NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Ransomware: An Enduring Risk to Organizations and Individuals

February 12, 2016

TLP: **WHITE** | ***The NJCCIC assesses with high confidence that many businesses, schools, government agencies, and home users will remain at high risk of ransomware infections throughout 2016, as financially-motivated hackers continue to innovate and expand the targeting scope of their extortion campaigns.*** The most prevalent form of this profit-driven malware is known as crypto-ransomware, referring to the use of encryption to render files locked until a ransom is paid to release a decryption key. The observed increase in ransomware infections and development of new variants over the last two years illustrates the attractive incentives for criminal hackers, as the perceived return on investment outweighs the risk of attribution and prosecution. In recent months, numerous cybersecurity firms released threat predictions for 2016, with universal agreement that ransomware and other forms of cyber extortion would not only continue to increase, but expand into new digital territories. In addition to personal devices such as tablets and smartphones, hackers will probably target other Internet-connected devices including home automation systems, smart appliances, vehicles, and medical devices. Likewise, servers, websites, and cloud solutions are also at risk, particularly for those who outsource data storage and management to third-party vendors with poor cybersecurity practices.

- The tactics used to distribute ransomware often involve cunning social engineering tactics, such as carefully crafted phishing emails, designed to manipulate as many unsuspecting victims as possible to maximize profit. Other infection vectors include exploit kits, drive-by downloads, malvertising, and botnets.
- The developers and propagators of ransomware are able to obscure their identities and reduce the likelihood of attribution using a variety of tactics. Most variants of ransomware now rely on the Tor anonymity network for command and control, as well as the use of cryptocurrency, namely Bitcoin, for anonymously accepting ransom payments. In addition to built-in anti-forensic capabilities designed to avoid detection and forensic examination, newer variants attempt to eliminate data recovery options by encrypting additional connected drives and network shares, deleting Shadow Volume Copies and system restoration points, and even overwriting free disk space.
- Demonstrating the effectiveness of ransomware and the damages a single campaign can inflict, the Cyber Threat Alliance reported that the CryptoWall 3.0 variant infected hundreds of thousands of victims worldwide and netted criminals $325 million in less than one year. In 2015, Microsoft reported that it had removed ransomware infections from 24,000 computers after updating malware signatures in its Malicious Software Removal Tool. Furthermore, in the 2015 Kaspersky Security Bulletin, the cybersecurity company reported the detection of ransomware on over 50,000 computers on corporate networks, double the amount they detected in 2014.
- There is an expanding marketplace for customizable, user-friendly ransomware tools, ransomware-as-a-service offerings, and affiliate programs that allow average users with limited technical ability to distribute malware and conduct for-profit cyberattacks. In 2015, a ransomware kit named Tox was released that allowed any Internet user to distribute and profit from ransomware. Although the developer of Tox ultimately put the kit up for sale fearing discovery by law enforcement, other hackers quickly filled the void by offering affiliate programs that promised shared profit to anyone who distributes the ransomware to more victims.

For many organizations, ransomware may not be entirely preventable; however, the impact of a successful infection can be greatly reduced if a robust data backup process is in place. Comprehensive data backups should be scheduled as often as possible and must be kept offline in a separate and secure location. The most effective method to prevent ransomware infections is to conduct regular training and awareness exercises with all employees to ensure users are proficient in safe Internet-browsing techniques and the ability to identify phishing emails.

- For more information on current ransomware variants impacting US victims, including resources, indicators, decryption tools (if available), and mitigation recommendations, see our Ransomware Threat Profile.

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

How Ransomware Works

1. 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.
2. Once a system is infected, the ransomware contacts a C2 server to generate an encryption key and begins encrypting files on the victim's machine.
3. 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.
   - Ransomware may also delete Shadow Volume Copies, destroy restore points, and overwrite free disk space 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 variants resume where they left off when the system or device is powered on again.
4. 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 or software 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.
5. 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 Mitigation Strategies

While ransomware infections may not be entirely preventable due to the effectiveness of well-crafted 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. In order to increase the likelihood of preventing ransomware infections, organizations must conduct regular training and awareness exercises with all employees to ensure common understanding safe-browsing techniques and how to identify and avoid phishing attempts.

The following is a list of ransomware mitigation recommendations:

Data Protection:

- Schedule backups of data often and ensure they are kept offline in a separate and secure location. Consider maintaining multiple backups in different locations for redundancy. Test your backups regularly.
- If an online backup and recovery service is used, contact the service immediately after a ransomware infection is suspected to prevent the malware from overwriting previous file versions with the newly encrypted versions.

