View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by International Journal of Computer (IJC - Global Society of Scientific Research and...

International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

© Global Society of Scientific Research and Researchers

http://ijcjournal.org/

Comparative Analysis of Distinctive Features of the Ransomware Tactics in Relation to Other Malware

Simon Kihiu[a]*, Elisha Abade[b]

[a,b]*The University of Nairobi, School of computing and Informatics, P.O Box 30197, Nairobi, GPO, Kenya*

[a]*Email: smnkihiu@gmail.com*

[b]*Email: eabade@uonbi.ac.ke*

Abstract

Ransomware have become a real threat to the use of technology. Unlike other forms of malware that could target systems by deleting or editing some files and creating backdoor for the attacker to access the system, ransomware have gone a notch higher by targeting humans. This is achieved when a ransomware encrypts data of the infected computer and a note demanding for a ransom to be paid is printed on the screen. Due to the advancement in technology, ransomware use advanced and secure encryption algorithm that is difficult to decrypt even when the computational power is not limited. In this work, we present some of the major behavioral characteristics that we found to be common with ransomware and not with other malware. Our results show that a careful analysis of suspicious network and file activities can help detect a ransomware attack. Further, careful analysis of ransomware behavior can help develop a system that can detect an impeding ransomware attack and thereby eliminate it.

Keywords: Ransomware; Ransom; Malware; Cybercriminal; Cybersecurity.

1. Introduction

Since the birth of internet, more than two and half decades ago, cyber security threats and attacks have been on the rise and even worse, we have seen introduction of more sophisticated ways which are more robust and intelligent. Clark and his colleagues in [1] attest how Stuxnet make a good example depicting how cybercrime has become more sophisticated. Cybercriminals are now not interested in being known or being admired, thus they have come up with new ways to carry out an attack that are automated and anonymous. Ransomware have become a game changer in the history of cybercrime. Unlike other conventional malware, ransomware target human beings.

---

* Corresponding author.

They extort money from victims and deposit it in a digital wallet of the attacker without the attacker being present [2]. In 2016, Symantec considered ransomware as one of the most dangerous malware threat. This was after realization that, modern ransomware not only infect personal computers but also mobile application, IOT, and lately the cloud based services [3]. The author in [4], described three major attack vectors; home users, businesses, and government institutions. Choi and his colleagues in [5] attest that there is lack of a practical approach towards explaining the reason ransomware attack have become so rampant, and therefore the current study relies on a Cyber-Routine which is a theoretical approach. This theory follows Cohen and Felson's traditional Routine Activities Theory (RAT) to explain this form of crime of victimization [5]. Ransomware have been found to use standard cryptographic algorithms. This has therefore made the development of ransomware to be a relatively low effort endeavor as these libraries are already available. Poorly designed ransomware have also been found to be successful as they use scare tactics to unsuspecting victims who end up in paying ransoms [6]. Since ransomware uses an advanced encryption algorithm, there is no method of ridding the attacked computer of ransomware aside from paying the ransom, which means that prevention is of paramount importance. There are also no developed systems, which are dedicated in detecting ransomware before they infect victim's data. The conventional anti-virus software's available are not designed to efficiently detect a ransomware, and they have difficulties in detecting polymorphic ransomware [7]. Our primary objective in this study was to get features that are common with ransomware but they are not common with other form of malware. The results will be used to advice on ways that can be used to detect an impeding ransomware attack and thereby thwart it before damage is done. We shall therefore remain focused on ransomware and their features and behavior that are varied from other form of malware which, can be useful in developing a machine learning algorithm that can be useful in securing systems against subtle attack tactics of ransomware. To be able to meet the objectives of our research study, we first look at other related works that will help us justify our study. We shall discuss the research design that was used to collect data used for analysis in this study, and the result of the experiment conducted will be presented and discussed to give a comprehensive conclusion and recommendation.

