



邮件攻击密取与社工

安洵信息技术有限公司

谷计划

VSRC成都沙龙站



目 录

C O N T E N T S

1

社工概述

2

信息收集

3

社工案例

4

邮件社工

谷计划

VSRC成都沙龙站

社工概述

社会工程学 (Social Engineering) 是一种通过人际交流的方式获得信息的非技术渗透手段。

社会工程学是黑客米特尼克在《欺骗的艺术》中率先提出的，其初始目的是为了全球的网民们能够懂得网络安全，提高警惕，防止不必要的个人损失。

社工师分类：

黑客渗透测试

间谍

特工

情报工作人员

诈骗人员

猎头

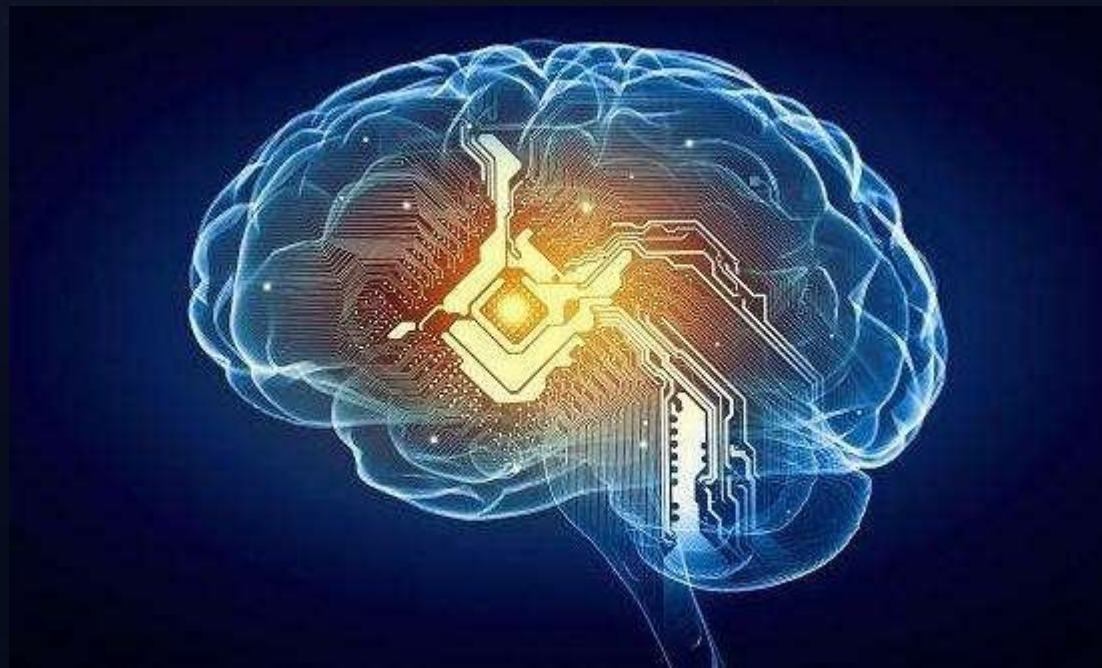
销售人员

平常人



社工概述

从广义上来说，社会工程学是一种通过对“人性”的心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段取得自身利益的手法，它并不能等同于一般的欺骗手法，社会工程学尤其复杂，即使自认为最警惕最小心的人，一样会被高明的社会工程学手段损害利益。



社工概述

被广泛运用于渗透入侵、公安破案、信息取证等领域

可获取所需的一切信息，任何人的思想活动

只需要很小的一个突破口，可攻破任何系统

掌握社工技术，就可以黑遍全世界



社工概述

现在的黑客攻击也不止是仅仅通过网络来进行远程的渗透与入侵，还会通过社会工程学在线下场景中针对人性弱点进行相应的攻击。这种手段非常有效，成功率也非常之高。

社工三大法宝：网络钓鱼、电话钓鱼、伪装模拟（包含很多）

狭义三大法宝：谷歌、社工库、QQ（等其他通讯工具）



333 pwned websites 5,687,892,700 pwned accounts 84,738 pastes 92,316,237 paste accounts

Largest breaches

	711,477,622	Onliner Spambot accounts
	593,427,119	Exploit.In accounts
	457,962,538	Anti Public Combo List accounts
	393,430,309	River City Media Spam List accounts
	359,420,698	MySpace accounts
	234,842,089	NetEase accounts
	164,611,595	LinkedIn accounts
	152,445,165	Adobe accounts
	131,577,763	Exactis accounts
	125,929,660	Apollo accounts

Recently added breaches

	575,437	Bombuj.eu accounts
	36,916	Hub4Tech accounts
	66,147,869	You've Been Scraped accounts
	66,308	AerServ accounts
	776,648	ForumCommunity accounts
	265,410	Technic accounts
	44,320,330	Data & Leads accounts
	9,363,740	Adapt accounts
	411,755	HTH Studios accounts
	5,788,169	Elasticsearch Instance of Sales Leads on AWS accounts

信息收集

与被攻击者相关的个人活动、社会活动、生活习惯、在线情况、网上可被搜索到的信息，简介、电话以及生日（可以分析密码，星座。让钓鱼更精准。）

如何收集信息：有许许多多的方式来获取一个人或一个组织的信息，而这些方法需要一定的技巧或者技能，社工师可以从不同的地方来收集：比如

一单位的信息，一张图片，一个Email，一个域名亦或者看门大爷
网站客服，百度，谷歌，**一切可以被利用的人或物。**

谷计划

VSRC成都沙龙站

信息收集

信息收集（情报收集）是社会工程的一个重要环节。信息收集同时也是一个最费时、最费事、最费力的阶段，但这往往是决定攻击周期内成败的关键要素。

1、姓名

2、性别

3、出生日期

4、身份证号

5、身份证家庭住址

6、身份证所在公安局

7、快递收货地址

8、大致活动范围

9、QQ

10、手机号

11、邮箱

12、银行卡号（银行开户行）

13、支付宝

14、贴吧、百度、微博、猎聘、58、同城、网盘、微信

15、常用ID

16、学历（小/初/高/大学/履历）

17、目标性格详细分析

18、常用密码

19、照片EXIF信息

谷划

VSRC 成都沙龙站

社工方法与思路

1、信息收集→信息整合→数据归类

2、幻象伪造→构造陷阱→获取信任

3、信息利用→漏洞辅助→攻击系统

基于社工进行的攻击需要对人性缺陷、想法、思维进行分析理解来展开攻击，而不再是直接利用计算机漏洞去不停测试从而展开攻击。

社工案例

- ✓ 一同学手机不慎丢失
- ✓ 监控只拍摄到小偷的侧脸
- ✓ 手机丢失后迅速被小偷拔卡关机

(以下案例纯属虚构)

●●●● 中国电信 89%

13:48

8月15日 星期一
丙申年七月十三

丢失的 iPhone

此 iPhone 已丢失。请给我打电话。谢谢!

139-0674-

轻点以呼叫

紧急情况

社工案例



- 1、收到钓鱼短信
- 2、短信发件人号码跟钓鱼网站域名
- 3、通过域名查询注册人、注册信息（whois信息）
- 4、通过域名追溯IP、收集站点信息
- 5、数据检索 查询相关站点资料
- 6、整理信息，进行下一步。

