



NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Ransomware: Lucrative Cyber Crime Tactics Rapidly Evolving

July 7, 2015

TLP: **WHITE** | The NJCCIC assesses ransomware infections will continue to increase steadily and pose a threat to the public and private sector, as well as home users, as the technical barriers to conduct these cybercrime campaigns continue to drop and the return on investment for cybercriminals remains extremely high. Ransomware variants are likely to increasingly target mobile devices as users rely more heavily on tablets and smartphones, and also bundle with additional malware designed to steal login credentials and financial information. Moreover, the tactics used to distribute malware through spam emails or compromised websites are becoming more sophisticated, as are anti-forensic capabilities that enable malware to delete themselves after infection in order to avoid detection, extraction, and examination. *The NJCCIC recommends all organizations and home users familiarize themselves with ransomware tactics and implement the necessary security and backup strategies to mitigate this threat.*

Threat Overview

Ransomware is a type of malicious software (malware) that attempts to extort money from victims by restricting access to a computer system or files. The most prevalent form of this profit-motivated malware, referred to as crypto-ransomware due to the use of encryption algorithms, is on the rise as many new variants are being developed by hackers and international cybercrime groups. The security firm Symantec reported a 112 percent increase in ransomware attacks in 2014, largely due to a 4,000 percent increase in crypto-ransomware infections.¹ In the first quarter of 2015, ransomware infections rose 165 percent according to McAfee Labs.²

- The steady increase in ransomware is largely driven by more elusive variants of crypto-ransomware that rely on the Tor anonymity network for command and control (C2), as well as the use of online currency, namely Bitcoin, for anonymously accepting ransom payments. Some of the most recent strains posing a threat to US businesses and home users include CryptoWall 3.0, the CTB-Locker ransomware family, two similar strains called TeslaCrypt and Alpha Crypt, and TorrentLocker.³
- Since April 2014, the FBI's Internet Crime Complaint Center (IC3) has received 992 Cryptowall-related complaints, with victims reporting losses totaling over \$18 million. The potential losses for victims goes beyond the ransom fee to recover files, and may include network mitigation and other IT services, loss of productivity, legal fees, and credit monitoring for victims.⁴
- There is an expanding marketplace for off-the-shelf cybercrime tools that allow average users with limited technical ability to distribute malware and conduct for-profit cyber attacks. A ransomware kit named Tox was released in early 2015 that allows any internet user to enter a ransom amount and reason for their campaign, then download a ransomware executable file disguised as a Microsoft screensaver file (.scr) to send to potential victims. The tool provided a user interface to track the number of victims and total profits from paid ransom.⁵

How Ransomware Works

Ransomware infections occur when a user opens a malicious email attachment, clicks on a malicious link, or visits a website infected with malicious code, known as a drive-by download.

Once a system is infected, the ransomware contacts a command and control (C2) server to generate an encryption key and begins encrypting files on the victim's machine.

The ransomware runs quietly in the background performing in-depth searches of all disk folders, including removable drives and network shares, and encrypts as many files as it can.³

- Ransomware may also delete shadow volume copies and destroy restore points to prevent victims from recovering their files and systems without paying the ransom.
- If a system is powered off as files are being encrypted, some ransomware will resume where it left off when the system or device is powered on again.

After files are encrypted, a ransom note is displayed on the screen with instructions on how and where to pay the ransom, and the length of time before the hacker destroys the decryption key.

- Some recent variants offer victims a 'second chance' to pay after the initial timer expires; however, the 'second chance' is often at least double the original ransom amount.

If the victim pays the ransom, the malware is supposed to contact the C2 server for the decryption key and begin decrypting the victim's files, however, in many cases the files are never decrypted.

- Some ransomware files can delete themselves in order to avoid detection and analysis by security researchers or law enforcement.

