

Re: vbscript script file

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-09/3691.html>

From: Torgeir Bakken \ (MVP) (Torgeir.Bakken-spam_at_hydro.com)

Date: 09/02/04

Date: Fri, 03 Sep 2004 00:26:02 +0200

anonymous@discussions.microsoft.com wrote:

> *most of my music and picture files have been transformed*
> *into vbscript script files. Does anyone know how to*
> *change them back.*
>
> *I have no idea how it happened, but I have lost a lot of*
> *files!*

Hi

Most likely you are infected by a worm...the infamous loveletter.vbs or a variant of it.

Most loveletter worms just set .mp3 files to hidden (that is why you could recover them), but for .jpg files, the story is different, they are deleted.

loveletter usual extension handling:

MP2, MP3:

Creates a new file with extension .VBS (adds to old file name). It writes its body to it and sets the file attribute "hidden" to the original file.

JPG, JPEG:

Creates new file with extension .VBS (adds this extension to old file name and extension) (i.e. PIC1.JPG.VBS). Writes worm body to it and deletes original file.

You might be able to save some of the JPG files if you have not made to many changes to the hard disk yet:

<http://www.claymania.com/zefrjpg.html>

See also:

<http://www.symantec.com/avcenter/venc/data/vbs.loveletter.a.html>

Here is some info from an another newsgroup post:

<quote>

From: Walter (castigamatti@tiscalinet.it)

Subject: I-Worm.LoveLetter

Newsgroups: it.comp.aiuto

Date: 2000/05/06

I-Worm.LoveLetter is Internet worm written in the scripting language "Visual Basic Script" (VBS). It works only on computers on which the Windows Scripting Host (WSH) is installed. The worm performs destructive actions and sends its copy by E-mail.

Destructive actions:

After starting from the VBS file the worm searches all files on all local and mapped network drivers. For some extensions of filenames the worm does the following:

VBS, VBE:

Overwrites files with the worm body.

JS, JSE, CSS, VSH, HST, HTA:

Creates a new file with original filename and extension .VBS and deletes original file.

JPG, JPEG:

Creates new file with extension .VBS (adds this extension to old file name and extension) (i.e. PIC1.JPG.VBS). Writes worm body to it and deletes original file.

MP2, MP3:

Creates a new file with extension .VBS (adds to old file name, see above for details). It writes its body to it and sets the file attribute "hidden" to the original file.

MIRC32.EXE, MLINK32.EXE, SCRIPT.INI, MIRC.HLP, MIRC.INI:

If one of these files was found the worm creates the file SCRIPT.INI in the directory were one of the above files resides.

The worm also creates some files with its body in system directory.

MSKERNEL32.VBS, WIN32DLL.VBS, LOVE-LETTER-FOR-YOU.TXT.VBS

It sets appropriates keys in the system registry (Automatic run keys) with full names of files:

MSKernel32.vbs, Win32DLL.vbs

It adds system registry keys:

microsoft.public.windowsxp.general: Re: vbscript script file

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
\MSKernel32

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
\RunServices\Win32DLL

Spreading via E-mail

The worm sends itself via E-mail. To achieve this the worm sends itself to each address from address book. It works only when the email program Outlook 97/98/2000 is installed.

The letter's subject:

ILOVEYOU

Message body:

kindly check the attached LOVELETTER coming from me.

Attached file name:

LOVE-LETTER-FOR-YOU.TXT.vbs

The virus creates a HTML dropper in Windows system directory. The HTML dropper displays the message:

This HTML file need ActiveX Control
To Enable to read this HTML file
– Please press 'YES' button to Enable ActiveX

After this the dropper creates the MSKERNEL32.VBS with the worm body and sets it for auto execution from system registry.

</quote>

--

torgeir, Microsoft MVP Scripting and WMI, Porsgrunn Norway
Administration scripting examples and an ONLINE version of
the 1328 page Scripting Guide:
<http://www.microsoft.com/technet/scriptcenter/default.mspx>