Crypto Ransomware

Defense Counter Measure Guide

hackmiami

Crypto Ransomware Defense Countermeasure Guide

Published by
HackMIami
@hackmiami
www.hackmiami.org

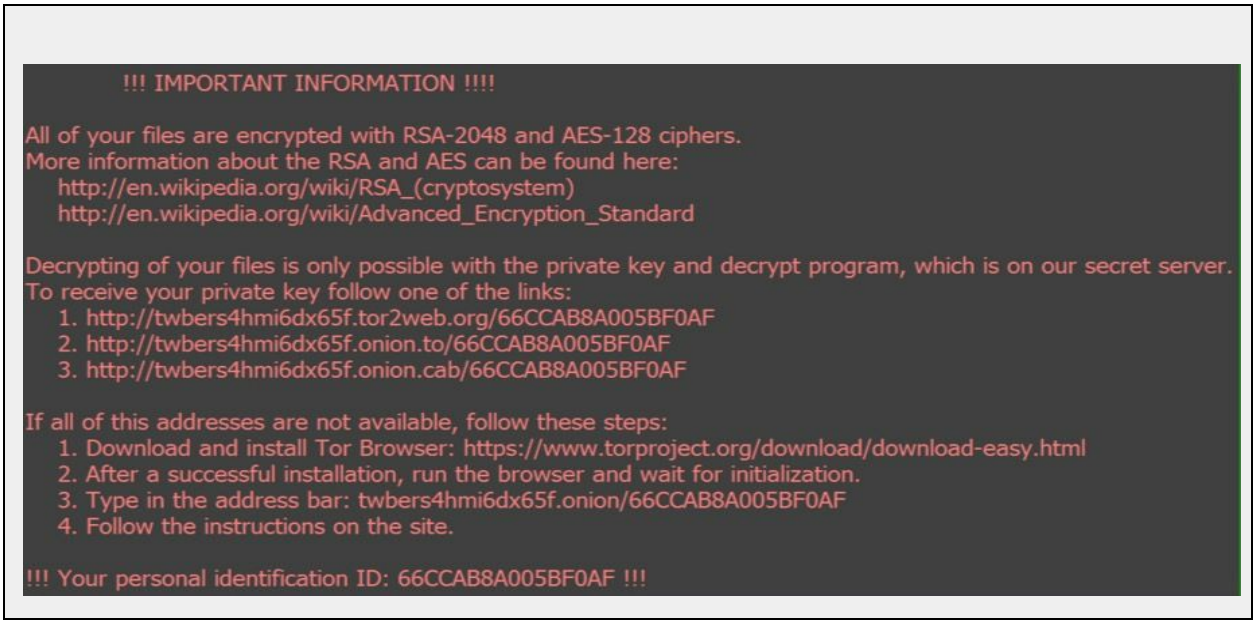
Background

Crypto ransomware is a variant of malicious software (or malware) that denies access to data on a system by encrypting user data and crucial system files. A message is displayed to victims demanding ransom payment in order to provide keys to decrypt the files and return the affected system and files to a usable state. Ransomware will also attempt to encrypt files on attached and network storage.

Current modus operandi of malicious actors consists in delivering ransomware payload via email attachments (MS Office documents are the preferred delivery files), drive by download on rogue or compromised websites, or in some cases removable media. Some of the variants of crypto ransomware actively damage operating system backup mechanisms in order to prevent victims from restoring their systems. This is done by removing any Volume Snapshot Service files (Also known and Volume Shadow Copy Files). It has also been observed that network shares, mapped and unmapped, can be affected as well.

After installation and entrenchment, victims are presented with messages demanding payment in order to decrypt their files. Malicious actors prefer the use of digital currencies, specifically bitcoin as a means of paying ransom. Bitcoin is a decentralized digital currency that provides malicious actors some level of anonymity and ability to obfuscate the flow of ransom payments, making it more difficult to be traced.

Fig. 1 - Examples of messages on infected systems demanding ransom with payment instructions.



As seen in the above figure (**Figure 1**), victims are directed to make payment, often by visiting a website hosted on the TOR network, where the instructions on how to pay the ransom will be provided. Malicious actors will then request a specific number of bitcoins. In some cases, the malicious actors will also specify a deadline where if payment is not sent then ransom will increase.

The following guide provides pointers to prevent, remediate and understand infection and entrenchment process of Crypto Ransomware. Remediation of these threats must be approached considering specific malware variant indicators of compromise and behavior. It is also recommended that affected parties seek help before considering paying ransom. It has also been reported that even after paying ransom some files and systems have not been completely restored leaving victims' computers with corrupted or partially returned files - or complete data loss.

