Global Information Assurance Certification Paper

What is the VBS.Stages.A Worm?
Patricia A. Dooley
November 28, 2000

Introduction

The VBS.Stages.A Worm was reportedly created by an Argentinean virus writer going by the name of "Zulu". He launched the worm just prior to the U.S. Memorial Day weekend but the results and/or damage did not start to manifest itself until the second week of June (12-15 June 2000). On the following Monday several antivirus companies began warning about the rapidly spreading VBS worm, by the end of that same week it had managed to spread globally. The VBS.Stages.A Worm is also known as 'Stages Worm', 'SHS_STAGES.A', 'IRC/Stages.worm', 'Life_Stages Worm', 'I-Worm.Scrapworm' and the 'Bloodhound.VBS Worm'.

What is the VBS.Stages.A Worm?

The VBS.Stages.A Worm is written in Visual Basic. "Visual Basic is a programming environment from Microsoft in which a programmer uses a graphical user interface to choose and modify preselected sections of code written in the Beginner's All-Purpose Symbolic Instruction code programming language." The VBS.Stages.A Worm is not overly malicious in that it does not delete files or wipe your hard drive but instead acts as a denial-of-service by overloading corporate e-mail servers. It fills buffers by repeatedly mass mailing itself as an Microsoft Outlook e-mail attachment and then immediately deletes any trace of the copies to make sure the e-mails don't show up in the 'Sent Items' folder and raise a profile that might cause suspicion. In addition to mailing itself out, it copies itself directly to local or remote (networked) drives with random names. These files are created in the root directory and the 'My Documents' and 'Windows\Start\Menu\Programs' directories. "Then it creates the following files into the Window System directory: 'MSINFO16.TLB', SCANREG.VBS', 'VBASET.OLB' and the following files into the Recycled directory: 'DBINDEX.VBS', 'MSRCYCLD.DAT', 'RCYCLDBN.DAT', 'RECYCLED.VXD'". It also modifies configuration (.ini) files and can spread itself via mIRC and Pirch (Internet Relay Chat programs) chat when the infected user joins a chat group.

What does VBS.Stages.A Worm look like?

The VBS.Stages.A Worm is different from previous e-mail worms in that it randomly generates the 'subject' line to one of twelve variations. The variations are: "Fw: Life Stages", "Fw: Funny", "Fw: Jokes", "Fw: Life Stages text", "Fw: Funny text", "Fw; Jokes text", "Life Stages", "Funny", "Jokes", "Life Stages text", "Funny text", "Jokes text."[2] The worm itself is an attachment that appears to be a text file and even assumes the icon of one, but is actually a Microsoft Shell Scrap Object file. "These types of files are executable and can contain a wide variety of objects. The scrap object (.shs) extension does not appear in Windows Explorer even if all file extensions are displayed." This tends to fool users into thinking it is a harmless text file instead of an active worm.

The attachment when opened looks like this:

The male stages of life:

Age. Seduction lines.
17 My parents are away for the weekend.
25 My girlfriend is away for the weekend.
35 My fiancée is away for the weekend.
48 My wife is away for the weekend.
66 My second wife is dead.

Age. Favorite sport.
17 Sex.
25 Sex.
35 Sex.
48 Sex.
66 Napping.

Age. Definition of a successful date.
17 Tongue.
25 Breakfast.

35 She didn't set back my therapy.
48 I didn't have to meet her kids.
66 Got home alive.

The female stages of life:

Age. Favorite fantasy.
17 Tall, dark and handsome.
25 Tall, dark and handsome with money.
35 Tall, dark and handsome with money and a brain.
48 A man with hair.
66 A man.

Age. Ideal date.
17 He offers to pay.
25 He pays.
35 He cooks breakfast next morning.
48 He cooks breakfast next morning for the kids.
66 He can chew his breakfast. [1]

How you get 'infected'.

Infection can occur one of two ways; e-mail or mIRC/Pirch chat. Infection by e-mail occurs when you receive the e-mail and open the attachment. As you are reading the 'Joke' text (attachment) the 'worm' is modifying your system registry, the Regedit.exe and the Mirc.ini files. In addition it is mailing itself out to up to a hundred randomly selected addresses in your address book. The VBS.Stages.A worm is accomplishing all this in the background without you being aware of any of it occurring. Infection by mIRC/Pirch occurs when you are already in a chat room that is then entered by an 'infected' member. The 'infected' person's SOUND32B.DLL file was modified by the VBS.Stages.A worm to spread itself.

How to get rid of it.

Most of the major antivirus companies have available downloadable tools to remove the VBS.Stages.A worm from your system. They include detailed instructions but require that you are somewhat knowledgeable about Windows and DOS.

F-Secure has come out with a "Manual disinfection can be done by following the steps below. Note that these instructions assume that you have Windows installed to C:\Windows. If you have Windows installed to any other location, please change the path.

