи ранее неизвестного Java-эксплоита, установившего уникальное вредоносного программное обеспечение. Представители компании говорят, что в результате атаки пользовательские данные не пострадали, а сложный вредоносный софт был обнаружен на компьютерах "ограниченной группы инженеров".

Внутренняя служба безопасности Facebook работала с неназванной антивирусной компанией, чтобы выйти на командный сервер злоумышленников, где собирались ворованные у инженеров данные. По словам директора по безопасности Facebook Джо Салливана, на серверах также были обнаружены данные, принадлежащие нескольким другим компаниям. Он отметил, что Facebook уведомила эти компании о своей находке, а также передала данные об атаках в ФБР США. В социальной сети говорят, что расследование по факту промышленного шпионажа пока не завершено, передает cybersecurity.ru.

Салливан рассказал, что впервые следы атаки специалисты Facebook обнаружили в логах нескольких DNS-серверов компании. Дальнейшее расследование показало, что неизвестным хакерам удалось получить доступ к компьютерам инженеров, специализирующихся на ряде мобильных проектов Facebook. Криминалистический анализ ноутбуков показал, что внутри команды разработчиков Facebook атакованных систем было несколько.

По словам Салливана, судя по конкретным действиям хакеров, злоумышленники изначально проектировали атаку именно под Facebook, так как прежде использованная последовательность действий во время нападений на западные компании не применялась.

Интересно отметить, что атака на Facebook по времени произошла именно тогда, когда сервис микроблогов Twitter сообщил об утечке данных о 250 000 пользовательских аккаунтов, в том числе хешированных версией паролей пользователей. Хотя в самой Twitter не сообщили о том, кто и как смог украсть данные, Роберт Лорд, директор по информационной безопасности Twitter, сообщил, что тогдашняя атака на Twitter была связана с плагином Java и призвал через свой блог отключить плагины Java в браузерах.

В Facebook и Twitter рассказали, что перед атаками их сотрудники столкнулись с волной целевого мошеннического спама, при помощи которого сотрудники переправлялись на поддельные сайты, где их компьютеры заражались вредоносным программным обеспечением. Джо Салливан из Facebook говорит, что в данном случае их компании злоумышленники использовали Java-эксплоит, который работает даже в самой последней версии Java 7 Update 13. Он отметил, что Oracle уже уведомлена о еще одной критической проблеме в Java 7.

Также Салливан заявил, что использованный Java-эксплоит работает как в Mac, так и в Windows. Сейчас сигнатуры этого вредоноса уже добавлены во многие популярные антивирусные продукты.

В компании, комментируя последнюю атаку, заявили, что она не имела отношения к самой социальной сети и пользовательским данным, на сей раз атакующие пытались заниматься именно промышленным шпионажем, охотясь за технологическими разработками крупнейшей социальной сети в мире.

Facebook ничего не сообщила о том, куда вели следы хакеров.

Источник: http://www.anti-malware.ru

Twitter сообщил о масштабных хакерских атаках на американские компании

Отдел информационной безопасности Twitter сообщил о направленных на сервис кибер-атаках, поставив их в одном ряду с аналогичными нападениями на другие американские IT- и медиакомпании. Об этом сообщается на официальной странице крупнейшего в мире сервиса микроблогов.

По словам руководителя отдела информационной безопасности Twitter Боба Лорда, на прошедшей неделе в компании обнаружили новые механизмы доступа к данным, которыми могли пользоваться хакеры. Специалисты выявили одну кибер-атаку, которую удалось отразить, но при этом признали, что хакеры могли получить доступ к информации 250 тысяч пользователей сервиса. Речь идет, в частности, об именах пользователей, их электронных адресах и паролях, сообщает lenta.ru.

В Twitter заявили, что не считают эту атаку единичным случаем, подчеркнув, что осуществившие ее хакеры были профессионалами.

Всем клиентам, чьи данные могли быть доступны хакерам, было направлено письмо с уведомлением. В качестве меры предосторожности представители Twitter предложили этим пользователям сменить пароли, а остальным проверить, являются ли их пароли достаточно безопасными. Эти рекомендации распространяются не только на сервис микроблогов, но и на любые другие сайты.

При этом, по мнению Twitter, другие компании и организации недавно подверглись аналогичным атакам. В отделе информационной безопасности напомнили о череде крупных хакерских атак, направленных на американские медиакомпании, в том числе на издания New York Times и Wall Street Journal. «Именно поэтому мы решили сообщить об этой атаке, хотя пока только собираем информацию», — заявил Боб Лорд. В настоящий момент Twitter сотрудничает с правительством и правоохранительным органами США с целью найти и привлечь к ответственности хакеров, причастных к нападению, и в результате сделать интернет безопаснее для всех пользователей.

30 января газета New York Times сообщили об атаках на сайт издания и взломе почты десятков ее сотрудников. Газета написала, что нападения продолжались в течение четырех месяцев, начиная с октября 2012 года, и осуществлялись из Китая. На следующий день о постоянных атаках китайских хакеров заявило американское издание The Wall Street Journal. В посольстве Китая в США причастность Китая к нападениям на американские СМИ не признали.

