NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

# Ransomware: An Enduring Risk to Organizations and Individuals

**October 27, 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. Enterprise administrators managing Microsoft Office 2016 should use Group Policy to block macros for end users. Microsoft provides detailed instructions here.
- 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.
- Disable Remote Desktop Protocol (RDP) on systems and servers if it is not needed in your environment.
- 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.
- Implement a behavior blocker to prevent ransomware from executing or making any unauthorized changes to systems or files.
- Consider utilizing a free or commercially available anti-ransomware tool by any of the leading computer security software vendors.
- To counteract ransomware variants that modify the Master Boot Record (MRB) and encrypt the Master File Table (MFT), Cisco Talos has released a Windows disk filter driver called MBRFilter, available on GitHub here.
- For Mac OS X users, consider installing the free tool, *RansomWhere?* Information about this tool is available on the Objective-See website here and the tool itself can be downloaded 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.
- Depending on the variant, a free decryption tool may be available. To determine which variant infected your system, please see the Appendix of this product or use the ID Ransomware website.
- 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

**777** targets Windows OS and currently, the method of distribution is unknown. Very little is known about this variant as of yet but early reports state that it appends .777 to the encrypted file extensions, does not delete Shadow Volume Copies, and demands a ransom of $1500 USD. As more is discovered about 777, it will be added to this entry.

- Bleeping Computer provides more information about 777 here.
- Emsisoft offers a decryption tool for files encrypted by 777 here.

**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 are 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 most recent version, **7ev3n-HONE$T**, operates in much the same was as its predecessor, but uses different lock screens and drops its ransom demand to 1 bitcoin.

- Bleeping Computer provides information on repairing damage done to a system after a 7ev3n infection, found here. Information about 7ev3n-HONE$T is available here.
- Decryption tools for 7ev3n-HONE$T are available on GitHub, here.
- Additional decryption tools for 7ev3n are available here and here.

**8lock8** targets Windows OS, is based on Hidden Tear, and is distributed via malicious attachments in spam emails and through file sharing networks. It uses AES-256 to encrypt files and appends *.8lock8* to the file names. After the encryption process is complete, 8lock8 creates a ransom note named *READ_IT.txt* and places it in each folder that contains the encrypted files.

- PC Risk provides more information about 8lock8 here.
- Bleeping Computer provides a free decryption tool for 8lock8 within its forums here.

**Alma Locker** targets Windows OS and is distributed via the RIG exploit kit. Once executed, it targets specific files and encrypts them using AES-128. Alma Locker creates a unique 8-character victim ID by combining the serial number of the C:\ drive and the MAC address of the first network interface. It appends a random 5-character extension to encrypted files. Alma Locker claims to allow its victims to decrypt test files for free but the link for decryption currently leads to an internal server error. Alma Locker currently demands a ransom payment of 1 Bitcoin to be paid within five days.

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

**Alpha** targets Windows OS and, currently, the method of distribution is unknown. Once installed, it places its main executable file in %APPDATA%\Windows\svchost.exe and creates an autorun file named “Microsoft” which allows the encryption process to continue through system reboots. Alpha encrypts files using AES-256 and creates a ransom note named “Read Me (How Decrypt) !!!!.txt.” Alpha is selective about which files it encrypts, targeting files located on the Desktop, within the My Pictures folder, and the Cookies folder on the C: drive. On non-system drives, Alpha encrypts everything except .ini files. It will encrypt everything, however, within shared folders. Encrypted files display .encrypt as their extension. Alpha demands a ransom payment of $400 USD in iTunes gift cards.

- Bleeping Computer provides more information about Alpha here and here.

- A decryption tool for Alpha is available from Bleeping Computer 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.

**AnonPop** is malware designed to look like ransomware, claiming to encrypt files and demanding a ransom payment from the victim. However, AnonPop deletes files rather than encrypting them and then displays a JPG image of the ransom note and payment instructions. It targets Windows OS and is distributed via phishing emails masquerading as complaints from the Office of the Attorney General. These phishing emails contain ZIP files labeled complaint376878.zip that deliver a malicious batch file designed to look like a PDF file. When launched, the batch file abuses PowerShell commands to install additional malware, some of which is designed to maintain persistence on the infected machine and cause a system shutdown. AnonPop deletes files from user profile folders, program files folders, the temp folder, as well as files saved to the desktop. It will also delete files from mapped drives. Fortunately, it does not overwrite the deleted files so data recovery is possible by either restoring Shadow Volume Copies or using a data recovery tool. AnonPop demands a ransom payment of $125 USD within the first 24 hours, $199 USD after 24 hours, and threatens to delete all files and the operating system after 72 hours.

- Bleeping Computer provides more information about AnonPop, including removal and file restoration instructions, here.

**Apocalypse** targets Windows OS and the method of distribution is currently unknown. Once installed, this variant stores itself on c:\Program Files (x86)\windowsupdate.exe, creates an autorun file named "Windows Update Svc," and proceeds to encrypt targeted files. Apocalypse appends all encrypted files with the following extensions: *.encrypted*, *.SecureCrypted*, *.bleepYourFiles*, *Wheres_my_files.txt*, or *.F***YourData* (expletive removed). The ApocalypseVM version appends encrypted files with either *.encrypted* or *.locked*. The Al-Namrood version appends files with the extension *.unavailable* and it primarily infects servers via Remote Desktop Protocol (RDP). The lock screen that Apocalypse displays after the encryption process can be bypassed by booting the infected system into Safe Mode with Networking.

- Bleeping Computer provides more information about Apocalypse here and here.
- Emsisoft provides a decryption tool for Apocalypse, available here.
- Emsisoft provides a decryption tool for ApocalypseVM, available here.
- Emsisoft provides a decryption tool for Al-Namrood, available here.

**AutoLocky** targets Windows OS and, currently, the method of distribution is unknown. The malware's icon, though, was designed to look like an Adobe PDF icon so researchers speculate that it is distributed via phishing emails. It tries to impersonate the more familiar Locky variant by appending .locky to encrypted files but it differs in its style of ransom note and does not use Tor to contact its C2 servers. AutoLocky is written in AutoIt, an open-source scripting language used for automation in Microsoft Windows. Although it does use strong, AES 128 encryption, it does not delete Shadow Volume Copies on infected systems allowing for file recovery without paying the ransom. AutoLocky demands a 0.75 Bitcoin ransom to decrypt files.

- Bleeping Computer provides more information about AutoLocky here.
- Emsisoft offers a decryption tool for files encrypted by AutoLocky, available here.

**BadBlock** targets Windows OS and is distributed via websites containing malicious Javascript or exploit kits delivering fake Adobe Flash Player updates, as well as through malicious email attachments. Researchers note that this variant is so poorly coded that it not only encrypts data files, but it also encrypts Windows system files and executables, rendering the system completely unusable if it is rebooted after infection. BadBlock also displays a ransom note during encryption, allowing the victim to terminate the process *badransom.exe* in Task Manager and prevent further file encryption. It demands a ransom payment of 2 Bitcoin.

- Bleeping Computer provides more information about BadBlock here.
- Emsisoft offers a free decryption tool for BadBlock, available here.

**Bandarchor** targets Windows OS and is distributed via the Neutrino exploit kit and through malicious email attachments. The first stage of a Bandarchor infection is the download of a dropper encrypted with a custom crypter. The second stage is the decryption of the crypter. Bandarchor then injects a copy of itself into the system's memory and begins encrypting the victim's files using AES-256. Bandarchor makes HTTP POST request to its C2 server in order to retrieve encryption keys. All files encrypted by Bandarchor display the following file extension format: .id-[ID]_[EMAIL_ADDRESS]. The email address displayed in the filenames is that of the attacker behind the campaign. The ransom payment demand for Bandarchor is currently unknown.

- ReaQta provides more information about Bandarchor here.
- The NJCCIC is not currently aware of any decryption tools available for Bandarchor.

**Bart** targets Windows OS and is distributed via email attachments containing JavaScript that, when opened, installs RockLoader, a malware dropper that attackers have also used to infect victims with Locky and Dridex. Once downloaded, Bart will only run if the infected system language is not Russian, Ukrainian, or Belorussian. After the language check is complete, Bart begins encrypting targeted files and locking them into a password-protected ZIP file, appending each with a .zip extension. It is important to note that Bart does not connect to any C2 server prior to, during, or after the encryption process. Therefore, firewall configurations designed to block such traffic will not prevent this variant from encrypting files. It is recommended to block Bart at the email gateway by blocking zipped executables. Bart demands a ransom payment of 3 Bitcoin.

- ProofPoint provides more information about Bart here.
- The NJCCIC is not aware of any decryption tools available for Bart.

**BitStak** targets Windows OS and the method of distribution is currently unknown. Once executed, BitStak encrypts files in the following folders: Program Files, Program Files (x86), Documents, Downloads, Videos, Music, Pictures, as well as those on the Desktop and within mapped network drives. During the encryption process, this variant renames each affected file and folder with a random letter combination and appends all encrypted files with the extension .bitstak. BitStak demands a ransom payment of 0.07867 Bitcoin and threatens to delete files if payment is not received within three days.

- Bleeping Computer provides more information about BitStak here.
- Bleeping Computer also provides a free decryption tool for BitStack here.

