National Cybersecurity and Communications Integration Center

01 November 2013

Cryptolocker Ransomware

Cryptolocker Description

The following product is a coordinated effort between NCCIC, U.S. Secret Service and The Cyber Intelligence Network (CIN), provided to assist in prevention, detection and mitigation of a new ransomeware campaign. Ransomware is malware that restricts access to infected computers and requires victims to pay a ransom in order to regain full access. Cryptolocker is particularly interesting in that it functions by encrypting victims computer files with a combination of RSA-2048 and AES-256 encryption. Once encrypted, victims are provided a window of time in which they can pay the actors to receive the key needed to decrypt their files.

At this time, the primary means of infection appears to be phishing emails containing malicious attachments.[1] According to a trusted third party, at least some of these emails have come from the Cutwail botnet. Cutwail is a well-known spam botnet that has previously launched campaigns distributing the Gameover Zeus Trojan among other forms of malware.[2] This may indicate that those responsible for this campaign are using third party cyber-crime services to spread this malware. In addition, there have been reports that some victims had the malware dropped onto their machines through a preexisting backdoor existing from a previous infection with Zeus botnet malware. This may indicate the actor's use of a pay per install third party service.

Malicious emails have been delivered with various lures including subject lines payroll or package tracking from UPS, and FedEx; as well as bank correspondence and voicemail notifications. Some identified keywords used in these emails include:

- Payroll Received by Intuit
- ADP RUN: Payroll Processed Alert
- Payroll Manager Payroll Invoice ADP RUN
- Payroll Processed Alert Annual form ACH Notification
- Annual Form - Authorization to Use Privately Owned Vehicle on State Business
- DNB Complaint - (Number)

In addition, the malware has the ability to locate files located within shared network drives, USB drives, external hard drives, network file shares and even some cloud storage drives. This means that if the malware can infect one user who has access to all the shared file drives within an organization's network, it's possible all those files may become encrypted.

Due to the nature of asymmetric encryption, victims need access to a private key to decrypt their files. Unfortunately, this private key is stored on the actors C2 server. When the malware finishes the encryption process, a warning message appears on the victims screen indicating their files have been encrypted and to recover them, the victim needs to pay a fine of between 100 – 300 Dollars or Euros. Payment is accepted via bitcoin, GreenDot or MoneyPak. The message indicates that victims have a window of between 72 – 100 hours to pay the ransom or the private key needed to decrypt the files will be deleted from the C2 and victims will lose the ability to decrypt affected files. Each public and private key combination is different so one victim's private key will not work to decrypt the files of another victim.[3] It should be noted that the actors behind this campaign are not stealing victim information; they are simply holding it hostage.[4]

Unfortunately once the malware has successfully encrypted a victims files there is no way to decrypt them without the private key. This highlights the importance of backing up files as the best method of system recovery is to remove the malware and restore files from backup. Reports indicate that users who have paid the fine have been able to get their files back. However, some of the C2 servers are being taken offline and payments sent by users have not been received, leaving the victim poorer without the decryption key. Some victims have claimed online that by posting complaints on public forums discussing Cryptolocker, they have received "customer support" from the malicious actors themselves who have assisted the victims in ensuring their payment is registered and that they receive the decryption key. As awareness of this malware continues to spread, antivirus vendors are updating their signatures to detect its presence.

