

【高级威胁追踪(APT)】Patchwork组织更新技术卷土重来，针对境内教育科研单位再次发起攻击行动



此图片来自微信公众平台
未经允许不可引用

深瞻情报实验室 [深信服千里目安全技术中心](#)
深信服千里目安全技术中心

gh_c644c6e98b08

深信服千里目安全技术中心专注网络安全各技术领域研究及应用，囊括六大技术实验室和一个创新研究院，聚焦国内外漏洞、攻防对抗技术、终端安全、高级威胁、威胁情报等安全技术领域专业研究，最终赋能于产品。

2023-04-20 11:45 Posted on [北京](#)

收录于合集 #高级持续威胁追踪 51个

概述

近期，深信服深瞻情报实验室联合深信服安服应急响应中心监测到APT组织对国内高校和科研单位的最新攻击动态，并结合深信服创新研究院混动图AI模型分析，将该样本归因为Patchwork组织发起的攻击。Patchwork组织，又称摩诃草、白象、APT-Q-36、APT-C-09，是一个来自于南亚地区的境外APT组织。该组织主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，其中以窃取敏感信息为主。相关攻击活动最早可以追溯到2009年11月，至今还非常活跃。在针对中国地区的攻击中，该组织主要针对政府机构、科研教育领域进行攻击，其中以科研教育领域为主。

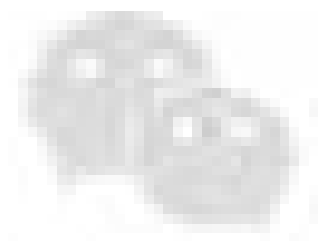
在本次攻击活动中，我们监测到Patchwork组织使用钓鱼邮件攻击高校和科研机构的事件，本次事件相关的邮件附件名称为“全国妇联2023年修订《妇女权益保障工作指导意见》”、“先进结构与复合材料等4个重点专项2023年度项目申报指南的通知”、“长江设计集团有限公司2023年度招聘公告”。

邮件内容以职场中的性骚扰事件或项目申报通知为由，引诱用户打开带有密码的压缩包文件，压缩包中包含一个恶意lnk文件，用于下载第二阶段BADNEWS远控。通过分析我们发现该组织对以往使用的BADNEWS，进行了更新，对关键功能的调用顺序和方式做出了改进，更换了控制指令和调整对应功能的实现，替换部分关键字字符串。



分析

在本次攻击活动中，解压后的文件为.pdf.lnk的双后缀文件，实际为lnk文件，双击后会执行文件中的powershell命令。由于lnk文件不会显示后缀名，可以使用cmd的“dir”指令或者右键文件属性进行查看文件，以防执行恶意的钓鱼文件，下表为该文件详细信息。



此图片来自微信公众平台
未经允许不可引用

该LNK文件会从<https://shhh2564.b-cdn.net/abc.pdf>下载诱饵文件并打开，接着从<https://shhh2564.b-cdn.net/c>下载文件到C:\ProgramData\Microsoft\DeviceSync\p，将p文件复制为同路径下的OneDrive.exe，并删除p文件，最后创建计划任务每隔1分钟执行OneDrive.exe。

