# Detection and Prevention of Crypto-Ransomware

Daniel Gonzalez Thaier Hayajneh
Fordham Center for Cybersecurity
Fordham University, New York, NY, USA
{Dgonzalez50, thayajneh}@fordham.edu

***Abstract* - Crypto-ransomware is a challenging threat that ciphers a user's files while hiding the decryption key until a ransom is paid by the victim. This type of malware is a lucrative business for cybercriminals, generating millions of dollars annually. The spread of ransomware is increasing as traditional detection-based protection, such as antivirus and anti-malware, has proven ineffective at preventing attacks. Additionally, this form of malware is incorporating advanced encryption algorithms and expanding the number of file types it targets. Cybercriminals have found a lucrative market and no one is safe from being the next victim. Encrypting ransomware targets business small and large as well as the regular home user. This paper discusses ransomware methods of infection, technology behind it and what can be done to help prevent becoming the next victim. The paper investigates the most common types of crypto-ransomware, various payload methods of infection, typical behavior of crypto ransomware, its tactics, how an attack is ordinarily carried out, what files are most commonly targeted on a victim's computer, and recommendations for prevention and safeguards are listed as well.**

**Index Terms – Bitcoin; Domain Generated Algorithm (DGA); Crypto-Ransomware; Cryptographic Ransomware (CGR); Private-key cryptosystem ransomware**

## I. Introduction

Crypto-ransomware is a special type of malware which aims to encrypt the files on the victim's device using strong cryptography. The malware then notifies the user, after the files are encrypted, that their files were encrypted and demands a ransom (usually in Bit-Coins or other cryptocurrency) for decryption and release of the files. There is usually some sort of timer or deadline posted warning the user that after the time has expired their files are no longer accessible for recovery by the recovery key. The attacker will keep a copy of decryption key stored only on his server to prevent victims from recovering their files and force them to pay the ransom. Users can only regain access to their files through the use of anonymous payment (e.g., Bit-coin); this makes tracking of these individuals or organizations very difficult. Encouraged by the financial "success" of these variants, hackers developed several families of ransomware. An important note: Bit-Coin is the standard choice of currency for these attackers because Bitcoin transactions are typically irreversible and only refunded by the receiver of the funds [17].

The AIDS Trojan was the first generation ransomware malware. This Trojan also known as pc cyborg appeared back in 1989 long before today's internet as we know it. This virus was spread via 5 1/4 floppy and replaced the autoexec.bat file. When the victims pc was reboot 90 times the Trojan would activate and begin encrypting the boot drive. A message would be display on the desktop informing the victim that they would have to pay the sum of 189.00 dollars to have the files decrypted and restored. The software AIDSOUT was a reliable removal program for the Trojan and another program known as clearaid recovered encrypted plaintext after the Trojan was triggered. The program clearaid automatically reversed the encryption.

The earliest variations of Ransomware have been around for nearly a decade (1st generation of ransomware actually occurred in 1989), what started initially as a slow trickle of attack campaigns scams in Russia (where it was widely popular among cybercriminals as an easy form of extortion) it has gained an international prominence. Ransomware variants are developing new attack vectors such as Spam / Social engineering; direct drive-by-download [2], Drive-by-download through malvertising [3], and Malware installation tools and botnets [4]. Combating ransomware is difficult for a number of reasons. This malware type is easy to obtain or create [13] it generates immediate returns, creating lucrative opportunities for the attackers. It's a simple to create a variant; there are a number of well-documented crypto-libraries on the web.

Even law enforcement agencies have not been immune and have fallen victim to ransomware [11], losing valuable case files and forcing these organizations to ignore their own advice and pay the attackers.

Malware and in particular crypto-ransomware is a topic that is in the forefront of today's cybersecurity landscape. For the purpose of this informative paper I have research and compiled the necessary data and information to present to my audience (the reader). I have researched the back history of the earliest recorded instance of ransomware and I go into detail on the behavior, types, structure and internal workings of the most common families of ransomware. Additionally I discuss the common payloads, infection platforms and methodology that ransomware employs. I have also outlined recommended strategies and actions to help mitigate data loss.

