Superfish: Adware Preinstalled on Lenovo Laptops

By Onuma

Published: 2015-02-24 · Archived: 2026-04-05 14:42:51 UTC

On February 19th of 2015, it became known that Lenovo's laptops had been shipped with an adware called Superfish preinstalled. There are two major problems with this issue.

The first one being that the hardware maker had been shipping consumer laptops with an adware preinstalled for several months — starting in September 2014 up until February 2015.

Another problem is related to how Superfish behaves. Its ability to produce self-signed certificates possibly allows a malicious third person to intercept SSL/TLS connections or, to put it simply, web browser sessions to "https" links.

Now, let's take a closer look at the latter problem by watching actual behavior of Superfish.

Below is a screenshot of an online banking website, accessed via Internet Explorer, from a clean PC without the adware. Clicking on the lock icon, it shows the information of the SSL certificate:

Fig 1. Accessing online banking site from a clean laptop

The SSL certificate is issued by Certificate Authority (CA) to ensure the ownership of the website. In this case, VeriSign is the certificate issuer who guarantees the identity of "Japan xxxx BANK Co,Ltd." The certificate is

also used to encrypt a user ID or a password on an encrypted session. Safety of a connection is guaranteed in this way.

The next screenshot is of the same website. But this time it is accessed via Internet Explorer from a Superfish-infected PC. Its SSL certificate now shows “Superfish” as its issuer instead of “VeriSign.”

Fig 2. Accessing online banking site from an infected laptop

What is the cause of this change? Superfish has its own CA on its software. This makes it possible to hijack a user’s web session, generate a self-signed certificate and establish an SSL connection using it. Unfortunately, web browsers treat the Superfish-generated certificate as legitimate. So, the CA is now Superfish, not VeriSign.

In addition, a private key for generating a certificate is included in the software and available to anyone who wants it. The password of the key has also been revealed on the Internet. With the key-password pair, someone with malicious intent could possibly intercept the data transmitted through the encrypted connection, or inject malicious code in it. The worst possible scenario in this case is data theft from a web session with an online banking site.

Users of Lenovo laptops with Superfish are strongly encouraged to delete both a software named “Superfish Inc. Visual Discovery” (from Windows Control Panel) and Superfish’s certificate (from the list of Trusted Root Certification Authorities).

> #Lenovo laptop users with #Superfish are strongly encouraged to delete both the #adware AND certificate

> Tweet

Kaspersky products can help you indentify if your laptop is affected. Our product detects the adware as Not-a-virus:AdWare.Win32.Superfish.b.

Lenovo is offering the Automatic Removal Tool for Superfish in their Security Advisory (LEN-2015-101).

Source: https://www.kaspersky.com/blog/lenovo-pc-with-adware-superfish-preinstalled/7712/