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
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

David Cullison
Nov. 20, 2000

Merry Christmas - The NAVIDAD Virus

Ah, the holiday season - peace, love, and good will to men. Our Spanish-speaking friends from either South America or Cuba are suspected of sending out an early Christmas present to the Internet. [(2)] I'm a member of the firewall team at a large government installation and late on November 3, 2000, our e-mail team made us aware of the latest virus threat - the NAVIDAD virus. Fortunately, we have been blocking all .EXE e-mail attachments at the firewall for some time. Unfortunately, we still have to be alert for the inevitable infection via POP3, web based e-mail clients, and PCs with modems. No matter how many alerts you send to users warning against the dangers of opening unexpected attachments (especially executables), some just can't seem to resist the temptation. We now know that we were not the only ones working late. According to the Associated Press, at least 10 Fortune 500 companies were infected along with hundreds of others. [(3)] As I will describe below, NAVIDAD is flawed and fairly benign, but still able to spread fast enough that McAfee has upgraded its rating to "medium" and the U.S. Army had just raised its risk assessment to "high" because it has experienced several infections.[(7)]

How It Works

NAVIDAD targets Microsoft Windows 95/98/NT/2000 platforms and propagates by scanning the user's Outlook inbox for e-mail messages containing a single attachment. It then uses the Messaging Application Programming Interface (MAPI) to reply to those messages, using the original subject line and message body, adding the NAVIDAD.EXE file as an attachment.[(2)] This virus uses some of the "Social Engineering" techniques discussed in the GSEC course. By arriving at the victim's inbox as a reply, it immediately fools the user into trusting the sender. Nobody suspects his or her friends or co-workers would send anything dangerous or destructive; and with an attachment named NAVIDAD.EXE, it can only be sent in the time after Halloween and before Christmas. Any other time, an attachment with that name would seem suspicious. The combination of a seemingly trustworthy name on the "From:" line, a familiar subject, and good timing greatly increases the probability that the attachment will be opened and executed.

When a user runs the NAVIDAD.EXE attachment, an error message box is displayed containing the text "UI", and a blue eye icon is placed on the taskbar. Placing the cursor over the eye icon displays "Lo estamos mirando," in Spanish, which means "We are watching it" in English. Clicking on the eye icon returns the message "Nunca presionar este boton" in Spanish, which translates to "Never press this button." At this point the user has two choices, either click the button or close the window. If the user clicks the button, a message box is returned containing the following text: [(4)]

Title: Feliz Navidad
Message: Lamentablemente cayo en la tentacion y perdio su computaroda

Translated to English, this message reads:

Title: Merry Christmas
Message: Unfortunately, you have fallen to temptation and have lost you computer

© SANS Institute 2000 - 2005

Author retains full rights.

If the user closes the dialog box by clicking on the X instead, a message box is returned containing the following text:

Title: Feliz Navidad
Message: buena eleccion…

Translated to English, this message reads:

Title: Merry Christmas
Message: good choice

In either case, the virus creates new or modifies existing registry entries and copies itself to a file named WINSVRC.VXD in the system subdirectory below the Windows root. By default, this is C:\WINDOWS\SYSTEM on Windows 95/98 computers and C:\WINNT\SYSTEM32 on Windows NT and Windows 2000 machines. It then adds two new and modifies one existing registry as described below:

Windows 95/98: *(4)*

1) *Added*: HKEY_USERS\.Default\Software\Navidad

2) *Added*: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Value name: Win32BaseServiceMOD Value data: C:\Windows\System\Winsvrc.exe

3) *Modified*: HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command
Value name: (Default) Value data: "%1"%*
changed to:
Value name: (Default) Value data: C:\Windows\System\Winsvrc.exe"%1"%*

Windows NT/2000: *(4)*

1) *Added*: HKEY_CURRENT_USER\Software\Navidad

2) *Added*: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Value name: Win32BaseServiceMOD Value data: C:\Winnt\System32\Winsvrc.exe

3) *Modified*: HKEY_CLASSES_ROOT\exefile\shell\open\command
Value name: (Default) Value data: "%1"%*
changed to:
Value name: (Default) Value data: C:\Winnt\System32\winsvrc.exe "%1"%*

The 1st addition was supposed to be used to determine whether or not the system was already infected. However, analysis of the NAVIDAD code revealed an error in the second modification that rendered the first one useless. Ironically, the error is what holds the most cause for concern to the user. The combination of the 2nd and 3rd entries is supposed to cause the worm to run every time any executable program is launched. However, because the file extension on the WINSVRC.VXD file does not match the one in the registry entry (.EXE), WINSVRC.VXD

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

never executes. Consequently, after a computer becomes infected, an error dialog box is displayed when the user attempts to run any .EXE file. [1] The user is prompted for the location of the WINSVRC.EXE file when, if the code had been error-free, the system should have quietly launched the virus again. The end result is that no executable programs can be launched, which may cause problems if the system is rebooted. [5] Even without the error, NAVIDAD doesn't do any real damage to its victims. The only real danger is that it could potentially result in a Denial of Service (DoS) situation if permitted to spread rapidly. April Goostree, an anti-virus researcher at McAfee, warns "the attachment could bring down a mail system if enough programs are run and are sending out response emails to all the addresses within the system."[6]

How to Remove It

McAfee, Symantec, F-Secure, and others now have fixes for NAVIDAD. However, if you can't wait, or can't even get your computer to the point where you can download an automated fix, it can be removed manually. Remember that once infected, you can no longer launch .EXE files. In order to restore the registry to its original state, you must first rename REGEDIT.EXE to REGEDIT.COM. Once you're able to run REGEDIT, you can restore or remove the registry entries listed above, remove the NAVIDAD.VXD file, and restart your computer. A step-by-step manual removal process is available from Symantec at http://www.sarc.com/avcenter/venc/data/w32.navidad.html. [5]

Is it really a Virus?

