Global Information Assurance Certification Paper

David Allan Masters

Exploit Details:

Name: network.vbs aka netlog

Variants: netlogA, netlogB, netlogC

Operating System: Windows 95, Windows 98, Windows NT, and Windows 2000

Protocols/Services: Windows Scripting Host, VBScript, Windows Share

Brief Description: The Network.VBS exploit is a worm. According to the NSA glossary of terms a worm is " An independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads". This differs from a virus which is "A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself." The network.VBS worm is written in Visual Basic Scripting language. There are a number of other worms written in Visual Basic Scripting language these include Disable.Worm, CoolNotePad.worm, Stages.A, Bubbleboy. One of the most famous VBS worms is the LoveLetter worm. Network.VBS is different than most other VBS worms because it does not use email to replicate itself.

Network.vbs replicates by generating IP addresses and then attempting to connect to that address using Windows scripting host commands. Once it finds an IP address that it can connect to it records the IP address in a log. Then it maps the victims' hard drive using the capability of Windows (95, 98 NT) programs to share directories. Once it maps the victims' hard it copies itself to multiple locations on the victims' machine and starts the process again.

None of the analysis of network.VBS that was researched indicates how the attacker retrieves the log of infected machines. Although, Abe Sin of the San Diego Supercomputer Center notes that the exploit also erases the log file (if it exists) upon startup. He believes that this is a bug in the exploit, as there is no value to the would-be intruder to destroy a list of vulnerable hosts.

Network.vbs was announced this exploit is a self-replicating and self-transmitting worm in CERT Incident Note IN-2000-02 (URL http://www.cert.org/incident_notes/IN-2000-02.html)

Protocol Description

Network.vbs uses the VBScript scripting language developed by Microsoft for automating web pages. It is a variant of the Visual Basic for Applications computer language that is built into several Microsoft applications. The VBScript accesses file

sharing on the victims' machine. According to PCHelp (URL: http://www.nwinternet.com/~pchelp/security/issues/sharing.htm#manage) when File and Printer Sharing is first enabled, it is enabled on all network devices, including even Dial-Up Networking. This means that when a home user sets up his own LAN using Microsoft's simple, handy, built-in networking, and if that user turns on file sharing, his shared resources immediately become available over the existing dial-up or other link to the Internet. Microsoft is calling this "Windows Networking" using the protocol "CIFS" but according to Jacco de Leeuw (URL: http://huizen.dds.nl/~jacco2/samba/smb.html#netbios) it is one of the most popular protocols that computers use to communicate over a network. It is called "SMB" (Server Message Block). SMB is a standard used by many different programs including DEC Pathworks, Samba and Windows (95, 98, NT) and any SMB compliant program can share printers and files with other SMB complaint program. SMB-based networks use a variety of underlying protocols, but the most popular are "NetBIOS over NetBEUI" and "NetBIOS over TCP/IP". Because of the Internet, NetBIOS over TCP/IP has become the most popular method of transport. The default setting for Windows based operating systems is NetBIOS over TCP/IP turned on without any passwords or other protection.

This is the vulnerability in Windows (95,98, NT) that network.VBS uses to copy itself from one computer to another.

Description of variants

There are three variants netlog.A, netlog.B and netlog.C. Netlog.A and netlog.B differ in the log entries, where they copy themselves and what drive letter they use for the remote share. Netlog.C places an illegally altered version of a legitimate program on the victims computer. Here is a description of all three variants.

VARIANT:

Netlog.A

When executed, VBS/Netlog first creates a log file, "c:\network.log" and writes the following line to it:

Log file Open

Then the worm enters in an infinite loop. In the loop, it first generates a random IP class C subnet address. At the start the first number in the IP address is random number between 199 and 214, however, after 50 iterations in the loop the number is random between 1 and 254. Second and third number in the IP address are always between 1 and 254. After the IP address has been generated the worm writes this to its log file:

Subnet : *.*.*.0
where an asterisk ("*") is replaced with a number.

Next VBS/Netlog goes trough the entire subnet address space (1-254) and looks a share named "C" from each machine. This is the default name for a shared "C:" drive.