**Black Shades** targets Windows OS and, although the current distribution method has not yet been verified, it is believed to be distributed as fake videos, cracks, and patches. Once it is executed on a system, it deletes Shadow Volume Copies to prevent file restoration. Black Shades then determines the victim's IP address, creates a unique victim ID, and checks for Internet access. If it is unable to connect to the website http://icanhazip to verify the victim's IP address, the program will crash. It encrypts targeted files using AES-256 and drops a file containing the victim ID, named YourID.txt, in each folder. Black Shades appends all encrypted files with the extension .silent and keeps a running tally of files on its C2 server. After the encryption process is completed, Black Shades attempts to delete itself from the infected system. This variant is unique in that its ransom demand is very low at $30 USD and it accepts payment via both PayPal and Bitcoin.

- Bleeping Computer provides more information about Black Shades here.

- The NJCCIC is not aware of any decryption tools available for Black Shades.

**Bucbi**, a ransomware family that was first released in 2014, has recently been seen in circulation again. It targets Windows OS and, although it was previously distributed via exploit kits or phishing emails, Bucbi is now being delivered via brute-force attack on Remote Desktop Protocol (RDP) accounts located on Internet-connected remote desktop servers running Windows. Once the target server is compromised, the ransomware executable file is dropped and launched. It then encrypts all files on the local drives, with the exception of those located in C:\WINDOWS, C:\Windows, C:\Program Files, and C:\Program Files (x86). Bucbi does not change or append the file extensions of encrypted files and, instead, uses the GOST block cipher – a Russian government standard symmetric key block cipher – to generate unique file names. Bucbi demands a ransom payment of 5 Bitcoin.

- Palo Alto Networks provides more information about Bucbi here.
- The NJCCIC is not aware of any decryption tools available for Bucbi.

**Central Security Treatment Organization** (CSTO) targets Windows OS and its method of distribution is currently unknown. Once a system is infected, CSTO collects information such as the Windows OS version and bit-type, the current service pack, the user and computer names, as well as the type of CPU. This information is then sent via UDP to 4096 different IP addresses, one of which is a C2 server. CSTO also compiles this information, as well as a list of the victim's encrypted files, into a fake PNG file and uploads it to Imgur.com. Imgur then responds with a unique file name which CSTO broadcasts via UDP to the 4096 IP addresses, notifying its C2 server that a new infection has occurred. CSTO also uses the *WlanGetNetworkBssList* function of the victim's system to compile a list of nearby wireless local area networks (WLANs) Set Service Identifiers (SSIDs) and then queries the Google Maps API to determine the victim's location. CSTO makes a backup of certain shortcuts on the victim's desktop and stores them in a folder called *old_shortcuts*, the purpose of which is currently unknown. It deletes Shadow Volume Copies and encrypts targeted files, appending *.cry* to each encrypted file name. To maintain persistence, CSTO creates a randomly-named scheduled task that launches when the victim logs into the system. CSTO demands a ransom payment of $625 USD worth of Bitcoin and threatens to double the amount to $1250 if the ransom is not paid within 3 days and 18 hours.

- Bleeping Computer provides more information about CSTO here.
- The NJCCIC is not currently aware of any free decryption tool available for CSTO.

**Cerber** targets Windows OS and is distributed via malvertising delivered by the Nuclear Exploit Kit. Some reports suggest that it is also being sold in the Russian underground market as "Ransomware-as-a-Service" (RaaS). When this infection first occurs, Cerber determines the location of the victim. If the victim resides outside the list of "protected" countries, Cerber installs itself in the %AppData%\{2ED2A2FE-872C-D4A0-17AC-E301404F1CBA}\ folder and names itself after a random Windows executable. Afterwards, it configures Windows to automatically boot in Safe Mode with Networking at the next restart. Cerber scans all files on the victim's drives and looks for specific file extensions. It encrypts the matching files and file names using AES-256 and then changes the file extension to .cerber. Finally, Cerber creates ransom notes named #DECRYPTMYFILES#.html, #DECRYPTMYFILES#.txt, and #DECRYPTMYFILES#.vbs, the last of which contains a VBScript causing the infected computer to speak to the victim. Researchers have recently discovered that Cerber is leveraging the same spam distributor responsible for spreading the Dridex financial Trojan.
UPDATE 7/15/2016: In addition to recently incorporating DDoS attacks and using malicious Windows Script Files in its attacks, Cerber is now targeting Office 365 users through emailed documents containing malicious macros. Since Microsoft disables macros by default, the attackers behind Cerber rely on social engineering tactics to trick users into manually enabling the malicious macros and launching the malware.
UPDATE 8/4/2016: A new version of Cerber appends .cerber2 to encrypted files, displays a new ransom note, and removes a flaw that allowed Trend Micro's decryption tool to decrypt files, rendering it useless for this version.
UPDATE 8/31/2016: A new version of Cerber appends .cerber3 to encrypted files.
UPDATE 10/4/2016: A new version of Cerber appends a random four character extension to encrypted files.

- Bleeping Computer provides more information about Cerber, found here.
- FireEye provides more information about the partnership between Cerber and the Dridex spam distributor here.
- Trend Micro provides a free decryption tool for the first Cerber variant, available here.

- Check Point provides a free decryption tool for both the Cerber and Cerber2 variants, available here. Additional information about this tool is available from Bleeping Computer here.

**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.
UPDATE 7/28/2016: A rival ransomware developer obtained and released approximately 3,500 decryption keys for Chimera which allowed security researchers to create a free decryption tool.

- Malwarebytes provides more information about Chimera, found here.
- NoMoreRansom.org provides a free decryption tool for Chimera here and instructions are located here.

**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.

**Comrade Circle** targets Windows OS and is distributed via phishing emails containing Word documents embedded with a malicious macro. Similar to the Fantom variant, Comrade Circle displays a fake "Windows Update" screen during the encryption process and disappears when the process is complete. It looks for files on local drives as well as network shares that are not password-protected. Comrade Circle renames encrypted files using six to sixteen random characters and appends *.comrade* to the newly created file names. The attackers behind this campaign request that victims send payment directly to a provided Bitcoin wallet address and follow-up with an email providing the personal ID number that is displayed on the ransom note to receive the decryption key. The attackers try to play on victims' sympathies by claiming they will donate 50 percent of the ransom payment to "poor people" and that they "are good people that help other people with getting a job and making the world better." The ransom payment demand is currently unknown.

- Enigma Software provides more information about Comrade Circle here.
- The NJCCIC is not currently aware of any free decryption tools for Comrade Circle.

**Coverton** targets Windows OS and, currently, the method of distribution is unknown. Once installed, it copies itself to %UserProfile%\userlog.exe and configures itself to automatically run when Windows starts. It then encrypts targeted files with AES-256 and creates a ransom note named "!!!-WARNING-!!!" in both .html and .txt formats. Encrypted files display the .coverton, .enigma, or .czvxce extensions. Coverton deletes Shadow Volume Copies to prevent file restoration. Some reports state that it leaves victims with corrupted files even if the ransom is paid and the decryption process has executed. Coverton demands a ransom payment of 1 Bitcoin**.**

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

**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.

**CrypMIC** targets Windows OS and is distributed via the Neutrino exploit kit. CrypMIC closely mimics CryptXXX in attack vectors, distribution and C2 communication methods, ransom note text, and the user interface of its payment site. However, it does not append any extension to the names of encrypted files, making it difficult to determine which files have been impacted and what variant is responsible. CrypMIC also checks to see if it is running in a virtual machine (VM) and sends that information to its C2 server via port 443. To prevent file restoration, CrypMIC deletes Shadow Volume Copies using the vssadmin tool. The ransom payment demand for CrypMIC is 1.2 to 1.4 Bitcoin.

- Trend Micro provides more information about CrypMIC here.
- The NJCCIC is not aware of any decryption tools available for CrypMIC.

**Crypren** targets both Windows OS and Linux distributions based on Debian and spreads via phishing emails and infected PDF, DOC, and ZIP files. It uses a combination of AES-256 and RSA-2048 encryption and appends all encrypted files with the extension .ENCRYPTED. At this time, Crypren does not damage or delete Shadow Volume Copies so it may be possible to restore data from these sources if infected with this variant. It demands a ransom payment of 0.1 Bitcoin.

- Enigma Software provides more information about Crypren here.
- A decryption tool for Crypren is available on GitHub here.

**CryptFile2** targets Windows OS and is distributed via the Nuclear and Neutrino exploit kits. More recently, it has been spread via large-scale email campaigns designed to primarily target U.S. government agencies and educational institutions. The subject of these emails promise discounted flights from American Airlines and, within the body of the emails, there are embedded URLs leading to downloadable Microsoft Word documents containing malicious macros. If these macros are enabled by the recipient, the ransomware payload downloads and executes on the system. CryptFile2 contacts its C2 server and requests a file named *default.jpg* and then encrypts targeted files, appending a combination of a unique victim ID number and the attacker's email address to the encrypted file names in the following format: *.id_[personalid]_[attackeremail].scl*. The ransom payment demand for CryptFile2 is currently unknown.

- Proofpoint provides more information about CryptFile2 here and here.
- The NJCCIC is not currently aware of any decryption tools available for CryptFile2.

