TREND MICRO™ Securing Your Web World

CSDN用户密码泄漏事件

Peter Zang • China Regional TrendLab

2011年12月21日

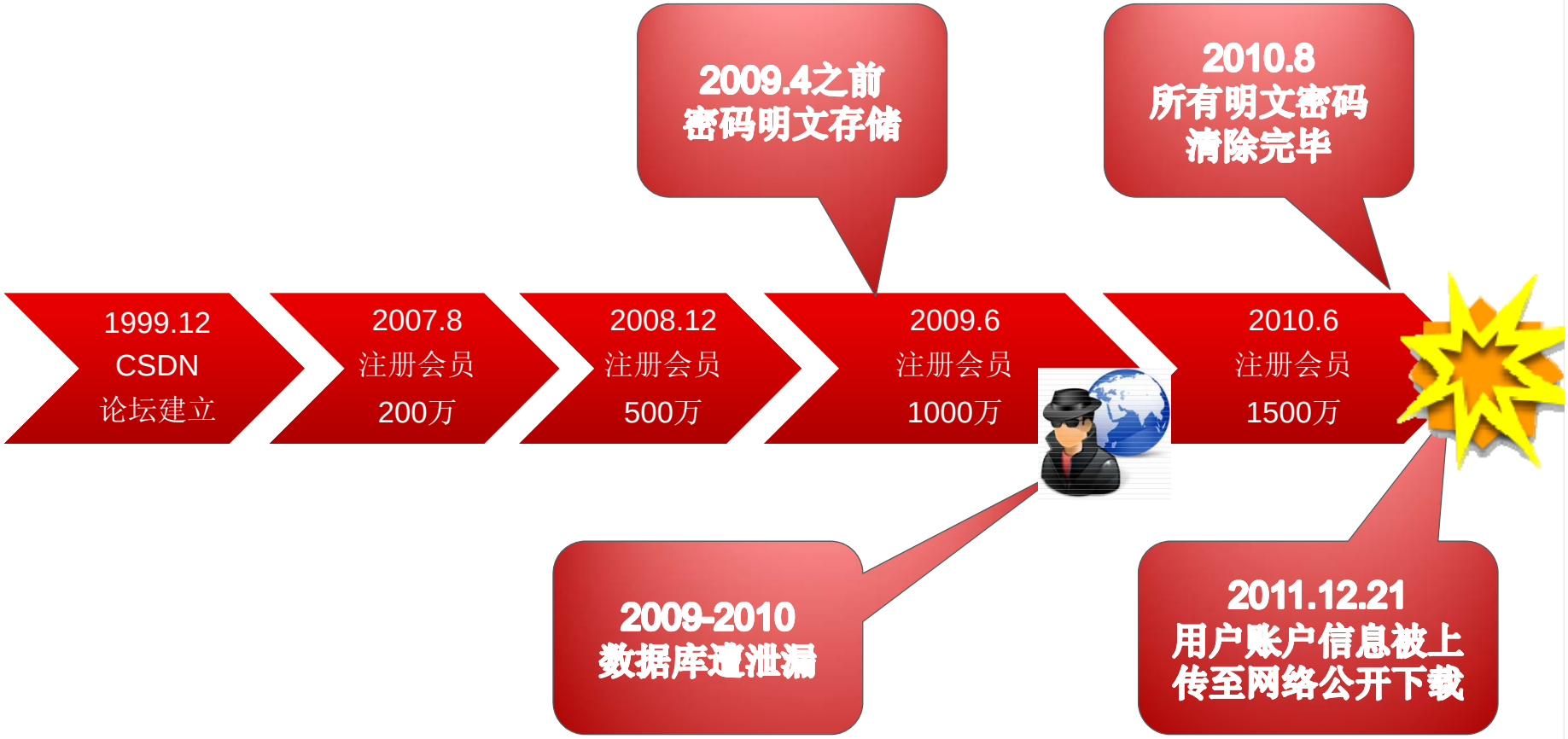
几乎整个中国的IT从业人员
都在讨论同一件事

CSDN用户帐号、密码及邮箱信息被曝

数量超过6,000,000

TREND MICRO

时间线



触目惊心的数据

程序员的安全习惯

TREND MICRO

那些坏习惯！

• 纯数字密码	**2,890,000+**
• 纯小写字母密码	**740,000+**
• 纯大写字母密码	**30,000+**
• 123456789做密码	**230,000+**
• 12345678做密码	**210,000+**
• 弱密码	**5,900,000+**

那些好习惯.....

