RESEARCH REVIEW JOURNALS
Volume-04
Issue-02
February-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

Ransomware: Technical Learnings from Attack

[1]Ajay Sangwan, [2]P. Alagu Manoharan & [3]R. Radha Raman Chaudhary

ARTICLE DETAILS

Article History
Published Online: 20February 2019

Keywords
Ransomware, crypto-ransomware, Technology

ABSTRACT

Ransomware is the most commonly known attack till date and all the security professionals are working on how to safeguard environment from such attacks and how to recover the data once the encryption has happened. Here we will be discussing about one of the well-known ransomwares called as Crypto-Ransomware.

We have seen, this is the nightmare for some of the professionals but let's discuss about the positivity and methods we can use in future to safeguard systems in future. In this document we will learn the method used by hackers to safeguard the encryption from all the potential methods to unlock it. We are aware of the technology new discoveries, and new methodology to rectify such attacks, but we do not have clear idea how it all starts and how it starts it's work in the backend and when the time comes, administrators are left with no options other than paying to hackers to get the data back.

1. Introduction

Ransomware is the technique used to encrypt the data drives at file level and makes it inaccessible till the time administrator provides the key to decrypt it. These files are encrypted in such order that the starting of the encryption does not gives any idea that it is encrypting the files in backend and with the time, it starts encrypting operating system files from where the administrator gets the idea that something is happening. Here we will discuss about one of the most critical ransomware known as Crypto-Ransomware working and how it uses the encryption algorithms and makes the situation worse for administrator.

Let's start with the types of ransomware known till the date and know there working and understand the working behavior of it. There are three types of ransomware known till the date and they are **Scareware Ransomware, Lock Screen Ransomware and Crypto Ransomware**.

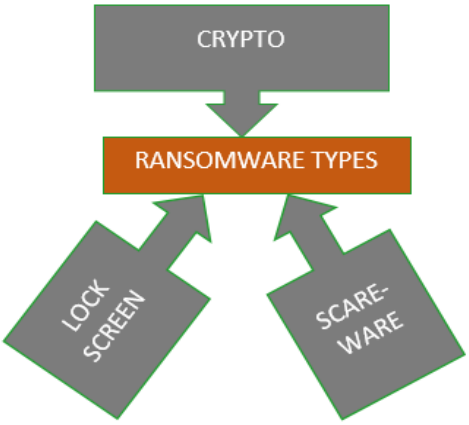

Fig-1. Types of Ransomware

This figure provides the types of Ransomware identified and reported so far from different part of globes. **Lock Screen Ransomware** if one of the well-known among the types, but the solution was already designed by the operating system manufacturing companies. The operating system recovery feature helps in resolving this type of attack. Due to this limitation of attack, impact was not spread as desired by attackers. **Scareware** is second type of ransomware attack. **Scareware** was designed in such a way that the Microsoft users gets pop-ups on their machines "The files on machine are corrupted and can be resolved once you download the software from the website". This attack was limited to the Microsoft Operating System users and attackers was charging some-ware around 4-10$ for the software suggested by the pop-ups. Users think that the files in their machines are infected and they must purchase the software to mitigate the issue. Many users purchased the software which was just for scaring purpose. Most common attack of this type was **Antivirus XP 2008**. Over the period, Scareware started downloading the malware on the victim's machine and resulted in malfunctioning of the operating system. Malware like this was not difficult to remove from the operating system and the impact was also limited to the users of Microsoft Operating system. **Crypto-Ransomware** is one of the major attacks which left the victims helpless and was difficult to identify at initial stage and the remediation is also not yet feasible. Crypto-Ransomware uses file encryption to lock all the files on the victim's systems. In cases where users were infected with scareware or lock screen ransomware, their system files were not impacted. In this, users are faced with losing their data if the ransom is not paid within the allotted time. Over the period, the attackers manage to implement new techniques to strengthen their impact on the infected system. In September 2013, Crypto-Locker was released and was the first cryptographic malware spread by downloads from compromised websites. Computers that were at risk of being infected were those running workstation operating system like Windows XP, Vista, Windows-7, Windows-8 and Windows Servers like 2008, Windows 2008R2, Windows 2012. Apple or Linux were not at risk during this time. Ransom paid for these attacks were in the form of digital currency like Bitcoin, which is still not legal in any countries.

