GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

GIAC Advanced Incident Handing and Hacker Exploits Practical Assignment

Wilfred McInnis
PH2000

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

12 Sep 00

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction

I work in an organization where until recently the duties for IS security have been a secondary or at times a tertiary function. Although our network spans the country and is made up of many autonomous LANs we have been quite fortunate in that the occurrences of malicious code have been minimal. These rare incidents, for the most part, have been eradicated without wide spread problems. Credit for this goes to our education and awareness programs, anti-viral scanning software (with automatic downloads of current signature files) and to our limited access to the Internet.

Future development of our network will include greater connectivity to the Internet and increased reliance on Internet based e-mail (rather than Intranet). It is for this reason that I have selected Option 2 for my practical and chose to research VBS.Stages.A worm.

Trend Micro's Security Info describes VBS_Stages.A as an Internet worms which spreads using multiple applications such as Outlook, mIRC or PIRCH or by spreading to itself to mapped drives. Like other known VBS worms, this may arrive as an email attachment labeled LIFE_STAGES.TXT.SHS. When the scrap file is executed it launches the notepad and displays a text file containing a joke about the stages of life.

Exploit Details

Name: VBS_Stages.A

Aliases: IRC/Stages.worm
I-Worm.Scrapwowm
LIFE_STAGES.TXT.SHS
ShellScrap.worm
VBS/LifeStages
VBS/Stages.14559
VBS/Stages.2543
VBS/Stages.27536
VBS/Stages.worm

© SANS Institute 2000 - 2005 Author retains full rights.

VBS/STAGES

Variants: none

Operating Systems: Windows 9x, 2000 and NT

Protocols: VBS_Stages.A uses Outlook, mIRC, PIRCH and mapped drives to propagate itself. The worm also takes advantage of the fact that once a user is logged in on a Windows platform they have all rights to read, write, delete and execute all applications and systems files by default.

Description: The email attachment is a .SHS file. This is a Microsoft scrap object file. Scrap object files are executable. In this case the executable code opens notepad and displays a text document joke about the stages of life. As the user is reading the text file the worm is spreading itself using the methods mentioned above. The size of the attachment is always 39936 bytes. The SHS-extension is not visible, even if Windows Explorer properties have been set to show all filename extensions. This worm was authored by Zulu and utilized the mIRC script created by SimpleSimon.

Protocol Description

The inner workings of this worm are best explained by its author. It will use OUTLOOK to send itself to all contacts in the address book if the number of addresses is less than 101. If that number is more than 100 it will try to select 100 random addresses. Subject and body will be selected from some random choices. It will be run only once in each computer since it uses the registry to check if it was already run.

Network spreading. It will try to find Windows in each share (not only mapped drives) to copy itself to the startup directory, so it can be run at the next startup of the machine having the share. If it cannot find Windows in it, it will copy itself to the root of the share, waiting for someone to run it. All this includes a check so a loop between shares sending the file won't happen.

IRC spreading (MIRC and PIRCH). This includes a check in each startup,

© SANS Institute 2000 - 2005 Author retains full rights.

so the worm will still work in new MIRC and PIRCH installations. The MIRC script has a 1 in 2 chance of sending the SHS file on join or part (it alternates which event). It intercepts commands that could alter or damage the worm with the input event and also blocks all identifiers. It sends the SHS file to people when a file is received or sent and also to anyone on the notify list the first time a person appears. The script emulates the unload, remote, and events commands.

The MIRC script hides DCC sends using socket commands. Because of a problem while testing, it allows 10 seconds before closing the socket in case it has sent the data but the user has not received all of it.

There is a lot of protection in the MIRC script from IRC helpers such as those on "#nohack", "#dmsetup", etc. If the infected user enters a "bad" channel the script will try to ignore everyone in the channel and then part. The same is true if the infected user enters a channel with a topic with one of the disallowed words. If a person says "virus", "worm", "stages", "trojan", "spread", "infect", ".shs", "remote", "events", "unload", "script" or "dccallow" in either a query window, DCC chat window, channel, notice, topic, fserve, server notice, action, kick, part message, or quit message, then that user will be ignored. To stop easy fixes to this worm on IRC, the script looks for and modifies all urls. This prevents someone from saying, "Go to www.nohack.net/bin/remover.exe to get cured".

Invisible DCC sending on join event in PIRCH.

The worm uses the SHS extension, which is invisible by default, so the worm file ("LIFE_STAGES.TXT.SHS") will look like "LIFE_STAGES.TXT" even if Windows is set to show all extensions.

Shows a TXT file when run, so it will show what the user expects.

When the file is run from startup directory it won't create and show the TXT file. So if the SHS file was copied there by the network code to infect that machine, it won't be noticed.

To find the SHS file, if Word is installed it will use it to do the search. If Word is not installed, it will search for the file using VBScript code looking

© SANS Institute 2000 - 2005 Author retains full rights.

in many common paths and all subdirectories of those paths. Both methods will look for SHS files with the size of the worm in case that the file was not found with the original name.