2. Related Works

Ransomware are classified into two types based on their mode of execution [8]. These are autonomous ransomware which, destructive activity starts without the need to contact command and control server. The other variants contact command and control server before the destructive activity can start, and these can be blocked by detecting network signatures. Various variants of ransomware share some common traits like the use of latest technologies such as cryptocurrencies and anonymous hidden network. A research was conducted to compare traits of twenty-nine variants of ransomware that were uncovered from December 1989 to July 2015 [8]. It was observed that over and above them sharing most of the traits, the use of stronger encryption algorithm started in 2013. There were also additional improvement in the ransomwares that were uncovered post 2013. They include the use of cryptocurrency (Bitcoin) which allows the exchange of digital currency anonymously through the use of Tor network. It is impractical to decode files encrypted with strong and properly implemented cryptography. Most of these secure ransomware variants utilize a combination of public key cryptography such as remote public key generation, AES-256 block ciphers, and command and control server communication [8]. Therefore, it is an important practice to use comprehensive best security techniques with

sophisticated backup solution as part of an excellent security for cyber safety. However, in 2015 Kaspersky lab collaborated with the National High Tech Crime Unit of the Netherlands police to generate a repository of decryption keys and a decryption application for victims of the coinvault ransomware. Kaspersky have also developed a countermeasure known as the system watcher module to keep local protected copies of files and restore changes made by cryptomalware [9]. According to an experimental analysis of ransomware on windows and android platform conducted in [10] analyzed all variants of ransomware using Cuckoo sandbox and Anubis. The authors observed that all variants of ransomware try to be installed in a computer by making some changes in a computer. These changes were found in registry file system activities where some files were downloaded, others altered, and others deleted. Network traffic was also analyzed and they observed that it gave some vital information in case of ransomware attack. These information gathered includes, connection type, connection port that was observed to be port 80 and port 443 for TCP and port 53 for UDP, also the encryption standards that were utilized were captured in the network traffic. All the current variants of these groups were found to use both RSA-2048 bit encryption for public key and AES-256 bit encryption for encrypting the victim's files. The authors in [10] also attest that ransomware variants behave in a specific manner but utilize various payloads and these were significant advancement in the encryption techniques used by ransomware. The results of the experimental investigation in windows setting showed that, ransomware detection is possible through monitoring abnormal registry activities and file system, and in Android settings, the evaluation showed possibility of ransomware attacks could be decreased by paying closer attention to permissions that were requested by the android applications. The authors in [11] observed that mobile devices are also prone to ransomware attacks, and since there is little research done on this, most devices relies on traditional mechanism to protect them from attack. This therefore render them unsecured as ransomware use very subtle attack tricks rendering them undetected even by the advanced mobile malware detection methods. However, Scaife and his colleagues in [12] noted that, the use of CryptoDrop, an early-warning detection system that was able to make an alert whenever there was unusual activity in the file, like interfering with large amount of file data simultaneously, could be used to protect systems against ransomware attack. They also noted that, different indicators that are known to be common to ransomware could be used together to parameterize the system to enhance early detection with low false positives. They therefore concluded that ransomware like other malware have characteristics that are common to them and therefore an in depth analysis could yield a system that can minimize on the amount of victims data loss. The internet threat report [13] showed that the growth of wearable and handheld devices like smart watches are also contributing factor to the spread of ransomware attack, this is because of the vital personal information they contain and therefore making them a soft target Tseng and his colleagues in [14] conducted an experimental analysis where they used deep learning method to detect ransomware. In the evaluation, the authors successfully demonstrated that a deep-learning model could timely detect the latest ransomware in high-speed network. However, due to high reward for ransomware, more and more ransomware families appear making it more difficult to detect them. The authors in [15] established that the number of ransomware families with sophisticated destructive potential remains reasonably small. These malware locks the victim's computer desktop or attempt to encrypt or delete the victim's files using only superficial techniques. This study also showed that stopping an advanced ransomware attacks is not as complex as it has been argued before in other reports. This report proposed that it is practical to design a ransomware protective system that can halt a large proportion of ransomware attack by monitoring abnormal file system

activity. A close examination on the file system activities of multiple ransomware samples recommends that by looking at input-output request and protecting Master File Table (MFT) in the NTFS file systems, it is feasible to detect and prevent a significant number of zero-day ransomware attacks.

2.1. Research gap

There is a very small amount of information in regards to malware research. There are no sufficient peer-reviewed documents on malware, and an approved methodology that can be used during malware analysis. This, therefore, makes malware analysis lag behind vulnerability analysis, which have been well researched on, hence reliable exploits databases, and well peer-reviewed data sources exist. There is still a gap in malware analysis that can be mitigated by development of a formal methodology of malware analysis that will also include the vocabulary associated with malware analysis [8].

