SUMMARY

of

What we know about "PETYA"

Issued : 27/06/17 at 21h45 GMT+1 by Hacknowledge

1.

Introduction

Petya is a ransomware.Its origin is not clear yet. It could be a variaton of Petya (hence the name) or Wannacry.

2.

Patching

It seems that Petya uses a modified version of the NSA Eternalblue exploit to propagate

3.

Lateral movement

It seems that Petya uses the NSA Eternalblue exploit but also spreads in internal networks with WMIC and PSEXEC.

That's why patched systems can get hit. Once a first machine is infected, Petya uses LSADump to get Admin password and infect other machines A single infected system on the network possessing administrative credentials is capable of spreading this infection to all the other computers through WMI or PSEXEC.

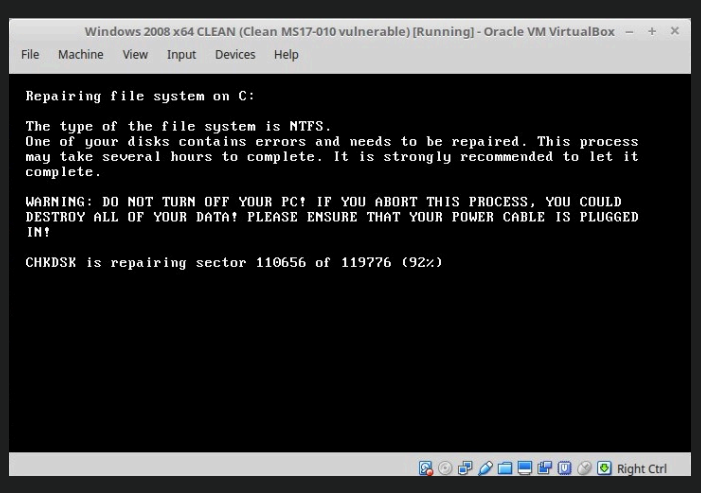
DO'S & DON'TS

DO'S

- Make sure you have applied the latest windows patches (especially the ones concerning SMB protocol)
- Make sure you have backup (better safe than sorry)
- Make sure no machine is exposing port 445 on the internet
- If machine reboots and you see chkdsk message, power off immediately! This is the encryption process. If you do not power on, files are fine.
- You can use MS AppLocker to disable execution of a file called perfc.dat and the PSExec utility

DON'TS

- Pay the ransom (as the email address is already blocked since +/- 2h)
- Open attachments sent to your RH email address. Last year, Petya targeted businesses via recruitment pages. Exploits targeted those receiving CVs/resumes.



Possible Killswitch

Simply create a file C:\Windows\perfc

Hacknowledge