邮 件 攻 击 密 取 与 社 工

安洵信息技术有限公司

谷神计划

VSRC成都沙龙站

目　录

C O N T E N T S

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。

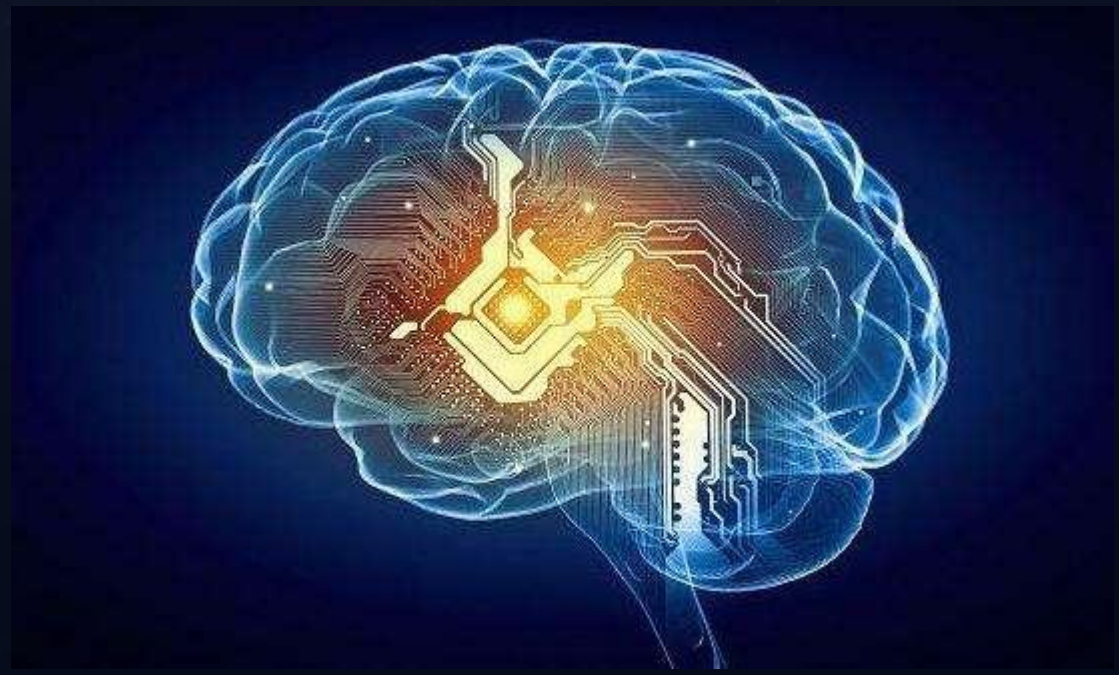
社会工程学是黑客米特尼克在《欺骗的艺术》中率先提出的，其初始目的是为了让全球的网民们能够懂得网络安全，提高警惕，防止不必要的个人损失。

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来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	5,687,892,700	84,738	92,316,237
pwned websites	pwned accounts	pastes	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**。

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

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

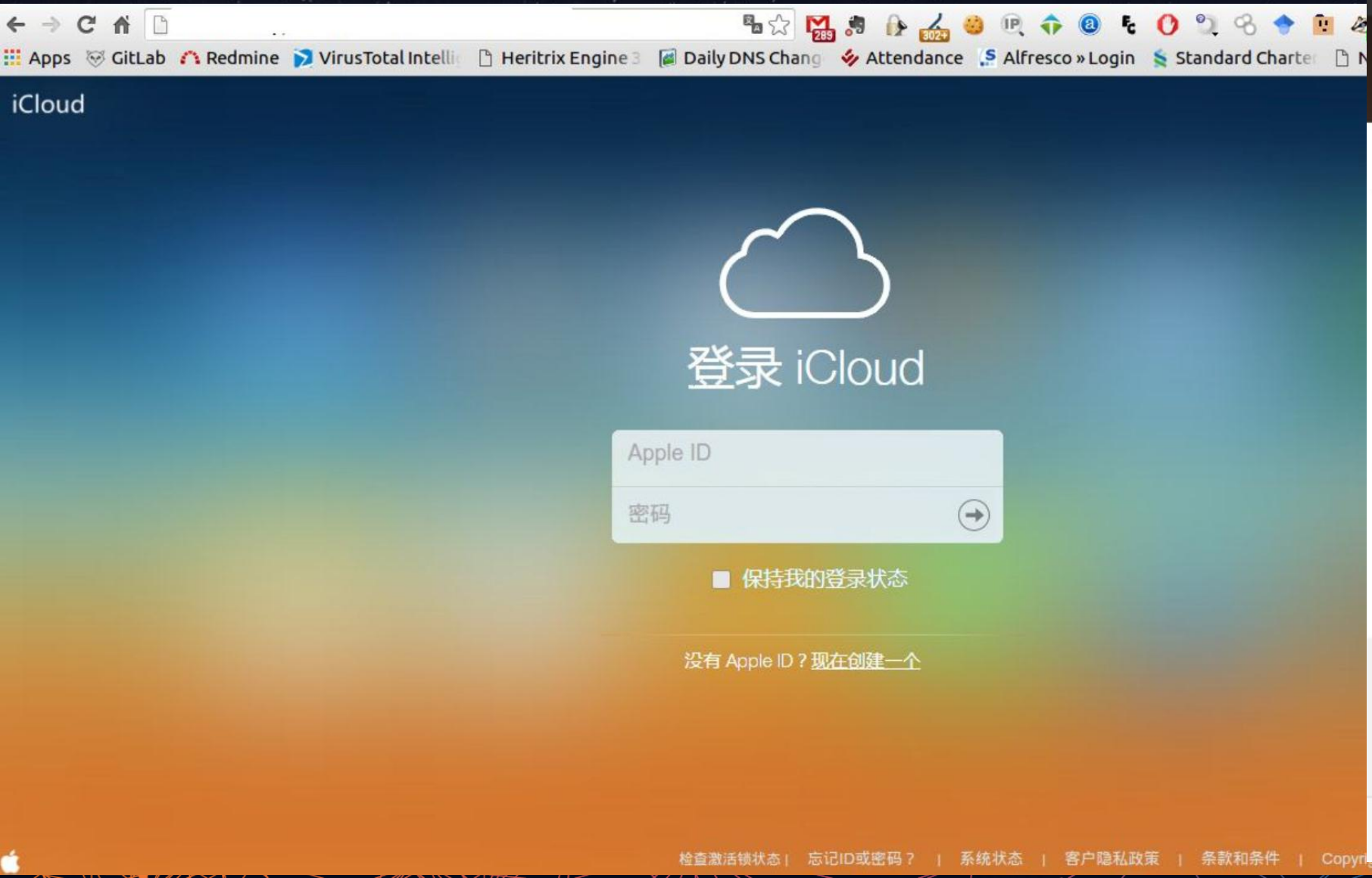
- ✓ 一同学手机不慎丢失
- ✓ 监控只拍摄到小偷的侧脸
- ✓ 手机丢失后迅速被小偷拔卡关机