谷划

VSRC成都沙龙站

社工案例

社工案例

▶ 初步信息整理

 域名注册信息：

域名：Ap***d.cn

注册商：成都西部数码科技有限公司


注册人：刘**

创建时间：2017年01月10日

过期时间：2018年01月10日

邮箱：yu*****uzu@163.com

站点IP：43.**.**.12

 服务器Header信息：

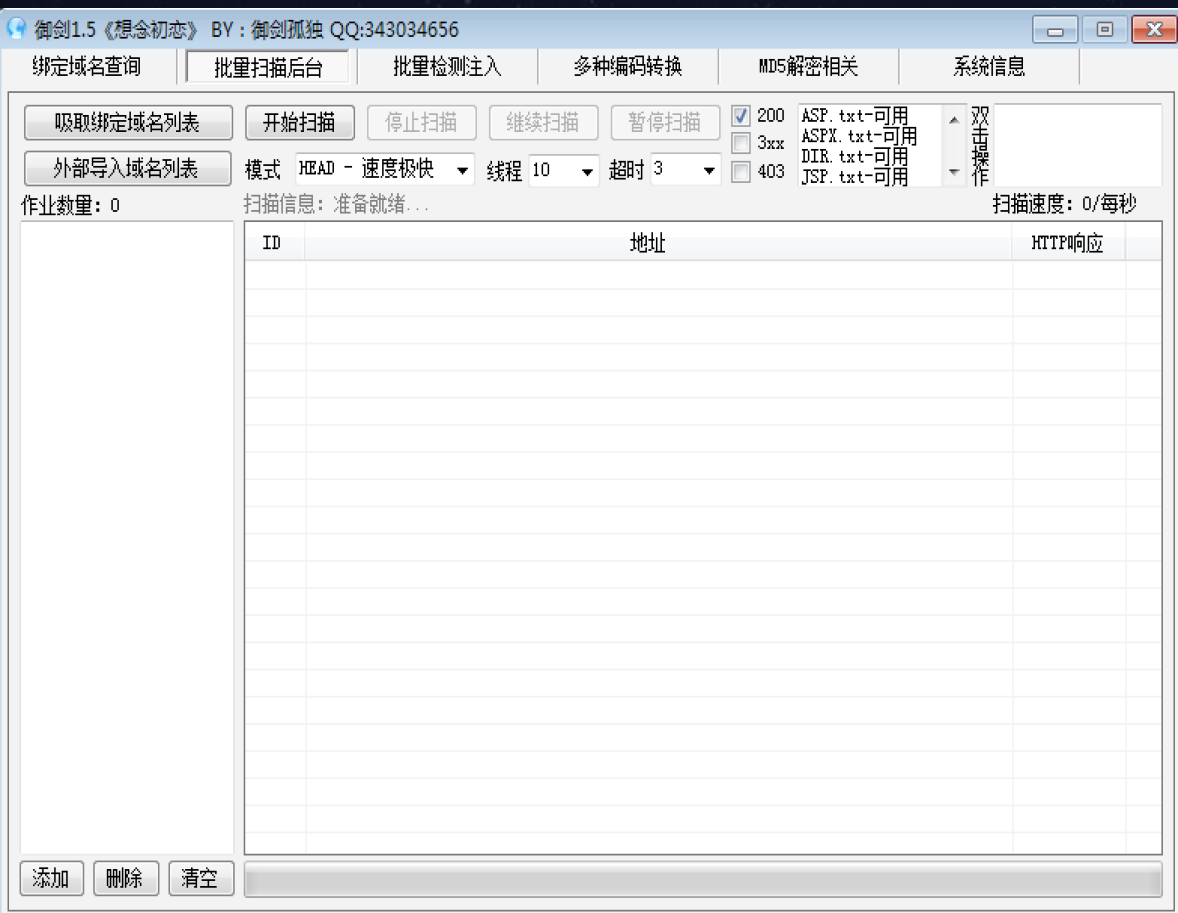
```
▼ Response Headers    view source
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection: keep-alive
Content-Encoding: gzip
Content-Length: 1505
Content-Type: text/html; charset=utf-8
Date: Wed, 12 Dec 2018 08:32:50 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
P3P: CP="IDC DSP COR ADM DEVI TAIi PSA PSD IVAi IVDi CONI CIAi CDi Pubi Ri DOI TSDi Pubi. (Un) NRSi OROi RUMi SUi. (Un) a. (Un) b. (Un) c. (Un) d. (Un) e. (Un) f. (Un) g. (Un) h. (Un) i. (Un) j. (Un) k. (Un) l. (Un) m. (Un) n. (Un) o. (Un) p. (Un) q. (Un) r. (Un) s. (Un) t. (Un) u. (Un) v. (Un) w. (Un) x. (Un) y. (Un) z. (Un) AA. (Un) AB. (Un) AC. (Un) AD. (Un) AE. (Un) AF. (Un) AG. (Un) AH. (Un) AI. (Un) AJ. (Un) AK. (Un) AL. (Un) AM. (Un) AN. (Un) AO. (Un) AP. (Un) AQ. (Un) AR. (Un) AS. (Un) AT. (Un) AU. (Un) AV. (Un) AW. (Un) AX. (Un) AY. (Un) AZ. (Un) BA. (Un) BB. (Un) BC. (Un) BD. (Un) BE. (Un) BF. (Un) BG. (Un) BH. (Un) BI. (Un) BJ. (Un) BK. (Un) BL. (Un) BM. (Un) BN. (Un) BO. (Un) BP. (Un) BQ. (Un) BR. (Un) BS. (Un) BT. (Un) BU. (Un) BV. (Un) BW. (Un) BX. (Un) BY. (Un) BZ. (Un) CA. (Un) CB. (Un) CC. (Un) CD. (Un) CE. (Un) CF. (Un) CG. (Un) CH. (Un) CI. (Un) CJ. (Un) CK. (Un) CL. (Un) CM. (Un) CN. (Un) CO. (Un) CP. (Un) CQ. (Un) CR. (Un) CS. (Un) CT. (Un) CU. (Un) CV. (Un) CW. (Un) CX. (Un) CY. (Un) CZ. (Un) DA. (Un) DB. (Un) DC. (Un) DD. (Un) DE. (Un) DF. (Un) DG. (Un) DH. (Un) DI. (Un) DJ. (Un) DK. (Un) DL. (Un) DM. (Un) DN. (Un) DO. (Un) DP. (Un) DQ. (Un) DR. (Un) DS. (Un) DT. (Un) DU. (Un) DV. (Un) DW. (Un) DX. (Un) DY. (Un) DZ. (Un) EA. (Un) EB. (Un) EC. (Un) ED. (Un) EE. (Un) EF. (Un) EG. (Un) EH. (Un) EI. (Un) EJ. (Un) EK. (Un) EL. (Un) EM. (Un) EN. (Un) EO. (Un) EP. (Un) EQ. (Un) ER. (Un) ES. (Un) ET. (Un) EU. (Un) EV. (Un) EW. (Un) EX. (Un) EY. (Un) EZ. (Un) FA. (Un) FB. (Un) FC. (Un) FD. (Un) FE. (Un) FF. (Un) FG. (Un) FH. (Un) FI. (Un) FJ. (Un) FK. (Un) FL. (Un) FM. (Un) FN. (Un) FO. (Un) FP. (Un) FQ. (Un) FR. (Un) FS. (Un) FT. (Un) FU. (Un) FV. (Un) FW. (Un) FX. (Un) FY. (Un) FZ. (Un) GA. (Un) GB. (Un) GC. (Un) GD. (Un) GE. (Un) GF. (Un) GG. (Un) GH. (Un) GI. (Un) GJ. (Un) GK. (Un) GL. (Un) GM. (Un) GN. (Un) GO. (Un) GP. (Un) GQ. (Un) GR. (Un) GS. (Un) GT. (Un) GU. (Un) GV. (Un) GW. (Un) GX. (Un) GY. (Un) GZ. (Un) HA. (Un) HB. (Un) HC. (Un) HD. (Un) HE. (Un) HF. (Un) HG. (Un) HH. (Un) HI. (Un) HJ. (Un) HK. (Un) HL. (Un) HM. (Un) HN. (Un) HO. (Un) HP. (Un) HQ. (Un) HR. (Un) HS. (Un) HT. (Un) HU. (Un) HV. (Un) HW. (Un) HX. (Un) HY. (Un) HZ. (Un) IA. (Un) IB. (Un) IC. (Un) ID. (Un) IE. (Un) IF. (Un) IG. (Un) IH. (Un) II. (Un) IJ. (Un) IK. (Un) IL. (Un) IM. (Un) IN. (Un) IO. (Un) IP. (Un) IQ. (Un) IR. (Un) IS. (Un) IT. (Un) IU. (Un) IV. (Un) IW. (Un) IX. (Un) IY. (Un) IZ. (Un) JA. (Un) JB. (Un) JC. (Un) JD. (Un) JE. (Un) JF. (Un) JG. (Un) JH. (Un) JI. (Un) JJ. (Un) JK. (Un) JL. (Un) JM. (Un) JN. (Un) JO. (Un) JP. (Un) JQ. (Un) JR. (Un) JS. (Un) JT. (Un) JU. (Un) JV. (Un) JW. (Un) JX. (Un) JY. (Un) JZ. (Un) KA. (Un) KB. (Un) KC. (Un) KD. (Un) KE. (Un) KF. (Un) KG. (Un) KH. (Un) KI. (Un) KJ. (Un) KK. (Un) KL. (Un) KM. (Un) KN. (Un) KO. (Un) KP. (Un) KQ. (Un) KR. (Un) KS. (Un) KT. (Un) KU. (Un) KV. (Un) KW. (Un) KX. (Un) KY. (Un) KZ. (Un) LA. (Un) LB. (Un) LC. (Un) LD. (Un) LE. (Un) LF. (Un) LG. (Un) LH. (Un) LI. (Un) LJ. (Un) LK. (Un) LL. (Un) LM. (Un) LN. (Un) LO. (Un) LP. (Un) LQ. (Un) LR. (Un) LS. (Un) LT. (Un) LU. (Un) LV. (Un) LW. (Un) LX. (Un) LY. (Un) LZ. (Un) MA. (Un) MB. (Un) MC. (Un) MD. (Un) ME. (Un) MF. (Un) MG. (Un) MH. (Un) MI. (Un) MJ. (Un) MK. (Un) ML. (Un) MN. (Un) MO. (Un) MP. (Un) MQ. (Un) MR. (Un) MS. (Un) MT. (Un) MU. (Un) MV. (Un) MW. (Un) MX. (Un) MY. (Un) MZ. (Un) NA. (Un) NB. (Un) NC. (Un) ND. (Un) NE. (Un) NF. (Un) NG. (Un) NH. (Un) NI. (Un) NJ. (Un) NK. (Un) NL. (Un) NM. (Un) NO. (Un) NP. (Un) NQ. (Un) NR. (Un) NS. (Un) NT. (Un) NU. (Un) NV. (Un) NW. (Un) NX. (Un) NY. (Un) NZ. (Un) OA. (Un) OB. (Un) OC. (Un) OD. (Un) OE. (Un) OF. (Un) OG. (Un) OH. (Un) OI. (Un) OJ. (Un) OK. (Un) OL. (Un) OM. (Un) ON. (Un) OP. (Un) OQ. (Un) OR. (Un) OS. (Un) OT. (Un) OU. (Un) OV. (Un) OW. (Un) OX. (Un) OY. (Un) OZ. (Un) PA. (Un) PB. (Un) PC. (Un) PD. (Un) PE. (Un) PF. (Un) PG. (Un) PH. (Un) PI. (Un) PJ. (Un) PK. (Un) PL. (Un) PM. (Un) PN. (Un) PO. (Un) PP. (Un) PQ. (Un) PR. (Un) PS. (Un) PT. (Un) PU. (Un) PV. (Un) PW. (Un) PX. (Un) PY. (Un) PZ. (Un) QA. (Un) QB. (Un) QC. (Un) QD. (Un) QE. (Un) QF. (Un) QG. (Un) QH. (Un) QI. (Un) QJ. (Un) QK. (Un) QL. (Un) QM. (Un) QN. (Un) QO. (Un) QP. (Un) QQ. (Un) QR. (Un) QS. (Un) QT. (Un) QU. (Un) QV. (Un) QW. (Un) QX. (Un) QY. (Un) QZ. (Un) RA. (Un) RB. (Un) RC. (Un) RD. (Un) RE. (Un) RF. (Un) RG. (Un) RH. (Un) RI. (Un) RJ. (Un) RK. (Un) RL. (Un) RM. (Un) RN. (Un) RO. (Un) RP. (Un) RQ. (Un) RR. (Un) RS. (Un) RT. (Un) RU. (Un) RV. (Un) RW. (Un) RX. (Un) RY. (Un) RZ. (Un) SA. (Un) SB. (Un) SC. (Un) SD. (Un) SE. (Un) SF. (Un) SG. (Un) SH. (Un) SI. (Un) SJ. (Un) SK. (Un) SL. (Un) SM. (Un) SN. (Un) SO. (Un) SP. (Un) SQ. (Un) SR. (Un) SS. (Un) ST. (Un) SU. (Un) SV. (Un) SW. (Un) SX. (Un) SY. (Un) SZ. (Un) TA. (Un) TB. (Un) TC. (Un) TD. (Un) TE. (Un) TF. (Un) TG. (Un) TH. (Un) TI. (Un) TJ. (Un) TK. (Un) TL. (Un) TM. (Un) TN. (Un) TO. (Un) TP. (Un) TQ. (Un) TR. (Un) TS. (Un) TT. (Un) TU. (Un) TV. (Un) TW. (Un) TX. (Un) TY. (Un) TZ. (Un) UA. (Un) UB. (Un) UC. (Un) UD. (Un) UE. (Un) UF. (Un) UG. (Un) UH. (Un) UI. (Un) UJ. (Un) UK. (Un) UL. (Un) UM. (Un) UN. (Un) UO. (Un) UP. (Un) UQ. (Un) UR. (Un) US. (Un) UT. (Un) UU. (Un) UV. (Un) UW. (Un) UX. (Un) UY. (Un) UZ. (Un) VA. (Un) VB. (Un) VC. (Un) VD. (Un) VE. (Un) VF. (Un) VG. (Un) VH. (Un) VI. (Un) VJ. (Un) VK. (Un) VL. (Un) VM. (Un) VN. (Un) VO. (Un) VP. (Un) VQ. (Un) VR. (Un) VS. (Un) VT. (Un) VU. (Un) VW. (Un) VX. (Un) VY. (Un) VZ. (Un) WA. (Un) WB. (Un) WC. (Un) WD. (Un) WE. (Un) WF. (Un) WG. (Un) WH. (Un) WI. (Un) WJ. (Un) WK. (Un) WL. (Un) WM. (Un) WN. (Un) WO. (Un) WP. (Un) WQ. (Un) WR. (Un) WS. (Un) WT. (Un) WU. (Un) WV. (Un) WW. (Un) WX. (Un) WY. (Un) WZ. (Un) XA. (Un) XB. (Un) XC. (Un) XD. (Un) XE. (Un) XF. (Un) XG. (Un) XH. (Un) XI. (Un) XJ. (Un) XK. (Un) XL. (Un) XM. (Un) XN. (Un) XO. (Un) XP. (Un) XQ. (Un) XR. (Un) XS. (Un) XT. (Un) XU. (Un) XV. (Un) XW. (Un) XX. (Un) XY. (Un) XZ. (Un) YA. (Un) YB. (Un) YC. (Un) YD. (Un) YE. (Un) YF. (Un) YG. (Un) YH. (Un) YI. (Un) YJ. (Un) YK. (Un) YL. (Un) YM. (Un) YN. (Un) YO. (Un) YP. (Un) YQ. (Un) YR. (Un) YS. (Un) YT. (Un) YU. (Un) YV. (Un) YW. (Un) YX. (Un) YY. (Un) YZ. (Un) ZA. (Un) ZB. (Un) ZC. (Un) ZD. (Un) ZE. (Un) ZF. (Un) ZG. (Un) ZH. (Un) ZI. (Un) ZJ. (Un) ZK. (Un) ZL. (Un) ZM. (Un) ZN. (Un) ZO. (Un) ZP. (Un) ZQ. (Un) ZR. (Un) ZS. (Un) ZT. (Un) ZU. (Un) ZV. (Un) ZW. (Un) ZX. (Un) ZY. (Un) ZZ. (Un)

Pragma: no-cache
Server: Microsoft-IIS/8.5
Set-Cookie: cisessionb4f3a0afc8d7e25e4583cb1f183d3fb5=mck9rnb9l45q0; path=/
Vary: Accept-Encoding
X-Cache: MISS from SSS_VIP_118
X-Powered-By: PHP/5.3.27
X-Powered-By: ASP.NET
```