2. Crypto-Ransomware

RRIJM 2015, All Rights Reserved

Crypto-ransomware has grown to such a level that the attackers now use the best possible methods to avoid any leaks in private keys, which is used to decrypt the encrypted files on victim's operating system. Due to least knowledge on Crypto Ransomware the victims are growing in multiples. In this document we will discuss about the types of encryption used for the process and the mechanisms used by the attackers to force the victim to pay the amount of the data recovery.

Once the victim downloads the ransomware, unknowingly, the program executes with just a click of the user. The format of the file can be any depending upon the variety. We will be discussing about the executable format of the file which is used by the windows to install the software and register it on the victim's system registry.

Ransomware source code executes the code and start encrypting the files with the formats defined. Formats for **Text**: doc, docx, msg, odt, wpd, wps, txt; **Data Files**: csv, pps, ppt, pptx; **Audio Files**: aif, iif, m3u, m4a, mid, mp3, mpa, mav, wma; **Video Files**: 3gp, 3g2, avi, flv, m4v, mov, mp4, mpg, vob, wmv; **3D Image Files**: 3dm, 3ds, max, obj, blend; **Raster Image Files**: bmp, gif, png, jpeg, psd, tif, gif, ico; **Vector Image Files**: ai, eps, ps, svg; **Page Layout Files**: pdf, indd, pct, epub; **Spreadsheet Files**: xls, xlr, xlsx; **Database Files**: accdb, sqlite, dbf, mbd, pdb, sql, db; **Games Files**: dem, gam, nes, rom, sav; **Temp Files**: bkp, bak, tmp; **Config Files**: cfg, conf, ini, prf; **Source Files**: html, php, js, c, cc, py, lua, go, java. Once the encryption on these formats will be done, then code will start writing the values in Registry for showing errors and alert messages.

In Registry, codes will be changed for the files so that the values cannot be determined by the applications to read the file from the folder mentioned. As the files are now encrypted and format of the files are now changed to "**. encrypted**", so no file opening applications can read the content as it is encrypted.

3. High Level Description of AES-256

AES-256 is one of the most secure algorithms for encryption of data as mentioned by US National Security Agency. This algorithm uses 128 fixed block size and key size of 256 bits. AES-256 operates on a "4 x 4" column-major order array of bytes. AES calculations are done in a particular finite field.

1. **Key Expension** – round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. **Initial round key addition** – each byte of the state is combined with a block of the round key using bitwise-XOR.
3. **9, 11, 13 rounds**

a. **SubBytes** – a non-linear substitution step where each byte is replaced with another according to a lookup table.

b. **ShiftRows** – a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

c. **MixColumns** – a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.

d. AddRoundKey

1. **Final round** (making 10, 12 or 14 rounds in total)

A. SubBytes
B. ShiftRows
C. AddRoundKey

4. Optimization of Cipher

On systems with 32-bits or larger words, it is possible to speed up execution of this cipher by combining the SubBytes and ShiftTows steps with the MixColumns step by transforming them into a sequence of table lookups. This requires four 256-entry 32-bit tables (together occupying 4096 bytes). A round can then ber performed with 16 table lookup operations and 12 32-bit exclusive-or operations, followed by four 32-bit exclusive-or operation can be performed with a single 256-entry 32-bit table (occupying 1024 bytes) followed by circular rotation operations. Using a byte-oriented approach, it is possible to combine the SubBytes, ShiftRows and MixColumns steps into a single round operation.

