Prevention Of Ransomware Infections

Original Issue Date:-November 17, 2016
Update:-September 08, 2022
Virus Type:- Ransomware

It has been observed that "Ransomware malware" attacks are on rise affecting financial institutions, businesses and academic institutions in the country. Ransomware are type of malicious software (malware) that scramble the contents of a computer or server (associated network shares and removable media) and demands payment/ransom to unlock it, usually in the form of anonymous decentralized virtual currency "BITCOINS". Ransomware causes temporary or permanent loss of sensitive or proprietary information, financial losses, and disruption to regular operations and potential harm to an organization's reputation. This Advisory is intended to provide further information about Ransomware, its main characteristics, the proliferation mechanisms and to provide prevention or mitigation measures against ransomware.

Modus Operandi of Ransomware Attacks :

Infection/Propagation

Ransomware is typically spread through spear phishing emails that contain malicious attachments in the form of archived content (zip/rar) containing a JavaScript file. Other possible infection vectors includes drive-by-download attacks, specially crafted web links in emails. Upon visiting such infected/compromised websites or web links, a piece of malware is dropped on victim's machine, which executes itself without user's knowledge. It has also been reported that the ransomware propagates through insecure Remote Desktop connections (RDP). Ransomware attempts to extort money from victims by displaying an extortion alert indicating that their computer has been locked or all files have been encrypted, and demand that a ransom is paid to restore access.

Impact

Ransomware variants are capable of performing following activities:

- Encrypt the specific files present on the infected system, the encryption and the targeted file types varies by ransomware versions, hence make files unusable.
- Capable of infecting or encrypting the files present on network share drives and USB drives.
- Extensions of the unusable /encrypted files depends upon the type of the ransomware, such as ".cerber", ".crypt", ".zepto", ".locky" , ".xtbl", ".vault", "xrtn", "crySIS", ".lock", ".R5A". ".lock", etc.
- Make use of native Windows utilities such as WMIC and/or VSSAdmin to delete backups and shadow copies.
- Demands ransom amount of money for providing the decryption key for the encrypted files.
- Some versions of the ransomware are capable of targeting the databases also by identifying the current running processes and if found any, they kill those processes and thereafter encrypts the database.
- Capable of detecting the virtual machine environments by checking the VM specific file names , paths, hooked modules, known sandbox volume serial numbers, and VM specific DLLs.
- Make network connections to the call back server to send uniquely identifiable system information.
- Make file system and registry changes such as installation of specific windows themes representing ransomware encryption.
- Capable of keeping persistence by creating command processor, screensaver, startup.run and Run Once registry entries.

Paying the ransom does not guarantee that the encrypted files will be released. In addition, decrypting files does not mean the malware infection itself has been removed. It has also been reported that attackers have gone one level deeper by typically targeting the backend databases / backup which stores critical financial data. In contrast with the conventional ransomware methodology, wherein "IN-ONE-GO" encryption of the files /documents is carried out, in the latest attacks, attacker tampers specific fields /records of databases which are sensitive in nature and

subsequently demand ransom, an indication of persistent access to the critical assets of an enterprise network.

Variants

Some of the well-known ransomwares that are spreading widely are :

Black Basta, Hive, Diavol, Egregor, ProLock, Cryptolocker, locky, cerber, zepto, .CryptoHasYou., 7ev3n, Alpha Ransomware, AutoLocky, BandarChor, BitCrypt, Booyah, Brazillian, Chimera, Crybola, Cryptear, CryptFile2, CryptInfinite, CryptoDefense, CryptoHost, CryptoJoker, CryptoMix, CryptoTorLocker, CryptoWall, CryptoXXXC2.0, CTB-Locker, CTB-Locker WEB, DeCryptProtect, DMALocker, Gopher, HydraCrypt, Jigsaw, KeRanger, KEYBTC, KEYHolder, KryptoLocker, Linux.Encoder, Locker, Lortok, NanoLocker, Nemucod, Offline Ransomware, OMG!Ransomware, Operation Global3, PClock, Petya, PornoLocker, PowerWare, Radamant, Rakhni, Ranmoh, Ransom32, Rector, EmindMe, Rokku, scraper, SkidLocker /Pompous, SynoLocker, TeslaCrypt, TorrentLocker, Troldesh, TrueCrypter, UmbreCrypt, VaultCrypt, Virus-Encoder.

Cyber security companies are working on **decryption tools for such encrypted files,** but, till date decryption for only some of the ransomwares are possible. For those files for which the decryption tools are not available, there is no way to retrieve the private key that can be used to decrypt those files. Brute forcing the decryption key is not realistic due to the length of time required to break this type of cryptography. Restoring to earlier operating system state may fail as the malware may delete the volume shadow copies (restore points in windows) as the first step immediately after infection.

Some of the prevalent ransomware variants observed in Indian cyberspace are CryptoLocker, Reveton, CTB-Locker, Cryptowall, Cerber, TeslaCrypt. Ransomwareare evolving in their methods of propagation, encryption, and the targets sought.

CERT-In has issued alerts on ransomware such as Black Basta, Hive, Diavol, Cryptolocker, Locky, Cerberetc etc. The same may be seen on CERT-In website www.cert-in.org.in

Best Practices and remedial measures

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

- 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.
- 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
- 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.
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Application white listing/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.
- Maintain updated Antivirus software on all systems
- 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.
- 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.
- Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.

- Disable remote Desktop Connections, employ least-privileged accounts. Limit users who can log in using Remote Desktop, set an account lockout policy. Ensure proper RDP logging and configuration.
- Restrict access using firewalls and allow only to selected remote endpoints, VPN may also be used with dedicated pool for RDP access
- Use strong authentication protocol, such as Network Level Authentication (NLA) in Windows.
- Additional Security measures that may be considered are
    - Use RDP Gateways for better management
    - Change the listening port for Remote Desktop
    - Tunnel Remote Desktop connections through IPSec or SSH
    - Two-factor authentication may also be considered for highly critical systems
- If not required consider disabling, PowerShell / windows script hosting.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations.
- Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption.
- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level anti-exploitation tools.
- 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
- 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.
- Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to CERT-In and Law Enforcement agencies

Prevention Tools:

- Tool (NoMoreCry) to prevent Wannacry Ransomware by CCN-CERT: https://loreto.ccn-cert.cni.es/index.php/s/tYxMah1T7x7FhND?path=CCN-CERT%20NoMoreCry%20Tool
- Sophos: Hitman.Pro https://www.hitmanpro.com/en-us/content/ransomware-remover
- Bitdefender Anti-Crypto Vaccine and Anti-Ransomware (discontinued) https://labs.bitdefender.com/2016/03/combination-crypto-ransomware-vaccine-released/
- Malwarebytes Anti-Ransomware(formally Crypto Monitor) https://blog.malwarebytes.com/malwarebytes-news/2016/01/introducing-the-malwarebytes-anti-ransomware-beta/
- Trendmicro Ransomware Screen Unlocker tool: https://esupport.trendmicro.com/en-us/home/pages/technical-support/1105975.aspx

Removal Tools:

Download Free Bot Removal Tool

Decryption Methodology and Tools:

Decryption tools for some of the ransomware are available which allows users to decrypt their unusable/encrypted files without paying ransom. Not all tools are capable to decrypt the files, instead users are advised to try the below mentioned decryption tools.

List of decryption tools are mentioned below:

- http://www.avg.com/in-en/ransomware-decryption-tools
- https://noransom.kaspersky.com/
- https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor
- https://decrypter.emsisoft.com/