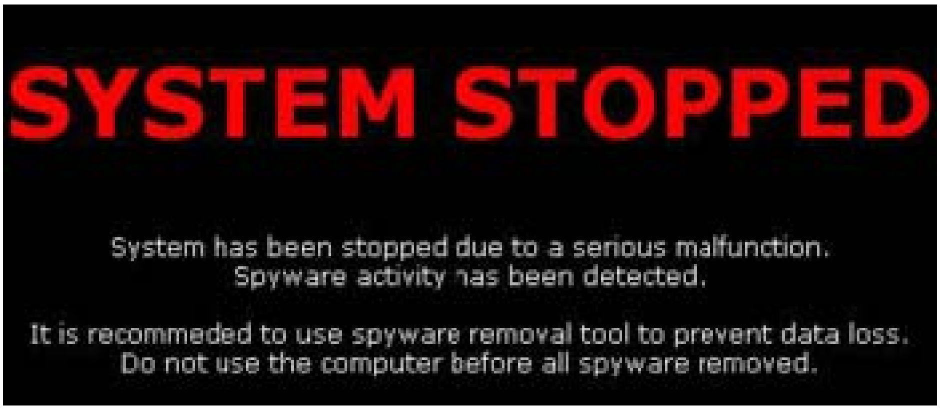
Spy Sheriff Exposed

It's been a long time since anything PC related actually made me angry enough that I felt compelled to write about it here. I am not sure if that means I am getting old, soft, or just plain lazy. Spy Sheriff, as I was about to learn, was primed to knock me out of my complacency. The story started several days ago when I got a call from a family member who wanted me to remove what they said was a particularly nasty malware infection. They claimed it was so severe it made it nearly impossible to use their PC. I figured they were embellishing things somewhat in the hopes of getting faster service. Family will do that to you sometimes. It turns out, though, that this time they weren't.



SYSTEM STOPPED

System has been stopped due to a serious malfunction.
Spyware activity has been detected.

It is recommeded to use spyware removal tool to prevent data loss.
Do not use the computer before all spyware removed.

Upon arriving on the scene and after booting into Windows XP I soon noticed several things are wrong:

-Windows background had been changed to a ridiculous fright screen claiming serious malfunction and threatening data loss so programs had been halted
-Repeated pop-up screens claiming false virus/spyware infections only removable through 30 usd Spy Sheriff registration payment granting you program S/N
-Internet Explorer browser home page hijack which was also used to pimp their dubious services and pretend they have a legitimate product, which they don't

That's all well and good, but how do I get rid of it once I am infected? Well, that seems to depend on what variant you have and whether it came by itself or loaded with some other malicious programs (Smitfraud) for instance. From what I can gather after the fact Spy Sheriff seems to install by using an IE browser exploit. The machine I removed it from was actually running a firewall which didn't protect against this infection either. I also should mention that while the method listed below worked for me, your results may vary. I also came across a much more thoughtful removal method which I thought I would link here.

I got started by visiting the Add/Remove programs sections by the way of CP to see if Spy Sheriff was listed. It was, so I chose remove and was informed that the action couldn't proceed because the program was active. Not about to let this stop me I went to the Run box by the way of the start menu and entered MSconfig. From there I searched around under the start-up tab for what files Spy Sheriff was loading. After a while I found the two files to be install.exe, and ibm00001.exe. After unchecking both of these I rebooted the machine. From here I ran Ad-aware and it found and seems to have removed Spy Sheriff. I did, however, have to manually remove the Winstall.exe, and secure32.html files from the the root. Attempts to run Ad-aware before using Msconfig and then uninstalling Spy Sheriff were in my case unsuccessful. I have also heard that Microsoft's AntiSpyware Beta if used properly is effective here. More information on this threat is also available on Ad-aware's site.

I would like to take a minute here to offer a few suggestions. Consider running a non-Microsoft browser--either Firefox or Opera. While neither of these programs has perfect security track records they are much better than IE. Not only that, but when an exploit is found it is patched much more quickly. Next, watch what sites you are visiting. Best as I can tell they seem to have picked up Spy Sheriff at one of the shady online games sites. That leads to the second tip: Pay close attention to the types of sites that you are visiting; sticking to reputable stand-up sites doesn't make you bullet-proof, but it does cut down your risk of infections. Last, but not least: Consider completely turning off Windows installs. Do you really need to install software through your browser? Possibly, but I bet for the majority of you like me the answer is no. To do this type in “about:config” in Firefox scroll down near the bottom of the page to xpinstall.enabled and set it to false.

Conclusion:

Although I am sure no one from Spy Sheriff would admit it, what is going on here is actually virtual kidnapping. Pay us 30 usd if you ever want to see your PC again. Even if you are flush with cash you should NEVER do this. After all, if this racket they have going here is financially successful for the makers of Spy Sheriff, you can bet that will encourage them to distribute more garbage like this onto the internet.

Jim Adkins

This page comes from
Monster-Hardware:
http://www.monster-hardware.com

The URL for this page is:
http://www.monster-hardware.com/modules.php?name=Content&pa=showpage&pid=39