近日,天涯社区承认约4000万用户的邮箱、社区密码等资料外泄
昨天,京东商城也出现漏洞,用户资料难保
黑色产业链有严格的分级代理制度

黑客产业规模价值达上百亿元

打开一个导航页广告及流量收入就有2000万元

“这两天改密码改到手软。”北京CBD工作的白领李浩告诉记者,通过查询,得知自己的天涯账号已被泄露,而他的开心网、人人网、微博等几乎所有账号都使用相同ID、密码,不得不一一更改。

中国互联网正在遭遇史上最大规模的用户信息泄露事件——12月21日至26日短短几天时间,多家大型网站的用户数据库被泄露,几千万用户账号和密码被公开。

而业内人士认为,最近公开的仅仅是部分在黑客交易市场中流传很久的老旧数据库,不同黑客组织实际掌握的用户数据库规模应该远大于1亿条,而目前中国黑客的黑色产业链规模价值或达上百亿元。

数字 1.21亿人

CNNIC《第28次中国互联网络发展状况统计报告》显示,2011年上半年,有过账号或密码被盗经历的网民达到1.21亿人,占24.9%。

京东商城用户资料大量泄露

漏洞报告平台乌云27日发布消息称,有漏洞导致京东商城用户资料已大量泄露。

该漏洞详情为:“京东商城在某些业务上存在用户权限控制不当的漏洞,导致用任意用户登录系统后,都可以正常访问到所有用户的信息,包括姓名、地址、电话、Email等。”

昨天京东已经确认,称危害等级为中,漏洞评级为10,并且将马上处理。

新浪微博否认用户密码外泄

CSDN、天涯社区等知名大论坛的用户密码大批外泄事件导致互联网界“草木皆兵”。26日,据传用户密码已外泄的新浪微博、人人网、开心网等网站先后公开声明账户密码安全;支付宝、腾讯QQ等互联网服务亦公开了用户资料加密流程。

继本月中旬CSDN网站600万用户账户信息和密码外泄后,天涯社区上周日承认用户资料外泄,据估算约有4000万用户的邮箱、社区密码等资料外泄。前者是中国最大的计算机技术社区,后者是最大的论坛社区,二者密码泄露事件引起各界关注,众多其他网站也发生密码泄露的传言开始大规模流传。

天涯社区提醒修改密码

新浪微博26日下午正式回应称,新浪微博用户账号信息采用加密存储,并未被盗。在对流传的数据资料包进一步研究后,新浪微博表示“经核实,该份数据绝大部分不是新浪微博账号。极小部分用户因使用和其他网站相同账号密码,可能导致其微博账号不安全。我们已对这部分用户做了保护,并提醒所有用户尽快进行账号安全设置”。

记者使用与天涯社区相同的注册邮箱登录新浪微博时,亦收到系统首页提示称,该邮箱与一些网站外泄资料中的邮箱相同,并要求修改密码。

人人网、开心网26日表示,网站密码采用加密方式保存,从未发生过外泄情况。

看点

某活跃于黑色产业链的知名黑客,一年能够赚5000多万;一些大网站的数据库是明码标价,一个库端下来,价值600多万;黑色产业链的人开始向一些网站收保护费,标准是一个月两万。

知名黑客一年能赚5000多万

随着泄密事件愈演愈烈,隐藏在背后的黑客产业链也浮出水面。

天涯社区公关经理初蒙26日告诉记者,天涯被盗取的用户账号规模低于网络传言的4000万。不过,业内人士预计,泄露网站数据库的行为可能会引发连锁效应,更多网站的数据会被黑客放出。

在今年9月的一场信息安全论坛上,Chown Group(信息安全专业委员会)发起者之一李麒曾表示,目前中国黑客的黑色产业链规模价值上百亿元。他举例称,某活跃于黑色产业链的知名黑客,一年能够赚5000多万;一些大网站的数据库是明码标价,一个库端下来,价值600多万;黑色产业链的人开始向一些网站收保护费,标准是一个月两万。