It makes 2 backup copies of the worm with different names, one in Windows' "SYSTEM" directory and other in the recycled bin directory of the drive where Windows is located (if it doesn't exist the worm creates it). It copies the SHS file to some places with random names. These files may make the worm come back after removing it if someone runs them. It creates two VBS files to restore the worm from backup copies if the main copy is deleted. One of these is run at each startup (using the registry) and the other is run using ICQ's startup if ICQ is installed. Since these files will have a backup copy, each of them is able to restore the other, including also the registry settings needed. These VBS files are also able to restore the other VBS by using the SHS file, if the backup copy was deleted. In addition, they will delete the SHS file if it is found in the startup directory. So, when the worm comes from the network using that directory it will be run and it will create these VBS files, so it could be deleted later by any of them.

Changes the SHS file icon to the TXT file icon and it sets the TXT extension to be always visible (even when Windows is set to hide known extensions). This way, since the SHS extension is always invisible, after the first run, the SHS file will
be seen as a TXT file (same icon and extension).

It moves "REGEDIT.EXE" to make it more difficult to remove the worm from the registry. It will be named "RECYCLED.VXD" and it will be located in the recycle bin directory. REG files will still work and will have the correct icon.

It uses the recycle bin directory to store some backup files and "REGEDIT.EXE". These files won't be seen in many utilities, so it will be more difficult to find and delete them. Also, some versions of some antiviral programs don't check this directory (recycle bin).

The SHS file will change its contents and size after the first run. Since the VBS file
inside it searches for the SHS file with the original size, it won't find it after

© SANS Institute 2000 - 2005 Author retains full rights.

the first
run. Therefore, this means that the worm won't work when sending it manually after a first run, it will only work when it is sent by itself (since it will have the original size).
All copies of the worm that are created in the first run are like the original, so this
won't be a problem when spreading.

Encrypted strings. The encryption function uses as seed a value that is taken by reading itself (similar to HTML/VBS.Zulu 3.1 virus).

Description of Variants

Although no variants are listed, it is important to note that the worm would arrive in the following format with

From: name-of-the infected-user
To: random-name-from-addr-book
Subject: (Random subject)*
Body: (body)
Attachment: LIFE_STAGES.TXT.SHS

*Random subject

The subject line is variable but limited to twelve possibilities based on the following format:
Subject: (Sub1 + Sub2 + Sub 3),
where Sub 1->> "FW:",""
Sub 2->> "Life Stages", "Funny", "Jokes"
Sub 3->> "text",""

One example would be "FW: Jokes text".

How the Exploit Works

When the file attachment is opened, the worm shows the following text:

© SANS Institute 2000 - 2005 Author retains full rights.

- 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 fiancee 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.	Definiton 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.	Favourite fantasy.
17	Tall, dark and hansome.
25	Tall, dark and hansome with money.
35	Tall, dark and hansome with money and a brain.
48	A man with hair.
66	A man.

Age.	Ideal date.
17	He offers to pay.
25	He pays.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

35 He cooks breakfast next morning.
48 He cooks breakfast next morning for the kids.
66 He can chew his breakfast.

It copies itself to the Windows directory with the name "LIFE_STAGES.TXT.SHS". Then it creates the following files into the Windows System directory:

MSINFO16.TLB
SCANREG.VBS
VBASET.OLB

And the following files into the Recycled directory:
DBINDEX.VBS
MSRCYCLD.DAT
RCYCLDBN.DAT
RECYCLED.VXD

The worm creates files with random names. The names are have one of the strings below, followed by a line ("-") or an underline ("_") and a random number between 0 - 999.

IMPORTANT
INFO
REPORT
SECRET
UNKNOWN

The file extension is always ".TXT.SHS". For example, the name of the file can be "UNKNOWN-123.TXT.SHS" or "IMPORTANT_432.TXT.SHS". These files are created to the root directory, "My Documents" and "Windows\StartMenu\Programs" directories in every mapped network drive.

Furthermore, the worm modifies the association of ".REG" files to point to the copy of "REGEDIT.EXE" that it has created to the Recycled directory as "RECYCLED.VXD". The original "REGEDIT.EXE" is deleted from the Windows directory.

VBS/Stages.A makes modifications to the Windows registry. It adds the

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

following key, so it will be executed when the system is restarted:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\ScanReg

In addition, it changes Windows configuration in such a way that the extension of ".TXT" files is always displayed - regardless of the Windows Explorer configuration.

This worm was found in early June 2000. It started to spread globally later during the same month.

How to Protect Against It

It is recommended the following precautions are taken:

- Ensure that you are running anti-virus software with the latest signature update.
- Never share an entire drive, only share specific directories to specific users as required. When sharing a directory, never allow unrestricted access, always use a strong password to protect the share or limit access to the share to specific users.
- Where possible, do not use persistent mapped network drives.
- Filter email attachments to restrict .VBS and .SHS attachment.

If you become infected 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:

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
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
```

Source Code

Included as separate file "Source Code.doc"

References

F-Secure Computer Virus Information Pages
Symantec AntiVirus Research Center
Trend Micro-Security Info-Virus Encyclopedia
www.coderz.net/zulu

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.