

Troubleshooting

Compromised Computers

The Georgia Public Library Service HelpDesk often detects very high outward traffic or utilization on public library T1 connections to the outside world. Typically this indicates that a computer in the library has been compromised and is being used, for example, as an illicit download site.

The public library network administrator should investigate and secure the source computer. Here are some suggestions for troubleshooting the problem:

1. Isolate the problem PC or Server by unplugging each one in turn from the hub and watching to see if the usage drops.
2. Disconnect the suspect computer from your network.
3. Check the suspect machine for suspicious processes/services running in the background.
4. Check the suspect machine to see whether an unusual amount of disk space is being used.
5. Use Task Manager to identify any rogue processes that may be running and try to kill them.
6. Go to <http://www.sysinternals.com> and download the "TCPView" freeware utility. Launch it on the computer and use it to determine what unauthorized process is running and listening or communicating on suspicious ports with remote computers. Use the utility to try to kill the process.
7. Search the computer for Trojan files, making sure you look in hidden and system folders. Sometimes the files are hidden in folders that have been given reserved names like "LPT1," "PRN," "COM1," etc. (see [Microsoft Knowledgebase article 120716](#)) Often these folders are in the "deleted items" directories.
8. Start the computer in Safe Mode and delete the unauthorized files.
9. Check for suspicious programs being launched from the Startup group.
10. Check the following keys on the machine to see if there are any suspicious processes being launched.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

Troubleshooting

The following are some general suggestions to help ensure computer security:

- Ensure all machines are kept current with the latest Security Updates and Service Packs
- If your computers run Windows XP, consider activating the built-in firewall feature
- Make sure users have "non-dictionary" passwords
- Consider installing a firewall to help protect your network from unauthorized external access

Please contact the Georgia Public Library Service HelpDesk at helpdesk@georgialibraries.org for further assistance.



GEORGIA PUBLIC LIBRARY SERVICE

1800 Century Place, Suite 150
Atlanta, GA 30345-4304
404.982.3560
404.982.3563
www.georgialibraries.org