CMSGu2015-04

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Ransomware Removal

CERT-MU

National Computer Board
Mauritius

July 2015

Issue No. 4

Version 1.0

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to make users aware of ransomware, how it is propagated and how they can protect themselves against it.

1.2 Audience

The target audience for this document includes all users of the Internet.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 gives a background on ransomware.

Section 3 illustrates a ransomware variation.

Section 4 lists some known ransomware families.

Section 5 explains how to protect against ransomware.

Section 6 concludes the document.

Section 7 contains a list of references that have been used in this document.

2.0 Background

Ransomware is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Some ransomware encrypts files (called Cryptolocker). Other ransomware use TOR to hide C&C communications (called CTB Locker).

Users may encounter this threat through a variety of means. Ransomware can be downloaded by ignorant users by visiting malicious or compromised websites. It can also arrive as a payload, either dropped or downloaded by other malware. Some ransomware are delivered as attachments to spammed email.

Once executed in the system, a ransomware can either lock the computer screen or encrypt predetermined files with a password. In the first instance, a ransomware shows a full-screen image or notification, which prevents victims from using their system. This also shows the instructions on how users can pay for the ransom. The second type of ransomware locks files like documents, spreadsheets and other important files.

Ransomware is considered a “scareware” as it forces users to pay a fee (or ransom) by scaring or intimidating them.

2.1 Risks of ransomware

- Not being able to access any files or functions on infected computers ever again.
- Still not being allowed access to your files or functions, even when you have paid the ransom.

2.2 How is ransomware spread?

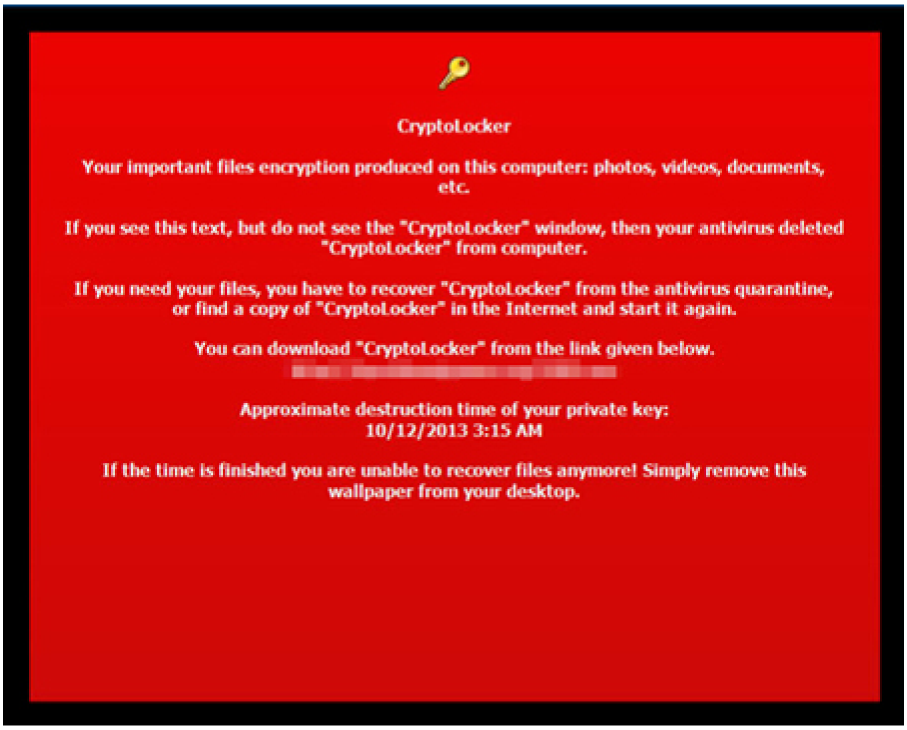
Your computer could be infected by ransomware when you or colleagues inadvertently:

- Open a malicious attachment in an email
- Click on a malicious link in an email, instant message, social networking site or other website
- Visit a corrupt website

- Open infected files from web-based digital file delivery websites, for example Dropbox
- Open corrupt macros in application documents (word processing, spreadsheets etc.)
- Connect corrupt USB connected devices (e.g. memory sticks, external hard drives, MP3 players)
- Insert corrupt CDs/DVDs into computers

3.0 Ransomware Example: CryptoLocker

CryptoLocker is a variant of ransomware that encrypts files, aside from locking the system. This is to ensure that users will still pay up even if the malware itself was deleted. Like previous types of ransomware, CryptoLocker demands payment from affected users, this time to unlock their now-encrypted files.



