INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

PETYA WREAKS HAVOC WORLDWIDE

A serious ransomware attack, similar to WannaCry, has reached Asia after spreading from Europe to the US, hitting businesses, banks, airports, power stations, port operators and government systems. This ransomware is being described by the press and security researchers as “Petya Ransomware.” Read more on Fin24.

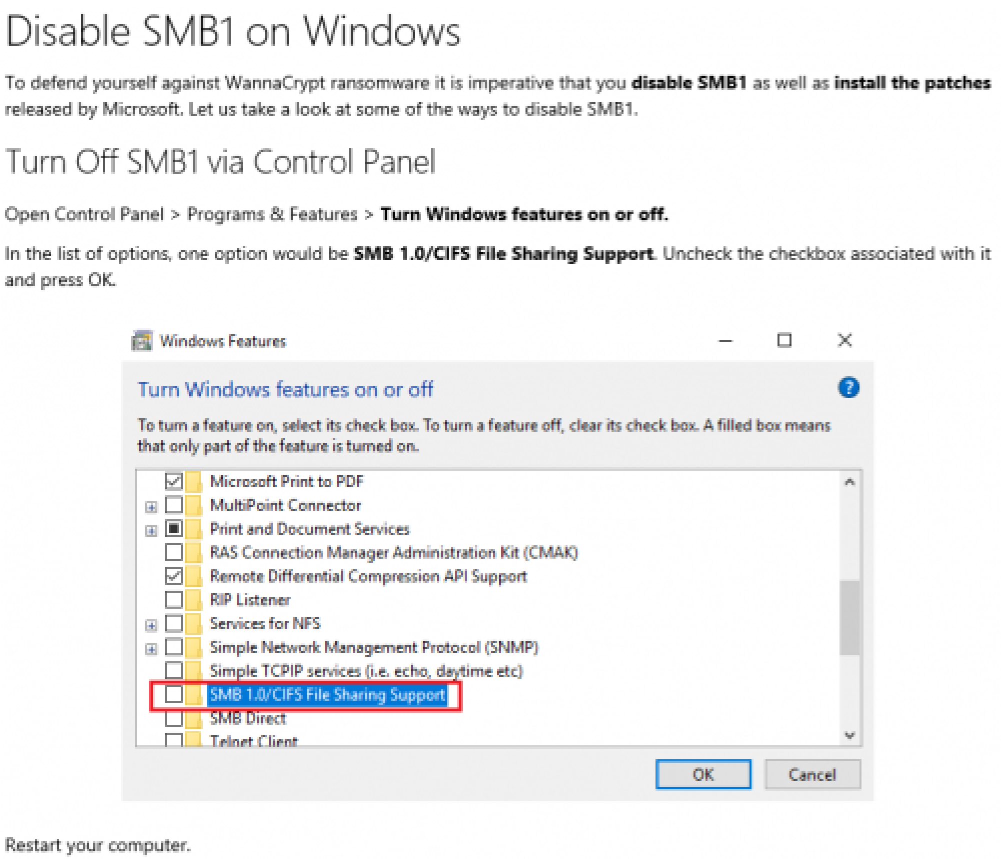
"Ransomware is a type of computer virus usually downloaded that attacks and takes over a computer, sometimes installing a password or encrypting the entire hard drive, preventing any access. The victim is then extorted for money, usually payable in Bitcoin, in order to unlock their precious data."

"This is a new generation of ransomware designed to take timely advantage of recent exploits. This current version is targeting the same vulnerabilities that were exploited during the recent Wannacry attack this past May. This latest attack, known as Petya, is something we are referring to as a ransomworm. In this variant, rather than targeting a single organization, it uses a broad-brush approach that targets any device it can find that its attached worm is able to exploit." (www.blog.fortinet.com)

While many of you might not be too concerned about this attack, since it originally happened in Ukraine, a small country on the other side of the world, the nature of the Internet and the fact that we are all connected in some way or another, means that it will only be a matter of time before we start to experience attacks on South African soil. There are already reports of infected emails from the Ukraine attack being detected in parts of Western Europe and the USA.

This attack seems to have began with a extensive phishing attack of emails sent out with infected Excel attachments, or a Trojan virus that attempts to disguise itself as a type of Microsoft Excel online document. Once opened the infected attachment will gain control over the victim's computer and start encrypting the hard drive contents, preventing any access.

To ensure that you don't fall prey to this attack, you can follow these instructions from Microsoft.



Disable SMB1 on Windows

To defend yourself against WannaCrypt ransomware it is imperative that you **disable SMB1** as well as **install the patches** released by Microsoft. Let us take a look at some of the ways to disable SMB1.

Turn Off SMB1 via Control Panel

Open Control Panel > Programs & Features > **Turn Windows features on or off.**

In the list of options, one option would be **SMB 1.0/CIFS File Sharing Support**. Uncheck the checkbox associated with it and press OK.

Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

☑ Microsoft Print to PDF
□ MultiPoint Connector
■ Print and Document Services
□ RAS Connection Manager Administration Kit (CMAK)
☑ Remote Differential Compression API Support
□ RIP Listener
□ Services for NFS
□ Simple Network Management Protocol (SNMP)
□ Simple TCPIP services (i.e. echo, daytime etc)
□ SMB 1.0/CIFS File Sharing Support
□ SMB Direct
□ Telnet Client

Restart your computer.

Please be wary of emails that come from unknown sources, (or even from senders who are unaware that their computers are controlled by ransomware and are busy sending out infected emails.) especially if they have .XLS, .PDF and .HTML attachments or ask you to login to verify details or click on links.

- *The best defense against ransomware is to outwit attackers by not being vulnerable to their threats in the first place. This means backing up important data daily, so that even if your computer gets infected, you won't be forced to pay to see your data again. Do you have a backup of ALL your important data? Operating systems can be easily rebuilt or reinstalled - your personal data cannot.*
- *Be aware of emails that carry a malicious attachments or instruct you to click on a URL.*
- *Watch out for "malvertising" - this involves compromising an advertiser's network by embedding malware in ads that get delivered through web sites you know and trust. Ad blockers are one way to block malicious ads, and patching known browser security holes will also thwart some malvertising. Is your computer up-to-date?*
- *Finally, don't be trigger-happy and click on links, no matter how legitimate they might look. Think first before clicking. If you have doubts about an email, phone up the IT HelpDesk and find out or ask your local computer geek for their opinion.*

*Many of you are on holiday and at home where your protection *might* not be a good as what we enjoy at the university.*

[ARTICLE BY DAVID WILES]

Posted in:E-mail,Security | Tagged:Petya,Ransomware,WannaCry | With 0 comments