Summary from Symantec Security Response Newsletter - January/February 2004

Multiple medium-to-high risk worm outbreaks, based on the MyDoom, Netsky, and Beagle worm families, largely dominated the months of January and February. Both the MyDoom and Beagle worms contained back-doors that were the target of reasonably widespread activity soon after their release. The successor to one of last year's most prolific worms was also released. W32.Welchia.B was discovered on February 11, 2004. However, it eventually turned out to be not as nearly virulent as its predecessor.

Also in February, W32.Doomjuice was released, which is similar to Welchia, in that it attempts to delete previously infected hosts. W32.Doomjuice attempts to remove any instances of the W32.MyDoom.A and W32.MyDoom.B worms. It also launches a Denial of Service (DoS) attack against the Microsoft corporate Web site.

The most significant vulnerability released in January was the Multiple Vendor H.323 Protocol Implementation Vulnerabilities. In February, critical vulnerabilities in the Microsoft Windows operating system were announced. Two severe vulnerabilities were reported in the Microsoft Abstract Syntax Notation 1 (ASN.1) handling Library. A DoS exploit was released for one of the ASN.1 vulnerabilities. The exploit designed for >the ASN.1 vulnerability also induced a DoS condition against Microsoft IIS.

A portion of the Microsoft Windows 2000 and NT 4.0 source code was leaked on the Internet, and then freely circulated via various file-sharing networks. Security Professionals speculate that the ultimate impact of the leakage is to assist attackers in locating vulnerabilities and developing exploits that target Windows, due to the implied ease in auditing the source code.

Security News
<http://www.securityfocus.com/"http://www.securityfocus.com/>http://www.securityfocus.com/

Editors Note: Thanks to Symantec fot this extract

Netsky-P on the prowl

By Shawna McAlearney, News Writer
22 Mar 2004 | SearchSecurity.com

Antivirus vendors are warning of a Netsky variant that, among other things, exploits the Microsoft MIME header vulnerability to spread on Windows 95, 98, ME, NT, 2000 and XP systems.

This vulnerability allows the auto execution of e-mail attachments on systems running Internet Explorer 5.01 or 5.5 without Service Pack 2, according to Santa Clara, Calif.-based McAfee AVERT. A patch was issued several years ago.

"The worm appears to be the next in the now well-known 'virus' war between the creators of Netsky and Bagle," said an advisory from Tokyo-based Trend Micro. "Netsky-P … makes use of celebrity names like 'Britney Spears' and 'Eminem' in the files it drops; its message body also contains statements seeming to originate from certain antivirus vendors declaring that 'no virus' has been found. The subject line varies, but includes a number of seeming harmless examples, such as 'Protected Mail Request', 'Mail Authentication."

Netsky-P propagates via e-mail using its own Simple Mail Transfer Protocol (SMTP) engine and also spoofs addresses.

"The virus writers are now increasing the complexity of their creations -- possibly an effect of this ongoing 'war', in an attempt to outdo their opponent," David Kopp, head of Trend Micro's TrendLabs Europe, said in a statement. "We are now seeing the inclusion of payloads and social engineering to a far greater degree. Computer users should remain extremely vigilant as this particularly unsettled time."

Latest Bagle worm both nasty and sneaky

By Edward Hurley, News Writer
18 Mar 2004 | SearchSecurity.com

A new Bagle variant has surfaced using a novel technique to propogate. Rather than attach itself to an e-mail, the worm uses a URL in the message to download the malicious code.

Bagle-Q can also spread as an attachment but the new attack methods makes it a little worrisome. Specifically, it exploits the object tag vulnerability in popup windows in Microsoft Outlook.

Or this Ask the Expert: "What is the most cost-effective way to battle viruses?"
The worm sends out HTML e-mails containing a URL that automatically downloads an .html file, which then drops a Visual Basic script. That script actually downloads the Bagle-Q file via an HTTP request to TCP port 81 on the system that sent the worm. The worm is saved as "directs.exe" in the system folder.

Bagle-Q does some nasty things to systems after infecting them. It terminates a range of security applications including antivirus scanners and personal firewalls. It also makes several copies of itself with enticing names in folders containing "shar" so systems involved with peer-to-peer sharing would download the worm. For example, the worm copies itself as "Adobe Photoshop 9 full.exe," " Matrix 3 Revolution English Subtitles.exe" or "Windows Sourcecode update.doc.exe." The worm also tries to append itself to executable files on infected systems.

