Analysis of Ransomware on Windows platform

Adel Hamdan Mohammad

Computer Science Department The world Islamic Sciences and Education University Amman-Jordan

Summary
Ransomware is a very serious problem which all organization and individual may face. No doubt that ransomware cost individual an organization billions of dollars. A lot of researchers talk about ransomware and its effect. The number of researches that talk about ransomware still needs more investigation. In this research, the author analyzes the impact of ransomware only on windows platforms. The author select windows platform since windows is widely spread and used. Analyzing of ransomware is done based on analyzing the behavior of selected ransomware families. The author monitors the behavior of ransomware and which files are created during the infection process. The author also demonstrates the encryption techniques used by ransomware families. Finally, the author notes that protecting Windows operating system is highly possible by monitoring system files and registry entry.

Key words:
Ransomware, encryption, ransomware behavior.

1. Introduction

In this world, world of digitization, every piece of information is stored digitally. Digitization has improved the style of our life. Nowadays, information needs to be accessed 24 hours a day, 7 days in the week, and 365 days in the year. No doubt that the Internet is one of the most used methods to allow us to access information. Attackers, mainly, use email links, email attachments, and web sites to attack individuals and organizations [1]. Ransomware is one of the most dangerous malicious software. Ransomware is a form of malicious software that can infect individuals and organizations. Ransomware mainly spread through different methods such as email links and email attachments. Ransomware makes data inaccessible to users [1,2]. After infection of ransomware the attacker asks for payment and mainly payment is done using bitcoin [3].

In this research, the author will talk about ransomware as one of the most serious attacks which can infect individual and organization. This research will focus on analyzing samples of ransomware from different families related to Windows platform. Despite that all families of ransomware behave in an almost similar manner but there are few differences. This research, also, will provide insight into how ransomware works.

The rest of this paper organized as follows: section two talks about ransomware analysis. In section three the author demonstrates ransomware families in general and dataset used in this research. Section four talks about related studies to this research. In section five, the author demonstrates his experiments and analysis. Finally, in section six, the author talks about his conclusion and future works.

2. Ransomware Analysis

There are several types of ransomware. some researcher says that ransomware has more than 100 forms and patterns. Other researcher says that ransomware has three types and according to other researcher ransomware has only two main forms [4,5]. Most security and anti-virus companies tend to divide ransomware into two types which are crypto ransomware and locker ransomware [6,7].

Ransomware spread through different methods such as email link, email attachment and web sites [8]. up to this moment there is no individual method or tool can protect against ransomware [3]. Most research talks about protecting against ransomware say that there is no anti-virus, method, and tool guarantee to detect ransomware. several anti-virus tools succeed in detecting some types of ransomware, but it fails to detect others. Some researcher who talks about ransomware protecting says that educating users and following strict security policy is very helpful in protecting from ransomware [3].

One of the worst ransomware attacks is WannaCry attack in 2017. WannaCry attack is a ransomware attack that blocks users from accessing his files [2]. Detecting and preventing from ransomware done by following several methods and tools. Mainly ransomware detection methods based on its activity such as file system activities, registry activity and network activity [9].

Ransomware affects all types of organizations such as manufacturing, telecommunication, business, marketing, transport and health service [10,11]. A recent study in 2017 indicates that the number of mobile infected by ransomware is increased which means that not only desktop systems are the target of ransomware [12].

3. Ransomware Families and Dataset

The number of ransomware families is varied and increased. Up to this moment the number of ransomware

Manuscript received June 6, 2020
Manuscript revised June 20, 2020

families is not fixed. According to Kaspersky, the top ransomware families detected by Kaspersky are CTB-Locker, Locky, TeslaCrypt, Scatter, Cryakl, CryptoWall, Shade, generic verdict Crysis, and Cryrar/ACCDFISA [13]. Another researcher talks about more than 20 ransomware families [14]. Mark Loman says that ransomware can be categorized into only three categories based on the method used by attackers and these three categories are cryptoworm, ransomware as a service, and automated active adversary [15]. In this research, the author will investigate 10 ransomware families.