System Management

- Ensure anti-virus software is up-to-date with the latest definitions and schedule scans as often as permitted.
- Enable automated patches for operating systems, software, plugins, and web browsers.
- Follow the Principle of Least Privilege for all user accounts; enable User Access Control (UAC) to prevent unauthorized changes.
- Turn off unused wireless connections.
- Disable macros on Microsoft Office software.
- Use ad blocking extensions in browsers to prevent "drive-by" infections from ads containing malicious code.
- Disable the vssadmin.exe tool by renaming it to prevent ransomware from deleting Shadow Volume Copies. Instructions on how to rename this tool are included here.
- Disable Windows Script Host and Windows PowerShell.
- Use web and email protection to block access to malicious websites and scan all emails, attachments, and downloads and configure email servers to proactively block emails containing suspicious attachments such as .exe, .vbs, and .scr.

- 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. CryptoPrevent is a free tool that can help automate this process and prevent ransomware from executing. Download it here.

Network Management

- Keep firewall turned on and properly configured.
- Close and monitor unused ports.
- Block known malicious Tor IP addresses. A list of active Tor nodes updated every 30 minutes can be found here.

Mobile Device Management

- 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, and avoid “jailbreaking” the device.
- For Android users: disable the “unknown sources” option in the Android security settings menu, only install apps from the official Google Play store, and avoid "rooting" the device.

Post-Infection Remediation

- 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 do not 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.

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 at njccic@cyber.nj.gov or visit www.cyber.nj.gov.

Appendix

7ev3n targets the Windows OS and spreads via spam emails containing malicious attachments, as well as file sharing networks. It installs multiple files in the %LocalAppData% folder, each of which controls different functions including disabling bootup recovery options, deleting the ransomware installation file, encrypting data, and gaining administrator privileges. This variant also adds registry keys that disables various Windows function keys such as F1, F3, F4, F10, Alt, Num Lock, Ctrl, Enter, Escape, Shift, and Tab. Files encrypted by 7ev3n be labeled with a .r5a extension. This variant is unique in that it demands 13 bitcoins as payment, the largest ransom amount demanded thus far in a variant (bitcoin to US dollar conversion fluctuates daily, available here). It also locks victims out of Windows recovery options making it challenging to repair the damage done by 7ev3n.

- The NJCCIC is not aware of any decryption tools available for 7ev3n.
- Bleeping Computer provides information on repairing damage done to a system after a 7ev3n infection, found here.

Alpha Crypt targets all versions of the Windows OS and spreads via the Angler exploit kit. It creates a randomly named executable file in the %AppData% folder and then performs a scan for all available drives, including removable media, network shares, and DropBox mappings. Once all drives are located, it begins locking files using AES encryption and deletes Shadow Volume Copies to prevent data restoration. Files encrypted by Alpha Crypt will display .ezz as their extension. It also creates a text file ransom note in each folder that contains encrypted files and changes the desktop wallpaper image to the ransom note as well. Payment is accepted only in the form of bitcoin. Alpha Crypt has a graphical user interface (GUI) that is nearly identical to TeslaCrypt, according to Bleeping Computer.

- Files encrypted by Alpha Crypt may be decrypted using the TeslaDecoder tool, found here, if the decryption key is present on the infected system and has not been destroyed.

Chimera targets Windows OS and spreads via spear-phishing emails containing a link to a URL or a Dropbox file that hosts malicious downloads. Chimera then encrypts all files on the target system as well as data stored on mapped network drives, changing the file extensions to .crypt. Once that process is complete, Chimera displays a ransom note that threatens to release victims' private data online if they do not pay. If payment is made, Chimera transfers the decryption key from the C2 server to the infected system using Bitmessage, a peer-to-peer (P2P) messaging application. The ransomware also offers victims the ability to become part of their "affiliate program" by helping infect other systems. Despite threats made by Chimera's note, researchers determined that this ransomware does not have the capability of publishing victims' files.

- Malwarebytes provides more information about Chimera, found here.
- The NJCCIC is not aware of any decryption tools available for Chimera.

