Situational Advisory

10 June 2014

DISTRIBUTION NOTICE - TLP: GREEN

(U) **Warning**: This product is **UNCLASSIFIED//FOR OFFICIAL USE ONLY** (U//FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with the DHS policy for FOUO information and is not to be released to the public, media, or other personnel who do not have an authorized *need-to-know* without appropriate prior authorization. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector officials without prior approval.

(U) The **Traffic Light Protocol** (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. This document is "TLP: **GREEN**". Recipients may share this information only with peers and partner organizations within their sector or community, but not via publicly accessible channels. For more information on the Traffic Light Protocol please go to http://www.us-cert.gov/tlp/.

(U//FOUO) New Ransomware "CryptoWall" Rapidly Infecting Systems Across the United States

(U) Scope and Distribution

(U//FOUO) This product addresses the recent wave of CryptoWall (not to be confused with "CryptoLocker"[1]) ransomware[2] infections throughout the United States. Included are prevention and incident response mitigation strategies, as well as a description of the malware and helpful sources. This product is **U//FOUO / TLP: GREEN** and *should be shared as widely as possible* with all partners.

(U) Key Points

- (U//FOUO) CryptoWall is a new form of ransomware that has impacted numerous organizations across the United States, including municipal agencies.
- (U) The primary infection vectors for CryptoWall are spear-phishing emails, made to look like communications from legitimate companies, and compromised advertisements displayed on highly trafficked websites.
- (U) Upon executing on a system CryptoWall immediately begins to encrypt any files the user has access to, including data on shared drives.
- (U) The damage done to affected files by CryptoWall is irreversible and typically requires restoring locked files from existing back-ups.
- (U//FOUO) Currently, while some (but not all) major anti-virus software companies can now detect the attack after-the-fact, CryptoWall can still encrypt files on the infected computer before being discovered.

(U) Background

(U//FOUO) CryptoWall is a new ransomware discovered in late April 2014 that affects all versions of Windows.[i] The most common infection vectors for CryptoWall are spear-phishing e-mails with malicious attachments (e.g. PDFs which, when opened, executes CryptoWall) or compromised advertisements on highly trafficked websites, such as news or social media sites.

[1] See US-CERT Alert #TA13-309A "CryptoLocker Ransomware Infections" published November 05, 2013, last revised June 05, 2014: http://www.us-cert.gov/ncas/alerts/TA13-309A

[2] (U) Ransomware is a type of malicious software designed to block access to a computer system or files until a sum of money is paid.

(U//FOUO) Upon execution, CryptoWall immediately encrypts all user-accessible files on the local drive and any mapped networks or storage devices. After encrypting the accessible files CryptoWall displays a message giving victims a 100-hour countdown while demanding a payment of approximately $500 in bitcoins in exchange for the decryption key – though this amount has varied according to open source reporting. If the user does not pay within the demanded timeframe, the amount of the ransom increases.

(U//FOUO) Several CryptoWall spear-phishing e-mails identified to this point have been crafted to look like communications from legitimate companies and requested the user download or open an "EFAX". Other malicious emails may be disguised as notifications sent from UPS or the "Payroll Department".[ii]

(U//FOUO) Open source reporting indicates that the actors behind CryptoWall are utilizing an off-the-shelf exploit kit[3] known as "RIG", which hijacks advertising on high profile websites to redirect visitors to other malware-laden sites.[iii]

(U//FOUO) Per incident reports shared by analysts across the country, CryptoWall has done damage to numerous organizations in the past month:

- (U//FOUO) In late May 2014, a local fire department in Northern California was infected by CryptoWall, resulting in the compromise of at least one computer and one server, destroying vital information. The agency was able to restore their systems and the data from a backup.
- (U//FOUO) In early June 2014, several local public safety agencies in Southern California were infected by CryptoWall, resulting in the compromise of over one hundred computers and ten servers. The agencies were able to restore their systems from a backup with assistance from the MS-ISAC.
- (U//FOUO) In late May 2014, a municipal agency in Virginia found that two of their computers had been infected with CryptoWall.