（以下案例纯属虚构）

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。

社工案例


Apps
GitLab
Redmine
VirusTotal Intelli
Heritrix Engine 3
Daily DNS Chang
Attendance
Alfresco » Login
Standard Charte
iCloud
登录 iCloud
Apple ID
密码
保持我的登录状态
没有 Apple ID？现在创建一个
检查激活锁状态
忘记ID或密码？
系统状态
客户隐私政策
条款和条件


中国联通
16:15
45%
Apple ID
验证您的出生日期或设备屏幕锁以继续
00000000
设备屏幕锁
取消
继续
更多选购方式：前往 Apple Store 零售店，致电 400-666-8800 或查找在你附近的授权经销商。
中国

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

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 CNT"

Pragma: no-cache

Server: Microsoft-IIS/8.5

Set-Cookie: cisessionb4f3a0afc8d7e25e4583cb1f183d3fb5=mck9rnb9l45q0; path=/

Vary: Accept-Encoding

X-Cache: MISS from SSS_VIP_118

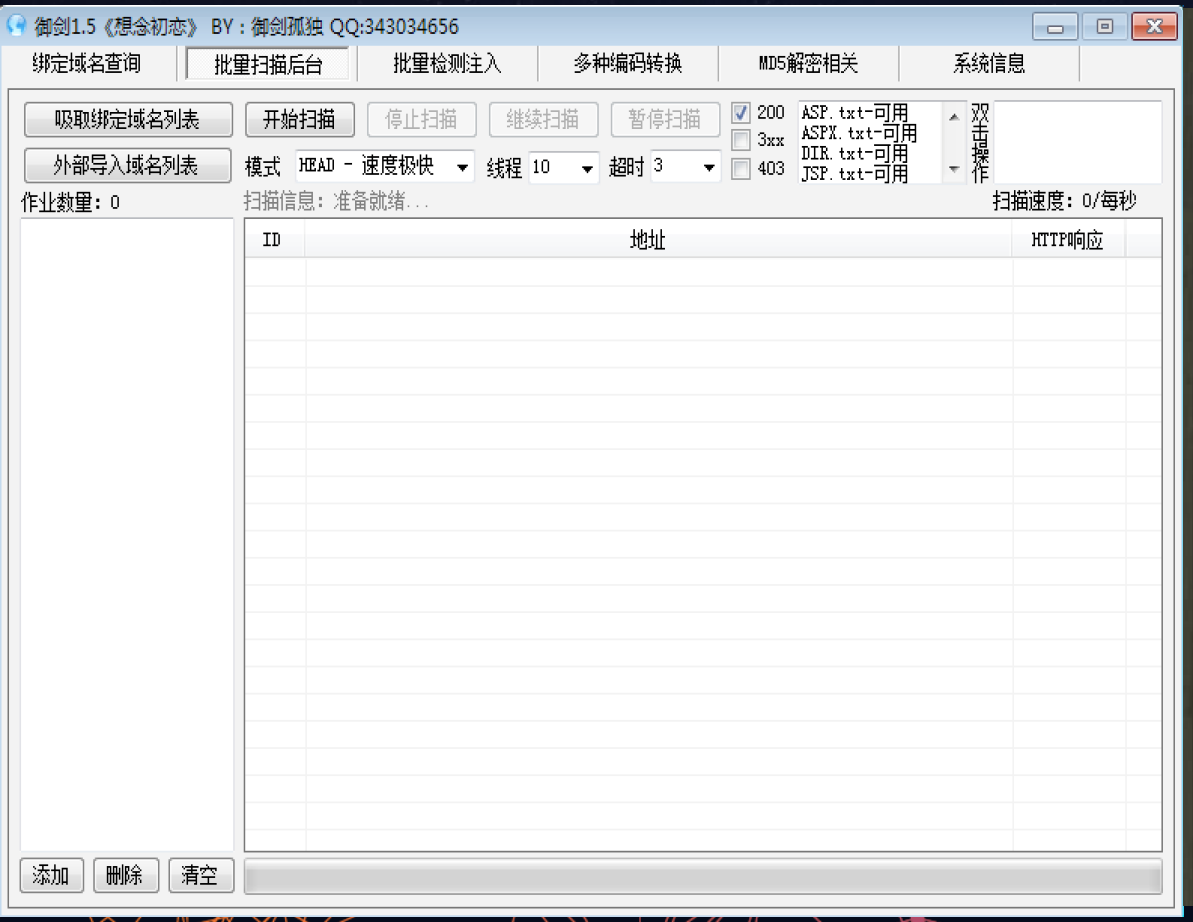
X-Powered-By: PHP/5.3.27

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。



社工案例

渗透站点—找到后台地址

/sysmanage/login/