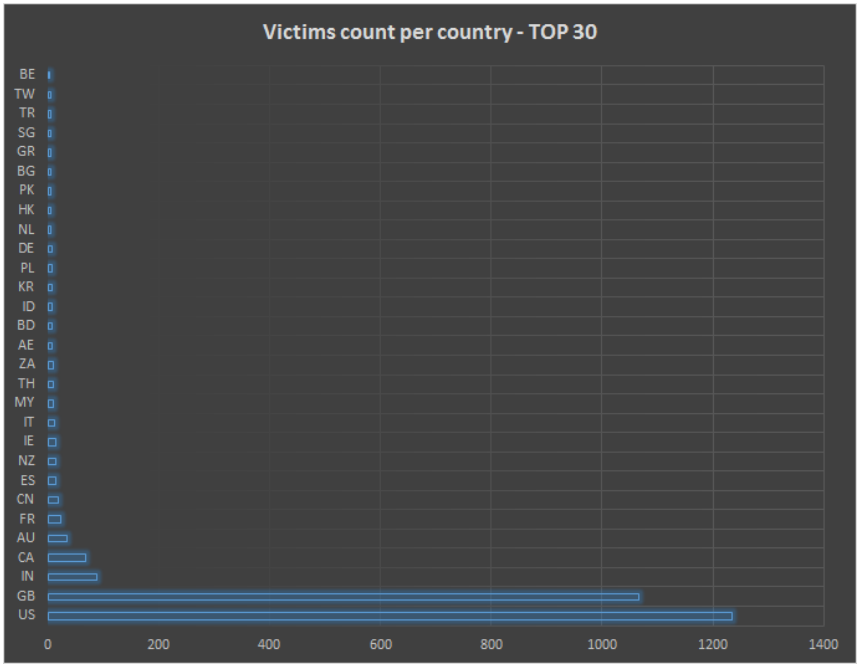
Infection

Multiple reports of Cryptolocker infections have surfaced in third party and open source reporting since the ransomeware's September discovery; some of which include:

- On 06 September 2013, when CryptoLocker was first identified, a private sector partner in Northern California was affected by CryptoLocker, which destroyed a number of files.
- In September 2013, a law enforcement agency in Northern California was infected by CryptoLocker and required a month to repair the damage.
- In September 2013 a Missouri Sheriff's Office reported department-wide infection with CryptoLocker, which seriously affected their operations.

- On 16 October 2013, a Connecticut State Agency was affected by Cryptolocker, which infected a laptop and a number of office files located on the connected share-drive for the agency. Though a majority of the affected files were recovered through a backup, some files were lost. Between 23 October 2013 and 25 October 2013 approximately 125 outbound e-mails were blocked at the mail gateway with the subject of "Voice Message from Unknown Caller".
- On 23 October 2013, a Southern California municipal city government received a spear-phishing e-mail with the CryptoLocker attachment.
- On approximately 25 October 2013, a Kansas Public Utility company reported infection that destroyed some administrative files.[5]

Although it appears the phishing campaign has a wide distribution, the phishing emails apparent focus on payroll related items could indicate that commercial organizations are the intended targets.[6]



Kapersky Lab researchers were able to reverse engineer the DGS algorithm used by Cryptolocker and locate and sinkhole 3 C2 domains. Their findings showed that the highest presence of Cryptolocker malware exists in the US and UK. In addition, on 16 October 2013, 1,266 unique IPs were identified contacting the sinkholed domains. This gives a glimpse into the size of this campaign.

Prevention

The following preventative measures are recommended to protect your organization from a Cryptolocker infection:

- Ensure all employees are aware of the threat and do not open suspicious e-mails or unexpected attachments.
- End-users should verify the identity of the sender of any attachments, whether through an informal consistency check of the e-mail address and content of the e-mail or formal communication with the sender.
- Perform regular backups of all systems to limit the impact of data and/or system loss.
- Apply changes to your Intrusion Detection/Prevention Systems and Firewalls to detect the indicators of compromise in Appendix A and block any associated domains or IP addresses.
- Restrict access to sensitive files & ensure personnel only can access the data necessary to perform their jobs.
- Secure open share drives by only allowing writable access to necessary user groups or authenticated users.
- Update all anti-virus programs and enable automatic updates for malware-signatures and software.
- Ensure the timely updating/patching of all software by using automatic updating and/or patching.

Individuals and organizations can use the Windows Group or Local Policy Editor to create Software Restriction Policies that block executables from running when they are located in specific paths. Microsoft provides additional Software Restriction Policy configuration guidance:[7],[8],[9]

Mitigation

If you believe your computer has been infected with the Cryptolocker virus:

- Immediately disconnect your system from the wireless or wired network. This will prevent the virus from further encrypting any more files on the network. [10]
- Immediately turn off any data synchronization software that automatically synchronizes your data changes with other servers. They may be useful, but can propagate the corrupted files as the synchronizer will consider the newly Cryptolocker-encrypted versions the most recent version to back-up.
- Delete the Registry values and files to stop the program from continuing the loading and encryption process.
- It is important to note that Cryptolocker spawns two processes of itself. If you only terminate one process, the other process will automatically launch. You must use a program such as "Process Explorer" and click on the first process and select "Kill Tree". This will terminate both processes at the same time. The encrypted data can then be restored via a backup.
- To restore files you should be able to use "Shadow Volume Copies" (previous versions of your files), which are only available with Windows XP Service Pack 2, Windows Vista, Windows 7, and Windows 8.
- To manually restore individual files, right-click on the file, go into "Properties", and select the "Previous Versions" tab. This tab will list all copies of the file that have been stored in a Shadow Volume Copy and the date they were backed up. To restore a previous version of the file, click on the "Copy" button and then select the directory you wish to restore the file to. This same method can be used to restore entire folders.
- A program called "Shadow Explorer" has been used by other users to restore multiple folders at once. However, use your judgment in downloading freeware.
- If System Restore is enabled on your computer, then it is possible to restore previous versions of the encrypted files once the virus has been disabled.
- Currently there is no known way to retrieve the private key that can be used to decrypt the encrypted files.
- If possible, turn on file provisioning within your backup system.