This paper is organized as follows. Section 2 covers general sources of malware infections and general tactics that ransomware employs to remain covert. Section 3 focuses on the six most common crypto ransomware families. Section 4 delves into types and categories of ransomware. A typical scenario outline or workflow of a malware/ransomware infection is covered in section 5. Section 6 covers in detail the behavior of ransomware and strategies malware employs to accomplish its

978-1-5386-1104-3/17/$31.00 ©2017 IEEE

task. Section 7 is concerned with mitigating strategies to help detect and prevent infection. Recommendations on minimizing loss due to an infected or compromised system or systems are covered in section 8. Section 9 concludes this paper.

## II. Sources of Infection

Email is still a viable method/ preferred method of attack. Most malware infection occurs by malicious office document payloads and drive-by downloads. Known as phishing attacks where a user receives email with an attachment that looks genuine, the attachment contains a hidden executable that installs and runs the ransomware. Malicious MS-office documents maybe part of an email claiming to be a fax or an invoice. These are often referred to as spam email campaigns.

Internet ads are a typical source of drive by downloads. A typical scenario is an unsuspecting user visits or views an infect blog. Typically, a malicious Flash movie that runs in the background is loaded from a suspicious site via a JavaScript, taking advantage of known vulnerabilities within Flash application, and it then downloads the malware. In either case, the actual malware is typically delivered from a randomly generated subdomain of a legitimate domain. Attackers may compromise the DNS account for a legitimate domain and register different subdomains, then use those subdomains to launch cyberattacks; usually these subdomains are only used once.

Ransomware uses multiple strategies to gain access to the victim's system:

- Via spam emails that contain malicious links or attachments.
- Using security exploits in vulnerable software
- Redirecting Internet traffic to suspicious websites
- Compromising innocent websites by injecting malicious code in their web pages
- Drive-by downloads
- Malvertising campaigns
- Self-propagation (spreading from one infected computer to another)

In what follows, we numerate few of the common tactics that ransomware uses to remain hidden and maintain the anonymity of its makers and distributors:

- Encrypt all the communications with Command and Control servers to make it very difficult to be observed in network traffic.
- Use built-in network traffic anonymizers, such as TOR and Bitcoin to obfuscate unlawful acts from law enforcement and to collect ransom payments.
- Hide from antivirus by utilizing sandboxing mechanisms.
- Utilize domain shadowing to help conceal exploits and communication between the payload and the servers controlled by the cyber attacker.
- Deploy encrypted payloads so that it is difficult for AV/anti-malware to detect the malware
- Uses polymorphic behavior, which allows ransomware to create a new variant, but does not alter the malware's function
- Utilizes dormancy – ransomware can remain inactive on the system until the computer is at its most vulnerable

Ransomware is unlike traditional Trojan attacks (which tries evading detection and stealing sensitive information, i.e. personal financial data). Ransomware does not steal its victim's information, but rather denies the victim access to their information. The detection of ransomware after an attack does not restore the lost data since the attack encrypts files with critical information. Therefore, ransomware will make its presence immediately known by encrypting files and demanding payment in exchange for the decryption keys. Since there is critical information at stake, victims of the attack are more likely to pay the ransom to decrypt their files and gain access to their data.

Moreover, in some cases, users may decrease their security or use lightweight cryptography [22, 23, 25] to keep the system's performance high [19, 20, 21, 32, 33]. It is also worth mentioning that some systems are vulnerable to attacks that cannot be prevented using cryptographic protocols, such as: jamming [25], MAC misbehaving [26], packet dropping [27], wormholes [28, 29] and localization [30, 31].

## III. Crypto-Ransomware Families

Six of the most common families of crypto-ransomware are:

1. Dirty Decrypt
2. CryptoLocker
3. CryptoWall / Cryptodefense
4. Critroni / CTB Locker
5. TorrentLocker
6. Cryptographic Locker

Cryptolocker makes up the most prevalent of crypto-ransomware families [6].

CryptoWall surfaced in 2014 [7]. New strains/variations of CryptoWall have been reported.

Critroni acts much like CryptoWall—both families require the TOR browser for payments [9, 10], since communication protocols have shifted from plaintext (HTTP) to encrypted (TOR, HTTPS).

DirtyDecrypt targets and encrypts eight different file formats (one of the earlier iterations of ransomware) [11].

CTB-Locker emerged as one of the first ransomware variants to be sold as a service (RASS) in underground forums.