While researching NAVIDAD, I quickly realized that categorizing this type of malicious code is not an exact science. The general press seems to regard any incident of this type as a "virus." For example, the Associated Press ran an article with the headline "Computer Virus Strikes 10 Companies." [6] McAfee labels it as a virus with a sub-type of "internet worm." [2] Trend Micro's web page has a category called "Virus Type" under which NAVIDAD is listed as a Trojan. [4] All of this has led me to the conclusion that the term "virus" can be considered an umbrella term as well as a specific category of malware. Well, is it a virus, a worm, or a trojan? After reading the definitions for each of these terms from McAfee, Trend Micro, Symantec, and the GSEC courseware, I have come to the conclusion that there is a valid argument for each with respect to NAVIDAD.

On page 3 of the GSEC "Malicious Software" module, it states that "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. If the code requires the user to open an e-mail or load a screen saver or take some other action, then it is called a virus." [8] The same point is made on page 16 of the module during an analysis of the ILOVEYOU virus. Using that measurement, NAVIDAD certainly appears to be a virus - the user must run the attachment to activate the code. However, McAfee lists it as a worm. Using the GSEC course definition of a worm, that could work also, because once activated, it is able to spread from one machine to potentially many others over the network without the user's assistance or knowledge. Trend Micro's "Trojan" assessment also has merit because trojans are defined as "programs with an intended action that is not documented or revealed." [8] NAVIDAD fits neatly there, too, because the user surely does not expect that

© SANS Institute 2000 - 2005 Author retains full rights.

running the attachment will cause his or her inbox to be scanned or that registry entries will be modified. However, based on the stated definitions, I'll use the approach recommended when taking the Microsoft certification exams - when in doubt, give the Microsoft answer. Therefore, according to the GSEC definition, this thing is a virus first because it can't do anything until the user activates it.

Summary

While it turns out that NAVIDAD is relatively harmless, it is interesting on at least three levels. First, it highlights how difficult it is to categorize and define a particular piece of malware as a virus, worm, or trojan. In the end they're just terms anyway, and the important thing is to identify the problem and remove it, no matter what it's called. Second, as a SANS GIAC student, NAVIDAD is interesting because of its "Social Engineering" aspects. It relies on its ability to exploit human curiosity and trust. Finally, NAVIDAD serves to remind us how diligent all users must be in protecting their computers and data. Undoubtedly, a variant with a different file extension, better code, and a little more bite will be released very soon. It is vitally important that all users install anti-virus software and keep it up to date. Additionally, all other available tools such as firewalls, content scanners, and file encryption should be used when possible. The key is awareness. The sooner you know the threat, the sooner you can prepare. Everyone should subscribe to a mailing list such as that provided by the CERT Coordination Center at www.cert.org or at least scan the CERT Advisories page frequently. As the programs, protocols, and networks we rely on every day become more and more powerful and sophisticated, so do the viruses, worms, and trojans that attack them.

© SANS Institute 2000 - 2005 Author retains full rights.

References

1. CERT Coordination Center. "CERT/CC Current Activity" 16 November 2000.
URL: http://www.cert.org/current/current_activity.html#virus
(November 16, 2000).

2. McAfee. "AVERT Virus Profile." 16 November 2000.
URL: http://vil.nai.com/vil/dispvirus.asp?virus_k=98881
(November 17, 2000).

3. Hopper, D. Ian. "Computer Virus Strikes 10 Companies." 11 November 2000.
URL: http://dailynews.yahoo.com/htx/ap/20001111/us/navidad_virus_2.html
(November 17, 2000).

4. Trend Micro. "TROJ_NAVIDAD.A." 11 November 2000.
URL: htttp://www.antivirus.com/vinfo/virusencyclo/default2.asp
(November 16, 2000).

5. Chien, Eric. "W32.Navidad." 11 November 2000.
URL: http://www.sarc.com/avcenter/venc/data/w32.navidad.html
(November 16, 2000).

6. Luening, Erich. "Christmas virus causes mild clamor on the desktop." 10 November 2000.
URL: http://news.cnet.com/news/0-1007-200-3627220.html (November 15, 2000).

7. "Navidad, Hybris viruses on the loose." Lubbock Avalanche-Journal. 16 November 2000.
URL: http://www.lubbockonline.com/low_res/stories/111600/sci_111600076.shtml
(November 19, 2000).

8. Kerby, Fred. "Malicious Software." SANS GIAC Level One. 25 September 2000.

© SANS Institute 2000 - 2005 Author retains full rights.