CoinVault is part of the CryptoGraphic Locker ransomware family and targets Windows OS. It spreads via spam emails containing infected .zip file attachments disguised as PDF files. Files encrypted by CoinVault gain a .clf extension. It allows victims to decrypt one file for free as the decryption function is included in the executable file. Victims impacted can find a list of encrypted files labeled "CoinvaultFileList.txt" in their infected system's temp folder.

- Bleeping Computer provides more information about CoinVault, found here.
- Security firm Kaspersky Labs offers a tool to decrypt files encrypted by CoinVault, available here.

CrypBoss is a family of ransomware that includes the **HydraCrypt** and **UmbreCrypt** variants. This family targets Windows OS and is distributed via the Angler Exploit Kit. They all delete Shadow Volume Copies to prevent file restoration and use AES encryption to lock victims' files. Differences include appended file extensions (.hydracrypt_ID_[8 random characters] and .umbrecrypt_ID_[victim_id]) and the way in which the ransom notes are written. HydraCrypt threatens to release victims' private data on the Dark Web.

- Emsisoft offers a decryption tool for files encrypted by HydraCrypt and UmbreCrypt, available here. Instructions on how to use the tool are available here.
- MakeUseOf provides more information about the CrypBoss family of ransomware, available here.

CryptoJoker targets Windows OS and spreads via spam and phishing campaigns. It infects systems by disguising the installation file as a PDF. Once the executable is launched, it maintains persistence, contacts its C2 server, terminates various processes, deletes Shadow Volume Copies, disables Windows startup repair, scans all mapped drives, and encrypts files using AES-256 encryption. Once encrypted, affected files will display the .crjoker extension.

- Bleeping Computer provides more information about CryptoJoker, found here.
- The NJCCIC is not aware of any decryption tools available for CryptoJoker.

CryptoWall, a successor to the now-defunct CryptoLocker, targets Windows OS and spreads via spam, drive-by downloads, malvertising campaigns, and exploit kits such as Nuclear and Angler. Once it has been executed on a system, it maintains persistence, escalates privileges, destroys all system restore points, and deletes all Shadow Volume Copies to prevent file restoration before beginning the encryption process. **CryptoWall 4.0** is the latest variant and operates much like its predecessors; it continues to connect to compromised websites in order to download the payload, uses RC4 encryption, and it still uses Tor to direct victims to payment instructions. However, one of the most notable differences is that CryptoWall 4.0 not only encrypts files, but it also encrypts *file names* to prevent victims from identifying and restoring them from backups.

- Talos Intel provides more information about CryptoWall 4.0, found here.
- The NJCCIC is not aware of any decryption tools available for the CryptoWall variants.

CTB-Locker (Curve-Tor-Bitcoin-Locker), also known as Critroni, was the first crypto-ransomware to use the Tor network for C2. It targets all versions of Windows and, beginning in mid-2015, it specifically targeted users looking to upgrade to the Windows 10 OS. 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, according to a post on Bleeping Computer.

- The NJCCIC is not aware of any decryption tools available for CTB-Locker.

DecryptorMax, also known as CryptInfinite, targets Windows OS and spreads via malicious Word documents masquerading as resumes in spam emails. The infection occurs when a recipient opens the attached file and enables the macros. Files locked by DecryptorMax display .crinf as the file extension. Additional capabilities include deleting all Shadow Volume Copies and disabling Windows Startup Repair. DecryptorMax changes the victim's desktop wallpaper to an image of the ransom note. Payment is accepted via PayPal MyCash voucher codes.

- Bleeping Computer provides more information on DecryptorMax, found here.
- Emsisoft offers a decryption tool for files encrypted by DecryptorMax, available here.

FBI MoneyPak Ransomware targets Mac OS X, iOS, and Windows OS and uses JavaScript code to hijack Safari, Chrome, Firefox, and Internet Explorer web browsers. The infection occurs when a victim visits a website that contains modified JavaScript code which the browser then tries to execute. The code creates an iframe loop and rapidly loads the same ransom note repeatedly, preventing the victim from leaving the website or exiting the application. This strain of ransomware does not actually encrypt any files on infected devices.

- Malwarebytes provides instructions on how to remove FBI MoneyPak Ransomware from your browser, found here. Makeusof.com also provides removal instructions, found here.

Hidden Tear targets Windows OS and is the first open-source, modifiable ransomware kit. It uses AES encryption and claims to be undetectable by antivirus software. Its developers advertise its release as being "only for educational purposes" but one hacking group has already been discovered using a modified version of the ransomware to infect victims. Files encrypted by Hidden Tear will gain a .locked file name extension.