**CryptMix**, a combination of CryptXXX and CryptoWall, targets Windows OS and is distributed via phishing emails and drive-by downloads. Once installed, it proceeds to encrypt 862 file types and change their extension to .CODE. CryptMix initially demands a ransom payment of 5 Bitcoins but doubles the amount if the ransom is not paid within a set time period. It also promises to donate a portion of the paid ransom to a children's charity as well as provide three years of "free tech support" to the victim.

- Softpedia has more information about CryptMix here.
- The NJCCIC is not aware of any decryption tools available for CryptMix.

**CryptoBit** targets Windows OS and is distributed via the Rig exploit kit. Once a target system is infected, CryptoBit places a fake user-agent and fake referrer line in the HTTP traffic in order to masquerade as legitimate web traffic. After establishing contact with its C2 server, it encrypts files on the victim's machine and then blocks the entire screen with an immovable ransom note. This note can be removed, however, after rebooting the system. Key files named HITLERSNASTYLITTLECRYPTEROMGWTFHELP.KEY23 have also been discovered on infected systems. The attacker behind the campaign requests victims send an email to multiple email addresses listed on the ransom note but no ransom demand amount is displayed.

- Palo Alto Networks provides more information about CryptoBit here.
- The NJCCIC is not currently aware of any decryption tools available for CryptoBit.

**CryptoHost** targets Windows OS and is currently distributed through a compromised uTorrent installer. Once installed, it extracts its executable file to the %AppData% folder and launches it. It then attempts to delete the HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot key to prevent the system from being booted into safe mode and monitors for strings associated with security software. Instead of encrypting files, however, CryptoHost moves all targeted files to a password-protected RAR archive located here: C:\Users\[username]\AppData\Roaming folder. The name of the archive is an SHA1 hash of the processor ID number, the volume serial number of the C drive, and the serial number of the motherboard. The password for the RAR archive is this SHA1 hash plus username. Once this process is completed, CryptoHost displays a ransom note demanding .33 Bitcoin to recover files.

- Bleeping Computer provides more information about CryptoHost, including instructions on how to recover files and remove the infection, 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.

**CryptoRoger** targets Windows OS and the method of distribution is currently unknown. Once executed, this variant encrypts targeted files using AES-256 and then stores the MD5 hash of the original, non-encrypted file, placing it in the %AppData%\files.txt file. Files encrypted by CryptoRoger are appended with the extension .crptrgr. It maintains persistence by placing a Virtual Basic script (.vbs) file in the Windows Startup folder and it will encrypt any new files created after the initial infection. The ransom note instructs victims to download and install uTox, a messaging client, and then contact the attacker using a specific uTox identifier. CryptoRoger demands a ransom payment of 0.5 Bitcoin and threatens to increase the amount several times if the victim does not “behave professionally.”

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

**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.

**CryptXXX** targets Windows OS and is distributed through the Bedep Trojan spread via the Angler Exploit Kit. It is shipped as a dynamic-link library (DLL) file dropped by the Bedep Trojan into folders contained within AppData\Local\Temp. The execution of the DLL is randomly and deliberately delayed to make it more difficult for the victim to make the connection between the infection and the attack vector, specifically the compromised website distributing the infection. It can detect if it is running in a virtual environment and contains anti-analysis capabilities. It checks the registry for the CPU name and installs a hook procedure to monitor for mouse events. Files encrypted by

CryptXXX display .crypt, .cryp1, crypz, or a random string of characters as the extension. It encrypts files located on all local and mounted drives and searches for credentials and Bitcoin to steal. It also collects browser and mail client information as well as cookie data and transmits it back to the attacker using a custom command and control (C2) protocol over TCP port 443. CryptXXX demands a $500 ransom to decrypt files. The most recent versions are **CryptXXX 3.0**, **CryptXXX 3.100**, and **UltraCrypter**. It has been reported that UltraCrypter is not recognizing ransom payments leaving victims who have paid with no decryption key. CryptXXX 3.100 is bundled with StillerX, a module designed to steal login credentials, distributed via the Neutrino Exploit Kit and includes a payment portal.
UPDATE 7/8/2016: A new version of CryptXXX does not append any extensions to encrypted files, making it more difficult to determine which variant caused the infection. It also does not include any method of contacting the attacker should there be problems submitting payment.
UPDATE 7/14/2016: Free decryption keys for encrypted files displaying the extension .cryp1 and .crypz are currently available through their respective decryption websites. It is currently unknown whether this was a deliberate decision made by the developers or if it is a result of a coding error within the payment system.
UPDATE 7/20/2016: A new version of CryptXXX not only appends the extensions of encrypted files, but also renames the entire file to a string of letters and numbers making file identification difficult for victims.

- Proofpoint provides more information about CryptXXX here and CryptXXX 2.0 here.
- Kaspersky Labs provides a CryptXXX decryption tool here. Information about the tool and this variant can be found here.
- Kaspersky Labs provides information about CryptXXX 2.0 and its decryption tool here.
- The NJCCIC is currently not aware of any decryption tool available for CryptXXX 3.0 or UltraCrypter but more information can be found about it on Bleeping Computer here and here.
- Proofpoint provides more information about CryptXXX 3.100 here.

**CryPy** targets Windows OS and its method of distribution is currently unknown. It encrypts files using AES-256 and renames encrypted files beginning with the letters CRY, followed by a long string of random characters, and appending *.cry* to the new file name. CryPy's C2 server is responsible for generating each new file name and a random 32-character password for each encrypted file. This requires CryPy to initiate a connection to the server after each file is encrypted, which delays the encryption process but also protects the keys and the key generation routine from the attacker's adversaries. The ransom payment amount is currently unknown. CryPy threatens to permanently delete a random file for every six hours the ransom is not paid. After 96 hours, CryPy claims it will permanently delete the decryption keys, making file recovery impossible.

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

**Crysis** targets Windows OS and is distributed as malicious attachments in spam emails and disguised as installation files for legitimate software. Once it infects a system, it creates registry entries to maintain persistence and encrypts all file types, with the exception of system and malware files, on fixed, removable, and network drives. Crysis then drops a ransom note on the desktop for the victim, providing two email addresses the victim can use to contact the attackers. The ransom demand is between 0.79 and 1.18 Bitcoin.

- We Live Security provides more information about Crysis here.
- The NJCCIC is not aware of any decryption tools available for Crysis.

**CTB-Faker** pretends to be the CTB-Locker ransomware variant and targets Windows OS. It is distributed through malicious links posted on fake profile pages hosted on adult entertainment websites. Clicking these links will download a WinRAR SFX file to the victim's computer and extract a number of batch files, executables, and VBS files into the C:\ProgramData folder. The first sign of a CTB-Faker infection is a pop-up error message that pretends to be a graphic card error. Additional signs include slowed system performance and a spike in CPU usage. CTB-Faker moves all targeted files into a password-protected ZIP file and then reboots the system before displaying a ransom note claiming that the

victim's files were encrypted by CTB-Locker. CTB-Faker demands an initial ransom payment amount of 0.0868 Bitcoin or $50 USD with a threat to double the price if payment is not submitted within seven days.

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

**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.

- Bitdefender Labs has created a free CTB-Locker infection prevention tool, or "vaccine," available here.
- The NJCCIC is not aware of any decryption tools available for CTB-Locker.

**CuteRansomware** targets Windows OS and is based on source code from a publically available ransomware module called "my-Little-Ransomware," posted on the open-source Git repository, GitHub. It is distributed via Google Docs, although it could easily be modified to spread via other cloud apps and platforms. CuteRansomware uses Google Docs to deliver malicious files to victims and as a C2 server, storing encryption keys and data exfiltrated from victims' machines. This distribution method bypasses network firewalls and intrusion prevention systems as data is transmitted over SSL due to Google Docs use of HTTPS. CuteRansomware is also difficult to block because the only way to avoid it is to block the specific instance of the app containing the malware. Currently, this variant looks to be specifically targeting Chinese victims, as affected files are appended with the Chinese translation for ".encrypted" and notes within the code are written in Chinese. The ransom payment demand for CuteRansomware is currently unknown.

- Netskope provides more information about cureRansomware here.
- The NJCCIC is not currently aware of any decryption tools available for cuteRansomware.

**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.

**Ded Cryptor** targets both English-speaking and Russian-speaking Windows OS users and the method of distribution is currently unknown. Ded Cryptor is an EDA2-based ransomware variant and, although EDA2 ransomware could be decrypted for free in the past, the author of this malware has instituted a change that renders current free decryption tools ineffective. Once installed, this variant creates an AES key and encrypts the infected system's User Profile folder and the files contained within it. When that process is complete, it then encrypts the AES key and sends it back to its C2 server. This variant does not create a ransom note text file but the ransom instructions are displayed on the desktop background image. Ded Cryptor appends all encrypted files with the extension .ded and demands a ransom payment of 2 Bitcoin.

