EC-COUNCIL

NOTPETYA: BRIEFING & ACTION GUIDE

FROM THE DESK OF EC-COUNCIL GROUP CISO

CONTENTS

What is NotPETYA?
(or PETYA)

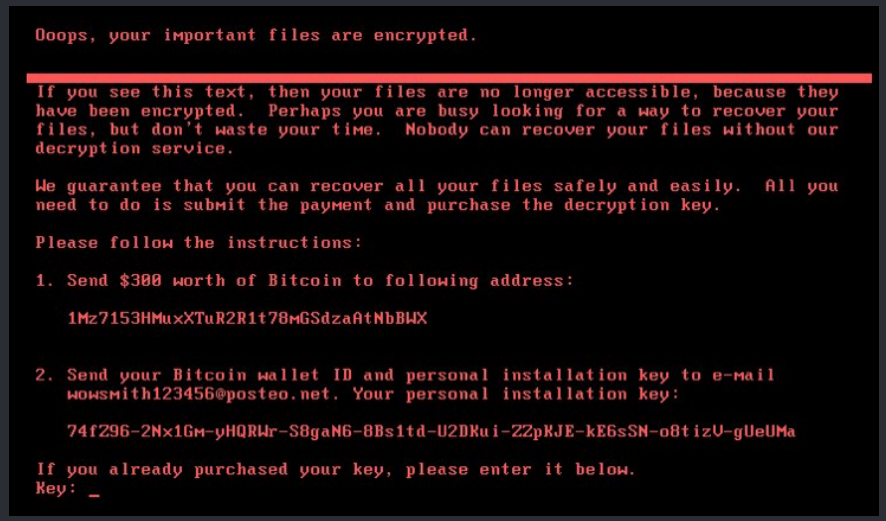
Though the name is similar to ransomware that first appeared in 2016, this is a completely new strain. Hence, researchers have named it NotPetya while others are classifying it as close to
"GoldenEye" malware (Petya + Mischa).

This ransomware spreads through a combined client-side attack (CVE-2017-0199) and network based threat (MS17-010). It spread rapidly using ETERNALBLUE (MS17-010), while it harvested password hashes and psexec as infection vectors from each infected machine.

Infection Process

1. Arrived via an update to an accounting system in Ukraine (ME Doc)
2. 2.Spread like a worm from an infected machine
3. Exploited Windows SMB vulnerability (aka EternalBlue), fix by Microsoft was released (MS17-010)
4. Spreads into the local network using Eternal Blue, psexec , WMIC
5. Encrypts MFT (Master File Tree) tables for NTFS partitions
6. Overwrites the MBR (Master Boot Record) with a custom bootloader
7. Shows a ransom note demanding USD 300, same bitcoin wallet
8. Prevents victims from booting their computer.
9. Hard coded local kill switch

There is no guarantee of recovery of files as the email (wowsmith123456@posteo.net) is no longer valid. This is actually most likely NOT ransomware but instead it is most probably destructive wiper malware disguised as ransomware. Close reading of the code shows there is no way for data to be recovered – only destroyed.



