图虫网 - 沈振宇

我们收到来自一个与图虫网(tuchong.com)关系密切的人的来信，说图虫网近期可能发布手机 APP 的消息，希望拿到图虫网手机 APP 的设计方案和源代码，由此展开的一系列工作。

首先要做的是收集信息，先从 whois 信息下手：

```
Domain Name : tuchong.com

Registrar: eName Technology Co.,Ltd.

Registrant Contact Information :
ShenZhenyu
Shen Zhenyu
zhenyupku@gmail.com
CN shang hai shang hai No.236 Lane.1333 Meichuan Rd. 200333
tel: 86 13811777117
fax: 86 13811777117
```

站长注册 Email 信息为：zhenyupku@gmail.com

从天涯数据库第 47 库查到这个 email 地址的常用密码是 lucylucy

不过用这个密码登陆 Gmail 提示失败，登陆 Gmail 找回密码提示绑定手机为 117 结尾，域名 whois 中登记的信息应该是真实的。既然是上海的大城市，用 Gmail 和密码 lucylucy 登陆一下陌陌，发现成功。

真实姓名：沈振宇，陌陌号 1165378，注册 Email 是 zhenyupku@gmail.com，登陆，密码是 lucylucy。这个人就是图虫网的站长了，也就是主要目标了。

如果用手机直接登陆陌陌，原本登陆陌陌的设备会提示下线，得知陌陌号以后可以用自

己的陌陌号先查看一下登录时间和距离。

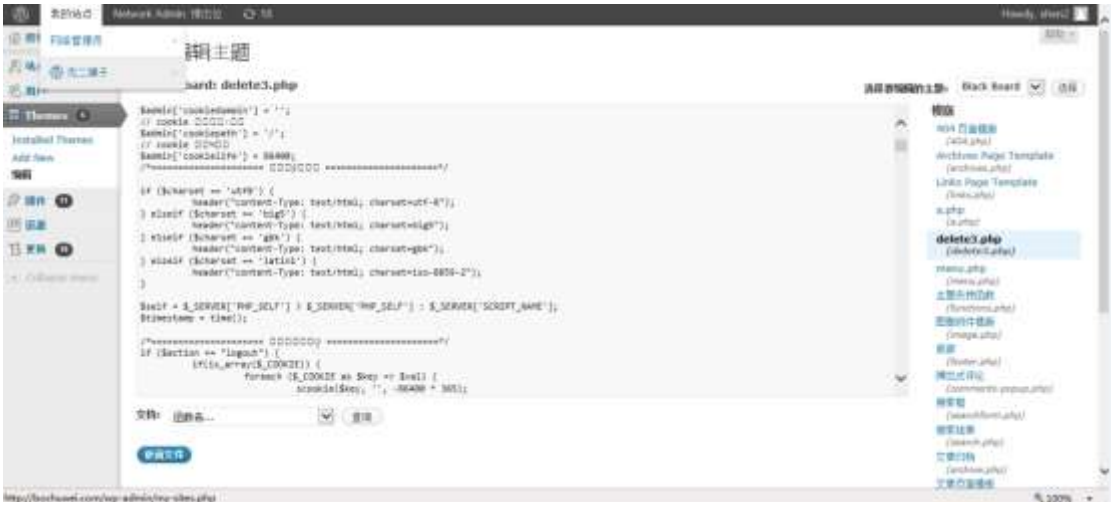
陌陌资料就叫沈振宇，提示上一次登陆是 41 天前，10934KM 距离是国内，看来 email 中的 pku 指的就是毕业于北京大学了。在沈振宇的资料末端的个人主页看到这样的资料：

首先是可以确认目标没有偏，另外一个是从中得到了一些信息，沈振宇高中就读于复旦大学附属中学，考入北京大学，个人博客主页是 http://shen2.cn/

打开个人主页，发现是个 wordpress 站点，直接访问 wp-login.php 可以登陆后台，猜了

几个用户名，admin,zhenyu,shenzhenyu,zhenyupku,shenzheyupku 都不对，发现用户名 shen2 是正确的，密码就是 lucylucy，成功登陆。