将捕获到的键盘记录以文本的方式保存在%temp%目录下的kednfbdnfby.dat文件中，代替了原先使用的“kpro98.dat”文件名。

```

*OneDrive.exe x
          ff ff ff
0040809e 51          PUSH    ECX
0040809f 50          PUSH    EAX
004080a0 ff 15 6c    CALL    dword ptr [->KERNEL32.DLL::GetProcAddress]
          b0 43 00
004080a6 68 e8 03    PUSH    0x3e8
          00 00
004080ab 56          PUSH    ESI
004080ac 57          PUSH    EDI          Temp
004080ad a3 0c 1f    MOV     [DAT_00451f0c],EAX          = ??
          45 00
004080b2 ff d0      CALL    EAX          call GetEnvironmentVariable
004080b4 6a 19      PUSH    0x19
004080b6 e8 3e f8    CALL    FUN_004178f9          undefined FUN_004178f9()
          00 00
004080bb 8b f0      MOV     ESI,EAX
004080bd 68 d0 07    PUSH    0x7d0
          00 00
004080c2 c7 46 10    MOV     dword ptr [ESI + 0x10],0x0
          00 00 00 00
004080c9 c7 46 14    MOV     dword ptr [ESI + 0x14],0x0
          00 00 00 00
004080d0 c6 46 18 00 MOV     byte ptr [ESI + 0x18],0x0
004080d4 c7 06 6b    MOV     dword ptr [ESI],0x6e64656b
          65 64 6e
004080da c7 46 04    MOV     dword ptr [ESI + 0x4],0x6e646266
          66 62 64 6e
004080e1 c7 46 08    MOV     dword ptr [ESI + 0x8],0x2e796266
          66 62 79 2e
004080e8 c7 46 0c    MOV     dword ptr [ESI + 0xc],0x746164          kednfbdnfby.dat
          64 61 74 00
004080ef e8 06 74    CALL    FID_conflict:<lambda_invoker_cdecl>          void * FID_conflict:<lambda_invo...
          01 00
004080f4 68 d0 07    PUSH    0x7d0
          00 00
  
```

使用正常的WEB服务（myexternalip.com，api.ipify.org，ifconfig.me）获取主机IP外网地址。

The screenshot shows a debugger window with the following assembly code and registers:

```

008431C6 68 F8888800 push OneDrive.00888AF8
008431C8 E9 02050000 jmp OneDrive.008436D2
008431D0 6A 00 push 0x0
008431D2 68 00000000 push 0x00000000
008431D7 6A 00 push 0x0
008431D9 6A 00 push 0x0
008431DB 57 push edi
008431DD 50 push eax
008431DD FF15 4C1E890 call dword ptr ds:[0x091E4C]
008431E3 894424 0C mov dword ptr ss:[esp+0xC],eax
008431E7 85C0 test eax,eax
008431E9 74 B9 jc short OneDrive.008431A4
008431EB 68 C4000000 push 0xC4
008431F0 8D8424 24020 lea eax,dword ptr ss:[esp+0x224]
008431F7 6A 00 push 0x0
008431F9 50 push eax
008431FA E8 D1620100 call OneDrive.008594D0
008431FF 83C4 0C add esp,0xC
00843202 68 D0070000 push 0x7D0
00843207 FF5424 18 call dword ptr ss:[esp+0x18]
0084320B 8D4424 34 lea eax,dword ptr ss:[esp+0x34]
0084320F 50 push eax
00843210 68 C4000000 push 0xC4
ds:[00891E4C]=75034FD0 (wininet.InternetOpenURL)
  
```

The registers window shows:

```

寄存器 (FPU)
EAX 00C00004 ASCII "接"
ECX E906E355
EDX 00000000
EBX 00E28DF8 ASCII "IP retriever"
ESP 00AFF8A0
EBP 00AFFBA8
ESI 00AFFD74
EDI 00E30480 ASCII "http://myextern
EIP 008431DD OneDrive.008431DD
C 0 ES 002B 32位 0(FFFFFFFF)
P 0 CS 0023 32位 0(FFFFFFFF)
A 0 SS 002B 32位 0(FFFFFFFF)
Z 0 DS 002B 32位 0(FFFFFFFF)
S 0 FS 0053 32位 9D7000(FFF)
T 0 GS 002B 32位 0(FFFFFFFF)
D 0
0 0 LastErrr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
  
```

The memory dump at the bottom shows:

```

地址  HEX 数据  ASCII
0087B000 C0 47 22 75 00 46 22 75 F0 46 22 75 30 48 22 75 00AFF8A0 00C00004 ASCII "接"
0087B010 60 36 22 75 00 00 00 00 70 49 7D 74 00 00 00 00 00AFF8A4 00E30480 ASCII "http://myexternalip.com/raw"
0087B020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00AFF8A8 00000000
0087B030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00AFF8AC 00000000
  
