Dear HIPAA HITECH EXPRESS customers,

You may have been reading in the press about the "Superfish" adware that has been installed on Lenovo computers in the past year. We are sending this to help you understand the problem, clarify who is affected and suggest a plan of action.. Even if you are not directly affected, we suggest that you read this to understand how your data can be put at risk by purchasing products from untrustworthy sources. If you purchased Lenovo laptops or desktop computers in 2014 or 2015 you will need to take action.

Background:

Over the past decade internet advertising and data mining applications have sprung up to "help you" by watching your internet access habits and suggest lower cost alternatives. These are implemented using cookies and sometimes installed applications. They are often annoying and can be very harmful if the user is not careful to use the SSL protocol for exchanging passwords and other sensitive information. SSL encrypts communications and establishes trust that the site you are communicating with is not a hoax. SSL can be identified in the browser URL by a "https://" as opposed to "http://" and in some browsers by a small lock icon.

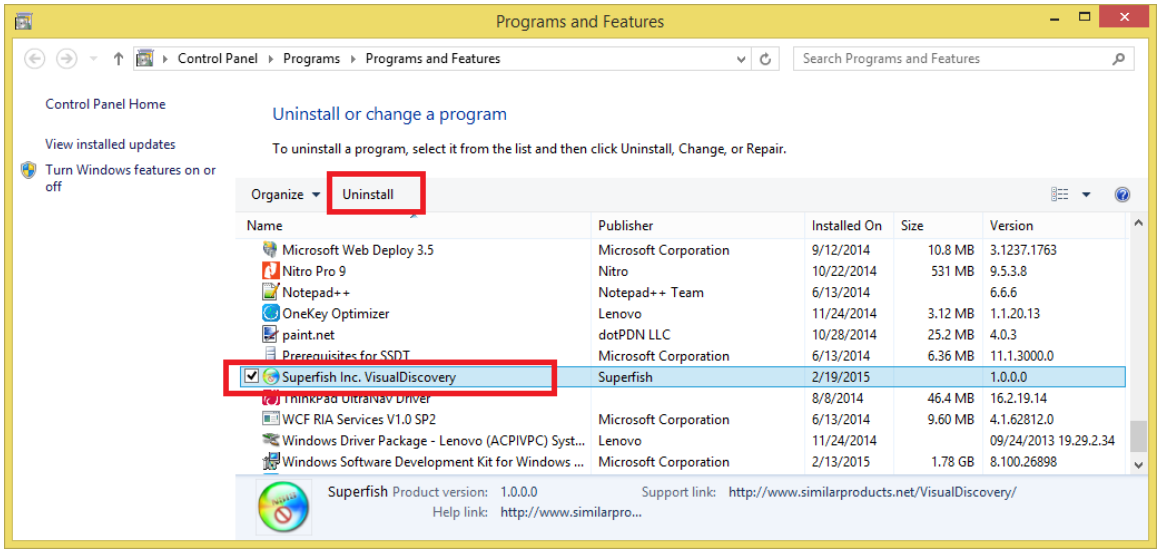
Occasionally your browser may inform you that the site in the URL is not trusted. It is important to take this warning seriously and not accept it as trusted without explicit knowledge. Your computer knows which sites are trusted from a store of "certificates" that are put in your system during its initial configuration by the vendor and then added to as you accept trust from new sites. The software vendors and website administrators then establish their trustworthiness with respect to these certificates. If an untrustworthy one finds its way into your store of certificates you have a situation where you cannot guarantee that the encryption is effective or that the site you are communicating with is not a hoax.

Superfish:

Superfish installed an application and a certificate on Lenovo systems that intercepts your web browser SSL communications and pretends to be the destination site to your browser and pretends to be your browser to the destination site. This is called a "Man-in-the-Middle" attack and is a very serious problem. It is the reason that we have SSL. Superfish uses the "trusted" certificate to do a very untrustworthy thing. It forwards information from your SSL "encrypted" web session to a third party for analysis and to provide you with advertising. While the intent may not be malicious, the effect is a serious violation of HIPAA and the trust of you, your patients and your customers. When Superfish is in place none of the SSL communications, including access to your private patient records, are confidential. Nor are passwords, interactions with financial institutions and any other "privileged" communications that should be encrypted by SSL.

What to do:

First, establish if you are directly affected. Computers that may be affected were sold by Lenovo between September 2014 and February 2015. If you have systems that were purchased during that period, check your control panel to see if it is present. If it is, use the manual Uninstaller to remove the Superfish software.



This removes the software, but does not remove the certificate. It is important to remove the certificate to prevent misuse of it in the future.

Go to the site:

http://support.lenovo.com/us/en/product_security/superfish

Follow the steps shown in section "B".

Incident Response and Reporting:

If you find the software in any of your systems you should treat it as a security event and follow-up should be done according to your Incident Response Plan. Your plan should at a minimum include 4 actions.

1. Removal of the software and certificate from all systems.
2. Determination of what PHI was accessed from these systems prior to removal.
3. Contact Lenovo to determine what information was transmitted off of these systems the Superfish server.
4. If the amount of PHI that may have been accessed is above the breach reporting threshold AND PHI from the system was transmitted to the Superfish server, you will need to file a breach report.

If you get as far as action 4 you probably will also want to be in contact with your legal counsel as Lenovo clearly is responsible for any costs associated with this breach.

We hope this has been of use to you. If you have further questions, please do not hesitate to call us.

Eric Hummel
QIP Solutions
eric.hummel@qipsolutions.com
703 980-3378
www.qipsolutions.com