社工案例

▶ 渗透站点—漏洞为辅

对站点开展渗透，祭出一些站点神器。



The Web of WebScan

本站已收录593,534,625条数据

输入你要查询的ip或域名

获取地址

查询旁站

查询C段

获取服务器信息

导出数据

社工案例

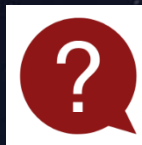
▶ 渗透站点—找到后台地址

/sysmanage/login/

欢迎使用

账号	<input type="text"/>
密码	<input type="password"/>

登录



后台情况：

后台系统：未知

开发语言：PHP

可能框架：CI

存在漏洞：不存在

登陆验证码：无

登陆次数限制：无

渗透

社工案例

套取相关信息

我 13:31:06
您能提供给我吗？我打个电话给他试试

我 13:31:22
拜托了！！

我 13:31:25
十分着急！！

高红梅 13:31:33
亲，您联系下QQ：2[REDACTED]1567

高红梅 13:31:39
电话：07[REDACTED]1116

信息情况：

QQ号码

电话号码

谷划

VSRC成都沙龙站

社工案例

获取后台密码

Crunch

```
hex-lower = [0123456789abcdef]
hex-upper = [0123456789ABCDEF]

numeric = [0123456789]
numeric-space = [0123456789 ]

symbols14 = [!@#%&*()-_+=]
symbols14-space = [!@#%&*()-_+= ]

symbols-all = [!@#%&*()-_+=~[]{}|\:;'"<>.,?/]
symbols-all-space = [!@#%&*()-_+=~[]{}|\:;'"<>.,?/ ]

alpha = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
alpha-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ ]
alpha-numeric = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
alpha-numeric-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
alpha-numeric-symbol14 = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#%&*()-_+=]
alpha-numeric-symbol14-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#%&*()-_+= ]
alpha-numeric-all = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#%&*()-_+=~[]{}|\:;'"<>.,?/]
alpha-numeric-all-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#%&*()-_+=~[]{}|\:;'"<>.,?/ ]

lalpha = [abcdefghijklmnopqrstuvwxyz]
```

Burp Suite Professional v1.5.01 - licensed to LarryLau

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

1 x 2 x 3 x 4 x ...

Target Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type:

POST /sysmanage/login/in HTTP/1.1
Host: a1 . m
Proxy-Connection: keep-alive
Content-Length: 41
Cache-Control: max-age=0
Origin: http://ap . 1
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac ; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://a /sysmanage/login/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cisessionb4f3a0 . 145q0

username=admin&pwd=\$admin%408888&sauthcode=

1 payload position Length: 706

获取后台账号 : admin 密码 : admin0557@

VSRC成都沙龙站

社工案例

幻象伪造、巧设陷阱

面临的问题：

- 登陆日志里，除了自己的IP并没有发现其他用户登陆的记录？
- 或者设置了定时清除？
- 怎么寻找小偷的登陆IP呢？

谷划

VSRC 成都沙龙站

社工案例

幻象伪造、巧设陷阱

- 1、了解钓鱼网站的接收信息规则
- 2、设想小偷接收到信息后的操作
- 3、利用规则，进行操作
- 4、登录后台，等待小偷删除
- 5、查看删除日志，获得小偷IP



IP地址: 60.