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

社工案例

套取相关信息

信息情况：

QQ号码

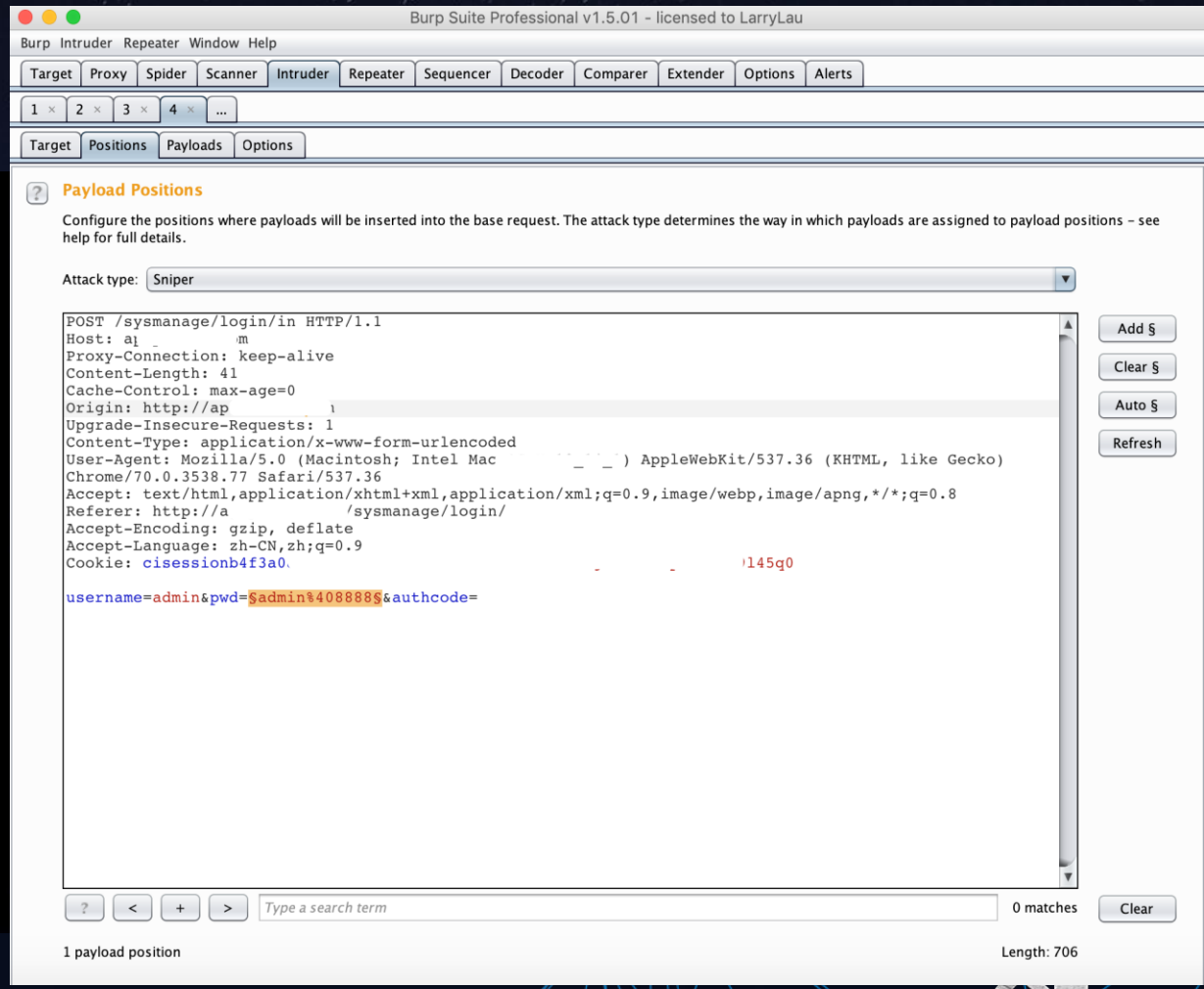
电话号码

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

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

lalpha                   = [abcdefghijklmnopqrstuvwxyz]
```



获取后台账号：admin 密码：admin0557@

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？

社工案例

幻象伪造、巧设陷阱

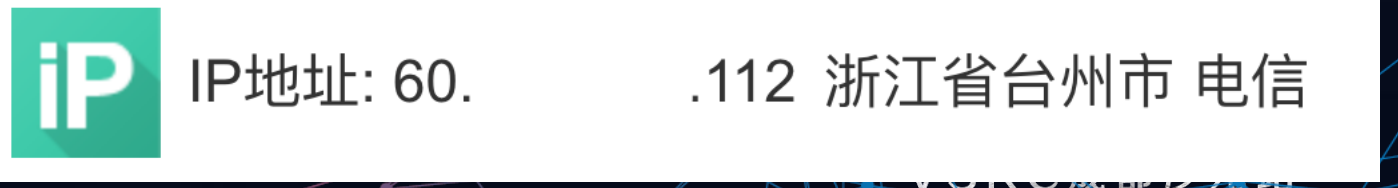
1、了解钓鱼网站的接收信息规则

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



社工案例

进行IP定位

地址：浙江省台州市XX区XX路XXX号

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

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

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*****

.....

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）

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 cobs201@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

