



**UNIVERSITY OF NAIROBI**

**COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES  
SCHOOL OF COMPUTING AND INFORMATICS**

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

**Kihiu Simon Mungai**

**P53/86204/2016**

**Supervisor: Dr. Elisha Abade**

Research Project Report Submitted in Partial Fulfillment of the Requirement for the Award of the  
Degree of Master of Science in Distributed Computing Technology.

**2020**

**Declaration**

I hereby declare that this project report is my original work under the supervision of Dr Elisha Abade has never been submitted elsewhere for examination, award of degree or publication. Where other people work has been used, this has been properly acknowledged by citation and referencing in accordance with University of Nairobi requirements.

---

Simon Kihui

---

Date

P53/86204/2016

**Declaration by supervisor**

This project report is submitted to the School of Computing and Informatics for examination with my approval as the research supervisor.

---

Dr Elisha Abade

---

Date

School of Computing and Informatics

## **Dedication**

This work is dedicated to my wife Joyce Wanjiru and my son Paul Kihiu for their Love, understanding and their moral support in the whole period I was conducting this study. My father Paul Kihiu (Posthumously) for believing in me and making me understand the value of education and mother, Mary Wangari for teaching me basic math symbols at a tender age, and teaching me the value of hard work and discipline.

## **Acknowledgement**

I would like to thank the Almighty God for the strength and guidance He has given me throughout the research period. My sincere gratitude to my research supervisor Dr. Elisha Obade whose valuable guidance helped me patch this project and make it a success. I would also like to sincerely thank Avenue Group It manager, Mr. Geoffrey Gitagia for his guidance and brainstorming in choosing a feasible research theme. My sincere thanks to Avenue Group Chief Operating Officer, Dr. Andrew Kekovole for his mentorship in the industry, I would also wish to thank my friends and classmates for their encouragement and support throughout this project period.

## **Abstract**

Ransomware have become a real threat to the use of technology, unlike other form of malware which could target systems by deleting some files, editing some files and some creating backdoor for the attacker to access the system, ransomware have gone a notch higher by targeting human. This is achieved when ransomware encrypt 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 which is difficult to decrypt even when the computational power is not limited.

Ransomware is mostly spread through the use of a phishing email which tricks the victim into clicking on a link that is loaded with malicious files or downloading an attachment which is loaded with malicious files. Due to this, it is of benefit to educate the employees so as to be more careful when interacting with emails of unknown origin.

Attackers are capitalizing on the fact that ransomware attack is highly automated and therefore there are limited chances of getting the attacker, the whole process from attack to ransom payment is fully automated. There is no system that have so far been developed to get rid of ransomware and therefore prevention of attack is of paramount importance. This study therefore seek to investigate the distinctive features of ransomware that are not available to other forms of malware. These features can be used to help detect an impending ransomware attack and thereby stop any possible data encryption midway. The conventional antivirus have no capability to fully detect and stop ransomware attack and therefore necessitating some more extra measure to keep the system secure against the ransomware.

This study will also seek to study the state and preparedness of Kenyan companies in regard to ransomware attacks. The fact that very few companies in Kenya take cyber security with seriousness it deserve makes Kenyan companies an easy target to cyber criminals. There is a major cyber security professional gap in Kenya and the few available come at an added cost to the company, therefore, small and medium companies fail to meet this important requirement to safeguard their digital asset.

In this work we present some of the major behavior that were found to be common with ransomware and not with other malware. These peculiar behaviors can be captured from suspicious network activities to suspicious file activities. Our results show that a careful analysis of suspicious network and file activities can help detect a ransomware attack, also careful analysis of ransomware behavior can help develop a system that can detect an impending ransomware attack and thereby eliminate it.

## **Acronyms**

IoT	-	Internet of Things
NHS	-	National Hospital Service
DDoS	-	Distributed Denial of Service
RaaS	-	Ransomware as a service
IT	-	Information Technology
MFT	-	Master File Table
WPAD	-	Web proxy auto discovery.
AV	-	Antivirus
CPU	-	Central Processing Unit.
HDD	-	Hard Disk.
SDN	-	Software defined networking
NTFS	-	New technology file system
I/O	-	Input output
UDP	-	User datagram protocols
TCP	-	Transmission control protocols
NetBIOS	-	Network Basic Input/output System
LLNMR	-	Link-local Multicast name resolution

## Table of Contents

Declaration .....	ii
Dedication .....	iii
Acknowledgement .....	iv
Abstract .....	v
Table of Contents .....	vii
1. CHAPTER ONE .....	1
INTRODUCTION .....	1
1.1 Background of the Problem .....	1
1.2 Problem Statement .....	3
1.3 Research Objectives .....	4
1.4 Research Questions .....	4
1.5 Justification of the Problem .....	5
1.6 Limitation of the Study .....	6
2. CHAPTER TWO .....	7
THEORETICAL LITERATURE REVIEW .....	7
2.1 Malware/ Malicious Code .....	7
2.2 How Antivirus Software Works .....	7
2.2.1 Virus definition .....	8
2.2.2 Heuristics .....	8
2.3 Ransomware .....	8
2.4 Public Key Cryptography .....	11
2.5 Time Series of Ransomware .....	11
2.6 Common Ransomware .....	13
2.7 Future of Ransomware .....	14
2.8 How Ransomware Work .....	15
2.9 Ransomware as a Service .....	17
2.10 Bitcoin .....	18
2.11 Empirical Literature Review .....	18
2.12 Ransom Payment .....	24

2.13 Current Solution to Ransomware Attack .....	25
2.14 Conceptual Architecture .....	26
3. CHAPTER THREE .....	27
RESEARCH METHODOLOGY .....	27
3.0 Research Design .....	27
3.1 Sample Size and Sampling Frame .....	29
3.2 Research Instruments.....	30
3.3 Questionnaire.....	31
3.4 Observation.....	31
3.5 Target population .....	32
4. CHAPTER FOUR.....	33
RESULTS AND DISCUSSIONS .....	33
4.1 Ransomware and other malware execution - Cuckoo sandbox results .....	33
4.2 Network Traffic Results and Analysis .....	33
4.2.1 Network traffic protocols. ....	34
4.2.2 NBNS protocol.....	35
4.2.3 LLMNR.....	35
4.2.4 External host communication.....	36
4.2.5 Malicious URLs in process memory dump.....	37
4.2.6 Private info from internet browser/ locate browser. ....	38
4.2.7 Use of hidden Tor browser. ....	39
4.2.8 Contacting Command and control server. ....	40
4.2.9 Locker Ransomware.....	41
4.2.10 Querying computer NetBIOS Name. ....	42
4.3 File Manipulation .....	42
4.3.1 Creating/ writing new files.....	43
4.3.2 Deleting files. ....	43
4.3.3 Moving files. ....	45
4.3.4 Adding file extension. ....	45
4.3.5 Creating Office documents.....	47
4.3.6 Dropping files mime types .....	47



4.3.7 Dropping executable files.....	48
4.4 Registry Manipulation .....	49
4.4.1 Registry changes to make malware take control of the system.....	49
4.4.2 Generating cryptographic key. ....	50
4.4.3 Querying and opening Regkey. ....	51
4.4.4 Registry key interactions. ....	52
4.4.5 Terminating processes. ....	52
4.4.6 Encrypting data / Lock screen.....	53
4.4.7 Use of windows utility.....	54
4.4.8 Writing messages.....	55
4.4.9 Creating new/ injecting suspicious process.....	55
4.4.10 Anti-virtualization. ....	56
4.5 Questionnaire Results and Discussions .....	57
4.5.1 Ransomware threat.....	57
4.5.2 Ransomware attack mitigations. ....	57
4.5.3 Ransomware distribution .....	58
4.5.4 Other types of malware that are not ransomware.....	59
4.5.5 Types of malware other than ransomware.....	60
4.5.6 Cybersecurity & Digital Forensic Department And Accompanying Policies In Organizations?.....	61
4.6 Ransomware and Other Malware Look Up In Virus Total Results .....	62
5. CHAPTER FIVE .....	64
CONCLUSION AND RECOMENDATION .....	64
References.....	68
Appendices.....	73
Appendix 1: Questionnaire.....	73
Appendix 2: Questionnaire Responses.....	74

## List of Figures

Figure 1: A typical Ransomware Note .....	10
Figure 2: Evolution of different variants of Ransomware .....	12
Figure 3: The five common Ransomware variants in the countries .....	14
Figure 4: Windows based Ransomware life-cycle.....	16
Figure 5: How Ransomware works.....	17
Figure 6: Conceptual Architecture .....	26
Figure 7: Network traffic protocols .....	35
Figure 8: External Host communication .....	37
Figure 9: Malicious URLs in Process memory dump.....	38
Figure 10: Use of Hidden Tor Browser.....	40
Figure 11: Contacting Command and control server .....	40
Figure 12: Locker Ransomware note .....	41
Figure 13: Querying computer NetBIOS Name .....	42
Figure 14: Creating/ Writing new Files. ....	43
Figure 15: Deleting Files .....	44
Figure 16: Moving Files.....	45
Figure 17: Adding file extension.....	46
Figure 18: Dropping files Mime types.....	48
Figure 19: Generating cryptographic key .....	51
Figure 20: Querying and opening Regkey .....	51
Figure 21: Registry key interactions .....	52
Figure 22: Have you ever encountered a ransomware attack or threat in your company?.....	57
Figure 23: If you have ever experienced a ransomware attack or threat, how did your company recover from the attack?.....	58
Figure 24: How was the ransomware introduced into your system? .....	59
Figure 25: Have you ever been infected by another malware other than ransomware? .....	60
Figure 26: Which other malware that have ever infected your system? .....	61
Figure 27: Cybersecurity & Digital forensic department and accompanying policies in organizations? .....	62
Figure 28: Ransomware and other malware look up in Virus total detection rate.....	63
Figure 29: Ransomware and other malware look up in Virus total detection rate.....	63