.112 浙江省台州市 电信

社工案例

▶ 进行IP定位



地址：浙江省台州市XX区XX路XXX号

谷划

VSRC 成都沙龙站

社工案例

价值信息挖掘

信息情况：

邮箱地址

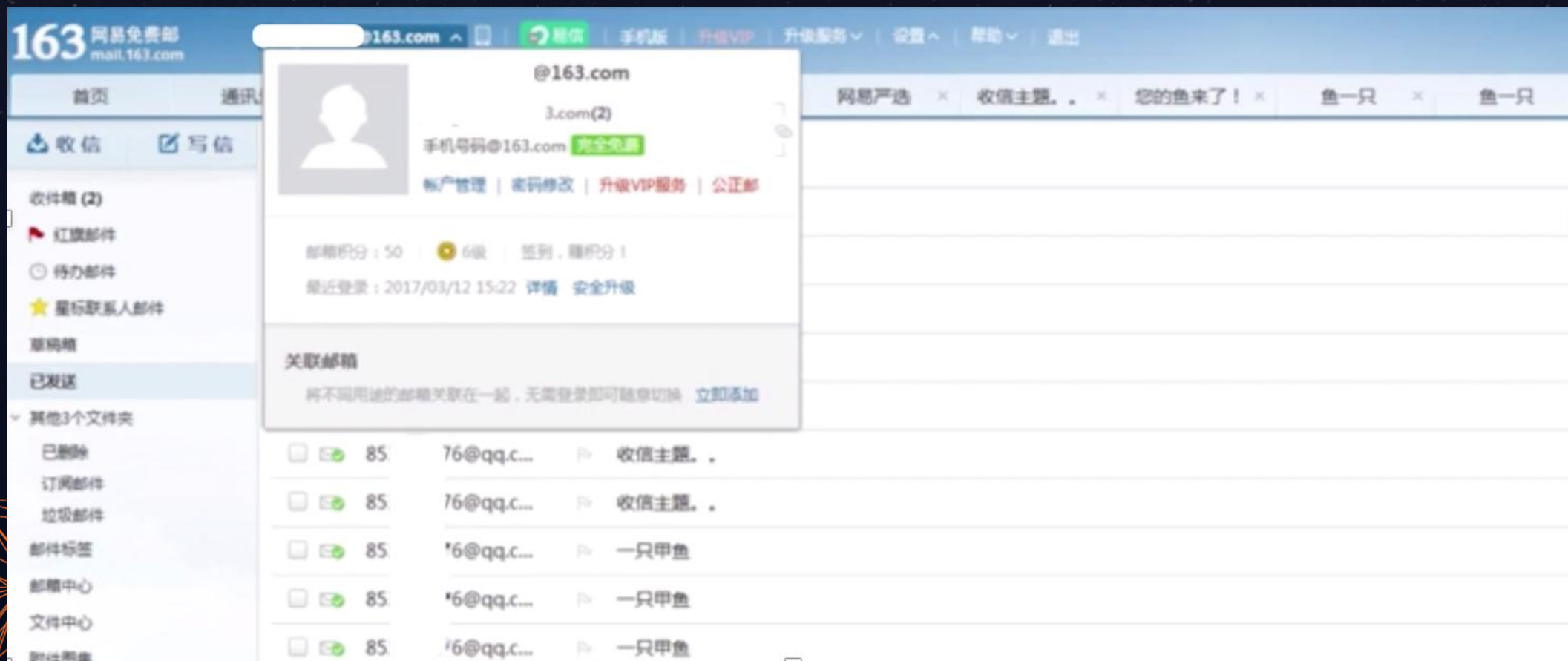
邮箱密码

QQ号码

SMTP地址:	smtp.163.com
发信邮箱地址:	_____@163.com
发信邮箱密码:	*****
收信邮件地址:	(_____@qq.com
发件人名称:	██████
收信主题:	鱼
收信主题选择:	系统默认主题 ▾
SMTP设置说明:	此功能为自行设置的邮件服务器发送通知，请进入您企业邮局开做SMTP服务后再进行设
短信通知API接口:	http://www._____.ckzz_email_api.asp
功能启动开关:	启动SMTP服务（邮件通知） ▾
网关状态:	[SMTP接口（邮件通知）使用中]
通知网关说明:	此功能支持QQ、手机短信、邮件接收提醒，QQ机器人通知使用费100元/月，专业版免

社工案例

价值信息挖掘



收获大量同伙信息，各种QQ邮箱！

社工案例

▶ 进一步社工

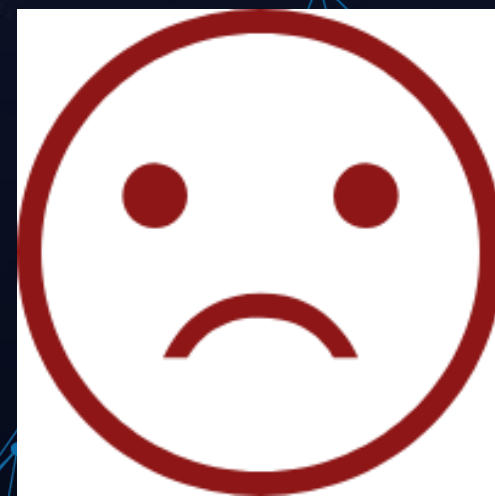
通过拿到的QQ号码等进行深入的勾兑

通过添加QQ好友，

目标非常警惕，

各种暗号接头

勾兑失败



社工案例

总结失败经验

- 1、缺乏信任
- 2、对目标掌握信息太少

谷划

VSRC 成都沙龙站

社工案例

最终成果

获取到了什么？

域名：ap*****cn

IP地址：60.***.***.112

后台账号：admin

密码：admin0557@

邮箱：j*****@163.com

邮箱密码：Abc1*****

地址：浙江省***市*****

QQ：*****76

手机号码：133*****

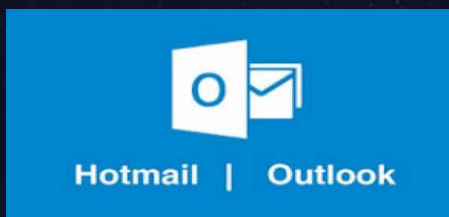
.....

谷
划

VSRC 成都沙龙站

邮件社工

思路与方法



邮件服务器

- 1、攻击邮件服务器（搞邮服）
- 2、获取邮箱账号密码（搞密码）
- 3、一键取证模式（AX模式）

谷划

VSRC成都沙龙站

邮件社工

▶ 邮件工作与流程

- 1、获取邮件服务器信息
- 2、确定工作方式
- 3、开展特定策略

nn: mekas4real@gmail.com	gmail、facebook、skype等
so: helton2@yahoo.com	fiverr、VPN账号、 cloudflare等
ref: ebaby4few@yahoo.com	有facebook、fiverr、
mr: jobs201@gmail.com	名和服务器等。
so: helton2@gmail.com	用于facebook、
so: helton2@mail.com	用于Fiverr、
+234 80	用于whatsapp等

石划

VSRC 成都沙龙站

邮件社工

Dig获取Mx记录

<https://toolbox.googleapps.com/apps/dig/>

```
tibet.net. IN MX
;ANSWER
tibet.net. 14399 IN MX 1 aspmx1.google.com.
tibet.net. 14399 IN MX 10 aspmx2.googlemail.com.
tibet.net. 14399 IN MX 10 aspmx3.googlemail.com.
tibet.net. 14399 IN MX 5 alt2.aspmx1.google.com.
tibet.net. 14399 IN MX 5 alt1.aspmx1.google.com.
;AUTHORITY
```

```
MacBook-Pro:~ netisvv$ dig @8.8.8.8 mx hku.hk
```

```
; <<>> DiG 9.10.6 <<>> @8.8.8.8 mx hku.hk
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43803
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;hku.hk.                                IN      MX

;; ANSWER SECTION:
hku.hk.                2527    IN      MX      10 hku-nsp2.hku.hk.
hku.hk.                2527    IN      MX      15 hku-nsp1.hku.hk.

;; Query time: 187 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Dec 13 10:24:36 CST 2018
;; MSG SIZE rcvd: 85
```

```
MacBook-Pro:~ netisvv$ nslookup
```

```
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=mx
> i-soon.net
Server:                8.8.8.8
Address:                8.8.8.8#53

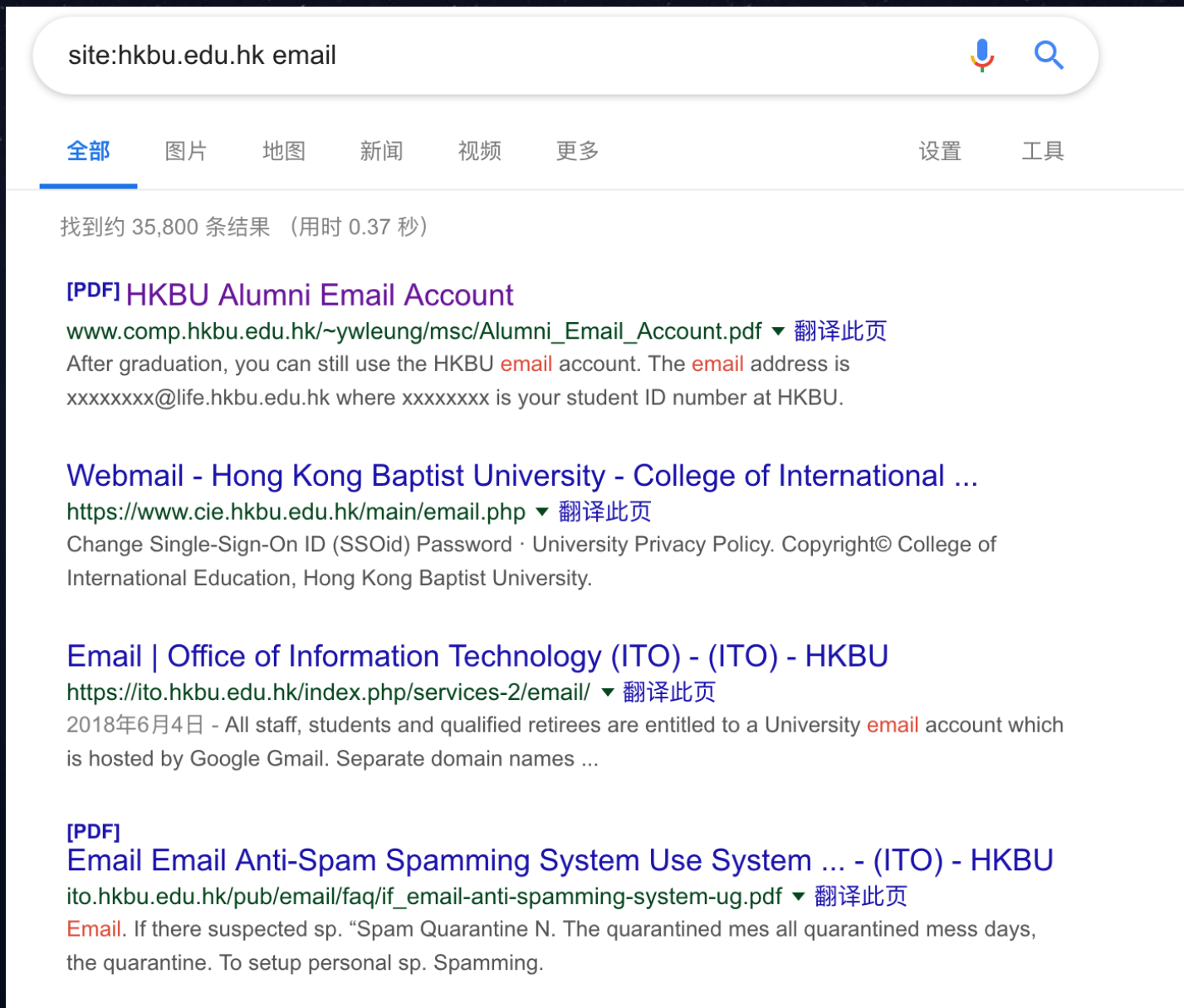
Non-authoritative answer:
i-soon.net             mail exchanger = 5 mxbiz1.qq.com.
i-soon.net             mail exchanger = 10 mxbiz2.qq.com.
```