If the share is found, the worm maps the remote drive to local machine as "J:" drive and adds one line to the log file:

> Copying files to : *.*.*.*\C
> and copies itself to the following locations in the remote share:
>
> j:\network.vbs
> j:\windows\network.vbs
> j:\windows\start menu\programs\startup\network.vbs
> j:\win95\start menu\programs\startup\network.vbs
> j:\win95\startm~1\programs\startup\network.vbs
> j:\wind95\network.vbs

Therefore, infecting the remote machine. When the remote machine is restarted, the worm will be executed.

Then, if files were copied, the following line will be added to the log file:

> Successful copy to : *.*.*.*\C

Finally the worm takes the next address in the subnet, or chooses a next random IP address and starts again.

VARIANT:

Netlog.B

This variant consists of two files. It copies itself only to:

> C:\windows\start menu\programs\startup\network.vbs
> C:\windows\start menu\programs\startup\network.exe

It maps the remote drive to local machine as "Z:" (not "J:" as the VBS/Netlog.A variant does).

When it creates the log file "c:\network.log", the added line is different as well:

> Copyright (c) 1993-1995 Microsoft Corp.

(Note: the Copyright (c) 1993-1995 Microsoft Corp. line is added to the log by network.VBS and not part of Katrin Tocheva and Sami Rautiainens' analysis).

VARIANT

Netlog.C

This variant of VBS.Network places an illegally altered version of a legitimate program,
distributed.net, on the computer. It also attempts to copy itself across a network by first locating shared network drives and then mapping them to a local drive letter. Once a Windows 95/98/NT drive is infected, the worm tries to copy itself to the StartUp folder of the drive to ensure execution at startup. The worm remains in memory until the system is restarted.

This variant of VBS.Network places the following two files in the C:\Windows folder:

Dnetc.exe
Dnetc.ini

These are modified versions of the distributed.net program. The presence of these files alone is not an indication of infection. These files can legitimately reside on the computer without having been placed there by VBS.Network.C. In addition, the Network.vbs file may be copied to one or more locations, including the root folder, \Windows, \Windows\System, and \Windows\Start Menu\Programs\StartUp.

(Netlog.A and Netlog.B descriptions are from Katrin Tocheva and Sami Rautiainen at F-Secure and log.C is from Symantec at URL: http://service1.symantec.com/SUPPORT/nav.nsf/docid/2000030116551006).

How the exploit works

Intruders use network.vbs to actively exploit Windows networking shares to make remote connections across the Internet using VB script. Network.vbs installs itself in the system-wide "startup" folder. This causes the script to be started anytime a user logs into the machine. In the cases that the machine has no login the script starts on bootup.

The first thing the script does is to open C:\network.log on the local machine.

Then it generates a random four-octet IP address. This is done according to an algorithm.

The first octet is randomly selected between 199 and 214 for the first 50 IP addresses after which it is randomly selected between 1 and 254.

The second and third octets are randomly selected between 1 and 254.

The fourth octet begins at 1.

Then, the generated address is written to C:\network.log

For each host address from 1 to 254 in the generated range, network.vbs attempts to remotely mount a share named "C" from the remote computer as J: on the local computer.

If the "C" share of a remote computer is mounted successfully, it checks for the existence of a log file c:\Network.log, a "legitimate" script named Network.vbs (with a capital N) can also be found on most W9x hosts. It deletes it if it is found. Then it copies network.vbs to the following locations on the remotely mounted filesystem:

"j:\"
"j:\windows\startm~1\programs\startup\"
"j:\windows\"
"j:\windows\start menu\programs\startup\"
"j:\win95\start menu\programs\startup\"
"j:\win95\startm~1\programs\startup\"
"j:\wind95\"

If the first copy is successful, the address of the target system is written to C:\network.log. A new copy of the log file is then opened.

The program then starts infinite loop. With each iteration of the loop, it does the following:

Increment the fourth octet of the network address by one. If the value of the fourth octet is 255, pick a new random address using the algorithm above. (note that the increment is done first, which means that the any address where the fourth octet is 1 will never be attacked). The IP address of the network is logged to the log file.

Attempt to find a windows share on the remote host.

If successful, try and mount any drives found on j:

If successful, attempt to copy c:\network.vbs into the directories. A note is written to the log file saying that files are being copied.

