Tech Training: HijackThis

HijackThis is a free malware discovery tool for both personal and business use. HijackThis is quite powerful and should be used only by qualified technicians, as misuse could damage Windows. If you have not used this utility before, please see TJ for help in running it.

Running HijackThis

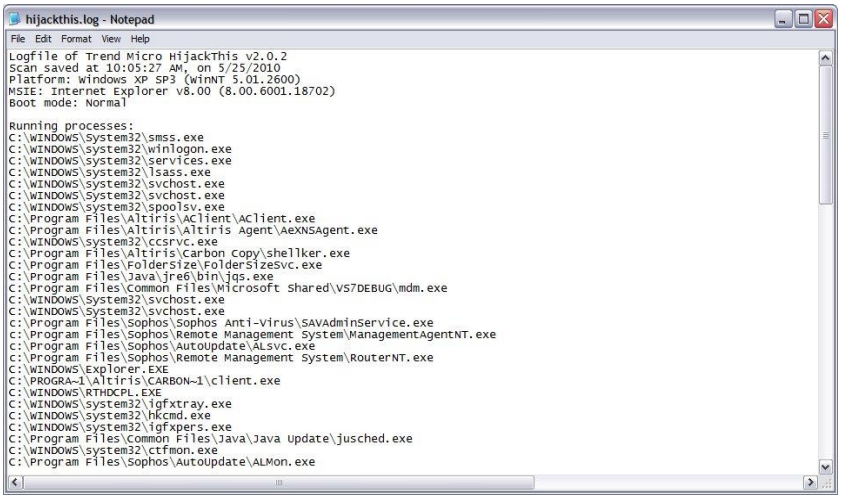
HijackThis is available on the Trend Micro website (http://free.antivirus.com/hijackthis/). You can also get a copy from the Utilities page of the Client Services internal website.

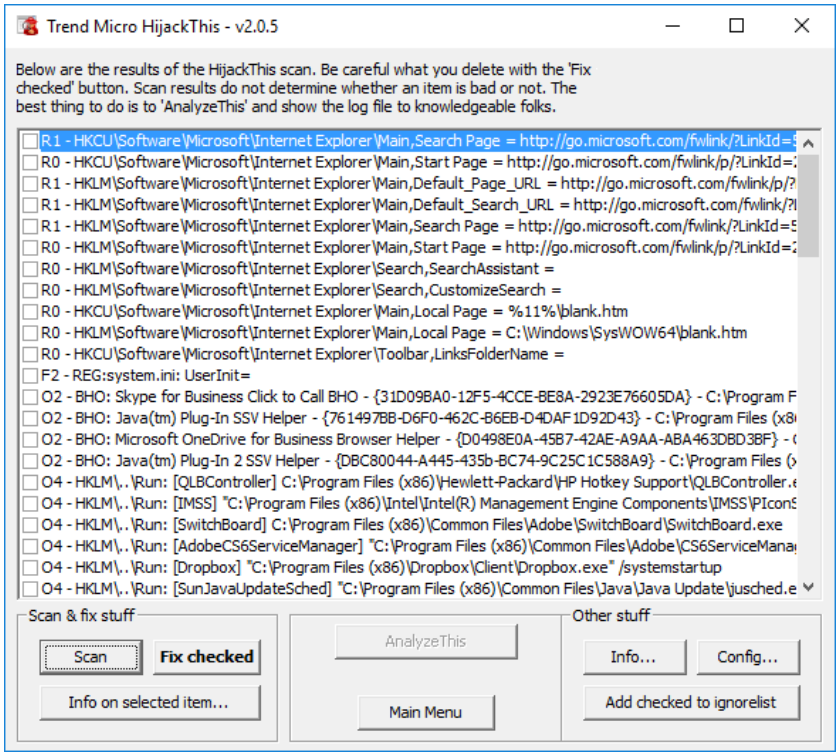
HijackThis is a stand-alone executable and does not require installation.

HijackThis scans Windows for all running processes and attempts to identify them. Once identified, it allows you to select those you'd like to remove. When the scan is complete, the results are stored in a log file and displayed for you to analyze in Windows Notepad.

If you'd like assistance in analyzing the results:

- Click Save Log
- Copy the entire log
- Browse to the HijackThis website
  - http://hijackthis.de
- Paste the log into the Log File text box
- Click Analyze
- Browse the results of the analysis for red Xs and question marks. Read the descriptions to identify malicious processes running on the computer.





- Place a check in items you want HijackThis to remove
- Click Fix Checked
- Restart the computer