(U//FOUO) Thus far, the majority of victims are located in the United States, though numerous victims have been affected across multiple sectors. ***In at least one incident, CryptoWall masqueraded as a program that claims the user needs to decrypt a file before being able to read it. Once the user tries to open the file, CryptoWall replicates itself across multiple locations on the user's machine and demands payment. CryptoWall may also be disguised as legitimate software updates such as (but not limited to) Abode Reader, Flash Player, and Java Runtime Environment updates.***[iv]

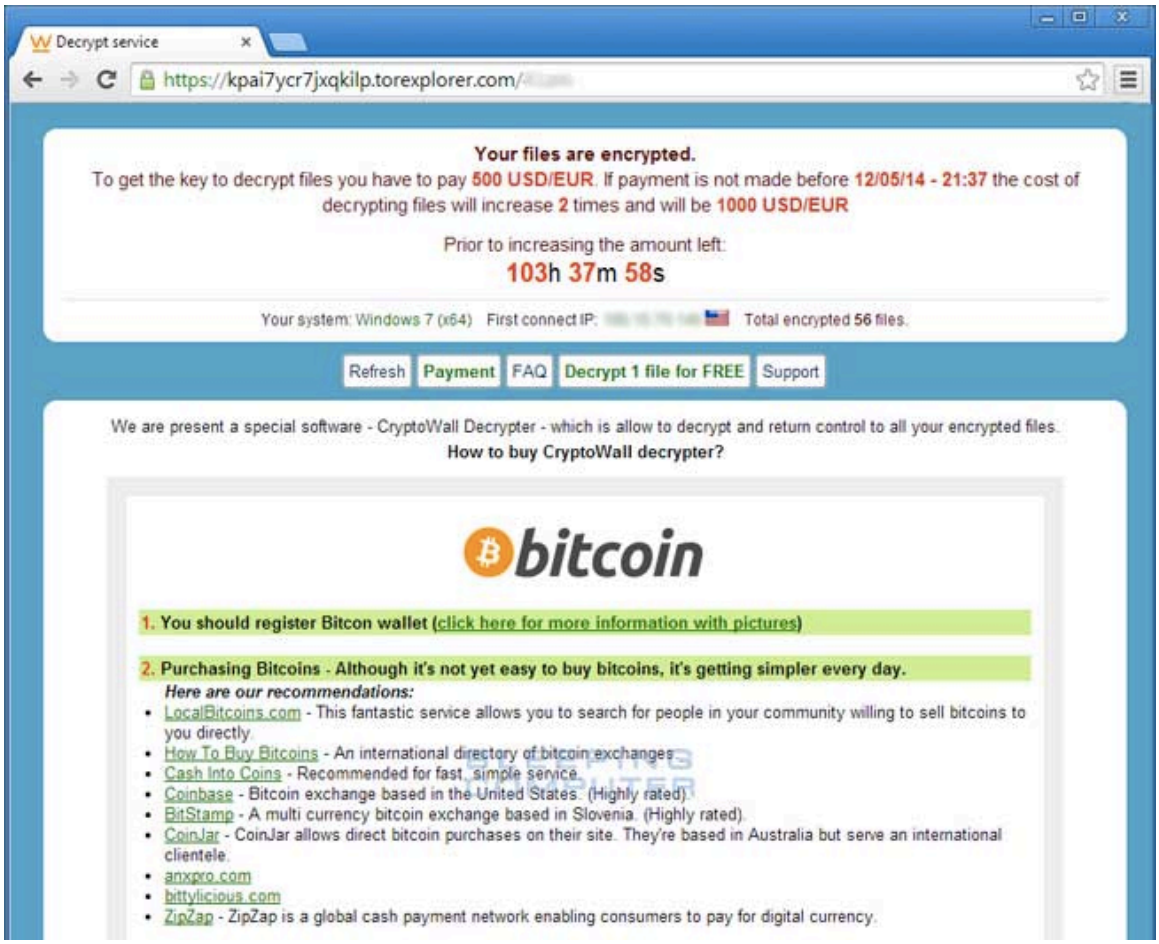
(U//FOUO) Due to the strength of the encryption, which uses unique RSA-2048 bit keys generated in each infection, the private decryption key is necessary to decrypt the affected files. A number of the victims have had to wipe the affected files and restore them from back-ups. Because CryptoWall can encrypt across the network (i.e. anything the user has access to, including anything on accessible mapped networks) it is possible the malicious actors are targeting organizations that would be most damaged by the malware.