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

**DetoxCrypto** targets Windows OS and is distributed as an executable file that contains other files and executables. There are currently two versions of this variant, although security researchers expect more versions to emerge as indications point to a possible Ransomware-as-a-Service (RaaS) affiliate program. One version launches from an executable named *Pokemongo.exe* and has a Pokémon-themed ransom note. Another version, dubbed Calipso, launches from an executable

named *calipso.exe* and displays an image of a computer locked in chains with a stack of coins, along with generic ransom note text. The executables for DetoxCrypto reside within the main distribution executable, along with an audio file, a wallpaper image file, and a file named *MicrosoftHost.exe* that performs the encryption process. Neither version appends any extension to encrypted file names. Calipso stands apart from other variants because it takes a screen capture of the victim's infected machine and uploads it to the attacker. The ransom payment amount is currently unknown.
UPDATE 8/26/2016: A new version, named Serpico and written in Serbsko-Croatia, was discovered.
UPDATE 9/1/2016: A new version, dubbed Nullbyte, masquerades as the NecroBot Pokémon Go application and is distributed through a Github application. After installation, Nullbyte displays the standard NecroBot interface prompting the victim to login and then steals any credentials entered into the form. After the credentials are sent to its C2 server, Nullbyte begins encrypting files using AES encryption and appending *_nullbyte* to the file names. It also terminates the following processes to hinder removal of the infection or prevent the victim from searching online for help: chrome, cmd, taskmgr, firefox, iexplore, and opera. Lastly, Nullbyte takes a screenshot of victim's active screen and uploads it to its C2 server before displaying a lock screen and asking for a ransom payment of 0.1 Bitcoin.
UPDATE 9/16/2016: A new version tries to fool users by imitating the antivirus software, Malwarebytes, by arriving in an executable file named *Malwerbyte.exe*.

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

**DMA Locker** targets Windows OS and one known method of distribution is through Remote Desktop. Once an infection occurs and the executable is launched, DMA Locker terminates any applications used for backing up data and adds registry keys to maintain persistence. It then whitelists all system and executable files and proceeds to encrypt all other files located on local drives, mapped network shares, and even unmapped network shares. Unlike other variants, DMA Locker does not add a custom extension to encrypted files but, instead, adds an identifier into the file headers. In earlier versions of DMA Locker, one AES key was used for all encrypted files but the most recent version generates a new random key for each file. DMA Locker demands a ransom of 4 Bitcoin (approximately $1700 USD at the time of this publication). The latest version, **DMA Locker 4.0**, is distributed via the Neutrino exploit kit and is unable to encrypt files while offline as it needs to make contact with its C2 server in order to download the public RSA key for encryption. If the target computer is not connected to the Internet at the time of infection, this ransomware will install itself and wait until the system establishes an Internet connection before encrypting data. Every file is then encrypted with a different key.
UPDATE: A new version of DMA Locker appends *.XPTLOCK5.0* to encrypted files.

- Bleeping Computer provides more information about DMA Locker here.
- MalwareBytes provides additional information about DMA Locker here and here.
- MalwareBytes provides additional information about DMA Locker 4.0 here.
- Earlier versions of DMA Locker can be decrypted by using this tool. However, the NJCCIC is not aware of any decryption tool available for the latest version of DMA Locker.
- A Malwarebytes analyst has created a free decryption tool for the *XPTLOCK5.0* version of DMA Locker, available on Google Drive, here.

**Dogspectus,** also known as **Cyber.Police**, targets Android OS and spreads via a currently unnamed exploit kit. If an Android device is used to visit a website hosting malicious advertisements, the hostile Javascript code contained within those ads exploits several Android vulnerabilities to quietly install Dogspectus without the knowledge of the victim. Packaged as an Android .apk application, it does not display an "application permissions" dialogue box before installing itself onto the device. Dogspectus does not actually encrypt any data but rather locks access to the infected device until the victim pays the ransom. Currently, files can be recovered from an infected Android device without paying the ransom and is done by connecting the device to a computer and manually copying the files to the computer's hard drive. The malware itself can be removed from the device by performing a factory reset which deletes all files and applications that have been previously installed. Dogspectus demands a $200 ransom payable only via Apple iTunes gift cards.

- Blue Coat Labs provides more information about Dogspectus here.

**Domino** targets Windows OS, it is based on Hidden Tear, and its current method of distribution is unknown. It masquerades as a KMSPico Windows activation crack installation file. When executed, it places a randomly named file into the %Temp% folder which then extracts a password-protected zip file named *Help.zip*. The password for this ZIP file is abc123456 and, within it, are two additional files: *help.exe*, which launches the encryption process, and *HelloWorld.exe*, the executable responsible for generating the ransom note. Encrypted files will display the .domino file extension. Domino demands a ransom payment of 1 Bitcoin and threatens to delete the victim's decryption key after 72 hours.

- Bleeping Computer provides more information about Domino here.
- Bleeping Computer provides a free decryption tool for Domino here.

**DXXD** targets Windows servers and the method of distribution is currently unknown. Once infected, the server will display a specially crafted login screen that lets victims know they have been attacked and lists email addresses of the hackers so victims can contact them for further instructions. DXXD appends the extension *.dxxd* to encrypted files. The ransom payment demand for DXXD is currently unknown.

- Bleeping Computer provides more information about DXXD here.
- Bleeping Computer provides a decryption tool for DXXD, available here.
- To decrypt the newest version of DXXD, follow the instructions on the Bleeping Computer website, here.

**EduCrypt** targets Windows OS and the method of distribution is currently unknown. Its code is based on the open-source ransomware kit, Hidden Tear, and was designed to teach victims a lesson, not to generate profit. EduCrypt only targets a small number of folders and file types and does not connect to a C2 server. It uses the password HDJ7D-HF54D-8DN7D for the files it encrypts and appends those files with the extension .isis. EduCrypt's ransom note does not demand any payment but it does lecture the victim on unsafe downloading practices and provides a link to a free decryption tool.

- Bleeping Computer provides more information about EduCrypt here**.**
- Although EduCrypt's ransom note provides a link to a decryption tool, the NJCCIC recommends using the tool provided by Bleeping Computer, **here**, as it is a known and trustworthy source.

**El Gato** targets Android OS and is distributed via a legitimate cloud service provider. It requests and receives commands from its C2 server via unencrypted HTTP traffic. El Gato's capabilities include: file encryption and decryption, sending and exfiltrating SMS messages, locking the infected device, and killing application processes. El Gato displays a picture of a cat on the locked device screen. The ransom payment demand for this variant is currently unknown.

- McAfee provides more information about El Gato here.
- The NJCCIC is not currently aware of any decryption tools available for El Gato.

**Exotic Ransomware** targets Windows OS and, as it appears to still be in development, its method of distribution is currently unknown. Exotic only targets files within specific folders under the User Profile. It will encrypt a wide variety of file types, including executable files. It uses AES-128 to encrypt them and appends *.exotic* to the file names after renaming the files to a random set of characters. Exotic also looks for certain processes such as *msconfig*, *taskmgr*, *cmd*, *regedit*, and CCleaner64 and terminates them. Lastly, it displays a countdown timer on the lock screen and, once the timer reaches zero, it shuts down the computer. Exotic demands a ransom payment of $50 USD worth of Bitcoin.

- Bleeping Computer provides more information about Exotic Ransomware here.
- The NJCCIC is not currently aware of any free decryption tools for Exotic Ransomware.

**Fantom** targets Windows OS and its method of distribution is currently unknown. Its code is based on EDA2, an open-source ransomware project published in early 2016. Fantom masquerades as a critical Windows update, displaying a fake but convincing Windows update screen to fool victims into believing they are receiving a legitimate patch from Microsoft. Once the update screen is displayed, victims become unable to switch to any other application. Pressing Ctrl+F4 will remove the fake update screen but it will not stop the encryption process. Fantom encrypts files using AES-128 and appends the .fantom extension to the file names. In each folder, it leaves a ransom note named

*DECRYPT_YOUR_FILES.HTML*. Once the encryption process ends, Fantom creates two batch files that delete Shadow Volume Copies and the fake Windows update executable, *WindowsUpdate.exe*. The ransom payment amount is currently unknown.
UPDATE 9/21/2016: A new version of Fantom uses the filenames of targeted files to determine how much ransom to charge the victim. It also uses the filename to generate a payment email address to display to the victim.

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

**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.

**FLocker**, short for "Frantic Locker," targets Android OS and is capable of encrypting files on Android-powered smart TVs. It is distributed by malicious links spread via SMS messages or encountered during internet browsing. These malicious links lead to an Android application package (APK) file which proceeds to download and infect the victim's Android-powered device. Once the malicious APK has been installed, FLocker waits 30 minutes before taking any further action. After that half hour passes, FLocker begins prompting the victim to allow it administrative access to the device. If the victim declines, the screen freezes and displays a phony system update alert to trick the victim into giving the ransomware administrative access. Once the escalated privileges have been obtained, FLocker establishes communication with a C2 server to download an additional APK and a ransom note HTML file with an enabled JavaScript interface. The ransom note demands a payment of $200 USD in iTunes gift cards.

- Trend Micro provides more information about FLocker here.
- In the event of an infection, Trend Micro recommends contacting the device vendor for a solution. The victim can also enable ADB bugging and connect the device to a PC, launch the ADB shell, and execute the command "PM clear %pkg%" to kill the ransomware process and unlock the screen. Lastly, deactivate the administrator privileges granted to the malicious application and delete it.