The variant also opens a backdoor on infected systems. It listens on TCP port 2556 for instructions from the attacker, who has full control over the compromised system, according to an advisory from F-Secure.

To spread, the worm searches systems for e-mail addresses in a wide range of files. It then sends out the messages containing the tainted link using its own SMTP engine. The worm spoofs the From address on the messages so it appears to come from the recipients' domain. It uses a variety of official sounding usernames such as "management," "administration," or "staff," according to Symantec.

Besides updating antivirus signature files, users should also consider blocking TCP port 81, both inbound and outbound, suggested Sophos. Preventing inbound traffic would mean systems wouldn't be able to spread the worm any further. Blocking outbound traffic prevents systems from downloading the Bagle-Q file in the first place. In either case, blocking such traffic won't likely affect any network services, Sophos said.

The Bagle family of worms has been quite prolific this year. The first one appeared in January, and since then multiple variants of appeared.

W32.Netsky.N@mm
Category2
Discovered on: March 16, 2004
Last Updated on: March 16, 2004 03:05:44 PM

W32.Netsky.N@mm is a mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives.
The "sender" of the email is spoofed, and its subject, message body, and attachment vary. The attachment has a .pif extension.

This threat is compressed with tELock.

Note: The worm has an MD5 hash value of 0xDD4D58534FA472E4735A532D15A6547F.

Also Known As: W32/Netsky.n@MM [McAfee], I-Worm.NetSky.o [Kaspersky]
Variants: W32.Netsky.gen@mm
Type: Worm

Infection Length: 33,792 bytes
Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
Systems Not Affected: DOS, Linux, Macintosh, OS/2, UNIX

protection
Virus Definitions (Intelligent Updater) *

March 17, 2004
Virus Definitions (LiveUpdate™) **

March 17, 2004

*

Intelligent Updater definitions are released daily, but require manual download and installation.
Click here to download manually.

**

LiveUpdate virus definitions are usually released every Wednesday.
Click here for instructions on using LiveUpdate.

threat assessment

Wild:

* Number of infections: 0 - 49
* Number of sites: 0 - 2
* Geographical distribution: Low
* Threat containment: Easy

* Removal: Easy

Threat Metrics
Low Low High

Wild:
Low

Damage:
Low

Distribution:
High

Damage

* Payload Trigger: n/a
* Payload: n/a

o Large scale e-mailing: Sends itself to the email addresses retrieved from the file system.
    o Deletes files: n/a
    o Modifies files: n/a
    o Degrades performance: n/a
    o Causes system instability: n/a

o Releases confidential info: n/a
o Compromises security settings: n/a

Distribution

* Subject of email: Varies.
* Name of attachment: Varies with a .zip, .pif, .exe, or .scr extension.
* Size of attachment: 34,054 bytes
* Time stamp of attachment: n/a
* Ports: n/a
* Shared drives: n/a
* Target of infection: n/a

technical details

When W32.Netsky.N@mm runs, it does the following:

1. Creates a mutex named "NetDy_Mutex_Psycho". This mutex allows only one instance of the worm to execute.

2. Copies itself as %Windir%\VisualGuard.exe.

3. Creates the following files:
   * %Windir%\base64.tmp (46,308 bytes): MIME-encoded version of the executable
   * %Windir%\zip1.tmp (46,478 bytes): MIME-encoded version of worm in zip archive
   * %Windir%\zip2.tmp (46,490 bytes): MIME-encoded version of worm in zip archive
   * %Windir%\zip3.tmp (46,464 bytes): MIME-encoded version of worm in zip archive
   * %Windir%\zip4.tmp (46,646 bytes): MIME-encoded version of worm in zip archive
   * %Windir%\zip5.tmp (46,658 bytes): MIME-encoded version of worm in zip archive
   * %Windir%\zip6.tmp (46,670 bytes): MIME-encoded version of worm in zip archive
   * %Windir%\zipped.tmp (34,054 bytes): Worm in zip archive

4. Adds the value:

   "NetDy"="%Windir%\VisualGuard.exe"

   to the registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

   so that the worm runs when you start Windows.