(U//FOUO) The success of CryptoWall is likely due to the widespread spear-phishing campaign, the effective spear-phishing lures used by the malicious actors, the diversity in infection vectors – including spear-phishing and malicious advertisements, the fact that numerous anti-virus providers still cannot detect CryptoWall, and the rapidity with which CryptoWall activates upon execution and begins causing damage.

[3] (U) An exploit kit is a type of malware that exploits security holes found in software applications (e.g. Adobe Reader) for the purpose of spreading and executing malware.

(U//FOUO) It is very likely we will continue to see more ransomware similar to CryptoWall in the near future due to this successful campaign and due to the availability of "off the shelf" malware and exploit kits for sale on underground cybercrime forums.

(U) An example of the CryptoWall lock-screen can be seen below.



(U//FOUO) CryptoWall Lock-Screen from a 8 May 2014 Open Source Incident

(U//FOUO) Files that have executed CryptoWall include the following[v]:

- A shortcut icon to a web page named "Decrypt Instructions"
- A file named "DECRYPT_INSTRUCTIONS.html"
- A file named "DECRYPT_INSTRUCTIONS.txt"

(U//FOUO) If users see these files on their computer they should be advised to delete them immediately and notify their systems administrator.

(U) Preventative Measures

(U) Technical indicators from the Multiple State Information Sharing and Analysis Center[vi] (MS-ISAC) can be found in the Appendix.[vii]

(U) The following preventative measures are recommended to protect your organization from a CryptoWall infection:

- (U) Restrict access to sensitive files & ensure personnel only can access the data necessary to perform their jobs.
- (U) Instruct users not to open any files that appear on the desktop with the name "DECRYPT_INSTRUCTIONS"
- (U) Ensure that all users are running patched versions of Flash, Java and the Silverlight multimedia program, as those are programs the exploit kit attempts to exploit.
- (U) Ensure the timely updating/patching of all software by using automatic updating and/or patching.
- (U) Ensure all employees are aware of the threat and do not open suspicious e-mails or unexpected attachments, including those e-mails requesting the employee "open a Fax" or "EFAX".
- (U) Instruct end-users to 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.
- (U) Perform regular backups of all systems to limit the impact of data and/or system loss.
- (U) Ensure backups are stored externally to limit the possibility that the backup files are impacted as well.
- (U) Block execution of applications in the AppData Temp folders, as infections tend to run from these locations.
- (U) Block zip files from mail server or configure server to unzip and check attachments before sending it through.
- (U) Completely block password protected zip files
- (U) Block malicious domains at the external router to ensure that any machines infected are not able to communicate with the Command and Control servers to complete the encryption process.
- (U) Utilize an e-mail spam filter and ensure it is updated to identify the most recent malware variants, including CryptoWall.
- (U) Update all anti-virus programs and enable automatic updates for malware-signatures and software.
- (U) Apply changes to your Intrusion Detection/Prevention Systems and Firewalls to detect the indicators of compromise in the Appendix and block any associated domains or IP addresses.
- (U) Secure open share drives by only allowing writable access to necessary user groups or authenticated users.

(U) Post-Infection Mitigation Measures[4]

(U) If you believe your computer has been infected with the CryptoWall virus:

- (U) Immediately disconnect your systems from the wireless or wired network. This will prevent the virus from further encrypting any more files on the network.
- (U) Immediately turn off any data synchronization software that automatically synchronizes your data changes with other servers, which can propagate the corrupted files as the synchronizer will consider the newly CryptoWall-encrypted versions the most recent version to back-up.
- (U) If *confident* in an infection - pull the power plug or remove the battery immediately so as to shut down the Operating System and halt the encryption process.
- (U) Contact your IT manager.

[4] (U) Always consult an IT professional before employing any mitigation measures.