5. High Level Discussion of Generating Private Key

Once the data in the described format has been encrypted then a key value gets generated to decrypt the data again in the desired format. Now, we will discuss about the process we propose to safeguard the key for decryption. Once the data is encrypted and key with format "**. pem**" gets generated, I will store the key on remote server over the internet. A secure HMAC value will be used to copy the key to the server over the internet and while downloading the key, a local key needs to be placed in the space provided on the victim's screen. Let's discuss about the process used by **HMAC**. HMAC (keyed-hash message authentication code or hash-based message authentication code) is a specific type of message authentication code (MAC) involving cryptographic has function and a secret cryptographic key. It may be used to simultaneously verify both the data integrity and the authentication of a message as with any MAC. Any Cryptographic has function, such as SHA-2, SHA-3 (Secure Hashing Algorithm) may be used in calculation of a HMAC; the resulting MAC algorithm is termed HMAC-X, where X is the hash function used (eg: HMAC-SHA256 or HMAC-SHA3). The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output and the size and quality of the key. HMAC uses two passes of hash computation. The secret key is first used to derive two keys – inner and outer. The first pass of the algorithm produces an internal hash derived from the message and the inner key. The second pass produces the final HMAC code derived from the inner hash result and the outer key. Thus, the algorithm provides better immunity against **Length Extension Attacks**. An Iterative hash function breaks up a message into blocks of a fixed size and iterates over them with a compression function. Note: HMAC does not encrypt the message instead, the message must be sent alongside the HMAC hash. Parties with the secret key will hash the message again themselves and if it is authentic, the received and computed hashes will match.

RRIJM 2015, All Rights Reserved

Function created to call the portal for HTTP will be used to connect to hacker's server hosted over the internet using domain name or Public IP address (optional). To connect to the server, there is a key stored on the victim's machine which will help victim's machine to authenticate to the server and connect it over the internet. This key will be retrieved by the victim once the hacker will provide the path and password of key on his machine. Once the victim able to provide the passcode from the local file on his PC, then victim's machine will then try to access the path of the server where it stored the file containing the Private Key for decryption. This process of accessing the hacker's portal to store and retrieve the private key from victim's machine is done using **GET** and **POST** operation used in **HTTP** and **HTTPS** for data read and write process. Vitim's machine will connect to hacker's server hosted over internet and save the private key to make it difficult for victim to recover the useful data on his machine. This method was not introduced by hackers before 2017. Hackers were using victim's machine to store the private key "**. pem**" to decrypt the data. This method had loophole which was allowing user to find the key to decrypt the data and making hacker helpless for ransom. With the method, encrypting data and storing key on remote server allows the hacker to have the complete transparency and full control on the private encryption key.

If we discuss about the Crypto-Locker, the data used to be encrypted by the use of encryption algorithm, but the limitation was there. Limitation was leaving the private encryption key over the victim's machine which was later found by the administrator and used the same to decrypt the data encrypted. Over the period, this attack is no longer surety of ransom for the hackers. All the efforts done by hackers does not provide ransom. Now the administrators have clear idea of how it is working, and they easily fetch the private key.

In this document, we discuss about the limitation of other ransomware types (Crypto-Locker, Scareware, Lock-Screen Ransomware) and how secure is the private encryption key. This project needs some pre-requisites which includes deactivation of anti-virus on host machine, Administrator rights, files should be available to encrypt i.e. they should not be encrypted while running this setup.

This document provides us the working of encryption process, limitation of other ransomware attacks reported so far, how secure is the data if it is not encrypted, and most importantly clicking the file types which are not genuine and cannot be trusted. The most important part that we covered in this document, once we have all the efforts in place to achieve the desired encryption then how to secure the important part of the process, in this case it is Private Encryption Key. All the efforts done by the hacker or administrator are worthless if they cannot secure the key process or data of the machine. The hackers have used the process of most secure algorithms against the users themselves by their data, which are not easy to decrypt without private encryption key. This process is like the same process used by many of the other processes which are used to encrypt the data to safeguard the data from the hackers or from misuse. This process defines the similar processes and uses some of the processes used to read and write the data over the internet over HTTP or HTTPS. One of the key features that we have used in this process is storing the private encryption key over the remote server over internet using either **domain name or Public IP address**. This process of storing the private encryption key over the remote server is one of distinguishing feature which makes this type of attack one of the secure attacks.