**FSociety** targets Windows OS and its code is based on EDA2, an open-source ransomware project published in early 2016. Its ransom note image contains the logo of the fictional hacking group featured on the television show, *Mr. Robot*. Security researchers who discovered this variant noted that it seems to be in the early stages of development and it not being actively distributed as no ransom note text or contact information were found and it only currently targets a test folder on the Windows desktop. FSociety appends *.locked* to encrypted file names.
UPDATE 10/2/2016: A new version of the FSociety ransomware was discovered. It appends *.realfs0ciety@sigaint.org.fs0ciety* to encrypted file names and generates ransom notes named *fs0ciety.html*. Contact the security researchers on the Bleeping Computer forum here for help with this variant.

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

**Globe** targets Windows OS and its method of distribution is currently unknown. Once installed, Globe employs its anti-forensic capabilities as it determines whether or not it is running within a sandbox or a virtual machine (VM) such as Anubis, VirtualBox, VMware, or Virtual PC. If any of these are present, Globe will terminate itself. If none are detected, Globe begins the encryption process using the Blowfish encryption algorithm, targeting 995 file extensions and appending *.globe* or *.purge* to the name of every file it encrypts. It then creates an autorun.inf file which displays a ransom note using an HTML Application file named *How to restore files.hta* which opens when the victim logs into Windows. Globe deletes Shadow Volume Copies to prevent file restoration and disables Windows Startup Repair. Lastly, Globe will change the

victim's desktop wallpaper to display an image featuring characters from the movie, *The Purge: Election Year*. UPDATE 10/6/2016: A number of new versions of Globe were seen in the wild and append the following extensions to encrypted files: *[random].encrypted, .[random].raid10, .[mia.kokers@aol.com], and .[random].globe*.

- Bleeping Computer provides more information about Globe here.
- Emsisoft provides a decryption tool for Globe, available here.

**GPCode** targets Windows OS and the method of distribution is currently unknown, although several open source reports suggest that the attackers exploit vulnerabilities in servers to spread the infection. Originally released in June 2006, GPCode could be derypted without paying the ransom. However, recent versions are unbreakable and not only encrypt data, but some versions corrupt operating systems by encrypting .exe and .dll files as well. GPCode encrypts local files, shared folders, and even administrative shares, according to victims. It also deletes Shadow Volume Copies to prevent file restoration. Files encrypted by GPCode are appended with either the extension .LOL! or .OMG!. The attackers behind GPCode offers to decrypt one to two of the victim's encrypted files before demanding payment for the rest. GPCode threatens to delete all of the victim's files and decryption keys if payment is not received within one month.

- The Bleeping Computer forum has more information about GPCode here.
- The NJCCIC is not aware of any decryption tools available for GPCode.

**HDDCryptor**, also known as **Mamba**, targets Windows OS and is distributed via files downloaded from malicious websites. When the initial binary file is executed, a number of files are downloaded into a root folder on the infected system. HDDCryptor then creates a user account named "mythbusters" along with a password of "123456." It also adds a new boot service named "Defragment Service" to gain and maintain persistence. It uses a tool named *netpass.exe* to scan network folders and steal credentials. Executables *dcon.exe* and *mount.exe* are then used to encrypt files on the infected system's hard drive as well as files located on all mapped network drives. One that process is complete, HDDCryptor proceeds to rewrite the Master Boot Records (MBRs) for all partitions containing a custom boot loader to prevent the operating system from loading after the system is restarted. It then reboots the infected system and displays a ransom note requesting the victim contact the attacker via email. HDDCryptor demands a ransom payment of 1 Bitcoin.

- Bleeping Computer provides more information about HDDCryptor here.
- The NJCCIC is not currently aware of any free decryption tool available for HDDCryptor.

**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.

**Hitler-Ransomware**, or Hitler-Ransonware as it is displayed on its lock screen, targets Windows OS and its method of distribution is currently unknown. Rather than appending extensions to names of encrypted files, Hitler-Ransomware removes all extensions for files located in specific folders. It extracts the following files into the infected system's %Temp% folder: chrst.exe, ErOne.vbs, and firefox32.exe, which is also copied into the startup folder to be automatically launched upon system reboot. It also kills the following processes: taskmgr, utilman, sethc, and cmd. Hitler-Ransomware will cause the infected system to crash and will also delete all files under the %UserProfile% folder when the system restarts if the ransom demand is not met within an hour. Hitler-Ransomware demands a ransom amount of 25 Euros payable via a Vodafone card code.

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

**HolyCrypt** targets Windows OS and its method of distribution is currently unknown. HolyCrypt is written in Python and compiled into a single Windows executable file using PyInstaller. It targets certain files located in the %UserProfile% folder using AES encryption. HolyCrypt prepends impacted file names with the word "encrypted." Once that routine is complete, it creates an alert file and sets it as the desktop wallpaper and the ransom note which includes a threat to delete the decryption key after 24 hours of non-payment. The ransom payment demand for HolyCrypt is currently unknown.

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

**JapanLocker** is an open-source PHP ransomware variant that targets web servers. Despite the name, the hacking group behind the creation of this variant is based in Indonesia. They use search engines such as Shodan.io to scan for vulnerabilities within websites and then they exploit those vulnerabilities in order to gain access to the server. The encryption method used is a combination of Base64 encoding, ROT13, and basic data swapping. This basic encryption method allows for affected files to be easily decrypted.

- Fortinet provides more information about JapanLocker here.
- Fortinet provides a free decryption tool for JapanLocker, available here.

**Jigsaw** targets Windows OS and, currently, the method of distribution is unknown. Once an infection occurs, Jigsaw scans victims' drives for specific file extensions and encrypts them using AES. Files encrypted by Jigsaw display the following extensions: .fun, .kkk, .gws, .btc, .payms, .epic, and .xyz. A list of encrypted files is located on the infected system in the following location: %UserProfile%\AppData\Roaming\System32Work\EncryptedFileList.txt. This variant is unique in that it not only threatens to start deleting files if the victim does not pay, but it actually carries out that threat, deleting one file every 60 minutes and deleting 1,000 files when the infected system is rebooted. Some versions of Jigsaw have been found to execute after specific dates. Ransom prices vary from $20 to $200 worth of Bitcoin, but one version has been seen demanding $5000 USD worth of Bitcoin. A later version of Jigsaw was rebranded as **CryptoHitman** and adds the extension .porno or .pornoransom to all encrypted files. Both versions can be decrypted but it is important to first to terminate the suerdf.exe and hogfh.exe processes in Task Manager to prevent file deletion. Then, disable startup entries for those executables prior to running the decryption tool to prevent recurring instances. The latest rebranding is called **Invisible Empire** and adds the extension .payransom to encrypted files. In addition, Jigsaw developers have added a "live chat" feature allowing the attacker to provide instructions and further pressure the victim into paying the ransom. UPDATE 7/29/2016: A new version of Jigsaw features an Anonymous-themed ransom note, appends .xyz to encrypted files, and demands $250 USD worth of Bitcoin. The free decryption tool listed below has been updated to decrypt this version.

- Bleeping Computer has more information about Jigsaw here, CryptoHitman here, and Invisible Empire here.
- A decryption tool for Jigsaw, CryptoHitman, and Invisible Empire is available for download here. Instructions on how to use the tool and decrypt files are available on the Bleeping Computer website.

**JuicyLemon** targets Windows OS and is distributed via the Angler exploit kit, network shares, and malicious email attachments. Once a system is infected, JuicyLemon adds various values to the registry,, encrypts specific files types, contacts its C2 server via HTTP, and then drops a .bat file which deletes the original executable. JuicyLemon requests that victims send one of their encrypted files to *support@juicylemon.biz* or *provectus@protonmail.com*. It completely renames encrypted files to a combination of a unique victim ID number, an email address, and a Bitcoin wallet address. JuicyLemon demands a ransom payment of 1000 euros worth of Bitcoin.

- Cylance provides more information about JuicyLemon here.
- Bleeping Computer provides a free decryption tool for JuicyLemon here.

**KimcilWare** targets websites using the Magento eCommerce platform. The exact method of compromise is currently unknown, but files located on the victimized web server are encrypted with Rijndael 256. Additional analysis reveals that KimCilWare opens up a backdoor into the server and allows attackers full control over the targeted website. This variant

uses one of two scripts to encrypt the targeted files. One script changes the file extensions on all encrypted files to .kimcilware and the other script changes them to .locked. The first script demands a ransom of $140 USD and the second demands 1 Bitcoin.

- Bleeping Computer provides more information about KimcilWare here.
- Fortinet provides technical analysis on KimcilWare here.
- The NJCCIC is not aware of any decryption tools available for KimcilWare.

**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.

**KozyJozy** targets Windows OS and the method of distribution is currently unknown. It encrypts files using RSA-2048. Files encrypted by KozyJozy are appended with a random extension displaying the following pattern: .31392E30362E32303136_(0-20)_LSBJ1. Additional extensions include ZHM1 and KTR1. KozyJozy deletes Shadow Volume Copies using the command Delete Shadows /All /Quiet but does not overwrite the space so victims may be able to recover files using data recovery software.

- Trend Micro provides more information about KozyJozy here.
- The NJCCIC is not aware of any decryption tools available for KozyJozy.

