Enterprise Security and Risk Management Advisory- Ransomeware

Connected World.
Connected Experiences.

Document Ownership

Department	Date
Tech Mahindra	Tuesday, June 27, 2017

Date	June 27 2017
Revision	1
Classification	Malware
Type	Ransomeware
Name and Variant	Petya / PetWrap Ransomware

Table of Content

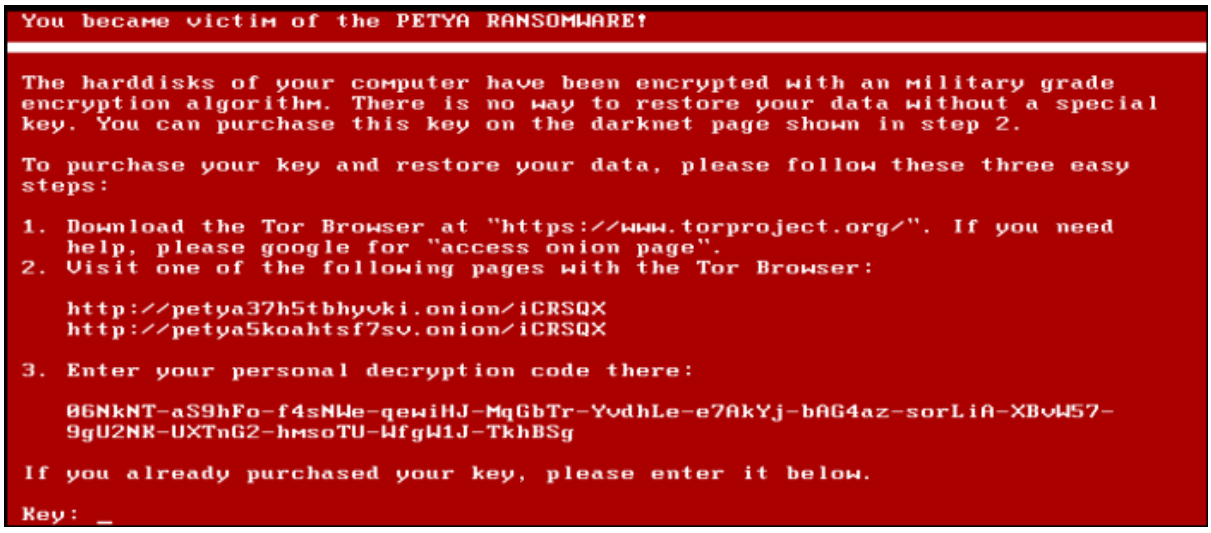
1. Overview

Ransomware-Petya is different than regular ransomware in that upon execution, it infects low-level structure (MBR [Master Boot Record], MFT [Master File Table]) and doesn't allow the computer to boot normally. It will infect MBR and on restart, it has its own low language code to encrypt MFT, which makes the drive inaccessible.

Affected countries: UK, Ukraine, India, the Netherlands, Spain, Denmark, and others

2. Technical Details

Encrypts MFT (Master File Tree) tables for NTFS partitions and overwrites the MBR (Master Boot Record) with a custom bootloader that shows a ransom note and prevents victims from booting their computer.Indicators of Compromise: The below screen shot will be displayed during boot time.



3. Containment

a) Block source E-mail address wowsmith123456@posteo.net
b) Block domains:
- http://mischapuk6hyrn72.onion/
- http://petya3jxfp2f7g3i.onion/
- http://petya3sen7dyko2n.onion/
- http://mischa5xyix2mrhd.onion/MZ2MMJ
- http://mischapuk6hyrn72.onion/MZ2MMJ
- http://petya3jxfp2f7g3i.onion/MZ2MMJ
- http://petya3sen7dyko2n.onion/MZ2MMJ
- http://benkow.cc/71b6a493388e7d0b40c83ce903bc6b04.bin

c) COFFEINOFFICE.XYZ http://french-cooking.com/
d) Block IPs:
- 95.141.115.108
- 185.165.29.78
- 84.200.16.242
- 111.90.139.247

e) Apply patches:
- Refer(in Russian): https://habrahabr.ru/post/331762/

f) Disable SMBv1
g) Update Anti-Virus hashes

- a809a63bc5e31670ff117d838522dec433f74bee
- bec678164cedea578a7aff4589018fa41551c27f
- d5bf3f100e7dbcc434d7c58ebf64052329a60fc2
- aba7aa41057c8a6b184ba5776c20f7e8fc97c657
- 0ff07caedad54c9b65e5873ac2d81b3126754aac
- 51eafbb626103765d3aedfd098b94d0e77de1196
- 078de2dc59ce59f503c63bd61f1ef8353dc7cf5f
- 7ca37b86f4acc702f108449c391dd2485b5ca18c
- 2bc182f04b935c7e358ed9c9e6df09ae6af47168
- 1b83c00143a1bb2bf16b46c01f36d53fb66f82b5
- 82920a2ad0138a2a8efc744ae5849c6dde6b435d
- myguy.xls
  EE29B9C01318A1E23836B949942DB14D4811246FDAE2F41DF9F0DCD922C63BC6
- BCA9D6.exe
  17DACEDB6F0379A65160D73C0AE3AA1F03465AE75CB6AE754C7DCB3017AF1FBD

4. Preventing Ransomeware

Ransomware is one of many types of malware, and the methods for its delivery are common to most other types. **You can minimise the risk of being infected by ransomware by taking the same precautions necessary to guard against malware in general**.

a) Avoid opening attachments in emails from untrusted sources. If your company allows, implement rules to block attachments with common executable extensions.
b) Keep your Antivirus up to date to help avoid other infections that may bring the ransomware to your machine.
c) Windows users should take the following general steps to protect themselves:
   - Apply security updates in MS17-010
   - Block inbound connections on TCP Port 445
   - Create and maintain good back-ups so that if an infection occurs, you can restore your data

5. Precautionary measures

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location.
- Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Only download software – especially free software – from sites you know and trust.
- Enable automated patches for your operating system and Web browser

6. Recommended Steps for Remediation

- **Contact law enforcement. We strongly encourage you to contact a local government agencies like NCSC (National Cyber Security Center), CERT(Computer Emergency Response Team), FBI etc., upon discovery to report an intrusion and request assistance. Maintain and provide relevant logs.**
- **Contact Tech Mahindra ESRM (Enterprise Security and Risk Management) team for implementing Incident response and business continuity plan.**