INFECTION PROCESS

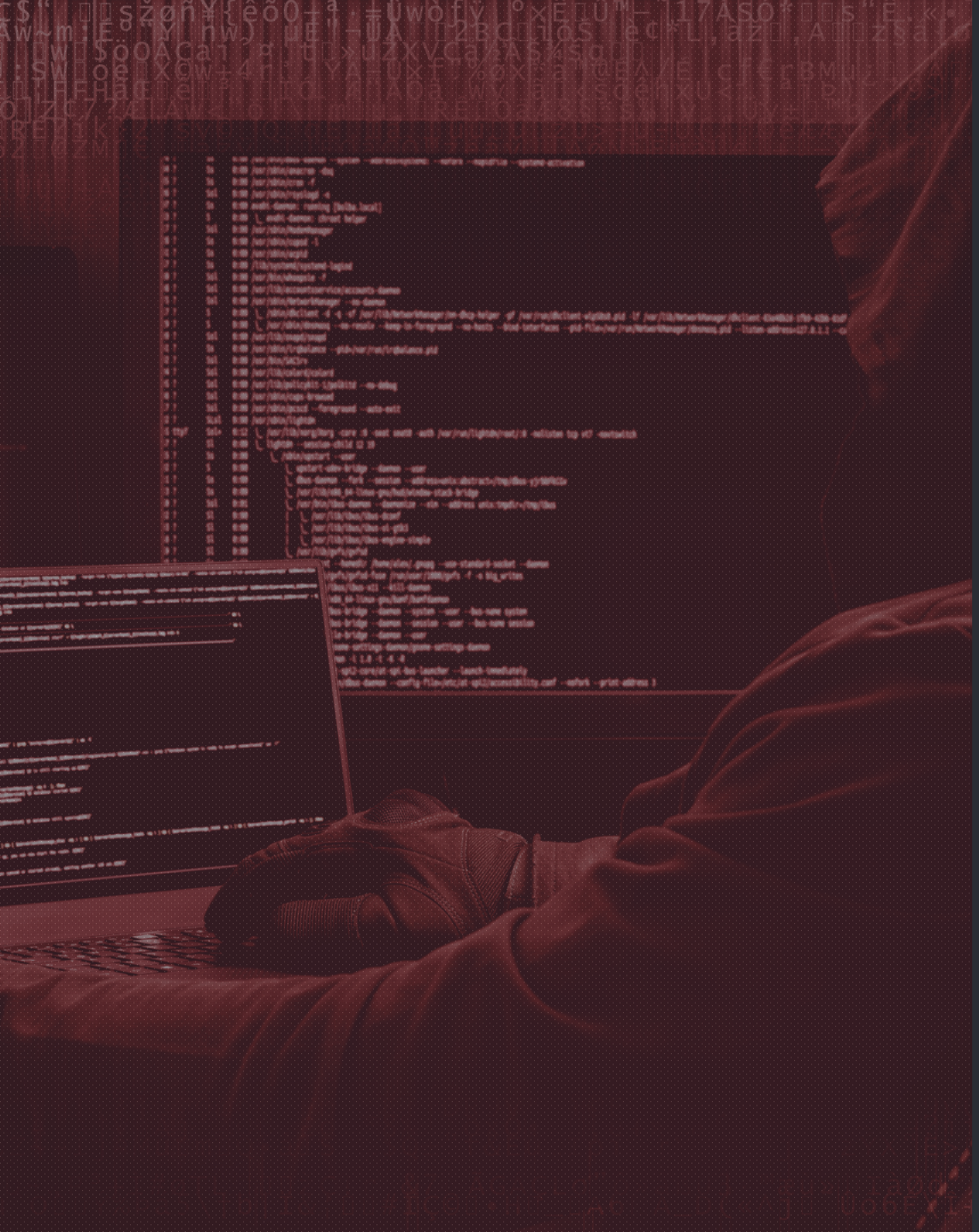
- Arrived via an update to an accounting system in Ukraine (ME Doc)
- Spread like a worm from an infected machine
- Exploited Windows SMB vulnerability (aka EternalBlue), fix by Microsoft was released (MS17-010)
- Spreads into the local network using Eternal Blue, psexec , WMIC
- Encrypts MFT (Master File Tree) tables for NTFS partitions
- Overwrites the MBR (Master Boot Record) with a custom bootloader
- Shows a ransom note demanding USD 300, same bitcoin wallet
- Prevents victims from booting their computer.
- Hard coded local kill switch

No guarantee of recovery of files as the email (wowsmith123456@posteo.net) is no longer valid.

Action Guide

- Improve Detection (Implement IoCs in SoC, where available)
- Updated AV / Anit-Malware systems
- Kill Switch

- **Implement IoCs into SoC and timely incident response**
  - IoCs are detailed
  - Clears the windows event log using Wevtutil
  - Detected indicator that file is ransomware
  - Disable Automatic reboot
  - Prevent local admin privileges for normal user operations
- **Avoid SMB (Port 445) and RDP on servers [Guidance]**
- **Disable SMB1 or Block incoming traffic to port 445**
- **Kill Switch: Create a file in %windir% called perfc.dat , prevents creation of perfc.dat file by Malware. Deny write permissions to perfc.dat .**
- **If infected**
  - Report to law enforcement agencies and ISAC (where applicable)
  - Activate your incident response plan



Indicators of Compromise (IoCs) & Remediation

- Improve Detection (Implement IoCs in SoC, where available)
- Updated AV / Anti-Malware systems

