PETYA RANSOMWARE

INTRODUCTION

Malware: is a program specifically designed to disrupt, damage, or gain authorized access to a computer system.

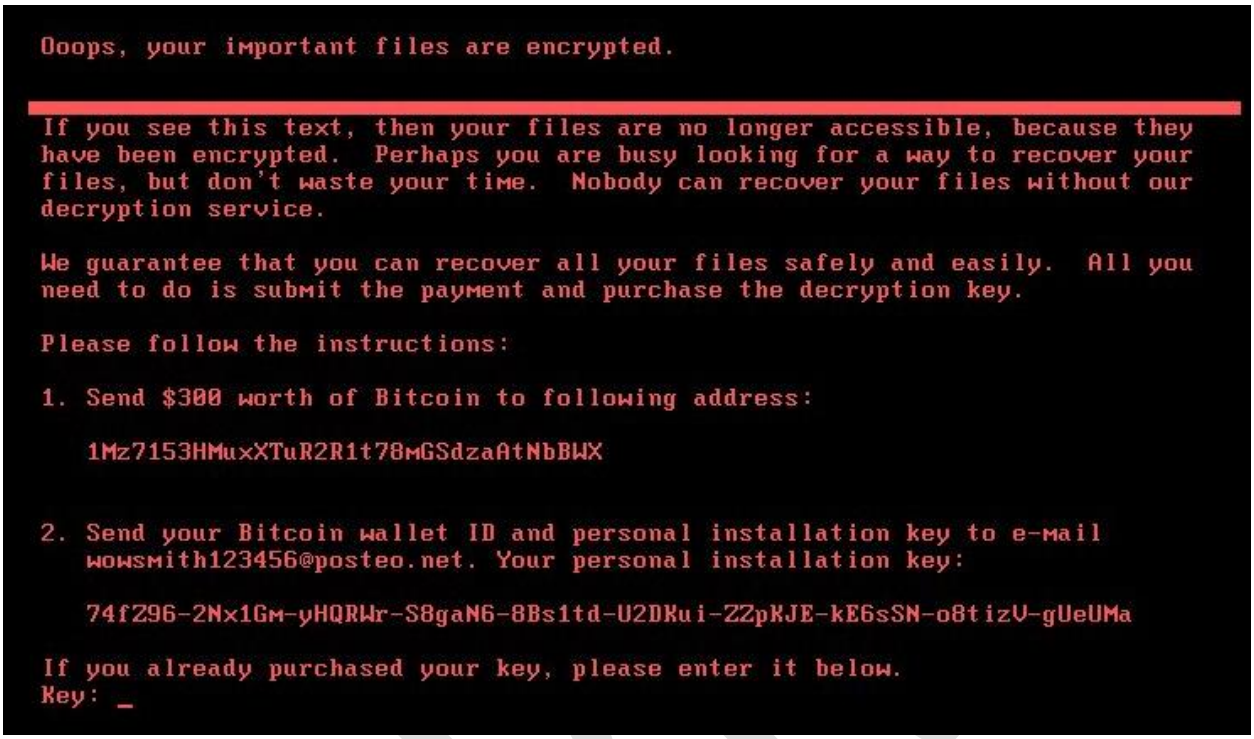
Ransomware: is a type of malware that prevent user from having access to their **Computer** files either by encrypting their files or by locking the system's screen unless a ransom is paid.

Petya: Petya is a malware that targets Microsoft Windows-based systems, infecting the master boot record to execute a payload which encrypts the NTFS file table, then demanding a payment in bitcoin to re-gain access to the system.

Typically, when a user becomes infected by a crypto-ransomware, the infection targets and encrypts the files on the victim's hard drives. This leaves the operating system working properly, but with the user unable to open the encrypted documents. The Petya Ransomware takes it to the next level by encrypting portions of the hard drive itself that make it so you are unable to access anything on the drive, including Windows. At the time of this writing, the ransom payments are at 9 bitcoins and there is no way to decrypt your drive for free. This ransomware is currently being distributed via emails that are targeting the human resources departments of German companies. These emails contain Dropbox links to malicious downloadable applications, that when executed will install the Petya Ransomware on the computer.

Source: thehackernews.com

The following ransomware note is displayed on infected machines, demanding that $300 in bitcoins be paid to recover files:



Operation:

Versions of Petya utilize a payload which infects the computer's master boot record, both overwriting the Windows bootloader, and then triggering a restart. On the next startup, the payload is executed, which encrypts the Master File Table of the NTFS file system, and then displays the ransom message demanding a payment made in Bitcoin.

The original payload requires the user to grant it administrative privileges, one variant of Petya was bundled with an alternate payload known as Mischa, which is used if Petya fails to install. Mischa is a more conventional ransomware payload which encrypts user documents, as well as executable files, and does not require administrative privileges to execute. The earlier versions of Petya disguised its payload as a PDF file, attached to an e-mail. The "***notpetya***" variant utilized in the 2017 attack utilizes the same eternal "**Blue Exploit"** that was used by WannaCry.

PROACTIVE:

1. Update your Microsoft OS from Microsoft Site
2. Have a robust backup strategy
3. Update your antivirus
4. Don't open suspicious email or attachments

REACTIVE:

1. Unplug system from network
2. Restore system from backup
3. Report Incident to cerrt.ng
    a. Email: support@cerrt.ng
    b. Phone: 0800 – 9988 – 7766 – 5544
    c. No 28 Portharcourt Crescent, Area 11, Garki – Abuja, Nigeria

REFERENCE:

- http://www.pandasecurity.com/intelligenceplatform/wannasave.htm?gclid=CNONzMHN4NQCFYoQ0wodk6UKcA
- https://en.wikipedia.org/wiki/Petya_(malware)
- https://www.theguardian.com/world/2017/jun/27/petya-ransomwareattack-strikes-companies-across-europe
- https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know