M E M O R A N D U M

TO: All Locations

FROM: Information Technology Services (ITS)

SUBJECT: ***** VERY IMPORTANT *** NEW COMPUTER VIRUS - W32/Sasser.worm**

A new computer virus called "W32/Sasser.worm" is spreading throughout the computing community. The worm spreads with the file name "avserv2.exe" and unlike many recent worms **DOES NOT** spread vial e-mail. **NO USER INTERVENTION IS REQUIRED TO BECOME INFECTED OR TO FURTHER PROPAGATE THE VIRUS.** The worm works by instructing vulnerable systems to download and execute the viral code.

The virus copies itself to the Windows directory as avserve2.exe and creates a registry run key to load itself at startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "averserve2.exe" =C:\WINDOWS\avserve2.exe

As the worm scans random IP addresses, it listens on successive TCP ports starting at 1068. It also acts as an FTP server on TCP port 5554, and creates a remote shell on TCP port 9996. A file named win2.log is created on the root of the C: drive. This file contains an IP address. Copies of the worm are created in the Windows System directory as #_up.exe.

Examples

- C:\WINDOWS\system32\11583_up.exe
- C:\WINDOWS\system32\16913_up.exe
- C:\WINDOWS\system32\29739_up.exe

A side effect of the worm is for LSASS.EXE to crash. By default, the system will reboot after the crash occurs.

NOTE: Infected systems should install the Microsoft update to be protected from the exploit used by this worm. See: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

In order to minimize the risks of such vulnerabilities to your computing environment, we encourage you to subscribe to the Windows Update service by going to http://www.windowsupdate.com

http://www.magnetmail.net/Actions/linktosite.cfm?message_id=15398%26user_id=Msedu1%26recipient_id=6134423%26site=http://www.windowsupdate.com and also subscribe to Microsoft's security notification service at http://register.microsoft.com/subscription/subscribeme.asp?id=135<http://www.magnetmail.net/Actions/linktosite.cfm?message_id=15398%26user_id=Msedu1%26recipient_id=6134423%26site=http://register.microsoft.com/subscription/subscribeme.asp?ID=135> if you have not already done so. By subscribing to these two services, you will automatically receive information on the latest software updates and the latest security notifications thereby improving the likelihood that your computing environment will be safe from worms and viruses.

NOTE: The amount of users attempting to update their machines has caused the Microsoft site to be very busy. Also, the actual update may take an extended period of time to load.

M-DCPS employees and students are reminded that it is against the M-DCPS Official Network & Data Security Policy to connect ANY “non M-DCPS authorized” computing devices to any M-DCPS owned school or administrative network.

Additional Technical Notes to School Site Computer Technicians:

Due to increased security measures that ITS Network Services staff will be required to take in order to block the W32/Sasser.worm threat, school site technicians that remotely connect to their school servers may experience some difficulties. If you experience a problem while remotely connecting to a school server, contact Network Services via bhorta1@dadeschools.net. Please include the following information in the e-mail: your name, phone number, name of school site, and the nature of connection problem. Network Services staff will follow-up with a response as soon as possible.

Questions regarding this memo should be directed to Support Services at 305-995-3705(0).