- **Block URLs**
  - 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 COFFEINOFFICE.XYZ
  - http://french-cooking.com/

- **Block IP addresses**
  - 95.141.115.108; 185.165.29.78; 84.200.16.242; 111.90.139.247

- **Update AV Hashes**
  - a809a63bc5e31670ff117d838522dec433f74bee
  - bec678164cedea578a7aff4589018fa41551c27f
  - d5bf3f100e7dbcc434d7c58ebf64052329a60fc2
  - aba7aa41057c8a6b184ba5776c20f7e8fc97c657
  - 0ff07caedad54c9b65e5873ac2d81b3126754aac
  - 51eafbb626103765d3aedfd098b94d0e77de1196
  - 078de2dc59ce59f503c63bd61f1ef8353dc7cf5f
  - 7ca37b86f4acc702f108449c391dd2485b5ca18c
  - 2bc182f04b935c7e358ed9c9e6df09ae6af47168
  - 1b83c00143a1bb2bf16b46c01f36d53fb66f82b5
  - 82920a2ad0138a2a8efc744ae5849c6dde6b435d
  - 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745 (main 32-bit DLL)
  - 64b0b58a2c030c77f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5 (signed PSEXEC.EXE)
  - fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1 (main 32-bit DLL)
  - 02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f (64-bit EXE)
  - eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998 (32-bit EXE)

User Awareness Script

- Phishing
- Attachments
- Respond and Report

Dear Colleagues,

In last few days, a massive cyber attack has infected machines around the world and is demanding ransom to release files. This attack, called "NotPetya," has so far has impacted critical infrastructure sectors like energy, banking, transportation, telecom and other businesses in many countries by infecting a large number of computers.

In this heightened situation, we request you stay vigilant while using your computers. While dealing with any emails from external unknown email addresses, do not click any link or execute any unknown attachments.

We request you to follow best practices while performing your daily operations as outlined below.

Phishing & Attachments:

- Do not open attachments in unsolicited e-mails, even if they come from people in your contact list.
- Do not click on a URL contained in an unsolicited e-mail.
- Use a browser to type URLs or navigate through a URL domain.
- Report any suspicious emails/attachments to the IT or IS team.

House Keeping:

- Adhere to the company computer usage policy.
- Do not download software, videos, MP3s, etc.
- Ensure your anti-virus is updated and running on your machine.
- Backup your critical data periodically.
- Set aside time for updating, patching, and anti-virus updates.
- Use the account with the lowest level of user privileges to complete each task and avoid using accounts with admin Privileges unless necessary.

If Infected, immediately disconnect your machine from the network by pulling the LAN cable and call the information security team. Do not tamper with the machine or data. Do not try to restore your data on your own.

<CISO Signature Block>

REFERENCES

Prepared by Subrahmanya Gupta BODA, Group CISO, EC-Council, C|CISO, gupta.boda@eccouncil.org

Overview

- http://www.telegraph.co.uk/technology/2017/06/27/petya-cyber-attack-everything-know-global-ransomware-outbreak/
- http://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017
- https://www.us-cert.gov/ncas/current-activity/2017/06/27/Multiple-Petya-Ransomware-Infections-Reported
- https://www.binarydefense.com/petya-ransomware-without-fluff/
- https://medium.com/@thegrugq/pnyetya-yet-another-ransomware-outbreak-59afd1ee89d4

Spread / impact

- https://intel.malwaretech.com/

Advisories

- https://www.us-cert.gov/ncas/alerts/TA17-132A
- https://blog.malwarebytes.com/threat-analysis/2016/12/goldeneye-ransomware-the-petyamischa-combo-rebranded/
- https://www.crowdstrike.com/blog/fast-spreading-petrwrap-ransomware-attack-combines-eternalblue-exploit-credential-stealing/

Prevention Scripts

- https://twitter.com/0xAmit/status/879778335286452224

Decryption related

- None found yet

History

- https://blog.malwarebytes.com/threat-analysis/2016/05/petya-and-mischa-ransomware-duet-p1/
- https://securelist.com/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/77762

DISCLAIMER

This briefing is for informational purposes only and should not be utilized as a solution to the NOTPETYA attack. If you believe you have been affected or have questions on how to remediate, reach out to a security consulting company.