## List of Tables

Table 1: Twenty nine variants in nine families of the commonly cited ransomware.....	20
Table 2: getting the sample size of a known population .....	30
Table 3: Network traffic protocols .....	34
Table 4: Suspicious protocols .....	36
Table 5: External Host communication.....	37
Table 6: Malicious URLs in Process memory dump. ....	38
Table 7: Steal private info from internet browser/ Locate browser .....	39
Table 8: Use of Hidden Tor Browser .....	39
Table 9: Contacting Command and control server .....	40
Table 10: Creating/ Writing new Files. ....	43
Table 11: Deleting Files .....	44
Table 12: Adding file extension .....	46
Table 13: Creating Office documents .....	47
Table 14: Dropping files Mime types .....	48
Table 15: Dropping executable Files .....	49
Table 16: Registry changes to make malware take control of the system .....	50
Table 17: Generating cryptographic key .....	50
Table 18: Querying and opening Regkey.....	51
Table 19: Terminating processes.....	53
Table 20: Encrypting data / Lock screen.....	54
Table 21: Use of windows utility .....	54
Table 22: Writing messages .....	55
Table 23: Creating new/ injecting suspicious Process .....	56
Table 24: Anti-virtualization .....	56

## Equations

Equation 1: Sample Size and Sampling Frame.....	29
---	----

# 1. CHAPTER ONE

## INTRODUCTION

### 1.1 Background of the Problem

Since the birth of internet, more than two and half decades ago, the cybersecurity threats and attacks have been on raise and even worse have seen an introduction of more sophisticated ways which are more robust and intelligent. Stuxnet and Zeus make a good example depicting how cybercrime have become more and more professional. The cybercriminal are now not interested in being known or being admired, thus therefore they have come up with new ways to carry out an attack, which are automated and anonymous. Ransomware have become a game changer in the history of cybercrime, unlike other conventional malware, ransomware target human being, they extort money from victims and deposit it in a digital wallet of the attacker without the attacker being present. (Wall, 2015).

In the 2017 Symantec and McAfee, Control risk and others considered ransomware as one of the most dangerous malware threat. This was after realization that, modern ransomware not only infect personal computer but also Mobile application, IOT and lately the cloud based services (Rajput, 2017).

According to Rajput, 2017, there are three major attack vectors, this is so because of characteristics associated with the data set stored in the computer systems but also due to the user awareness and vulnerability. He noted home users as a specific target, this is because of lack of knowledge and also awareness. Businesses is also a good target because of the kind of information that businesses rely upon running their daily activities, once businesses have been denied access to their vital data, the only way out is to make a ransom payment to avoid total loss of the data. Public institutions are the third target; this includes government agencies due to the large volume of data that are in their servers, which also include confidential information.

Release rate of malicious code and other programmed threats have been on rise and Symantec Preliminary results published in 2008, suggested that, there is more malicious code than authentic programs online.

Microsoft report (2011), noted that there is a huge online repository for malicious code such that there is only one download in every fourteen downloads that is not a malicious code.

Cybercriminal have also mastered the art of using Social media to spread malware to unsuspecting users devices.

Further, 2016 experienced a surge in the use of ransomware and reemergence of distributed denial of service attacks using Internet of Things botnets against personal information. This consists of a growing number of online, offline user accounts and online services. In 2017, this tendency was expected to continue since cybercriminals are working to improve ransomware and Internet of Things botnets. The demand for new ways to secure data in the cloud have also raised as the new attacks have been reported to be more professionally targeted attacks as well as data manipulation attacks.

According to Choi, Scott & LeClair (2016), there is lacking a practical approach towards explaining as to why 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.

Cohen and Felson in their work they developed the RAT theory in 1979 that looked at three principles that lead to rampant ransomware deployment. The first principle looked at the attacker who could be motivated by various factors, the second principle looked at the target which could be suitable for the attack to be carried out and the third principle looked at the lack of previous studies that could guide in mitigating the future attacks. Efficient use of RAT has been used to get lead of situational crime strategy.

Ransomware have been found to use standard cryptographic algorithms, this have therefore made the development of ransomware to be 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 ransom (Nieuwenhuizen, 2017).

According to Nieuwenhuizen (2017), ransomware have become an enticing business model for cyber criminals due to its high returns, unlike other crimes where criminals risk being caught, in ransomware attack the attacker have very little chances of being caught once the ransomware is developed as it is highly automated. Nieuwenhuizen (2017) observed three possible reasons as to why ransomware have become so successful.

- i. The use of crypto-currency as a means of ransom payment that have made it anonymous and seamless.
- ii. The use of already securely developed encryption standards in development of ransomware and the introduction of Ransomware-as-a-Service.
- iii. Ransomware is distributed by the use of spam emails, or redirection to a link that is a trap toward accessing infected material and thereafter downloading to your local system, which are both cost effective means of distribution.

Since ransomware uses an advanced encryption algorithm there is no method of ridding attacked computer of ransomware aside from paying the ransom, which means that prevention is key. There are also no developed systems, which are dedicated to detecting ransomware before they infect victim's data. The conventional anti-virus available are not designed to efficiently detect a ransomware, and they have difficulties in detecting polymorphic ransomwares (Mbol, Robert & Sadighian, 2016). Even the-state-of -the-art research tactics, which showed almost perfect detection and accuracy on non-ransomware Android malware, identified only 48.47% of the ransomware dataset (H.Bos et al., 2015).

## **1.2 Problem Statement**

Ransomware have been there for more than a decade, as the technology advances the use of even more advanced ransomware have been experienced and therefore becoming a real problem. In the early days, ransomware was known by attacking home users who could unknowingly click on a fake attachment in an email which could in turn lock their PC files and photos. This approach has shifted to now attacking businesses which have more computers, more valuable resources and also due to their ability to pay the ransom.

There has been a rise in the number of variants of ransomware and each new variant come with a new signature, this have made it difficult in employing the conventional methods; signature and heuristics-based detection techniques.

This study will focus on understanding the key characteristics of ransomware that are not common with other malwares that can be used to detect ransomware before it encrypts victim's data and therefore be eliminated. There have been various studies that have been conducted to show characteristics of various variants of ransomware that are realized after an attack.

Ransomware have developed from the implementation of symmetric key encryption algorithm to currently asymmetric key generation algorithm.

This study therefore will come up with data and especially collected from TCP dump and analyzed using wireshark and registry changes showing the distinct features of ransomware that are not common with others malwares that can be used to inform an impending threat of ransomware attack.

### **1.3 Research Objectives**

Since the development of ransomware that uses secure encryption algorithm, and anonymizing web like TOR that have made it possible for an attack and ransom demand to be implemented covertly attacks have raised globally. Therefore, the purpose of this study will be to analyze ransomware, other malware using cuckoo sandbox and compare the analysis results. This will inform the researcher on the keys features that are depicted by ransomware and are not depicted by other malware. This will therefore help the researcher to meet the following objectives.

#### **1.3.1 Research Objectives**

- i. To investigate the specific distinctive features of the ransomware tactics in relation to other malwares.
  - a. To probe if changes made in the registry by ransomware are the same changes made by other types of malware.
  - b. To compare the network traffic during ransomware execution, other malware execution.
- ii. To find out the prevalence of ransomware and other types of malware in Kenya.
- iii. To investigate effective ways of detecting ransomware before an attack occur.
- iv. To find out if the conventional antivirus can be used to detect an impending ransomware attack.
- v. To propose the best security measures that can be used to ward off ransomware.

### **1.4 Research Questions**

- 1) What are the specific distinctive features of the ransomware tactics in relation to other malwares?

- a. Are changes made in the registry by ransomware the same changes made by other types of malware?
  - b. Is there any difference in network traffic during ransomware execution and other malware execution?
- 2) What is the prevalence rate of ransomware and other forms of malware in Kenya?
  - 3) What are the effective ways of detecting ransomware before an attack occur?
  - 4) Can conventional antivirus be used to detect and stop ransomware attack?
  - 5) What are the best security measures that can be used to ward off ransomware?

### **1.5 Justification of the Problem**

The conventional malwares usually infect devices where they could delete, edit some files, change registry or even create a backdoor in the system. With the advent of ransomware the tactics have changed, ransomware are designed to target humans where they demand for ransom. Both computer systems and mobile devices are prone to ransomware attacks. Traditional protection methods are the one still in use to get rid of ransomware since there have been no much research conducted on this. The precise attack schemes they use have rendered even futuristic mobile malware protection methods unsuccessful to get rid of ransomware (Andronio, Zanero & Maggi, 2015).

Ransomware attacker have several ways that they can gain access to the organization systems. A study conducted by Global ransomware study in 2018 sought to understand how ransomware attacker gain access to the organizations as one of their objectives, they used the following means that can be used by a ransomware attacker as the main tools:

- a. Phishing via email or social media sites.
- b. Visiting a compromised website to make a download.
- c. Infection through a botnet.
- d. Use of a worm that could spread across the network by the attacker.