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 aspmx.l.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.aspmx.l.google.com.
tibet.net. 14399 IN MX 5 alt1.aspmx.l.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 xxxxxxxx@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

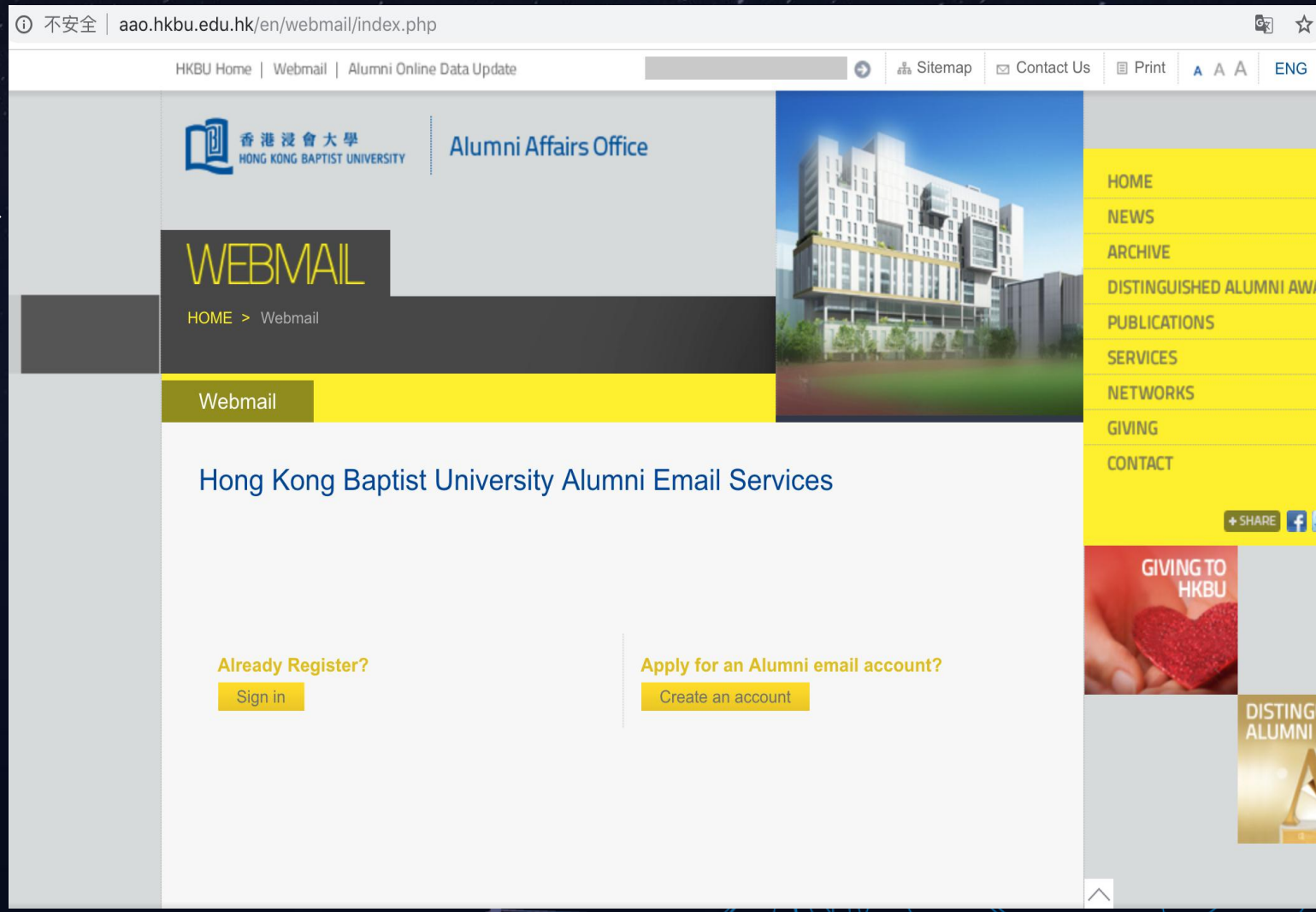
邮件服务器攻击

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

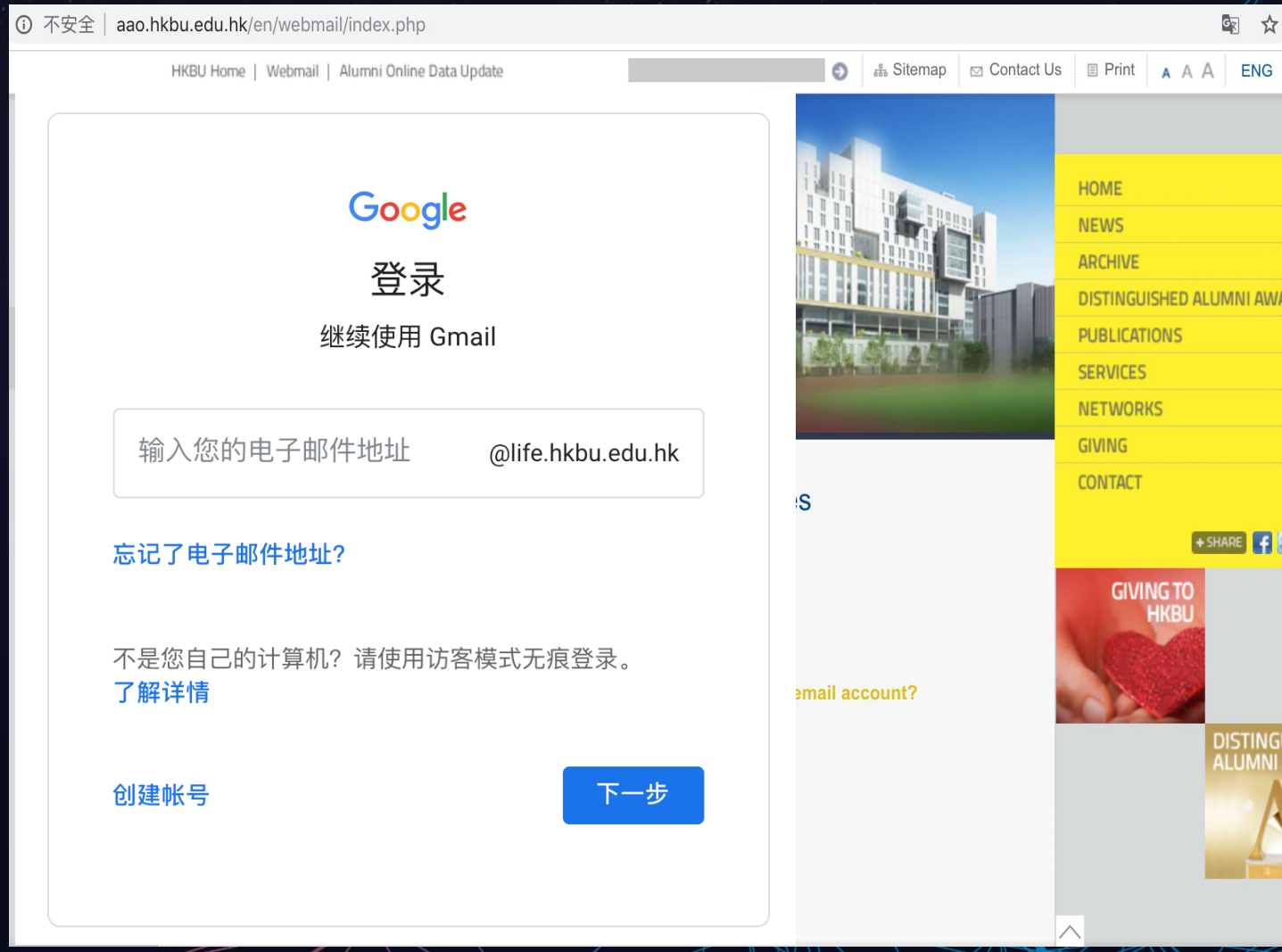
邮件服务器攻击

1、获取邮件服务器信息

2、漏洞辅助

3、开展特定策略

Google Hack



邮件社工

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.
```

邮件社工

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**

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

The system verifying your account information

邮件社工

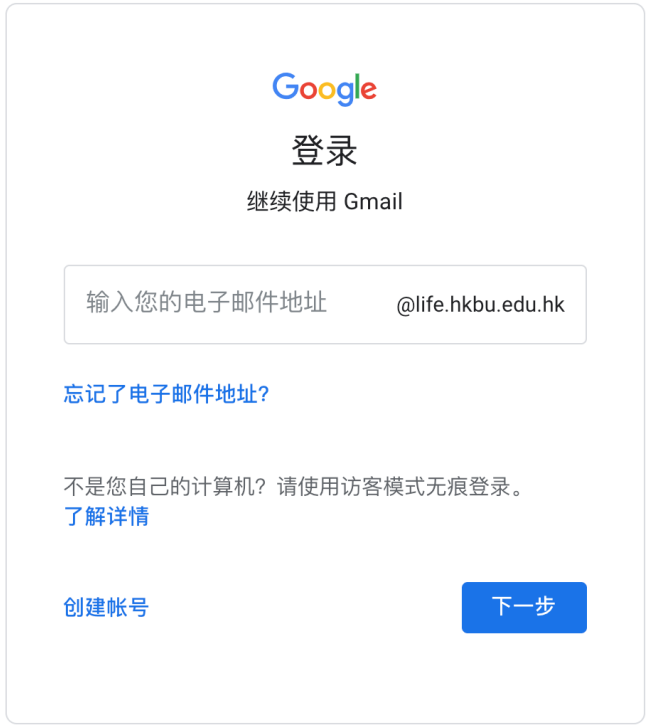
邮件社工

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



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)