3. Research Design

We conducted an experiment using Cuckoo sandbox for dynamically analyzing the selected ransomware and other malware. We used binaries for real malicious codes and therefore we implemented system virtualization. Before any execution of the binaries was carried out a snapshot of the virtualized Windows7 was taken after which the system could be taken back to its initial state after running the analysis. This was to provide for the uniformity of all the analysis to be carried out. Figure 1 shows the conceptual architecture. After installing Cuckoo sandbox, there are two ways to upload the binaries; Cuckoo graphical user interface and Cuckoo command line interface, in this study we used graphical user interface to upload the binaries into Cuckoo malware analysis server. Cuckoo malware analysis server is connected to Windows7 virtual machine through a virtual network, after malware has been executed in virtualized Windows7, the Cuckoo result server collects all the analysis results, which we are able to access for analysis through Cuckoo graphical user interface.

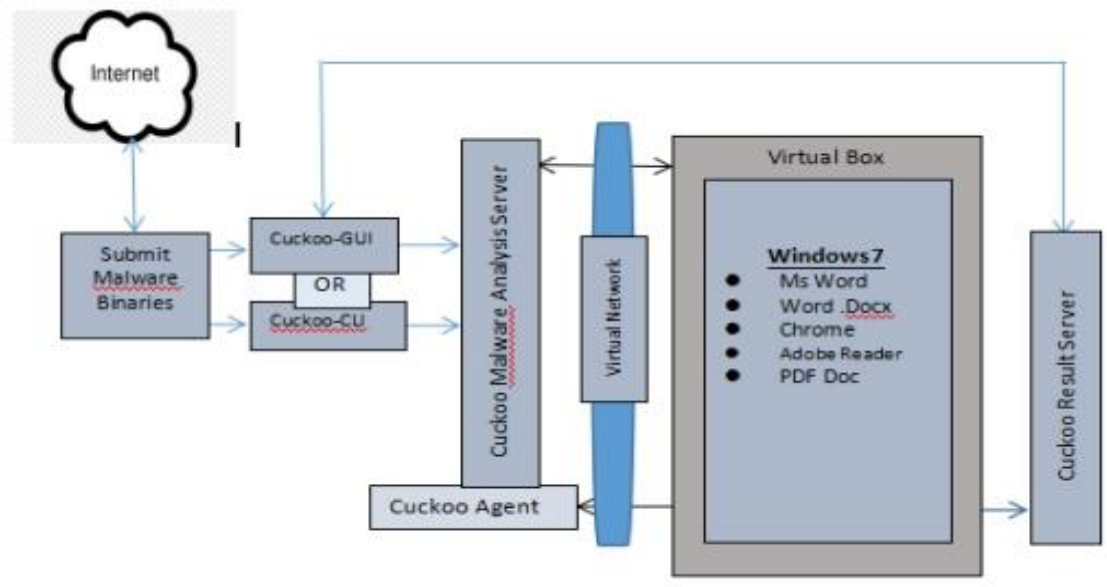


Figure 1: Conceptual architecture

4. Results and Discussion

4.1. Hidden Tor browser

Ransomware has been known to use Tor browser to leverage on its anonymity making it difficult to know the source of the attack. Figure 2 shows that the WannaCry ransomware dumped Tor link in the memory, the victim through the ransom note will be instructed on how to use the link to download and install the Tor browser. The victim henceforth will be required to use Tor browser for any other communication with the attacker. Digital currency, Bitcoin, is the preferred means of payment, Bitcoin digital wallet of the attacker cannot be traced and hence adding another layer of anonymity [16].

Figure 2: Hidden Tor browser

4.2. Contacting command and control server and cryptographic key exchange

There are strains of ransomware that hide their network traffic by using compromised proxy web servers to contact command and control server, updating a list of addresses frequently can be used to block the ransomware [17]. Morato and his colleagues in [17] argue that one of the methods that can be used to detect ransomware is through network traffic control analysis to track DNS requests to certain blacklisted domains that generate domain names dynamically. In our experiment, we captured Ransomware contacting command and control server using secure protocols, the exchange of cryptographically generated key was implemented securely using Transport Layer Security Version-1(TLSv1) protocols. In the dynamic analysis of Petrwrap.exe ransomware this was captured in the analysis of traffic packets and analyzed using Wireshark. The exchange of the key is shown in Figure 3.