(U) Information Gaps / Requests for Information (RFIs)

- (U//FOUO) Who are the malicious actors behind CryptoWall?
- (U//FOUO) Is there any way to get the private decryption key without paying the ransom?
- (U//FOUO) How many organizations have been affected by CryptoWall?
- (U//FOUO) Is CryptoWall currently being offered for sale on underground cybercrime forums?

(U//FOUO) If you have information responsive to any of the above RFIs, or any more information about CryptoLocker in general that has not been covered here, please contact the Utah SIAC cyber analysts at (801) 256-2360 or siac@utah.gov.

(U) Sources/Credit

(U//FOUO) This product was produced through the coordinated efforts of the following organizations and CIN members:

- (U) Arizona Counter Terrorism Information Center (ACTIC)
- (U) The Center for Internet Security (CIS)
- (U) Iowa Department of Administrative Services
- (U) KC Regional Terrorism Early Warning (KCTEW)
- (U) Northern California Regional Intelligence Center (NCRIC)
- (U) Orange County Intelligence Assessment Center (OCIAC)
- (U) Virginia Fusion Center

(U) Appendix: Technical Indicators for CryptoWall from the MS-ISAC[viii] (for IT Professionals)

Domain Indicators:

yoyosasa.com
wawamediana.com
qoweiuwea.com
khalisimilisi.com
dominikanabestplace.com
nofbiatdominicana.com
dominicanajoker.com
likeyoudominicana.com
newsbrontima.com
yaroshwelcome.com

Sample Email Indicators:

INCOMING FAX REPORT: Remote ID: <{3 digits}-{3 digits}-{3 digits}>
Fax Message at <yyyy-mm-dd hh:mi:ss EST boundary="———————{23 digits}"
UPS Exception Notification, Tracking Number <tracking number>

ex. INCOMING FAX REPORT: Remote ID: 385-567-7335
ex. Message at 2014-05-06 08:11:55 EST boundary="———————050206007030402050403 03"
ex. UPS Exception Notification, Tracking Number 1Z522A9A6892487822

Sample Email Sender Name <Sender Email Address>:

Incoming Fax
Fax Message
UPS Quantum View <auto-notify@ups.com>

Registry Indicators:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\<random>.exe
"Debugger" = 'svchost.exe'
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CryptoWall Decrypter
HKEY_LOCAL_MACHINE\SOFTWARE\CryptoWall Decrypter

Other Registry Changes Made by CryptoWall:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings "WarnOnHTTPSToHTTPRedirect" = '0'
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings "WarnOnHTTPSToHTTPRedirect" = '0'
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings "WarnOnHTTPSToHTTPRedirect" = '0'
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore "DisableSR " = '1'

File System Indicators:

DECRYPT_INSTRUCTION.txt
DECRYPT_INSTRUCTION.html
DECRYPT_INSTRUCTION.url
%UserProfile%\Application Data\Microsoft\[random].exe
%Documents and Settings%\All Users\Start Menu\Programs\CryptoWall Decrypter
%Documents and Settings%\All Users\Application Data\CryptoWall Decrypter
%Program Files%\CryptoWall Decrypter

(U) Endnotes

[i] (U) Per NetStandard "*Virus Alert: Crypto is Back*" dated 29 May 2014. http://www.netstandard.com/virus-alert-crypto-back/
[ii] (U) By Tomas Meskauskas of PCrisk.com "*CryptoWall Virus*" dated 9 May 2014 http://www.pcrisk.com/removal-guides/7844-cryptowall-virus
[iii] (U) By Andrew Tsonchev of Cisco "*RIG Exploit Kit Strikes Oil*" dated 5 June 2014 http://blogs.cisco.com/security/rig-exploit-kit-strikes-oil/
[iv] (U) Per EnigmaSoftware "*CryptoWall Ransomware*" http://www.enigmasoftware.com/cryptowallransomware-removal/
[v] CIS Cyber Alert – *CryptoWall Indicators* – TLP: White, Center for Internet Security, date June 9th, 2014
[vi] *Supra*
[vii] *Supra*
[viii] *Supra*