Crypto Locker and Crypto Wall have some common characteristics:

The ransomware retrieves a public key from the Command and control server and only then performs the encryption; secondly they both used WinCrypto for file encryption. One of the primary strengths of crypto-ransomware is the crypto libraries it uses to perform encryption. Two well-known ransomware, CryptoLocker and CryptoWall relied on Microsoft CryptoAPI. That reliance on the API made early detection easier and allowed for intercepting session keys.

CTB Locker is a highly sophisticated ransomware variant of CryptoLocker. CTB stands for Curve, TOR and Bitcoin. Curve refers to the ransomware's persistent Elliptic Curve Cryptography that uses RSA encryption to deny victims access to their files. T refers to TOR; it uses the infamous P2P network to hide illegal activity from law enforcement agencies. B refers to Bitcoin, the payment method victims use to pay the ransom, which is also designed to protect the attackers' location from being revealed.

The criminals perpetrating these attacks do not need advanced technical skills; the malware is now purchased as turn-key. It is ready to be used out of the "box' and even includes a dashboard where an attacker can track successful infections and the return on their investment.

## IV. Types of Ransomware

### A. Non-Cryptographic Ransomware (NCR)

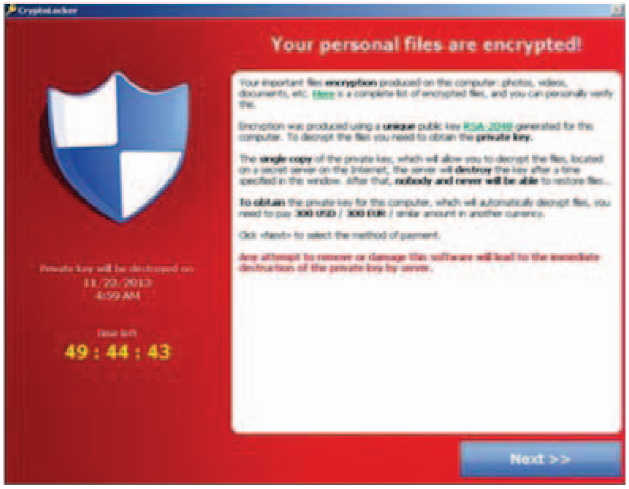
Some ransomware payloads do not use encryption. In these instances, the payload is simply an application designed to restrict interaction with the computer system by locking the screen or even modifying the MBR (master boot record and/or partition table). This type of ransomware is considered relatively weak and the damage can be reversed without paying the ransom.

### B. CryptoGraphic Ransomware (CGR)

Cryptographic Ransomware (CGR) uses cryptographic algorithms to encrypt files to be held for ransom. The malware will start encrypting the user data silently; after encryption is complete the victim is informed that all of his/her data is encrypted and can only be decrypted if he/she pays the ransom. Earlier versions of Cryptographic Ransomware would store the decrypt key on the host pc (this would allow the possibility of recovering the key by reverse engineering), later iterations would have the ransomware contact a command and control (C&C) server and then begin encryption, decrypt key would reside on server, not the host pc. Early versions of Critroni / CTB Locker would encrypt files after contacting the C&C server; however, this 'flaw' would facilitate the prevention of the infection by security teams by allowing them to audit the traffic and discontinue the connection before the malware is able to complete the attack. Ransomware writers would correct this 'flaw' by encrypting files before communicating to the C&C.

### C. Private-key cryptosystem ransomware

Some ransomware use private-key cryptosystems such as classical ciphers, DES family or modern private-key cryptosystems to encrypt the victim's files. CryptorBit is one example of ransomware which uses a self-designed classical cipher cryptosystems similar to polyalphabetic substitution ciphers in just first 512 bytes of target files [15].



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 the 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
11/22/2013
4:59 AM

Time left
49 : 44 : 43

Figure 1 Crypto-Locker Ransomware Display [4]

## V. Typical Scenario of Ransomware

Outlined below are the typically steps in the infection of a victim computer.

Step 1 (victim): The ransomware is spread via mail spams or other form of propagation. CryptoLocker is most commonly spread through emails sent to company email addresses that purport to be customer support related issues from large and well-known companies. These emails typically contain a zip attachment that infects the computer if the victim opens the attachment.

