Alert (TA17-181A)

More Alerts

Petya Ransomware

Original release date: July 01, 2017 | Last revised: February 15, 2018

Systems Affected

Microsoft Windows operating systems

Overview

This Alert has been updated to reflect the U.S. Government's public attribution of the "NotPetya" malware variant to the Russian military. Additional information may be found in a Statement from the White House Press Secretary. For more information related to NotPetya activity, go to https://www.us-cert.gov/grizzlysteppe.

The scope of this Alert's analysis is limited to the newest Petya malware variant that surfaced on June 27, 2017. This malware is referred to as "NotPetya" throughout this Alert.

On June 27, 2017, NCCIC [13] was notified of Petya malware events occurring in multiple countries and affecting multiple sectors. This variant of the Petya malware—referred to as NotPetya—encrypts files with extensions from a hard-coded list. Additionally, if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable. NotPetya differs from previous Petya malware primarily in its propagation methods.

The NCCIC Code Analysis Team produced a Malware Initial Findings Report (MIFR) to provide in-depth technical analysis of the malware. In coordination with public and private sector partners, NCCIC is also providing additional indicators of compromise (IOCs) in comma-separated-value (CSV) form for information sharing purposes.

Available Files:

- MIFR-10130295.pdf
- MIFR-10130295_stix.xml
- TA-17-181B_IOCs.csv

Description

NotPetya leverages multiple propagation methods to spread within an infected network. According to malware analysis, NotPetya attempts the lateral movement techniques below:

- PsExec - a legitimate Windows administration tool
- WMI - Windows Management Instrumentation, a legitimate Windows component
- EternalBlue - the same Windows SMBv1 exploit used by WannaCry
- EternalRomance - another Windows SMBv1 exploit

Microsoft released a security update for the MS17-010 SMB vulnerability on March 14, 2017, which addressed the EternalBlue and EternalRomance lateral movement techniques.

Technical Details

NCCIC received a sample of the NotPetya malware variant and performed a detailed analysis. Based on the analysis, NotPetya encrypts the victim’s files with a dynamically generated, 128-bit key and creates a unique ID of the victim. However, there is no evidence of a relationship between the encryption key and the victim’s ID, which means it may not be possible for the attacker to decrypt the victim’s files even if the ransom is paid. It behaves more like destructive malware rather than ransomware.

NCCIC observed multiple methods used by NotPetya to propagate across a network. The first and—in most cases—most effective method, uses a modified version of the Mimikatz tool to steal the user’s Windows credentials. The cyber threat actor can then use the stolen credentials, along with the native Windows Management Instrumentation Command Line (WMIC) tool or the Microsoft SysInternals utility, psexec.exe, to access other systems on the network. Another method for propagation uses the EternalBlue exploit tool to target unpatched systems running a vulnerable version of SMBv1. In this case, the malware attempts to identify other hosts on the network by checking the compromised system’s IP physical address mapping table. Next, it scans for other systems that are vulnerable to the SMB exploit and installs the malicious payload. Refer to the malware report, MIFR-10130295, for more details on these methods.

The analyzed sample of NotPetya encrypts the compromised system’s files with a 128-bit Advanced Encryption Standard (AES) algorithm during runtime. The malware then writes a text file on the “C:\” drive that includes a static Bitcoin wallet location as well as unique personal installation key intended for the victim to use when making the ransom payment and the user’s Bitcoin wallet ID. NotPetya modifies the master boot record (MBR) to enable encryption of the master file table (MFT) and the original MBR, and then reboots the system. Based on the encryption methods used, it appears unlikely that the files could be restored, even if the attacker received the victim’s unique key and Bitcoin wallet ID.

The delivery mechanism of NotPetya during the June 27, 2017, event was determined to be the Ukrainian tax accounting software, M.E.Doc. The cyber threat actors used a backdoor to compromise M.E. Doc's development environment as far back as April 14, 2017. This backdoor allowed the threat actor to run arbitrary commands, exfiltrate files, and download and execute arbitrary exploits on the affected system. Organizations should treat systems with M.E.Doc installed as suspicious, and should examine these systems for additional malicious activity. [12]

Impact

According to multiple reports, this NotPetya malware campaign has infected organizations in several sectors, including finance, transportation, energy, commercial facilities, and healthcare. While these victims are business entities, other Windows systems are also at risk, such as:

- those that do not have patches installed for the vulnerabilities in MS17-010, CVE-2017-0144, and CVE-2017-0145, and
- those who operate on the shared network of affected organizations.

Negative consequences of malware infection include:

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization's reputation.