Ransomware Variants

The following are examples of crypto-ransomware strains currently impacting businesses, governments, and home users in the US and worldwide. All of the samples below target the Windows operating system and the majority only accept ransom payment in Bitcoin, demonstrating the shift to crypto-currency for anonymity and to inhibit forensic analysis by researchers and law enforcement.

TeslaCrypt emerged in February 2015 and is spread via exploit kits such as Angler, Sweet Orange, or Nuclear. In addition to scanning all system drives for files to encrypt, including removable drives, network shares, and DropBox mappings, TeslaCrypt attempts to delete all Volume Shadow Copies and system restore points to prevent the recovery of files. TeslaCrypt is also able to detect if it is running in a virtual environment before fully executing in order to prevent analysis by security and law enforcement. Files encrypted by TeslaCrypt display an .ecc or .exx extension. In addition to Bitcoin, ransom payment is accepted via PayPal My Cash.⁶

- The Talos Group from Cisco offers a tool to decrypt files encrypted by TeslaCrypt, available [here](#).

Alpha Crypt appeared soon after TeslaCrypt in April 2015 and the two use a nearly identical graphical user interface (GUI) and behave similarly deleting files Volume Shadow Copy Service (VSS) to prevent file recovery, however Alpha Crypt appears to be spread only via the Angler exploit kit. Files encrypted by Alpha Crypt will display an .ezz extension and a text file ransom note is created in each folder where files are encrypted and displayed as the wallpaper on the desktop.⁷

CTB-Locker (Curve-Tor-Bitcoin-Locker), also known as Critroni, appeared in 2014 and was the first crypto-ransomware to use the Tor network for C2. CTB-Locker is spread through drive-by downloads using exploit kits on compromised web pages, as well as spam email with .zip or .cab attachments. The ‘Curve’ portion of the name refers to the use of elliptic curve cryptography to encrypt files. The following extensions may be added to files encrypted by CTB-Locker: .ctbl, .ctb2, or random characters such as .ftelhdd or .ztswgmc.⁸

CryptoWall emerged in the US in early 2014 and has evolved to the current version of Cryptowall 3.0, which relies on the Tor network for C2 and checks to see if it is running on a virtual machine to prevent analysis by researchers. CryptoWall is spread through spam email attachments or drive-by downloads from compromised websites, and exploits Microsoft privilege escalation vulnerability CVE-2013-3660 to gain greater control of the infected system. Encrypted files will gain a .cryptowall extension.⁹

TorrentLocker also appeared in early 2014 and although it identifies itself as CryptoLocker, it is not related. TorrentLocker is most commonly spread via spam emails relating to unpaid invoices, package delivery, and unpaid speeding tickets. Once executed, malware files are installed in the %AppData%, %Temp%, or %WinDir% folders of the infected system, all system drives and network shares are scanned for files to encrypt, and all Shadow Volume Copies are deleted to prevent data restoration. Files encrypted by Torrentlocker will display an .encrypted extension.¹⁰

CoinVault was released in November 2014 and is part of the CryptoGraphic Locker ransomware family. CoinVault infects users who open a ‘.zip’ file attachment from spam email. Files encrypted by CoinVault gain a .clf extension. CoinVault uniquely allows victims to decrypt one file for free to prove that it can do so and attempt to persuade victims to pay the ransom.¹¹

- Security firm Kaspersky Labs offers a tool to decrypt files encrypted by CoinVault, available [here](#).

Locker appeared for a short period in May 2015 after remaining dormant on infected machines after a trojan downloader was installed via malicious advertising. Locker remained inactive on infected PCs until activated by the malware developer. Once executed, Locker deleted Shadow Volume Copies and added a ‘7z.encrypted’ extension to encrypted files. The developer later apologized for the ransomware and announced an automatic decryption process starting on 2 June 2015.¹²

VirLock is a polymorphic worm with file infecting capabilities, in addition to both ransomware tactics of locking the infected computer’s screen and encrypting files. Files encrypted by VirLock gain an .exe extension. Because VirLock is polymorphic, it continuously changes its code each time it runs to avoid detection and make it difficult for researchers to analyze it.¹³

- Security firm ESET offers a tool to decrypt files encrypted by VirLock, available [here](#).

