

Appendix

Malicious Codes: A Sampler

The following are some of the malicious codes that top the list of threats¹. Of course, new viruses and their variants crop up like mushrooms so it is safer to always consult the anti-virus websites for updates.

The best sites for up to date information are:

<http://securityresponse.symantec.com/avcenter/vinfodb.html>

<http://us.mcafee.com/virusInfo/default.asp>

BackDoor-Sub7

This is a Trojan Horse (SubType: Remote Access) and, therefore, does not self-replicate. It does, however, (among other things) allow the attacker to download files onto the victim's system and run them. Backdoor-Sub7 "registers the file extension .dl as an executable file type that can be run by the operating system just like any .exe file... Because the extension is not usually associated with executable files, some virus scanners will not scan these files and the victim will not suspect these files." (McAfee)

JS/Kak@M

This virus (SubType: VBScript worm) propagates itself through e-mail and newsgroup messages using MS Outlook Express. JS/Kak uses JavaScript and an ActiveX control (Scriptlet Typelib). The script first checks to see if MS Internet Explorer 5 or higher is installed. "If it is, using an ActiveX exploit known as 'Scriptlet TypeLib', the script writes the KAK.HTA file to the Startup folder of the local machine. This will launch the code embedded in the HTA file at the next Windows startup." This virus even has the ability to re-infect a user if the preview pane is enabled and the user browses between folders which contain an infected message.

VBS/Haptime@MM

Haptime is a virus (SubType: E-mail) and can spread by means of embedded VBScript contained in the body of HTML e-mail messages and web pages. Once an infected document is opened, the computer gets infected; the machine then begins transmitting the virus via e-mail and LAN.

This virus will attach itself to files and delete files, as well as spread itself. "When the script is permitted to run, the virus inserts itself at the end of .ASP, .HTM, .HTML, .HTT, and .VBS files. If the current day plus the current month is equal to 13, the virus attempts to delete .DLL and .EXE files on local and network drives."

W32/Hybris.gen@MM

Hybris comes with a teasing message:

From: Hahaha [hahaha@sexyfun.net]

Subject: Snowwhite and the Seven Dwarfs - The REAL story!

Body: Today, Snowwhite was turning 18. The 7 Dwarfs always where very educated and polite with Snowwhite. When they go out work at morning, they promised a *huge* surprise. Snowwhite was anxious. Suddlenly, the door open, and the Seven Dwarfs enter...

Attachment: sexy virgin.scr or joke.exe or midgets.scr or dwarf4you.exe

But this Virus (SubType: Internet worm) does not stop at mere titillation. Hybris even has the capability to send the same message (as above) in different languages depending on what's installed in the computer system.

It first tries to infect the WSOCK32.DLL file in the WINDOWS\SYSTEM directory. (It has other ways and means to infect the file should it fail the first - or even second - time). "The modified WSOCK32.DLL file watches all Internet activity and attempts to mail a copy of the worm, in the form of a .EXE or .SCR file, to any valid e-mail address sent over the Internet connection, whether part of a e-mail message, web page, or newsgroup posting."

W32/Magistr.a@MM

W32/Magistr@MM is a combination of a files infector virus and an e-mail worm. It infects PE type files (.exe) in the Windows directory and subdirectory; and at the same time, through its worm capabilities, it slithers and sends itself to e-mail addresses stored in the Windows address book, Outlook Express mailboxes, etc. "The messages sent by the worm contain varying subject headings, body text, and attachments. The body of the message is derived from the contents of other files on the victim's computer. It may send more than one attachment and may include non .EXE or non-viral files along with an infectious .EXE file."

Moreover, "the viral code is encrypted, polymorphic, and uses anti-debugging techniques to make it difficult to detect. Email addresses have been seen encrypted in infected files. These addresses are believed to represent other users that have also been infected from the same point of origin."

This virus has an even more sneaky variant, the W32/Magistr.b@MM (SubType: File Infector). Other than the original characteristics, it also uses a more complex encryption technique; deletes all .NTZ files on the local machine; terminates the ZoneAlarm firewall user interface process if it is running (not the entire program); creates a SYSTEM.INI [boot]shell value to run itself at startup; uses random file extensions on the executables which it sends (.bat, .com, .exe, .pif); reportedly retrieves email addresses from Eudora mailbox files (.MBX); overwrites the WIN.COM/NTLDR file at times; and sends .GIF files found on the local machine to others along with itself.

W32/Nimda@MM

This virus (SubType: Internet worm) has a high risk assessment. "This worm virus infects using several methods including mass-mailing, network share propagation, the Microsoft Web Folder Transversal vulnerability (also used by W32/CodeBlue), and a Microsoft incorrect MIME Header vulnerability. It also attempts to create network shares, and utilize the backdoor created by the W32/CodeRed.c worm."

