THE CONVERSATION
Academic rigour, journalistic flair

# Lenovo’s security debacle reveals blurred boundary between adware and malware

February 24, 2015 6.53pm GMT

Who’s looking after your keys? kris krüg, CC BY-SA

## Author

**Bill Buchanan**
Head, Centre for Distributed Computing, Networks and Security, Edinburgh Napier University

A widely disliked habit of PC vendors is their bundling of all manner of unwanted software into brand new computers – demo software, games, or part-functional trials. Faced with shrinking margins vendors have treated this as an alternative income stream, going so far as to include adware that generates revenue through monitoring users’ surfing habits, for example.

While some software such as virus scanners can be useful, Lenovo, the world’s biggest computer seller, has discovered just how badly it can backfire when including insufficiently tested – or just plain malicious – software.

With vendors often doing little in the way of due diligence, third-party software can include those with backdoors, or which could present privacy problems, or contain ways to trick users into paying for subscriptions. More often the focus is on pushing content and advertising, based on tracking user’s web browsing habits, or targeted marketing, where search results from trusted sites such as Google are tampered with before they’re presented to the user.

## SSL redirect

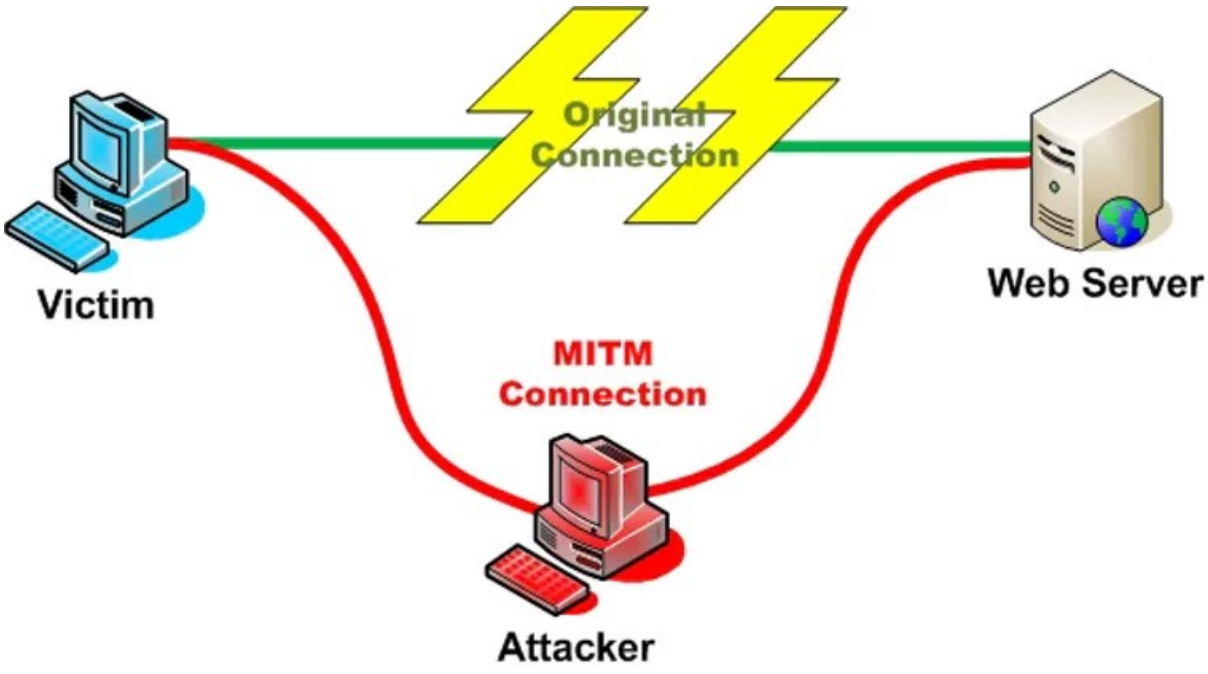
Lenovo's own-goal was to include Superfish: adware that alters search results in order to inject its own, and offers competing products whenever the user mouse-overs keywords in the page.

Encrypted communications require a private and a public key, separate but mathematically linked. The public key, which is published and available, is used by others to encrypt messages and send them to the owner of the public key. The public key's owner uses their secret, private key to decrypt them.

In order to be sure public keys belong to who they claim to, they are verified by certificates signed by trusted authorities. Superfish, however, in order to intercept encrypted search requests made over HTTPS (typically used by Google), installs a self-signed root certificate on the system. This, despite offering no checking or verification of keys, allows Superfish to takes control of encrypted traffic by masquerading as the site's own certificate. So, for example, when connecting to the Bank of America, the Superfish certificate would claim to be from the Bank of America.

This is called a man-in-the-middle attack, where one site impersonates another in order to fool other parties into communicating with it. The user thinks they are connecting to a valid site as the browser reports it has checked the site's identity via its certificate, but in fact traffic is going to another site, using another connection.

Can you see the problem? In an effort to pry into user's searches in order to show more adverts, Superfish created a security hole through which others can get in too. This was done as the private key for securing the data sent to Superfish has been cracked. Doing so also allows intruders to see search queries or any other traffic, even though it appears to the user that they are communicating securely with Google.