Malware (ransomware) dataset is one of the most challenging in any security research. Collecting ransomware is not an easy task. In this research, 90% of the dataset is collected from Total Virus [16]. The rest of the dataset is collected manually from different security forums. Dataset used in this research in demonstrated in table 1.

Table 1: Dataset

Family	Number of samples
CTB-Locker	2
Cerber	50
Jigsaw	5
Petya	2
Reveton	2
TeslaCrypt	50
WannaCry	1
Crypto wall	2
CryptoLocker	2
Shade	5

4. Related Studies

Monika [1]. In this research authors talk about providing insight on ransomware and how ransomware evolved. Besides that, in this research authors analyze sample of selected ransomware families in windows and android. Seventeen windows and eight androids selected ransomware were analyzed. Experiments in this research demonstrate that ransomware variants behave in a similar manner. Also experiments in this research demonstrate that detection of ransomware is possible by monitoring abnormal activities. In this research, the authors say that implementing a practical defense is possible for windows platform. Also, the authors observe that windows 10 is quite effective against ransomware.

Jinal P [17] in this research authors demonstrate that there has been important progress in the encryption technique. Authors in this research say that careful analysis of ransomware behavior can lead to ransomware detection. Also experiments in this research demonstrate that ransomware families show very similar characteristics.

Toshima [18]. In this research author study different kinds of ransomware attacks from its point of origin. Toshima in this research provides awareness of several kinds of ransomware variants from 1989 to 2017. Also, in this research author analyze the effects of malware on windows and the android platform. Besides that, author provide a guideline to protect against ransomware. Also, the author demonstrates that different families of ransomware exhibit similar characteristics.

Jasmeen [19]. In this research the behavior of crypto ransomware is analyzed. The analysis was done in a virtual environment. Experiments in this research done on a set of crypto ransomware. ransomware activities are monitored on a windows system. All variants of ransomware affect the same registry value and delete existing files. Authors demonstrate that ransomware uses very strong encryption to attack which means that cracking the encryption is impossible.

Jaimin Modi [14]. In this thesis, the author presents network level detection of ransomware. Also, in this research author present a new approach for detecting ransomware in an encrypted network. The author in this research demonstrates that network traffic characteristics can be divided into three categories (connection based, encryption based, and certificate based). Depending on these characteristics the author explores a feature that separates ransomware traffic from normal traffic. In this research, the author’s approach is to extract useful information from the network connection. Also, the author utilizes machine learning for detecting ransomware.

Abdullahi Arabo [20]. In this research authors investigate a study to determine the relationship between a process behavior and its nature to determine whether it is ransomware or not. Analysis in this research conducted on 7 ransomware,41 benign software and 34 malware samples. Results demonstrate the ability to distinguish between harmful and harmless applications.

Adel Hamdan [3]. In this research, the author talks about ransomware and its growth. The author demonstrates several studies that talk about ransomware and its effect. In this research, the author concludes that educating users and following strict security policies is an important factor to minimize the possibility of ransomware appearance. Also, the author says that there is no single method or tool guarantee to fight against all types of ransomware. besides that, the author talks about machine learning methods and their ability to be used in the future for ransomware detection [21,22].

Akashdeep [23]. In this research, the authors present an anti-malware detection system. Authors in this research reviewed existing crypto and locker ransomware. in this research, the author studies ransomware propagation, attack techniques, and new emerging threat vectors as file encryption ransomware and screen locker ransomware. besides that, the authors designed and tested cloud-based malware detection system. Authors in this research investigate if malware can be detected using a cloud-based setup against ransomware and they check if it is better than existing signature based anti-virus and scanners.

Daniel Morato [24]. In this research authors propose an algorithm that can detect ransomware action and prevent further activity on files. 19 different families of ransomware were used in testing. The results of the experiments are promising. One important thing in this research is that, recovery of lost files is possible. The algorithm used is called REDFISH. Detection of ransomware based on its basic behavior of reading, writing and removing files.