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

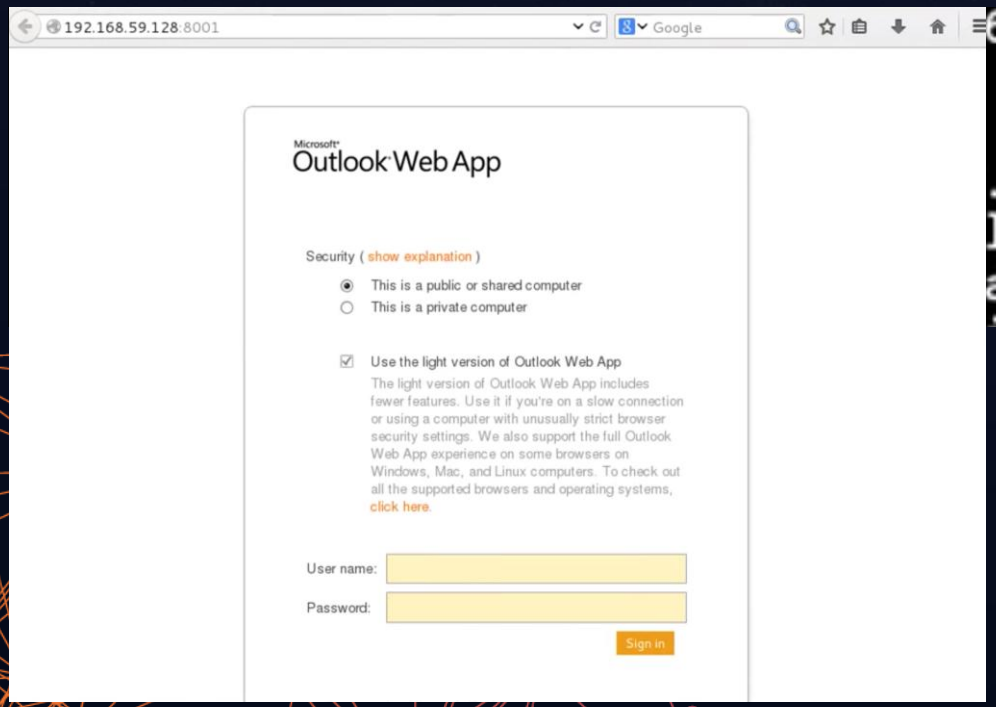
```
[VERBOSE] Started website [office365] on [http://192.168.59.128:8000]
[VERBOSE] Started website [owa      ] on [http://192.168.59.128:8001]
[VERBOSE] Started website [citrix   ] on [http://192.168.59.128:8002]
[VERBOSE] Created VHOST [office365.example.com] -> [http://192.168.59.128:8000]
[VERBOSE]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

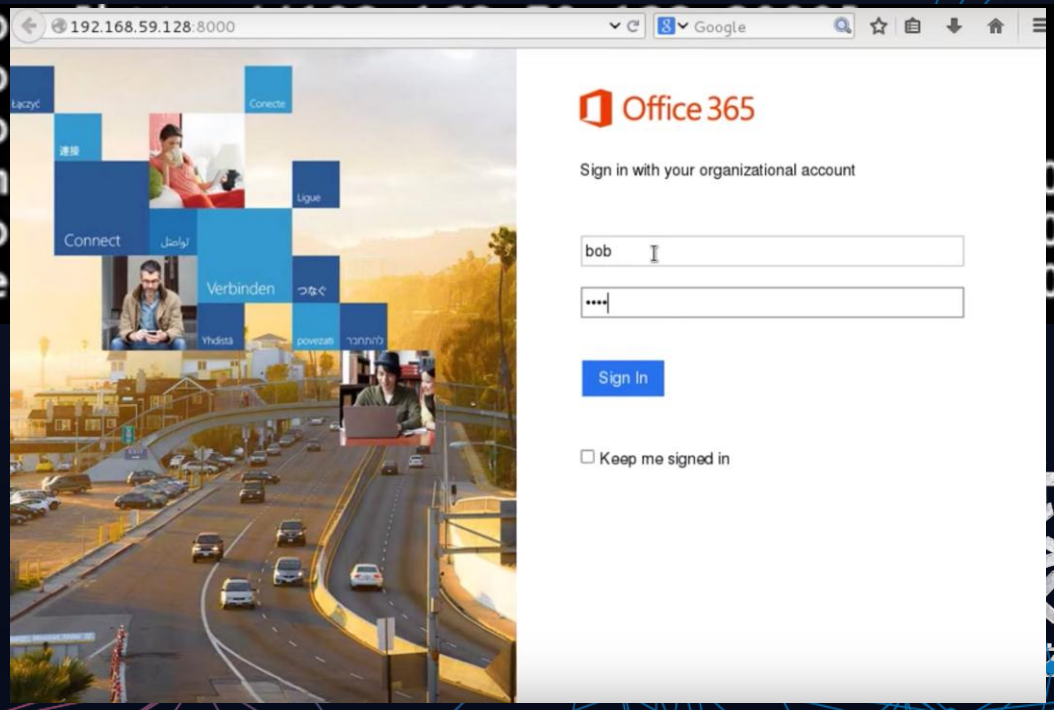
邮件社工

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

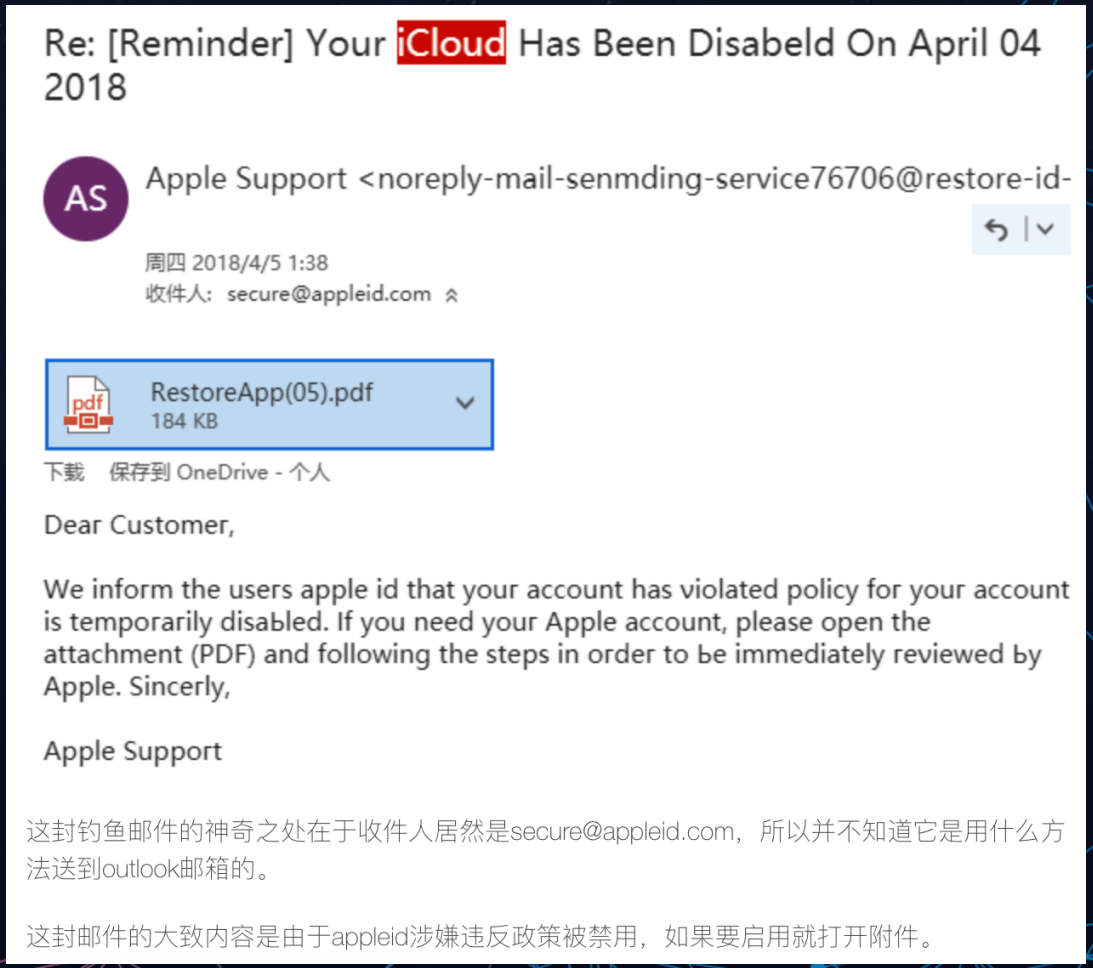




邮件社工

邮箱附件挂马

2、伪造发送各种附件挂马



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。

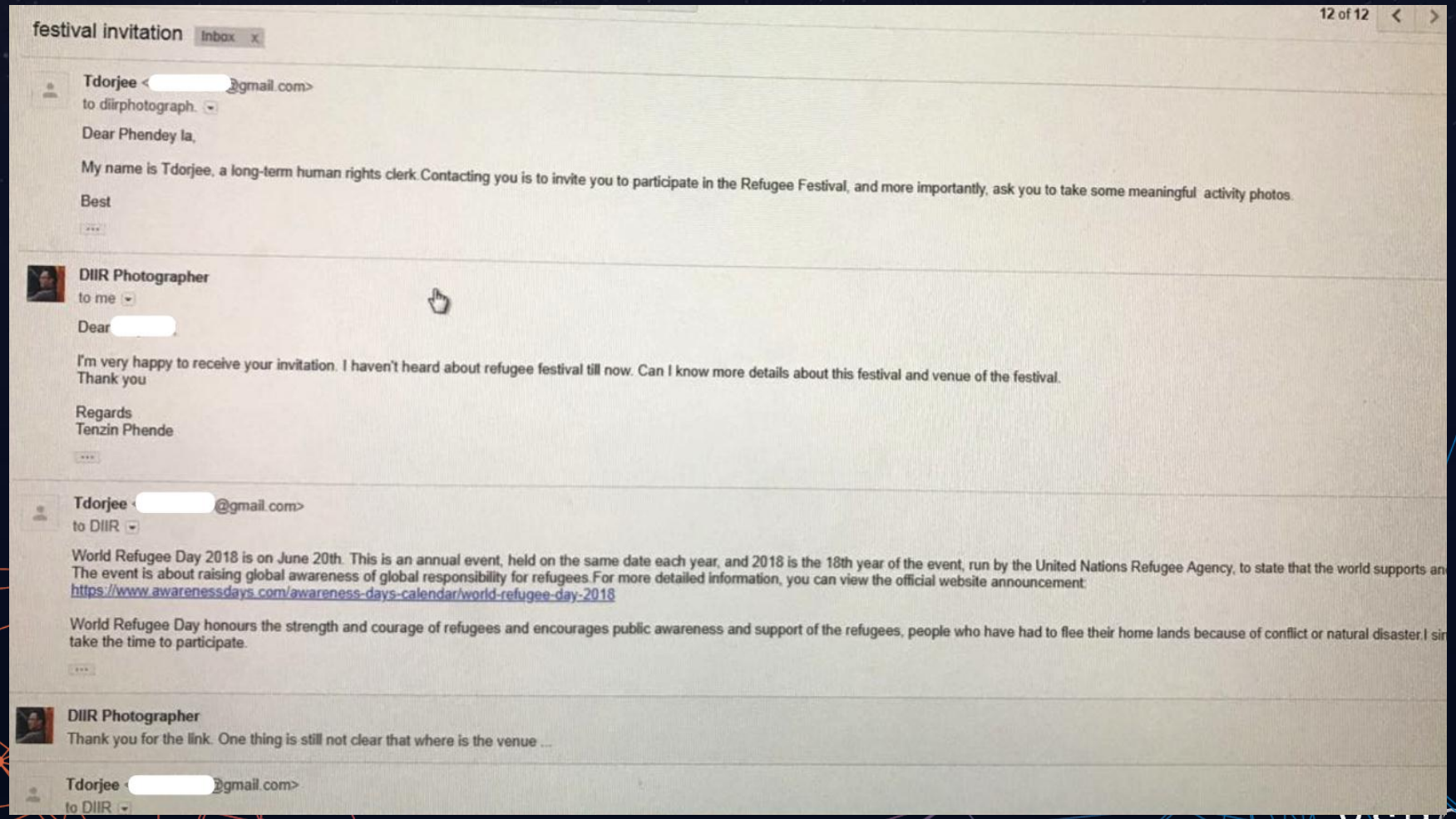
邮件社工

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！