Network.vbs then generates a new random network address range and starts the process over. It will continue to cycle through random address space implanting copies of itself onto vulnerable computers until the user logs out, the machine is shut down or administrative intervention prevents further execution.

The program stops when the user logs out or the machine is shut down. (Exploit description from URL: http://security.sdsc.edu/publications/network.vbs.shtml)

The script is dependent on particular files in particular locations, most notably it copies c:\network.vbs to the remote site. If that instance of the exploit does not exist, the copy will fail.

The log file will indicate successful copy even if the copy does fail for the reason above.

As discussed before, the exploit also erases the log file (if it exists) upon startup. This means that records of already compromised hosts may be lost. While this may be of no consequence to the compromised site, it means that it is probably impossible to determine that all of the hosts have been compromised by a particular site. It is believed that this to be a bug in the exploit, as there is no value to the would-be intruder to destroy a list of vulnerable hosts.

The true threat of Network.vbs is its ability to promulgate itself rapidly across the network virtually undetected. Since it is impossible to determine all the hosts, which have been compromised, this exploit will probably continue to propagate from infected hosts to vulnerable hosts. A modification of this exploit could easily be used to install remote control tools such as Back Orifice or Distributed Denial of Service tools such as WinTrin00. Or, the user of this exploit can use the logs generated by the exploit to compile a list of vulnerable machines, then quickly install the above tools or other similar items according to Abe Singer at the San Diego Supercomputer Center.

According to the CERT Incident Note "the network.vbs script demonstrates one pervasive method of propagation intruders can leverage to deploy tools on Windows-based computer systems connected to the Internet. They are aware of one infected computer that attempted to infect a range of at least 2,400,000 other IP addresses before being detected and stopped." They also claim that "there may also be denial of service issues due to packet traffic if network.vbs is able to infect and execute from a large number of machines in a concentrated area."

Diagram

The network.vbs worm attempts to connect to a share using an algorithm to select IP addresses. The hosts that it connects to it infects by copying itself to multiple directories and then repeating the process. A diagram of this would look like figure 1.