Now, as we have secured the data from being retrieved or decrypt by victim or administrator, next step of action is the way the ransom needs to be charged without getting into the hands of law enforcements. To meet this requirement, the traditional technology used to store, and transfer ransom are not used, rather Bitcoin. **Bitcoin** is a form of **cryptocurrency**, a form of **electronic cash**. It is a decentralized digital currency without a central bank or single administrator that can be sent from **user-to-user** on the **peer-to-peer** bitcoin network without the need intermediaries. Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain. Bitcoin was invented by an unknown person or group of people using the name Satoshi Nakamoto and released a open-source software in 2009. Bitcoins are created as a reward for a process known as mining. They can be exchanged for other currencies, products and services. Bitcoin has been criticized for, its use in illegal transactions, its high electricity consumption, price volatility, thefts from exchanges and the possibility that bitcoin is an economic bubble. Bitcoin has also been used an investment, although several regulatory agencies have issued investor alerts about bitcoin. All the properties described above supports the statement of security for hackers where they can charge the ransom in the form of bitcoin which are not traceable and cannot be determined by any of the servers as this is not something server dependent.

6. Conclusion

From this document we have seen that ransomware is the tool which encrypts the data and generates the key for against the encrypted files and stores it somewhere on the system itself which is not full proof in terms of attack. So, in this document I have discussed about the storing of the key over the network, possibly hacker's portal, in sub directory. This approach makes the recovery difficult and impossible for the victim to get the key without proper guidelines/script to fetch the key over the internet.

Disclaimer

This document does not violate any content copyrights. This document is not intended to appreciate the hacking or attacking someone's machine without their concerns. This document also does not encourage the use of this document to produce any illegal activity according your country law for Cyber. This document is only for study and research purpose. This document also discusses the latest algorithms used to encrypt the data on machine AES-256, how to make sure the data decrypted is retrieved securely using hashing algorithms i.e. SHA-2, SHA-3. This document also discusses about the process that can be used to store or retrieve the data over the internet using HTTP and HTTPS' GET and POST method.