Step 2 (execution): In this step the ransomware is executed by an unaware user by social engineering methods. Cryptolocker zip files use executables masked as PDF files and contain PDF icons with typical naming conventions similar to Example_12345.pdf.exe. Since the zip files appear to be PDF files, most people unassumingly open them. After execution it mostly generates a large random symmetric session key. Cryptolocker then tries to delete the victim's volume shadow copies, so the restoration will be disabled. When the victim opens the file, the ransomware takes the following actions: First, it stores itself in memory in a user folder, such as AppData. Second, it creates a key in the registry so that it executes each time the computer is started up. Lastly, it spawns two processes of itself: One is the main process, the second minor process is to protect the main process against termination.

Step 3 (public key exchange): Cryptolocker attempts to find a live C&C server by connecting to domains generated by a domain generated algorithm (DGA and will use domain names, such as kjqwymybbdrew.biz and jkaeaxjmnxvpv.ru. Once the live C&C server is found, it communicates with it and receives a public encryption key that will then be used to encrypt the victim's data files.

Step 4 (Encryption): As soon as the infection specific public key has been obtained, the victim's data will be encrypted. General files that are targeted include the following:

- Doc—this includes text, word processor files, spreadsheets, etc.
- img—images
- av—audio and video files
- src—source code files
- cad—design files
- db—databases
- sec—security related files, such as certificates, key chains, password managers
- arch—archives
- fin—financial software
- bak—various backups

It's interesting to note that crypto-ransomware will search for as many as 70 image formats, including popular extensions (PNG, JPG) as well as various types of raw images.

Step 5 (Display message): After infection is completed, a message is displayed on the victim's screen.

Step 6 (Decryption): If the victim agrees to pay the ransom, the attacker will send the corresponding private key to the victim to unlock the files.

Ransomware, like other classes of malware, uses a number of strategies to evade detection, propagate, and attack users. For example, it can perform multi-infection or process injection, transfer a user's information to a third party, encrypt files, and establish secure communication with C&C servers.

## VI. Ransomware Behavior

The most indicative behavior of ransomware is the encryption of the victim's data. Ransomware will read victims' original data, encrypt the original data, and then get rid of the original data. It's important to note that the detection of system calls to encryption libraries is not enough to protect against ransomware since many ransomware variants will use their own versions of these algorithms. Ransomware activity can be grouped into three types:

Type A ransomware will overwrite the contents of the original file replacing the original content with the encrypted contents. It may optionally rename the file. Type B ransomware builds on Type A by moving the file out of the user's documents folder into a temporary directory. It then begins writing the encrypted version and then returns the file to the user's directory. When it returns the file, the file may have a new name. Type C ransomware will create a new, independent file that contains an encrypted version of the original files, and will delete or overwrite the original file.

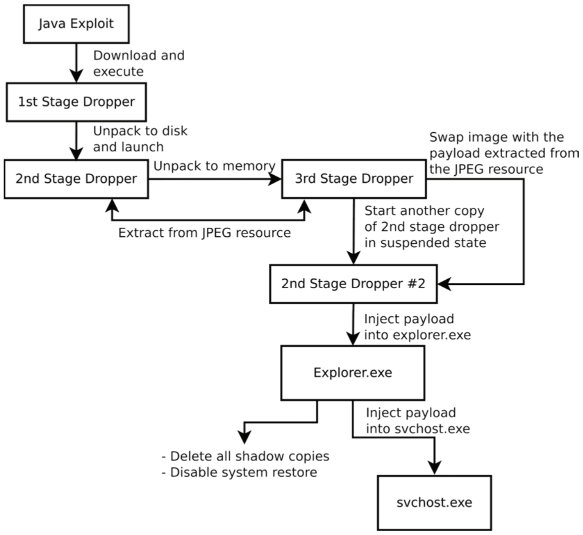

Java Exploit
Download and execute
1st Stage Dropper
Unpack to disk and launch
2nd Stage Dropper
Unpack to memory
3rd Stage Dropper
Swap image with the payload extracted from the JPEG resource
Extract from JPEG resource
Start another copy of 2nd stage dropper in suspended state
2nd Stage Dropper #2
Inject payload into explorer.exe
Explorer.exe
Inject payload into svchost.exe
- Delete all shadow copies
- Disable system restore
svchost.exe