Though in this report there was an option of giving any other way that ransomware could attack, those were the major means that were considered.

According to Sentinel: Global Ransomware Study (2018), 2018 saw a rise in ransomware attack from 48% in 2016 to 56% in 2018. This is according to the data collected where surveyed top management from Information Technology risk assessors function, fraud, or auditor functions



reported that their organization had been attacked by ransomware in 2018. This report also noted that; the surveyed companies had to defend themselves against an average of five ransomware in 2018.

According to Popoola, Ojewande, Sweetwilliams, John & Atayero (2017), Ransomware have changed tact and are now attacking companies instead of individuals. This have seen a tremendous growth in digital extortion in the last six years. This have largely been contributed by the raise in number of people who owns mobiles devices which in turn run millions of online applications and services which can be used as a gateway by the attacker to gain access to these devices. They also observed that about 80% of ransomware attacks are as a result of unpatched flash, this therefore have rendered ransomware as the biggest cyber scam in businesses.

The internet of things (IoT) will enable more and more devices including wearable computers in addition to smart TVs, smart watches, smart locks, smart clothing and smart fridges to be connected to the internet, this therefore will create a conducive environment for the ransomware to spread. Cyber criminals have advanced such that there is even ransomware-as-a-Service offered in the darknet, which allow even inexperienced cybercriminals to have an access to customizable ransomware (Salvi & Kerkar, 2016)

## **1.6 Limitation of the Study**

- i. Ransomware are encrypted form of malware and due to encryption it makes it harder for antivirus scanner to detect them.
- ii. Due to limited time to carry out this study, looking for factors that can be utilized in protecting zero-day attack will not be feasible. Therefore, only the distinctive features of ransomware as compared with other malware will be considered.
- iii. Some malware are able to detect a virtualized environment and therefore they fail to execute the same way they would have executed in a real environment

## **2. CHAPTER TWO**

### **THEORETICAL LITERATURE REVIEW**

#### **2.1 Malware/ Malicious Code**

Malware is a broad term used to refer to various types of malicious code, familiar types of malware include; Rootki, Adware, Virus, Spyware, Ransomware, Keylogger, Trojan, Malicious crypto-mining and Exploits, Worms

Broadband internet has helped in the rise of malicious software which were initially written as a prank. Recent malware has been designed with the intent of extorting the computer users. In 2008 Symantec in their published preliminary results suggested that the release of malicious software may have exceeded the release rate of authentic software applications (Ray & Nath 2016).

There are two major ways in which a computer system can become infected by malwares

- a) The internet; many programmed threats are on the internet where an internet user may click a fake link that in turn get re-directed to a virus download site. Computer updates and many more other software are also pushed over the internet and sometimes they get infected and when downloaded they infect your computer.
- b) Malicious email attachment; attackers have mastered the art of social engineering; victims are lured with an email that seems in line with their line of job. Those emails come with a download file attached that bears the file name of an interest to the user, these attachments are infected with virus and when downloaded they infect the victim computers system.

#### **2.2 How Antivirus Software Works**

Antivirus commonly abbreviated as AV is a computer program that is intended to protect a computer system from programmed threats, which when introduced in a computer system it interfere with the normal working of a computer, may change file extensions of some documents rendering them inaccessible and act as a backdoor allowing an attacker to steal some sensitive information. They are self-replicating spreading from one computer to another. Antivirus may work by protecting infection of a computer by a malware or by removing already installed

malware. They therefore scan computer comparing the signature of all programs with signature in its database and in case a certain program signature is found to match with the one in AV database, it will be removed or stopped from installing in the system (Wanjala & Jacob, 2018).

Malware can be identified by running them in a sandbox, this is a virtual environment that allows malware to be executed without interfering with the host system, and then their behavior is noted. Data mining is the latest technique that is used in detecting malware; together with machine learning uses a series of file properties pulled out from the file. Based on an algorithm they are able to categorize codes as either malicious or authentic based on the behavior of a file.

### ***2.2.1 Virus definition.***

Antivirus firms use honeypots to harvest malicious software's from the wild, after which they analyze them and if proven to be malicious their signature is extracted and added to signature database. Antivirus will be comparing any software signature with the one in the database and in case it matches one in the database it will be blocked, or it will be removed. Malware authors have recently developed polymorphic, oligomorphic and even metamorphic, which are able to modify themselves thereby disguising themselves and hence therefore will not match virus signature in the database (Szor, 2005).

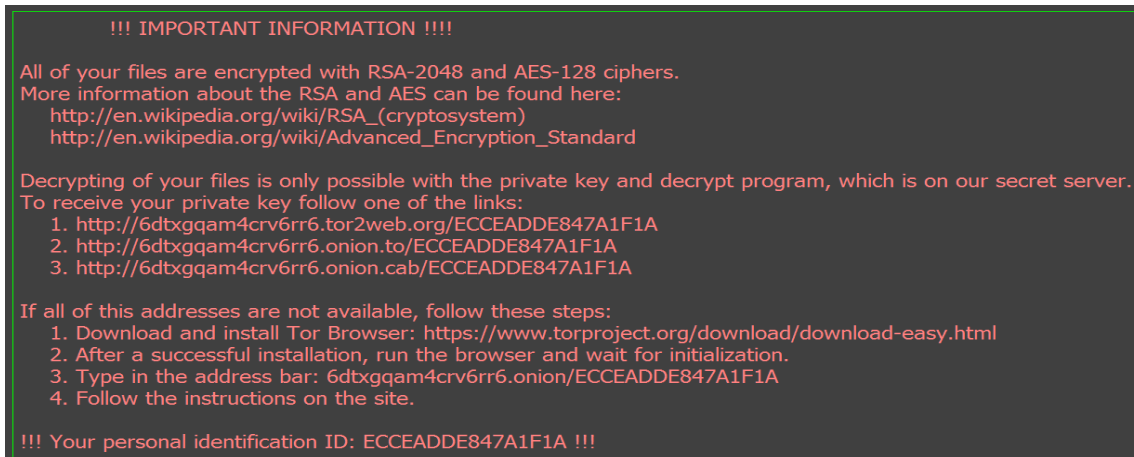
### ***2.2.2 Heuristics.***

A single virus has been modified to come up with varying features, this leads to different strains of virus called variants. This new variant cannot be detected by signature based method since they have been slightly modified and therefore signature change. Virus researcher therefore get the core features which does not change even after slight variation. This unique core features of a virus family help in developing a generic signature which usually relies on wildcard characters that contain non-specific code (Director, Hawes, Director, Grooten, Executive, Sketchley, & Gracey, 2013).

## **2.3 Ransomware**

Young and Yung (2004) stated that upcoming attacks would mix complex cryptographic algorithm to develop malware that will be used to attack information system (Luo and Liao, 2007). Recently, the surfacing of new malware type called ransomware, begun to gain attentiveness among cyber security professionals and researchers. Striking major threat to the

security of data, ransomware exploit the victims who are internet users by taking possession of their files by encrypting them hence rendering them inaccessible, and then demanding for a ransom to be paid in form of Bitcoin for decryption key to be supplied. Being on the lookout for system vulnerabilities, ransomware always encrypts victim's files using a secure public key cryptography and leave a pop-up message on the screen demanding for a ransom to be paid for the attacker to decrypt the files. Ransom is paid by sending money to the selected online currency account or by purchase of pharmaceutical medicines from the cybercriminal preferred online drugs store (Luo and Liao, 2007). Payment could also be requested in Bitcoin or other untraceable currency (Zavarsky, & Lindskog, 2016). The first ransomware discovered and implemented asymmetric key generation algorithm was CryptoWall 3.0 in early 2015, this was followed later by discovery of CryptoWall 4.0 and Locky. The use of asymmetric key generation algorithm has revolutionized the deployment of ransomware in victimization of computer users. This has been made so since every communication after ransomware is introduced to a computer system become automated only depending on the attacked machine and the command and control (C&C) server. It has also been noted that a well implemented asymmetric crypto-ransomware is not feasibly breakable even when the computing power is unlimited (Cabaj, Gregorczyk, Mazurczyk, Nowakowski & Żórawski 2018). Cabaj et al. (2018), attest that using a Software-Defined Networking based method for distinguishing ransomware variants that focuses on ransomware communication characteristics, careful scanning of HTTP messages patterns and their size can be used as an early detection mechanisms of ransomware threats.



*Figure 1: A typical Ransomware Note*

Retrieved from: <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransom-notes-know-what-ransomware-hit-you>

Ransomware relies on two tactics to extort money from the victim; for a crypto ransomware they encrypt some selected files or even all files, another tactic relied upon is achieved by locker ransomware, this work by locking the screen denying the victim access to the computer. In either case a demand for a ransom is printed on the screen, this demand come with a promise to release the private key stored in command and control server afterwards. Paying ransom is not encouraged as this will make one to appear a weaker target and the victim might be targeted again, also this will not guarantee for your data to be decrypted and one might end up losing all the necessary information, therefore having your files backed up is encouraged as the best option from recovering from a ransomware attack.

The crypto family goes through various stages from when the victim's machine is infected to the time the ransomware contact command and control server for decryption key. The locker ransomware similarly follows the same steps though it does not encrypt data but it escalate the privileges to be administrator allowing it to locks the computer system from access by the user (Zavarsky, & Lindskog, 2016).

