**您的密码可能已泄露!**

近期互联网出现一大热门事件，众多大型网站信息泄露事件，引起了各行业及网民的关注。

针对本次信息泄露事件，CNCERT/CC（国家计算机网络应急技术处理协调中心）发布了威胁通报1：截至2011年12月29日，CNCERT通过公开渠道获得疑似泄露的数据库有26个，涉及帐号、密码2.78亿条。其中，具有与网站、论坛相关联信息的（例如，被声称属于某个网站的数据）数据库有12个，涉及数据1.36亿条；无法判断网站、论坛关联性的数据库有14个，涉及数据1.42亿条。

知道创宇安全研究人员在本次泄露事件过程中，通过互联网免费下载的方式获取了CSDN和天涯的泄露数据，通过对这些泄露数据的分析发现，其中接近80%的用户密码可被自动化工具破解，对此，知道创宇进行了一些密码分布及用户习惯的分析。

# “CSDN网站”账户信息泄露及分析

CSDN是中国软件开发联盟（Chinese software develop net）的英文缩写，是中国最大的开发者技术社区。它是集[新闻](http://baike.baidu.com/view/14325.htm)、[论坛](http://baike.baidu.com/view/4394.htm)、[群组](http://baike.baidu.com/view/1141960.htm)、[Blog](http://baike.baidu.com/view/560.htm)、[文档](http://baike.baidu.com/view/55621.htm" \t "_blank)、[下载](http://baike.baidu.com/view/4238.htm)、读书、[Tag](http://baike.baidu.com/view/728.htm)、网摘、搜索、.[NET](http://baike.baidu.com/view/25172.htm)、[Java](http://baike.baidu.com/view/29.htm" \t "_blank)、游戏、视频、人才、外包、第二书店、《程序员》杂志等多种项目于一体的大型综合性IT门户网站，有很强的专业性，其会员囊括了中国地区众多的优秀[程序员](http://baike.baidu.com/view/39175.htm)，是国内最大的IT技术交流社区。

在本次泄密事件中，互联网上可供下载的CSDN账户信息共计6,428,632 条，其中包含了用户昵称、用户密码以及用户的注册邮箱地址。

知道创宇安全研究人员通过对这些公开下载的信息分析后发现，借助自动化破解工具并结合一些社会工程学的知识，即可破解80%以上的用户密码。而使用了包含大小写字符的密码仅占1.63%，弱密码2比例则高达42% 。

# “天涯网站”账户信息泄露及分析

天涯社区，创办于1999年3月，自创立以来，以其开放、包容、充满人文关怀的特色受到了全球华人[网民](http://baike.baidu.com/view/7657.htm" \t "_blank)的推崇，经过十年的发展，已经成为以[论坛](http://baike.baidu.com/view/4394.htm)、[部落](http://baike.baidu.com/view/4262.htm)、[博客](http://baike.baidu.com/view/1509.htm)为基础交流方式，综合提供个人[空间](http://baike.baidu.com/view/31260.htm)、[相册](http://baike.baidu.com/view/222377.htm)、音乐盒子、分类信息、站内消息、[虚拟商店](http://baike.baidu.com/view/156198.htm)、来吧、问答、企业品牌家园等一系列功能服务，并以人文[情感](http://baike.baidu.com/view/6251.htm)为核心的综合性[虚拟社区](http://baike.baidu.com/view/1587.htm)和大型网络[社交](http://baike.baidu.com/view/822170.htm)平台。

本次泄密事件中，可通过互联网下载的天涯账户信息共31,761,029条，通过分析人员的分析发现，其中60.7%的密码是全由数字组成，而其中9.8%的密码则是全由字母组成。

# 泄露数据对比分析

全数字密码占据比例较高

天涯泄露数据中的有60.7%的密码是全数字密码，CSDN泄露数据中全数字密码则占45.03%，密码字符组成特性分布图如下：

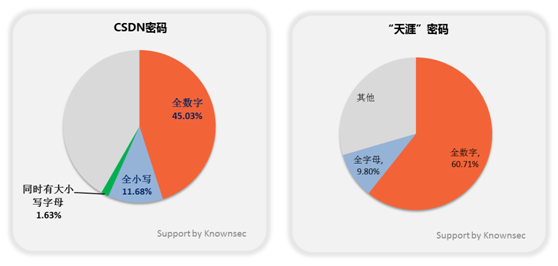


图1：密码字符组成特性分布图

天涯泄露数据中的常用密码TOP10几乎全部都是纯数字弱口令，CSDN泄露数据中常用密码TOP10除了纯数字还包括“dearbook”和“147258369”3。



图2：CSDN和天涯泄露信息中常用密码TOP 10分布

用户缺少密码长度意识

CDSN泄露数据中36%的密码长度为8位，天涯泄露数据中33%的密码长度为6位，而8位密码长度和6位密码长度分别是CSDN和天涯在注册用户时，网站所要求的最低密码长度。换言之，多数人对密码的强度设置是依赖网站的默认密码策略。