VaultCrypt is a crypto-ransomware that also seeks to steal user data, and although it has only affected victims in Russia thus far, English language payment instructions were circulated suggesting it may soon spread to Western targets. VaultCrypt is spread via spam emails or drive-by downloads, and also bundled into openly available software. It uses a Windows batch file using Visual Basic scripts and Gnu Private Guard (GnuPG) to encrypt data, adding a .vault extension to encrypted files. Once executed, VaultCrypt extracts the victim’s login credentials stored in web browsers and sends the stolen data back to its control server. After the encryption process finishes, VaultCrypt deletes itself.¹⁴

Troldesh, also identified by the names Encoder.858 or Shade, is another variant that has primarily targeted Russian users thus far, however, an English translation was added to the ransom message suggesting it may soon expand to Western countries. Troldesh is spread via spam email and adds an .xtb extension to encrypted files. The cybercriminals responsible for Troldesh provide an email address that victims can contact and attempt to negotiate down the price of the decryption key.¹⁵

Mobile Ransomware: The first case of ransomware targeting mobile devices was detected in 2014, targeting Google's Android OS. The ransomware file, Android.Trojan.SLocker.DZ, is spread via spam emails with .zip file attachments and does not encrypt files on the phone, instead it disables the home screen and back buttons on the device and displays an FBI warning on the infected device. Ransom payment is demanded via MoneyPal or PayPal MyCash, rather than Bitcoin.¹⁶

Ransomware Mitigation

While ransomware infections may not be entirely preventable due to the effectiveness of well-crafted spear-phishing emails or drive-by downloads from otherwise legitimate sites, the most effective strategy to mitigate the impact of ransomware is having a comprehensive data backup protocol.

- Schedule backups of data often and ensure they are kept offline in a separate and secure location.
- If an online backup and recovery service is used, contact the service immediately after a ransomware infection is suspected to prevent previous file versions from becoming overwritten with the newly encrypted versions.
- Ensure anti-virus software is up-to-date with the latest definitions and scheduled to run scans as often as permitted.
- Enable automated patches for operating systems, software, and web browsers.
- Follow the Principle of Least Privilege for all user accounts; enable User Access Control (UAC) to prevent unauthorized changes.
- Use web and email protection to block access to malicious websites and scan all emails, attachments, and downloads.
- Close and monitor unused ports.
- Use ad blocking extensions in browsers to prevent "drive-by" infections from ads containing malicious code.
- Configure systems by modifying the Group Policy Editor to prevent executables (.exe, .rar, .pdf.exe, .zip) from running in %appdata%, %localappdata%, %temp% and the Recycle Bin.
- Alert the appropriate information security contact within your organization if unusual activity is seen on networks, computers, or mobile devices.
- Disconnect from networks immediately if an infection is suspected and don't reconnect until the computer or device has been thoroughly scanned and cleaned.
- If an infection occurs, after removing the malware and cleaning the machine, make sure to change all system, network, and online account passwords.
- For Apple iOS users: ensure your data is backed up on iCloud and enable two-factor authentication; only download media and apps from the official iTunes and App Stores; avoid 'jailbreaking' the device.⁴
- For Android users: disable the "unknown sources" option in the Android security settings menu and only install apps from the official Google Play store; avoid "rooting" the device.

Reporting

If your organization is the victim of a ransomware infection, or would like to learn more about the NJCCIC, please contact a Cyber Liaison Officer at njccic@cyber.nj.gov or visit www.cyber.nj.gov.