Figure 3: Contacting command and control server and cryptographic key exchang*e*

4.3. Deleting files

The authors in [18] attest that ransomware attempt to delete backup files. The authors argue that when privileges to delete backup files are not granted some strains of ransomware attempt to bypass user access control. This was shown by Cerber ransomware that was found to escalate its privileges to administrator after which it deletes shadow copies. We observed that ransomware delete large number of files from the infected system, which is a

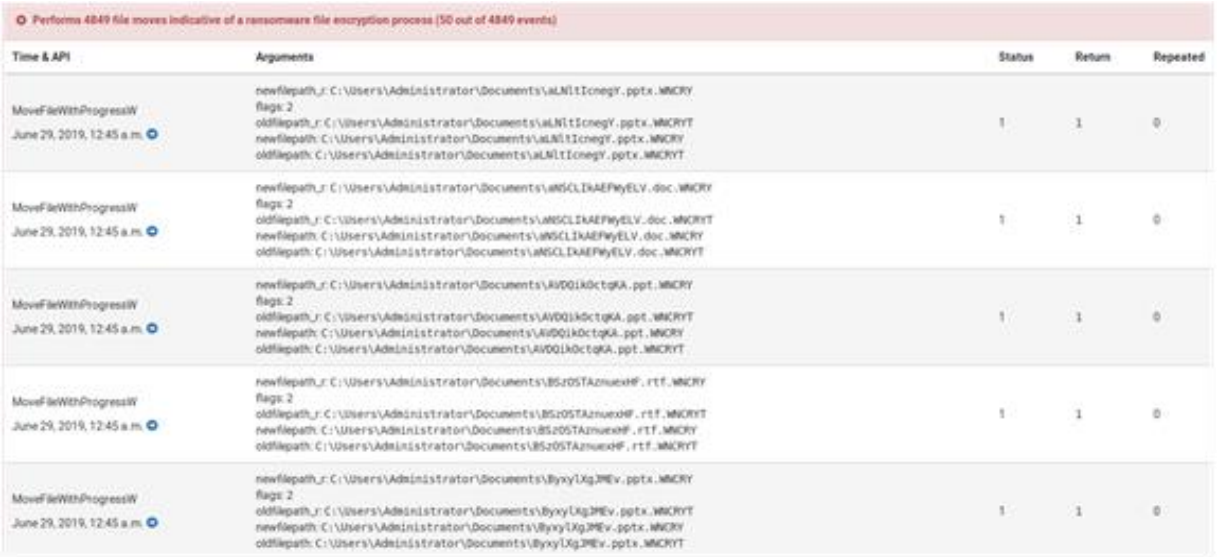
clear suggestion that it is actually a ransomware, wiper malware or system destruction malware. Ransomware is known to delete Windows shadow copies, by deleting these copies it make sure that the encrypted data cannot be decrypted to its original unencrypted version of the same data and the victim cannot be able to recover encrypted files without paying the ransom [18]. Figure 4 shows a sample of deleted files at 5174 during the analysis of WannaCry.

Deletes a large number of files from the system indicative of ransomware, wiper malware or system destruction (50 out of 5174 events)

file	C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\~SDB412.tmp
file	C:\Python27\tcl\tcl8.5\msgs\en_au.msg.WNCRYT
file	C:\Users\Administrator\AppData\Local\Microsoft\Media Player\Sync Playlists\en-US\000064B5\~SD8F62.tmp
file	C:\Users\Symo\AppData\Local\Google\Chrome\User Data\Default\page_load_capping_opt_out.db
file	C:\Users\All Users\Microsoft\Windows Defender\Scans\History\~SDC6E2.tmp
file	C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Extensions\pjkljhegncpnkpknbcohdijeoejaedia\8.2_0_locales\ru\~SD8254.tmp
file	C:\Users\Symo\AppData\Local\Google\Chrome\User Data\Default\Extensions\felcaaldnbdncclmgdcncolpebgiejap\1.2_0_locales\ru\~SDFCD2.tmp
file	C:\Users\Symo\AppData\Roaming\Microsoft\Windows\Cookies\symo@adobe[2].txt
file	C:\Users\All Users\Mozilla\updates\~SDC831.tmp
file	C:\Python26\Lib\email\test\data\msg_39.txt.WNCRYT
file	C:\Python26\Lib\idlelib\HISTORY.txt
file	C:\Python27\Lib\test\~SD4348.tmp
file	C:\Users\All Users\Microsoft\HTML Help\~SDA959.tmp
file	C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\7419.311.0.0_0\cast_setup\chromecast_logo_grey.png
file	C:\Users\All Users\Microsoft\User Account Pictures\Default Pictures\usertile39.bmp.WNCRYT
file	C:\Python27\tcl\tcl8.5\msgs\af.msg
file	C:\Users\All Users\Microsoft\Windows\Caches\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x0000000000000006.db
file	C:\Users\Symo\AppData\Local\Google\Chrome\User Data\Default\Extensions\aohghmighlieiainnegkcijnfilokake\0.10_0_locales\sk\~SDE9AD.tmp

