Windows Enterprise Administrator Tips
Compromised System Forensics

Wayne Hauber [AIT]
August 7, 2003

This document contains some tips from a "forensics" standpoint on how to determine if a Windows system has been compromised. Once it is determined it HAS be compromised you need to make the determination on whether or not it should be rebuilt.

If you have additions, corrections, or comments on any of these procedures, please email Wayne Hauber at wjhauber@iastate.edu so they may be included in the future.

This document was composed by reviewing a number of computers to learn the MO of the folks perpetrating the RPC attacks (as related to MS03-026 starting in July 2003). I am taking a conservative view of compromised systems. If they have been compromised for any length of time, it is dangerous to attempt to clean them. Over the last few months, I have found scripts that reset all of the local security policies, keystroke capture programs, brute force password crackers, network scanners and all manner of proxies. To successfully clean a system, you will spend a number of hours digging through the system to ferret out all of the damage. Rather than do that, I would rather back up all of the important files and wipe the system.

With that said you can learn a lot about a compromised system and determine the damage by locating all of the network active programs and looking at the folders they are being run from.

1. Turn on the display of all hidden files and system files (folder options control panel).

2. Get a copy of "fport" from www.foundstone.com and put it on a floppy. You can run "fport" from a command prompt to see which programs are opening network ports. If you see a program that you don't recognize, look in its directory for other suspicious programs. If you are lucky will find the root kit the hacker left behind. Be aware that some campus systems have been broken into several times and may have multiple root kits.

3. Search for batch, command and ini files (.bat, .cmd or .ini) Perhaps you will find something that was left behind by the hacker. Secure.bat, start.bat and registry changing batch files are commonly used to wipe or change local settings. Look for the strings "xdcc", "Servu" and firedaemon. Perhaps you will find more of the root kit.

4. Once you have found the root kit, browse to it and enable the "create date" column from the View, Select columns menu. Look at the create date. If all of the rootkit was installed on the same date, you can use the create date to find other files that were installed. Use the Advanced options of Search to select a date search then change the date type to "Create date". Search for all of the files created on the same date as the root kit. Perhaps you will find more of the tools.

5. Go to the Administrative Tools control panel and select the Services management console. Look for services that you don't recognize. Do you see the "firedaemon" service? Do you see parts of the root kit running as services?

6. Open the Task manager. Are parts of the root kit listed? For example, this week we saw a program called wupdated.exe running as a port 139 scanner. I found a bogus copy of msmsgs.exe running as a spam proxy.

7. If you suspect the existence of an ftp server, you can sometimes locate it and the root directory with no additional information. Perform another search. This time search on size. Find all files larger than some large number, say 1024. The list will be long. Sort by size. Large files such as DVD's will sort towards the large end of the list. If you find contraband, note the directory and inspect it. It may be the root directory of the ftp server.

8. Inspect any suspicious batch and command files. Do you see scripts that reset the local security policies? This especially common in files named start.bat, secure.bat and any registry related batch files.

I find that this sort of detective work can take a couple of hours or more. When you are done you will have enough information to properly evaluate the system. Some hackers do enough damage that there is no question that a reformat and rebuild is necessary. Others may be gentler and do less damage. I rarely feel comfortable enough to recommend a cleanup. I more frequently recommend that a system be backed up and wiped clean. Your experience may be different. Only careful detective work will determine how clean your system really is.

Unfortunately, there is no quick fix.