**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.

**LockLock** targets Windows OS and is an EDA2-based ransomware variant. The method of distribution is currently unknown. LockLock encrypts files using AES-256 and appends *.locklock* to the names of encrypted files. It requests the victim contact the attacker via email or skype, at the addresses provided on the ransom note. The ransom payment demand for LockLock is currently unknown.

- Bleeping Computer provides more information about LockLock here.
- Victims may be able to have their files decrypted by contacting security researcher *Demonslay335* on the Bleeping Computer forums here.

**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*, *.zepto*, or *.odin* 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. The Locky campaign went dark between June 1 and June 21, 2016 but has since resurfaced. It now includes anti-analysis and sandbox evasion features and tries to collect unpaid debts from victims.
UPDATE 7/20/2016: **Locky** now has the ability to encrypt files even if the infected system is offline and the ransomware cannot connect to its C2 server. This new feature allows Locky to be effective even if network firewalls prevent outbound connection attempts.
UPDATE 8/26/2016: **Locky** is now being delivered and executed as a DLL file rather than an EXE file in order to bypass executable blockers.
UPDATE 9/6/2016: **Locky** is now delivered with an embedded RSA key, eliminating the need to contact its C2 server to encrypt files.
UPDATE 10/24/2016: A new version of Locky has surfaced appending *.sh*t* (expletive removed) to the names of encrypted files. It is currently being distributed via phishing emails with the subject line of *Receipt ###-###* containing malicious hypertext application (HTA), JavaScript (JS), or Windows Script File (WSF) attachments. After encrypting files using AES encryption, it displays ransom notes named *_WHAT_is.html*, *_[2_digit_number]_WHAT_is.html*, and *_WHAT_is.bmp*.
UPDATE 10/25/2016: Another new version of Locky has begun appending *.thor* to the names of encrypted files and renaming those files using the following naming convention: *first_8_hexadecimal_chars_of_id]-[next_4_hexadecimal_chars_of_id]-[next_4_hexadecimal_chars_of_id]-[4_hexadecimal_chars]-[12_hexadecimal_chars].thor*. It is currently being distributed via phishing emails with the subject line of *Budget forecast* that contain a ZIP attachment named *budget_xls_[random_chars].zip*. This ZIP file contains a malicious VBS file.

- Sophos Labs provides more information about Locky here.
- FireEye provides more information about the most recent Locky campaign here.
- Bitdefender Labs has created a free Locky infection prevention tool, or "vaccine," available here.
- The NJCCC is not aware of any decryption tools available for Locky.

**Maktub Locker** targets Windows OS and spreads through a spam campaign that includes a malicious .scr attachment designed to look like a "Terms of Service" (TOS) agreement. Once the victim opens the attached document, a malicious script begins to quietly run and encrypt files in the background. It targets files on local drives, removable drives, and network. It does not need to call out to a C2 server to obtain the encryption key – encryption can take place offline as well as online. Maktub Locker compresses files before it encrypts them and then deletes the originals. Extensions appended to the file names are random but follow an [a-z]{4,6} pattern.

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

**MarsJoke** targets Windows OS and is distributed via spam emails that use fraudulent branding from legitimate air carriers and shipping companies. This spam campaign primarily targets U.S. state and local government agencies, as well as educational institutions. Other targets include the healthcare, telecommunications, insurance, and technology. Subject lines include: *Checking tracking number*, *Check your package*, Check your TN, *Check your tracking number*, *Tracking Information*, and *Track your package*. These emails contain malicious links that, if clicked, download an executable file named *file_6.exe* to the victim's system. Once the executable is launched, MarsJoke immediately begins to encrypt files, although it doesn't change the file name or extension. Once the encryption process is complete, the victim's desktop background is changed and a ransom note is displayed. MarsJoke threatens to delete the decryption key if the ransom is not paid within 96 hours. MarsJoke demands a ransom payment amount of 0.7 Bitcoin.

- Proofpoint provides more information about MarsJoke here.
- Kaspersky's free decryption tool, Rannoh Decryptor, can now decrypt MarsJoke.

**MIRCOP**, also known as **Crypt888**, targets Windows OS and is distributed via email containing a malicious Word document designed to resemble a Thai customs form. If the document is opened and macros are enabled, a PowerShell script downloads and installs onto the machine which, in turn, installs and launches the ransomware. Once executed, MIRCOP drops the following three executable files into the %temp% folder: c.exe (steals information), x.exe, and y.exe (encrypts files). Files encrypted by MIRCOP are prepended with the word "Lock." MIRCOP accuses the victim of stealing money, claims to know about the victim, and demands a ransom payment of 48.48 Bitcoin.

- Trend Micro provides more information about MIRCOP here.
- Bleeping Computer provides a free decryption tool for MIRCOP here.

**MM Locker** targets Windows OS and it is distributed via malicious email attachments and crack executables for various games. Once a system is infected, MM Locker contacts its C2 server via a POST request, transmitting the victim's username and computer name and a hardcoded token labeled *servkey*. It then receives the ransom amount and a JPG to be displayed on the infected system, as well as the decryption tool. Once this exchange is completed, MM Locker signals that the process has been completed by sending a Uniform Resource Identifier (URI) labeled */finished.php*. MM Locker encrypts a number of file types, including tax files, and appends .locked to the file names. MM Locker demands a ransom of 0.501049 Bitcoin and threatens to delete the decryption key if payment is not received within 72 hours.

- Sensors Tech Forum provides more information about MM Locker here.
- The NJCCIC is not currently aware of any decryption tool available for MM Locker.

**MSIL/Samas.A/Samsam** targets vulnerable servers running outdated versions of JBoss, an open-source business application server program written in Java. The criminals behind this ransomware campaign use JexBoss, an open-source JBoss testing/exploitation tool, and reGeorg/tunnel.jsp, a tunneling tool, to gain entry into a targeted network by scanning for and exploiting these server-side vulnerabilities. Once inside, they deliver the payload using psexec.exe and launch samsam.exe to begin the encryption process. This variant deletes Shadow Volume Copies using vssadmin.exe and wipes free space on the hard drive to prevent file restoration. It also has the capability of moving laterally through infected networks to encrypt files on endpoint machines. Files impacted by MSIL/Samas.A/Samsam will display encrypted.RSA as their extension. The healthcare sector has specifically been targeted by this variant.

- JBossDeveloper has more information about securing and hardening JBoss here.
- Cisco Talos has additional information about MSIL/Samas.A/Samsam here.
- The NJCCIC is not aware of any decryption tools available for MSIL/Samas.A/Samsam.

**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.

**Nemucod**, a variant named after the dropper used to deliver the malicious payload, targets Windows OS and is distributed via spam emails containing ZIP files which, in turn, contain a JavaScript file. Once executed, the JavaScript file downloads the following 5 files onto the infected system: a.exe,, a1.exe, a2.exe, a.php, and php4ts.dll. The JavaScript file then launches a.exe which interprets the PHP file in order to begin the encryption process using simple XOR. Files encrypted by Nemucod are appended with the extension .crypted. Nemucod demands a ransom payment of 0.37070 Bitcoin.

- ReaQta has more information about Nemucod here.
- A free decryption tool for Nemucod is available on GitHub here.
- Emsisoft also provides a free decryption tool for Nemucod here.

**NoobCrypt** targets Windows OS and its method of distribution is currently unknown. This variant was named after the text it displays if the victim enters "123" in the decryption key field. If this code is entered, NoobCrypt taunts the victim with the following pop-up message: "123 is not the code! You idiot. GO PAY IF U WANT UR PC BACK. NOOB HAH." Each release of this variant is associated with a specific Bitcoin address and ransom amount and security researchers have used that information to determine the decryption keys. The ransom payment demand for NoobCrypt varies.

- Bleeping Computer provides more information about NoobCrypt, as well as decryption instructions, here.

**Nuke** ransomware targets Windows OS and its distribution method is currently unknown. It uses AES-256 to encrypt files and appends *.nuclear55* to file names after renaming the files to a random set of characters. Nuke then generates two ransom notes, *!!_RECOVERY_instructions_!!.html* and *!!_RECOVERY_instructions_!!.txt* and then changes the desktop wallpaper. Although it does not provide any payment instructions and no ransom amount is listed on the notes, Nuke provides an email address for the victim to use to contact the attacker in order to arrange payment. It also threatens to destroy the decryption key if payment is not received within 96 hours. The ransom payment demand for Nuke is currently unknown.

- PC Risk provides more information about Nuke here.
- The NJCCIC is not currently aware of any free decryption tool available for Nuke.

**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 or .padcrypt. 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.

**Petya** targets Windows OS and is distributed via email campaigns designed to look like the sender is seeking a job within the recipient's company. The emails contain a link that leads the recipient to a self-extracting ransomware executable file named Bewerbungsmappe-gepackt.exe. Once this file is executed, Petya overwrites the hard drive's Master Boot Record

(MBR) which prevents the OS from loading and displays a blue screen. It will then reboot the infected machine, appear to run CHKDSK, encrypt the Master File Table (MFT), and flash a red lock screen with an ASCII image of a skull and crossbones followed by a screen outlining a ransom demand. The modified MBR eliminates both the infected machine's ability to start the OS normally or in "Safe Mode." Petya can only successfully infect a machine if the executable is launched via an account with administrator privileges. The latest version of Petya comes bundled with a second ransomware program, called **Mischa**, that begins to encrypts victims' files in the event that Petya is unable to encrypt the MFT.
UPDATE 7/28/2016: The developers of Petya and Mischa have begun enticing new distributors as they now offer their malware as an affiliate program, or Ransomware-as-a-Service (RaaS).

