黑客探秘民营五百强企业邮服变诈骗温床

笔者近期收到了一封诈骗的 Email，其实像这种诈骗类的 Email 再普通不过了，几乎每天都能收到那么几封。

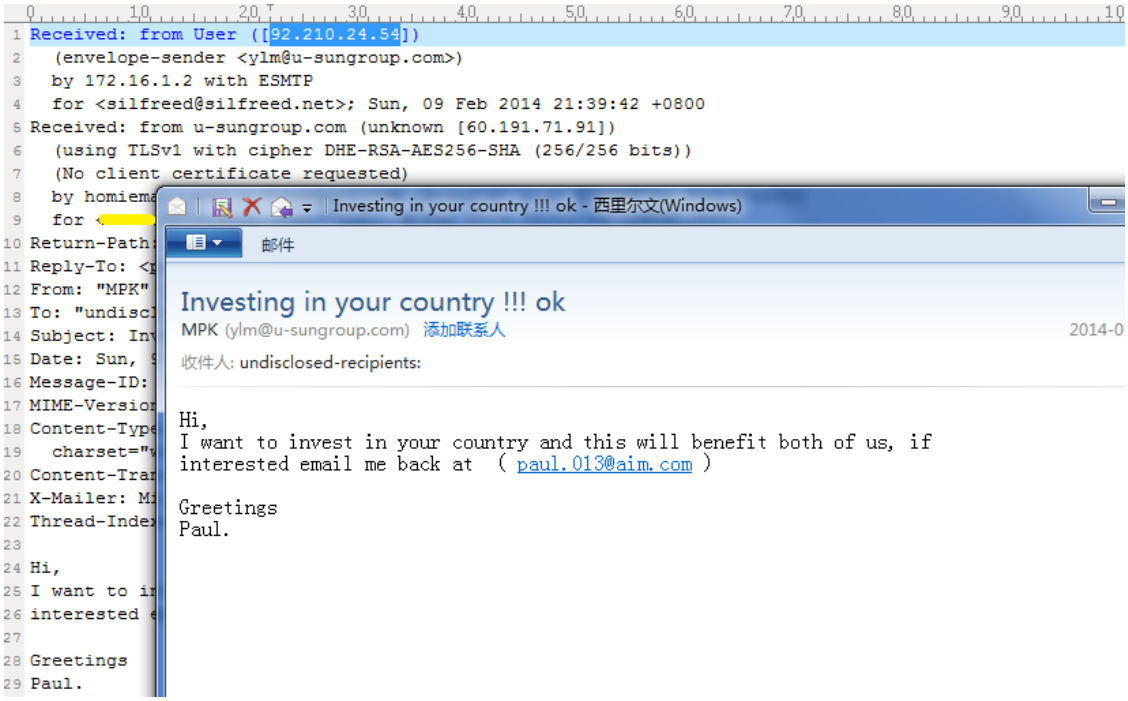
令笔者觉得不可思议的是通过这封 Email 分析，笔者看到了一条由国际黑客主导的黑色利益产业链，在国际媒体大肆渲染中国黑客威胁论大背景下，许多中国的企业邮服却成为了国际犯罪团伙的炮灰。

笔者通过非正常手段调查后发现多数中枪的是中国大陆的企业邮箱，而这其中甚至还有民营企业 500 强，黑客通过这些邮服四处发送诈骗邮件，不仅损坏了中国的网络形象，也直接损害了中国的经济利益。

笔者收到的 Email 其实只有短短了几行，大意如下：

“我想在贵国家进行投资，(投资)将对我们双方都有利，如果感兴趣请回复我。。。”

对于这种 Email 笔者感觉就类似于“我在东莞被抓了，速汇 5000 元到 x 警官卡里，别打电话，出来再说，快！”一样可笑。



通过邮件头可以看到这封 Email 由 92.210.24.54 一个德国 ip 发送出。

诡异的地方是发件人的域名 u-sungroup.com 却是浙江永翔集团的主站域名。

从邮件头也可以看到发送邮件的服务器 ip 是 60.191.71.91，然后笔者通过 dig 命令查看了 u-sungroup.com 的 MX 解析记录如下。

```
; <<>> DiG 9.3.4-P1 <<>> MX u-sungroup.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34157
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; QUESTION SECTION:
;u-sungroup.com.                        IN      MX

;; ANSWER SECTION:
u-sungroup.com.         3600    IN      MX      10 mail.u-sungroup.com.

;; AUTHORITY SECTION:
u-sungroup.com.         172799  IN      NS      ns4.dns-diy.com.
u-sungroup.com.         172799  IN      NS      ns3.dns-diy.com.

;; ADDITIONAL SECTION:
mail.u-sungroup.com.    3600    IN      A       60.191.71.91
ns3.dns-diy.com.        147669  IN      A       218.107.207.23
ns3.dns-diy.com.        147669  IN      A       60.191.248.79
ns4.dns-diy.com.        161288  IN      A       222.76.219.47
```