Figure 4: Deleting files

4.4. Moving and appending new file extensions



Performs 4849 file moves indicative of a ransomware file encryption process (50 out of 4849 events)

Time & API	Arguments	Status	Return	Repeated
MoveFileWithProgressW June 29, 2019, 12:45 a.m.	newfilepath_r: C:\Users\Administrator\Documents\aLNltIcnegY.pptx.WNCRY flags: 2 oldfilepath_r: C:\Users\Administrator\Documents\aLNltIcnegY.pptx.WNCRYT newfilepath: C:\Users\Administrator\Documents\aLNltIcnegY.pptx.WNCRY oldfilepath: C:\Users\Administrator\Documents\aLNltIcnegY.pptx.WNCRYT	1	1	0
MoveFileWithProgressW June 29, 2019, 12:45 a.m.	newfilepath_r: C:\Users\Administrator\Documents\aNSCLIkAEFWyELV.doc.WNCRY flags: 2 oldfilepath_r: C:\Users\Administrator\Documents\aNSCLIkAEFWyELV.doc.WNCRYT newfilepath: C:\Users\Administrator\Documents\aNSCLIkAEFWyELV.doc.WNCRY oldfilepath: C:\Users\Administrator\Documents\aNSCLIkAEFWyELV.doc.WNCRYT	1	1	0
MoveFileWithProgressW June 29, 2019, 12:45 a.m.	newfilepath_r: C:\Users\Administrator\Documents\AVDQikOctqKA.ppt.WNCRY flags: 2 oldfilepath_r: C:\Users\Administrator\Documents\AVDQikOctqKA.ppt.WNCRYT newfilepath: C:\Users\Administrator\Documents\AVDQikOctqKA.ppt.WNCRY oldfilepath: C:\Users\Administrator\Documents\AVDQikOctqKA.ppt.WNCRYT	1	1	0
MoveFileWithProgressW June 29, 2019, 12:45 a.m.	newfilepath_r: C:\Users\Administrator\Documents\BSzOSTAznuexHF.rtf.WNCRY flags: 2 oldfilepath_r: C:\Users\Administrator\Documents\BSzOSTAznuexHF.rtf.WNCRYT newfilepath: C:\Users\Administrator\Documents\BSzOSTAznuexHF.rtf.WNCRY oldfilepath: C:\Users\Administrator\Documents\BSzOSTAznuexHF.rtf.WNCRYT	1	1	0
MoveFileWithProgressW June 29, 2019, 12:45 a.m.	newfilepath_r: C:\Users\Administrator\Documents\ByxylXgJMEv.pptx.WNCRY flags: 2 oldfilepath_r: C:\Users\Administrator\Documents\ByxylXgJMEv.pptx.WNCRYT newfilepath: C:\Users\Administrator\Documents\ByxylXgJMEv.pptx.WNCRY oldfilepath: C:\Users\Administrator\Documents\ByxylXgJMEv.pptx.WNCRYT	1	1	0

Figure 5: Moving and appending new file extensions

The author in [6] argues that, analyzing file characteristics of a ransomware can offer more information of an attacking ransomware not only by identifying ransomware notes but also from known file extensions. He notes

that ransomware also performs write, move, delete and rename encrypted files by appending a new file extension over the existing extension. During the analysis of WannaCry binary, 4849 files were moved indicative of ransomware file encryption process, the appended file extension could also be used to suggest the ransomware under investigation, during the binary execution and analysis the appended file extension was .WNCCRY, which explicitly suggest the binary to be WannaCry. Figure 5 shows the sample results of file movement and appending of a new file extension.

4.5. Generating cryptographic key

Ransomware were found to use windows APIs to generate a cryptographic key. Assymetric key generation algorithm is employed to generate a secure key that is used to encrypt files in the system. The generated key is shared with Command & Control server. During the dynamic analysis of WannaCry captured in Figure 6, secure cryptographic key was generated and the message for sending encrypted key was encrypted making it difficult to decipher the key that can be used to decrypt files.