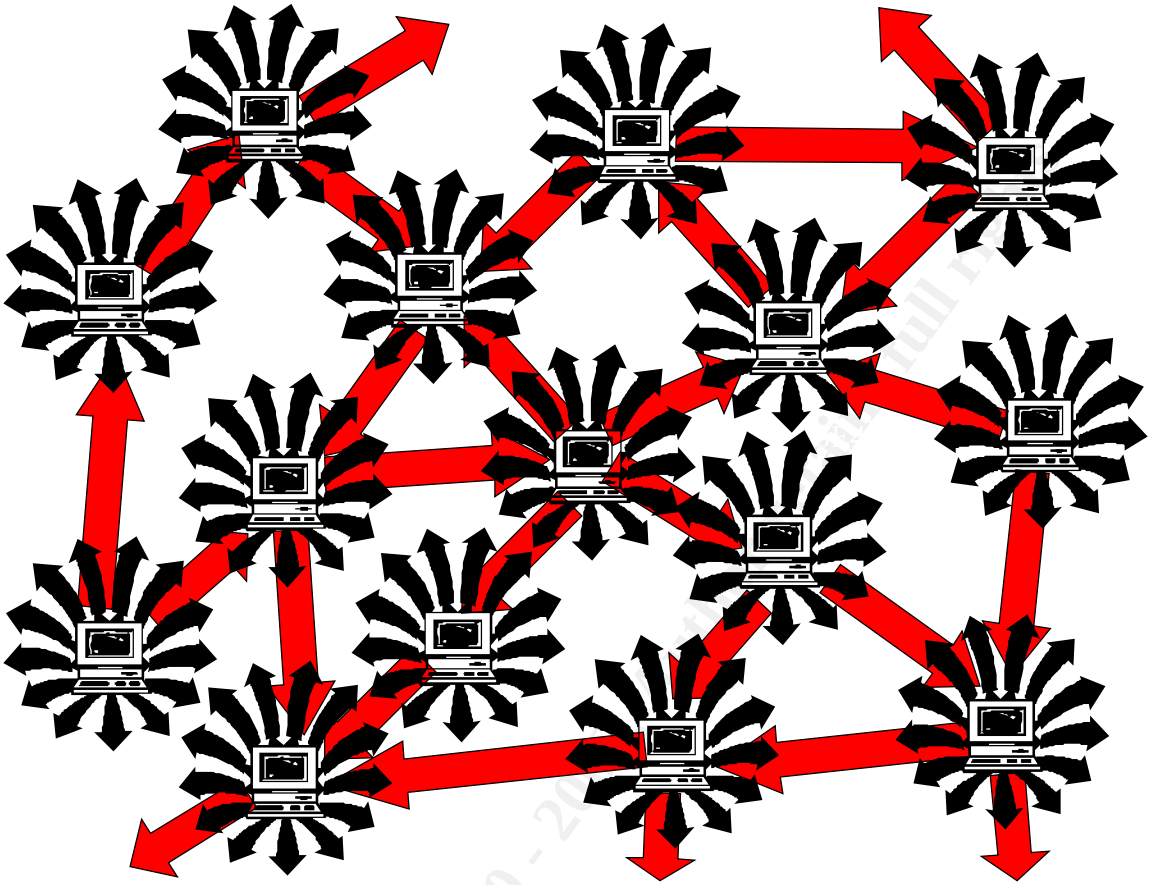

Figure 1 network.vbs in action

The network.vbs worm in each host tries to contact the IP address that it generated to copy itself into specific directory locations and then restart the process.

How to use the exploit

Running this network.vbs installs the program on to the local machine. It then begins to scan for available shares over the Internet using the algorithm to generate random IP addresses. Once if finds an IP address it maps the remote drive and copies itself into the shared directory. It then writes the IP address to the log file. An attacker could use network.vbs to deliver any one of a number of exploits. The log file could also be used to gain a list of the machines that are vulnerable to this type of exploit for further probing and hacking but none of the research indicated how the attacker might retrieve the log.

Signature of the attack

The network.vbs program can be found in the following locations on an infected computer: (According to Abe Singer at the San Diego Supercomputer Center)

c:\windows\startm~1\programs\startup\
c:\
c:\windows\
c:\windows\start menu\programs\startup\
c:\win95\start menu\programs\startup\
c:\win95\startm~1\programs\startup\
c:\win95\

A running network.vbs will not show up in the task bar, but the process "wscript" will appear in the task manager. This process may also appear for legitimate unrelated reasons.

A running network.vbs will also create a file called "c:\network.log" This file will be unopenable with tools such as notepad while the script is running, since the script has it open. It can be viewed by making a copy of the file and viewing the copy.

How to protect against it

Disabling running of programs from the startup folder will stop the program from starting when a user logs in. This solution may be unacceptable to users who wish to have tools automatically load on startup, such as system-tray utilities.

Another solution is to remove the VBS association. VBS/LoveLetter and related viruses have to the have the association for the VBS extension to the Windows Scripting Host (WSH) to spread. If this association is removed, you will not be able to execute VBScripts by double-clicking them. Here are the instructions for removing Visual Basic Script files from Windows 95:

1. Open "My Computer"
2. Select "View/Options"
3. Locate "VBScript Script File" from the "File Types" tab.
4. Select "Remove".
5. Select "Yes".

Now the VBS association is removed.

You may wish to insure your anti-virus software is configured to test file names ending in .VBS to help detect virus outbreaks involving malicious VBScript code.

"Trusted" remote hosts may still be able to infect a system, which allows authenticated shares, as the exploit runs with the user ID and permissions of the user logged into the remote hosts.

The larger problem is preventing Windows networking shares. Several steps can be taken to stop networking shares in Windows. This involves disabling File Sharing on your computer. If you wish to disable the File Sharing on your computer:

1. Click on Start, then Settings, then Control Panel

2. Double-click on the icon marked Network

3. In this new menu, there is a button about halfway down marked File and Print Sharing. Click it.

4. Uncheck both boxes and click OK.

File and Print sharing is now disabled. Disabling unauthenticated file-shares will remove the vulnerability of exploit by an unauthenticated user on a remote host.

