Petya Ransomware

Section 16, Lecture 53

How to Protect Yourself from Ransomware Attacks


What to do immediately? Go and apply those goddamn patches against EternalBlue (MS17-010) and disable the unsecured, 30-year-old SMBv1 file-sharing protocol on your Windows systems and servers.

Since Petya Ransomware is also taking advantage of WMIC and PSEXEC tools to infect fully-patched Windows computers, you are also advised to disable WMIC (Windows Management Instrumentation Command-line).

Researcher finds Petya ransomware encrypt systems after rebooting the computer. So if your system is infected with Petya ransomware and it tries to restart, just do not power it back on.

"*If machine reboots and you see this message, power off immediately! This is the encryption process. If you do not power on, files are fine.*" ‏HackerFantastic tweeted.

To safeguard against any ransomware infection, you should always be suspicious of unwanted files and documents sent over an email and should never click on links inside them unless verifying the source.

To always have a tight grip on your valuable data, keep a good back-up routine in place that makes their copies to an external storage device that isn't always connected to your PC.

Moreover, make sure that you run a good and effective anti-virus security suite on your system, and keep it up-to-date. Most importantly, always browse the Internet safely

*Source:- Thehackernews*