- Delete the following files from the Windows system directory
  MSINFO16.TLB, SCANREG.VBS and VBASET.OLB
- Delete the following files from the Recycled directory
  DBINDEX.VBS, MSRCYCLD.DAT, RCYCLDBN.DAT
- Unhide and move 'RECYCLED.VXD' to the Windows directory and rename it as 'REGEDIT.EXE'. This can be done from the command prompt with the following commands:
  - attrib -h -s -r c:\recycled\recycled.vxd
  - move c:\recycled\recycled.vxd c:\windows\regedit.exe
- Restore the association of .reg files by changing the registry:
  HKEY_CLASSES_ROOT\regfile\DefaultIcon\(Default) = 'C:\Windows\regedit.exe,1'
  HKEY_CLASSES_ROOT\regfile\shell\open\command = 'regedit.exe %1'
- Remove the autostart registry entry
  HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\ScanReg " [4]

The Symantec AntiVirus Research Center has developed a free, downloadable tool to repair the damage done by the worm:

http://www.symantec.com/avcenter/venc/data/fix.vbs.stages.html [5]

How to protect against it.

The first line of defense against the VBS Stages.A worm is you. How many times have you heard the warnings "Don't open files with attachments unless you are expecting them", "Don't open executable files" and "Don't open files from people you don't know". Of course the VBS Stages.A worm gets around the second one by not looking like an executable file and the last one by mailing it from someone's address book and assuming you know the people whose mailing lists you are on. That still leaves the first one, if you receive an unexpected file with attachments, a good practice is to telephone the person you have received the file from and verbally confirm they sent you the file. The reverse is also true and a simple courtesy, telephone the person so they know to expect a file with attachments from you.

Another defense-in-depth is to modify your firewall or filters to stop or block incoming files with unusual or suspicious attachments. "SARC (Symantec Antivirus Research Center) suggests that corporate customers configure their email filtering systems to filter out or stop all incoming emails that have attachments with .SHS extensions."[6]

Users can download and install several security updates (mostly free) that will effectively block unwanted .shs files.

Microsoft's Outlook email security update available at Microsoft's web site to block files with SHS extensions:

http://www.microsoft.com/windows2000/downloads/recommended/sp1/default.asp

Trend Micro has their Desktop Antivirus Solution Certified for Microsoft Windows 2000 –'PC-cillin 2000' available at Trend Micro's web site:

http://www.antivirus.com/pc-cillin/products/news_pr041400.htm

Summary.

Now that we know how the VBS Stages.A Worm works, what it looks like and how to defend against it should we feel safe? Maybe from the VBS Stages.A Worm, but as Steve Trilling of Symantec says "We see 10 to 15 new viruses every day"[2], now do you feel paranoid? Good. That uneasy feeling just might be enough to get you to upload that antivirus software you've 'been meaning' to load and it might keep you updating your security software. Wait, Steve Trilling was talking about viruses not worms, but does the VBS Stages.A Worm really fit the definition of a worm?

According to the SANS Institute a "malicious code is called a worm when it requires no specific action on the part of the user to enable infection and propagation. It just spreads." On the other hand "A virus is a piece of parasitic code (or program) written specifically to execute on behalf of the user without the user's permission (or knowledge)…If the code requires the user to open an email or load a screen saver or take some other action, then it is called a virus."[7] If we accept these definitions then the references used earlier, while correct in the breakdown and analysis of the functionality of the VBS Stages.A Worm were incorrect in naming it a worm. The VBS Stages.A Worm requires the user to open an e-mail attachment before it modifies files, replicates and mails itself out, or to join a chat room where it infects the other chat room members, all this is accomplished without the user's knowledge. The VBS Stages.A Worm therefore fits the definition of a virus to a tee. This is further substantiated by Micro Trend's virus encyclopedia, which further defines VBS Stages.A Worm (a.k.a. Bloodhound.A) as a 'boot virus'. The VBS Stages.A Worm might be more appropriately named the VBS Stages.A Virus.

You can lower the risk of being 'infected' by a virus or worm but unless you unplug your computer you can never be 'safe'. The price of connectivity is to be ever vigilant.

References:

1. Sullivan, Bob (MSNBC). "'Stages.worm' on the loose" (June 19, 2000) URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2589845,00.html (October 19, 2000)

2. Szucs, Lisa and Bloxsom, Iolande. "'Life Stages' Worm Spreading Rapidly" (June 19, 2000) URL: http://www.techtv.com/cybercrime/viruses/story/0,9955,2590003,00.html (October 20, 2000)

3. Whatis?com "Visual Basic" (May 23, 2000) URL: http://www.whatis.com/WhatIs_Definition_Page/0,4152,213309,00.html (November 9, 2000)

4. Tocheva, Katrin, Hypponen, Mikko and Rautiainen, Sami. "F-Secure Computer Virus Information Pages: 'Stages'" URL: http://www.f-secure.com/v-descs/stages.htm (November 8, 2000)

5. Symantec SARC, "What is the VBS.Stages.A worm? Virus Information (June 19, 2000)URL: http://service1.symantec.com/SUPPORT/nav.nsf/949e46314f0916a0852565d00073bbfd/

06c3043abd94dbbb88256903007453e5?OpenDocument (November 8, 2000)

6. Ewell, Brian, Symantec, "VBS.Stages.A" Symantec AntiVirus Research Center (June 22, 2000) URL: http://www.symantec.com/avcenter/venc/data/vbs.stages.a.html (November 7, 2000)

7. Kerby, Fred. "Malicious Software" SANS Security Essentials, Edited by Phillip Boyle (June 3, 2000) URL: http://www.sans.org/momaudio/s=1.1.6/a=Qxr0Q9cdbCI/kerbyvirus (November 28, 2000)

8. Micro Trend, Virus Information Center, Virus Encyclopedia, URL: http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=BLOODHOUND.A* (November 14, 2000)