McAfee Labs [25]. In this report, McAfee Labs indicated that ransomware attacks increased by 118%. Also, this report indicates the rise of new ransomware families. This report indicates three top families of ransomware which are Dharma, GandCrab, and Ryuk. McAfee Labs reports show several important statistics about ransomware, see figure 1 [25].

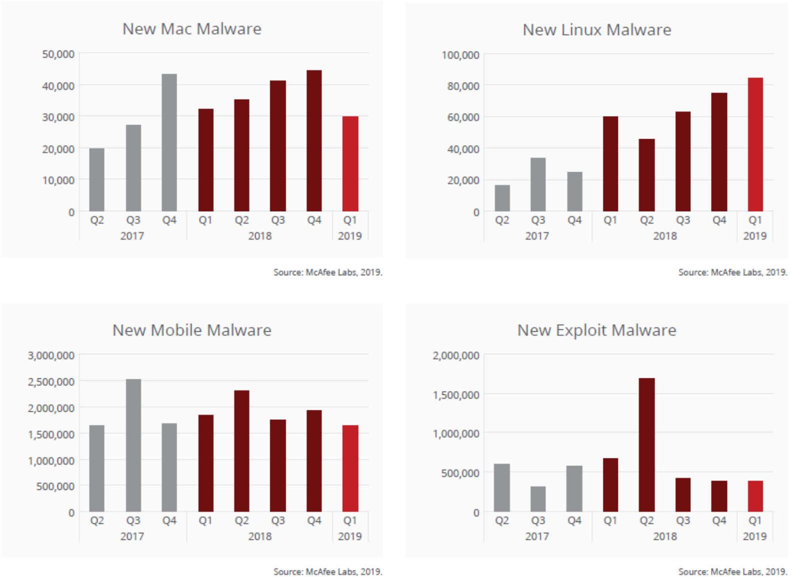

Fig. 1 McAfee Labs threat statistics

5. Experiments and analysis

All ransomware samples are analyzed using Cuckoo sandbox, Oracle VM VirtualBox, Virtual Windows 7 and Virtual Windows 10. After observing and analyzing a report is documented. Changes is observed in file system activities, encryption used, locking methods, and registry activities.

Before going in depth and analyzing ransomware families' behavior. The author will introduce main features and characteristics of each family. CTB-Locker, CTB-Locker stands for "Curve-Tor-Bitcoin-Locker". CTB released in 2016 and mainly delivered by email. Using social engineering techniques attackers cheat victims to download and run the encryption file. CTB Locker uses a combination of symmetric and asymmetric key encryption. CTB-Locker mainly spread through files delivered by email or links. CTB-Locker is one of the top ransomware threats for the financial industry. Cerber ransomware is an evolving type of ransomware called crypto ransomware [3,26]. Cerber is a sophisticated malware. Cerber ransomware starts his action by reading network and environment data. Cerber is an application that makes use of RaaS (Ransomware as a Service). A piece of important information author must mention is that If Cerber detects your location (Geolocation) is from Azerbaijan, Belarus, Armenia, Georgia, Kazakhstan, Moldova, Russia, Kyrgyzstan, Tajikistan, Turkmenistan, Ukraine or Uzbekistan, it will not encrypt or affect your machine [26]. Jigsaw is a form of encryption malware born in 2016. Jigsaw spread through attachments and spam emails. Jigsaw creates files and affects registry entry. Petya ransomware is considered a family of encrypting ransomware discovered in 2016. This malware target windows platform and it is affecting the master boot record and overwrite windows bootloader. This malware mostly threatened enterprises and businesses. Petya uses EternalBlue exploit as a means to propagate itself [27]. Reveton ransomware is a ransomware application. Reveton fraudulently claims to be a legitimate application. Reveton first evolved in Europe in 2012. Due to Reveton behavior it is called "Police Trojan". [28 ,29]. TeslaCrypt is very similar to Cryptolocker. Mainly TeslaCrypt target game play data. TeslaCrypt first detected in 2015.