Nimda can be triggered by merely viewing an e-mail message in the MS Outlook Express preview pane (but double-clicking the attachment is required to execute the virus using other mail clients). The subject as well as the attachment name in an email message may vary, but the message body is blank. Nimda may even use the icon for an IE HTML document. Users of Microsoft Internet Explorer 5.01 or 5.5 are the ones greatly affected, when the patch SP2 is not installed. WinNT/2K systems cannot be infected from an email message.

Even viewing an infected web page can transmit the virus into your computer. WinNT/2K systems cannot be infected by accessing an infected .ASP, .HTM, or .HTML document.

It does other nasty things, too, like prepending .exe files with the worm code and sending itself to other "victims" by means of e-mail addresses.

W32/SirCam@MM

SirCam is a mass mailing virus (SubType: Email) that sends itself and a user's documents to names found in the Windows address book as well as those in the temporary Internet cached files/ web browser cache.

To avoid detection, it conceals itself in the Recycled Folder where it does the dirty work of replicating itself. It also makes copies of itself in the Windows Systems folder.

W95/MTX.gen@M

W32/MTX@MM is a combination of a Virus, Worm and Backdoor. (It's typed mainly as a virus; SubType: Internet worm). It sends 32 bit PE (.exe) files with deceiving variable filenames as well as modifies .exe and .dll files in the windows folder. It has the capability to block access to some anti-virus sites; and when an attempt to access such sites is made, the user's web browser may crash.

It sends itself via e-mail with a randomly chosen filenames, such as BILL_GATES_PIECE.JPG.pif; I_am_sorry.DOC.pif; Me_nude.AVI.pif; METALLICA_SONG.MP3.pif; zipped_files.EXE; etc.

According to Symantecⁱⁱ, the following are the recent virus alerts:

VBS.VBSWG2.Z@mm

VBS.VBSWG2.Z@mm is an encrypted VBScript worm that sends itself to all recipients in your Microsoft Outlook address book. It arrives as an attachment named Mawanella.vbs.

W32.Badtrans.13312@mm

It is a MAPI worm that replies to all unread mails in your email message folders and drops a backdoor Trojan.

VBS.SST

VBS.SST is a VBS email worm that arrives with an attachment named AnnaKournikova.jpg.vbs. When executed, the worm emails itself to everyone in your address book.

W95.Hybris.gen

W95.Hybris.gen is a worm that spreads as an attachment to outgoing email messages. When the worm is executed, the Wsock32.dll file is modified or replaced. This enables the worm to attach itself to all outbound email.

NOTE: NAV previously detected this worm as Backdoor.Trojan, and then as W32.Hybris.gen.

W32.HLLW.Bymer

W32.HLLW.Bymer is a worm that spreads over shared network drives. It searches for shared folders on the network, and then copies itself to the \Windows\System folder.

NOTE: NAV previously detected this worm as Backdoor.Trojan, and then as Dnet.Dropper.

W32.Prolin.Worm

W32.Prolin.Worm uses Microsoft Outlook to email itself to everyone in the Outlook address book.

Subject: A great Shockwave flash movie.

Message: Check out this new flash movie that I downloaded just now ... It's Great Bye

This worm will rename and then copy all .zip and .jpg files to C:\. It will then delete the original .zip and .jpg files.

W32.Navidad

W32.Navidad is a mass-mailing worm program. The worm replies to all Microsoft Outlook Inbox messages that contain a single attachment. The worm utilizes the existing

email subject line and body, and attaches itself as Navidad.exe. Due to bugs in the code, after being executed, the worm causes your system to stop functioning correctly.

Wscript.KakWorm

Wscript.KakWorm spreads using Microsoft Outlook Express. The worm attaches itself to all outgoing messages using the Signature feature of Outlook Express.

W32.HLLW.Qaz.A

W32.HLLW.Qaz.A can spread over a network and enables a remote user to connect to and control the computer.

W32.FunLove.4099

W32.FunLove.4099. is a virus that replicates under Windows 95/98 and Windows NT. It infects programs that have .exe, .scr, or .ocx extensions. What is notable about this virus is that it uses a new strategy to attack the Windows NT file security system, and it runs as a service on Windows NT systems.

W95.MTX

The W95.MTX virus infects Windows program files, such as Explorer.exe. If this happens, Windows may no longer run. This virus also has the capability of blocking your Internet connection to the Web sites of anti-virus vendors, such as Symantec.

ⁱ <http://vil.nai.com>

ⁱⁱ <http://www.symantec.com>