按照这个架构，应该是同一个 wordpress 程序，上面跑了很对分站，解析了多个域名。因此可以进入站点管理“网络管理员”，在主题或者插件编辑处获取权限。



不过在这里我已经发现有前人的足迹了，看到好几个 webshell，最早的后门是在 2013 年 1 月 1 日创建的。在服务器的数据库配置发现另外一个密码是 qingchunwuhui!407，后面发现一些备案用的是这个密码。

继续使用 zhenyupku@gmail.com 搜索网上相关信息，来确认站长更多信息。在网上搜到了一点有意思的东西，是几年前沈振宇注册的站点，同样的密码也是 lucylucy，不知道 lucy

是何方神圣。

同时也可以确认到站长沈振宇的 QQ 号是：27102887

接下来就是对站长的 Email 展开社工了。

还是从个人博客下手。在个人博客后台中登记的 Email 地址是 zhenyu@tuchong.com，是图虫网的企业邮箱。

来查一下图虫网的 MX 记录：

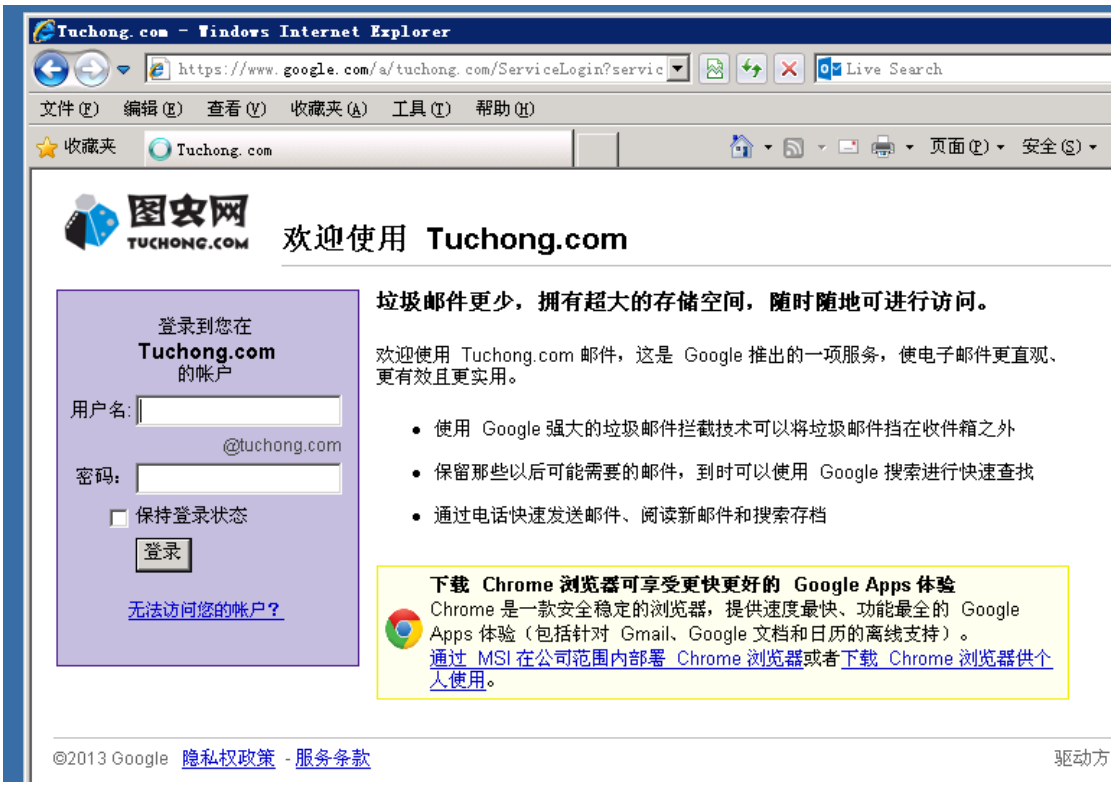
mx:tuchong.com Find Problems mx

Pref	Hostname	IP Address	TTL		
10	ASPMX.L.GOOGLE.COM	173.194.64.26	4 hrs	Blacklist Check	SMTP Test
20	ALT1.ASPMX.L.GOOGLE.COM	74.125.137.26	4 hrs	Blacklist Check	SMTP Test
20	ALT2.ASPMX.L.GOOGLE.COM	173.194.68.26	4 hrs	Blacklist Check	SMTP Test
30	ASPMX2.GOOGLEMAIL.COM	74.125.137.26	4 hrs	Blacklist Check	SMTP Test
30	ASPMX3.GOOGLEMAIL.COM	173.194.68.26	4 hrs	Blacklist Check	SMTP Test