TeslaCrypt considered an advanced form of encryption that can lock more than 150 different files type. TeslaCrypt attacker uses social engineering methods to trick users to click or to download a link. TeslaCrypt appears with different versions such as V2.0, V3.0 and V3.01.

New versions of TeslaCrypt encrypt Word file, PDF file, JPEG file, and other types of files [30]. WannaCry attack appears in 2017. WannaCry targeting windows operating system. WannaCry is ransomware worm that spread through networks. WannaCry spread through SMB network protocol. Crypto wall is ransomware that uses an advanced technique for encryption. Crypto wall first appearance in 2014. Crypto wall spread fast and easy to use. Crypto wall hides it self-inside the Operating System and adds itself to the startup folder. CryptoLocker is a ransomware that occurs in 2014. CryptoLocker mainly target windows Operating systems. CryptoLocker can encrypt stick USB memory. One important thing to mention here is that CryptoLocker seeks for your files on the cloud. Shade is encryption ransomware. after entrances of your machine, Shade scans all your computer files looking for a matching list of files extension to encrypt. Shade has been appearing around 2014. Shade Ransomware is the greatest distributed malware via Email [31,32,33].

After analyzing of ransomware behavior. The author observes that a .txt file is created at the start of execution and the .txt file is modified constantly. Also, some types of ransomware create .log, .tmp, and .dmp files. The author observes that all ransomware families modify \PIPE\lsarpc file. LSARPC is a set of calls, transmitted with Remote Procedure Call (RPC) to a system called the local security authority. This file used in Microsoft platform to achieve management tasks on domain security policy from a remote machine. Besides that, the author observes that crypto wall family made changes on PIPE\lsarpc and .exe file inside temp folder of the administrator account. Also, the author observes that crypto wall infects itself to svchost.exe and iexplore.exe. crypto wall families apply modifications on the start menu even after rebooting.

Related to CTB-Locker. Author note that CTB-Locker create a random execution file in the %AppData% or %LocalAppData% folder. CTB-Locker encrypt files such as .doc, .docx,.xls, and .pdf. CTB-Locker create a file in the directory which created in the beginning of encryption named !Decrypt-All-Files-(random 7 characters).TXT or !Decrypt-All-Files-(random 7 characters).BMP. besides that, Author note that CTB-Locker change wallpaper to be %MyDocuments%\AllFilesAreLocked <userid>.bmp file. The file bath created by ransomware in windows 7 is C:\Users\<User>\AppData\Local\<random>.exe.

Related to Cerber. Cerber is the most active ransomware. Cerber uses a ransomware-as-a-service (RaaS) model. Mainly Cerber runs in the background during the encryption phase. Cerber encrypting different file types including .jpg, .doc,. raw, etc. besides that Cerber adds a .cerber extension. Author note that Cerber creates three different files (#decrypt my files#.txt, #decrypt my files#.html, and #decrypt my files#.vbs). these files contain payment steps.

Related to jigsaw author notice that using MsConfig jigsaw removes auto-run for firefox.exe. Jigsaw ransomware create files such as %SYSTEMDRIVE%\users\ok\appdata\roaming\frfx\firefox.exe, C:\Users\user\AppData\Local\Chrome32\Chrome32.EXE, and C:\Users\user\AppData\Local\Drpbx\drpbx.exe. besides that, the author note that Jigsaw creates some registry entry such as %APPDATA%\frfx, %APPDATA%\System32Work And %APPDATA%\WIND0WS.

Related to Petya author notice that Petya is executed using rundll32.exe perfc.dat. Petya attempt to create a file "C:\Windows\perfc". Once installed Petya tries to modify the master boot record. Besides that, Petya encrypts the master file table of NTFS file system.

Related to Reveton. Reveton creates a ctfmon.lnk file. Author notes that running Windows in safe mode and deletes this file may fix the problem. The file created in Win 7 is: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup\[reveton_filename]dll.lnk.

Related to TeslaCrypt. TeslaCrypt search for files related to several games such as World of Warcraft, Call of Duty and encrypt files. Files encrypted include saving data, the profile of players, game stored points in the hard drive. The author notes that sometimes files are renamed to "+REcovER+dpyww+".