图中显示该域名的 MX 解析记录为 mail.u-sungroup.com，而起邮服的 ip 正是 60.191.71.91。

这意味着什么呢？这意味着这封 Email 并不是伪造，至于是不是账号被盗，估计也八九不离十。

笔者补充一下，虚假 Email 有很多种，通常分为完全伪造的 Email 和盗用账号发送的欺诈的 Email，其区别在于前者可以在任意一台机器上进行伪造，后者则是盗用账号后登陆发送的，后者除了正文外其他部分和进行正常网络活动的 Email 没有两样，不容易被反垃圾邮件系统拦截。

笔者发现永翔集团的各个网站其实是和邮服在同一个 ip 下的，通过历遍目录漏洞笔者发现了网站的数据库和一枚疑似 webshell 的文件。疑似后门的脚本路径在/admin/manage/databackup/ice.asp。

笔者通过数据库管理员账号登陆后台后使用数据库备份功能将 ice.asp 备份为.txt 文件后得到该一句话后门密码为：icesword，于是顺着其他黑客的后门就上来了。

脚本显示后门创建时间是 2012-11-25 21:31:02，后来笔者又找到几个后门，分别是根目录的 ad.asp(创建于 2012-11-25 22:02:51)、根目录的 zer0.asa(创建于 2012-11-25 21:35:49，密码 000000) 和根目录的 test.asp(创建于 2012-11-25 21:38:19，密码 S.S.T)。

这几个后门创建于同一天，根据其创建的时间基本可以确定没有修改过文件创建时间。

根据笔者的直觉，这个古老的后门显然只是国内小黑通过 ewebeditor 编辑器搞上来的，跟发 Email 的诈骗犯不是同一批。

那么不妨来看看 Email 的记录。

```
2014/02/09-21:46:55 113296 Connect from 92.210.24.54
2014/02/09-21:46:55 113296 command = EHLO User
2014/02/09-21:46:55 113296 max message size = 41943040
2014/02/09-21:46:56 113296 command = AUTH LOGIN
2014/02/09-21:46:58 113296 smtp authenticate success! Username = ylm@u-sungroup.com
2014/02/09-21:46:58 113296 command = RSET
2014/02/09-21:47:01 113296 command = MAIL FROM:<ylm@u-sungroup.com>
2014/02/09-21:47:01 113296 mail from = ylm@u-sungroup.com
2014/02/09-21:47:01 113296 command = RCPT TO:<wolvertonbenefice@gmail.com>
2014/02/09-21:47:01 113296 rcpt to = wolvertonbenefice@gmail.com
2014/02/09-21:47:02 113296 command = RCPT TO:<wolves@googlegroups.com>
2014/02/09-21:47:02 113296 rcpt to = wolves@googlegroups.com
2014/02/09-21:47:02 113296 command = RCPT TO:<wolvesdouglasco@gmail.com>
```

```
2014/02/09-21:47:02 113296 rcpt to = wolvesdouglasco@gmail.com
2014/02/09-21:47:03 113296 command = RCPT TO:<wolveshawks@aol.com.attendees>
2014/02/09-21:47:03 113296 rcpt to = wolveshawks@aol.com.attendees
2014/02/09-21:47:04 113296 command = RCPT TO:<wolvie71us@yahoo.com>
2014/02/09-21:47:04 113296 rcpt to = wolvie71us@yahoo.com
2014/02/09-21:47:04 113296 command = RCPT TO:<wolwitz@gmail.com>
2014/02/09-21:47:04 113296 rcpt to = wolwitz@gmail.com
2014/02/09-21:47:05 113296 command = RCPT TO:<wolyby@yahoo.com>
2014/02/09-21:47:05 113296 rcpt to = wolyby@yahoo.com
2014/02/09-21:47:05 113296 command = RCPT TO:<wom@vsattui.com>
2014/02/09-21:47:05 113296 rcpt to = wom@vsattui.com
2014/02/09-21:47:06 113296 command = RCPT TO:<woma@ix.netcom.com>
2014/02/09-21:47:06 113296 rcpt to = woma@ix.netcom.com
2014/02/09-21:47:06 113296 command = RCPT TO:<woma1@hotmail.de>
2014/02/09-21:47:06 113296 rcpt to = woma1@hotmail.de
2014/02/09-21:47:07 113296 command = RCPT TO:<womack5@bellsouth.net>
2014/02/09-21:47:07 113296 rcpt to = womack5@bellsouth.net
2014/02/09-21:47:07 113296 command = RCPT TO:<womacks4@jps.net>
2014/02/09-21:47:07 113296 rcpt to = womacks4@jps.net
2014/02/09-21:47:08 113296 command = RCPT TO:<womadbelfast@gmail.com>
2014/02/09-21:47:08 113296 rcpt to = womadbelfast@gmail.com
2014/02/09-21:47:08 113296 command = RCPT TO:<womam999@gmail.com>
2014/02/09-21:47:08 113296 rcpt to = womam999@gmail.com
2014/02/09-21:47:09 113296 command = RCPT TO:<woman@flointer.com>
2014/02/09-21:47:09 113296 rcpt to = woman@flointer.com
2014/02/09-21:47:09 113296 command = RCPT TO:<woman@me.com>
2014/02/09-21:47:09 113296 rcpt to = woman@me.com
2014/02/09-21:47:10 113296 command = RCPT TO:<woman2no@yahoo.com>
2014/02/09-21:47:10 113296 rcpt to = woman2no@yahoo.com
2014/02/09-21:47:10 113296 command = RCPT TO:<womanchildc@gmail.com>
2014/02/09-21:47:10 113296 rcpt to = womanchildc@gmail.com
2014/02/09-21:47:11 113296 command = RCPT TO:<womanistmusings@gmail.com>
2014/02/09-21:47:11 113296 rcpt to = womanistmusings@gmail.com
2014/02/09-21:47:11 113296 command = RCPT TO:<womanlakelodge@ds.net>
2014/02/09-21:47:11 113296 rcpt to = womanlakelodge@ds.net
2014/02/09-21:47:12 113296 command = DATA
2014/02/09-21:47:12 113296 go ahead, end data with CRLF.CRLF
2014/02/09-21:47:16 113296 data bytes received = 552
2014/02/09-21:47:17 113296 message[1391953636.3488.113296,S=727] accepted for delivery
2014/02/09-21:47:17 113296 command = QUIT
2014/02/09-21:47:18 113296 End connection
```

