Global Information Assurance Certification Paper

Jeffrey Cuthbertson
November 22, 2000

Kicking off the holiday season with something special…
Introducing the NAVIDAD virus

This paper is intended as an overview of a new virus that is spreading rapidly around the world. With the holidays approaching, and the name of the offending attachment suggesting all the warmth and bonhomie of the Yule season, it is likely that diffusion of this virus may accelerate.

Known variously as TROJ_NAVIDAD.A, W32/Navidad@M, w32.Navidad, I-Worm.Navidad , W32/Watchit and Win32/Navidad.Worm, this new virus (11/03/2000) purported to have originated in South America, is considered to be in the wild, and spreading rapidly. The virus will make changes to the system registry and can render the infected system inoperable.

According to the Trend Micro "Trend World Virus Tracking Center" (http://wtc.trendmicro.com/wtc/) the TROJ_NAVIDAD.A virus is currently the 4th ranking worldwide, based on computers infected; it is not on the list for infected files.

Navidad is not a boot virus like ILOVEYOU, it does not pose a security threat or publish confidential information like PrettyPark.Worm, and unlike the 29 versions of VBS.Loveletter reported by Symantec's research center (SARC), http://www.symantec.com/avcenter/venc/data/vbs.loveletter.a.html , it does not have an IRC component to aid in its replication, nor does it overwrite files. Unlike QAZ there is no backdoor process, and no network awareness. Essentially, Navidad is tamer, and simpler to fix than these.

You might be at your computer thinking about your Christmas shopping list and trolling for special deals. Outlook indicates that you have a new mail message, so you check and see a message from someone you know. The attachment, NAVIDAD.EXE, seems like it might be a holiday greeting, so you click on it.

This Trojan cum Internet worm is able to spread exponentially by use of Outlook. Once the navidad.exe file is executed, you will see an Error message on your screen, containing only the characters UI. When you acknowledge the error message, by clicking on the 'OK' button, the virus will activate and the worm will save a copy of the Trojan "winsvrc.vxd" to the

Windows\System directory and create registry entries, as noted below. Using Microsoft MAPI, the virus will open your inbox (Outlook or Outlook Express), and reply to all messages after attaching the Navidad.exe file. The subject line will be left intact, with the exception that it may, or may not add RE: to the subject line - (I have read ambiguous and contradicting descriptions of this.) Thus does the Trojan propagate itself, annoying your correspondents, and remanding you to an ignominious, and sadly appropriate membership in the Fraternal Order of "emailers non grata".

Following the mass mailing an icon (graphic of an eye) will appear in your systray by the clock. McAfee provided the following (*italicized*) information on some of the symptoms.

"When the "eye" icon is clicked, a button appears. reading, "Nunca presionar este boton". Translated this means, never press this button. When the button is pressed, a messages box is displayed entitled, "Feliz Navidad", which reads "Lamentablemente cayo en la tentacion y perdio su computadora". Translated this reads, Merry Christmas, Unfortunately you've given in to temptation and lose your computer."
Interpretation: Do Not Click the Button!

The following (*italicized*) is a description of registry changes occurring after execution of the Navidad.exe attachment. It is also from McAfee's website: http://vil.nai.com/vil/virusSummary.asp?virus_k=98881

HKEY_CURRENT_USER\SOFTWARE\Navidad

*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ Win32BaseServiceMOD=C:\WINDOWS\SYSTEM**winsvrc.exe***

*HKEY_CLASSES_ROOT\exefile\shell\open\command\ (default)=C:\WINDOWS\SYSTEM**winsvrc.exe "%1" %****

*HKEY_LOCAL MACHINE\Software\CLASSES\exefile\shell\open\command\ (default)=C:\WINDOWS\SYSTEM**winsvrc.exe "%1" %***
In the last 2 entries above, the previous value was
*"%1" %**

The misnaming of the registry entry filename "winsrvc.exe" vs. "winsrvc.vxd" is the bug in the code that will cause your system to issue an error message each time that a .exe file is executed. This has the undesired effect of making your system nearly inoperable.

IMPORTANT - Please read before proceeding to manual correction
If you are not comfortable working with the registry, don't do it. You may escalate a nuisance into a non-recoverable problem. If you decide to proceed, please create, or update an emergency repair disk. You can rename rdisk.exe to rdisk.com and run it from the DOS prompt. If you would prefer, you can use scripts that are available from various companies to correct the registry entries. They can be reached from this link.