Figure 2 Crypto Wall Infection Workflow. [3]

The Ransomware may also perform additional operations to frustrate recoverability. TeslaCrypt and its variants disable and remove Microsoft Windows volume shadow copies [10]. A crypto-ransomware intrusion lists the victim's files and encrypts any private files it finds. The ransomware randomly encrypt and delete user's private files. Without the decryption key, the victim cannot access any of the files. Encryption keys can be created locally by the malware on the victim's computer or on C&C servers, and then sent to the jeopardized computer. An attacker can use tailored detrimental functions, or Windows API functions to delete the original files. The ransomware can also overwrite files with the encrypted version, or use the Windows Secure Deletion API to perform secure deletion.

File deletion is a basic operation performed by the file system. Programs and applications will generally create and delete temporary files, which is a normal operating system procedure . However, when many files are deleted from a user's documents, this may be indicative of a malware attack. Type C ransomware will use file deletion instead of overwriting. This type of ransomware performs a large number of these create and delete operations, so early detection may depend on capturing this behavior.

When an application reads an unrelated number of files as it writes, this is referred to as file type funneling. It's not uncommon for applications to read multiple file types but write only a single type during a program execution. For example, many word processors (like MS word) will allow a user to embed various file types, but will write only a single file type. Ransomware performs this harmless behavior at a much greater level. As ransomware continues to encrypts and writes data, there is a smaller number of output file types generated. If the number of file types a process has read and written is tracked and a threshold is established, then these attacks can be prevented.

Attackers who successfully carry out a ransomware attack will commonly lock the victim's desktop. Attackers will do so by creating a new desktop and making it persistent. After successfully infecting a user's pc, the malicious program will display a "ransom note," a message to the victim. This "ransom note" tells the user that their system has been "locked" and lists step by step instructions on submitting a ransom payment to retrieve access to the system. The ransom message is generated in various ways. A well-known procedure calls upon API functions (e.g., CreateDesktop) to develop a new desktop and make it the default configuration to lock the victim out of the system under attack. Attackers can also utilize HTML or create other types of repetitive windows to keep the ransom note on display.

Another approach to the lock banner is outlined as follows. A lock banner will be downloaded as a HTML page and will display images that are based on the victim's geographical location. It is then displayed in full screen in an IE window with hidden controls. The banner will play a local law enforcement warning. The warning usually states that the operating system is locked due to infringement against copyrighted materials or visiting child pornography sites (variation of shameware).

The next step, having successfully locked the desktop is to disable special keys by installing hook procedures that track keyboard input events. The disabled Windows keys are used to prevent the victims from accessing the start menu or and prevent the victims from using keyboard shortcuts.

- Crypto-ransomware uses all attack vectors to get into their victim's computers
- Communication with C&C servers is encrypted and difficult to pinpoint in network traffic
- Latest crypto-ransomware families will target a huge number of file formats from documents and images to CAD files and financial data

Crypto-ransomware is constantly evolving and improving features to enable that files cannot be recovered and flaws are getting fixed.

An important resource used for behavior-based malware detection is dynamic analysis. It runs and executes captured malware samples in a controlled environment, and records its behavior (e.g., system calls, API calls, and network traffic). However, malware detection systems that focus on this kind of stealthy malware behavior might fail to detect ransomware because this class of malicious code engages in activity that appears similar to be a benign applications that use encryption or compression, for example MS bit locker or some compression application.

## VII. Mitigation Strategies

### *API Call monitoring*

Many ransomware versions use Windows API functions to lock the victim's desktop. Those API calls can be used to model application behavior and help detect suspicious sequence of Windows API calls.

### *Monitoring File System Activity*

By closely monitoring the MFT table, you will be able to notice the deletion, creation and encryption of the files. For example, when the computer is under a ransomware attack, a compelling amount of status changes develop in a small amount of time in MFT entries of the deleted files. In order to differentiate between harmless and malignant file system activity, another possible manner consists of monitoring all I/O requests that user-mode processes generate. A system that contains protection capabilities can intercept the file system requests and discard suspicious requests before they reach the file system driver.