邮件社工

AX模式



festival invitation Inbox x

12 of 12

Tdorjee <[redacted]@gmail.com>
to diirphotograph.

Dear Phendey la,

My name is Tdorjee, a long-term human rights clerk.Contacting you is to invite you to participate in the Refugee Festival, and more importantly, ask you to take some meaningful activity photos.

Best

DIIR Photographer
to me

Dear [redacted],

I'm very happy to receive your invitation. I haven't heard about refugee festival till now. Can I know more details about this festival and venue of the festival.
Thank you

Regards
Tenzin Phende

Tdorjee <[redacted]@gmail.com>
to DIIR

World Refugee Day 2018 is on June 20th. This is an annual event, held on the same date each year, and 2018 is the 18th year of the event, run by the United Nations Refugee Agency, to state that the world supports an
The event is about raising global awareness of global responsibility for refugees.For more detailed information, you can view the official website announcement:
https://www.awarenessdays.com/awareness-days-calendar/world-refugee-day-2018

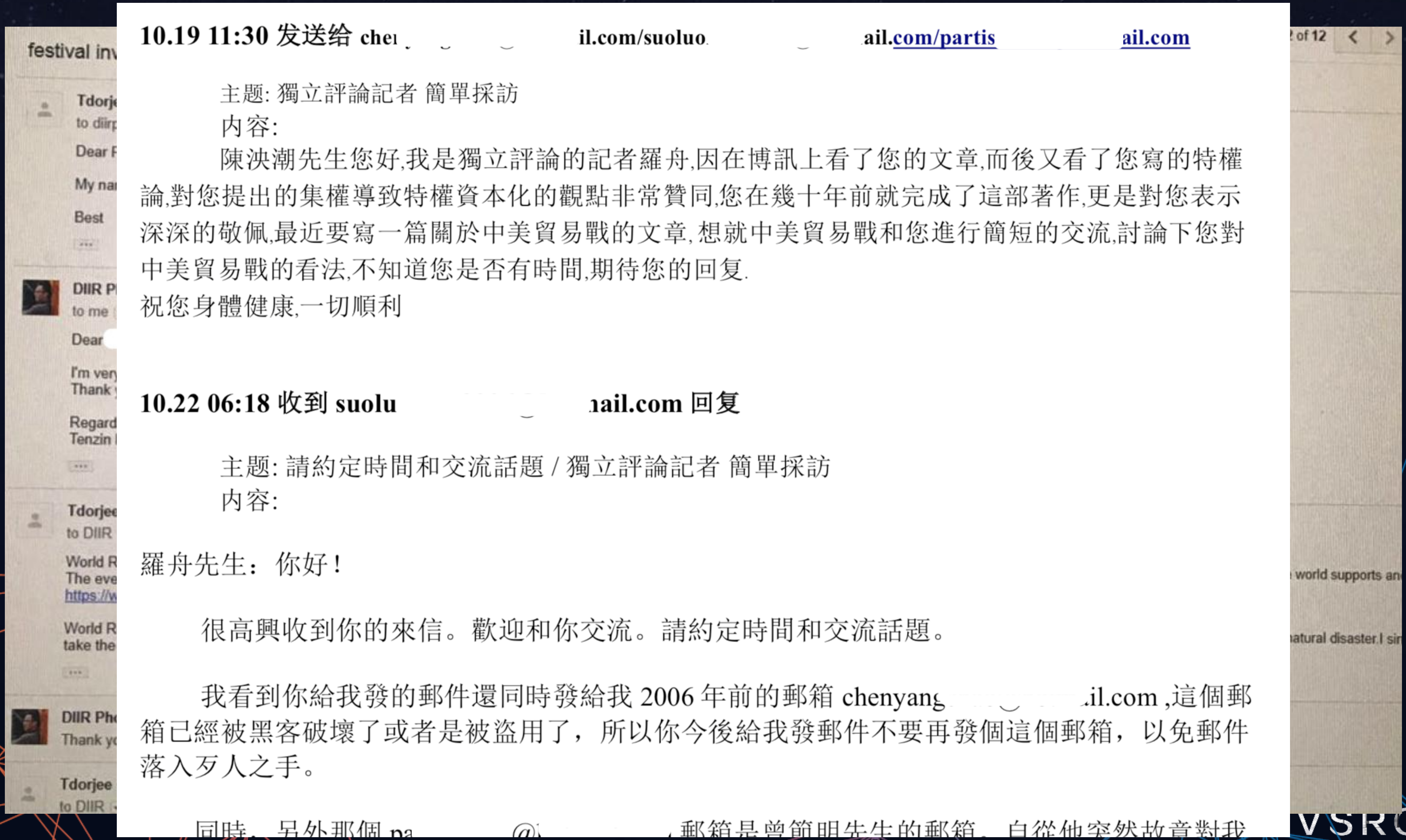
World Refugee Day honours the strength and courage of refugees and encourages public awareness and support of the refugees, people who have had to flee their home lands because of conflict or natural disaster.I sin
take the time to participate.

DIIR Photographer
Thank you for the link. One thing is still not clear that where is the venue ...

Tdorjee <[redacted]@gmail.com>
to DIIR

邮件社工

AX模式