长度**8位**以上

AND

同时使用**大写字母、小写字母、数字**

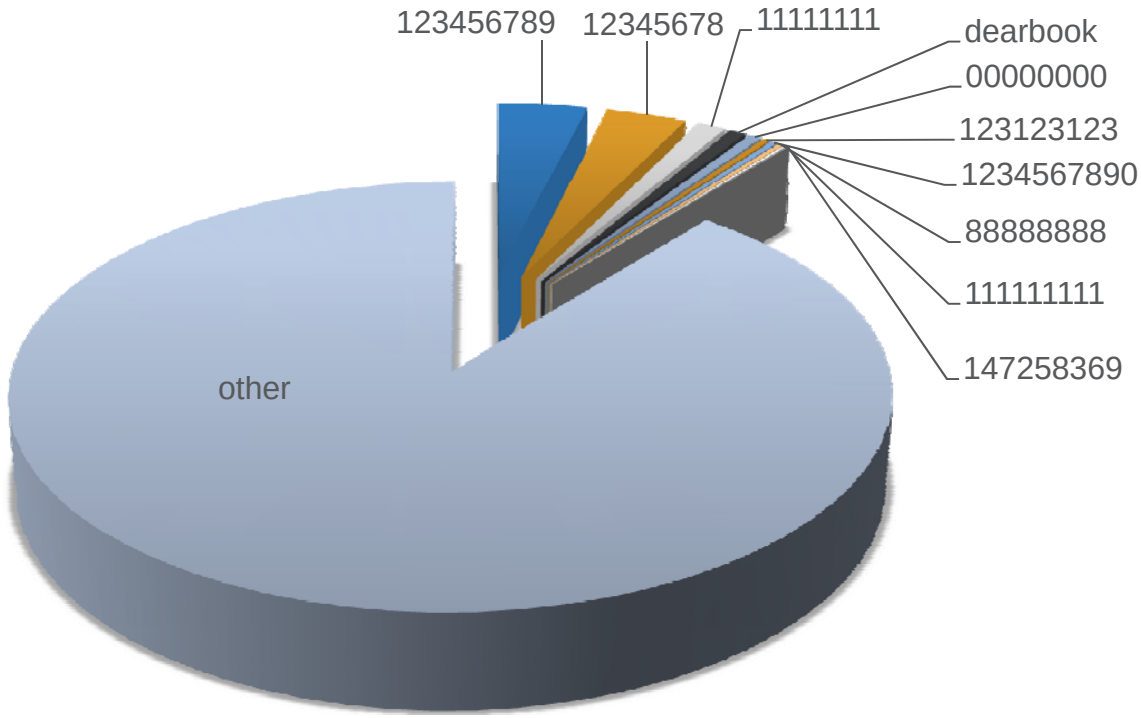
AND

不在常用的**密码字典**中

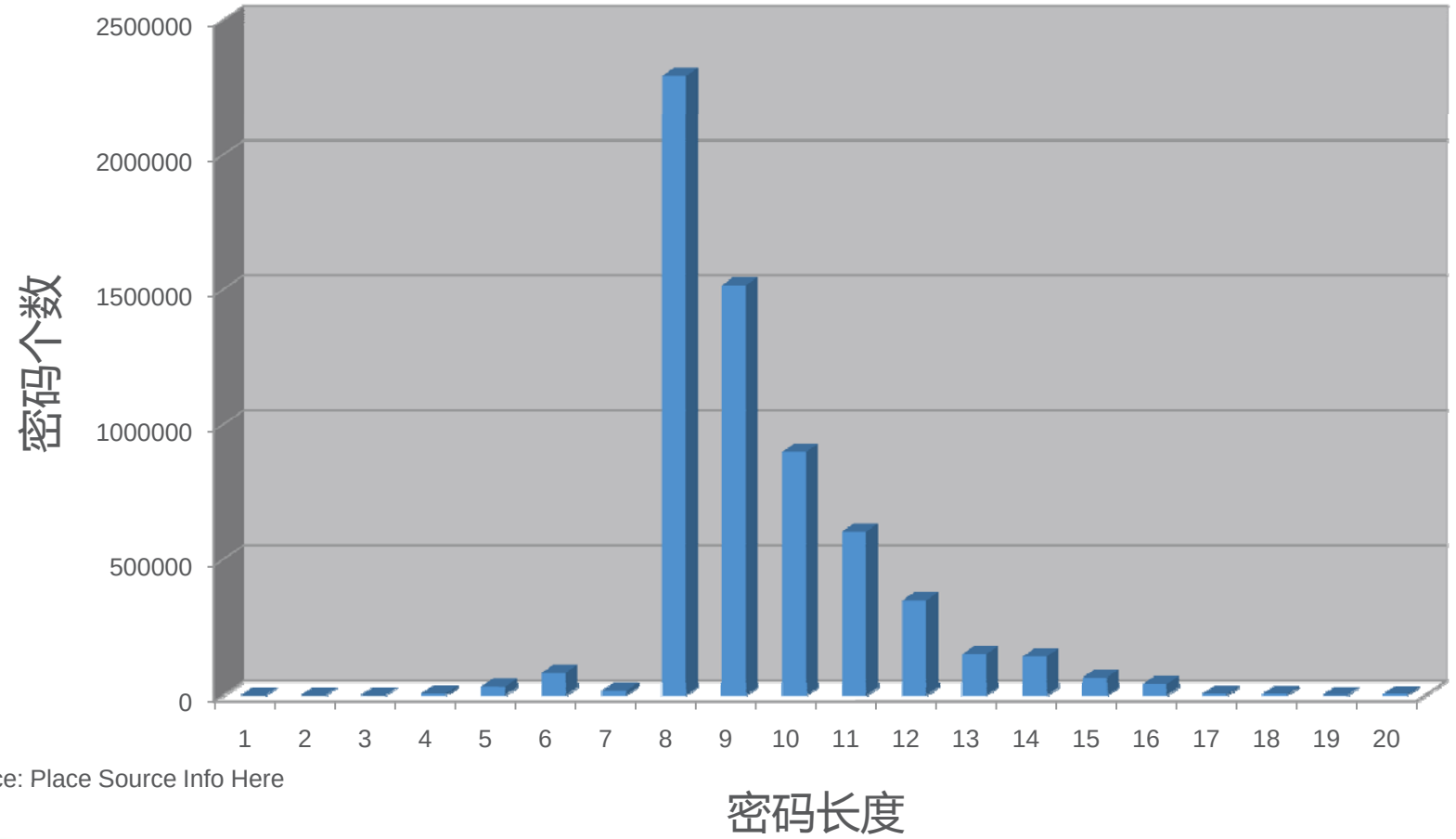
9,000-

CSDN常见密码TOP 10

- 123456789
- 12345678
- 11111111
- dearbook
- 00000000
- 123123123
- 1234567890
- 88888888
- 111111111
- 147258369