RRIJM 2015, All Rights Reserved

References

1. Abrams, L. (2012). Remove the FBI MoneyPak Ransomware or the Reveton Trojan. Retrieved September 22, 2018, from Bleeping Computer: http://www.bleepingcomputer.com/virus-removal/remove-fbi-monkeypak-ransomware
2. Abrams, L. (2018). CryptoLocker Ransomware Information Guide and FAQ. Retrieved October 8, 2018, from Bleeping Computer: http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information#files
3. Biaini, N. (2018). Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60M Annually from Ransomware Aone. Retrieved October 8, 2018, from TalosIntel: http://talosintel.com/angler-exposed/
4. Biasini, N. (2018). Your Files Are Encrypted with a "Windows 10 Upgrade". Retrieved October 8, 2018, from Cisco: http://blogs.cisco.com/security/talos/ctb-locker-win10
5. Boyd, C. (2013). Cryptolocker: Time to Backup. Retrieved October 7, 2018, from ThreatAttackSecurity: http://www.threattracksecurity.com/it-blog/cryptolocker-time-backup/
6. Bray, H. (2018). When hackers cripple data, police departments pay ransom. Retrieved September 19, 2018, from Boston Globe: https://www.bostonglobe.com/business/2018/04/06/tewksbury-police-pay-bitcoin- ransom-hackers/PkcE1GBTOfU52p31F9FM5L/story.html
7. Brook, C. (2014, October 9). More Details of Onion/Critroni Crypto Ransomware Emerge. Retrieved from Threat Post: https://threatpost.com/onion-ransomware-demands-bitcoins-uses-tor-advanced-encryption/107408/
8. Cannell, J. (2013). Cryptolocker Ransomware: What You Need To Know. Retrieved October 8, 2018, from Malwarebytes: https://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you- need-to-know/
9. CFOC. (2018). CryptoWall Ransomware Disguises as Resume in Email Attachment. Retrieved October 8, 2018, from CFOC: http://cfoc.org/cryptowall-ransomware-disguises-as- resume-in-email-attachment/
10. Chacos, B. (2014). CryptoLocker decrypted: Researchers reveal website that frees your files from ransomware. Retrieved September 22, 2018, from PCWorld: http://www.pcworld.com/article/2462280/cryptolocker-decrypted-researchers-reveal- website-that-frees-your-files-from-ransomware.html
11. Cobb, S. (2012). FBI Ransomware: Reveton seeks MoneyPak payment in the name of the law. Retrieved September 22, 2018, from WeLiveSecurity: http://www.welivesecurity.com/2012/08/20/fbi-ransomware-reveton-seeks-moneypak- payment-in-the-name-of-the-law/
12. Constantin, L. (2014). Massive malvertigins campain hits Yahoo, AOL, and other sites. Retrieved October 6, 2018, from Computer Word: http://www.computerworld.com/article/2837422/massive-malvertising-campaign-hits- yahoo-aol-and-other-sites.html
13. Diaz, V., & Preuss, M. (2018, October 9). Exploit Kits – A Different View. Retrieved from Securlist: https://securelist.com/analysis/publications/36342/exploit-kits-a-different-view/
14. FBI. (2014). GameOver Zeus Botnet Disrupted. Retrieved October 8, 2018, from FBI: https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted
15. FBI. (2018). Criminals continue to defraud and extort funds from victims using Cryptowall ransomware schemes. Retrieved September 15, 2018, from Internet Crimes Complaint Center: http://www.ic3.gov/media/2018/150623.aspx
