Superfish, Privdog and Other Scary Beasts
Scott Wilson
DASNR-IT

You may have caught some news this last week about a newly-discovered security hole – perhaps you heard something about Lenovo computers and something called “Superfish”. (If you’ve actually heard of “Privdog”, you can skip the rest of this article – you’re already well ahead of the game.)

Superfish is a company that makes a piece of software called “Visual Discovery”. Visual Discovery is bad. How bad is it? Somewhere between “Really, Seriously Bad” and “Apocalyptic”, depending on how many machines actually have it and how quickly it can be exploited. It’s technically marketing software, software that tracks what you’re looking at on the web and finds similar things to suggest to you; you’re probably already familiar with this process if you have any sort of Google account. If Superfish had stopped there, it wouldn’t be significant – annoying, perhaps, but not significant.

Superfish didn’t stop there. Instead, the company decided that its software should be able to see what you’re doing all the time, even if what you’re doing is supposedly secured. When you connect to a secured site (one that uses “https” instead of “http”) the site is supposed to confirm that it is who it says it is. It does this by handing your browser a certificate, which is a string of code that can be combined with another piece of code (I’m simplifying a lot here) to verify that the site is really Citibank or Amazon or whoever. All of the traffic between the site and your browser is encrypted, which means that anyone snooping on your network can’t see it. This is good, but means that Visual Discovery couldn’t see what was going on if you had a secure connection going.

Superfish decided to fix that. What Visual Discovery does is simple: it sets itself up as a Certificate Authority (an entity that verifies certificates) and acts as a proxy connection, meaning all of your traffic has to go through it. So when you connect to Citibank, it actually stops your connection and then makes its own connection to Citibank. This means that all of your traffic is now unencrypted, so Visual Design can read it and show you some ads.

“But wait,” I hear you say. “I started an encrypted session! Surely my browser isn’t going to let it just go unencrypted and not warn me!”

That’s true. So, to keep you from being scared by a bunch of browser warnings, Visual Discovery uses its certificate to re-encrypt the traffic and send it to your browser. However, since your browser thinks it should be talking to Citibank, VD (interesting initials, huh?) has to lie to it and say that yes, you are in fact connected to Citibank.

This seems pretty bad, but it gets worse. Since VD has no way of knowing what sites you’ll connect to, it has to make up certificates on the fly for any site. This means that the software has to have a copy of Superfish’s private signing key. Private signing keys are long strings of data that can be combined with other data to verify that the authority is who it says it is. They are supposed to be kept private, because if they aren’t, then they can be used for some really bad things.

Visual Discovery has a copy of the one Superfish uses. Worse, it has the password needed to generate the certificates. Worse, that password is NOT encrypted.
Can you see where this is going?

Anyone who is on a network with a machine or machines running Visual Discovery can make his own certificates, not only for sites but for software, meaning that when you think you’re connecting to Citibank.com and getting their banking app, you’re actually connecting to another site and running the software that the deceitful person wants you to run.

If you have a new Lenovo laptop (made since October 2014), you should be thinking about having it wiped and having a new version of Windows (NOT Lenovo’s version) installed.

Obviously, most OCES computers aren’t Lenovos, and as far as we know, don’t have any of Superfish’s software on them. However, that may not be good enough.

PrivDog is a piece of software made by Comodo software. It also sets itself as a proxy with a trusted root certificate and looks ate the secure traffic, for much the same reason. Unlike VD, PrivDog uses a different certificate on every system, so it’s not vulnerable to an attacker making fake certificates. The problem it has is simpler, but still bad: PrivDog doesn’t verify the certificates it gets from sites. That means that if you connect to a bogus site, instead of getting a warning, you’ll just be connected. In other words, you could still find yourself on an attack site without any warning from your browser.

There don’t appear to be a lot of people affected by this – perhaps only about 6,000 potential victims in the US, as it will only include those who installed certain Comodo products. (It’s unclear exactly which ones – it might be a good idea to contact DASNR IT if you have installed anything from Comodo.)

The common thread between Superfish and PrivDog is that both use the same core code, from a security company called Komodia, who have sold their code to a number of other software makers as well. Please contact DASNR-IT if you have installed software from any of the following:

- CartCrunch Israel LTD
- WiredTools LTD
- Say Media Group LTD
- Over the Rainbow Tech
- System Alerts
- ArcadeGiant
- Objectify Media Inc
- Catalytix Web Services
- OptimizerMonitor

This kind of willful breaking of the chain of trust that is used to secure the internet has the potential to be really dangerous; whether any of these iterations will be the fatal one remains to be seen.