密码长度统计



Source: Place Source Info Here

需要担心什么？

数据泄漏的危害

TREND MICRO

个人信息泄漏

- 从CSDN泄漏的数据中
  - 包含**所有用户**的邮箱信息

  - 有**400,000+**的帐号使用生日做密码

  - 有**150,000+**的帐号使用手机号做密码

  - 有**250,000+**的帐号使用QQ号做密码

形同虚设的密码 – one for all

- 在CSDN泄漏的帐户中，有部分账户密码可以直接登录新浪微博、人人网等其他社交网站网站

可能的泄漏途径

- 网页漏洞
- 数据库漏洞
- 系统漏洞
- 内部人员泄漏
- 数据或托管商泄漏
- ……

我们能做什么？

作为用户的我们

密码安全

- 建议：
  - 尽可能使用至少**14个字符或更多**。
  - 您的密码中的字符**变化越多越好**。
  - **使用整个键盘**，而不仅仅是经常使用或看到的字母和字符。
  - **定期更换密码**
- 避免
  - **任何语言的单词或短句**。例如：iloveyou, password
  - **倒拼单词、常见的错误拼写和缩写**。例如：drowssap, p@ssw0rd
  - **顺序或重复的字符。** 例如：12345678、222222、abcdefg或键盘上的相邻字母 (qwerty)。
  - **个人信息**。 例如：名字、生日、驾驶证、护照号码或类似信息。
  - **长期使用同一个密码**
  - **所有网站帐号使用同一个密码**

如何生成一个强壮的密码？

- 找依据熟悉的句子（中文/英文）
  - 我需要一个安全的密码
- 取出每个单词的首字母/拼音首字母
  - wxyygaqdmm （10位）
- 使用大小写混输
  - WXYYGaqdmm （10位）
- 在特定位置添加一些只有你自己知道含义的数字
  - WXYYG17084aqdmm （15位）
- 添加一些符号
  - #WXYYG17084aqdmm~ （17位）
- 添加相应的应用缩写
  - #WXYYG17084aqdmm~gml （20位）Gmail密码
  - #WXYYG17084aqdmm~qq （19位）QQ密码
  - #WXYYG17084aqdmm~msn （20位）MSN密码

测试一下自己的密码强度

- 网上有许多测试密码强度的网站
  - 测试密码的复杂度
  - 测试密码是否在常见的密码字典中

https://www.microsoft.com/security/pc-security/password-checker.aspx
http://howsecureismypassword.net/
http://am22tech.com/s/22/Tools/PasswordStrengthChecker.aspx

我们能做什么？

作为服务提供商的我们

TREND MICRO

用户越多，责任越大！

用户数据安全保护

- 妥善保护用户的用户名和口令
  - 限制用户输入一些非常容易被破解的口令
  - 不要明文保存用户的口令
  - 根据情况决定是否让浏览器保存口令
  - 使用安全的方式在网上的传输口令
- 妥善管理用户登录状态
  - 不要在cookie中存放用户的密码
  - 正确设计“记住密码”功能
  - 不要让cookie有权限访问所有的操作
  - 权衡cookie的过期时间
- 口令探测防护
  - 使用验证码
  - 设置用户口令失败次数
  - 系统全局防护

人祸甚于天灾

“世界上所有曾经最坚固的堡垒，都是从内部瓦解的。”

- 增强员工安全意识
- 部署完整的信息安全系统
- 完善信息安全管理流程

谁会是下一个？

后续情况

TREND MICRO

CSDN的道歉信

http://news.csdn.net/a/20111221/309505.html

【公告】致CSDN会员的公开道歉信

2011-12-21 20:41 | 181330次阅读 | 来源：CSDN【已有1259条评论】发表评论
关键词：csdn | 作者：CSDN | 收藏这篇资讯

尊敬的CSDN会员：

我们非常抱歉，近日发生了CSDN用户数据库泄露事件，您的用户密码可能被公开。我们恳切地请您修改CSDN相关密码，如果您在其他网站也使用同一密码。请一定同时修改相关网站的密码。

