Коммерсантъ

Цветные тематические страницы №25–32 являются составной частью газеты «Коммерсантъ».

Рег. №01243 22 декабря 1997 года. Распространяются только в составе газеты.

В 2008 году газета «Коммерсантъ» продолжит выпускать цветные тематические страницы.

Подписчики получат специальные выпуски: «Дом», «Телеком», «Авто», «Банк», «Путешественник», «Стиль», «Брокер», «Рождество» и другие.

4 601865 000240 08120

телеком

www.kommersant.ru Четверг 15 мая 2008 №81 (№3898 с момента возобновления издания)

Лейблы готовы к раздаче музыки

интернет-коммерция

Интернет-продажи музыки переживают настоящий бум, в то время как потребительский спрос на музыкальные компакт-диски постепенно снижается. Впрочем, ажиотаж на музыку в сети в большей степени на руку пиратским онлайн-магазинам и монополисту на западных рынках сервису Apple iTunes. Чтобы переломить ситуацию, звукозаписывающие лейблы решили бесплатно распространять музыку в интернете. Что ждет любителей музыки в интернете и кто за нее будет платить, разбиралась корреспондент «Ъ-Телекома» ОКСАНА ЗОТИКОВА.

Кризис на рынке музыки на компакт-дисках уже давно не новость. Еще год назад исследовательская компания Nielsen SoundScan сообщила, что с начала 2007 года продажи музыкальных CD в США упали на 20% по сравнению с тем же периодом прошлого года: с 1 января по 18 марта 2007 года в США было продано 89 млн музыкальных CD, в то время как за тот же период 2006 года — 112 млн. Согласно прогнозу PricewaterhouseCoopers, к 2011 году мировой объем продаж музыки на компакт-дисках составит $17,6 млрд, в интернете — $22,8 млрд. Тенденция обусловлена прежде всего бурно растущим рынком продаж MP3-плееров, а также телефонов, поддерживающих формат MP3. В прошлом году только в США, по данным Consumer Electronics Association, было продано MP3-плееров почти на $6 млрд.

Подобная тенденция наблюдается и в России. Гендиректор Universal Music Russia Дмитрий Коннов прогнозирует, что лет через пять на продажу компакт-дисков будет приходиться только 30–40% выручки лейблов в России. Выиграли от сложившейся ситуации далеко не все. Первыми на притоке покупателей музыки в сеть нажились пираты. Правообладатели столкнулись с ситуацией, когда многие интернет-магазины продавали музыку без соглашений с правообладателями, не выплачивая отчисления. Особенно это касается России, где музыку продавали по лицензиям обществ по коллективному управлению авторскими правами в интернете РОМС и ФАИР. Эти общества пользовались пробелом в законодательстве РФ, существовавшим до вступления в силу четвертой части ГК.

(Окончание на стр. 26)

Кибертерроризм захлестнул интернет. Если раньше DDoS-атаки на сайты компаний использовались главным образом в целях шантажа, то сейчас к помощи киберпреступников прибегают и солидные на первый взгляд организации, желающие свести счеты с конкурентами. Кто и как организует атаки и сколько на этом можно заработать, выяснял **Денис Зенкин**.

DDoS с большой дороги

IT-безопасность

В рунете вряд ли найдется много популярных сайтов, ни разу не подвергавшихся так называемым атакам DDoS («отказ обслуживания»). Им многократно подвергались серверы радиостанции «Эхо Москвы», издательского дома «Коммерсантъ», журнала Mobile Review. Социальные сети, в частности сообщества LiveJournal, широкопрофильные порталы (например Mail.ru), интернет-провайдеры («Мастерхост», «Зенон») также регулярно попадают под прицел кибертеррористов. Участи этой не избежали и разработчики систем информационной безопасности: известно много случаев, когда успешные атаки «валили» серверы, например, BlueSecurity или CastleCops.

Ширится практика использования DDoS и в политических целях — прежде всего в межпартийной борьбе и для выражения несогласия с действиями того или иного государства. Вспомните прошлогодний случай с демонтажом памятника воину-освободителю в Таллине и последовавшую за этим лавину DDoS-атак на веб-сайты эстонских правительственных учреждений. Такие действия несогласных все чаще сопутствуют внутренним и международным событиям. За примерами далеко ходить не приходится: арабо-израильский конфликт, пакистано-индийский конфликт, недавние события в Косово.