## **2.4 Public Key Cryptography**

Discovered by Rivest, Shamir and Adleman about 1970. This is a Cryptographic algorithm based on mathematical calculations that produce a one-way function; it is also referred to as asymmetric cryptography. This cryptographic system produces a pair of keys, one key, which is private, is kept as a secret, and the other key is disseminated freely as the public key. Both public and private key are mathematically related but it is not feasible to generate a private key given the public key. During a ransomware attack, private key is stored in a secret command and control server. This strategy only allows the encrypted data to be decrypted by this server and none other. This is way that has been used to ensure security and secrecy in digital communication is held at highest regard. Public key cryptography is very useful especially in financial transaction only that it has been used as a means of making a cyber-attack to be successful and anonymous.

## **2.5 Time Series of Ransomware**

According to Rajput (2017), ransomware infection started as early as 1989, the first discovered ransomware was called AID Trojan which was spread through spam mail. The early variants were never as dangerous since the concept of encryption was not as understood as it is now. They used weak encryption which could only encrypt file name and the means of payment which is supposed to be anonymous was unavailable, therefore it was unsuccessful. The year 2005 saw a great milestone, the first crypto ransomware was released as scareware which could pose as a fake antispyware. The fake antispyware asked for the user to pay a ransom in range of USD \$30 to USD \$90 with the promise to making victims corrupted data cleaned. Rajput, (2017) classified various variants of ransomware that have been discovered since 1989 chronologically as shown in the diagram below:

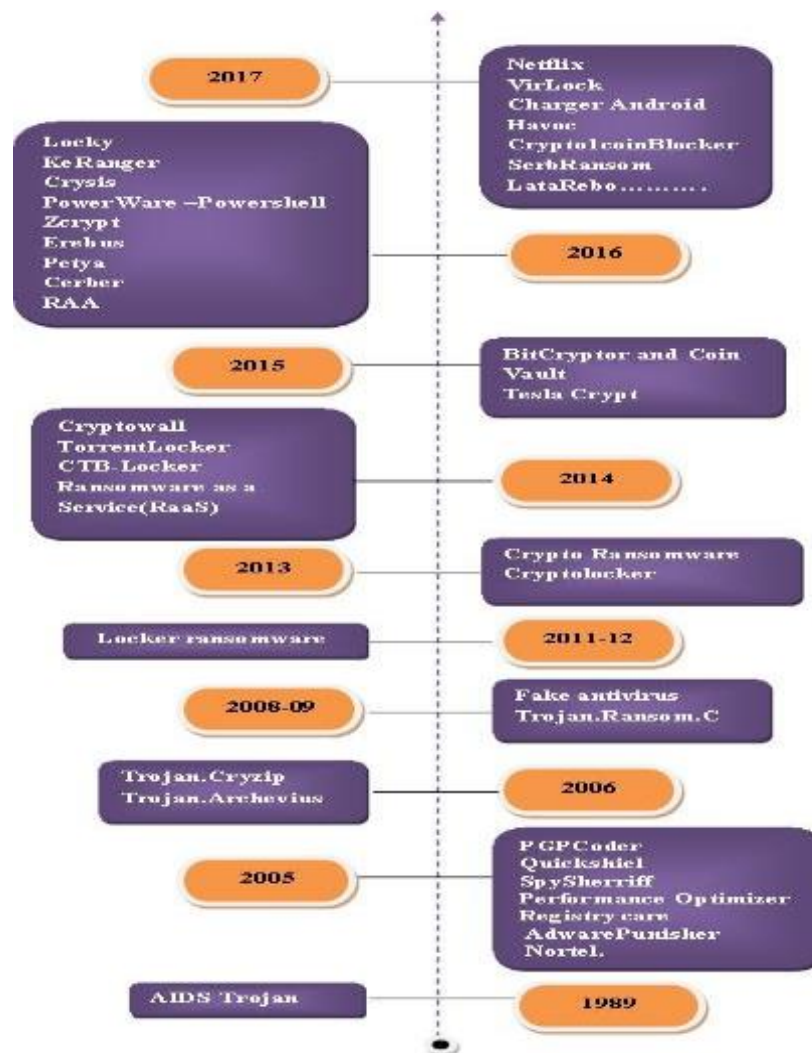


Figure 2: Evolution of different variants of Ransomware

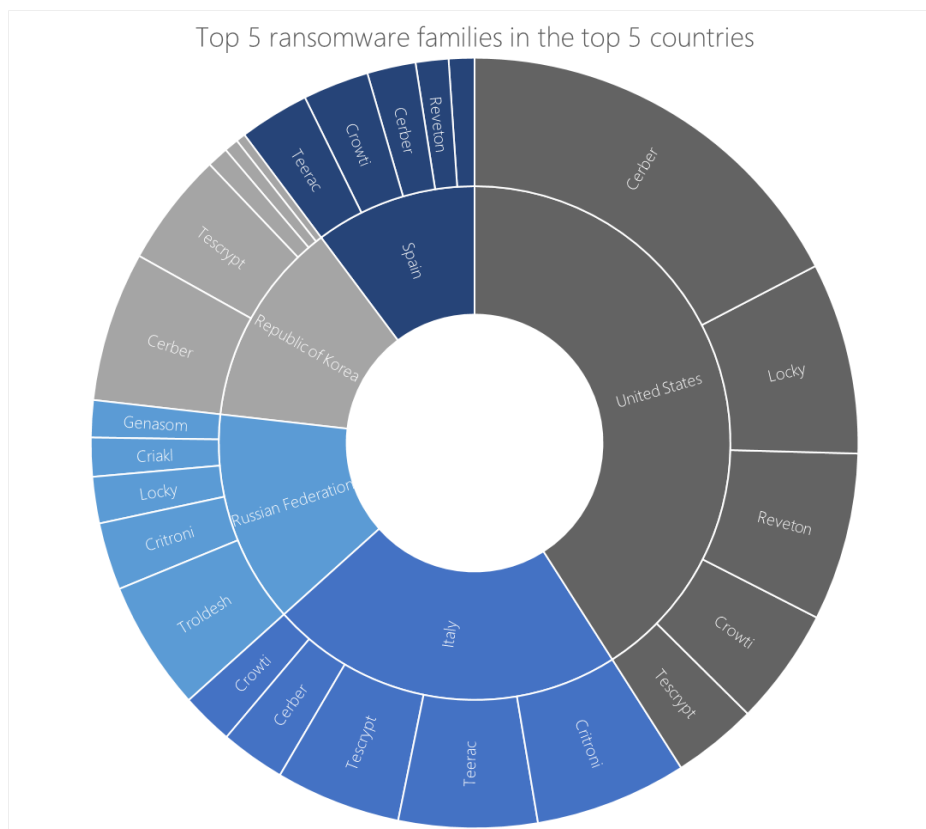
Retrieved from: Rajput (2017). Evolving Threat Agents: Ransomware and their Variants. *International Journal of Computer Applications*, 164(7), 28-34.

Newer generation are now deploying more advanced tactics like using stronger asymmetric encryption standards like AES-256 block ciphers to encrypt victim's data, stronger key generation algorithm and management methods, and also infecting network shares and removable media. These traits have proved effective and therefore it is evident that new ransomware families are advancing them and therefore ransomware should not just be wished away (Hampton, & Baig, 2015).

## **2.6 Common Ransomware**

In 2016, Malware Protection Centre trailed over 200 ransomware variants. More than half of those families were discovered in 2016, this discovery suggested that cybercriminals were actively developing and releasing new ransomware into the cyberspace. Cerber and Locky were observed to be the most common ransomware variants in the year 2016.





*Figure 3: The five common Ransomware variants in the countries*

Retrieved from Microsoft Malware Protection Centre; <https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx>

## 2.7 Future of Ransomware

Alexander Gostev (senior virus analyst) believes that ransomware hackers will have an advantage in future, as these online criminals would use advanced cryptographic algorithms. It is argued that the length of the cryptographic key generated continues to increase, this therefore make reversing of encryption impossible. This was observed in Gpcode ransom that used a 660-bit key. It is also anticipated that ransomware installer could be hidden by newer rootkits. These newewr rootkit are expected to work such that, if the password is broken, it triggers the ransomware to encrypt data randomly again, or after a predefined number of logins attempts are exceeded it destroy even the key making it permanently impossible to get the data again. This

technique if achieved it will hold the victim to total ransom. Nevertheless, there is no such rootkit that have been discovered (Luo & Liang 2007).

## **2.8 How Ransomware Work**

A ransomware attack goes through five stages; the five stages are as described below (Han, Hoe, Wing & Brohi, 2017).

### **Stage 1: Installation**

Ransomware oftenly spread through a phishing email that usually contain have malicious attachment or downloads that internet user might be enticed to make, malware will henceforth be downloaded and installed into the user system. This malware will thereafter spread through the network as they get installed in all computers in the network. Cryptoransomware hide the key in the Windows registry and will be activated every time the computer boot up.

### **Stage 2: Contacting Headquarters**

Ransomware attack is an autonomous attack, after installing into the computer system; it will thereafter contact the central server that is controlled by the malware designer and establish a secure connection. This usually happen before the ransomware can start encrypting the user data.