Related to WannaCry. WannaCry creates the following two registries. Key: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Random> Value: <Full_path>\tasksche.exe and Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Random>
Value: <Full_path>\tasksche.exe

Related to Crypto wall. Crypto wall encrypts file name and file content. New version of crypto wall contains malware dropper to escape from anti-virus detection. Author notice that Cerber will install itself into folder % AppData %. With Cerber ransomware windows will be automatically configured into safe mode and in Cerber in the next reboot will be starting automatically.

Related to CryptoLocker. CryptoLocker locks different types of files such as Microsoft office files, XML documents, and zipped files. CryptoLocker renames the files with (.encrypted) or (.Cryptolocker). The behavior of CryptoLocker and Crypto wall is very similar. Once the system is infected it is run new registries in windows startup.

Related to Shade. It starts the encryption process after immediately affecting your machine. After that Shade creates a file named "readme#.txt" to guide the victim about the process of payment. Mainly shade adds the extensions .xtbl and .ytbl.

encryptions used are as follows: CTB-Locker uses a combination of symmetric and asymmetric encryption. CTB-Locker, mainly, distributed via email with a zip file, when the user downloads the file, the downloader connects to malicious software. Then the file copy itself in a temporary directory. The encryption itself is done using AES, and the means to decrypt the files are encrypted using ECC public key. Communication is carried by Tor Network. Cerber encryption mainly uses the RSA-2048 key (AES CBC 256-bit). Once installed on your PC it will create a random file inside Local App Data or App Data folder. Cerber spread through malicious links or emails. Some types of Cerber encrypt all files using AES-256 or RC4. Jigsaw encryption mainly based on AES encryption. Jigsaw add, mostly, .FUN extension at the encrypted files. Jigsaw mainly uses AES algorithm. Jigsaw add .FUN, .BTC, and .KKK extensions to encrypted files. Petya encryption use SALSA20 algorithm. SALSA20 is closely related to ChaCha and a stream cipher developed by Daniel J. Bernstein [34]. ChaCha is a modification of SALSA20 appears in 2008. Old version of Reveton locks your screen instead of encrypting. After that reveton displays an image, full screen image, lock or disable task manager. The image displayed containing a message claiming to be from law enforcement. TeslaCrypt mainly uses asymmetric encryption. Some version of TeslaCrypt uses advanced Encryption Standard (AES) algorithm to encrypt files. TeslaCrypt encrypt files with .ecc extensions. TeslaCrypt 4.0 uses a complex RSA 4096 encryption algorithm. WannaCry uses a combination of the RSA and AES algorithms to encrypt files. Before encryption WannaCry lists all local drives. WannaCry target more than 20 types of file. WannaCry uses Tor network and The Tor server is renamed as taskhsvc.exe. Crypto Wall ransomware uses RSA and AES algorithm in encryption. Crypto Wall applies RSA public key from its C&C server. One important note to mention here if Crypto Wall fails to connect C&C server it will not encrypt any file. CryptoLocker WannaCry uses a combination of the RSA and AES algorithms to encrypt files. Mainly, crypto ransomware, if implemented, does a great number of file alterations. Shade mainly uses the AES 256 encryption algorithm. Unlike CryptoLocker, Crypto Wall and CTB-Locker shade install several infected malware on your computer.

6. Conclusion and future work.

Ransomware is a complicated problem. No doubt that ransomware has evolved rapidly, and it affects all types of organizations and individuals. In this paper, the author demonstrates and analyzes the effect of selected ransomware families on windows platform. Experiments are done using Oracle VM VirtualBox, Virtual windows 10, windows 7, and Cuckoo sandbox. Experiments show that most types of ransomware have similar behavior. All types of ransomware affect file system and registry entity. The author notes that all types of ransomware create some files in system files and rename other files in windows. The author concludes that defending against ransomware is highly possible by monitoring system files and registry activities. Also, the author notes that windows 10 is more effective against ransomware than Windows 7. The best procedure to do up to this minute is to continually back up the organization or individual data. Moreover, is to continually update your windows operating system. Install an anti-virus to monitor system file activity will be useful. Future work for the author will be adapting a machine learning method to monitor system file activity.