CryptoLocker

Your important files encryption produced on this computer: photos, videos, documents, etc.

If you see this text, but do not see the "CryptoLocker" window, then your antivirus deleted "CryptoLocker" from computer.

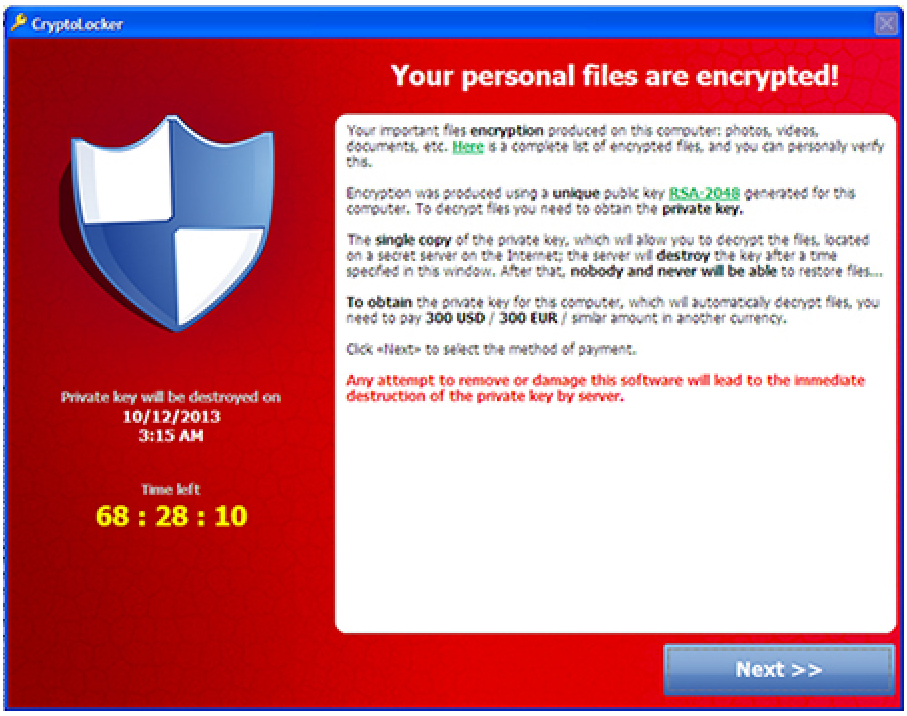
If you need your files, you have to recover "CryptoLocker" from the antivirus quarantine, or find a copy of "CryptoLocker" in the Internet and start it again.

You can download "CryptoLocker" from the link given below.
[redacted]

Approximate destruction time of your private key:
10/12/2013 3:15 AM

If the time is finished you are unable to recover files anymore! Simply remove this wallpaper from your desktop.

Figure 1 CryptoLocker Screen 1



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/12/2013
3:15 AM

Time left
68 : 28 : 10

Figure 2 CryptoLocker Screen 2

The malware uses an AES key to encrypt files. The AES key for decryption is written in the files encrypted by the malware. However, this key is encrypted with an RSA public key embedded in the malware, which means that a private key is needed to decrypt it. Unfortunately, the said private key is not available.

Near the end of 2013, a new variant of CryptoLocker emerged, with propagation routines. This variant, WORM_CRILOCK.A, can spread via removable drives, a routine unheard of in other CRILOCK variants. This means that the malware can easily spread compared to other variants. This new variant does not rely on downloader malware like CRILOCK to infect systems; rather, it pretends to be an activator for software in peer-to-peer (P2P) file sharing sites. Technical differences have led some researchers to believe this malware is a product of a copycat.

Another file encrypting ransomware soon came into the picture. This malware, known as CryptoDefense or Cryptorbit, like other encrypting ransomware, demands payment for its decryption services. Detected by Trend Micro as TROJ_CRYPTRBIT.H, this variant encrypts database, web, Office, video, images, scripts, text, and other non-binary files. It also deletes backup files to prevent restoration of encrypted files.