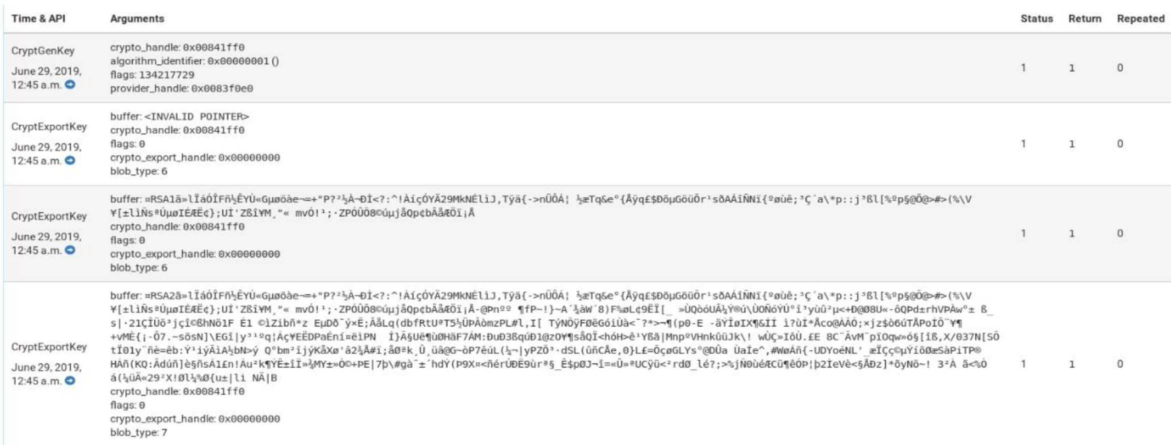


Figure 6: Generating cryptographic key

4.7. Ransomware and other malware look up in virus total results

The sampled ransomware and other malware were all submitted to Virus Total, which is a website that puts together many antivirus products, and online scan engines, users upload files of up to 550MB to the website or they can also send files of up to 32MB via emails. Virus Total is used to check for viruses that users installed antivirus may have missed or to verify any False positive that might have been realized. Cuckoo sandbox is used in Virus Total for dynamic analysis of malwares. According to [16], malware relies on the use of rather common techniques, which includes; injection in a legitimate process, running from %AppData% directory and using .exe which uses the same naming regime as normal Windows .exe, this behavior therefore will make a malware pass without being noticed by the user and even the installed AV.