Acknowledgement:

The authors are grateful to WISE University, Amman-Jordan, for the financial support granted to cover the publication of this research article.

References

[1] Monika, Pavol Zavarsky, Dale Lindskog, Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization, Procedia Computer Science 94 (2016),465 – 472.

[2] Savita Mohurle, Manisha Patil, A brief study of Wannacry Threat: Ransomware Attack 2017, International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May-June 2017.

[3] Adel Hamdan, Ransomware Evolution, growth and Recommendation for Detection, Modern Applied Science, 2020.

[4] Jesper B. S. Christensen,2017. Ransomware detection and mitigation tool, Technical University of Denmark, Department of Applied Mathematics and Computer Science, Master Thesis ,2017.

[5] McAfee,2019. McAfee Labs Threat Report. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf. (Accessed Dec 1,2019).

[6] Proofpoint ,2017. Proofpoint (2017). 2017 Q3 Threat Report, https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q317-threat-report_1.pdf.(Accessed January 1,2020).

[7] Cyber Threat Alliance, 2018, Lucrative ransomware attacks: Analysis of the cryptowall version 3 threat. Technical report, 2015.

https://www.cyberthreatalliance.org/wp-content/uploads/2018/02/cryptowall-report.pdf. (Accessed Jan 1,2020).

[8] Hirra Sultan,2018. Hirra Sultan, Aqeel Khalique, Shah Imran Alam, Safdar Tanweer, a survey on ransomware: evolution, growth, and impact ,International Journal of Advanced Research in Computer Science, DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5858, Volume 9, No. 2, March-April 2018.

[9] P. Zavarsky and D. Lindskog, “Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization,” vol. 94, pp. 465–472, 2016.

[10] “Ransomware Repercussions: Baltimore County Sewer Charges, 2 Medical Services Temporarily Suspended,” June 2019, "Last Access: July 4th 2019". [Online]. Available:https://www:trendmicro:com/vinfo/us/security/news/cybercrime-anddigital-threats/ransomware-repercussions-baltimore-county-sewercharges-

[11] medical-services-temporarily-suspended [3] Stephen Cobb, “Ransomware vs printing press? US newspapers face foreign cyberattack,” December 2018, "Last Access: July 4th 2019". [Online]. Available: https://www:welivesecurity:com/2018/12/31/ransomware-printing-press-newspapers

[12] EUROPOL, “Internet Organised Crime Thread Assessment (IOCTA) 2018,” Europol - European Police Office, Tech. Rep., 2018. [Online]. Available: https://doi:org/10:2813/858843

[13] Kaspersky security bulletin 2016. Story of the year the ransomware revolution. https://media.kaspersky.com/en/business-security/kaspersky-story-of-the-year-ransomware-revolution.pdf

[14] Jaimin Modi, Detecting Ransomware in Encrypted Network Traffic Using Machine Learning, A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Applied Science in the Department of Electrical and Computer Engineering, B.Eng., Gujarat Technological University, 2014.

[15] Mark Loman, Director, Engineering, How Ransomware Attacks, A Sophos Labs white paper November 2019. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf.

[16] Virus Total - Intelligence Search Engine, https://www.virustotal.com.

[17] Jinal P. Tailor, Ashish D. Patel, A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control, International Journal of Research and Scientific Innovation (IJRSI) | Volume IV, Issue VIS, June 2017.

[18] Toshima Singh Rajput, Evolving Threat Agents: Ransomware and their Variants, International Journal of Computer Applications (0975 – 8887) Volume 164 – No 7, April 2017.

[19] Jasmeen Kaur, Fehmi Jaafar, Pavol Zavarsky, An Empirical Analysis of Crypto-Ransomware Behavior. ICONS, Hong Kong, 2018: The Thirteenth International Conference on Systems,2018.