邮件社工

▶ 邮件服务器攻击

- 1、获取邮件服务器信息
- 2、漏洞辅助
- 3、开展特定策略

Google Hack



site:hkbu.edu.hk email

全部 图片 地图 新闻 视频 更多 设置 工具

找到约 35,800 条结果 (用时 0.37 秒)

[\[PDF\] HKBU Alumni Email Account](#)
www.comp.hkbu.edu.hk/~ywleung/msc/Alumni_Email_Account.pdf ▼ 翻译此页
After graduation, you can still use the HKBU **email** account. The **email** address is xxxxxxxx@life.hkbu.edu.hk where xxxxxxxx is your student ID number at HKBU.

[Webmail - Hong Kong Baptist University - College of International ...](#)
<https://www.cie.hkbu.edu.hk/main/email.php> ▼ 翻译此页
Change Single-Sign-On ID (SSOid) Password · University Privacy Policy. Copyright© College of International Education, Hong Kong Baptist University.

[Email | Office of Information Technology \(ITO\) - \(ITO\) - HKBU](#)
<https://ito.hkbu.edu.hk/index.php/services-2/email/> ▼ 翻译此页
2018年6月4日 - All staff, students and qualified retirees are entitled to a University **email** account which is hosted by Google Gmail. Separate domain names ...

[\[PDF\] Email Email Anti-Spam Spamming System Use System ... - \(ITO\) - HKBU](#)
ito.hkbu.edu.hk/pub/email/faq/if_email-anti-spamming-system-ug.pdf ▼ 翻译此页
Email. If there suspected sp. "Spam Quarantine N. The quarantined mes all quarantined mess days, the quarantine. To setup personal sp. Spamming.

邮件社工

▶ 邮件服务器攻击

- 1、获取邮件服务器信息
- 2、漏洞辅助
- 3、开展特定策略

Google Hack

HKBU Alumni Email Account

After graduation, you can still use the HKBU email account. The email address is xxxxxxx@life.hkbu.edu.hk where xxxxxxxx is your student ID number at HKBU. This email account is provided by Google to HKBU and the contact point is the HKBU [Alumni Affairs Office](#). If you have any questions about this email account, please send your enquiry to the Alumni Affairs Office (email: alumni@hkbu.edu.hk).

Steps for Accessing HKBU Alumni Email Account

1. Go to the Alumni Affairs Office webpage:
<http://aao.hkbu.edu.hk>
2. Select webmail:

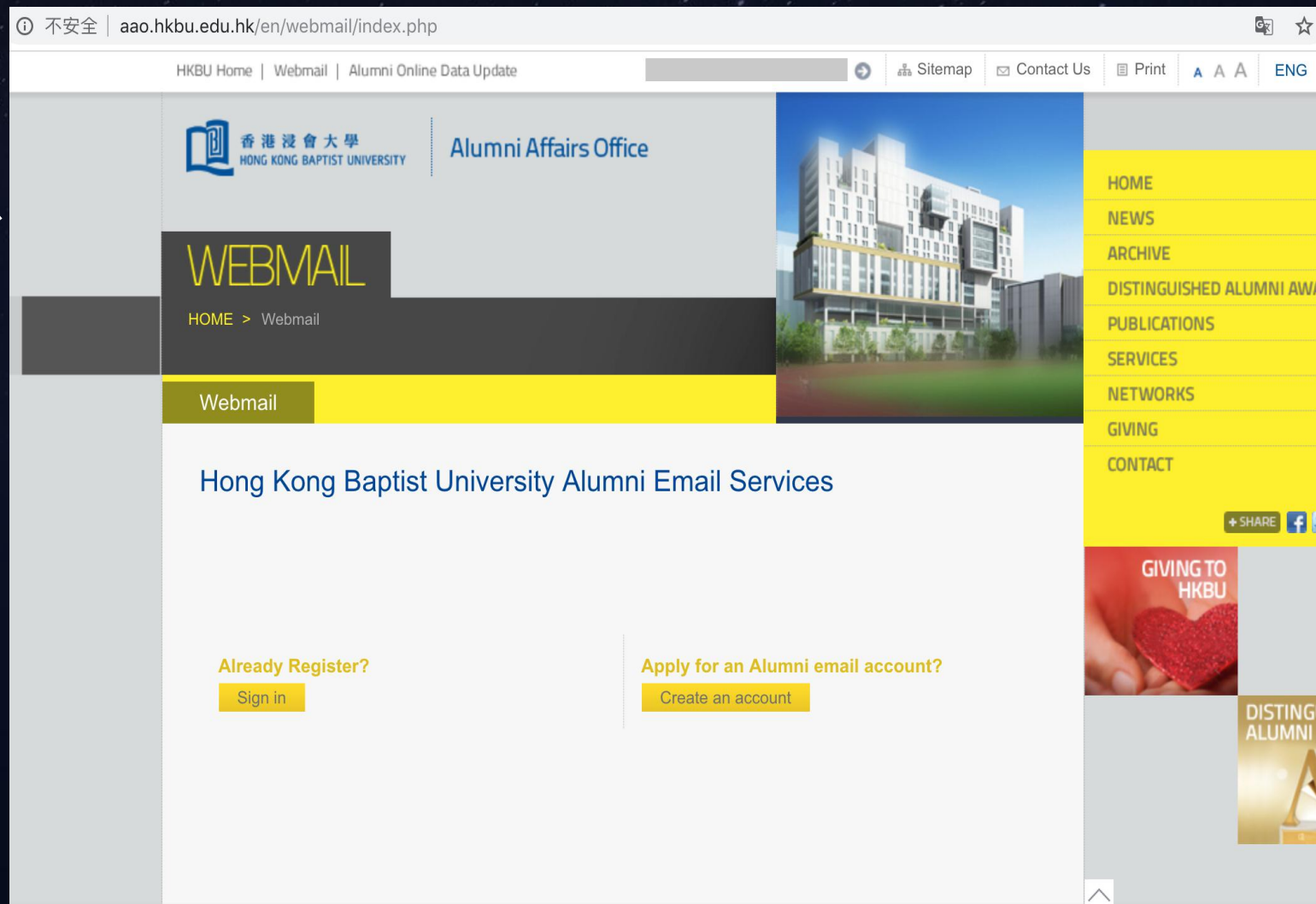


邮件社工

邮件服务器攻击

- 1、获取邮件服务器信息
- 2、漏洞辅助
- 3、开展特定策略

Google Hack



邮件社工

▶ 邮件服务器攻击

- 1、获取邮件服务器信息
- 2、漏洞辅助
- 3、开展特定策略

Google Hack



不安全 | aao.hkbu.edu.hk/en/webmail/index.php

HKBU Home | Webmail | Alumni Online Data Update

Sitemap Contact Us Print A A A ENG

Google

登录

继续使用 Gmail

输入您的电子邮件地址 @life.hkbu.edu.hk

[忘记了电子邮件地址?](#)

不是您自己的计算机? 请使用访客模式无痕登录。
[了解详情](#)

[创建帐号](#) [下一步](#)

HOME
NEWS
ARCHIVE
DISTINGUISHED ALUMNI AWARDS
PUBLICATIONS
SERVICES
NETWORKS
GIVING
CONTACT

+ SHARE f

GIVING TO HKBU

email account?