16. Fischer, T. (2014). Private and Public Key Cryptography and Ransomware. Retrieved October 8, 2018, from Center For Internet Security: https://msisac.cisecurity.org/documents/PublicandPrivateKeyCryptographyWhitePaper- Dec2014.pdf
17. Gallagher, S. (2018, November 9). New encryption ransomware targets Linux systems. Retrieved December 2, 2018, from ARS Technica: http://arstechnica.com/security/2018/11/new- encryption-ransomware-targets-linux-systems/
18. Howard, F. (2018). A closer look at the Angler exploit kit. Retrieved October 8, 2018, from Sophos: https://blogs.sophos.com/2018/07/21/a-closer-look-at-the-angler-exploit-kit/
19. Jarvis, K. (2013). CryptoLocker Ransomware. Retrieved October 8, 2018, from Dell Secure Works: http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker- ransomware/
20. Jeffers, D. (2013). Crime pays very well: Cryptolocker grosses up to $30 million in ransom. Retrieved September 22, 2018, from PCWorld: http://www.pcworld.com/article/2082204/crime-pays-very-well-cryptolocker-grosses-up- to-30-million-in-ransom.html
21. Keizer, G. (2011). Attackers exploit latest Flash Bug on large scale. Retrieved October 7, 2018, from ComputerWorld: http://www.computerworld.com/article/2509165/security0/attackers-exploit-latest-flash- bug-on-large-scale--says-researcher.html
22. Khanse, A. (2011). Where are the Windows registry files located in Windows 7 / 8 ? Retrieved October 8, 2018, from The Widows Club: http://www.thewindowsclub.com/where-are- the-windows-registry-files-located-in-windows-7
23. KnowBe4. (2018). What is CryptoLocker Ransomware? Retrieved September 22, 2018, from KnowBe4: https://www.knowbe4.com/what-is-cryptolocker-ransomware/
24. Kotov, V., & Rajpal, M. S. (2014). Understanding Crypto-Ransomware. Retrieved November 13, 2018, from Bromium: http://www.bromium.com/sites/default/files/bromium-report-ransomware.pdf
25. Krebs, B. (2012). Inside a 'Reveton' Ransomware Operation. Retrieved September 22, 2018, from KrebsonSecurity: http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/
26. Lahar, S. (2014). CryptoLocker Virus Affects Google Drive Files – Is your Cloud Safe? Retrieved October 10, 2018, from Datto: http://www.datto.com/blog/cryptolocker-virus-affects-google-drive-files
27. Llascu, L. (2018). CryptoWall 3.0 Prompt Delivery via RIG Exploit Kit and Google Drive.
28. Retrieved September 22, 2018, from Softpedia: http://news.softpedia.com/news/cryptowall-3-0-prompt-delivery-via-rig-exploit-kit-and- google-drive-485908.shtml
29. Luo, X. (2007). Awareness Education as the Key to Ransomware Prevention. Taylor & Francis. Retrieved November 1, 2018
30.
31. Malwarebytes. (2018, October 6). What is malvertising. Retrieved from Malwarebytes: https://blog.malwarebytes.org/malvertising-2/2018/02/what-is-malvertising/
32. Markoff, J. (2008). Antiviral 'Scareware' Just One More Intruder. Retrieved September 22, 2018, from NY Times: http://www.nytimes.com/2008/10/30/technology/internet/30virus.html
33. McAfee. (2018). McAfee Labs Threats Report. Retrieved September 16, 2018, from

