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

The "W32.Navidad@M" Worm
Michael Stan
December 1, 2000

Malware such as viruses and worms are becoming more prevalent, more sophisticated and multiple variants spun off of the original bad idea. The purpose of this paper is to discuss the mass mailing worm program known both as the W32.Navidad@M and its variants. Although this malware is often referred to as a virus it is actually a worm. A worm is a destructive program that is self - contained, and is able to spread copies or segments to other systems with out direct action by the user. My research as of Dec 1 2000, shows 13 versions of this worm Including : Emanuel, Emmanuel, I-Worm.Navidad, Navidad, TROJ_EMMANUEL, TROJ_NAVIDAD.A, W32.Navidad, W32.Navidad.16896, W32/Navidad-B, W32/Navidad.e@M, W32/Navidad.gen@M, W32.Wachit and Win32/Navidad.Worm.`

Overview

This malware has originated from South America, and many of the messages indicating you are infected will be in Spanish. This malware has been classified differently in each site I visited. At Trend Microsystem's site a Low Risk was indicated, where as on McAfee,s site, a medium risk was granted.

Symantec's web page also had a different rating but gave more detail for threat assessment and are as follows:

In the Wild the threat is High. The term min the wild refers to " number of independent sites infected, number of computers infected, the geographic distribution of infection, the ability of current technology to combat the threat and the complexity of the virus." The Damage assessment is High and refers to " the amount of harm that a given threat might inflict. This measurement includes triggered events, clogging email servers, deleting or modifying files, releasing confidential information, performance degradation, errors in the virus code, compromising security settings, and ease by which the damage might be fixed. "

The Distribution threat is medium, This assessment refers to " how quickly the threat is able to spread itself."

The W32Navidad@m propagates itself through email. Specifically Navidad targets users of Microsoft Outlook uses MAPI. MAPI according to Newtons's Telecom dictionary is

> " a set of API functions and an OLE interface that lets messaging clients such as Microsoft exchange interact with various messaging service providers."

As well affecting the users machine, this is a mass mailing problem that could easily turn into a denial of service issue as many mailboxes will be addressed and causing undue stress on various networks.

The victim will be infected after opening an NAVIDAD.EXE email attachment. (Does this sound familiar? It is apparently easy to get users to open unknown attachments.) Once the attachment is opened and executed registry entries are added and changed, then Navidad reads the users Outlook address book and any MAPI clients that are installed. Navidad then replicates itself and sends itself out as email replies to all addresses read.

An important point to remember is that there is an error in the executable program. The worm can be terminated when it is running. According to McAfee " When the dialog box with the Big Button label don't press me (sic) appears, press the little close window button in the top right corner (marked x). Another message box pops up, pressing OK on the message box makes the worm exit- the Blue eye in the message tray and the program terminates."

The changes to the victims registry are as follows:

Windows 95 or 98

The worm adds the following registry key:

> HKEY_USERS\.DEFAULT\Software\Navidad

Next, the virus adds the following registry key:

> HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

with the value:

© SANS Institute 2000 - 2005 Author retains full rights.

Win32BaseServiceMOD=\Windows\System\Winsvrc.exe

The worm copies itself into your Windows system directory as WINSVRC.VXD. Due to the difference in file name, the virus does not execute properly at startup.

After the file copy the virus modifies the following registry keys:

HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\exefile\shell\open\command

HKEY_CLASSES_ROOT\exefile\shell\open\command

to equal:

\Windows\System\winsvrc.exe "%1" %*"

Windows NT or Windows 2000

The worm adds the following registry key:

HKEY_CURRENT_USER\Software\Navidad

This key was supposed to be used to see if the computer was already infected. However, due to bugs in the code, the registry key is not utilized.

Next the virus adds the following registry key:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

with the value:

Win32BaseServiceMOD=\Winnt\System32\Winsvrc.exe

The worm copies itself into your Windows system directory as WINSVRC.VXD. Due to the difference in file name, the virus does not execute properly at startup.