### **Stage 3: Handshake and keys**

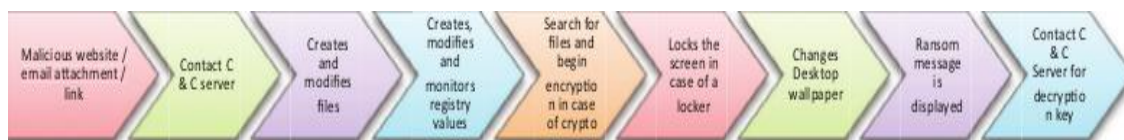
Handshake is the process whereby the ransomware in victim computer and the central server establish a communication link and thereby authenticating each other. Asymmetric key generation algorithm will be used by the central server to generate an asymmetric key used in encrypting the victim's data. Private key is deposited in the central server and the public key is deposited in the victim computer's registry. The cryptographic key that is generated using public key encryption algorithm is deployed in encrypting the victim's computer data and only the private key that is stored in the central server can be used to decrypt this data.

### **Stage 4: Encryption**

The generated cryptographic key will then be used to encrypt files that are saved in the attacked computer.

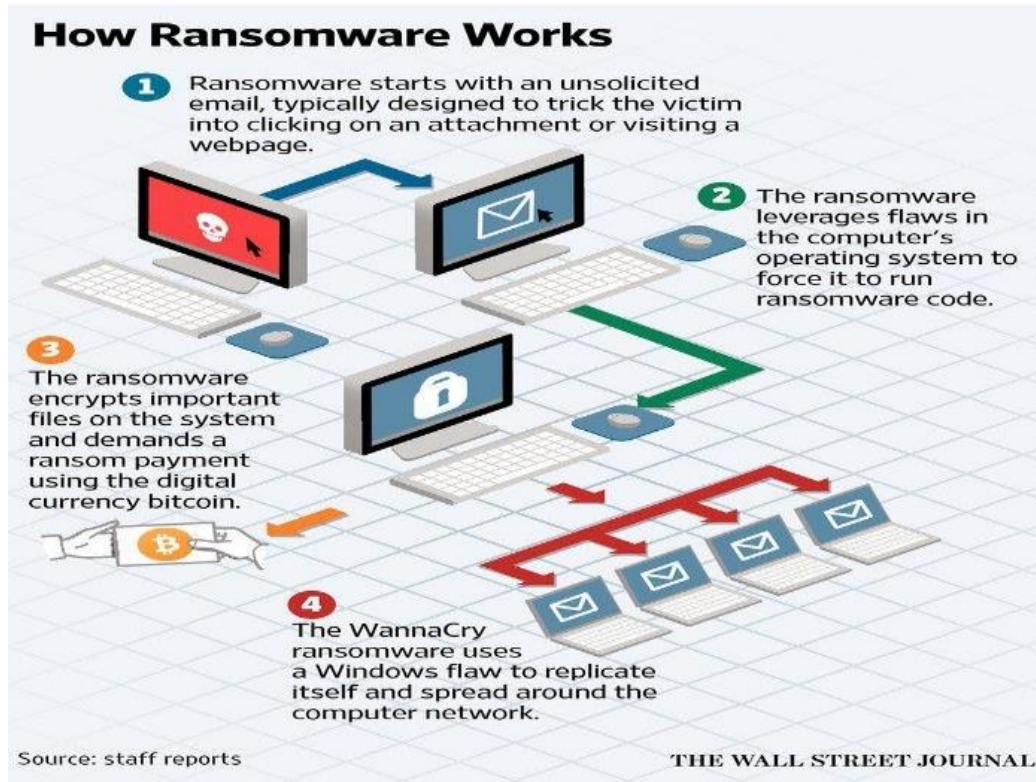
## Stage 5: Extortion

Ransomware note will be displayed on the screen after the files are encrypted; this note usually bears the encryption standards used to decrypt victim's data, victim's personal identification number, time limit within which ransom should be paid or it will double the amount demanded and eventually destroy the decryption key, steps to be followed in paying the ransom, and the ransom amount. This ransom should be paid using untraceable digital currency which have been made possible by the TOR browser.



*Figure 4: Windows based Ransomware life-cycle*

Retrieved from Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization paper.



*Figure 5:How Ransomware works*

Retrieved from International Journal of Advanced Research in Computer Science

## 2.9 Ransomware as a Service

Software as a service is a cloud-computing paradigm, which also include Infrastructure as a service and platform as a service. This paradigm allows third party provider to host their software in the cloud. They can therefore offer their software services to the user who can pay as they use model. Ransomware as a service borrows from this model, there are services in the darknet that offer ransomware as a service by allowing cybercriminal to attack their victims through the help of this model. This model provide for the attacker to pay a certain percentage of ransom to the service provider, which is done in Bitcoin. This model has made it possible for even the novice ransomware user to be able to launch an attack. A security firm Emsisoft found the latest ransomware as a service in 2016, which was named Ransom 32, it is a cross-platform in nature since it is written in NWJS.

## **2.10 Bitcoin**

Bitcoin is a decentralized and an anonymous p2p virtual currency which was invented by an unknown programmers known as Satoshi Nakamoto as a free software in 2009. There is no central reserve for bitcoin which can regulate the issuance and distribution. It is pegged in a rather new technology called Blockchain technology, this technology consist of thousands of nodes which should be updated whenever a single transaction is carried out and all the nodes should keep this history which is publically available (Andronio, Zanero & Maggi 2015). The anonymity of Bitcoin have previously been studied using clustering and flow analysis, neither of the method was able to show a relationship between Bitcoin addresses and their respective IP data. Leveraging anomalous relaying behavior (Koshy, Koshy and McDaniel 2014), they discussed on possible circumstances that Bitcoins could be related to their respective Bitcoin addresses. Bitcoin users are identified by their public-key which every user can be able to generate as many keys as the need could be, this make it very hard for a person seeking to track a Bitcoin user since one will have to map one user to many public key and make sure that the information available of the user match the public keys of the user, this therefore make it difficult to hack into Bitcoin (Reid & Harrigan 2013).

Bitcoin have therefore been used as the means of choice by which cybercriminal utilize in demanding for the ransom. According to Ali, Murthy, & Kohun (2016), TOR browser also create a secure channel that attackers rely upon for communication with their victims also because of the anonymous environment it create. Bitcoin being untraceable makes it the preferred digital currency in darknet and also explain the risk of using it.

## **2.11 Empirical Literature Review**

In an experimental analysis of ransomware that was conducted on window as well as on android platform by Zavarisky, & Lindskog, (2016), they analyzed all variants of ransomware using Cuckoo sandbox and Anubis. They observed that all variants of ransomware introduces new changes in a computer system as it attempt to be installed. The effected changes were observed

in registry, file system activities, where some files were downloaded, other 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.

The recent variants were observed to use both RSA-2048 bit and AES-256 bits encryption for public key and encrypting the victim's files respectively.

Hampton & Baig, (2015) conducted a research where they compared traits of twenty-nine variants of ransomware that were uncovered from December 1989 to July 2015. They observed that over and above them sharing most of the traits, the use of stronger encryption algorithm started in 2013. There was also some more and major improvement in the ransomwares that were uncovered post 2013, they include the use of cryptocurrency (Bitcoin). Bitcoin allow the exchange of digital currency anonymously through the use of TOR network. As shown in Tabl.1 bellow, they were able to show various traits shared among various variants of ransomwares and the use of latest technologies like cryptocurrencies and anonymous hidden networks.

Table 1: Twenty nine variants in nine families of the commonly cited ransomware

Strain	Date	Encrypts	String Cphr	PKI	Autonomy	DGA	HiddenTOR	HiddenI2P	HideClient	SecureEnc	SecureKeys	SecKeyMgmt	ScanNetDry	SecErase	PK DL	DH-ECC	C2 Server	C2 Hidden	PayProcOK	PayProvider	CryptCash	StealCred	StealProc
PC CYBORG	1989-12-19	√			√																		
One Half Virus	1994-10-31	√			√																		
GPCode	2004-12-01	√			√																		
GPCode.ac	2005-06-27	√		o	√					x	x	x									√	√	
GPCode.ad	2006-04-14	√		o	√					x	x	x									√	√	
GPCode.ae	2006-06-02	√		o	√					x	x	x									√	√	
GPCode.af	2006-06-06	√		o	√					x	x	x									√	√	
GPCode.af2	2006-06-06	√	x	o	√					x	x	x									√	√	
GPCode.ag	2006-06-07	√	x	√	√					x	√	x									√	√	
GPCode.ak	2008-06-05	√	x	√	√					o	o	o									√	√	
GPCode.ax	2010-11-20	√	√	√	√					√	√	√							o		√	√	
GPCode.bn	2011-03-26	√	√	√	√					√	√	x							o	o	√	√	
Reveton.2012	2012-04-04				√														o	o	√	√	
Cryptolocker	2013-05-09	√	√	√		o				√	√	√	√		√				o	o	√	√	
Reveton.2013	2013-09-10				√														o	o	√	√	√
Reveton.XY	2013-10-22				√														o	o	√	√	
CryptoLocker 2.0	2013-12-19	√	√	√						√	√	√	√		√				o		√	√	
CryptoDefense	2014-03-26	√	√	√			o			√	√	x							o				
CryptoDefense	2014-04-01	√	√	√			o			√	√	√		o					o				
CryptoWall	2014-06-26	√	√	√						√	√	√		o					o		√	√	
CTB-Locker	2014-07-15	√	√	√	o		o			√	√	√	√	o					o	o	√	√	
Reveton.2014	2014-08-19				√														o	o	√	o	√
CryptoWall 2.0	2014-10-01	√	√	√			o			√	√	√	√	o					o		√	√	
CryptoWall 3.0	2015-01-14	√	√	√				√		√	√	√	√	o					o		√	√	
Reveton.2015	2015-02-05				√														o	√	o	√	√
TeslaCrypt 0.2.5	2015-02-14	√	√				√			√	√	x							x		√	√	
TeslaCrypt 0.4.0	2015-02-14	√	√		o		√			√	√	o	√	√					o		√	√	
TeslaCrypt 2.0.0	2015-07-13	√	√	√	o		√			√	√	o	√	√					√	√	√	√	

Strain	Date	Encrypts	String Cphr	PKI	Autonomy	DGA	HiddenTOR	HiddenI2P	HideClient	SecureEnc	SecureKeys	SecKeyMgmt	ScanNetDry	SecErase	PK DL	DH-ECC	C2 Server	C2 Hidden	PayProcOK	PayProvider	CryptCash	StealCred	StealProc
TeslaCrypt 2.1	2015-09-07	√	√	√	o		√			√	√	√	√	√				√		√			

√ = well implemented; o = not fully implemented; x = implementation broken

Retrieved from Edith Cowan University – Research Online, Ransomware: Emergence of the cyber-extortion menace (conference paper).