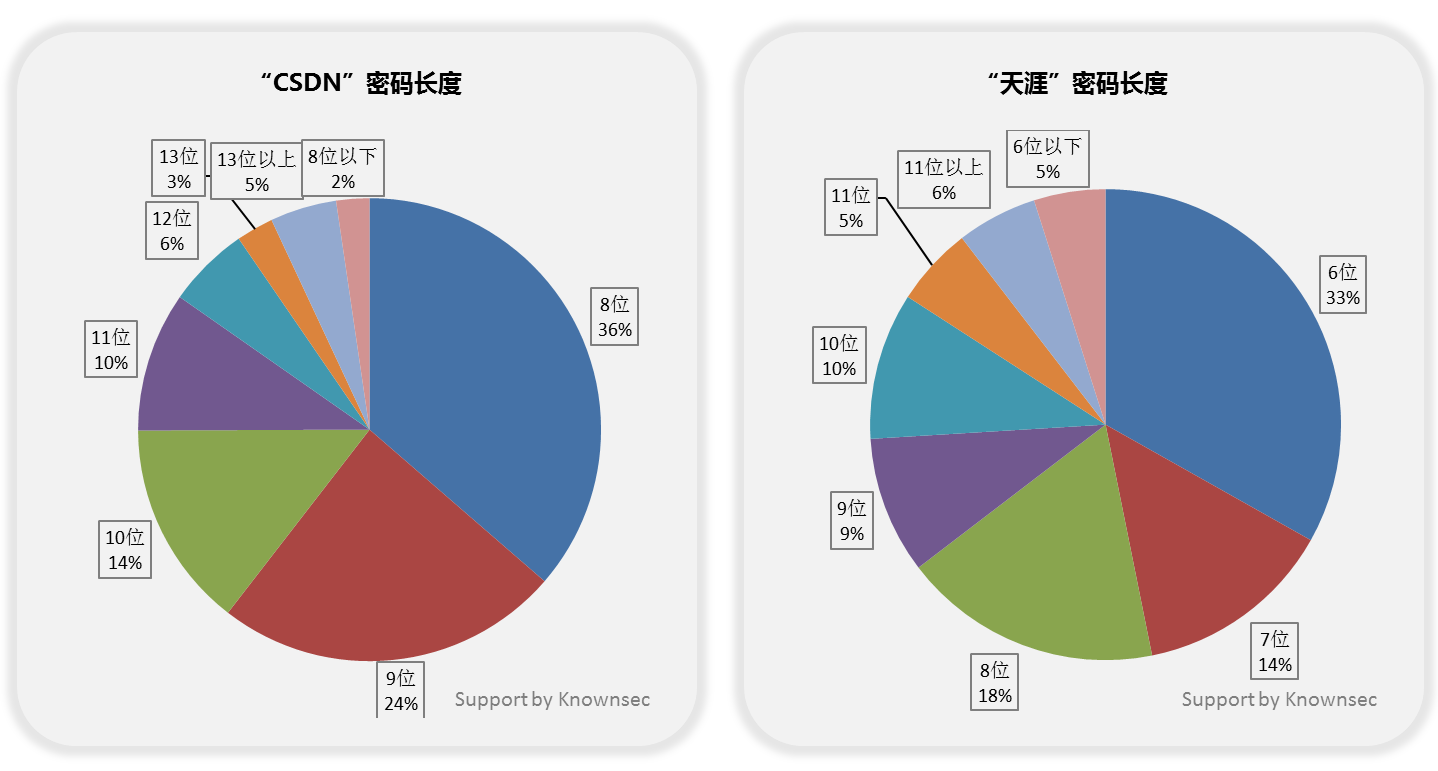


图3：用户密码长度分布情况

慎用个人信息做登录密码

个人信息作为密码的方法司空见惯。使用8位生日做密码的占6.03%，使用手机号做密码的占1.32%。

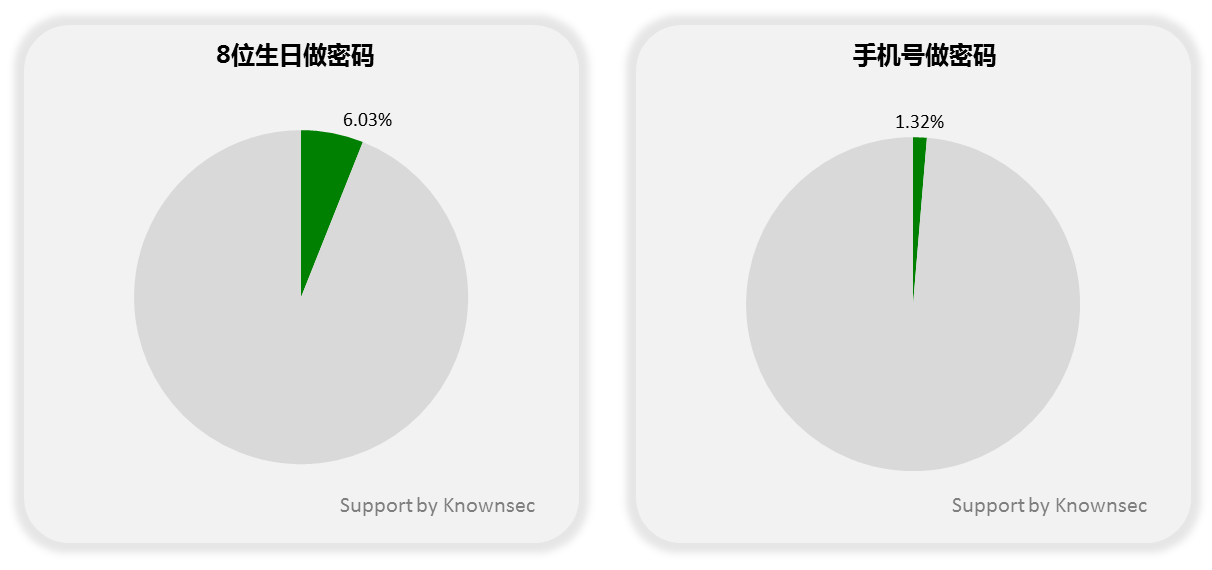


图4：使用个人信息作为密码的比例

职业/爱好与密码的关联度

通过分析发现，CSDN泄露数据中有13%的密码中包含用户名，但天涯泄露数据中这一数据仅占4.24%，显然搞IT的程序员更习惯使用这种密码。

