RANSOMWAREWORM - WANNACRY

Background:

On Friday, 12th May 2017 a ransomware campaign hit computer systems of private companies and public organizations across the globe. It is believed that ransomware delivery campaign has infected over 2,000,00 (approx) Windows systems worldwide till 15th May 2017.

Ransomware denies access to data/file/folder, by encrypting it. It can delete accessible backups, can spread to other computers in LAN, and encrypt all accessible data including data stored on local hard drives, network drives (file shares) and removable storage media such as USB drives. The principle behind ransomware is devastatingly simple, even if the technical details around new variants grow more complex and sophisticated by the day. The idea is that criminals block access to a system or its data until a certain amount of money is paid by the victim.

The ransomware, known as WannaCrypt, WannaCry, WanaCrypt0r, WCrypt, WCRYt. A total of 16 U.K. organizations have been affected by the ongoing attack, including the National Health Service (NHS), which was forced to reject patients, cancel operations, and reschedule appointments due to WannaCry. Also systems in Russia, Ukraine, India, and Taiwan. Infections are also spreading through the United States. The malware is notable for its multi-lingual ransom demands, which support more than two-dozen languages. Ransom between $300 to $600 is being demanded. There is code to 'rm' (delete) files in the virus, it seems to reset if the virus crashes.

WannaCry Ransomware is leveraging a Windows exploit harvested from the NSA called EternalBlue, which was dumped by the Shadow Brokers hacking group over a month April 2017.

Researchers has found an effective kill switch, which prevented many new infections, and allowed time to patch systems. Malware researchers advise against paying the WannaCryptor Ransomware ransom.

update: *A minor variant of the virus has been found, it looks to have had the killswitch hexedited out. On the other hand that is the only change: the encryption keys are the same, the bitcoin addresses are the same. On the other hand it is corrupt so the ransomware aspect of it doesn't work - it only propagates.*

Affected systems:

Unsupported versions of Windows - Windows XP, Vista, Server 2003 and Server 2008.

Impacted Country / Organisations:

• São Paulo Court of Justice (Brazil) • Vivo (Telefônica Brasil) (Brazil) • Lakeridge Health (Canada) • ATMs in china • PetroChina (China) • Public Security Bureaus (China) • Sun Yat-sen University (China) • Instituto Nacional de Salud (Colombia) • Renault (France) • Deutsche Bahn (Germany) • Telenor Hungary (Hungary) • Andhra Pradesh Police (India) • Dharmais Hospital (Indonesia) • Harapan Kita Hospital (Indonesia) • University of Milano-Bicocca (Italy) • Q-Park (The Netherlands) • Portugal Telecom (Portugal) • Automobile Dacia (Romania) • Ministry of Foreign Affairs (Romania) • MegaFon (Russia)	• Ministry of Internal Affairs (Russia) • Russian Railways (Russia) • LATAM Airlines Group (Chile) • Banco Bilbao Vizcaya Argentaria (Spain) • Telefónica (Spain) • Sandvik (Sweden) • Garena Blade and Soul (Thailand) • National Health Service (England) (United Kingdom) • NHS Scotland (United Kingdom) • Nissan UK (United Kingdom) • FedEx (United States) • Massachusetts Institute of Technology (United States) • Saudi Telecom Company (Saudi Arabia) • CGV (South Korea) • Bus Station (South Korea) Source: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#List_of_affected_organizations

WannaCry / WannaCryptor Ransomware Attack Description:

The WannaCry Ransomware uses the AES-128 encryption to encrypt the victim's files. The WannaCry Ransomware will search for the following file types on the victim's computer, encrypting them during the attack:

.123, .3dm, .3ds, .3g2, .3gp, .602, .7z, .aes, .ai, .ARC, .asc, .asf, .asp, .avi, .backup, .bak, .bmp, .brd, .c, .cgm, .class, .cpp, .crt, .cs, .csr, .csv, .db, .dbf, .dch, .dif, .dip, .doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .dwg, .edb, .eml, .fla, .flv, .frm, .gif, .gpg, .gz, .hwp, .ibd, .jar, .java, .jpeg, .jpg, .js, .jsp, .key, .lay, .lay6, .ldf, .m3u, .m4u, .max, .mdb, .mdf, .mid, .mkv, .mml, .mov, .mp3, .mp4, .mpeg, .mpg, .msg, .myd, .myi, .n, .nef, .odb, .odg, .odp, .ods, .odt, .ost, .otg, .otp, .ots, .ott, .p12, .PAQ, .pas, .pdf, .pem, .php, .pl, .png, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .psd, .pst, .rar, .raw, .rb, .rtf, .sch, .sh, .sin, .slk, .sql, .sqlite3, .sqlitedb, .stc, .std, .stw, .suo, .swf, .sxc, .sxd, .sxm, .sxw, .tar, .tarbz2, .tbk, .tgz, .tif, .tiff, .txt, .uop, .uot, .vb, .vdi, .vmdk, .vmx, .vob, .vsd, .vsdx, .wav, .wb2, .wk1, .wks, .wma, .wmv, .xlc, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .zip.