4.0 Known ransomware families

Within a couple of years, ransomware has evolved from a threat targeting Russian users into an attack affecting several European and North American countries. With payment schemes affording anonymity for its perpetrators, we may be seeing more of ransomware in the coming years. Thus, it is crucial for users to know how ransomware works and how to best protect themselves from this threat.

Below are known ransomware famiies:

Family Name	Aliases	Description
ACCDFISA	Anti Cyber Crime Department of Federal Internet Security Agency Ransom	First spotted early 2012; Encrypts files into a password-protected; Cybercriminals behind this ransomware asks payment thru *Moneypak*, *Paysafe*, or *Ukash* to restore the files and unlock the screen; Known as a multi-component malware packaged as a self-extracting (SFX) archive; May come bundled with third party applications such as *Sdelete* and *WinRAR*
ANDROIDOS_LOCKER		First mobile ransomware spotted; Uses Tor, a legitimate service that allows anonymous server connections; Users with mobile devices affected by this malware may find the files stored in their mobile device rendered useless and held for ransom
CRIBIT	BitCrypt	Similar to CRILOCK with its use of RSA-AES encryption for target files; Version 1 uses RSA-426; Version 2 uses RSA-1024; Appends the string *bitcryp1* (for version 1) and *bitcrypt2* (for version 2) to the extension name of the files it encrypts
CRILOCK	CryptoLocker	Employs Domain Generation Algorithm (DGA) for its C&C server connection; October 2013 - UPATRE was found to be the part of the spam mail that downloads ZBOT, which further downloads CRILOCK
CRITOLOCK	Cryptographic locker	Uses advanced encryption standard (AES-128) cryptosystem; The word *Cryptolocker* is written in the wallpaper it uses to change an affected computer's wallpaper
CRYPAURA		Encrypts files and appends the corresponding email address contact for file decryption
CRYPCTB	Critroni, CTB Locker, Curve-Tor-Bitcoin Locker	Encrypts data files; Ensures there is no recovery of encrypted files by deleting its shadow copies; Arrives via spam mail that contains an attachment, actually a downloader of this ransomware; Uses social engineering to lure users to open the attachment; Uses Tor to mask its C&C communications
CRYPDEF	CryptoDefense	To decrypt files, it asks users to pay ransom money in

		bitcoin currency
CRYPTCOIN	CoinVault	Encrypts files and demands users to pay in bitcoin to decrypt files; Offers a one-time free test to decrypt one file
CRYPTFILE		Uses unique public key generated RSA-2048 for file encryption and also asks users to pay 1 bitcoin to obtain private key for decrypting the files
CRYPWALL	CryptoWall, CryptWall, CryptoWall 3.0	Reported to be the updated version of CRYPTODEFENSE; Uses bitocin currency as mode of payment; Uses Tor network for anonymity purposes; Arrives via spam mail, following UPATRE-ZBOT-RANSOM infection chain; CryptoWall 3.0 comes bundled with FAREIT spyware
CRYPTROLF		Shows troll face image after file encryption
CRYPTTOR		Changes the wallpaper to picture of walls and asks users to pay the ransom
CRYPTOR	batch file ransomware	Arrives thru DOWNCRYPT; A batch file ransomware capable of encrypting user files using GNU Privacy Guard application
DOWNCRYPT	batch file ransomware	Arrives via spam email; Downloads BAT_CRYPTOR and its components such as a decoy document
VIRLOCK	VirLock, VirRansom	Infects document files, archives, and media files such as images
PGPCODER		Discovered in 2005; first ransomware seen
KOLLAH		One of the first ransomware that encrypts files using certain extension names; Target files include Microsoft Office documents, PDF files, and other files deemed information-rich and relevant to most users; Adds the string *GLAMOUR* to files it encrypts
KOVTER		Payload of the attack related to YouTube ads that lead to the Sweet Orange exploit kit
MATSNU		Backdoor that has screen locking capabilities; Asks for ransom
RANSOM		Generic detection for applications that restrict the users from fully accessing the system or encrypts some files and demands a *ransom* in order to decrypt or unlock the infected machine
REVETON	Police Ransom	Locks screen using a bogus display that warns the user that they have violated federal law; Message further declares the user's IP address has been identified by the Federal Bureau of Investigation (FBI) as visiting websites that feature illegal content
VBUZKY		64-bit ransomware; Attempts to use *Shell_TrayWnd* injection; Enables TESTSIGNING option of Windows 7
CRYPTOP	Ransomware archiver	Downloads GULCRYPT and its components
GULCRYPT	Ransomware archiver	Archives files with specific extensions; Leaves a ransom text file containing the instructions on who to contact and how to unpack the archives containing user's files
CRYPWEB	PHP ransomware	Encrypts the databases in the web server making the website unavailable; Uses HTTPS to communicate with the C&C server; Decrypt key is only available in the C&C server