DISTINGUISHED ALUMNI

邮件社工



邮件服务器攻击

- 1、获取邮件服务器信息
- 2、漏洞辅助
- 3、开展特定策略

```
[MacBook-Pro:~ netisvv$ dig @8.8.8.8 mx life.hkbu.edu.hk

; <<>> DiG 9.10.6 <<>> @8.8.8.8 mx life.hkbu.edu.hk
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50809
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;life.hkbu.edu.hk.                IN      MX

;; ANSWER SECTION:
life.hkbu.edu.hk.                6215   IN      MX      5 ALT1.ASPMX.L.GOOGLE.COM.
life.hkbu.edu.hk.                6215   IN      MX      1 ASPMX.L.GOOGLE.COM.
life.hkbu.edu.hk.                6215   IN      MX      10 ASPMX2.GOOGLEMAIL.COM.
life.hkbu.edu.hk.                6215   IN      MX      10 ASPMX3.GOOGLEMAIL.COM.
life.hkbu.edu.hk.                6215   IN      MX      5 ALT2.ASPMX.L.GOOGLE.COM.
```



邮件社工



邮件服务器攻击

- 1、获取邮件服务器信息
- 2、漏洞辅助
- 3、开展特定策略

```
[MacBook-Pro:~ netisvv$ dig @8.8.8.8 mx hkbu.edu.hk

; <<>> DiG 9.10.6 <<>> @8.8.8.8 mx hkbu.edu.hk
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63080
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;hkbu.edu.hk.                IN      MX

;; ANSWER SECTION:
hkbu.edu.hk.                426     IN      MX      20 mailgwy57.hkbu.edu.hk.
hkbu.edu.hk.                426     IN      MX      10 mailgwy56.hkbu.edu.hk.

;; Query time: 54 msec
```



邮件社工



邮件服务器攻击

- 1、获取邮件服务器信息
- 2、漏洞辅助
- 3、开展特定策略

3. Enter your Account information, "Email Address", "Password" and "Description" as below. After completed, press "Next" on top of screen. Then enter server information.

Email : Your email address
Password : Your password

Exchange

Email buuser1@hkbu.edu.hk

Password

Description buuser1@hkbu.edu.hk

Next

Server : exmail.hkbu.edu.hk
Domain : hkbu.edu.hk
Username : Your username

Exchange

Email buuser1@hkbu.edu.hk

Server server.company.com

Domain Optional

Username Required

Password

Description buuser1@hkbu.edu.hk

Next

The system verifying your account information

Verifying

Email buuser1@hkbu.edu.hk

Server exmail.hkbu.edu.hk

Domain hkbu.edu.hk

Username buuser1

Password

Description buuser1@hkbu.edu.hk

邮件社工



邮件服务器攻击

1、获取邮件服务器信息

@hkbu.edu.hk
exchange邮箱

@life.hkbu.edu.hk
Gmail企业邮箱

The image shows two screenshots of email login interfaces. The left screenshot is for Microsoft Exchange, featuring a security warning section with radio buttons for '公用计算机或共享计算机' (selected) and '私人计算机', and a checkbox for '使用 Outlook Web App Light'. It includes input fields for '用户名:' and '密码:', a '登录' button, and a footer stating '已连接到 Microsoft Exchange © 2010 Microsoft Corporation. 保留所有权利。'. The right screenshot is for Gmail, showing the 'Google 登录' header, '继续使用 Gmail' text, an input field for the email address containing '@life.hkbu.edu.hk', a '忘记了电子邮件地址?' link, a note about guest mode, a '了解详情' link, a '创建帐号' link, and a '下一步' button.

邮件社工

▶ 邮件服务器攻击

2、漏洞辅助

2017-12-14	↓	✓	Microsoft Office - Dynamic Data Exchange 'DDE' Payload Delivery (Metasploit)
2016-11-09	↓	✓	Microsoft Windows - LSASS SMB NTLM Exchange Null-Pointer Dereference (MS16-137)
2014-09-29	↓	✗	Microsoft Exchange - IIS HTTP Internal IP Address Disclosure (Metasploit)
2010-07-20	↓	✓	Microsoft Outlook Web Access for Exchange Server 2003 - Cross-Site Request Forgery
2008-10-15	↓	✓	Microsoft Outlook Web Access for Exchange Server 2003 - 'redir.asp' Open Redirection
2006-06-13	↓	✓	Microsoft Exchange Server 2000/2003 - Outlook Web Access Script Injection
1998-03-10	↓	✓	Microsoft Exchange Server 4.0/5.0 - SMTP HELO Argument Buffer Overflow
2001-12-07	↓	✓	Microsoft Windows Server 2000 - Internet Key Exchange Denial of Service (2)
2001-12-11	↓	✓	Microsoft Windows Server 2000 - Internet Key Exchange Denial of Service (1)
2000-11-10	↓	✓	Computer Associates InoculateIT 4.53 - Microsoft Exchange Agent
2010-11-11	↓	✓	Microsoft Exchange Server 2000 - XEXCH50 Heap Overflow (MS03-046) (Metasploit)
2005-04-19	↓	✓	Microsoft Exchange Server - Remote Code Execution (MS05-021)
2003-10-22	↓	✓	Microsoft Exchange Server 2000 - XEXCH50 Heap Overflow (PoC) (MS03-046)



谷刻

VSRC 成都沙龙站

邮件社工

▶ 邮箱密码钓鱼

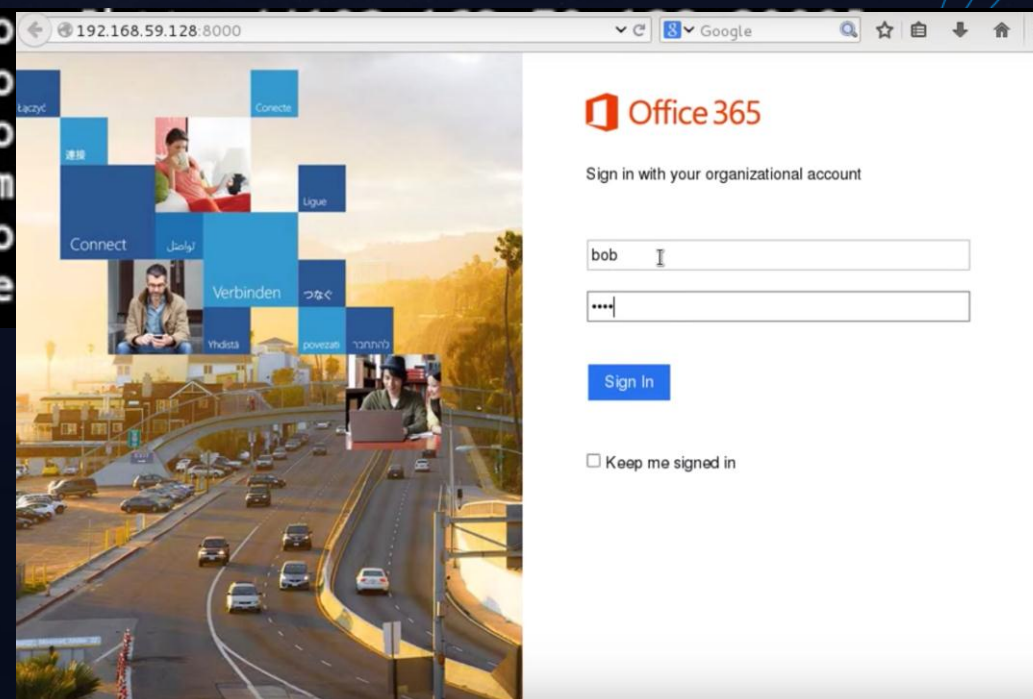
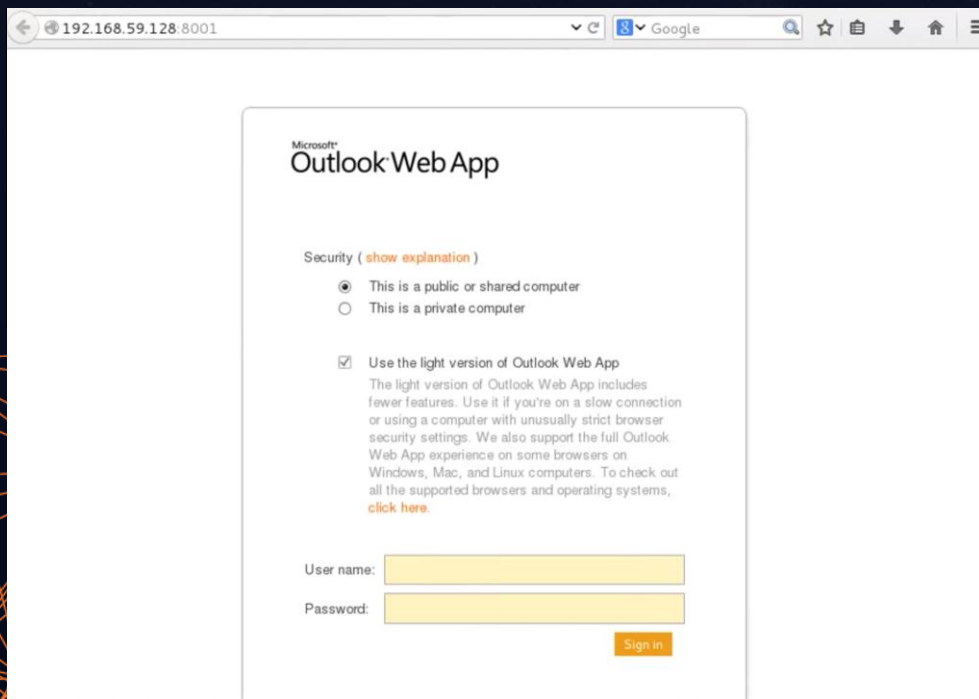
- 1、与目标勾兑，引起兴趣或者对问题重视
- 2、伪造获取邮箱密码的钓鱼网站，诱导输入邮箱密码

```
[VERBOSE] Started website [office365] on [http://192.168.59.128:8000]
[VERBOSE] Started website [owa      ] on [http://192.168.59.128:8001]
[VERBOSE] Started website [citrix   ] on [http://192.168.59.128:8002]
[VERBOSE] Created VHOST [office365.example.com] -> [http://192.168.59.128:8000]
[VERBOSE] Created VHOST [owa.example.com      ] -> [http://192.168.59.128:8001]
[VERBOSE] Created VHOST [citrix.example.com   ] -> [http://192.168.59.128:8002]
```

邮件社工

▶ 邮箱密码钓鱼

- 1、与目标勾兑，引起兴趣或者对问题重视
- 2、伪造获取邮箱密码的钓鱼网站，诱导输入邮箱密码



邮件社工

▶ 邮箱附件挂马

2、伪造发送各种附件挂马

docGen

操作区

Office版本: 11.0

URL:

Auth用户名:

Auth密码:

文档路径: ...