- The Register provides more information about Hidden Tear, found here.
- The NJCCIC is not aware of any decryption tools available for Hidden Tear.

Koler targets Android OS and spreads via infected websites and SMS messages designed to trick recipients into clicking on a malicious link hidden behind a URL shortener. It blocks the device screen with a persistent window showing a fake law enforcement warning and a demand for payment in the form of MoneyPak prepaid debit cards. Despite ransom note claims, Koler does not actually encrypt any files on the device.

- Information on how to remove Koler from an Android device can be found here.

Linux.Encoder targets Linux servers and Linux-based websites as it encrypts MySQL, Apache, and root folders. It exploits a flaw in Magento, an open-source content management system application designed for e-commerce sites. Files locked by Linux.Encoder display .encrypted as the file name extension. There are currently three versions of this ransomware.

- The best method for preventing a Linux.Encoder infection is to update Magento. The latest version of Magento can be found here.
- Bitdefender offers a Linux.Encoder decryption tool which can be downloaded here.
- DrWeb.com provides more detailed information about this ransomware, found here.

Lockdroid.E targets Android OS and is distributed through software downloaded from third party app stores. Disguised as a video player app, this variant uses clickjacking to gain administrative privileges on the infected device. It then encrypts data and changes the PIN code so the victim is no longer able to access the device. Additionally, Lockdroid.E threatens to delete all of the victim's data and publish the victim's browsing history to contacts stored within the device if the ransom is not paid.

- More information about Lockdroid.E can be found here.
- The NJCCIC is not aware of any decryption tools available for Lockdroid.E.

LockerPIN targets Android OS and is distributed through software downloaded from third party app stores. It is disguised as a software update embedded in a fake video player and, once installed, it gains administrative privileges and changes the PIN code so the victim is no longer able to access the device. The new PIN code set by the ransomware is never revealed to the victim, even if the ransom is paid. It maintains persistence by preventing deletion and disabling antivirus software.

- Information on how to remove LockerPIN from an Android device is available in post on Sensors Tech Forum, here. LockerPIN may not be able to be removed in all cases.

Locky targets Windows OS and its attack vector mimics that of the notorious banking Trojan, Dridex. It is distributed via phishing emails containing Word documents embedded with a malicious macro. If the victim opens the attachment and enables the macros to run, Locky downloads to the victim's system and begins encrypting various files including pictures, videos, source code, and Microsoft Office files, changing the extension to .locky when finished. Additionally, Locky encrypts files on mounted devices and accessible network shares. In a unique twist, Locky even encrypts Bitcoin wallet files, if present on the infected system, to give victims holding a large Bitcoin balance added incentive to pay the ransom. Lastly, it deletes Shadow Volume Copies to prevent file recovery.

- Sophos Labs provides more information about Locky here.
- The NJCCC is not aware of any decryption tools available for Locky.

NanoLocker targets Windows OS and spreads through spam email containing a malicious attachment disguised as a PDF file. When the victim clicks on the attachment, the ransomware displays a fake error and then begins encrypting files silently in the background. It uses a run-time generated AES-256 key to encrypt the files. This key is stored locally to a file on the victim's hard drive before it is encrypted using an RSA public key providing a short window of opportunity for the victim to capture the key file and use a decryption tool without having to pay the ransom. Unique to this variant, NanoLocker communicates with its C2 server using ICMP packets and demands a very low ransom amount – from 0.1 to 0.25 BTC (approximately $43 to $110 USD).

- Malware Clipboard provides more information about NanoLocker, available here.
- Bleeping Computer also provides information about NanoLocker, available here.
- A decryption tool for NanoLocker can be downloaded from Google Drive here; however, this tool will only work if the key is located before the encryption process is complete. The source code and additional information for the tool is located at GitHub here.

PadCrypt targets Windows OS and spreads through spam email containing an executable script disguised as a PDF file. Once installed, PadCrypt encrypts all data that resides in the targeted folders as well as on local drives and changes their file extensions to .ETC. It also deletes Shadow Volume Copies to prevent file recovery. PadCrypt is the first variant that comes with its own "Live Chat Support" feature for victims to contact the ransomware developer directly in order to navigate through the ransom payment process. In some instances, the developer may use it to initiate contact with the victim. It downloads its own uninstaller that can remove the malware but will not decrypt the encrypted files.