Filing a claim at the FBI Internet Crime Complaint Center (IC3) can also help law enforcement, industry, and the general public, in fighting ransomware campaigns and mitigating the risk of further infestation.

Technical details of infection/entrenchment and indicators of compromise (IOC) have been referenced as hyperlinks to make this guide brief and concise. Please refer to the last page for a full list of URL references.

The following items are proposed as guidelines to facilitate understanding of Crypto Ransomware infection/entrenchment/infestation process, remediation and prevention measures. The malware threatscape is very dynamic and constantly develops new features to defeat mitigation and remediation measures by developing new variants as well as mixing Crypto ransomware with other types of malware.

Identification

It is important to identify the variant of ransomware that has infected the system, as well as to confirm that your files are in fact encrypted. Some types of ransomware simply lock up your system or web browser. In the case of crypto malware, it is possible that a security firm or AV vendor has developed a decryptor tool that can enable you to decrypt your files without paying a ransom.

The following online tool can be used to help identify the ransomware by uploading a sample of an encrypted file and a copy of the file that contains the ransom note (payment instructions): https://id-ransomware.malwarehunterteam.com.

Infection/ Entrenchment (IOC Indicators) Most popular versions as of current time. An extensive list of ransomware can be found here.

- TeslaCrypt
- Locky (Said to be developed/distributed by Dridex Creators)
- CTB-Locker (Critroni or Curve-Tor-Bitcoin)
- CryptoLocker (Delivered as part of Zbot variant)
- Petya (Encrypts Master Boot Record)
- Coverton
- Maktub
- Samsam (Infestation associated to mass JBOSS exploitation campaign)
- CryptXXX (Said to be related to Reveton, delivered via Angler EK)

Warning: Please seek technical help before attempting remediation, as mishandling of these procedures may render your data and system unusable.

Remediation

- Disconnect the machine from the network (wireless and/or wired)
- Disconnect any external storage devices, such as attached hard drives (if they have not yet been encrypted)
- Disable any cloud storage services. If files in cloud storage have already been encrypted you may be able to restore previous versions of your files (Dropbox, Google Drive, OneDrive) after you have removed the ransomware or restored your system.
- Advise users not to connect any laptops nor connect to wifi until the situation has been handled.
- Review your system backups. Hopefully you have your full system or at least your important data backed up to a backup server, backup service, or backup drive. Determine if your backup data is recent and complete. The cleanest solution is to wipe the infected system and restore from your backups.
- ONLY delete the virus from the appdata folder if you are sure you will never pay the ransom (Verify IOC before attempting).
- Locate one of the following known registry locations for a list of infected files (CryptoLocker)
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "CryptoLocker_<version_number>"
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce "*CryptoLocker_<version_number"
- Export list of encrypted files
- Create a script and run it against your backup to recover files
- Wipe/Reload infected machine and educate that user on how to prevent it from happening again
- If MBR has been infected and no key is available, only offline/offsite backup following complete wipe of system will eliminate threat.
- Cisco Talos Ransomware technical guide
- Current removal/prevention tools http://www.techworld.com/security/7-best-ransomware-removal-tools-how-clean-up-cryptolocker-cryptowall-extortion-malware-3626974/

- Petya Ransomware decryption Tutorial
    - This tutorial includes a combination of tools designed to aid in recovering the key that is required to decrypt the affected hard drive. Requires removal of infected disk in order to read certain values from the boot sector.

Additional Resources

Open Source Intelligence:

- ***Abuse.ch Ransomware Tracker (https://ransomwaretracker.abuse.ch/tracker/)***

  This is an invaluable resource that can aid in the identification and remediation of infection sources of certain ransomware families. Information such as payment sites, distribution sites and Command and Control servers are distinguished through this tracker.

Known Decryptors:

- Nemucod .CRYPTED
- Xorist Family
- Tesla Crypt
- Locker
- Rakhni
- Radaman Family
- CoinVault/BitCryptor
- CrypBoss Family (HydraCrypt, UmbreCrypt)

Prevention Methods

- Hardcopy backups recommended when possible.
- Maintain several backups, including off-site and/or offline backups.
- Backup and System restore in windows systems.
    - *(System restore may need to be disabled in certain malware cleanups in order to completely get rid of specific malware)*
- Ramsonware can also install and spread via removable media. Enforce removable media sanitization and restriction policies.
- Patch and update systems.
- Enforcement of Minimal privilege in users will prevent malware install and network share and file encryption. (Principle of least privilege).
- Network segmentation may prevent further malware spread.
- Educate end users not to click on ads/popups/etc. Bookmark trusted sites. Do not open unsolicited attachments.
- If possible DISABLE Macros in Microsoft Office or apply Microsoft suggested macro control procedures (Link).
- Block macros in files originating from the Internet and external email systems (Office 2016)
- When viewing attachments use Microsoft User viewers as they enable document viewing without enabling Macros.