The WannaCryptor Ransomware is being distributed as a bogus messaging program that is being sent to victims through corrupted email messages. Once the WannaCryptor Ransomware encrypts the victim's data, it will identify the files that have been encrypted by adding the file extension '.wcry' to the end of each file's name. The WannaCryptor Ransomware also will delete the Shadow Volume Copies of affected files, preventing computer users from using this recovery method to recover the files. The WannaCryptor Ransomware delivers its ransom note by changing the infected computer's desktop wallpaper image. The desktop image will be contained in a BMP file named '!WannaCryptor!.bmp' and will display the following message for the victim:

'Ooops, your important files are encrypted.
If you see this text, but don't see the "Wanna Decryptor" window, then your antivirus removed the decrypt software, or you deleted it from your computer.'

This malware modifies files in the /Windows and /windows/system32 directories and enumerates other users on the network to infect. Both of these actions require administrative privileges. Ransomware is writing itself into a random character folder in the 'ProgramData' folder with the file name of "tasksche.exe" or in 'C:\Windows\' folder with the file-name "mssecsvc.exe" and "tasksche.exe".

Risk Assessment

- Remote Access : Remote desktop related string reads terminal service related keys (often RDP related), uses network protocols on unusual ports. Deletes volume snapshots.

- Persistence: Disables startup repair grants permissions using icacls (DACL modification). Modifies auto-execute functionality by setting/creating a value in the registry. Spawns a lot of processes Tries to suppress failures during boot.

- Fingerprint: Dropped file containing the Windows username (possible fingerprint attempt). Reads system information using Windows Management Instrumentation Commandline (WMIC). Reads the active computer name. Reads the cryptographic machine GUID.

- Spreading: Opens the MountPointManager (often used to detect additional infection locations)

Cryptography Details:

- Each infection generates a new RSA-2048 keypair.
- The public key is exported as blob and saved to 00000000.pky
- The private key is encrypted with the ransomware public key and saved as 00000000.eky
- Each file is encrypted using AES-128-ECB, with a unique AES key per file.
- The AES key is encrypted using the infection specific RSA keypair.

Bitcoin ransom addresses:

Addresses hard coded into the malware are as follows:

- https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

C&C centers

- `gx7ekbenv2riucmf.onion`
- `57g7spgrzlojinas.onion`
- `xxlvbrloxvriy2c5.onion`
- `76jdd2ir2embyv47.onion`
- `cwwnhwhlz52maqm7.onion`

Port Protocol Description

- Port 80: Hypertext Transfer Protocol (HTTP)
- Port 443: Hypertext Transfer Protocol over TLS/SSL (HTTPS)
- Port 9001: EMC2 (Legato) Networker or Sun Solstice Backup
- Port 9003: EMC2 (Legato) Networker or Sun Solstice Backup
- Port 9101: EMC2 (Legato) Networker or Sun Solstice Backup

Protection Methods

- Update Your Windows Machines the patch for the Eternalblue (MS17 -010). To protect Windows platforms that are in custom support only, including Windows XP, Windows 8, and Windows Server 2003, download and apply the patch from http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
- Disable SMBv1 as given in https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012
- Block ingress SMB traffic on port 445,Filter all SMB (TCP/445), NetBIOS (TCP/139), and RDP (TCP/3389). Block legacy protocols on the network.
- Update Anti-Virus software
- Do not open mail attachments from unknown or untrusted senders.
- An awareness and training program for end users for dealing this type of attack to successful. Thus, the employees must be aware of the threat including delivery mechanism.
- Disable office macros through a group policy.
- Enable scanning of all attachments at endpoints and email gateways.
- Backing up all important data preferably on a system that is not connected all to any LAN/WAN.
- Allowing only known application signatures to be executed i.e. application whitelisting
- Configuring access controls – including file, directory and network share permissions using least privilege rights assignments.
- Deploying and enabling all end-point protections and keeping all known signature updated.
- Having a proper email policy implemented ensuring safe access.
- Having a Ransomware prevention strategy suited to the business functions.

Impact on Indian CII sector:

Following CII may be vulnerable to WannaCry ransomware due to its inherent vulnerabilities associated with outdated Windows operating systems.

- Banking: ATM based on Windows OS platform may be impacted due to older version of OS.
- Telecom: Server based on windows 2003/2008 may be targeted.
- Government Sector: Systems not updated / patched.
- Transport : Systems used for passenger and cargo reservations may be impacted.
- Heavy industries and Public Enterprises: Unpatched systems deployed for financial transactions and payments.

Conclusion:

Paying a ransom has legal implications and may not guarantee that encrypted files will be decrypted. Adversaries may not provide the keys for decryption, the ransomware might not have the technical capability to decrypt data, or the data might be encrypted/deleted by multiple malacious actors. Requirement of a Ransomware Prevention Strategy is the best tool to future attacks.

Sharing of ransomware attack incidents will prevent the attack to prolifirate and thus creating an environment of cohesiveness and confidence amongst the organisations. It will help in preparing a strategy to protect against such attacks and also helps in making an overall National picture of threat exposure. Kindly contribute for safe and secure Digital India.