RRIJM 2015, All Rights Reserved

http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2018.pdf
34. McDowell, M. (2009). Avoiding Social Engineering and Phishing Attacks. Retrieved October 10, 2018, from US-CERT: https://www.us-cert.gov/ncas/tips/ST04-014
35. Microsoft. (2018). Corrupted files. Retrieved September 22, 2018, from Microsoft: http://windows.microsoft.com/en-us/windows/corrupted-files-faq#1TC=windows-7
36. Microsoft. (2018, October 9). Ransomware. Retrieved from Microsoft: https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
37. Microsoft. (2018, September 22). Watch out for fake virus alerts. Retrieved from Microsoft: http://www.microsoft.com/security/pc-security/antivirus-rogue.aspx
38. Microsoft. (n.d.). Volume Shadow Copy Service Overview. Retrieved October 8, 2018, from MSDN: https://msdn.microsoft.com/en-us/library/aa384649(v=vs.85).aspx
39. Microsoft. (n.d.). What is the AppData folder? Retrieved October 8, 2018, from Microsoft Windows: http://windows.microsoft.com/en-us/windows-8/what-appdata-folder
40. Muncaster, P. (2014). Malvertising Campaign May Have Exposed Three Million Users Per Day.
41. Retrieved October 6, 2018, from Infosecurity Magazine: http://www.infosecurity- magazine.com/news/malvertising-campaign-exposed-3/
42. MYERS, L. (2013). 11 things you can do to protect against ransomware, including Cryptolocker. Retrieved October 9, 2018, from WeLiveSecurity: http://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against- ransomware-including-cryptolocker/
43. Popper, N. (2018). For Ransom, Bitcoin Replaces the Bag of Bills. Retrieved September 22, 2018, from NYTimes: http://www.nytimes.com/2018/07/26/business/dealbook/for-ransom-bitcoin-replaces-the-bag-of-bills.html?_r=0
44. Rouse, M. (2011). CAD (computer-aided design). Retrieved October 9, 2018, from TechTarget: http://whatis.techtarget.com/definition/CAD-computer-aided-design
45. Rouse, M. (n.d.). Virtual Machine. Retrieved November 13, 2018, from TechTarget: http://searchservervirtualization.techtarget.com/definition/virtual-machine
46. Security, P. (2018). CryptoLocker: What Is and How to Avoid it. Retrieved October 9, 2018, from PandaSecurity: http://www.pandasecurity.com/mediacenter/malware/cryptolocker/
47. Sinitsyn, F. (2014). A new generation of ransomware. Retrieved October 8, 2018, from https://securelist.com/analysis/publications/64608/a-new-generation-of-ransomware/
48. TechNet. (2018, October 10). Group Policy. Retrieved from Technet: https://technet.microsoft.com/en-us/windowsserver/bb310732.aspx
49. TechTarget. (2012). Adobe Flash Player. Retrieved October 8, 2018, from TechTarget: http://searchcio.techtarget.com/definition/Adobe-Flash-Player
50. Techtarget. (2018, September 22). Bitcoin. Retrieved from TechTarget: http://whatis.techtarget.com/definition/Bitcoin
51. TOR.2018, October 9). Overview. Retrieved from TOR: https://www.torproject.org/about/overview.html.en
52. TrendMicro. (2018). Command-and-control (C&C) server. Retrieved September 22, 2018, from TrendMicro: http://www.trendmicro.com/vinfo/us/security/definition/command-and- control-(c-c)-server
53. TrendMicro. (2018, October 7). Exploit Kit. Retrieved from TrendMicro: http://www.trendmicro.com/vinfo/us/security/definition/Exploit-Kit
54. TrendMicro. (2018). 'Resume' Spam Used to Spread CryptoWall 3.0 Ransomware. Retrieved from TrendMicro: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and- digital-threats/-resume-spam-used-to-spread-cryptowall-3-0-ransomware
55. US-CERT. (2014). CryptoLocker Ransomware Infections. Retrieved October 7, 2018, from US CERT: https://www.us-cert.gov/ncas/alerts/TA13-309A
56. Wingfield, N. (2018). Windows 10 Signifies Microsoft's Shift in Strategy. Retrieved October 8, 2018, from New York Times: http://www.nytimes.com/2018/07/20/technology/windows-10-signifies-microsofts-shift-in-strategy.html?_r=0
57. WinZip. (n.d.). WinZip. Retrieved October 8, 2018, from WinZip Basic Information: http://www.winzip.com/aboutzip.html
58. Wisniewski, C. (2018). CryptoLocker, CryptoWall and Beyond: Mitigating the Rising Ransomware Threat. Retrieved October 10, 2018, from Sophos: https://secure2.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophos-cryptowall-cryptolocker- ransomware-wpna.pdf?la=en
59. Wolff, J. (2014). To Catch a Cyberthief. Retrieved October 8, 2018, from Slate: http://www.slate.com/articles/technology/technology/2014/06/evgeniy_bogachev_gameover_zeus_cryptolocker_how_the_fbi_shut_down_two_viruses.html
60. Woodruff, B. (2018, September 22). Scam Warning: Citadel Malware Delivers Reveton Ransomware in Attempts to Extort Money . Retrieved from FBI: https://www.fbi.gov/newark/press-releases/2012/scam-warning-citadel-malware-delivers- reveton-ransomware-in-attempts-to-extort-money
61. Yazdi, S. (2014). A Closer Look at Cryptolocker's DGA. Retrieved October 8, 2018, from Fortinet: http://blog.fortinet.com/post/a-closer-look-at-cryptolocker-s-dga
62. Zeltser, L. (2018). What Are Exploit Kits? Retrieved October 6, 2018, from Zeltser: https://zeltser.com/what-are-exploit-kits/
63. Zorabedian, J. (2018). Anatomy of a ransomware attack: CryptoLocker, CryptoWall. Retrieved September 20, 2018, from Sophos: https://blogs.sophos.com/2018/03/03/anatomy-of-a-ransomware-attack-cryptolocker-cryptowall-and-how-to-stay-safe-infographic/

RRIJM 2015, All Rights Reserved