Technology

Man Son Hing Martial Arts Academy

Case Study

SCENARIO

Problem	Solution
Office computer was massively infected with spyware and popup advertisements. Laptop was randomly crashing and rebooting.	Complete cleanup up office computer and new drivers for the laptop.

IN DEPTH PROCEDURES

- When the computer would boot up and attempt to load websites popups would become an issue and the computer would slow down to almost a halt.
- Inspected the Task Manger and found sever suspicious running programs. Rebooted the computer into safe-mode and ran a Spybot S&D scan. Deleted all found entries, but the problem of the popups still persisted.
- Tracked the popups down to a specific process that would activate when Internet Explorer was started and browsed with.
- It turned out that they had been infected with the "XP antivirus 2008" virus. This virus disguises itself as a real Antivirus but it is in fact categorized as a scam and malware. This virus is also very easy to contract. The program places a shortcut on your desktop and puts a small icon in the system tray that constantly informs you of its presence. If the user even runs his mouse over the taskbar icon the program will unload and embed itself in the operating system.
- Found all files associated with this virus and deleted manually in safe-mode with file explorer. Installed Kaspersky Antivirus to cleanup any traces of the virus including the registry.
- Kaspersky found the virus and partially removed it. HijackThis was used to delete any name servers left over that keep the IE home page from sticking to a certain site.
- Did a temporary file cleanup and registry fix with CCleaner and then moved on to the laptop.
- The stop errors were coming from the video card as is usually the case. Went to the Dell support site and downloaded the latest drivers for that model and rebooted the computer. Once installed, her laptop ceased receiving the stop errors. Installed the Kaspersky on the laptop.
- Removed Norton Antivirus on the home computer with the Norton Removal Tool and installed Kaspersky.