- Trend Micro has more information about Petya here.
- Bleeping Computer has more information about the combination of Petya and Mischa here.
- A decryption tool for Petya is available for download here. A web-based tool is available here. Additional information about the decryption tool can be found on Github and on the Bleeping Computer website.

**PizzaCrypts** targets Windows OS and is distributed via the Neutrino Exploit Kit. Once executed, this variant encrypts victims' files and appends them with the extension id-[victim's ID}_maestro@pizzacrypts.info. A ransom note labeled "Pizzacrypts Info.txt" is then dropped into every folder that contains encrypted files. The ransom payment demand for PizzaCrypts is currently unknown.

- PC Risk provides more information about PizzaCrypts here.
- The NJCCIC is not aware of any decryption tools available for PizzaCrypts.

**PokemonGo Ransomware** targets Windows OS and masquerades as a PokemonGo Windows application. It uses AES encryption and appends .locked to encrypted file names. PokemonGo Ransomware also installs a backdoor, creates an administrator account labeled "Hack3r" on the infected system, and then modifies the registry to hide the newly created account. It then creates network shares and spreads its executable file to other drives. PokemonGo Ransomware creates and places an *Autorun.inf* file in each drive to ensure that the executable is launched when the victim logs into Windows or when the infected removable drive is inserted into another system. The ransom note and screensaver generated by this variant currently target Arabic-speaking victims but security researchers believe it is still in development by its creator and new languages and features could be added before its release. The ransom payment demand for PokemonGo Ransomware is currently unknown.

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

**PowerWare** is a type of fileless ransomware that targets Windows OS, especially systems within the healthcare sector. This variant spreads via phishing emails containing Word documents labeled as invoices that are embedded with malicious macros. When these malicious attachments are opened, the executable leverages PowerShell to deliver the payload to the targeted system and encrypt the victim's files. This technique prevents PowerWare from raising any red flags by not writing any files to disk and blending in with legitimate activity on the system.

- Carbon Black has more information about PowerWare available here.
- The NJCCIC is not aware of any decryption tools available for PowerWare.

**Power Worm** targets Windows OS and is written in Windows PowerShell that 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.

**RAA** targets Windows OS and is distributed via emails containing JavaScript files disguised as document attachments. Opening the malicious file generates a phony Word document in the "My Documents" folder. Subsequently, RAA will identify all connected drives with open write permissions, scan them for specific files types, and proceed to encrypt them with AES using code from the CryptoJS library. Files encrypted by RAA display .locked as the extension. To prevent file restoration, it deletes Shadow Volume Copies as well as the Windows Volume Shadow Copy Service. RAA also installs Pony, a Trojan that decrypts and steals passwords, onto the infected system. RAA demands a ransom payment of 0.39 Bitcoin, or $250 USD.
UPDATE 9/12/2016: A new version of RAA arrives in a password-protected zip archive attachment, coded in JScript, and can perform encryption offline and without connecting to its C2 server. RAA #2 has been seen specifically targeting Russian-speaking corporate employees.

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

**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.

**R980** targets Windows OS and is distributed via compromised websites and email attachments containing malicious macros. It uses both AES-256 and RSA-4096 encryption algorithms to encrypt 151 targeted file types. R980 appends .crypt to encrypted file names. It creates a registry key to maintain persistence connects to its C2 server to retrieve a custom Bitcoin address for payment. The attacker uses disposable Mailinator email addresses to communicate with victims. The ransom payment demand for R980 is currently unknown.

- Trend Micro provides more information about R980 here.
- The NJCCIC is not currently aware of any decryption tool available for R980.

**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.

**RektLocker** targets Windows OS and the current distribution method is unknown. It uses RSA-2048 encryption and appends .rekt to all encrypted file names. RektLocker creates a ransom note labeled *Readme.txt* that includes the Bitcoin address for payment but it does not provide any way to communicate with the attacker. Without a method of communication to transmit the decryption key, files cannot be decrypted even if victims pay the ransom. RektLocker demands a ransom payment amount of 1 Bitcoin.

- Sensors Tech Forum provides more information about RektLocker here.
- The NJCCIC is not currently aware of any decryption tool available for RektLocker.

**Rokku** targets Windows OS and spreads through a well-written spear-phishing campaign that includes a malicious attachment containing an executable file. Once the victim opens the attachment, Rokku immediately deletes all Shadow Volume Copies to prevent data restoration. It then uses the Salsa20 algorithm to encrypt each targeted data file with its own unique key, stored within the last 252 bytes of the same associated file. This variant can be identified by its .rokku file extension. Unique elements of Rokku include the use of Google Website Translator Plugin to convert ransom notes into the victim's chosen language as well as the use of a QR code to make it easier for the victim to pay the ransom.

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

**Satana** targets Windows OS and the method of distribution is currently unknown. After a system is infected with Satana, it displays a User Account Control (UAC) pop-up notification asking the victim to allow a program from an unknown publisher to make changes to the computer. This notification is repeatedly displayed until the victim clicks "Yes." After the victim agrees to allow the changes, Satana then delivers a portable executable (PE) file, or dropper, that injects code into the Master Boot Record (MBR) designed to prevent Windows from booting after the system is restarted. Once that process is complete, Satana proceeds to encrypt targeted files and drop ransom notes named *!satana!.txt* in each associated folder. Files encrypted by Satana are renamed in the following fashion: *<email_address>_<original_name>* with the email address being randomly chosen from a preselected pool coded into the ransomware. It also prevents file restoration by deploying *vssadmin.exe* to delete Shadow Volume Copies. The randomly generated key used for encryption is transmitted from Satana's C2 server but, if that connection is prevented or interrupted, the key could be lost preventing victims who pay the ransom from being able to decrypt their files. The MBR can be repaired or restored from backup without paying the ransom but this will not decrypt encrypted files. Satana demands a ransom payment of 0.5 Bitcoin.

- Malwarebytes provides more information about Satana here.
- Kaspersky also provides more information about Satana here.
- The Windows Club provides detailed instructions on how to repair the MBR here.
- The NJCCIC is not currently aware of any free decryption tools available for Satana.

**Shark** targets Windows OS and is being offered as a Ransomware-as-a-Service (RaaS) kit via a publicly accessible, clearnet WordPress website. The developer keeps 20 percent of the ransom payments and the distributors using the service keep the remaining 80 percent. The ransomware kit is contained within a ZIP file named *PayloadBundle.zip* which contains a configuration builder, *Payload Builder.exe*, a warning to the distributor named, *Readme.txt*, and the ransomware executable file, *Shark.exe*. The configuration builder allows distributors to choose which folders and files to encrypt, which countries to target, and what email address to use to receive notifications after victims are infected. Shark appends .locked to encrypted file names. Shark's ransom amount depends on the price that the distributor sets. UPDATE 9/14/2016: Shark has now been rebranded by its developers as the **Atom Ransomware Affiliate Program**. It is still available on a Clearnet WordPress website but now includes the Atom Payload Builder, an EXE file which makes it easier for distributors to produce a working, customized ransomware build. It uses AES-256 to encrypt files and sends the decryption key and victim ID via HTTPS to its C2 servers.

- Bleeping Computer provides more information about Shark here.
- The NJCCIC is not currently aware of any decryption tool available for Shark or the rebranded Atom.

**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.

**Smrss32** targets Windows OS and is distributed manually via Remote Desktop Protocol (RDP). Smrss32 identifies itself as CryptoWall, although it is not as sophisticated. Smrss32 is named after its executable file, *smrss32.exe*, and targets 6,674 file extensions. It uses an AES symmetrical encryption algorithm and appends .encrypted to encrypted file names. Smrss32 demands a ransom payment of 1 Bitcoin.
UPDATE: 8/26/2016: **Smrss32** is now being distributed via email containing malicious attachments masquerading as news about the US election.

- Softpedia provides more information about Smrss32 here.
- Victims impacted by Smrss32 can contact security researchers on the Bleeping Computer forum here to have their files decrypted for free.

**SNSLocker** targets Windows OS and is distributed via malicious email attachments, file sharing networks, and browser hijacker malware that leads victims to poisoned links. It is written in .Net Framework 2.0 and leverages Microsoft .Net Crypto API. SNSLocker encrypts files using AES-256, appends the encrypted file extensions to .RSNSlocked, and demands a ransom payment of $300 USD. The creator of this variant encoded the location of the C2 server as well as the server's login credentials which has allowed security researchers to locate the decryption keys for victims impacted by SNSLocker.

- Trend Micro has more information about SNSLocker here.
- Trend Micro offers a decryption tool for files encrypted by SNSLocker, available here.