DDoS — быстро набирающая популярность разновидность хакерских атак. Словосочетание, имеющее аббревиатуру DDoS, на русский переводится как «распределенный отказ обслуживания». Цель атаки не в том, чтобы проникнуть в систему, а в том, чтобы парализовать ее работу. Представьте себе продавца газет, к которому внезапно выстраивается неимоверная очередь желающих приобрести свежую прессу. Естественно, что вы сможете получить свой экземпляр очень не скоро, если вообще получите.

По такому сценарию проходят DDoS-атаки в интернете. Десятки тысяч компьютеров вдруг начинают одновременно посылать на определенный сервер бессмысленные пакеты данных. Сервер пытается их обработать,

AFP

но не справляется. В результате добросовестные посетители не могут получить доступа к ресурсу. Для компаний, чья деятельность осуществляется именно в интернете (интернет-магазины, социальные сети, онлайн-СМИ и т. п.), такое происшествие оборачивается многомиллионными потерями и дурной славой. К примеру, российский филиал процессинговой системы ChronoPay, обслуживающий интернет-платежи, потерял три года назад около $700 тыс. из-за нескольких часов простоя по причине DDoS-атаки. Американский интернет-аукцион eBay по этой же причине не работал 22 часа и в течение последующих пяти дней потерял четверть своей стоимости на фондовом рынке.

DDoS. История проблемы

История появления DDoS-атак довольно поучительная. Технология, которая легла в основу этой разновидности хакерских атак, была создана исключительно в мирных целях. Она активно использовалась для изучения пропускной способности каналов передачи данных и для проверки их поведения в условиях пиковых нагрузок. Действительно, трудно придумать лучший вариант тестирования системы, чем симуляция «боевых» условий. Однако вскоре эта технология и инструменты попали в руки тех, кто нашел им иное применение.

Первые случаи хакерских DDoS-атак были зарегистрированы в 1996 году. Однако всерьез об этой проблеме заговорили только спустя четыре года, когда жертвами атак стали веб-сайты Amazon, Yahoo, eBay, CNN и даже ФБР. Главный вывод из этого был прост: «если они отключили Yahoo, то могут отключить кого угодно». Каждый сайт в любой момент мог стать мишенью для атаки. С тех пор DDoS стал обыденным явлением сетевой жизни: не проходит и месяца без сообщения о новом крупном происшествии. По данным Института компьютерной безопасности (США), примерно 55% всех хакерских атак имеют именно такую природу, а подсчеты компании Arbor Networks показывают, что каждый день в интернете происходит около 1300 DDoS-нападений.

DDoS давно стал гораздо большей проблемой, нежели спам. На долю электронной почты приходится приблизительно 1,5% объема данных, передаваемых через интернет. Таким образом, столь популярная проблема как спам (нежелательные почтовые рассылки) в глобальном масштабе — всего лишь незначительные помехи на уровне 1%. Объем же DDoS-данных достигает 5%, и последствия DDoS-атаки гораздо серьезнее.

Как все гениальное, технология DDoS проста и прозрачна. Конечно, массированные атаки на ресурсы, имеющие мощную защиту,— это удел профессиональных киберпреступников. Но для проведения средней силы атаки, которая не нанесет серьезного вреда жертве, не требуется каких-то особых навыков. С этой задачей может справиться даже любитель.

DDoS делится на два архитектурных типа: программируемый и автономный. Программируемый тип включает управляющую консоль, промежуточные компьютеры и компьютеры-солдаты. По сигналу с консоли промежуточные компьютеры посылают команду всем «солдатам» с указанием цели и типа атаки. Те, в свою очередь, начинают «бомбардировку» жертвы. Автономная архитектура предполагает использование сети «солдат», запрограммированных на атаку определенной цели. Несмотря на кажущийся недостаток гибкости и управляемости, они чрезвычайно опасны: такие компьютеры продолжают действовать даже после нейтрализации управляющего центра. «К сожалению, выйти на след хакера практически невозможно. Мало того что непосредственными исполнителями атаки являются компьютеры ничего не подозревающих пользователей, связь между ними и управляющей консолью также чрезвычайно запутанна: нападающие используют анонимные прокси-серверы для сокрытия своего местоположения»,— рассказывает Дмитрий Дукорский, технический консультант компании Kerio Technologies.

(Окончание на стр. 29)

страница 26
Платное ТВ: что ждет Россию

страница 28
Как воруют деньги с мобильника

страница 30
BlackBerry опоздал в Россию

REUTERS

страница 31
Авиация мобилизуется

страница 32
CeBit-2008: выставка дешевых ПК