According to Andronio, Zanero & Maggi (2015) mobile devices are also prone to ransomware attacks, and since there is little research done on this, most devices rely on traditional mechanisms to protect them from attack. This therefore renders them unsecured as ransomware uses very subtle attack tricks rendering them undetected even by the modern mobile malware detection methods. However, Scaife, Carter, Traynor, & Butler, (2016) noted that, the use of CryptoDrop a detection system that could raise an early-warning whenever there was unusual activity in the file, like interfering with large amounts of file data simultaneously, could be used to protect systems against ransomware attacks. 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 has characteristics that are common to them and therefore an in-depth analysis could yield a system that can minimize the amount of victims' data loss.

Zavarsky, & Lindskog (2016), conducted an experimental analysis of ransomware on Windows as well as on the Android platform; their findings demonstrated that different ransomware variants possess similar behavior even though they rely on different payloads to execute an attack. Detection of ransomware in both Windows and Android however varies, abnormal file system and registry activities are good indicators of an infected Windows system, whereas in the Android environment, detection can be deduced by the type of permission an Android application is requesting.

There is a very small amount of information in regard 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 has been well researched on and hence reliable exploits databases and well peer-reviewed data sources. There is still a gap in malware analysis that can be mitigated by development of a formal methodology of malware analysis which will also include the vocabulary associated with malware analysis (Hampton, & Baig, 2015).

Ransomware has been shown to be of two types based on their mode of execution. There is autonomous ransomware whose destructive activity starts as soon as they are executed without communication with a command and control server (Hampton, & Baig, 2015), other variants



require contacting command and control server before the encryption process start and these may be detected with careful observation of network signatures.

It is argued that, if data is encrypted using a well-implemented encryption algorithm it is impossible to recover the same data. The most recent ransomwares have been observed to rely on a combination of techniques as a means of increasing attack complexity; these techniques are; the use asymmetric key generation algorithm, the use of advanced encryption standards like AES-256 block ciphers, generation of the public key remotely, and contacting command and control server so as to automate the attack. (Hampton, & Baig, 2015). Therefore, it is advisable to use the best possible security standards together with a reliable backup plan as an integral part in achieving safety in the cyberspace. Nevertheless Kasparsky lab in collaboration with National High Tech Crime Unit of the Netherlands police have tried to outsmart Coinvault ransomware by developing possible decryption key and come up with a repository, and programs that can be used by the victims to decrypt their hijacked data. System watcher module is a system that have been developed by Kaspersky Lab, this system work by storing local copies of files that are protected and it is able to restore them hence undoing the changes effected by the cryptomalware.

A research conducted by Symantec in 2015 showed that the growth of wearable and hand held 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. Zavarsky & Lindskog (2016) conducted an experiment where they analyzed ransomware on Windows as well as on Android platform. They analyzed seventeen Windows ransomware families and eight Android ransomwares families, where they compared at least three variants from each family. They observed that different ransomware variants from different families use similar attack techniques though they deploy different payloads; also, they noted that encryption approaches have improved over time significantly. They concluded that active and careful analysis of peculiar file system, registry changes can signal a ransomware attack in Windows, and in-depth analysis of permissions requested by Android applications can signal a ransomware attack in Android.

Takafumi et al (2017), conducted an experimental analysis where they used deep learning method to detect ransomware, in this experimental evaluation they were able to successfully demonstrate that their deep-learning model can detect latest ransomware in high-speed network timely. However due to high reward for ransomware, more and more ransomware families appear making it more difficult to detect them.

There is no guarantee method of ridding your computer of cryptoware aside from paying the ransom, which means that prevention is key, on the side of the client there are several measures that can be used to remain safe;

1. Keeping your anti-virus up to date.
2. Opening email attachment only from those who you trust
3. Turn your user account control setting to always notify so that programs cannot make changes to your computer without telling you first.
4. Backup information using a cloud storage service such as one drive or Google drive.
5. Using open drive or portable operating system to access emails can be useful as well.
6. Companies should appreciate the risk posed by ransomware as a business risk and not a localized problem to ICT.

In another study conducted by Kharraz et al (2015), demonstrated that there is a small number of ransomware families with advanced destructive potential. These malwares use two superficial methods to hijack victim's data; blocking the user from accessing the computer desktop or accessing the victim-stored files and attempting to deny access by encrypting the data. They attest that unlike what it has previously believed it is actually not as complicated to stop advanced ransomware destructive activities. The finding also concluded that a practical defense system could be designed against ever-increasing ransomware victimization by; analyzing file system activities, careful observation of input output request and safeguarding Master File Table in the New Technology File Systems, it is also feasible to be aware of an impending zero-day ransomware attack and hence thwart the threat.

## 2.12 Ransom Payment

Paying ransom encourages future and further attacks as the attack criminals profile one as a soft target, this therefore could explain why law enforcers discourage the ransom payment. However the affected organization have a question to answer as to whether to fail to pay the ransom and loose the whole data, and or obey the authorities advice. The cost of paying the ransom can also affect the companies significantly, also if the given time to pay the ransom lapses the ransom usually doubles making it even more expensive and again companies cannot afford not to be away from the clients for long time. Before an organization come out from this dilemma and make a decision, which is far reaching, this could have a negative impact on the business leading to a huge business decline.

A survey conducted by University of Kent in February 2014, observed that cryptolocker victims agreed to pay the ransom by 40% of the victims agreeing to pay the ransom. It is generally not recommended to pay the ransom as this does not guarantee recovery of encrypted data and it might lead to loss of data and money, better still this act to motivate the cybercriminals.

Due to security of public key encryption, algorithm attackers are laying emphasis on first world countries, as they know they have important information in their systems and they have resources to pay the ransom. According to Symantec telemetry, 91% of the top 12 countries that reported ransomware attack in the past twelve months are all direct or indirect member of G20 organizations. The most affected nations include United States, Japan, United Kingdom, and Italy.

Attackers demand for payment in Bitcoin, this tendency has been necessitated by several factors;

- i. Bitcoin is a digital currency that is not regulated
- ii. Bitcoin does not have a central originator hence making it not easy to track and regulate
- iii. There's no legally acknowledged reserve of Bitcoin that could be relied upon on keeping track of all the transaction or even control the value
- iv. Bitcoin transaction cannot be traced to the issuer or to the beneficiary, this create a layer that keep the perpetrator anonymous, making it a currency of choice in the darknet.

### **2.13 Current Solution to Ransomware Attack**

As FBI Cyber Division Assistant Director James Trainor says, “There’s no one method or tool that will completely protect an organization from a ransomware attack. But contingency and remediation planning is crucial to business recovery and continuity – and these plans should be tested regularly”.

Current mitigations are commercial cleanup utilities implementing a classic signature-based approach like SURFRIGHTS hitman pro.Kiekstart, which is a bootable USB image that uses a live- forensic approach to look for artifacts of known ransomware. Other tools such as Avasts Ransomware removal for Android release the ransomed files by exploiting the naive design of certain families i.e. simplocker to recover the encryption key, which unfortunately is not generated on per -infection basis.

The research community knows very well that such approaches lack of generality. Also they are evidently limited to known samples, easy to evade and ineffective against new variants. From the user’s perspective, signature-based approaches must be constantly updated with new definitions and are rarely effective early.

Some of the recommendations of what you can do if you find yourself a victim of ransomware are as follows:

- i. Restore data from a backup if that data has not been encrypted or deleted by threat actors.
- ii. Attempt to find a decryption key that may exist (many security vendors have been publicly releasing decryption keys for free usage).
- iii. Make a business decision to move forward without the data that was lost.
- iv. Pay the ransom in order to retrieve sensitive data and restore your operational capability.