5. Deletes the values:

   Explorer
   system.
   msgsvr32
au.exe
   service
   DELETE ME
   d3dupdate.exe
   OLE
   Sentry
   gouday.exe
   rate.exe

Taskmon
Windows Services Host
sysmon.exe
srate.exe
ssate.exe

from the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

6. Deletes the value:

InProcServer32

from the registry key:

HKEY_CLASSES_ROOT\CLSID\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}

7. Deletes the following subkeys:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Explorer\PINF
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WksPatch

8. Retrieves email addresses from the files with these extensions:
   * .adb
   * .asp
   * .cgi
   * .dbx
   * .dhtm
   * .doc
   * .eml
   * .htm
   * .html
   * .jsp
   * .msg
   * .oft
   * .php
   * .pl
   * .rtf
   * .sht
   * .shtm
   * .tbb
   * .txt
   * .uin
   * .vbs
   * .wab
   * .wsh
   * .xml

Note: Due to a bug in the code, the worm will search a file for email addresses if the extension is a sub-string of one of the aforementioned extensions.

For example, the worm will scan the files with the .txt, .tx, and .t extensions.

9. Uses its own SMTP engine to send itself to the email addresses it finds. The worm uses the local DNS serv

er (retrieved using an API call), if available, to perform an MX lookup for the recipient address.

10. The email has the following characteristics:

From: <Spoofed>

Subject: The subject line is composed of multiple parts.

The first part may be one of the following:
* Re:
* Re: Re:

11. The second part may be one of the following:
* my
* your
* [blank]

And the third part may be one of the following:
o application
o approved
o approved
o bill
o corrected
o data
o details
o document
o document_all
o excel document
o file
o hello
o here
o hi
o important
o important
o improved
o information
o letter
o message
o patched
o product
o read it immediately
o screensaver
o text
o thanks!
o website
o word document

Message: The message is one of the following:
o Authentication required.
o I have attached your document.
o I have received your document. The corrected document is attached.
o Please confirm the document.
o Please read the attached file.
o Please read the document.

o Please read the important document.
o Please see the attached file for details.
o Requested file.
o See the file.
o Your details.
o Your document is attached to this mail.
o Your document is attached.
o Your document.
o Your file is attached.

Followed by:

(attachment_name) : No virus found
Powered by the new Norton OnlineScan
Get protected: www.symantec.com

Attachment: The attachment is one of the following with a .zip, .pif, .exe, or .scr extension:

o application_%s
o approved_%s
o bill_%s
o data_%s
o details_%s
o document_%s
o document_all_%s
o excel document_%s
o file_%s
o important_%s
o information_%s
o letter_%s
o message_%s
o product_%s
o screensaver_%s
o text_%s
o website_%s
o word document_%s

where %s is the portion of the "To" address before the "@".

recommendations

Symantec Security Response encourages all users and administrators to adhere to the following basic security "best practices":

* Turn off and remove unneeded services. By default, many operating systems install auxiliary services that are not critical, such as an FTP server, telnet, and a Web server. These services are avenues of attack. If they are removed, blended threats have less avenues of attack and you have fewer services to maintain through patch updates.
* If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
* Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
* Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
* Configure your email server to block or remove email that contains file attachments that are commonly

used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.
* Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.
* Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

removal instructions

The following instructions pertain to all current and recent Symantec antivirus products, including the Symantec AntiVirus and Norton AntiVirus product lines.

1. Disable System Restore (Windows Me/XP).
2. Update the virus definitions.
3. Run a full system scan and delete all the files detected as W32.Netsky.N@mm.
4. Delete the value that was added to the registry.

For specific details on each of these steps, read the following instructions.

1. Disabling System Restore (Windows Me/XP)
If you are running Windows Me or Windows XP, we recommend that you temporarily turn off System Restore. Windows Me/XP uses this feature, which is enabled by default, to restore the files on your computer in case they become damaged. If a virus, worm, or Trojan infects a computer, System Restore may back up the virus, worm, or Trojan on the computer.

Windows prevents outside programs, including antivirus programs, from modifying System Restore. Therefore, antivirus programs or tools cannot remove threats in the System Restore folder. As a result, System Restore has the potential of restoring an infected file on your computer, even after you have cleaned the infected files from all the other locations.

Also, a virus scan may detect a threat in the System Restore folder even though you have removed the threat.

For instructions on how to turn off System Restore, read your Windows documentation, or one of the following articles:

NOTE - Removal Tools for the Netsky and other current viruses and worms can be downloaded from this URL - <http://securityresponse.symantec.com/>