The (abbreviated) fix is as follows:
The following (*italicized*) description of registry changes is also from McAfee:
http://vil.nai.com/vil/virusSummary.asp?virus_k=98881

This problem can be recovered by opening an MS-DOS prompt and going into the Windows directory and then copying REGEDIT.EXE as REGEDIT.COM. You can then run REGEDIT from the START menu and browse to the registry path to remove the invalid entry mentioned above. This worm can be terminated on a system - when Navidad is running, click on the eye in the system tray. When the dialog box with the big button labeled don't press me (sic) appears, press the little close window button in the top right corner (marked X)

The following are detailed instructions for the manual removal of the virus from your system - Win95/98 or NT/2000. This information comes from Symantec's AntiVirus Research Center, written by Eric Chien.
http://www.symantec.com/avcenter/venc/data/w32.navidad.html

To remove W32.Navidad (on a Windows 95/98 system):

1. *On the Windows taskbar, click **Start** > **Programs** > **MS-DOS Prompt**. The command prompt will display the current directory, which should be the Windows directory. In most cases that will be displayed as:*
   C:\WINDOWS>
2. *Type **ren REGEDIT.EXE REGEDIT.COM**.*
3. *Press **Enter**.*
4. *Type **REGEDIT**.*
5. *Press **Enter**.*
6. *Modify the following Registry value:*
   HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command
   and change
   *"C:\WINDOWS\SYSTEM\winsvrc.vxd "%1" %**

to
*"%1" %**
For clarity, these seven characters are the following: double quote, percent sign, the numeral one, double quote, space, percent sign, and asterisk. Don't forget the space.

7. *Delete the registry key:*
   HKEY_USERS\.DEFAULT\Software\Navidad
8. *Restart your computer.*
9. *Using Windows Explorer, delete the \WINDOWS\SYSTEM\winsvrc.vxd file.*

To remove W32.Navidad (on a Windows NT / Windows 2000 system):

1. *On your Windows Desktop, double-click on your **My Computer** icon.*
2. *Press **CTRL-F**. A Find: All Files window should pop up. This will allow you to search for a specific file.*
3. *In the Named: field, type **REGEDIT.EXE**.*
4. *After it finds this file successfully, right-click on the filename REGEDIT.EXE. This will pop up a menu. Select **Rename**.*
5. *Type: **REGEDIT.COM**. This should rename the file to REGEDIT.COM.*
6. *Double-click on this program REGEDIT.COM.*
7. *Modify the following Registry value:*
   HKEY_CLASSES_ROOT\exefile\shell
   open\command
   and change
   *"C:\WINNT\SYSTEM32\winsvrc.vxd "%1" %**
   to
   *"%1" %**
   For clarity, these seven characters are the following: double quote, percent sign, the numeral one, double quote, space, percent sign, and asterisk. Don't forget the space.
8. *Delete the registry key:*
   HKEY_CURRENT_USER\Software\Navidad
9. *Restart your computer.*

Using Windows Explorer, delete the \WINNT\SYSTEM32\winsvrc.vxd file.

After making these manual adjustments, your system should be back to normal. If you have a problem either you have not made all of the corrections, or you have done one incorrectly, verify your changes, and be sure that you have removed the winsrvc.vxd file.

Scripts to remove the virus:

Symantec
http://www.symantec.com/avcenter/venc/data/w32.navidad.fix.html
This tool repairs damage done by the W32.Navidad worm.

TrendMicro
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_NAVIDAD.A
Use this tool, FIX NAVI, to automatically clean your system registry and delete the dropped file, WINSVRC.VXD. Restart the computer.

McAfee
http://download.nai.com/products/MCAFEE-AVERT/stand_alone/undo.zip
To repair the registry manually via a registry script file, extract the UNDO.REG file and copy to the STARTUP folder of the affected system. Reboot the affected system.

What can be, or is being done to protect computer systems from malicious code? There is an evolution in virus research. Virus fingerprinting has been the standard, but viruses are becoming more sophisticated. Many of them are polymorphic, they mutate as they replicate, changing their fingerprint. Heuristics is one area of new research. A heuristic approach will try to guess what changes may occur and relate them to the documented viruses. One of the problems with this approach now seems to be an occurrence of too many "false-positives."