- Bleeping Computer provides more information about PadCrypt, available here.
- The NJCCIC is not aware of any decryption tools available for PadCrypt.

Power Worm targets Windows OS and is written in Windows PowerShell which it uses to deliver its payload. It is most commonly spread via spam email containing malicious code. Power Worm deletes Shadow Volume Copies and, due to a programming error, also destroys its own decryption key resulting in unrecoverable files even if victims do choose to pay the ransom.

- Bleeping Computer provides more information about Power Worm, available here.
- The NJCCIC is not aware of any decryption tools available for Power Worm.

Radamant targets Windows OS and is distributed via the Rig exploit kit. It creates auto-run registry keys to establish and maintain persistence, contacts its C2 servers, scans all drives, deletes Shadow Volume Copies, and encrypts targeted files using AES-256. Encrypted files will display either the .RDM (first version) or .RRK (second version) file extensions. Radamant is also part of a ransomware kit that can be rented as a service from its developer for $1,000 per month.

- Emsisoft offers a decryption tool for affected files bearing the .RDM and .RRK extensions, available here. Instructions on how to use this tool are available here.

Ransom32 currently targets Windows but can easily be repackaged to affect Mac and Linux operating systems as it is based on JavaScript. It uses the NW.js (formerly node-webkit) framework designed for web and desktop applications to infect victims and spreads via spam containing a malicious compressed 32 MB RAR file. Once a system is infected, Ransom32 creates a shortcut named "ChromeService" in the Startup folder to maintain persistence. After using Tor to establish a connection to its C2 server, it exchanges keys, encrypts the victim's files using AES-128, and displays a ransom note. Ransom32 is part of a "ransomware-as-a-service" campaign and its creators offer customized versions for a 25 percent cut of the profits.

- Emsisoft provides more information about Ransom32, found here.
- The NJCCIC is not aware of any decryption tools available for Ransom32.

Simplelocker, which is Tor-enabled mobile device ransomware, targets Android OS and spreads through a Trojan downloader masquerading as a legitimate application. Once installed, it scans the device for various file types and encrypts them using AES, changing the file extensions to .enc. It also collects information like the IMEI number, device model, and manufacturer and sends it to a C2 server. Newer versions access the device camera and display a picture of the victims to scare them into paying the ransom.

- Information on how to remove Simplelocker from an Android device can be found here.

TeslaCrypt targets all versions of the Windows OS and spreads 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 Shadow Volume Copies and system restore points to prevent file recovery. 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 currently display the following extensions: .aaa, .abc, .ccc, .ecc, .exx, .micro, .mp3, .ttt, .vvv, .xxx, .xyz, .zzz. In addition to Bitcoin, ransom payment is accepted via PayPal My Cash, according to a post on Bleeping Computer.[6] There are multiple variants of TeslaCrypt currently in circulation.

- The Talos Group from Cisco offers a tool called TeslaDecrypt to decrypt files encrypted by some versions of TeslaCrypt. The Windows binary version can be found here and a Python script is available for download here.
- Another decryption tool called TeslaDecoder from BleepingComputer.com can be found here.
- Talos provides more information about TeslaCrypt, found here.
- Additional free tools specific to the removal of TeslaCrypt 3.0 can be downloaded here.

TorrentLocker targets Windows OS and, although sometimes it identifies itself as CryptoLocker, it is not related. This ransomware 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.

- Sophos Labs provides more information about TorrentLocker, found here.
- Bleeping Computer provides more information about TorrenLocker, found here.
- The NJCCIC is not aware of a decryption tool available for TorrentLocker.

VirLock is a polymorphic worm with file infecting capabilities that targets Windows OS and has the ability to lock the infected computer's screen and encrypt 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, according to Trend Micro.

- Security firm ESET offers a tool to decrypt files encrypted by VirLock, available here.

XRTN targets Windows OS and encrypts files with RSA-1024 encryption using Gnu Privacy Guard (GnuPG) encryption software. XRTN spreads through spam emails containing malicious attachments disguised as Word documents. Once a victim opens the attachment, a JavaScript file executes and proceeds to download a GnuPG executable file, an actual Word document, and a batch file designed to encrypt files. It then deletes all Shadow Volume Copies and overwrites free disk space to prevent file restoration. It also adds the .xrtn extension to all encrypted files.

- Bleeping Computer provides more information about XRTN is available here.
- The NJCCIC is not aware of any decryption tools available for XRTN.