单纯倒卖用户数据库并不赚钱

李麒称,目前黑色产业链已经有了严格的代理制度,金牌总代、区域总代、一级总代、二级总代,制造木马,大木马里再装小木马,针对不同的游戏都能做,此外,从制造木马到买卖、销售、分销、洗信已经有了一条龙服务。

一般而言,单纯倒卖用户数据库并不赚钱,有些数据库经过多次交易后,几百个账号的价格只有几分钱,因此不少黑客盗取用户数据库之后通过发布诈骗信息、转卖给黑公关或竞争对手等多种途径完成利益最大化的变现。

例如,不少黑客利用密码库尝试窃取QQ、MSN等聊天软件账号和微博、人人、邮箱等账号,向好友发送借钱诈骗消息,发布广告信息或钓鱼诈骗链接。

网游用户是黑客攻击重点对象

一些花销颇多的网游用户也是黑客攻击的重点对象。一些游戏厂商的用户数据库被黑客窃取后,可能被黑客转卖给其竞争对手,成为竞争厂商争夺用户资源的“营销对象”。金山网络安全专家李铁军透露,这些数据在刚被盗取出来时售价非常昂贵,某些游戏厂商上百万的玩家用户资料包可以卖到百万元的高价。

更严重的情况还有,当黑客利用密码库在网上支付平台自动批量发起交易,如果恰好试探出用户泄露的密码和网上支付密码相同,支付账户中的余额就可能被黑客全部盗取。

国内知名黑客绿色兵团创始人Goodwell昨日亦指出,如果能控制100万的用户电脑终端,不管是恶意插件还是木马或是小软件,只要黑客能“挟持”用户的一些操作,哪怕是打开IE跳到一个默认的导航页面,也能为其带来每年2000万元的广告及流量收入。

“明文密码”被看做罪魁祸首

在一系列的用户信息泄露事件中,采用的“明文密码”被看做是“罪魁祸首”。

数字 80%

据360分析评估,上述被盗号的1.21亿网民群体中,80%以上是因为黑客刷库后获取了网民的账号密码数据,危害远远超过盗号木马。

“最不安全的保存方式是直接存储明文,用户密码什么样,网站数据库就存成什么样。这种情况一旦数据库泄露,黑客就可直接掌握所有密码。”360安全工程师石晓虹博士对记者说。

“对黑客而言,明文密码的盗取简直就是探囊取物,不是他们想不想要,而是要不要的问题。”一位受害企业员工对记者说。

CSDN在道歉信中透露,CSDN网站早期使用过明文密码,使用明文是因为和一个第三方chat程序整合验证带来的,后来的程序员始终未对此进行处理。直到2009年4月当时的程序员修改了密码保存方式,改成了加密密码。但是直至2010年8月底CSDN才清理掉所有明文密码。采用明文密码是一个相对低端的模式,很容易就被黑客破解。

天涯被盗的是2009年之前备份数据

而天涯社区表示,由于历史原因,天涯社区早期使用过明文密码,此次被盗的是2009年之前的备份数据,2010年之后升级改造了天涯社区用户账号管理功能,使用了强加密算法,解决了用户账号的安全性问题。

而那些未使用过明文密码的网站如人人网、新浪微博等也很难独善其身。因为很多用户习惯用同一个用户名和密码来注册多个网站,一旦有一个账号密码泄露,就很可能波及其他重要账号的安全,例如网上支付、邮箱、聊天账号等。

因此,近日也有网上爆出人人网、开心网、多玩、世纪佳缘、珍爱网、美空网、百合网、178、7K7K等知名网站的用户数据资料也被公开。目前,不少网站都向用户发出修改密码的提示。

“从积极的角度考虑,此次事件对于公众提升安全意识起到了积极的作用,让网民知道即便电脑不中毒,账号同样可能被盗。”石晓虹表示,无论未来黑客是否会继续公开更多网站的数据库,只要网民注意重要账号单独设置密码、定期修改密码,就能够将黑客窃取网站数据库的安全威胁降到最低。

据《第一财经日报》《新京报》