### *Another strategy suggested is using decoy files*

The various attack strategies deployed by ransomware families to encrypt or delete a victim's files are very similar. Malware/ransomware's malevolent process aggressively attacks all files and attempts to encrypt and/or delete these targeted files in a very short period of time. Consequently by defining a file system activity model that is reflective of normal or typical file system behavior, it's possible to detect this attack and catch it in its early stages. However, an attacker could try to circumvent this detection by launching an attack campaign while attempting to mimic normal file user behavior. An example of this would be by avoiding overly aggressive encryption of all files and only targeting files with recent access or modification time and then encrypting them. By implementing this slight behavior change, this attack might not be detected by software or policies that monitor the behavior of the system. A promising method to detect these attacks would be to install these decoy files in several monitored locations. Decoy files have used to improve the security of hashed passwords and have been used extensively to detect illegally obtained data from file hosting services [15]. Monitoring decoy files can be used as an additional layered ring of defense on top of the I/O requests monitoring to help detect and prevent ransomware attacks.
Existing methods of detecting ransomware involve inspecting programs and their activity for malicious characteristics. Anti-Malware or AV programs attempt to define a suspicious program as malware and stop it by recognizing what the malware is and its function. A common technique used by most modern antivirus and IDS deployments is signature matching, which evaluates programs based on known malware features and flags. Systems that use signature detection incorporate several aspects to detect malicious code and their characteristics in modern malware to enable it to accurately identify known malware. However, malware that has not been previously observed or whose signature is unknown is difficult to identify in these systems.

The relative ease with which ransomware variants can be written, limits the effectiveness of traditional signature based detection systems. However these signature-based systems are ineffective in stopping ransomware variants that can auto run from a plugged usb drive. The usb drive can be hooked up to a pc and used open a terminal (running on the drive) and then launch a program without writing malicious software to the disk. This type of attack would defeat conventional anti-virus/malware and program whitelisting systems by bypassing their inspection point, execution from the disk.

Table 1: Crypto Ransomware Protocols and Domains [12]

| | | |
|---|---|---|
| | | |
| CryptoLocker | HTTP | DGA and |
| CryptoWall / | HTTP and later | Hardcoded |
| | | |
| | | |
| Cryptographic Locker | HTTP | No-IP / No- |

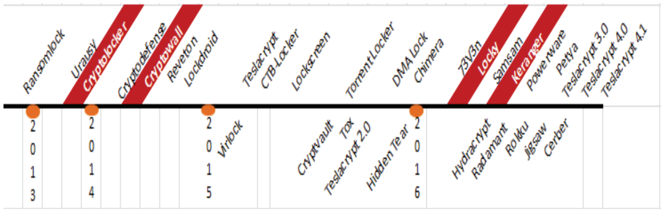


Figure 3 Crypto Ransomware Timeline [12]

File integrity monitors, such as Tripwire alert the administrator when system- critical files are modified. These monitors are based on relatively simple hash comparisons and they fail to distinguish between legitimate file accesses and malicious modifications. These integrity checks are primarily effective for files that rarely change (static); user data is expected to change frequently. Ransomware attackers generally go after a user's personal files (which as stated above are generally modified by the user often). This type of integrity monitoring is likely to produce many false alerts and in turn frustrate the user, increasing the probability that the user might turn off the protection software Detecting large changes or multiple changes of a user's data before it completes would allow the user to stop these changes and prevent ransomware access to the majority of the user data.

Prevention of such a threat is possible only in early stages of infection before files are encrypted. Antivirus and HIPS have two windows of opportunity to prevent the attack:

- At stage of drive-by exploit
- At stage of process injection

After that the malware will proceed with file encryption and detecting it at this stage might be too late.

## VIII. Recommendations

Here are some recommendations on how to minimize the losses in case of infection.

- Maintain regular backups of your files, preferably one on an external hard drive and one in the cloud – Dropbox/Google Drive.
- Unplug the drive after its finished copying files.
- Keep your Operating systems up to date including the latest security updates.
- Avoid using the administrator account; use a guest account with limited privileges.
- Turn off macros in the Microsoft Office suite – Word, Excel, PowerPoint, etc.
- Removed or disable the following plugins from browsers: Adobe Flash, Adobe Reader, Java and Silverlight. If required to use them, set the browser to ask to activate these plugins when needed.
- Adjust browser security and privacy settings for increased protection.
- Remove outdated plugins and add-ons from browsers and keep them updated to the latest version.
- Use an ad blocker to avoid the threat of potentially malicious ads.
- Never open spam emails or emails from unknown senders.
- Never download attachments from spam emails or suspicious emails.
- Never click links in spam emails or suspicious emails.
- Always keep UAC enabled. A number of tasks performed by crypto-ransomware require admin privileges.

