INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

PETYA SAAI WÊRELDWYD VERWOESTING

? Ernstige ransomware-aanval, soortgelyk aan WannaCrypt0r/WannaCry, het gisteraand Asië bereik nadat dit van Europa na Amerika versprei het. Verskeie groot besighede, hawens, banke, lughawens, kragstasies en regeringstelsels is swaar getref. Hierdie ransomware word deur die pers en sekuriteitsnavorsers beskryf as "Petya".

Ransomware is ? tipe rekenaarvirus wat afgelaai word en rekenaars aanval en oorneem. Soms installeer dit ? wagwoord of enkripteer die hele hardeskyf en belemmer enige toegang tot data. Die slagoffer word gevolglik gevra vir geld, gewoonlik betaalbaar d.m.v. Bitcoin, indien hy/sy data terug wil kry.

"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)

Aangesien die betrokke aanval oorspronklik in Ukraine, ? klein landjie aan die ander kant van die wêreld, gebeur het, is dit maklik om te ignoreer. Maar weens die aard van die Internet en die feit dat ons almal verbind is, beteken dit dat Suid-Afrika ook bereik kan word. Petya is intussen ook in Wes-Europa en Amerika opgemerk.

Dit blyk of Petya begin het met `n deeglike phishing-aanval deur e-posse met aangehegde, besmette Excel aanhangsels of ? Trojaanse virus in die vorm van ? aanlyn Microsoft Excel dokument. Sodra die aanhangsel oopgemaak word, neem dit die ontvanger se rekenaar oor, enkripteer die hardeskyf en verhoed dat jy toegang het tot jou data.

Rekenaars op die SUN-domain kan beskerm word deur die volgende instruksies van Microsoft te volg:

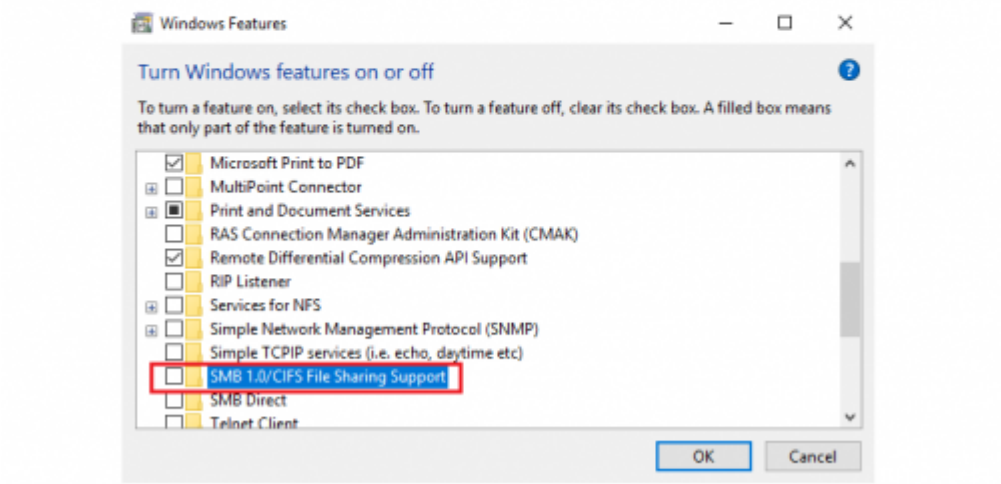
Disable SMB1 on Windows

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.



Restart your computer.

Wees versigtig vir e-posse van onbekende bronne, veral as dit .XLS, .PDF en .HTML aanhangsels het of jou vra om aan te teken en jou details te bevestig of op skakels te kliek.

- *Die beste beskerming teen ransomware is om nie jouself kwesbaar te laat nie. Dit beteken dat jy jou data gereeld moet rugsteun, sodat, indien jou rekenaar besmet word, jy steeds toegang daartoe elders kan kry.*
- *Wees versigtig vir e-posse met gevaarlike aanhangsels of wat vra dat jy op skakels kliek.*
- *Oppas vir "malvertising" – malware wat versteek word in advertensies op webwerwe wat jy ken en vertrou. Advertensieblokkers kan help om advertensies te blok en om te sorg dat jou webblaaier tot op datum opdateer is, sal ook keer dat daar sekuriteitsgapings is.*
- *En laastens, moenie kliekmal wees en op enigiets kliek nie – al lyk dit hoe oortuigend. Dink voor jy kliek. As jy twyfel, kontak die IT Dienstoonbank.*

[ARTIKEL DEUR DAVID WILES]

Posted in:E-pos,Sekuriteit | Tagged:Petya,Ransomware,WannaCry | With 0 comments