Источник: http://www.anti-malware.ru

11-летний хакер воровал данные участников online-игры

Исследователи все чаще сталкиваются с вредоносными программами, написанными детьми.

По даннымBBC, исследователи антивирусной компании AVG сообщили о программах, созданных для воровства виртуальной валюты. В ходе исследования, эксперты столкнулись с написанным «любителем» вредоносным кодом, использовавшимся для кражи данных. Как оказалось, автором кода был ребенок.

Исследователи сообщили, что в настоящее время дети в состоянии писать инструменты для взлома учетных записей на игровых web-сайтах и в соцсетях. Сотрудники компании AVG утверждают, что при обучении детей программированию, необходимо объяснять им как можно и как нельзя поступать, пока дети еще не понимают возможных последствий своих поступков.

Написанный детьми код имеет ряд общих характеристик, сообщают исследователи. Большинство вредоносных кодов написаны при помощи Visual Basic и C#, кроме того, они содержат элементарные ошибки, которые вряд ли допустил бы профессиональный хакер.

Эксперты изучили один конкретный экземпляр такого кода, замаскированный под чит-программу для геймеров игры Runescape, на которую подписаны свыше 200 млн online-игроков. Программа Runescape Gold Hack обещала игрокам якобы бесплатную виртуальную валюту для игры, но на самом деле с ее помощью злоумышленник осуществлял кражу данных ничего не подозревающих пользователей.

Как сообщил технический директор AVG Ювал Бен-Итцхак (Yuval Ben-Itzhak), исследуя исходный код программы, эксперты столкнулись с интересной информацией. Так, вредоносная программа воровала данные игроков и отсылала их на определенный адрес электронной почты. Разработчик программы включил в нее свой электронный адрес, пароль и другую информацию, чего бы никогда не сделал обычный хакер. Эксперты обнаружили, что адрес электронной почты принадлежит 11-летнему ребенку из Канады. Благодаря этой информации исследователи определили город, в котором проживает мальчик.

Эксперты отмечают, что сейчас в школах мира детей обучают программированию, а не простому использованию компьютеров. В Великобритании открылись внешкольные клубы при поддержке таких компаний, как Google и Microsoft. В связи с этим, Ювал Бен-Итцхак настаивает на том, чтобы объяснять детям, как нужно использовать полученные знания.

Источник:http://www.securitylab.ru

Как не стать жертвой мошенников

Всеукраинська социальная инициатива "Банк добрых дел" обеспокоена ростом мошеннических случаев, о которых в последнее время рассказывают правоохранители и средства массовой информации.

В начале 2013 года самыми распространенными схемами обмана граждан стали неправомерные операции с платежными картами, которые собирают деньги на лечение.

Как работают такие мошеннические схемы?

Первый сценарий. Родители больного ребенка публикуют информацию о карточном счете с просьбой перечислить средства на лечение. Впоследствии родителям звонят неизвестные и пытаются уточнить данные для зачисления средств.

Для этого просят сообщить всю информацию о выпущенной банковскую карту, втом числе CVV-код - три цифры на обороте карты. Затем "господа" перезванивают и просят сообщить смс-код, пришедший на мобильный телефон с запросом "Вы подтверждаете платеж на такую-то сумму?".

Если человек сообщил эту информацию, он, как правило, становится жертвой мошенников. Деньги, которые так долго и трудно собирались, исчезают.

Второй сценарий. Мошенники звонят и представляются работниками банка. Им якобы нужно "уточнить данные вашей карты". После серии общих вопросов о личных телефоны и адрес проживания, жертву просят еще раз напомнить секретное слово, которое было указано при оформлении карты.

CVV-код - тоже один из пунктов, которым интересуются злоумышленники. После таких разговоров результат неизменен: деньги исчезают.

Как инициатор проекта "Банк добрых дел" призывает всех, кто собирает средства на лечение через системы электронных платежей: отслеживайть информацию о своих банковских картах.

Помните, что согласно законодательству Украины частные банковские счета для сбора средств не считаются благотворительными и подлежат налогообложению на общих основаниях как доходы физических лиц. Будьте готовы, что от собранной суммы вам придется заплатить налог - 15-17 процентов.

Оптимальным выходом является обращение за помощью в благотворительные фонды. Именно они являются единственным законным и действенным механизмом сбора средств на лечение или операцию. Целевая финансовая помощь благотворительных фондов налогом не облагается.

Если вы сомневаетесь относительно репутации фонда - обратитесь к консультантам Укргазбанка, которые учавчтвуют в проекте "Банк добрых дел". Эксперты этой программы предоставят всю информацию по вопросам благотворительного сбора средств и перечень доверенных фондов, которые могут вам помочь.

Источник: http://www.epravda.com.ua

UA Linux
http://ualinux.com

Аналитика, обзоры, рекомендации.

user And LINUX

{ Secure Shell }

Нам можно доверять!

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.

Все права на материалы принадлежат их авторам и опубликованы в открытых источниках.
Адреса на оригинальные источники публикуются.

{

Для размещения рекламы обращаться по тел.:
+38 (048) 770-0425
+38 (094) 995-4425
Или на email: journal@ualinux.com

}