Solution

NCCIC recommends against paying ransoms; doing so enriches malicious actors while offering no guarantee that the encrypted files will be released. In this NotPetya incident, the email address for payment validation was shut down by the email provider, so payment is especially unlikely to lead to data recovery.[1] According to one NCCIC stakeholder, the sites listed below sites are used for payment in this activity. These sites are not included in the CSV package as IOCs.

hxxp://mischapuk6hyrn72[.]onion/
hxxp://petya3jxfp2f7g3i[.]onion/
hxxp://petya3sen7dyko2n[.]onion/
hxxp://mischa5xyix2mrhd[.]onion/MZ2MMJ
hxxp://mischapuk6hyrn72[.]onion/MZ2MMJ
hxxp://petya3jxfp2f7g3i[.]onion/MZ2MMJ
hxxp://petya3sen7dyko2n[.]onion/MZ2MMJ

Network Signatures

NCCIC recommends that organizations coordinate with their security vendors to ensure appropriate coverage for this threat. Given the overlap of functionality and the similarity of behaviors between WannaCry and NotPetya, many of the available rulesets can protect against both malware types when appropriately implemented. The following rulesets provided in publically available sources may help detect activity associated with these malware types:

- sid:2001569, “ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection”[2]
- sid:2012063, “ET NETBIOS Microsoft SRV2.SYS SMB Negotiate ProcessID? Function Table Dereference (CVE-2009-3103)”[3]
- sid:2024297, “ET CURRENT_EVENTS ETERNALBLUE Exploit M2 MS17-010”[4]
- sid:42944,"OS-WINDOWS Microsoft Windows SMB remote code execution attempt"[11]
- sid:42340,"OS-WINDOWS Microsoft Windows SMB anonymous session IPC share access attempt"[11]
- sid:41984,"OS-WINDOWS Microsoft Windows SMBv1 identical MID and FID type confusion attempt"[11]

Recommended Steps for Prevention

Review US-CERT’s Alert on The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations [6], and consider implementing the following best practices:

- Ensure you have fully patched your systems, and confirm that you have applied Microsoft’s patch for the MS17-010 SMB vulnerability dated March 14, 2017.[5]
- Conduct regular backups of data and test your backups regularly as part of a comprehensive disaster recovery plan.
- Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.
- Manage the use of privileged accounts. Implement the principle of least privilege. Do not assign administrative access to users unless absolutely needed. Those with a need for administrator accounts should only use them when necessary.
- Configure access controls, including file, directory, and network share permissions with the principle of least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Secure use of WMI by authorizing WMI users and setting permissions.
- Utilize host-based firewalls and block workstation-to-workstation communications to limit unnecessary lateral communications.
- Disable or limit remote WMI and file sharing.
- Block remote execution through PSEXEC.
- Segregate networks and functions.
- Harden network devices and secure access to infrastructure devices.
- Perform out-of-band network management.
- Validate integrity of hardware and software.

- Disable SMBv1 and block all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139; this applies to all boundary devices.

Note: *Disabling or blocking SMB may create problems by obstructing access to shared files, data, or devices. Weigh the benefits of mitigation against potential disruptions to users.*

Recommended Steps for Remediation

- NCCIC strongly encourages organizations contact a local Federal Bureau of Investigation (FBI) field office upon discovery to report an intrusion and request assistance. Maintain and provide relevant logs.
- Implement a security incident response and business continuity plan. Ideally, organizations should ensure they have appropriate backups so their response is simply to restore the data from a known clean backup.

Report Notice

DHS encourages recipients who identify the use of tools or techniques discussed in this document to report information to DHS or law enforcement immediately. To request incident response resources or technical assistance, contact NCCIC at NCCICcustomerservice@hq.dhs.gov or 888-282-0870. You can also report cyber crime incidents to the Internet Crime Complaint Center (IC3) at https://www.ic3.gov/default.aspx.

References

Statement from the White House Press Secretary
[1] Bleeping Computer: Email Provider Shuts Down Petya Inbox Preventing Victims…
[2] Emerging Threats 2001569
[3] Emerging Threats 2012063
[4] Emerging Threats 2024297
[5] Microsoft: Security Bulletin MS17-010
[6] US-CERT: The Increasing Threat to Network Infrastructure Devices and Recomm…
[7] F-Secure: (Eternal) Petya from a Developer's Perspective
[8] Microsoft |TechNet: New ransomware, old techniques: Petya adds worm capabil…
[9] US-CERT: Ransomware and Recent Variants
[10] Microsoft: Windows 10 platform resilience against the Petya ransomware att…
[11] Talos: New Ransomware Variant "Nyetya" Compromises Systems Worldwide
[12] Talos: The MeDoc Connection
[13] NCCIC is the parent organization of US-CERT
[14] New Ransomware Variant "Nyetya" Compromises Systems Worldwide
Microsoft: Update on Petya Malware attacks
Microsoft: Authorize WMI users and set permissions
Microsoft: Managing WMI Security
US-CERT Alert TA16-091A

Revisions

July 1, 2017: Initial version

July 3, 2017: Updated to include MIFR-10130295_stix.xml file. Substituted TA-17-181B_IOCs.csv for TA-17-181A_IOCs.csv.
July 7, 2017: Included further guidance from Microsoft in the Reference Section
July 28, 2017: Revised multiple sections based on additional analysis provided
February 15, 2018: Added attribution of the NotPetya malware variant to the Russian military and link to White House press statement.

This product is provided subject to this Notification **and this** Privacy & Use **policy.**