If you need to keep file-sharing open, put a password on all of your shared drives. When configuring a Windows share, require a password to connect to the share. In implementing password protection it is important to consider trust relationships between systems. Use the following procedure to password protect shared drives:

1. Double-click on My Computer

2. Click on your hard drive. Select the Sharing option.

3. You will have the option to either share this drive or not share it.

4. For each drive you share, set up a password below.

5. Repeat steps 2-4 for each hard drive in the computer.

If your security policy is such that Windows networking is not used between systems on your network and systems outside of your network, packet filtering can be used at network borders to prevent NETBIOS packets from entering and/or leaving a network. Alternatively, use packet filtering to allow NETBIOS packets only between those sites with which you want to do file sharing. The following ports are commonly associated with Windows networking:

```
netbios-ns      137/tcp     # NETBIOS Name Service
netbios-ns      137/udp
netbios-dgm     138/tcp     # NETBIOS Datagram Service
netbios-dgm     138/udp
```

```
netbios-ssn     139/tcp     # NETBIOS session service
netbios-ssn     139/udp
```

Another alternative is to entirely disable NETBIOS over TCP/IP in the network control panel. The NetBIOS solution to stopping network.VBS is from Kevin Houle (CERT Incident Note IN-2000-02).

How to Clean/Delete the Network.vbs worm

Removing the network.vbs script from an infected computer involves removing the running image from memory and deleting the copies of network.vbs from the hard drive. Other tools installed using the same method of propagation may be more difficult to detect and remove. Removing the exploit code from all the locations above will successfully remove the exploit from the machine.

Cleaning the worm is fairly simple. Using the Windows FIND command located under the Start Menu to locate and delete the network.vbs files. The following is a step by step process to remove the virus:

1. Click on Start, then Find, then Files or Folders
2. In the Named field, please enter network.vbs
3. Ensure that the Look in: field reads Local hard drives (C:,D:)
4. Click on Find Now
5. It will find one or two files named network.vbs. Delete them by right clicking on each item and selecting Delete, EXCEPT the one located in C:\WINDOWS\SAMPLES\WSH which is a harmless example script.

Deleting all instances of the network.vbs file cleans your system of the infection.

The Netlog variant B needs additional steps to clean a system of this variant. Search for network.exe as well as the network.vbs files and delete them. They should be located in the Startup folder. This cleans your system of the Netlog.B variant of the worm.

Source code/ Pseudo code

The network.vbs script from PCHelp (http://www.pchelp.org/news/scriptworm.htm) is contained a separate zipped file called 'networkvbs'. This code contains a single small alteration that renders it impotent. The remainder of it has been left intact. Thanks to PCHelp for the scrip and the insight into the workings of network.VBS.

Links to additional information.

http://www.sophos.com/virusinfo/analyses/vbsnetlog.html

http://www.cert.org/incident_notes/IN-2000-02.html

http://www.info-sec.com/internet/00/internet_041400a_j.shtml

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=VBS_NETLOG.WORM

http://security.sdsc.edu/publications/network.vbs.shtml

http://service1.symantec.com/SUPPORT/nav.nsf/docid/2000030116551006

http://www.symantec.com/avcenter/venc/data/vbs.network.html

http://www.nwinternet.com/~pchelp/security/issues/sharing.htm#manage

http://pchell.com/virus/vbsnetlog.shtml

http://huizen.dds.nl/~jacco2/samba/smb.html#netbios

Last Updated: May 28th, 2017

Upcoming Training

SANS Madrid 2017	Madrid, Spain	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Virginia Beach SEC504*	Virginia Beach, VA	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Rocky Mountain 2017 - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
Mentor Session - SEC504	Reston, VA	Jun 13, 2017 - Aug 01, 2017	Mentor
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Seattle SEC504	Seattle, WA	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS ICS & Energy-Houston 2017	Houston, TX	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Ottawa SEC504	Ottawa, ON	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Sacramento SEC504	Sacramento, CA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Annapolis SEC504	Annapolis, MD	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Phoenix SEC504	Phoenix, AZ	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Des Moines SEC504	Des Moines, IA	Jul 24, 2017 - Jul 29, 2017	Community SANS
Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
Community SANS Raleigh SEC504	Raleigh, NC	Aug 07, 2017 - Aug 12, 2017	Community SANS
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event