生成文档路径: ...

生成文档密码:

generate

说明区

- 1、该工具需要系统安装office 2007软件。
- 2、URL为木马存放的地址。
- 3、Auth用户名和Auth密码为下载木马需要的身份校验。
- 4、文档路径为源文档路径。
- 5、生成文档路径为生成文档存放路径,生成文档的名称为: "源文件名_gen.doc"。

更多说明

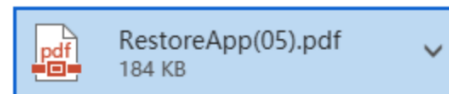
Re: [Reminder] Your **iCloud** Has Been Disabeld On April 04 2018



Apple Support <noreply-mail-senmding-service76706@restore-id-

周四 2018/4/5 1:38

收件人: secure@appleid.com ↗



下载 保存到 OneDrive - 个人

Dear Customer,

We inform the users apple id that your account has violated policy for your account is temporarily disabled. If you need your Apple account, please open the attachment (PDF) and following the steps in order to be immediately reviewed by Apple. Sincerely,

Apple Support

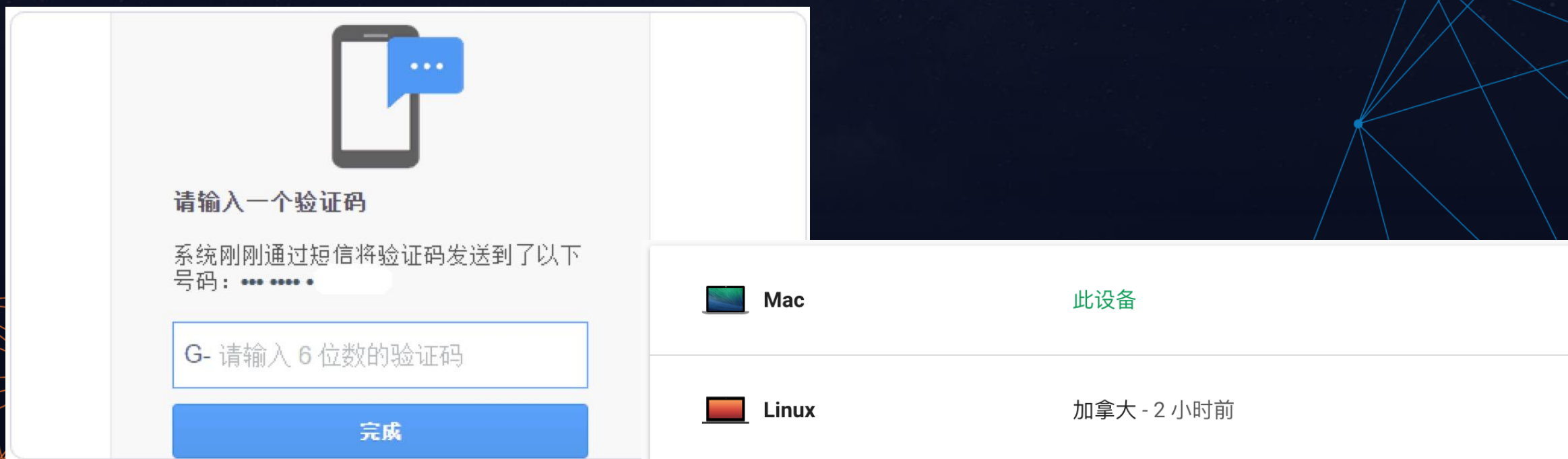
这封钓鱼邮件的神奇之处在于收件人居然是secure@appleid.com, 所以并不知道它是用什么方法送到outlook邮箱的。

这封邮件的大致内容是由于appleid涉嫌违反政策被禁用, 如果要启用就打开附件。

邮件社工

▶ 存在的问题跟弊端

1、对于Gmail，即使获取到密码，也绕不过二次验证！





请输入一个验证码

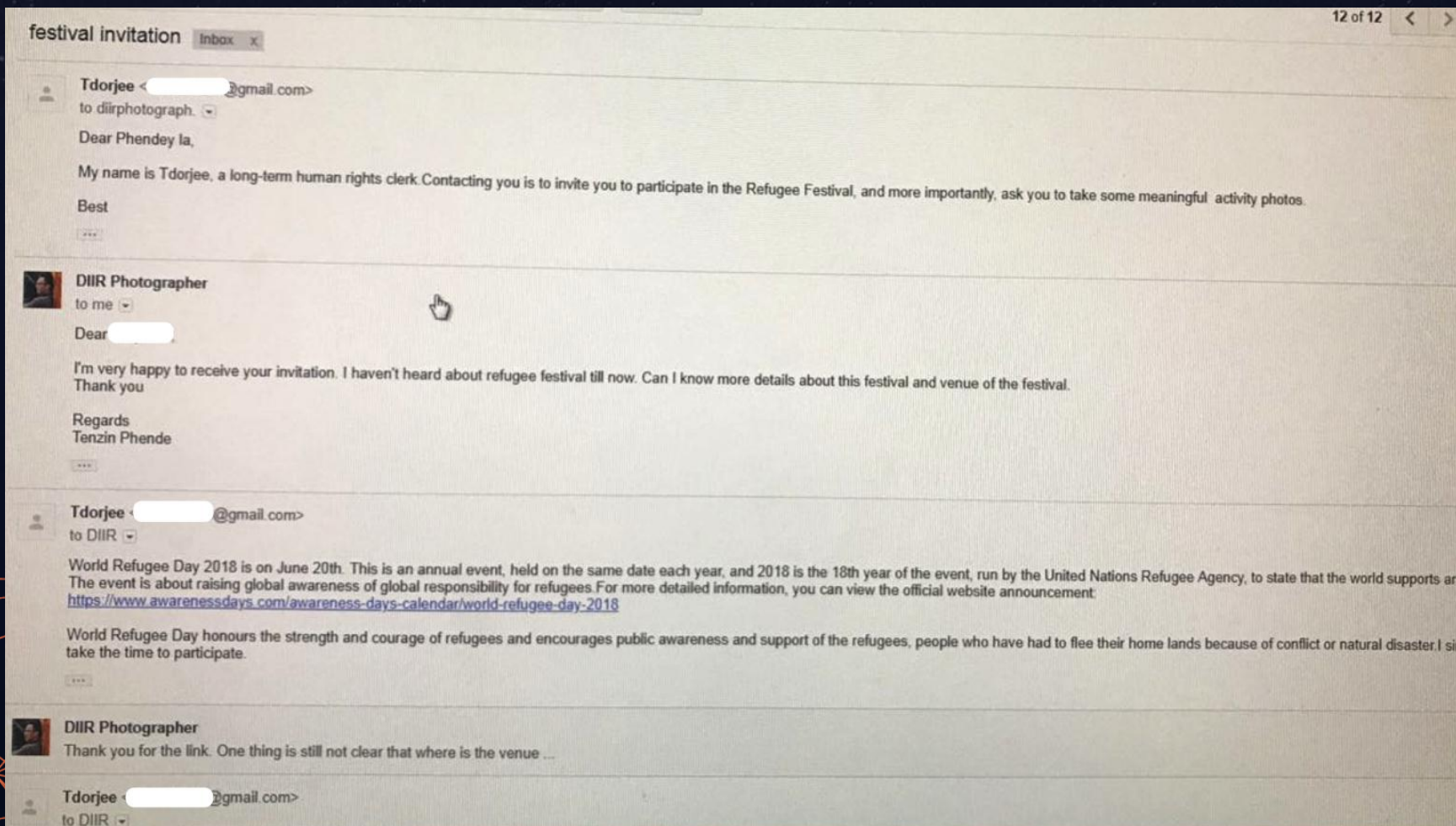
系统刚刚通过短信将验证码发送到了以下号码：●●●●●●

G- 请输入 6 位数的验证码

完成

 Mac	此设备
 Linux	加拿大 - 2 小时前

邮件社工



谷划

VSRC 成都沙龙站

邮件社工



10.19 11:30 发送给 che... il.com/suoluo... ail.com/partis ail.com

主题: 獨立評論記者 簡單採訪
内容:
陳泱潮先生您好,我是獨立評論的記者羅舟,因在博訊上看了您的文章,而後又看了您寫的特權論,對您提出的集權導致特權資本化的觀點非常贊同,您在幾十年前就完成了這部著作,更是對您表示深深的敬佩,最近要寫一篇關於中美貿易戰的文章,想就中美貿易戰和您進行簡短的交流,討論下您對中美貿易戰的看法,不知道您是否有時間,期待您的回復。
祝您身體健康,一切順利