```

将上一步获取到的外网IP地址在（api.iplocation.net，ipapi.co）等WEB服务中查询所属国家的名称

```

00843910 | 47 | inc edi
00843914 | 84C0 | test al,al
00843916 | 75 F8 | jnz short OneDrive.00843910
00843918 | 8BC0 | mov ecx,edx
0084391A | C1E9 02 | shr ecx,0x2
0084391D | F3:A5 | rep movs dword ptr es:[edi],dword ptr d
0084391F | 6A 00 | push 0x0
00843921 | 7A 00000000 | push 0x0

```

```

寄存器 (FPU)
EAX 00E83600 ASCII "rytip="
ECX 00000000
EDX 00000001
EBX 00E835D8 ASCII "https://api.iplocation.net/?cmd-ip-cou
ESP 00AFF900
EBP 00AFFD90

```

最后将获取到的信息加密后保存到一个字符串中。

通过分析得到收集的信息如下：

uu34	SmBIOS uuid
puiip89	外网 IP 地址
igggp	内网 IP 地址
usfghnam	用户名
osgh	Windows 系统版本
locghg	外网 IP 地址所属国家

收集的信息都会经过base64编码后进行AES-128的CBC模式加密，最后将加密后的数据再进行base64编码。AES-128加密使用的密钥为“qgdrbn8kloiuytr3”，IV为“feitrt74673ngbfj”。该加密方式同时也应用于C2下发的数据，下文简称该方式为AES-128加密。

```

FUN_004041d0():
local_8_0_1_ = 1;
pppppuVar15 = &local_d8;
if (0xf < local_c8_4_4_) {
    pppppuVar15 = local_d8;
}
pcVar1 = (char *) ((int)pppppuVar15 + 1);
do {
    cVar3 = *(char *) pppppuVar15;
    pppppuVar15 = (undefined4 *****) ((int)pppppuVar15 + 1);
} while (cVar3 != 0);
BaseE4_004021b0((int)pppppuVar15 - (int)pcVar1);

```

接着获取CreateThread函数地址，创建3个线程与C2：charliezard.shop的443端口通信，uri为/tagpdjjarzajgt/coewlzafloumm.php，通信内容会使用AES-128加密数据，每次传输最大数据为加密前5000字节。

```

Sleep(0x6a4);
CreateThread_00451fa8 = GetProcAddress(hModule, (LPCSTR)local_3c);
iVar6 = (*_CreateThread_00451fa8)(0,0,FUN_00409900,local_168,0,local_22c);
if (iVar6 != 0) {
    iVar6 = 0x21f;
    do {
        uVar5 = iVar6 / 10 + (iVar6 >> 0x1f);
        iVar6 = (uVar5 >> 0x1f) + uVar5;
    } while (0 < iVar6);
    Sleep(0x13ec);
    FUN_004041d0();
    local_8_0_1_ = 0x15;
    iVar6 = (*_CreateThread_00451fa8)(0,0,FUN_004092a0,local_2ac,0,local_230);
    if (iVar6 != 0) {
        Sleep(0x118);
        FUN_004041d0();
        local_8_0_1_ = 0x15;
        iVar6 = (*_CreateThread_00451fa8)(0,0,FUN_00409440,local_2c4,0,local_264);
        if (iVar6 != 0) {
            thunk_FUN_0041f4dd(puVar9);
            thunk_FUN_0041f4dd(puVar9);
        }
    }
}

```

线程FUN_00409900负责将收集到的信息使用POST方式发送给C2，内容为收集的系統信息加密数据。发送完成后进入随机1-101秒的睡眠，睡眠结束后重复信息发送的过程，用于验证主机是否在线。