图虫网的企业邮箱是解析到 Gmail 的，登陆地址就是：

mail.google.com/a/tuchong.com

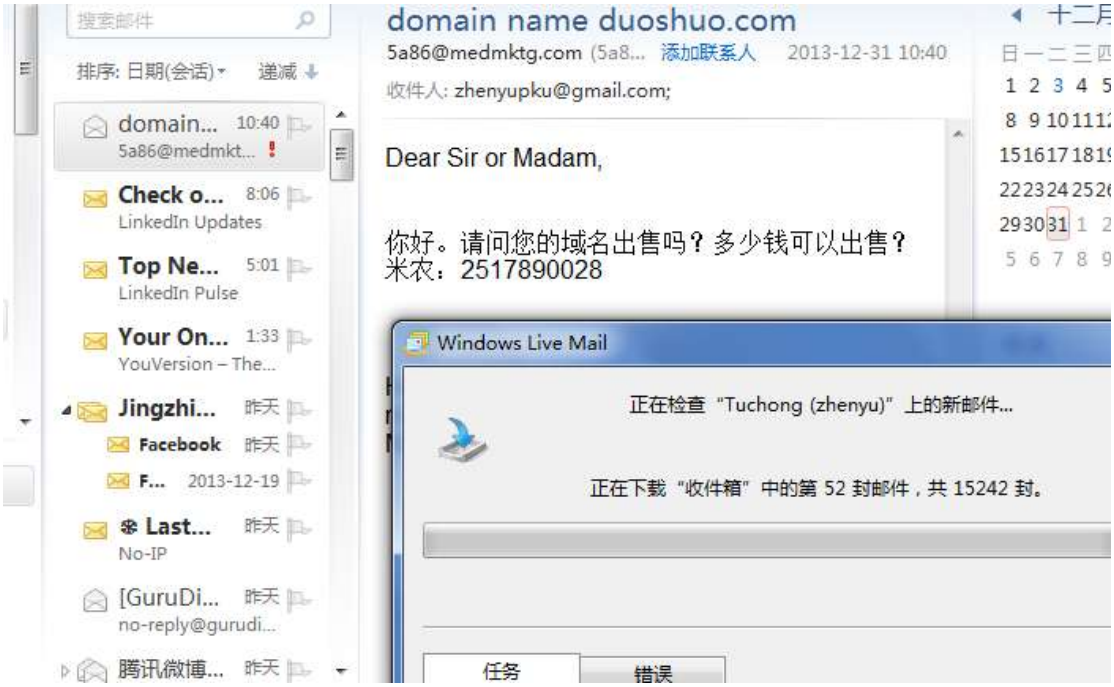
访问这个地址发现成功打开登陆页面：



考虑到图虫网对用户登陆的 ip 会有限制，我挂了个上海的服务器做代理来登陆。密码仍然是 lucylucy。

登陆后发现沈振宇吧所有的 Email 全都用 Gmail 的企业邮箱来登陆接收了：

Email 一共有：zhenyu@tuchong.com,zhenyupku@gmail.com,zhenyushen@sina.com,webmaster@poj.org,webmaster@tuchong.com,zhenyushen@intern.xiaomi.com，这样就省去了很多麻烦。