Sources

- ¹ Symantec. "Internet Security Threat Report 2015". Symantec. April 2015. URL: <https://know.elq.symantec.com/LP=1542>.
- ^{2,3} McAfee Press Release. "McAfee Labs Report Sees New Ransomware Surge 165 Percent in First Quarter of 2015". June 2015. URL: <http://www.mcafee.com/us/about/news/2015/q2/20150609-01.aspx?clickid=QAgwANzc91791P1wUCSLmTPLUkVS-OzLyxhy2Y0&lqmcate=Affiliate:IR:null:74047:10078:10078:null>.
- ⁴ Internet Crime Complaint Center. "CRIMINALS CONTINUE TO DEFRAUD AND EXTORT FUNDS FROM VICTIMS USING CRYPTOWALL RANSOMWARE SCHEMES". Fbi. 23 June 2015. URL: <http://www.ic3.gov/media/2015/150623.aspx>.
- ⁵ Walter, Jim. "Meet 'Tox': Ransomware for the Rest of Us". McAfee Labs. May 23, 2015. URL: <https://blogs.mcafee.com/mcafee-labs/meet-tox-ransomware-for-the-rest-of-us>.
- ^{6,7} Abrams, Lawrence. "TeslaCrypt and Alpha Crypt Ransomware Information Guide and FAQ". Bleeping Computer. May 2015. URL: <http://www.bleepingcomputer.com/virus-removal/teslacrypt-alphacrypt-ransomware-information#tesla>.
- ⁸ Abrams, Lawrence. "CTB Locker and Critroni Ransomware Information Guide and FAQ". Bleeping Computer. 29 January 2015. URL: <http://www.bleepingcomputer.com/virus-removal/ctb-locker-ransomware-information>.
- ⁹ Kirk, Jeremy. "CryptoWall ransomware variant has new defenses". PC World. 8 January 2015. URL: <http://www.pcworld.com/article/2867132/cryptowall-ransomware-variant-has-new-defenses.html>
- ¹⁰ Kaspersky Labs. "TorrentLocker Ransomware". Kaspersky Labs. 2015. URL: <http://www.kaspersky.com/internet-security-center/threats/torrentlocker-malware>
- ¹¹ Abrams, Lawrence. "CTB Locker and Critroni Ransomware Information Guide and FAQ". Bleeping Computer. 25 April 2015. URL: <http://www.bleepingcomputer.com/virus-removal/coinvault-ransomware-information#CryptoWall>
- ¹² Neagle, Colin. "Ransomware Creator Apologizes for 'Sleeper' Attack, Releases Decryption Keys". Network World. June 2015. URL: <http://www.networkworld.com/article/2929492/security0/ransomware-creator-apologizes-for-sleeper-attack-releases-decryption-keys.html>.
- ¹³ Trend Micro. "VIRLOCK Combines File Infection and Ransomware". Trend Micro. 13 March 2015. URL: <http://blog.trendmicro.com/trendlabs-security-intelligence/virlock-combines-file-infection-and-ransomware/>
- ¹⁴ Dinkar, Diwakar and Sharma, Rakesh. "VaultCrypt Ransomware Hides Its Traces While Stealing Web Credentials". McAfee Labs. April 2015. URL: <https://blogs.mcafee.com/mcafee-labs/vaultcrypt-ransomware-hides-its-traces-while-stealing-web-credentials>.
- ¹⁵ Neal, Dave. "Ransomware Attackers Open to Negotiation to Release Encrypted Files". V3.co.uk. June 2015. URL: <http://www.v3.co.uk/v3-uk/news/2411546/ransomware-attackers-open-to-negotiation-to-release-encrypted-files>.
- ¹⁶ Sword, Alexander. "Bitdefender: Android Ransomware Uses Fake FBI Porn Warning". Computer Business Review. May 2015. URL: <http://www.cbronline.com/news/mobility/security/bitdefender-android-ransomware-uses-fake-fbi-porn-warning-4585753>.

Traffic Light Protocol: **WHITE** information may be distributed without restriction.