**Stampado** targets Windows OS and is currently being marketed to potential attackers as a "Ransomware-as-a-Service" opportunity on the Dark Web. The developers of this ransomware kit are selling lifetime licenses for $39 USD each and offering customers the ability to customize various elements of the malware. Stampado allows malicious files to be sent to victims in one of the following file formats: .exe, .bat, .dll, .scr, and .cmd. According to the developers' video demonstration, Stampado does not require administrator privileges to run on victims' machines, appends .locked to encrypted files, and gives victims 96 hours to pay the ransom before permanently deleting the decryption key. The ransom note displays two countdown timers – one displaying the amount of time remaining until the decryption key is deleted and one showing the "Next Russian Roulette file deletion" when the malware will randomly delete one file for every six hours the ransom goes unpaid.
UPDATE 9/2/2016: A version of Stampado discovered by Emsisoft encrypts the files names of encrypted files, changing them to hex characters and appending the extension *.locked* to the new file name.
UPDATE 9/8/2016: **Philadelphia Ransomware**, a new version of Stampado, is now for sale on a dark web marketplace for $400 USD. It includes a fully customizable build, allowing attackers to create unique extensions to append to encrypted files, determine which folders will be searched for targeted file types, change the appearance of the file icon, edit the interface text, and add multiple languages. Other features include automatically detecting when a ransom payment has been made, displaying text in the appropriate language based on the victim's system, User Access Control manipulation, and spreading the infection via connected USB drives and other computers residing on the network. The most unique feature is the inclusion of a "Mercy Button" to allow attackers to decrypt their victims' files for free. A PHP script called "Bridges" is required for setup and Philadelphia Ransomware provides a client interface that allows attackers to manage multiple infections and encryption keys from their own systems. This version, along with previous versions, can be decrypted for free using the tool listed below.
UPDATE: 9/15/2016: Stampado now encrypts files that have already been encrypted by other ransomware variants, resulting in multiple layers of encryption. The tool listed below decrypts this version.

- Heimdal Security provides more information about Stampado here.
- Emsisoft provides a free decryption tool for Stampado, available here.
- Emsisoft provides a free decryption tool for Philadelphia Ransomware, available 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 most recent version is **TeslaCrypt 4.1A** which targets new file extensions and uses very sophisticated anti-analysis and evasion techniques, according to Endgame, Inc.
UPDATE 5/18/2016: The developers of TeslaCrypt have ended this ransomware campaign and released the master decryption key.

- 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.
- Bitdefender Labs has created a free TeslaCrypt infection prevention tool, or "vaccine," available here.
- Talos provides more information about TeslaCrypt, found here.
- Additional free tools specific to the removal of TeslaCrypt 3.0 can be downloaded here.
- ESET provides a free decryption tool for TeslaCrypt 3.0 and 4.0 here. Information on how to use the tool can be found 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. TorrentLocker appends .encrypted or .enc to encrypted files.

- 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.

**TowerWeb** targets Windows OS and the method of distribution is currently unknown. It is a screen locker that pretends to be ransomware and, once its executable is launched, the infected system continuously reboots itself. However, this process can be stopped by entering shutdown -a in the command line prompt. It also swaps the functions of the left and right mouse buttons to frustrate the victim. TowerWeb only deletes files in the user's profile, temp folder, and recycle bin and does not encrypt any files. TowerWeb demands a ransom payment of $100 to $125 USD but deleted files can be recovered using data recovery software.

- Bleeping Computer provides more information about TowerWeb here.
- Since TowerWeb does not encrypt files, no decryption tool is needed.

**Trojan.Encoder.6491** targets Windows OS and is the first recorded ransomware variant that is written in Go, the programming language developed by Google. Its method of distribution is currently unknown. Encoder's malicious executable file is named *Windows_Security.exe*. It targets 140 different file types and encrypts them using AES-256. Encoder even encrypts the file names using the Base64 method and then appends *.enc* to the files. It regularly checks the attacker's Bitcoin wallet to determine whether or not the payment has been made by the victim and, if it has, Encoder automatically decrypts the files. Encoder demands a ransom payment of 0.052300 Bitcoin.

- Dr. Web provides more information about Trojan.Encoder.6491 here.
- Dr. Web has created a decryption tool for Trojan.Encoder.6491, but only provides free decryption service for Dr. Web customers who have purchased commercial licenses for the company's products.

**Troldesh**, also known as **Encoder.858** and **Shade**, targets Windows OS and it is distributed via the Axpergle and Nuclear exploit kits. First seen in 2015, Troldesh previously provided an email address for victims to contact the attackers in order

to negotiate the payment of the ransom. A recently discovered version of Troldesh, however, now uses a payment portal located on the Dark Web and requires victims to use Tor in order to visit the site and submit the ransom amount. It also comes bundled with additional malware named Mexar, downloads the Teamspy bot to obtain remote control of the victim's machine, and requests URLs of other malware sites from its C2 server. It also scans the victim's machine for banking files and software in an attempt to extort as much money as possible out of the victim. The original version appended .xbtl or .cbtl to encrypted files. The new version of Troldesh appends either .da_vinci_code or .magic_software_syndicate to encrypted files. The ransom amount varies and one Check Point security researcher reported negotiating a discount from the attackers behind the campaign.

- Microsoft provides more information about Troldesh here and here.
- Kaspersky provides a free decryption tool for Troldesh/Shade here with instructions for how to use it here.
- Intel Security provides a free decryption tool for Trodesh/Shade here.

**TrueCrypter** targets Windows OS and, currently, the distribution method is unknown. Once installed, it checks to see if it is running within a sandbox or virtual machine. It also checks for security software processes and, if any are detected, TrueCrypter will terminate them. It encrypts files using AES-256 and stores the generated key at the end of each file. It also deletes Shadow Volume Copies to prevent file restoration. Files encrypted by TrueCrypter display the .enc file extension. It demands a ransom payment of .2 Bitcoin or $115 USD paid via Amazon gift cards. This variant, however, is poorly written and merely clicking the "Pay" button without submitting payment will begin the decryption process. Once the files are decrypted, TrueCrypter removes itself from the infected machine.

- Bleeping Computer provides more information about TrueCrypter here.
- To decrypt files encrypted by TrueCrypter, click on the "Pay" button without submitting payment.

**Unlock92** targets Windows OS and the method of distribution is currently unknown. For each victim, Unlock92 creates one random 64-character hexadecimal password and then locks files using symmetric AES encryption. Files encrypted by Unlock92 are appended with .CRRRT. Security researchers have determined that Unlock92 was created by the author of the Kozy.Jozy variant.

- Softpedia provides more information about Unlock92 here.
- Bleeping Computer provides a free decryption tool for Unlock92 here.

**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.

**WildFire**, previously known as **Zyklon** and **GNL**, targets Windows OS and is distributed via spam emails containing malicious Word documents sent by the Kelihos botnet. Once a system is infected by WildFire, it will attempt communication with one of four C2 servers before proceeding with the encryption process. Wildfire developers claim to use AES-256 encryption and a 32-character long password to prevent victims from accessing their files. Appended filenames associated with WildFire and previous strains include .locked and .zyklon. The ransom payment demand for WildFire is $299 USD but threatens to increase the price to $999 USD after the specific date listed on the ransom note.

- Cisco provides more information about WildFire here.
- McAfee provides a free decryption tool for WildFire, available here.
- Kaspersky provides a free decryption tool for WildFire, available here.

**Xorist** is a family of ransomware that targets Windows OS and is distributed as an automatic ransomware builder that allows cyber threat actors to create and customize their own version of the malware. Files encrypted by Xorist typically

display the following extensions, although creators can customize this feature as well: EnCiPhErEd, .73i87A, .p5tkjw, and .PoAr2w. Once a system is infected, Xorist will display a ransom note that instructs the victim to send an ID via SMS to a specific phone number. Once the victim follows the attacker's instructions, the attacker will then send a code back to the victim via SMS to begin the decryption process.

- Bleeping Computer provides more information about Xorist here.
- Emsisoft offers a decryption tool for files encrypted by Xorist 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 here.
- The NJCCIC is not aware of any decryption tools available for XRTN.

**ZCryptor** targets Windows OS and exhibits worm-like behavior. Initial attack vectors include spam email campaigns, macro malware, and fake Adobe Flash installers but, once a targeted system is infected, ZCryptor drops an autorun.inf file onto network drives and removable storage media. It maintains persistence by placing a zycrypt.lnk file in the start-up folder. It appends all encrypted files with the extension .zcrypt. It demands an initial ransom of 1.2 Bitcoin but threatens to raise the price to 5 Bitcoin if the victim does not pay within four days of infection. If a week passes before any ransom is paid, the decryption key will be destroyed, according to ZCryptor's ransom note.

- Microsoft provides more information about ZCryptor here.
- The NJCCIC is not aware of any decryption tools available for ZCryptor.

**Zimbra**, written in Python, specifically targets Synacor's Zimbra email collaboration platform. It is thought to be distributed by the attacker executing a Python script directly on the Zimbra server. Once launched, the Zimbra variant proceeds to generate an AES key, encrypt that with an RSA key, and then send the key back to the attacker via email. It then drops a ransom note labeled how.txt in the root folder and encrypts all of the emails and mailboxes located within the opt/zimbra/store folder. Files encrypted by Zimbra are appended with the extension .crypto. Zimbra demands a ransom payment of 3 Bitcoin.

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