因为可以一次性将所有的 Email 都收完了。

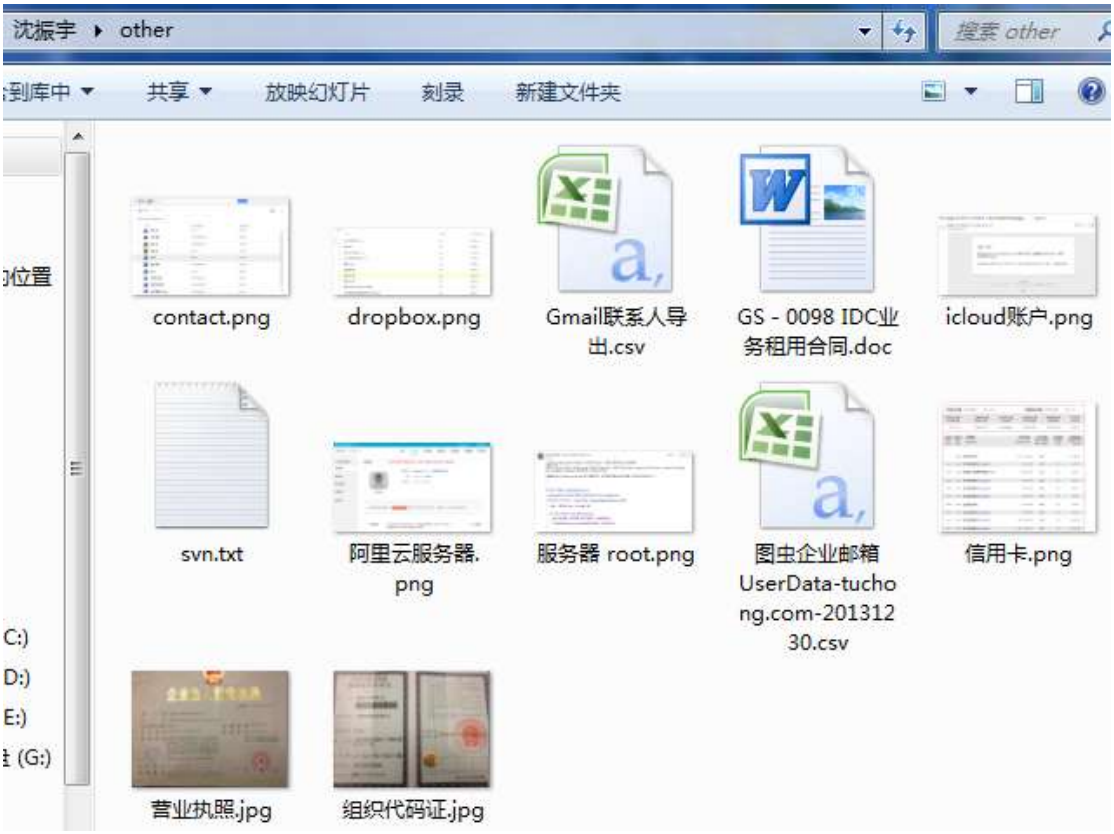
首先是找到了设计方案：

很符合 Windows8 的风格。然后是源码：

tree.txt

```
文件夹 PATH 列表
E:\TUCHONG-GALLERY
├─TuChong-Gallery
│   │  .DS_Store
│   │
│   ├─.git
│   │   │  config
│   │   │  description
│   │   │  HEAD
│   │   │  index
│   │   ├─branches
│   │   ├─hooks
│   │   │      applypatch-msg.sample
│   │   │      commit-msg.sample
│   │   │      post-update.sample
│   │   │      pre-applypatch.sample
│   │   │      pre-commit.sample
│   │   │      pre-push.sample
│   │   │      pre-rebase.sample
│   │   │      prepare-commit-msg.sample
│   │   │      update.sample
│   │   ├─info
│   │   │      exclude
│   │   ├─objects
│   │   │  ├─00
│   │   │  │      15e16c14ab58da5bd1a23504d00b4c2eeaae0f
```

收工之前还找了些别的东西：



还有站长父亲，45%股份的大股东的信息：

```
律师姓名： 沈伟明
律师事务所： 上海市三石律师事务所
性　别： 男
民　族： 汉族
政治面貌： 中共党员
学　历： 本科
执业范围： 金融、公司、劳动
执业状态： 正常执业
执业类别： 专职律师
首次执业时间： 1991-10-01
执业证号： 0919911106381
个人主页：
E-mail： shen71@citiz.com
shen717171@163.com

执业范围：
公司法　金融　劳动人事
执业证号：
13101199110872097
考核结果：
称职
个人主页：
E-mail：
Shen717171@163.com

http://mc.lawyers.org.cn/huangye/website/lawfirm.jsp?id=1e12902dcf4b43d19f6bcd43cfe6e85f

http://mc.lawyers.org.cn/huangye/website/lawyer.jsp?id=27c470ffb4bc4e62b9627e2dc18d6374


邮箱：ITLAW@163.COM
QQ：37632400
地址：上海市黄浦区黄河路355弄雅州大厦1号楼715室
邮编：200003
电话/传真：021-51028890
http://www.itlaw.com.cn/contact.html
```