再次向您致以深深的歉意！

关于CSDN网站用户帐号被泄露的声明：

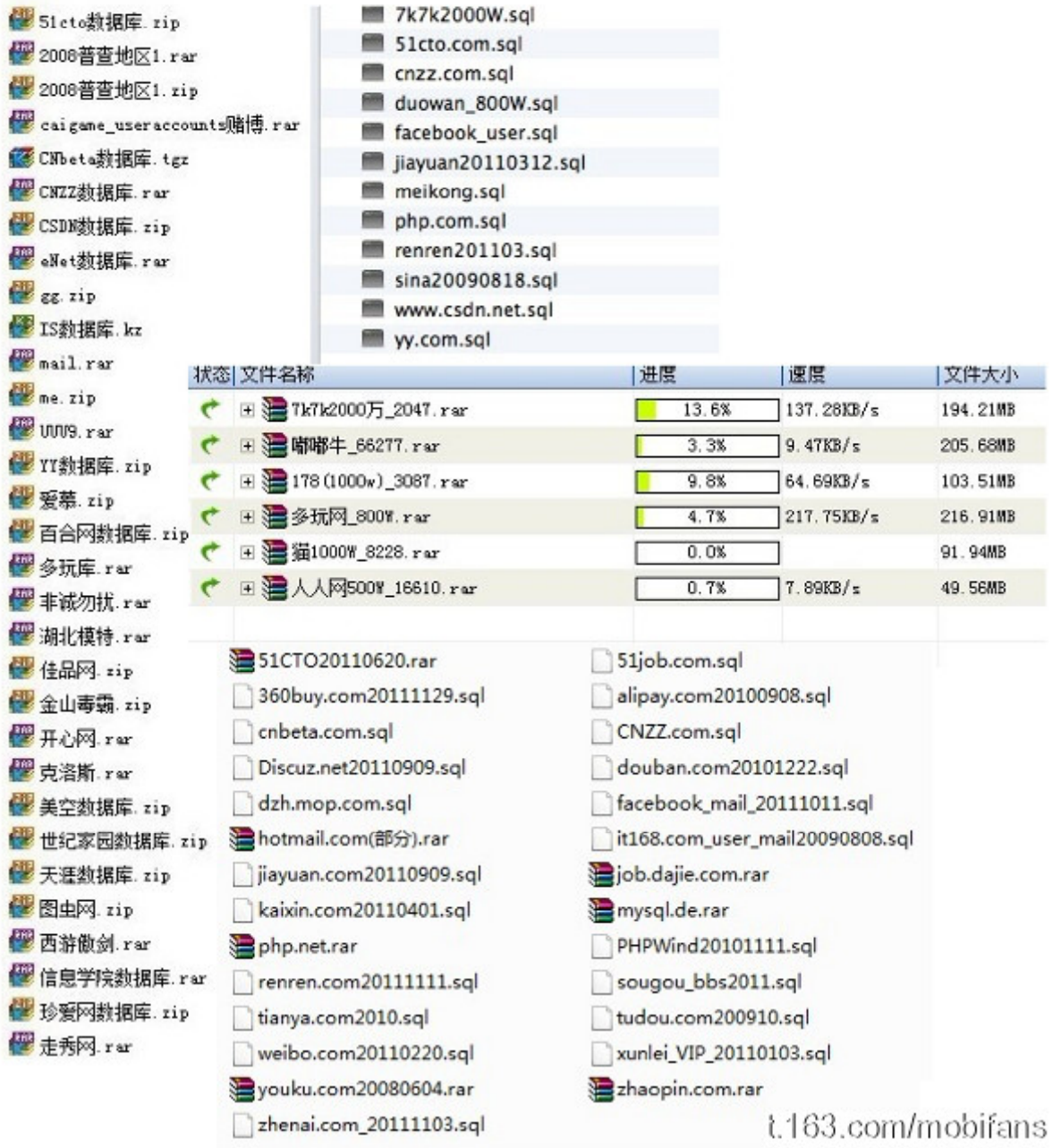
CSDN网站早期使用过明文密码，使用明文是因为和一个第三方chat程序整合验证带来的，后来的程序员始终未对此进行处理。一直到2009年4月当时的程序员修改了密码保存方式，改成了加密密码。

但部分老的明文密码未被清理，2010年8月底，对帐号数据库全部明文密码进行了清理。2011年元旦我们升级改造了CSDN帐号管理功能，使用了强加密算法，解决了CSDN帐号的各种安全性问题。

TREND MICRO

但事情并没有结束

- **人人网**被曝数据泄漏
- **178**被曝数据泄漏
- **多玩**被曝数据泄漏
- **百合网**被曝数据泄漏
- **51CTO**被曝数据泄漏
- **……**



To be continued…

TREND MICRO