## IX. Conclusion

Ransomware continues to plague unsuspecting victims due to its use of strong cryptography; this form of malware is becoming more complex and more dangerous. Elusive infection workflows make it improbable for standard detection-based security solutions, such as antivirus, to prevent the attack before the file encryption while a huge number of targeted file types endanger both home users and enterprises. Victims often have little choice but to pay the ransom, which in turns helps fuel a growing economy for attackers. This success in turn helps motivate cyber criminals to then develop and deploy new ransomware variants ( which can be done with ease).Malware detection is an arms race, as defenders provide mitigations, adversaries will modify their techniques.

## References

[1] E.Arnold. Tennessee sheriff pays ransom to cybercriminals, in bitcoin.http://www.bizjournals.com/memphis/blog/2014/11/tennessee-sheriff-pays-ransom-to-cybercriminals-in.html, 2014.

[2] Kotov V. CryptoDefense: The Ransomware Games have begun Bromium Labs. May 27, 2014.

[3] Larsen C. A Tangled Web, from Ransomware to Malvertising. Blue Coat. July 7, 2014. https://www.bluecoat.com/security-blog/2014-07-07/tangled-web-ransomware-malvertising, 2014.

[4]E. ARNOLD TENNESSEE SHERIFF PAYS RANSOM TO CYBERCRIMINALS, IN BITCOIN.

HTTP://WWW.BIZJOURNALS.COM/MEMPHIS/BLOG/2014/11/TENNESSEE-SHERIFF-PAYS-RANSOM-TO-CYBERCRIMINALS-IN.HTML, 2014.

[5] S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff. A sense of self for unix processes. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 1996.

[6] D. Carrigan. Police departments hit by ransomware virus. http://www.wcsh6. com/story/news/local/2015/04/10/police-departments-hit-by-ransomware-virus/25593777/, 2015.

[7] Jarvis K. CryptoLocker Ransomware. Dell SecureWorks. December 2013, 2013. http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker- ransomware/., 2014.

[8] V. Chandola, A. Banerjee, and V. Kumar. Anomaly detection: A survey. ACM Comput. Surv., 41(3), 2009.

[9] X. Chen, J. Andersen, Z. M. Mao, M. Bailey, and J. Nazario. Towards an under- standing of anti-virtualization and anti-debugging, 2008.

[10] T.Dewan. Teslacrypt joins ransomware field. https://blogs.mcafee.com/ mcafee-labs/teslacrypt-joins-ransomware-field, 2015.

[11] B. Fraga. Swansea police pay $750 “ransom” after computer virus strikes. The Herald News, 2013.

[12] Ducklin P. Destructive malware “CryptoLocker” on the loose—here’s what to do. Naked Security. October 2013, 2013. https://nakedsecurity.sophos.com/2013/10/12/destructive-malware-cryptolocker-on-the-loose, 2014.

[13] J. Walter. Meet tox: Ransomware for the rest of us. https://blogs.mcafee.com/ mcafee-labs/meet-tox-ransomware-for-the-rest-of-us/, 2015.

[14] T. DEWAN. TESLACRYPT JOINS RANSOMWARE fiELD. HTTPS://BLOGS.MCAFEE.COM/ MCAFEE-LABS/TESLACRYPT-JOINS-RANSOMWARE-fiELD, 2015

[15] Vadim Kotov Mantej Singh Rajpal . Understanding Crypto-Ransomware. Bromium . Nov 10, 2014

[16] Ugarte-Pedrero, Xabier, et al. "SoK: Deep packer inspection: A longitudinal study of the complexity of run-time packers." Security and Privacy (SP), 2015 IEEE Symposium on. IEEE, 2015.

[17] Viswanathan, A., Tan, K., & Neuman, C. (2013, October). Deconstructing the assessment of anomaly-based intrusion detectors. In International Workshop on Recent Advances in Intrusion Detection (pp. 286-306). Springer, Berlin, Heidelberg.