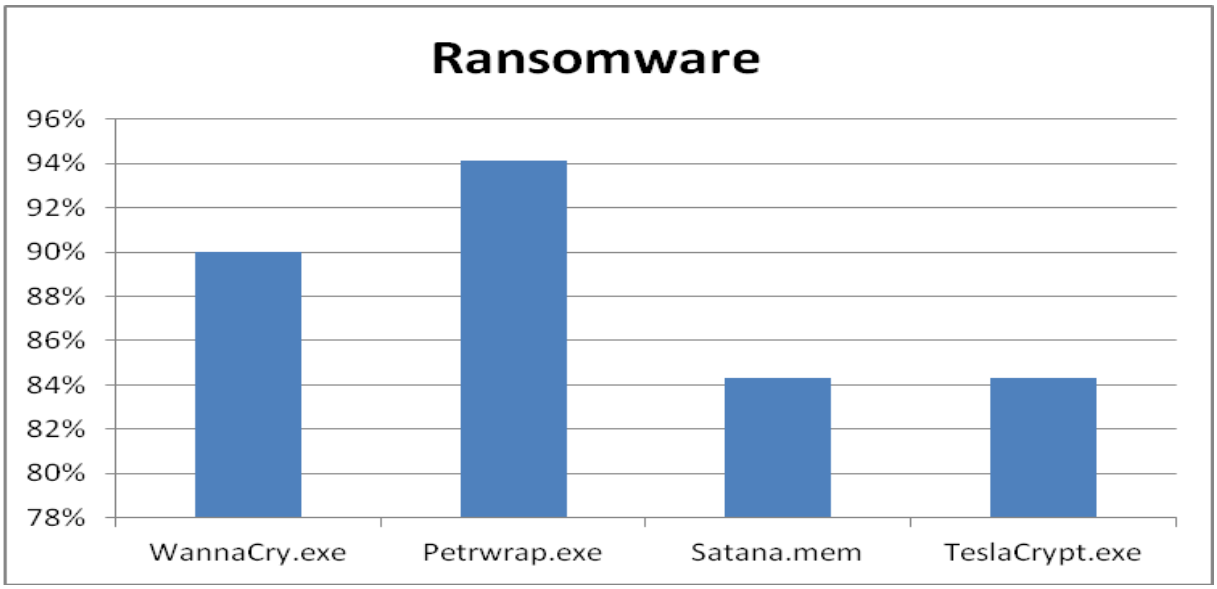


Figure 7: Ransomware detection percentage rating in Virus Total

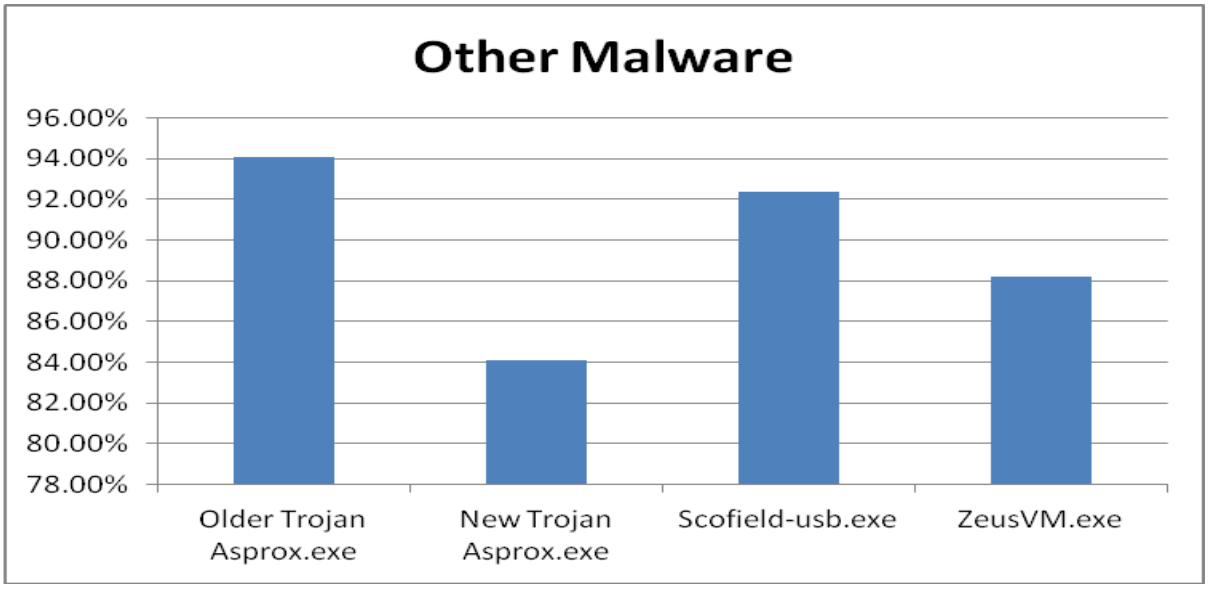


Figure 8: Other malware detection percentage rating in virus total

4.8. Limitation of the study

Cavallaro and his colleagues in [19] demonstrate how malware developers have mastered the art of developing malware that have ability to detect virtualized environment, this characteristics is called anti-virtualization. Virtualized environment and sandboxed environment detection and avoidance are the two major techniques used by developers to achieve anti-virtualization feature. Some strains of conventional malware and especially the latest malware being developed and ransomware have antivirtualization feature that make them not to execute as they would in a normal execution environment.

5. Conclusions and Recommendation

In conclusion, our research study, has confirmed that there exist some variation of ransomware from other forms of malware. The major variations that were recorded from the dynamic analysis of ransomware that were not common with other malware includes; contacting command and control server using secure protocols and encrypted message, downloading Tor browser that facilitate the communication between the victim and the attacker to facilitate ransom payment anonymously, moving and deleting files in large quantity to make it impossible to decrypt data to its original unencrypted data without the decryption key, appending new file extensions to the saved files which disassociate files with their files systems and thereby rendering them inaccessible, generating cryptographic key in the registry where the private key is stored in the Command & Control server and the public key in the victim machine. Although ransomware use subtle attack mechanisms, we observed their detection rate as malicious code to be like that of other malware in Virus Total. From our research study, we observed that careful monitoring of the network traffic and changes in Registry can signal a ransomware attack. Based on this observation we recommend for a further study in developing a system that can be able to continuously and actively monitor network traffic and any malicious activities in the registry like, cryptographic key generation which, has not been initiated by the computer user, raise an alarm by notifying the user and henceforth stop all those suspicious processes.