Technical Indicators

Cryptolocker does not need special or privileged account access to perform this function. According to reports, the malware targets victims running Windows 7, Vista, and XP operating systems.

Victim files are encrypted using Asymmetric encryption. Asymmetric encryption, as opposed to symmetric encryption uses two different keys for encrypting and decrypting messages. Asymmetric encryption is a more secure form of encryption as only one party is aware of the private key, while both sides know the public key. This allows encrypted messages to be sent where only the message receiver has the key needed to decrypt the message or file.

When initial infection occurs, Cryptolocker saves itself as a randomly named file within the %AppData% or %LocalAppData% and creates an autostart entry in the registry so that the malware launches when a user logs in. When the malware installs it will make a POST request to a hard-coded IP address or domain (e.g., http: / / 184.164.136.134 / home /). This Command and Control (C2) has changed multiple

times as it was flagged for abuse by security researchers. If a connection to the hardcoded C2 cannot be made, the malware seeks a live C2 server by using Domain Generation Algorithm (DGA). This algorithm allows the malware to generate 1,000 domains per day and seeks the first available connection. When the malware locates a C2 it sends an RSA-encrypted payload containing information about the malware version, the system language, an ID and Group ID. The C2 then responds with a public key made for that infected host. That key is then used to seek out a wide range of file extensions on the victim's machine and begin the encryption process. These extensions include:

***.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.pdf, *.eps, *.ai, *.indd, *.cdr, *.jpg, *.jpe, img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c.**

The following file paths are known to have been used by this infection and its droppers:[11]

XP

- C: \ Documents and Settings \ <User> \ Application Data \ <random name>.exe
- C: \ Documents and Settings \ <User> \ Local Application Data \ <random name>.exe

Windows Vista / 7

- C: \ Users \ <User> \ AppData \ Local \ <random name>.exe
- C: \ Users \ <User> \ AppData \ Local \ <random name>.exe

Cryptolocker samples have saved themselves as randomly named files in the %AppData% (XP) or %LocalAppData% (Vista / 7) folder and have added to the following registry key, which is used to autostart Cryptolocker when users log into their computers:

- HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run

It also modifies the following registry key to include "CryptoLocker_<version_number>" for a redundant start:

- HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ RunOnce

IP Indicators:[12]

192.210.230.39 [USA – NY]
194.28.174.119 [Ukraine]
212.71.250.4 [England]
86.124.164.25 [Romania]
87.255.51.229 [Netherlands]
93.189.44.187 [Russia]

Sample Email Indicators:
Subject: "Annual Form - Authorization to Use Privately Owned Vehicle on State Business"
Attachment: Attachments follow the naming convention of "Form_[Varying Digits and Numbers].zip.
For example: Form_nfcausa.org.zip, Form_20130810.exe, Form_f4f43454.com.zip.
Spoofed Sender: "fraud@aexp.com" "Dewayne@nfcausa.org"
Sender IP: 209.143.144.3
Sender Host: mail.netsential.com

Registry Indicators:
HKCU\Software\CryptoLocker
HKCU\Software\CryptoLocker\Files (This key reportedly contains a list of encrypted files)
HKCU\Software\Microsoft\Windows\CurrentVersion\Run CryptoLocker = <Reference to file location>

File System Indicators:
Windows Vista and later: C:\Users\<username>\AppData\Roaming\{CLSID}.exe
Windows XP and before: C:\Documents and Settings\<username>\Application Data\{CLSID}.exe

References

[1] http://www.computerworld.com.my/resource/security/cryptolocker-how-to-avoid-getting-infected-and-what-to-do-if-you-are/?page=1
[2] http://www.infosecurity-magazine.com/view/35180/cutwail-spam-campaign-dumps-blackhole-for-magnitude-exploit-kit/
[3] http://www.securelist.com/en/blog/208214109/Cryptolocker_Wants_Your_Money
[4] http://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/
[5] http://www.tripwire.com/state-of-security/top-security-stories/public-utilitys-systems-shut-cyber-attack/
[6] Trusted Third Party
[7] http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information#prevent
[8] http://support.microsoft.com/kb/310791
[9] http://technet.microsoft.com/en-us/library/cc786941(v=ws.10).aspx
[10] http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information
[11] Trusted Third Party
[12] Trusted Third Party