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

內容:

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,期待您的回复.

祝您身體健康,一切順利

10.22 06:18 收到 suolu nail.com 回复

主題: 請約定時間和交流話題 / 獨立評論記者 簡單採訪

內容:

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。

同時，另外那個 pa @ 郵箱是曾節明先生的郵箱，自從他突然故意對我

VSRC成都沙龙站

邮件社工

社工策略

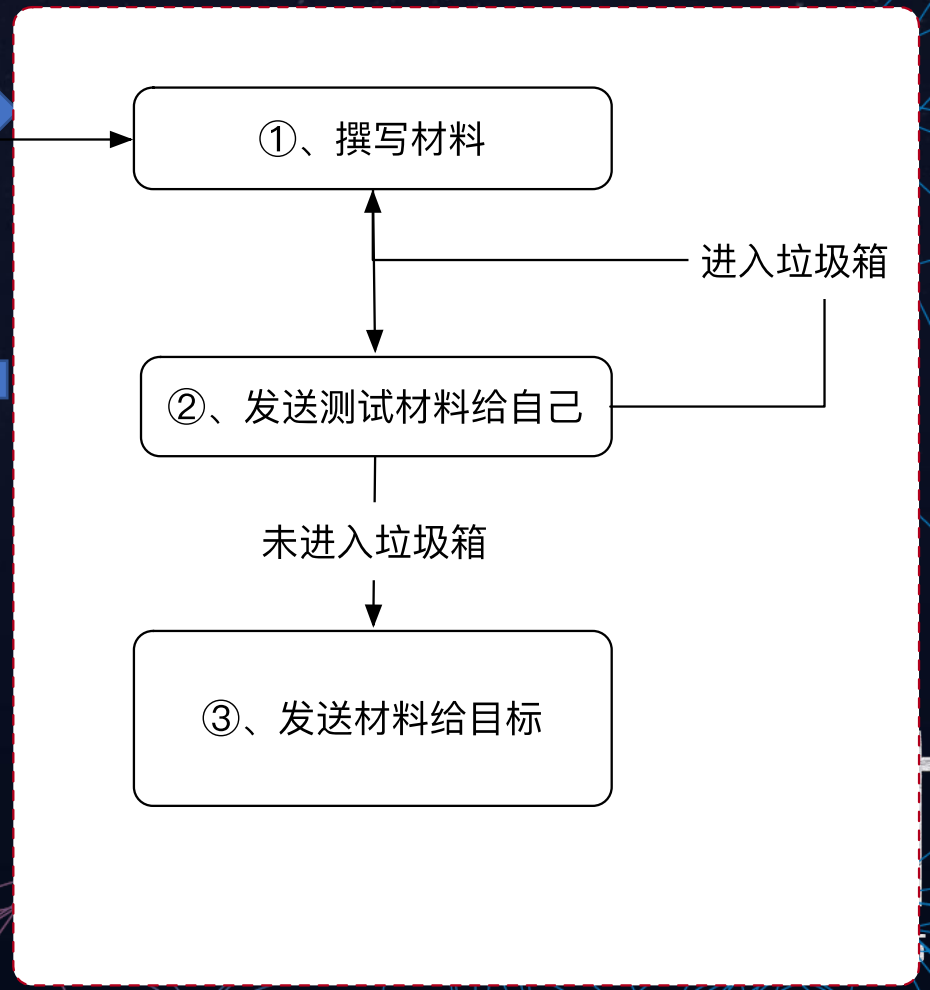
第一步、了解目标

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



邮件社工

社工策略

媒体采访

论文发表

会议咨询

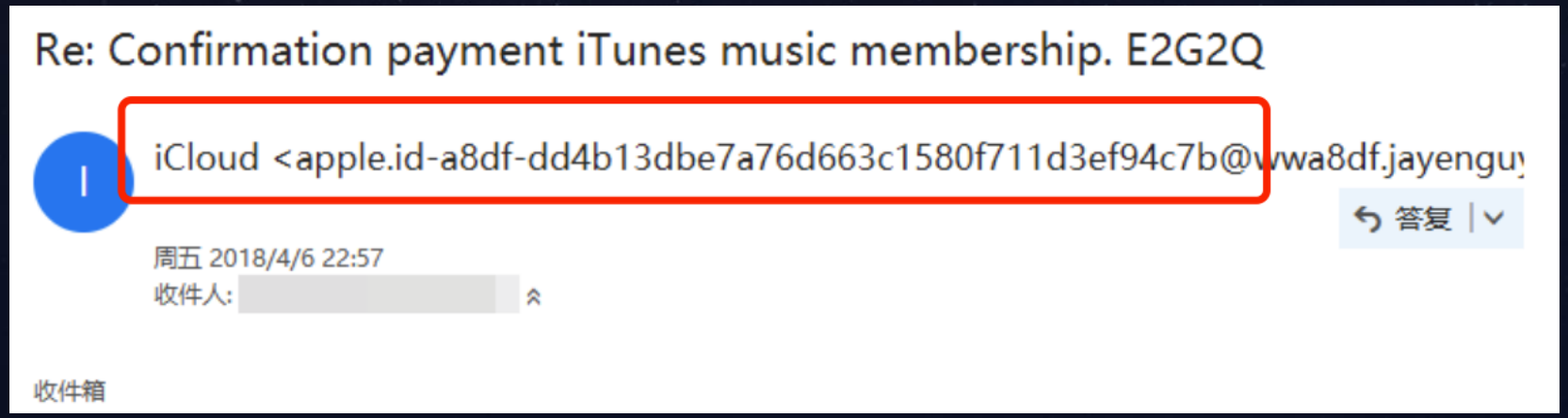
资讯文章

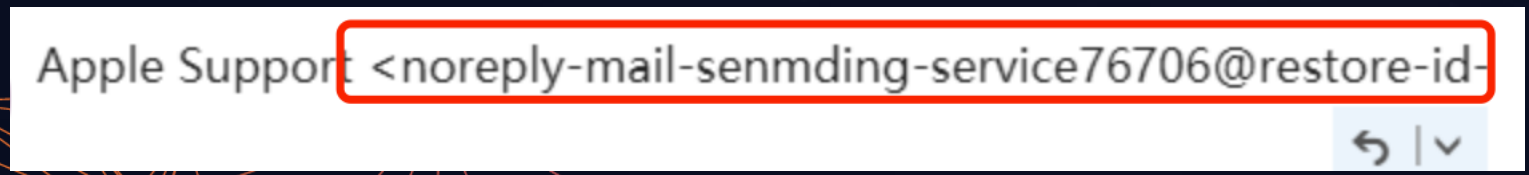
.....

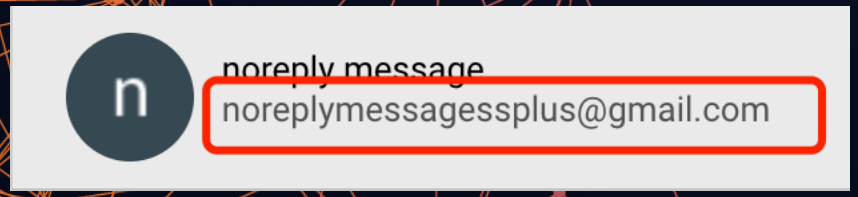
熟人、媒体、学生、学者、同行、难民.....

邮件社工

发件邮箱的重要性







邮件社工

总结

利用人的 **信任、恐惧、贪婪、激动...**

以达到我们要的目的.

人·才是最大的漏洞

---《我是谁：没有绝对安全的系统》

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

安洵信息

谷神划

VSRC成都沙龙站