Acknowledgements

I would like to express my special thanks to my family for their prayers and support. I would also like to extend my gratitude to my professors at the University of Nairobi for their guidance throughout this project.

References

[1]. A. Clark, Q. Zhu, R. Poovendran, & T. Başar, (2013, June). An impact-aware defense against stuxnet. In 2013 American Control Conference (pp. 4140-4147). IEEE.

[2]. D.S. Wall, “Dis-organised crime: Towards a distributed model of the organization of cybercrime.” The European Review of Organised Crime, vol. 2, 2015.

[3]. Internet security threat report. “ISTR Internet security threat report”. Internet: http://book.itep.ru/depository/surveys/ISTR22_Main-FINAL-APR24.pdf. 2017

[4]. T.S.Rajput. “Evolving Threat Agents: Ransomware and their Variants.” International Journal of Computer Applications, vol. 164, pp.28-34, 2015.

[5]. K. S. Choi, T.M. Scott, & D.P. LeClair. “Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory”. International Journal of Forensic Science & Pathology. 2016.

[6]. D. Nieuwenhuizen. “Abehavioural-based approach to ransomware detection”. Whitepaper. MWR Labs Whitepaper. 2017.

[7]. F. Mbol, J.M Robert, & A. Sadighian, (2016, November). An efficient approach to detect torrentlocker ransomware in computer systems. In International Conference on Cryptology and Network Security (pp. 532-541). Springer, Cham.

[8]. N. Hampton, & Z.A. Baig,. Ransomware: Emergence of the cyber-extortion menace. 2015

[9]. Kaspersky. (2015). "No Ransom: The National high tech crime unit of the Netherlands' police and Kaspersky lab helps victims to escape from Coinvault ransomware". Internet: https://www.kaspersky.com/about/press-releases/2015_no-ransom-the-national-high-tech-crime-unit-of-the-netherlands-police-and-kaspersky-lab-help-victims-to-escape-from-coinvault-ransomware,2016

[10]. P. Zavarsky, & D. Lindskog. "Experimental analysis of ransomware on windows and android platforms: Evolution and characterization." Procedia Computer Science, vol.94, pp.465-472, 2016.

[11]. N. Andronio, S. Zanero, & F. Maggi, (2015, November). Heldroid: Dissecting and detecting mobile ransomware. In International Symposium on Recent Advances in Intrusion Detection (pp. 382-404). Springer, Cham.

[12]. N. Scaife., H. Carter., P. Traynor., & K.R. Butler., (2016, June). Cryptolock (and drop it): stopping ransomware attacks on user data. In 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS) (pp. 303-312). IEEE.

[13]. Internet security threat report. "ISTR Internet security threat report". Internet: www.itu.int/en/ITUD/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf. 2015

[14]. A. Tseng, Y. Chen, Y. Kao, & T. Lin. "Deep learning for ransomware detection". IEICE Tech. Rep., vol. 116, pp.87-92, 2016.

[15]. A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, & E. Kirda, (2015, July). Cutting the gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 3-24). Springer, Cham.

[16]. A. Ali, R. Murthy, & F. Kohun. "Recovering from the nightmare of ransomware-how savvy users get hit with viruses and malware: a personal case study." Issues in Information Systems, vol.17,2016.

[17]. D. Morato, E. Berrueta, E. Magaña, E., & M. Izal,. (2018). Ransomware early detection by the analysis of file sharing traffic. Journal of Network and Computer Applications, vol. 124, pp.14-32.

[18]. J. Huang, J. Xu, X. Xing, P. Liu, & M.K. Qureshi. (2017, October). Flashguard: Leveraging intrinsic flash properties to defend against encryption ransomware. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 2231-2244.

[19]. L. Cavallaro, P. Saxena & R. Sekar, (2007). Anti-taint-analysis: Practical evasion techniques against information flow based malware defense. Secure Systems Lab at Stony Brook University, Tech. Rep, pp.1-18.