CERT Incident Note IN-2000-02: Unprotected Windows Networking Shares

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community. Updated: Friday, April 7, 2000
Date: Friday, March 3, 2000

Overview

Intruders are actively exploiting Windows networking shares that are made available for remote connections across the Internet. This is not a new problem, but the potential impact on the overall security of the Internet is increasing.

Description

We have received reports indicating a rise in activity related to a malicious Visual Basic Script (VBScript) known as "network.vbs". The malicious script is similar to a harmless example script distributed with some versions of Windows 98, found as:

> c:\windows\samples\wsh\network.vbs

The malicious network.vbs script attempts to do the following things:

- Open C:\network.log on the local machine
- Generate a random /24 network address block. The algorithm we have seen used to generate addresses is:
  - the first octet will be randomly selected between 199 and 214 the first 50 times, after which is it randomly selected between 1 and 254
  - the second and third octet are randomly selected between 1 and 254
  - the fourth octet begins at 1
- The generated /24 address is written to C:\network.log
- For each host address from 1 to 254 in the generated /24 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, 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.

- network.vbs then generates a new random /24 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 administrative intervention prevents further execution.

When configuring the C: drive of a Windows 9x machine to be shared, the default share name assigned is "C". If this default share name is used on a vulnerable computer, network.vbs performs it's file copies on the C: drive of the remote system. If network.vbs is successfully copied into a Windows startup folder on a remote system, the remote system could execute network.vbs when the system reboots or a new user logs into the system.

We have also seen variations of network.vbs that perform different actions, such as:

- Create deceptively titled malicious items in the Windows startup folder and in the user start menu
- Deploy distributed encryption cracking tools on vulnerable systems

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. We 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. 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.

Abe Singer from the San Diego Supercomputer Center has also published an analysis of network.vbs, available at:

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

Impact

Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Because site security on the Internet is interdependent, a compromised system not only creates problems for the system's owner, but it is also threat to other sites on the Internet. The greater immediate risk to the Internet community is the potentially large number of systems attached to the Internet with unprotected Windows networking shares combined with distributed attack tools such as those described in

> IN-2000-01, Windows Based DDOS Agents

Another threat includes malicious and destructive code, such as viruses or worms, which leverage unprotected Windows networking shares to propagate. One such example is the 911 worm described in

> IN-2000-03, 911 worm

There is great potential for the emergence of other instances of intruder tools that leverage unprotected Windows networking shares on a widespread basis.

Solutions

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.

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.

Several steps can be taken to prevent exploitation of the larger problem of unprotected Windows networking shares:

- Disable Windows networking shares in the Windows network control panel if the ability to share files is not needed. Or, you may choose to entirely disable NETBIOS over TCP/IP in the network control panel.
- When configuring a Windows share, require a password to connect to the share. The use of sound password practices is encouraged. It is also important to consider trust relationships between systems. Malicious code may be able to leverage situations where a vulnerable system is trusted by and already authenticated to a remote system.
- Restrict exported directories and files to the minimum required for an application. In other words, rather than exporting an entire disk, export only the directory or file needed. Export read-only where possible.
- 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 whom 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
  ```

  Keep in mind that packet filtering alone may not provide complete protection. Malicious code can enter a network through portable code downloaded from web sites or through email containing portable code or executable file attachments. For more information about Trojan horses and suggested strategies, please see

  > CA-99-02, Trojan Horses

  In the case of a tool like network.vbs, packet filtering may be most effective against preventing the exit of malicious packets from your network, thus preventing malicious code like network.vbs from spreading from your site to others.

Acknowledgments

We thank Abe Singer and the San Diego Supercomputer Center for contributions to this Incident Note.

Author: Kevin Houle

Copyright 2000 Carnegie Mellon University.