Lenovo stops Superfish preloads and issues advisory

February 21 2015, by Nancy Owano

Lenovo has seen calmer weeks. News sites in droves rang chimes and sirens over an adware program on some Lenovo models escalating to concerns about the potential risk of a Man in the Middle threat. Lenovo has been attempting to meet the storm head-on and has stopped preloads of the program called Superfish. In a statement, Lenovo said, "In our effort to enhance our user experience, we pre-installed a piece of third-party software, Superfish (based in Palo Alto, CA), on some of our consumer notebooks. We thought the product would enhance the

shopping experience, as intended by Superfish. It did not meet our expectations or those of our customers. In reality, we had customer complaints about the software."

Lenovo went on to discuss their response. "We acted swiftly and decisively once these concerns began to be raised. We apologize for causing any concern to any users for any reason – and we are always trying to learn from experience and improve what we do and how we do it. We stopped the preloads beginning in January. We shut down the server connections that enable the software also in January, and we are providing online resources to help users remove this software." Superfish was previously included on some consumer notebook products shipped between September 2014 and February 2015, said Lenovo. The company also said that the software has never been installed on any enterprise product—servers or storage—and these products were in no way impacted. Also, Lenovo said it never installed this software on ThinkPad notebooks nor Lenovo desktops or smartphones.

Superfish is a Palo Alto, California-based company which, with patented technology, developed a visual search engine. Writing in Bloomberg, Jordan Robertson said, "Superfish uses image-recognition algorithms that watch where users point on their screens and suggest ads based on the images they're looking at." The problem, said security watchers, is that it could potentially expose users to unauthorized activity monitoring. Robertson made the point that in general pre-installed software poses security and privacy concerns because questionable behavior is hard to detect and programs may be difficult to uninstall.

Lenovo's own security advisory issued the potential impact as "Man-in-the-Middle Attack" and called the severity "High." Lenovo said it ordered the pre-load removal in January and that "We will not preload this software in the future."

The advisory's description was of "Superfish intercept HTTP(S) traffic using a self-signed root certificate. This is stored in the local certificate store and provides a security concern."

On Friday, *PCWorld* senior editor Brad Chacos had the good news. "Bravo!" ran the headline to his story. "Windows Defender update fully removes Lenovo's dangerous Superfish malware." Chacos reported that Microsoft updated its Windows Defender to eradicate both the adware itself and the certificate potentially allowing encrypted web traffic to be compromised. Chacos said that a Microsoft spokesperson confirmed that "Microsoft security software detects and removes the Superfish software from Lenovo devices." Ed Bott in *ZDNet* on Friday similarly reported that Microsoft released the latest definitions for its Windows Defender software, included "as a standard feature on all Windows 8.x PCs. The new definitions, which are installed automatically, detect and remove the offending app and the certificate."

Update: As of Saturday, Chris Duckett, reporting in *ZDNet*, said that Lenovo has offered a removal tool.