线程FUN_00451a8负责对C2下发的指令作出响应，发送uugmkis参数附带机器唯一标识符获取C2下发的指令。



指令格式为：指令\$选项1\$选项2，指令和选项1都需要经过AES-128解密，选项2没有使用到，回传给C2的数据也都是经过AES-128加密过，对比以往的BADNEWS各个控制命令的实现，我们发现该组织舍弃了原先将执行结果保存到文件的环节，采用直接将数据加密后回传给C2，经分析得到所有的命令功能如下：

指令	功能	选项 1
3hdfghd1	指定文件读取	要读取文件的绝对路径
3fgbfjnb3	读取 kednfbdnfby.dat 文件（键盘记录）的内容	/
3gjdfghj6	执行 cmd 指令并将结果返回给 C2	要执行的 cmd 指令
3fgjfhg4	指定文件目录遍历	要遍历的文件夹路径，只获取文件路径
3gnfjkh7	文件下载和执行，下载的数据经过和上文相同方法解密后，写入到%temp%\ dp[4 个随机字符].exe，并执行	下载文件的 url
3ngjfng5	文件下载，下载的数据经过和上文相同方法解密后，写入到%temp%\[下载路径中的文件名]	下载文件的 url
3fghnbj2	屏幕截图	/

溯源归因

溯源归因-文件归因：

通过分析OneDrive.exe的存放路径C:\ProgramData\Microsoft\DeviceSync是该组织常用文件路径之一，对下载的RAT组件进行分析，其代码逻辑、通信的模式及URL格式等符合该组织专有远控BADNEWS的特征。


与BADNEWS相似之处表现在获取时区名称的代码过程。

检测是否为目标国家时区

```
-----  
local_ec = 0x73e6f43;  
uStack232 = 0x57e5c6f;  
uStack228 = 0x6f64e69;
```

```
-----  
pppppuVar13 = local_314;  
if (0xf < local_300) {  
    ccccccVar13 = local_314f01;
```

除此之外，通过深瞻情报实验室累积的情报数据，深信服创新研究院混动图AI模型也将该样本归因到摩诃草，也就是Patchwork组织。



安全内参: AI特征分析结论(TOP5)

- 1: 【摩诃草组织】
- 2: 【FerociousKitten组织】
- 3: 【拉撒路组织】
- 4: 【Andariel组织】
- 5: 【海莲花组织】

IOCS

IOC 类型	详细信息
domain	charliezard.shop
domain	shhh2564.b-cdn.net
domain	msit5214.b-cdn.net
url	https://msit5214.b-cdn.net/c
url	https://shhh2564.b-cdn.net/abc.pdf
url	https://shhh2564.b-cdn.net/c
md5	f4785bc53e5b3e47f9b5d73eda758c3a
md5	f54df58848a7ec47587887b40a3b9acf
md5	5bb083f686c1d9aba9cd6334a997c20e
sha256	5c89e1bafa787294856acc458fd9021ddefa67d9826bc2234252db773a8212b5

总结

Patchwork常使用鱼叉攻击对目标进行打点攻击，具有一定的危险性。主要针对教育、科研机构等行业进行攻击，窃取该类单位的高新技术研究资料或规划信息等，相关行业及单位需要警惕并加强网络防御。本次事件中，该组织改造BADNEWS攻击组件，不断加强其窃密、反分析及反取证能力，安全公司应加强相关技术的检测。

深信服蓝军高级威胁 (APT) 团队专注全球高级威胁事件的跟踪与分析，拥有一套完善的自动化分析溯源系统以及外部威胁监控系统，能够快速精准的对APT组织使用的攻击样本进行自动化分析和关联，同时积累并完善了几十个APT以及网络犯罪威胁组织的详细画像，成功帮助客户应急响应处置过多起APT及网络犯罪威胁组织攻击事件，未来随着安全对抗的不断升级，威胁组织会研究和更多新型的TTP，深信服高级威胁团队会持续监控，并对全球发现的新型安全事件进行深入分析与研究。

参考链接