笔者随便贴上日志中的一个完整的连接记录。

从日志中可以看出该黑客手段非常专业，使用自建程序开 10 个并发 smtp 连接，每个连接处理 20 个 email 发送请求。

日志的第一段是处理时间，第二段是 smtp 的 id，第三段是命令，笔者观察这个邮服日常的 smtp 的 id 不会过万，而笔者截取的这部分 ip 已经上了十万的级别，可以想象一共有多少人收到了诈骗 Email，上当率为万分之一的话那么会有多少。。。

而事实上，笔者统计到大约有超过 5000 条 Email 回信。

笔者深入对服务器日志进行分析发现，提出以下几个论点。

1, 黑客并不是通过暴力破解获取的账号和密码，因为发送垃圾邮件的账号存在多个；

笔者的统计信息收集自互联网，有很多人把自己收到的 Email 贴出来，例如 wtt,sjj 等账号。

2, 选择从未登陆的账户进行操作，不进行 pop3、imap 和 webmail 登陆，直接连接 smtp 发送 email；

黑客操作的僵尸账户的<createtime>字段和<lastvisittime>字段中的时间戳通常一样。

3, 黑客并不进行提权、脱裤等多余行为，Email 发送完成后清理后门跑路。

看到部分文件夹的修改日期为 2014 年 2 月，但是访问文件夹后发现目录下没有任何一个文件是 2 月创建或者修改的。

既然从服务器上得不到太多有用的信息，笔者只能对 paul.013 进行社工。

其实网上已经有红领巾揭露这个哥们的诈骗行为，在 blogspot 上面以随机字符生成 n 个地址，在上面发布 n 条垃圾信息和诈骗信息。

不过笔者想说，blogspot 上面的推广似乎并不是诈骗者本人，而是诈骗者在地下渠道发布的推广信息，进行推广的则是某些国产小黑？

笔者获得的诈骗者信息如下。

诈骗专用邮箱：paul.013@aim.com ， ch_colin@aim.com

诈骗邮箱的安全邮箱：s*****e@gmail.com

其他邮箱：ccolin147@cs.com ， paulk1@paulk.onmicrosoft.com
Hotmail 邮箱：ccolins@outlook.com
私人邮箱：ccolins@wp.pl ， ccolins@me.com
电话号码：*******17

统计了几个 ip 都是德国和波兰的，这里就不发了，最终查到这个哥们似乎是汽修出身，居住于离德国非常近的 PLAC ODRODZENIA(属波兰)。

最后笔者统计了一下中枪的邮服，有中国的和巴西的，以中国的居多，除了文中列出的浙江永翔集团，还有例如 conteck.net.cn(橙子云)，xjee.cn 等。

小编后记：

本文由习科论坛会员 xiaotianx 供稿，文章思路不错，故被小编选稿刊登，希望在社工学习和犯罪取证方向给大家带来一些启示。

另外小编特此提醒：入侵他人服务器的行为是非法的，这种未经授权的取证方式习科坚决不提倡不支持。另外我们已经在北美向国际刑警递交了该“汽修”黑客大神的相关信息，习科作为安全厂商坚决支持打击网络黑客犯罪行为。