Bad Lenovo

Last month we had the "Bad Google" issue, this month we have the "Bad Lenovo" edition. Lenovo is the third largest computer manufacturer in the world: they got their start by purchasing what was IBM's Personal Computer division. As such, they inherited outstanding designs and engineering from IBM, which have been maintained in the same high standards. Lenovo makes good stuff, at least hardware-wise.

What Lenovo did back in October – December 2104 was to install what is irreverently referred to as "junkware" or "crapware" on their consumer-level computers. The so-named "crapware" is mostly trial versions of various games, utilities, and apps. Software manufacturers pay Lenovo to put it on the machine in the hopes that you will try the software, like it, and buy the full version.

This practice is common in the industry, due to the razor-thin margins on consumer computers. Getting a few dollars for allowing trial software to be installed sounds pretty innocuous, and pads the computer maker's bottom line a bit. Well, it is innocuous except when the manufacturer does not do their due diligence on what is being installed. Lenovo apparently did not do any due diligence on their software load, because it included an advertising software called SuperFish. I don't know all the details about SuperFish, (more is coming out about this scandal daily) but I do know one super-bad factoid: it corrupts your computer's SSL Certificate library.

What is a SSL Certificate Library you may ask? It is what underpins the entire security model of web browsing. For example, any site that needs security has a web protocol named "SSL" enabled. What SSL does is establish a secure "channel" between your PC and say… your Bank. The secure channel is established by means of an SSL Certificate – a 3rd-Party software that proves the bank is who they say they are. The SSL certificate is accepted by your PC, and placed in the Certificate Library. All this happens in the background for you: the result you see is "https://..."instead of just "http://..." in the address bar, giving you assurance of security with your bank.

…Except if you have a Lenovo computer with SuperFish. What SuperFish did was put a fake certificate on your computer that opens up your browser to ANY certificate, including faked ones. On top of that, SuperFish and their advertisers can see ANTYHING you browsed, emailed, or whatever you did on your computer. It takes your secure, private channel and opens it up for anyone to see. **Oh yeah, it's bad… SuperBad.** So bad that Lenovo begged and got Microsoft to issue an emergency patch that removes SuperFish and restores your certificates library. (I wonder how much that cost Lenovo to get Microsoft to do that? Hmmm.)

The Class-Action lawsuits are already as thick as mosquitoes in a Louisiana swamp: I would not want to be a Lenovo defense lawyer right now, or for maybe the next 5-7 years. If you have **any Lenovo machine purchased in 2014-2015**, I recommend using the Lenovo SuperFish removal software on their website.
Lenovo SuperFish Removal Software

New York Times SuperFish/Lenovo Article

-John Becker

Phone: 630-852-1736 john@medofficesystems.com Fax: 630-214-4565