CRYPDIRT	Dirty Decrypt	First seen in 2013 before the emergence of Cryptolocker
CRYPTORBIT		Detection for images, text, and HTML files which contain ransom notes that are indicators of compromised (IOC)
CRYPTLOCK	TorrentLocker	Poses as CryptoLocker; newer variants display *crypt0l0cker* on the affected computer; uses a list of file extensions that it avoids encrypting, compared to usual ransomware that uses a list of file extensions to encrypt - this allows CRYPTLOCK to encrypt more files while making sure the affected computer still runs, ensuring users know that their files are encrypted and access to the Internet to pay the ransom is still present
CRYPFORT	CryptoFortress	Mimics TorrentLocker/CRYPTLOCK user interface; Uses wildcards to search for file extensions; encrypts files in shared folders
CRYPTESLA	TeslaCrypt	User interface is similar to CryptoLocker; encrypts game-related files
CRYPVAULT	VaultCrypt	Uses GnuPG encryption tool; downloads hacking tool to steal credentials stored in web browsers; uses sDelete 16 times to prevent/hinder recovery of files; has a customer support portal; is a batch script crypto-ransomware
CRYPSHED	Troldesh	First seen in Russia; added English translation to its ransom note to target other countries; aside from appending .xtbl to the file name of the encrypted files, it also encodes the file name, causing affected users to lose track of what files are lost
SYNOLOCK	SynoLocker	Exploits Synology NAS devices' operating system (DSM 4.3-3810 or earlier) to encrypt files stored in that device; has a customer support portal
KRYPTOVOR	Kriptovor	Part of a multi-component infection; aside from its crypto-ransomware component, it has an information stealing component that steals certain files, processes list, and captures desktop screenshot; uses an open source Delphi library called *LockBox 3* to encrypt files

Table 1 Known ransomware families (Source: TrendMicro)

5.0 Avoiding ransomware

5.1 Removing ransomware

Users infected by ransomware should do the following:

- Disable System Restore.
- Run your anti-malware to scan and remove ransomware-related files.

Note: Some ransomware requires extra removal steps such as deleting ransomware files in Windows Recovery Console. Be sure to follow all required steps to completely remove the specific ransomware your computer has.

5.2 Preventing ransomware

To prevent ransomware infections, keep these things in mind:

- Have security software (such as antivirus software) installed and most importantly up to date with a current subscription. Remember with the thousands of new malware variants running every day, having a set of old virus definitions is almost as bad has having no protection.
- Make sure all the software on your system is up to date. This includes the operating system, the browser and all of the plug-ins that a modern browser typically uses.
- Apply software patches as soon as they become available. Some ransomware arrive via vulnerability exploits. One of the most common infection vectors is a malicious exploit that leverage a software vulnerability. Keeping software up to date helps minimise the likelihood that your system has an exposed vulnerability on it.
- Bookmark trusted websites and access these websites via bookmarks.
- Scan your system regularly with anti-malware.
- Avoid clicking on links or opening attachments or emails from people you don't know or companies you don't do business with.
- Ensure you have smart screen (in Internet Explorer) turned on.
- Have a pop-up blocker running in your web browser.
- Regularly backup your important files.
- You can back up your files with a cloud storage service that keeps a history or archive of your files, such as OneDrive.

6.0 Conclusion

Ransomware is predominantly found on suspicious websites, and arrives either via a “drive-by download”, stealth download or through a user clicking on an infected advert. Some distribution via email has also been seen. As a result, it is imperative that users know how these types of malicious software spread and how they can protect themselves so that they do not have to pay ransom if ever they fall prey of such types of attacks.

7.0 References

- **www.getsafeonline.org/online-safety-and-security/ransomware/**
- **www.microsoft.com**
- **http://www.trendmicro.com/**
- **http://us.norton.com**