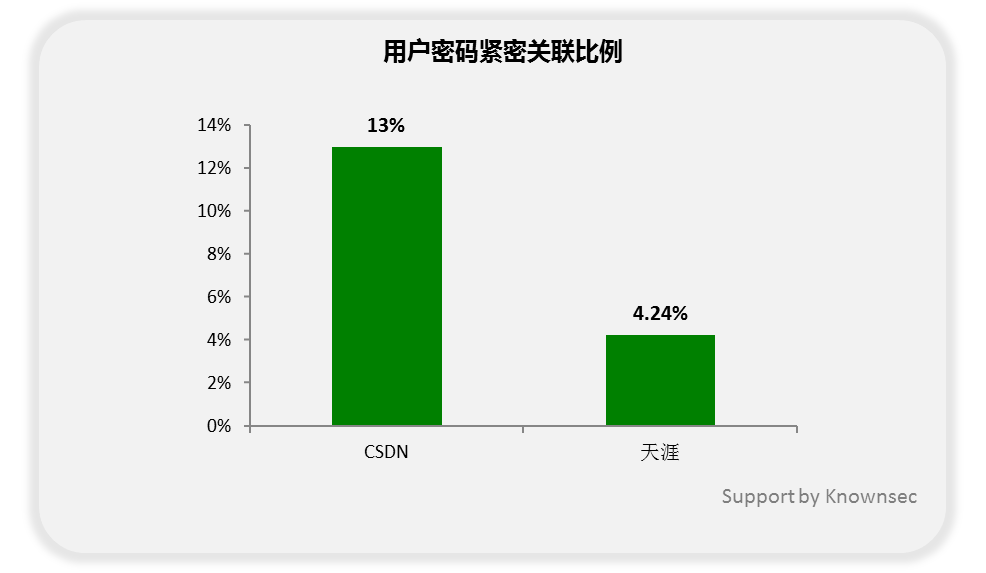


图5：用户密码与个人职业/爱好关联度

邮箱分布情况

通过分析CSDN和天涯的泄露信息发现，最常用被用来注册用户的邮箱是163邮箱和QQ邮箱，这两种信箱在CDSN泄露数据中据近60%的比例，在天涯泄露数据中则占据近40%，若这些用户在163或QQ信箱注册信息与CSDN或天涯的注册信息相同，则意味着，这些用户的信箱密码可能也会因此而泄露。