## 2.14 Conceptual Architecture

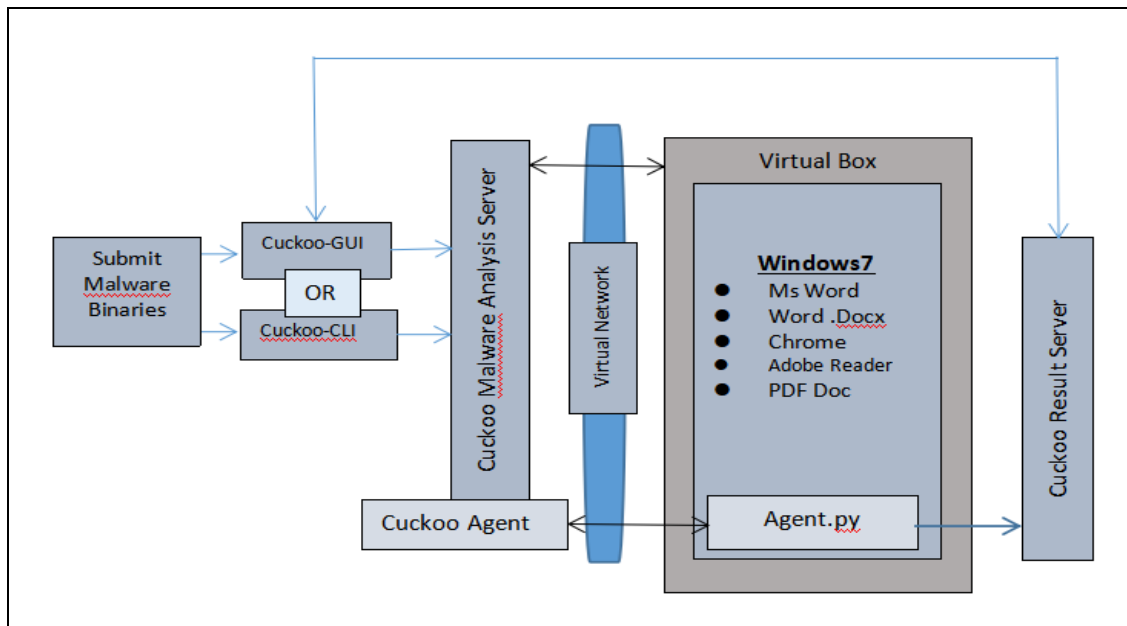


Figure 6: Conceptual Architecture

Source: Author

This conceptual architecture highlights the whole experiment process that was adhered to during the dynamic analysis of ransomware and other malware. Binaries were uploaded in to Cuckoo sandbox using Cuckoo graphical interface. The uploaded binaries will be executed in Windows7, cuckoo malware analysis server analyzes binaries in real time and the results are collected by Cuckoo results server. The collected results were then accessed through Cuckoo graphical interface for the conclusion to be deduced.

### **3. CHAPTER THREE**

#### **RESEARCH METHODOLOGY**

##### **Introduction**

In this section, focus would be on the research method to be used in carrying out the research, this would include the research design, methods of data collection and consideration that would be put into place, and how data would be analyzed and be interpreted to come up with the final report. It would also discuss the target population that would be relied upon in this study.

There are two malware analysis methodologies namely static and dynamic (Nayan zalavadiya, 2017). This study would be based on dynamic malware analysis also known as the analysis of infected file during malware execution. Dynamic analysis consists of execution of live malware and the behavioral features are retrieved for analysis, therefore it is never carried out in a real system and hence system virtualization is employed.

According to (Nayan zalavadiya et al. (2017) there are two basic approaches that are followed during dynamic malware analysis;

- i. Analyzing the dissimilarity between definite points: this is the dynamic analysis whereby malware is run in an isolated environment for a specific period, afterwards the changes are made to system and then the malware is evaluated with respect to the initial system position. The malware behavior report would be formulated in a form of a comparison.
- ii. Observing runtime-behavior: this is the dynamic analysis whereby malware are executed and their activities are monitored during runtime by using a specialized tools or a set of specialized tools.

##### **3.0 Research Design**

Kothari (2004) illustrated research design as the arrangement of conditions for gathering and investigation of data in a way that aspire to merge application to the study rationale with economy in the process. This can be described as the conceptual configuration within which the study is conducted. Kothari (2004) observed that research design is necessary since it facilitates the easy sailing of diverse study processes, and therefore making the study to be a proficient task that yield the maximum needed information while the cost and time needed to conduct the study remaining at minimum.

This study used a mixed research design, experimental and an online survey design to allow the researcher to collect data qualitatively and quantitatively. Due to harmful nature of the specimen that were analyzed which are also actual malicious binary, lab system virtualization was used. The experimental analysis focused on dynamic analysis of ransomware and other malware. The online survey design used tactfully designed questions that were distributed to respondents to help answer research questions.

Cuckoo sandbox, which is an open source automated malware investigation method, was installed in a Linux system. Cuckoo sandbox offer an environment that malware are automatically analyzed and give the results of what the malware does to the cuckoo server. It has the capacity to retrieve the following information; which will further be analyzed as per the objectives of this study to help come up with the conclusion.

- Process calls that were initiated by the malware.
- All files that were created, deleted, and changed by malware during its execution.
- Information that have been dumped into the memory by the malware during execution.
- All traffic activities that were generated during malware analysis and are collected in PCAP format that was later opened using Wireshark for further analysis.
- Screenshots that are taken during the execution of malware were retrieved for comparisons and hence aid in analysis.
- All information dumped into the memory can be retrieved for further analysis.

Passive system monitoring involved execution of the binary and in the background, Cuckoo sandbox collected and recorded all data related to the changes in the virtual system due to the execution of the malware.

Active system monitoring method involved running malware in Cuckoo sandbox to collect real-time data concerning their behavior, and the consequential impact on the infected virtualized machine.

Through the profiling of the malware using Cuckoo sandbox and techniques in this experimental analysis of ransomware and other malware, significant insight into the dependencies, strings, anti-virus signatures, and metadata related to a suspect file was accessed, and consequently utilized to shape a predictive evaluation as to the functionality and nature of the specimen.

A standardized virtual machine was used in this successive experimental study. For each experiment that was carried out to collect behavior of both ransomware and other malware, the virtual machine was reset to the same initial configuration and a new snapshot was taken. Binaries was loaded using web interface and the Cuckoo analysis was given time to collect the conclusion for the result to be accessed again on a web interface. All the analysis were fully automated using Cuckoo sandbox.

### 3.1 Sample Size and Sampling Frame

Sampling techniques refer to strategies utilized by researchers during the sampling process. The procedure is done when the examiner aims to draw conclusions for the general population after carrying out a study on a sample obtained from the same population. Krejcie and Morgan (1970) came up with a reference table that helps determine the sample size for a specific population. Because the target population is finite the Krejcie and Morgan (1970) method was utilized to calculate the sample size for the study.

*Equation 1: Sample Size and Sampling Frame*

$$S = \frac{X^2NP(1-P)}{d^2(N-1) + X^2P(1-P)}$$

Where:

S = the needed sample size.

X<sup>2</sup> = the table value of chi-square for 1 degree of freedom at the preferred confidence level (3.841).

N = the population size.

P = the population proportion (assumed to be .50 since this would offer the greatest sample size).

d = the degree of accuracy expressed as a proportion (.05).

For the best result when determining the sample size, a 95% confidence level is used which result in a risk estimated at 5%. At 95%, our response distribution is 50%.



It is not necessary to use the formula for the known population because the table offers all the provisions necessary to obtain the sample size. The population equal to or more than 1,000,000, the sample size is assumed to be 384.

*Table 2: Getting the sample size of a known population*

<i>Table for Determining Sample Size of a Known Population</i>									
N	S	N	S	N	S	N	S	N	S
10	10	100	80	280	162	800	260	2800	338
15	14	110	86	290	165	850	265	3000	341
20	19	120	92	300	169	900	269	3500	346
25	24	130	97	320	175	950	274	4000	351
30	28	140	103	340	181	1000	278	4500	354
35	32	150	108	360	186	1100	285	5000	357
40	36	160	113	380	191	1200	291	6000	361
45	40	170	118	400	196	1300	297	7000	364
50	44	180	123	420	201	1400	302	8000	367
55	48	190	127	440	205	1500	306	9000	368
60	52	200	132	460	210	1600	310	10000	370
65	56	210	136	480	214	1700	313	15000	375
70	59	220	140	500	217	1800	317	20000	377
75	63	230	144	550	226	1900	320	30000	379
80	66	240	148	600	234	2000	322	40000	380
85	70	250	152	650	242	2200	327	50000	381
90	73	260	155	700	248	2400	331	75000	382
95	76	270	159	750	254	2600	335	1000000	384

*Note: N is Population Size; S is Sample Size* *Source: Krejcie & Morgan, 1970*

### **3.2 Research Instruments**

According to Kothari (2004) and Ranjit Kumar (2011), defining research problem and planning research design paves way for the task of data collection. The researcher should decide the methods that will be used in data collection while also bearing in mind the kind of data to be collected. Kothari (2004) and Ranjit Kumar (2011) have discussed the two types, namely primary and secondary data. Primary data is gathered for the first time by the researcher and it is

considered the original data. On the other hand, the secondary data is the data that have already been gathered by another researcher and analyzed through statistical process.

### **3.3 Questionnaire**

Questionnaire is a list of predetermined questions that are distributed to respondents for them to give their answers, thus providing researcher with data that can be analyzed to answer research questions. An online questionnaire is considered to be the cheapest mode of administering questionnaire though they have a problem as they are associated with a low response rate. When the response is extremely low the collected data will definitely have a low practicability and applicability to the studied population.

This study employed a mixed research design and therefore questionnaires were used for the purpose of the survey research strategy.