[18] H. WEISBAUM. CRYPTOLOCKER CROOKS LAUNCH CUSTOMER SERVICE’ SITE. HTTP://WWW. CNBC.COM/ID/101195861, 2013.

[19] T. Hayajneh, S. Ullah, B. Mohd and K. Balagani, "An Enhanced WLAN Security System with FPGA Implementation for Multimedia Applications," IEEE Systems Journal, 2015.

[20] T. Hayajneh, B. Mohd, A. Itradat and A. Quttoum, "Performance and Information Security Evaluation with Firewalls," International Journal of Security and Its Applications, SERSC, vol. 7, no. 6, pp. 355-372, 2013.

[21] T. Hayajneh, S. Khasawneh, B. Mohd and A. Itradat, "Analyzing the Impact of Security Protocols on Wireless LAN with Multimedia Applications," in Proc. of The Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), 2012.

[22] B. J. Mohd, T. Hayajneh and A. Vasilakos, "A Survey on Lightweight Block Ciphers for Low-Resource Devices: Comparative Study and Open Issues," Journal of Network and Computer Applications, vol. 58, pp. 73-93, 2015.

[23] B. J. Mohd, T. Hayajneh, Z. AbuKhalaf, K. Yousef “Modeling and Optimization of the Lightweight HIGHT Block Cipher Design with FPGA Implementation,” Security and Communication Networks, John Wiley, Vol. 9, No. 13, pp 2200-2216, 2016. (DOI: 10.1002/sec.1479)

[24] BJ Mohd, T. Hayajneh, M. Z. Shakir, K. A. Qaraqe, AV Vasilakos “Energy Model for Light-Weight Block Ciphers for WBAN Applications,” In Proc. of IEEE 4th International Conference on Wireless Mobile Communication and Healthcare (IEEE MobiHealth'14), Athens, Greece, 2014.

[25] K. Panyim, T. Hayajneh, P. Krishnamurthy and D. D. Tipper, "On limited-range strategic/random jamming attacks in wireless ad hoc networks," in Proc. of IEEE Conference on Local Computer Networks (IEEE LCN), 2009.

[26] Hayajneh, Thaier, Ghada Almashaqbeh, and Sana Ullah. "A Green Approach for Selfish Misbehavior Detection in 802.11-Based Wireless Networks." Mobile Networks and Applications 20.5 (2015): 623-635.

[27] Hayajneh, T.; Krishnamurthy, P.; Tipper, D.; Kim, T. Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks. In Proceedings of the IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009; pp. 1–6.

[28] Hayajneh, T.; Krishnamurthy, P.; Tipper, D.; Le, A. Secure neighborhood creation in wireless ad hoc networks using hop count discrepancies. Mobile Netw. Appl. 2012, 17, 415–430.

[29] Hayajneh, T.; Krishnamurthy, P.; Tipper, D. Deworm: A simple protocol to detect wormhole attacks in wireless ad hoc networks. In Proceedings of the IEEE 3rd International Conference on Network and System Security, Gold Coast, Australia, 19–21 October 2009; pp. 73–80.

[30] Hayajneh, T.; Doomun, R.; Krishnamurthy, P.; Tipper, D. Source—Destination obfuscation in wireless ad hoc networks. Secur. Commun. Netw. 2011, 4, 888–901.

[31] Doomun, R.; Hayajneh, T.; Krishnamurthy, P.; Tipper, D. Secloud: Source and destination seclusion using clouds for wireless ad hoc networks. In Proceedings of the IEEE Symposium on Computers and Communications, Sousse, Tunisia, 5–8 July 2009; pp. 361–367.

[32] T. Hayajneh, B. J. Mohd, M Imran, G. Almashaqbeh, AV. Vasilakos, “Secure Authentication for Remote Patient Monitoring with Wireless Medical Sensor Networks,” Sensors, Vol. 16(4), 424, 2016. (DOI: 10.3390/s16040424)

[33] T. Hayajneh, R. Doomun, G. Al-Mashaqbeh, BJ Mohd “An energy-efficient and security aware route selection protocol for wireless sensor networks,” Security and Communication Networks, John Wiley, Vol. 7, No. 11, pp 2015-2038, 2014. (DOI: 10.1002/sec.915)