Some basic tips:
1. NEVER open an email attachment unless you know exactly what it is.

2. Use virus detection software - and UPDATE it regularly - at least once a week. Since Navidad was noticed on November 3rd, McAfee has listed 12, count'em, 12 new viruses.

3. Make use of some of the resources that I have included at the end of this document to learn more about the problems, tools and solutions to viruses.

4. Make sure that your systems are up to date with patches and hot fixes. If you take some time to harden your systems, you will be rewarded with more free time.

5. Commit some of the time saved in Tip Number 4, to doing some research. I have appended a number of links to get you started. The best way to learn more is to visit the following links and browse their sites. I'll bet that you can find everything you ever wanted to know (or never thought you'd need to

know) about viruses and related issues.

Sources - Informational Links

The following article, Antivirus software covers the perimeter, from Federal Computer Week gives a nice overview of different aspects of the problem, as well as providing information on a number of vendors, and their products. Also, available from Trend Micro, is a Virus Primer and a Safe Computing Guide.

Vendor Links
http://www.antivirus.com/vinfo/
http://www.symantec.com/avcenter/
http://vil.nai.com/VIL/newly-discovered-viruses.asp
http://www.securityportal.com/research/research.virus.html
http://www.ibm.com/link/www.av.ibm.com.html
http://www.commandcom.com/
http://www.icsa.net/html/communities/antivirus/index.shtml
http://www.icsa.net/html/hypeorhot/index.shtml
http://www.avp.ch/

Non-Profit Organization Links
http://www.sans.org/newlook/home.htm
http://www.cert.org/other_sources/viruses.html
http://www.wildlist.org/
http://www.marktplatz.ch/metro/caro.htm
http://www.eicar.org/
http://www.virusbtn.com/index.html
http://www.ualberta.ca/CNS/VIRUS/virusglos.htm

Terms: Credit for definitions is appended to each.

Back Door
This is a situation where an interloper places files and code on a system that will allow unauthorized, stealthful remote control of the system. This is a very serious breach and difficult to both detect, and correct.

Boot Virus
Boot sector viruses infect the boot sector or partition table of a disk. Computer systems are most likely to be attacked by boot sector viruses

when you boot the system with an infected disk from the floppy drive - the boot attempt does not have to be successful for the virus to infect the hard drive. Also, there are a few viruses that can infect the boot sector from executable programs- these are known as multi-partite viruses and they are relatively rare. Once the system is infected, the boot sector virus will attempt to infect every disk that is accessed by that computer. In general, boot sector viruses can be successfully removed.
http://www.antivirus.com/vinfo/virusencyclo/glossary.asp

Heuristic
: involving or serving as an aid to learning, discovery, or problem-solving by experimental and especially trial-and-error methods <*heuristic* techniques> <a *heuristic* assumption>; *also* **:** of or relating to exploratory problem-solving techniques that utilize self-educating techniques (as the evaluation of feedback) to improve performance <a *heuristic* computer program>
Credit: Merriam-Webster's Collegiate® Dictionary

In The Wild
A virus is referred to as "in the wild" if is has been verified by groups that track virus infections to have caused an infection outside a laboratory situation. A virus that has never been seen in a real world situation is not in the wild, and sometimes referred to as, in the zoo.
http://www.ualberta.ca/CNS/VIRUS/virusglos.htm

Polymorphic
Ability to mutate by changing code segments to look different from one infection to another. This type of virus is a challenge for ant-virus detection methods. http://www.ualberta.ca/CNS/VIRUS/virusglos.htm

Trojan
A Trojan horse is a program that performs some unexpected or unauthorized, usually malicious, actions, such as displaying messages, erasing files or formatting a disk. A Trojan horse doesn't infect other host files, thus cleaning is not necessary. To get rid of a Trojan, simply delete the program. http://www.antivirus.com/vinfo/virusencyclo/glossary.asp

VxD
This filetype is a Windows program, which can run in the background. A scanner implemented as a VxD has all the advantages of a DOS TSR but can have additional advantages: for instance, a good VxD will scan continuously.
http://www.ualberta.ca/CNS/VIRUS/virusglos.htm

Worm

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or email attachments. To get rid of a worm you just need to delete the program. http://www.antivirus.com/vinfo/virusencyclo/glossary.asp