Prevention Tools

- VoodooShield
- Improved spam filters

    - Barracuda
    - OpenDNS
    - Spamassassin
- Malwarebytes Anti-Ransomware
- Bitdefender Free Protection Tool install
- Defeating Ransomware with EventSentry & Auditing (Free Tool)- EventSentry
- Ransomware protection guide (Applocker) - Microsoft
- Cryptoprevent - Foolishit
- Remove Unnecessary Software
- Use no-script (Firefox Add-on)
- RansomWhere? Prevention tool for OS X.

Full Reference URLs

- Ransom malware costs $18 million in losses, says FBI - ZDNet
- Analysis of the CryptoCurrency Marketplace (2013) - HackMiami
- Tor - Torproject
- VoodooShield - VoodooShield
- Federal Bureau of Investigation Internet Crime Complaint Center - IC3
- Threat Spotlight: TeslaCrypt – Decrypt It Yourself - Cisco
- Look Into Locky Ransomware - MalwareBytes
- Threat Intelligence - New Locker: Prison Locker (aka: Power Locker ..or whatever those bad actor call it) - MalwareMustDie
- Crypto Ransomware - US-Cert
- Ransomware and Recent Variants - US-Cert
- CTB-Locker Ransomware Spreading Rapidly, Infects Thousands of Web Servers - TheHackerNews
- http://www.healthcareitnews.com/news/more-half-hospitals-hit-ransomware-last-12-months - HealthCare IT News
- Ransomware - TrendMicro
- Threat Refinement Ensues with CryptoLocker, SHOTODOR Backdoor - TrendMicro
- Targeted Ransomware - No Longer a Future Threat (PDF) - IntelSecurity
- https://www.proofpoint.com/us/threat-insight/post/cryptxxx-new-ransomware-actors-behind-reveton-dropping-angler ProofPoint
- RakhniDecryptor utility for removing Trojan-Ransom.Win32.Rakhni malicious software (.oshit and others) - Kaspersky
- Radamant Ransomware Decrypted, Files Can Be Retrieved for Free - SoftPedia
- Decrypter for HydraCrypt and UmbreCrypt available - EmsiSoft
- Microsoft Enhances Group Policy Controls for Office 2016 Macro Threats - Redmondmag
- Block Macros from Internet Office 2016 - Microsoft Malware Protection Center
- How to install Bitdender's free Ransomware Protection Tool - CyberArms
- The 7 best ransomware removal tools - how to clean up Cryptolocker, CryptoWall and extortion malware - Techworld
- Security Tips to Protect Against Ransomware - Microsoft
- Ransomware: Past, Present, and Future - Talos Intel
- Petya Ransomware's Encryption Defeated and Password Generator - BleepingComputer
- Malwarebytes Anti-Ransomware 0.9.14.361 Download - BleepingComputer
- Locker Unlocker v.1.0.5.0 - BleepingComputer
- Emsisoft offering decryption services for the Xorist Ransomware Family - BleepingComputer
- Paying the Coverton Ransomware May Not get your Data Back - BleepingComputer
- The Art of the Maktub Locker Ransomware - BleepingComputer
- Decryptor Released for the Nemucod Trojan's .CRYPTED Ransomware - BleepingCompute

- How to prevent ransomware: What one company learned the hard way - Pcworld
- Ransomware Tracker

Contributors

Rod Soto @rodsoto
Mauricio Tunnermann @taocyn
Gregory Lindor @_g3nuin3
Nathalie Vaiser @natv
David McEwan @mackhiami
Tim Krabec @tkrabec
Javier V.M. Bruno @_deftoner_

About HackMiami

HackMiami is the premier partnership resource in South Florida for information security services such as vulnerability analysis, penetration testing, digital forensics, and on-site training.

HackMiami seeks to develop and harness the participation of the global information security community through regular events, presentations, labs and competitions. These events allow the hacker community a forum to present their research, develop new techniques and methodologies, and at the same time provides a valuable networking resource for contracting opportunities. HackMiami events and research have been featured multiple times by prominent mainstream media outlets.

For more information on the HackMiami 2016 Conference, visit http://www.hackmiami.com
For more information on the HackMiami organization, visit http://www.hackmiami.org