A man-in-the-middle attack, as created by Superfish. owasp, CC BY-SA

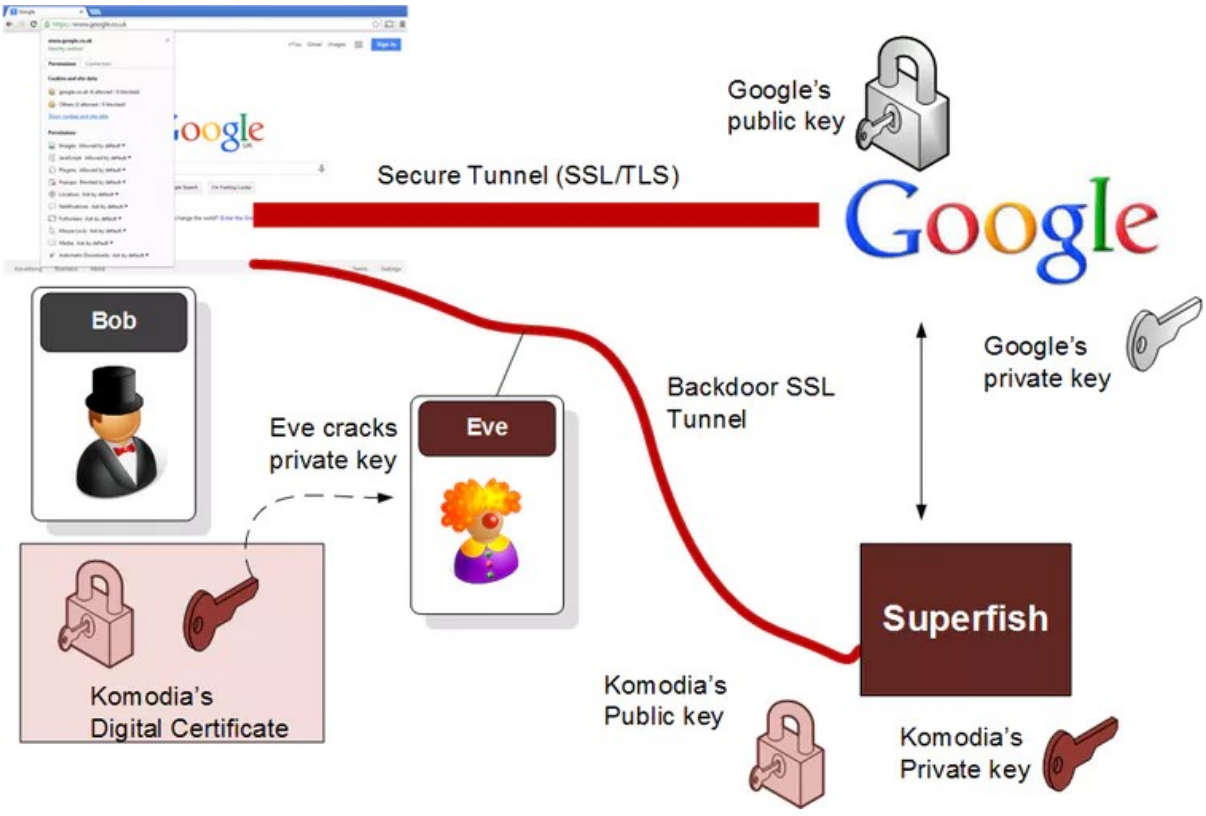
## Bad software used for bad ends

At the core of this problem is the use of SSL hijacker software developed by a firm called Komodia. As their website states:

> *The SSL hijacker uses Komodia's Redirector platform to allow you easy access to the data and the ability to modify, redirect, block, and record the data without triggering the target browser's certification warning.*

So we have a piece of software that can trick the user into connecting to website that is not necessarily what it seems or claims to be, bypassing the browser's built-in security that would alert them.

As if this wasn't bad enough, Superfish embedded the private key used to secure the traffic sent over the encrypted link along with its public key in the certificate. This should never happen, as a private key should not be shared. Not only does the certificate contain both keys, but the private key password has been cracked (it's "komedia", would you believe) and is the same for each on of the millions of computers on which Superfish is installed. And not just Superfish: the same weak certificates are bundled with many other software too.




Overview of the SSL redirect.

This is a spectacular security risk, meaning any intruder can access the data passing between any user with the certificate installed and any encrypted website they're connected to. It's like finding the best locks to secure your home, and then putting the keys under a plant pot outside the front door.

This wouldn't be the first time that security has failed in this way – not by defeating the encryption, but through a flawed set up and weak, easily guessable password. Antivirus software firms and Microsoft are already rolling out patches in order to detect and remove this software and its certificate.

Lenovo have sold over 16m Windows computers in the last quarter of 2014 – and many of these vulnerable. Not only that, but every one of those computers could potentially eavesdrop on the secure communications of every other, as the certificate password is the same for all.

This is likely to be extremely costly for Lenovo, in brand reputation but also in legal actions which have already begun. Although the issue was raised in January on the Lenovo forums, the firm claims to have had no idea of the problem it represented – that is bad enough in itself.

**Encryption** **Cybersecurity** **Malware**