[20] Abdullahi Arabo, Remi Dijoux, Timothee Poulain, Gregoire Chevalier, Detecting Ransomware Using Process Behavior Analysis, Procedia Computer Science 00 (2019) 000–000, www.elsevier.com/locate/procedia.

[21] Adel Hamdan,2011. Adel Hamdan, Raed Abu-Zitar, “Spam Detection Using Assisted Artificial Immune System”, Volume: 25, Issue: 8(2011) pp. 1275-1295, International Journal of Pattern Recognition and Artificial Intelligence, 2011.

[22] Adel Hamdan, Nidhal Al-omari, “Using Polynomial Neural Networks for Arabic Text Categorization”, European Journal of Scientific Research, Vol 152, Issue 3. 2019.

[23] Akashdeep Bhardwaj, Vinay Avasthi, Hanumat Sastry and G. V. B. Subrahmanyam, Ransomware Digital Extortion: A Rising New Age Threat, Indian Journal of Science and Technology, Vol 9(14), DOI: 10.17485/ijst/2016/v9i14/82936, April 2016

[24] Daniel Morato, Eduardo Berrueta, Eduardo Magana, Mikel Izal, Ransomware early detection by the analysis of file sharing traffic, Journal of Network and Computer Applications 124 (2018) 14–32.

[25] McAfee Labs Threats Report, August 2019, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

[26] Ade Kurniawan, Imam Riadi, Detection and Analysis Cerber Ransomware Based on Network Forensics Behavior, International Journal of Network Security, Vol.20, No.5, PP.836-843, Sept. 2018 (DOI: 10.6633/IJNS.201809 20(5).04)

[27] Ronny Richardson, Max North, Ransomware: Evolution, Mitigation and Prevention, International Management Review, Vol. 13 No. 1 2017.

[28] Nikolai Hampton Zubair A. Baig, RANSOMWARE: EMERGENCE OF THE CYBER-EXTORTION MENACE, 13th Australian Information Security Management Conference, held from the 30 November – 2 December 2015, (pp. 47-56), Edith Cowan University Joondalup Campus, Perth, Western Australia. This Conference Proceeding is posted at Research Online. https://ro.ecu.edu.au/ism/180. DOI: 10.4225/75/57b69aa9d938b

[29] "Garda í warn of 'Police Trojan' computer locking virus". TheJournal.ie. Retrieved 31 May 2016. https://www.thejournal.ie/gardai-garda-police-trojan-scam-virus-logo-locking-488837-Jun2012/.

[30] Sergiu SECHEL, A Comparative Assessment of Obfuscated Ransomware Detection Methods, Informatica Economică vol. 23, no. 2/2019, DOI: 10.12948/issn14531305/23.2.2019.05

[31] Sergiu Gatlan,2019, Shade Ransomware Is the Most Actively Distributed Malware via Email. https://www.bleepingcomputer.com/news/security/shade-ransomware-is-the-most-actively-distributed-malware-via-email/

[32] Tooska Dargahi, Ali Dehghantanha, Pooneh Nikkhah Bahrami, Mauro Conti, Giuseppe Bianchi & Loris Benedetto, A Cyber-Kill-Chain based taxonomy of crypto-ransomware features, Journal of Computer Virology and Hacking Techniques volume 15, pages277–305(2019). https://link.springer.com/article/10.1007/s11416-019-00338-7

[33] Juan M. Vilardy O. *, Leiner Barba J. and Cesar O. Torres M, Image Encryption and Decryption Systems Using the

Jigsaw Transform and the Iterative Finite Field Cosine Transform, Photonics 2019, 6, 121; doi:10.3390/photonics6040121, Received: 31 October 2019; Accepted: 22 November 2019; Published: 26 November 2019.

[34] https://en.wikipedia.org/wiki/Salsa20

Adel Hamdan Mohmmad, received bachelor's degree in computer science. Master and Ph.D. degree in computer information system. Author has several researches about text classification, machine learning and cybersecurity.

https://scholar.google.com/citations?user=crca_psAAAAJ&hl=en