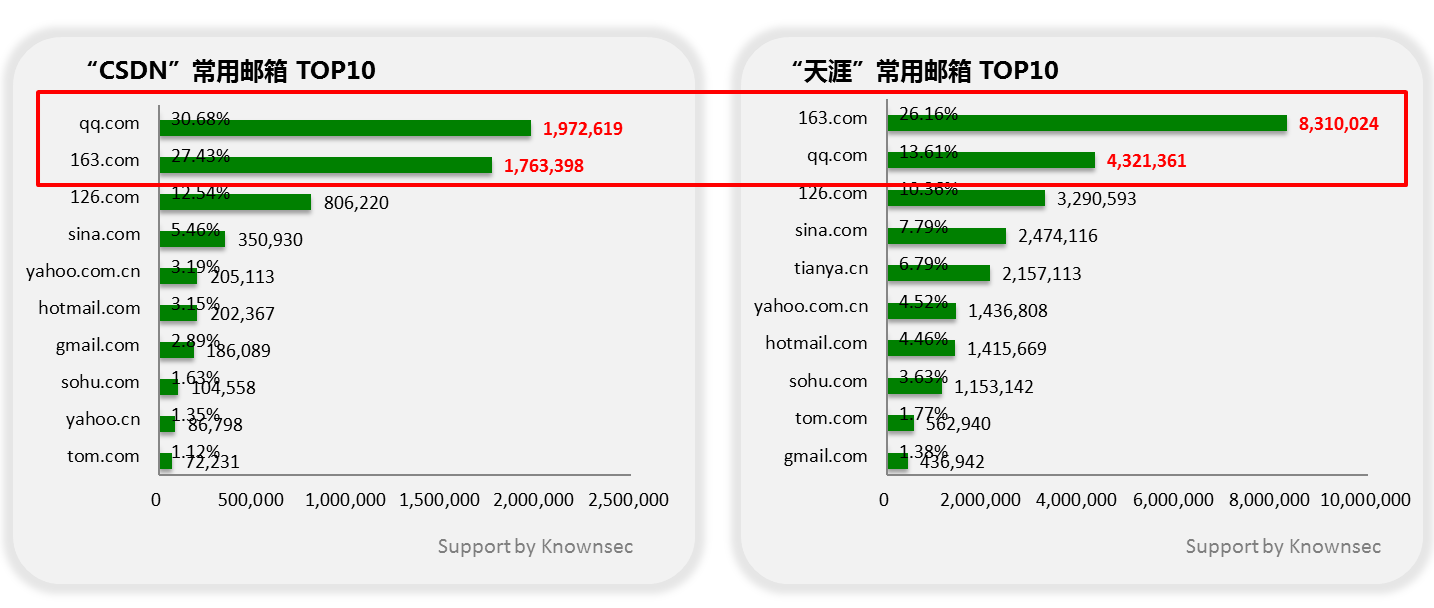


图6：常用邮箱分布情况

# 我们能做些什么？

透过近期的信息泄露事件的表面来看，还是暴露出互联网一些安全问题，如：网站服务提供商对用户数据保护不足（使用明文存储密码）、网站前端防护基于传统防护思路与方式等问题，对此，我们建议：

1. 国家及监管机构完善各行业的信息安全相关规定的同时监管机构引入专业的Web安全技术作为支撑手段，将安全方针有效落地
2. 大多数的信息泄露是由于Web安全漏洞造成的（例如SQL注入、XSS等），必须通过专业技术进行实时监控及防护
3. 广大互联网用户避免使用弱密码4并定期修改密码，避免登录没有经过安全认证或安全检测的网站

我们生活在互联网的时代，但我们的安全意识和安全手段却处于初级阶段。知道创宇公司是国内最早专注于提供互联网安全解决方案的创新型企业之一，我们的口号是“更好，更安全的互联网”。

*注1：全文可参考* [*http://www.cert.org.cn/articles/bulletin/common/2011123025709.shtml*](http://www.cert.org.cn/articles/bulletin/common/2011123025709.shtml)

*注2：弱密码指，由生日构成、由单独一个字母构成、包含用户名、由手机号码构成、最常用密码12345678、123456789构成的、由完整的一个英文单词构成的。*

*注3：密码147258369成为常见密码，是由于键盘上的数字小键盘排序而造成的。*

*注4：什么样的密码才算是强悍的密码？如：Kn0wnSec#^% —— 该密码有较高的长度，且 包含了大写字母（K和S）、小写字母（n、w、e、c）、数字（Kn0wn中的为数字0）和 特殊字符（#^%），但是，密码的前八位（即，Kn0wnSec）仍呈现出一定规律性，若将 此段设置为随机字符，则可使密码更为强悍。*