After the file copy the worm changes:

HKEY_LOCAL_MACHINE\SOFTWARE\CLASSES\exefile\shell\open\command

HKEY_CLASSES_ROOT\exefile\shell\open\command

to equal:

\Winnt\System32\winsvrc.exe "%1" %*"

As indicated earlier the filename has a mistake. You will be prompted for the location of WINSVRC.EXE the resulting effects will be that program files will not be able to be executed, instability in the system and problems rebooting

How do you know you have been infected?

The worm places a Blue Eye Icon in the system tray. When you place a cursor on this Icon or click it The following messages could appear:

"Lo estamos Mirado" translation "we are watching it"

"Nunca Presionar este boton" translation "never press this button"

" Lamentablemente cayo en la tentaxcion y perdio su computadora" translation " Merry Christmas, Unfortunately you've given in to temptation and lose your computer."

Also you will have problems running executable files and difficulty rebooting your system.

Eradication

© SANS Institute 2000 - 2005 Author retains full rights.

Because the worm has change registry entries eradication is not a simple process.

As mentioned earlier you can actually terminate the program if the Navidad attachment is running.

There are 2 options for manual removal:

A1) Identify and note the files associated with this worm as detected by the scanner.

A2) Download the UNDO.REG file from Mcafee.com, and open it.

A3) Click START|RUN, type REGEDIT and hit ENTER.

A4) Remove any keys that run the main worm under

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\Run\

A5) Exit the Registry

A6) Restart the system

A7) Delete the file(s) associated with this worm

Alternative Manual Instructions

B1) Identify and note the files associated with this worm as detected by the scanner.

B2) Click START|RUN, type

COMMAND /C COPY %WINDIR%\REGEDIT.EXE %WINDIR%\REGEDIT.COM

and hit ENTER

B3) Click START|RUN, type REGEDIT.COM and hit ENTER

B4) Remove references to the trojan from these keys of the registry

HKEY_CLASSES_ROOT\exefile\shell\open\command\

HKEY_LOCAL MACHINE\Software\CLASSES\exefile\shell\open\command

They should contain only the value not including brackets
["%1" %*].

B5) Remove any keys that run the main worm under

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\Run\

B6) Exit the Registry

B7) Restart the system

B8) Delete the worm program(s). If all is well the files should be deleted OK. If you get an error message saying that windows is unable to delete the file because it is in use, then you have made an error in the above procedure and should repeat the process.

Security

Rule Number 1 DO NOT open email attachment you are unfamiliar with especially .exe and .vbs attachments.

Rule Number 2 keep your virus definitions up to date. New malware and new variants existing malware versions are being produced at alarming rates. As a user you can never be 100% prepared, but you can have a plan to be as current as the industry will allow.

© SANS Institute 2000 - 2005 Author retains full rights.

References

1. Symantec. " W32/Navidad@M" 3 November 2000. URL: http://vil.mcafee.com/dispVirus.asp?virus_k=98881& (29 November 2000)

2. [techtips] INITIAL NOTIFICATION W32.Navidad VIRUS acert <majordom@shiloh.liwa.belvoir.army.mil>

3. ICSA Labs " W32/Navidad-M " 10-November 2000 http://www.icsa.net/html/hypeorhot/navidad.shtml (29 November 2000)

4. ZDNet " Avoiding the Navidad Worm" http://www.zdnet.com/zdhelp/stories/main/0,5594,2652472-2,00.html

5. Newton's Telecom Dictionary 16th Edition

6. Trend Micro, Virus Encyclopedia, Profile "TROJ_NAVIDAD.E" 01-Dec-2000. URL: http://www.antivirus.com/vinfo/virusencyclo/default5.asp?Vname=TROJ_NAVIDAD.E

© SANS Institute 2000 - 2005, Author reta

© SANS Institute 2000 - 2005 Author retains full rights.