10.22 06:18 收到 suolu... ail.com 回复

主题: 請約定時間和交流話題 / 獨立評論記者 簡單採訪
内容:
羅舟先生: 你好!
很高興收到你的來信。歡迎和你交流。請約定時間和交流話題。
我看到你給我發的郵件還同時發給我 2006 年前的郵箱 chenyang... .il.com, 這個郵箱已經被黑客破壞了或者是被盜用了, 所以你今後給我發郵件不要再發個這個郵箱, 以免郵件落入歹人之手。

谷
划

邮件社工

社工策略

第一步、了解目标

第二步、与目标沟通

第三步、投放“取证链接”

第四步、等待取证成功

第五步、获取邮件

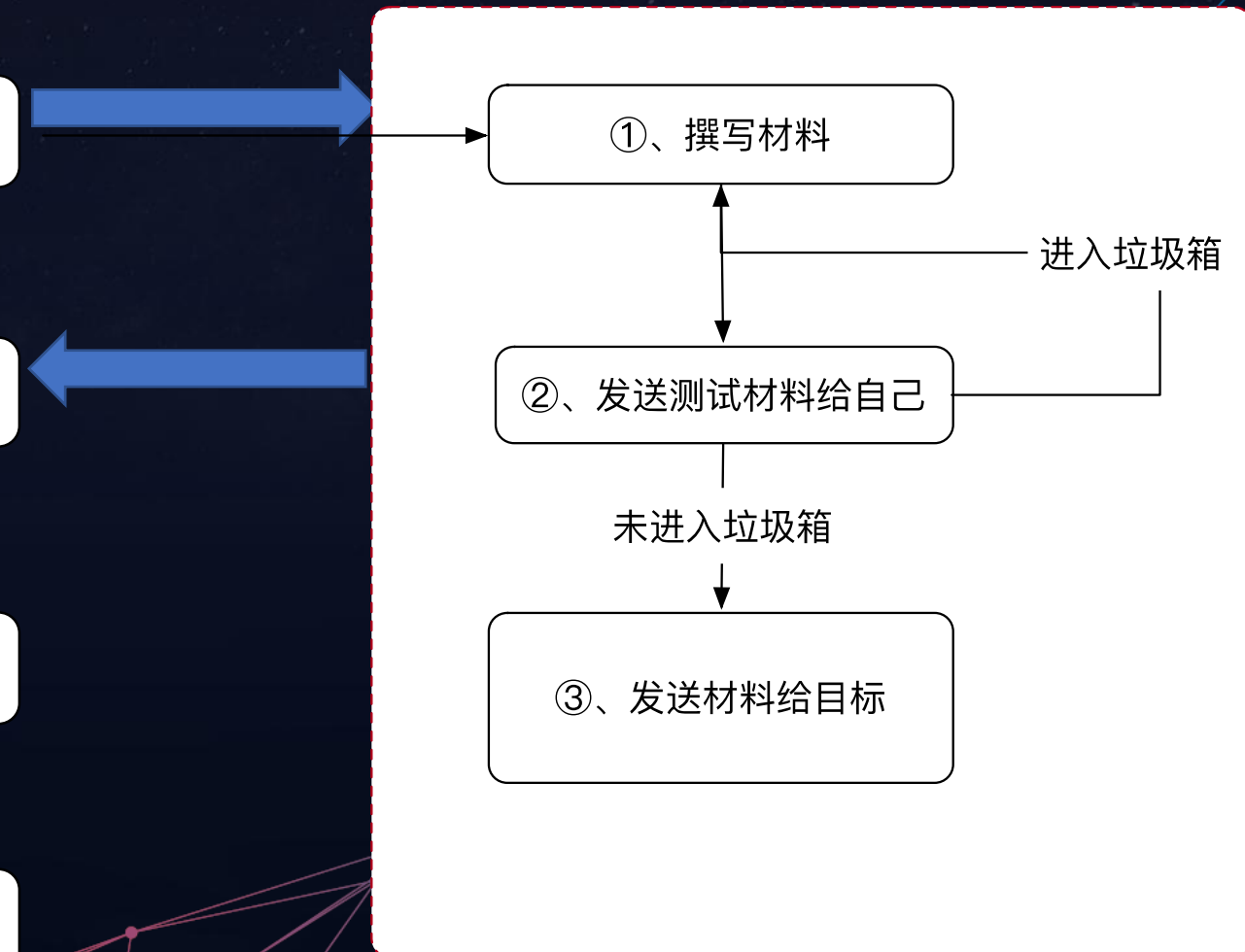
①、撰写材料

②、发送测试材料给自己

③、发送材料给目标

进入垃圾箱

未进入垃圾箱



邮件社工

▶ 社工策略



媒体采访



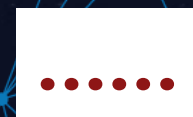
论文发表



会议咨询



资讯文章



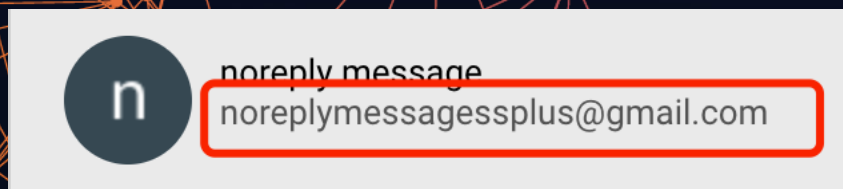
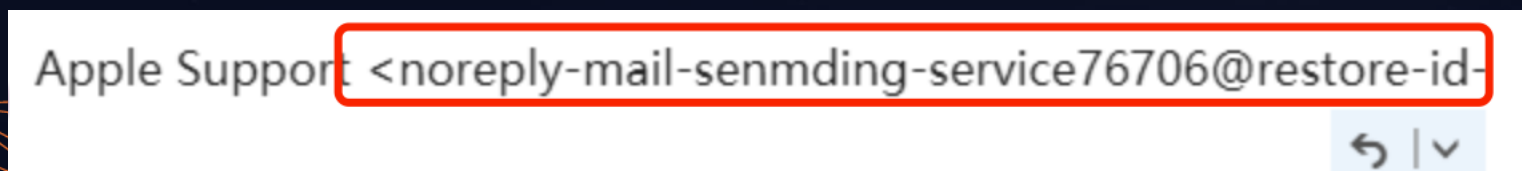
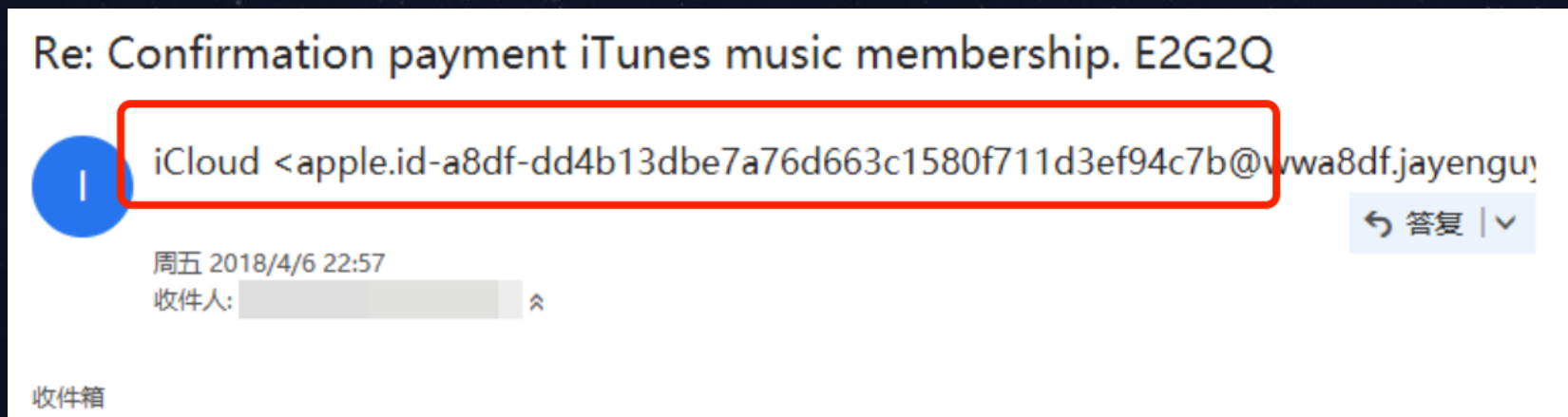
熟人、媒体、学生、学者、同行、难民.....

谷计划

VSRC 成都沙龙站

邮件社工

▶ 发件邮箱的重要性



谷
划

VSRC 成都沙龙站

邮件社工



利用人的 **信任、恐惧、贪婪、激动...**

以达到我们要的目的.

谷
划

VSRC 成都沙龙站

人·才是最大的漏洞

--- 《我是谁：没有绝对安全的系统》



谷划

VSRC 成都沙龙站

THANK YOU!



电话：400-066-5915

官网：www.i-soon.net

地址：上海市闵行区万源路2158号泓毅大厦A座1007室
成都市高新西区百草路366号萃峰国际B栋



谷计划

VSRC 成都沙龙站