### **3.4 Observation**

The observation method is commonly used in studies that related to behavioral science. In essence, people observe things around them, but this kind of observation is not considered scientific. Observation is a scientific tool and data collection technique for the researcher when it is used to formulate the research objective. This means that observation, as a tool of data collection is systematically planned and recorded, and is subjected to controls and checks on reliability and validity. Further, systematic observation allow the researcher to decide in advance the specific series of events that should be observed and utilize a pre-designed schedule to record the duration or frequency of the activities. Hence, the researcher works with a pre-defined observation method. This mainly involves timing or counting, hence creates a generation of quantitative data.

In this experimental analysis, observation of the process information, file system activity, system calls, collected traffic in PCAP format and directory data using the Cuckoo sandbox will help generate data that will be used for analysis and therefore a clear comparison of the feature.

### **3.5 Target population**

The target population was the IT department in various companies, IT was picked as it is the custodian of the organizational IT infrastructure and that they are responsible for maintaining the system security by making sure that all good practices in the use of the IT infrastructure are adhered to. Four variants of each category, ransomware and other malware were analyzed for the purpose of this study. Therefore a total of eight binaries were dynamically analyzed using the cuckoo sandbox and the resulting outcome which is essentially their distinct features was further analyzed to come up with features that will be distinct to ransomware and not to other analyzed malwares.

## **4. CHAPTER FOUR**

### **RESULTS AND DISCUSSIONS**

#### **4.1 Ransomware and other malware execution - Cuckoo sandbox results**

From the research questions that are highlighted in the research design, this study pursued:

To highlight major differences that are as a result of ransomware behavior and other form of malware behavior, these findings were collected from analysis that was carried out using cuckoo sandbox. This formed the major part that involved experiment. For the ease of presentation different features collected that were aimed at helping compare and contrast ransomware and other malware were grouped into various categories. These categories are as discussed below.

#### **4.2 Network Traffic Results and Analysis**

Network traffic was captured during the analysis of the sample ransomware and other malware that were used in this study. Cuckoo sandbox offer capability of downloading the pcap and opening them using various tools like Wireshark, Suricata, Bro, or network miner to help in further analysis of the captured traffic during the malware dynamic analysis.

After the ransomware and other malware were analyzed in cuckoo sandbox, the pcap that was collected was downloaded for further analysis using wireshark. This analysis was aimed at getting an in depth understanding of traffic that is usually generated during the execution of ransomware and other malware. Both ransomware and other malware were observed to dump malicious URL's. Another similarity that was noted during the analysis is that they all have capability to connect to an external host. Ransomware was noted to use this connection to steal browser private information which might include screenshots, password, documents, browser histories and even data stored in two-factor authentication software.

The goal was to check for any similarities and differences there was in the traffic generated. The tables below give the results of captured network traffic and description that from it a conclusion was deduced.

**4.2.1 Network traffic protocols.**

Ransomware and other malware were found to use some common network protocols, ARP, LLMNR, IGMPv3, UDP, NBNS, DNS, ICMP, BROWSER, TCP, all of these protocols are common to both ransomware and other malware, and they are not suspicious protocols as they are also used in other legitimate network traffic. Nevertheless some protocols like NBNS are known to present some vulnerabilities in windows. These network protocols are tabulated in Table.2.

*Table 3: Network traffic protocols*

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield- usb.exe	ZeusVM.exe	Wannacr y.exe	Petrwrap.exe	Satana.m em	TeslaCry pt.exe
ARP, LLMNR, IGMPv3, UDP, SSDP, NBNS, DNS, ICMP, BROWSER, TCP,	ARP, LLMNR, IGMPv3, UDP, ICMP, DNS, SSDP, NBNS, BROWSER TCP, HTTP	ARP, LLMNR, IGMPv3, UDP, DNS, ICMP, NBNS,SS DP, BROWS ER, TCP,	ARP, LLMNR, IGMPv3,U DP, NBNS, DNS, ICMP, SSDP, DNS, BROWSER , TCP,	ARP, LLMNR , IGMPv3 UDP, , UDP, DNS, ICMP, NBNS, SSDP, BROWS ER	ARP, LLMNR, IGMPv3, UDP, UDP, DNS, NBNS, SSDP, BROWSER ,TCP, TLSv1, HTTP,	ARP, LLMNR, IGMPv3, UDP, UDP,DN S, NBNS, SSDP, BROWS ER, TCP.	ARP, LLMNR, IGMPv3, UDP, UDP,DN S, NBNS, SSDP, BROWS ER, TCP.

Fig.7 below shows Network protocol as was captured in the dynamic analysis of Old Trojan Asprox.exe.

No.	Time	Source	Destination	Protocol	Length	Info
45	5.817215	192.168.56.101	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
46	5.817682	192.168.56.101	224.0.0.252	LLMNR	73	Standard query 0x6cda ANY Administrator
47	5.817684	192.168.56.101	224.0.0.252	LLMNR	73	Standard query 0x6cda ANY Administrator
48	5.819387	192.168.56.101	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
49	5.819390	192.168.56.101	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
50	5.824349	PcsCompu_d7:b2:77	Broadcast	ARP	42	Who has 192.168.56.1? Tell 192.168.56.101
51	5.824351	PcsCompu_d7:b2:77	Broadcast	ARP	42	Who has 192.168.56.1? Tell 192.168.56.101
52	5.824358	0a:00:27:00:00:00	PcsCompu_d7:b2:77	ARP	42	192.168.56.1 is at 0a:00:27:00:00:00
53	5.885174	192.168.56.101	192.168.56.255	NBNS	110	Registration NB ADMINISTRATOR<00>
54	5.885177	192.168.56.101	192.168.56.255	NBNS	110	Registration NB ADMINISTRATOR<00>
55	5.885299	192.168.56.101	192.168.56.255	NBNS	110	Registration NB WORKGROUP<00>
56	5.885302	192.168.56.101	192.168.56.255	NBNS	110	Registration NB WORKGROUP<00>
57	5.912447	192.168.56.101	224.0.0.252	LLMNR	73	Standard query 0x6cda ANY Administrator
58	5.912449	192.168.56.101	224.0.0.252	LLMNR	73	Standard query 0x6cda ANY Administrator
59	6.118628	192.168.56.101	224.0.0.252	LLMNR	64	Standard query 0xfa25 A wpad
60	6.118630	192.168.56.101	224.0.0.252	LLMNR	64	Standard query 0xfa25 A wpad
61	6.225648	192.168.56.101	224.0.0.252	LLMNR	64	Standard query 0xfa25 A wpad
62	6.225650	192.168.56.101	224.0.0.252	LLMNR	64	Standard query 0xfa25 A wpad
63	6.303491	192.168.56.101	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
64	6.303495	192.168.56.101	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
65	6.428635	192.168.56.101	192.168.56.255	NBNS	92	Name query NB WPAD<00>
66	6.428640	192.168.56.101	192.168.56.255	NBNS	92	Name query NB WPAD<00>
67	6.631561	192.168.56.101	192.168.56.255	NBNS	110	Registration NB ADMINISTRATOR<00>
68	6.631566	192.168.56.101	192.168.56.255	NBNS	110	Registration NB ADMINISTRATOR<00>
69	6.631651	192.168.56.101	192.168.56.255	NBNS	110	Registration NB WORKGROUP<00>
70	6.631654	192.168.56.101	192.168.56.255	NBNS	110	Registration NB WORKGROUP<00>
71	7.178685	192.168.56.101	192.168.56.255	NBNS	92	Name query NB WPAD<00>
72	7.178690	192.168.56.101	192.168.56.255	NBNS	92	Name query NB WPAD<00>
73	7.355285	192.168.56.101	192.168.56.255	NBNS	110	Registration NB ADMINISTRATOR<20>
74	7.355290	192.168.56.101	192.168.56.255	NBNS	110	Registration NB ADMINISTRATOR<20>
75	7.362575	192.168.56.101	192.168.56.1	DNS	85	Standard query 0xb567 A teredo.ipv6.microsoft.com
76	7.362620	192.168.56.1	192.168.56.101	ICMP	113	Destination unreachable (Port unreachable)
77	7.374399	192.168.56.101	224.0.0.252	LLMNR	66	Standard query 0xc79a A isatap
78	7.374401	192.168.56.101	224.0.0.252	LLMNR	66	Standard query 0xc79a A isatap
79	7.376672	192.168.56.101	192.168.56.1	DNS	85	Standard query 0xeb44 A teredo.ipv6.microsoft.com

Figure 7: Network traffic protocols

#### 4.2.2 NBNS protocol.

NetBIOS name service are protocols that are used in network to communicate a considerable amount of information about the status of the machine, specifically the nature of processes and sessions running at that layer. This protocol can be used by an attacker or a malicious program to query NetBIOS for information that can be used in attacking Windows NT and hosts domain. Both ransomware and other malware were found to have access to Windows command line and therefore they were able to initiate a node status query to discover information about other machine on the network. The screen shot bellow shows NetBIOS protocol as was captured in the dynamic analysis of Old Trojan Asprox.exe.

From the above capture it is evident that the virtual machine on 192.168.56.101 was able to dump it NetBIOS name table which is considered a dangerous response.

#### 4.2.3 LLMNR.

Link-Local Multicast Name Resolution is a protocol based on Domain Name System (DNS) that permits IPv4 and IPv6 hosts to carry out name resolution for hosts on the same local link. Therefore, LLMNR and NetBIOS have the similar application of resolving the host names on the

local network to facilitate communication between hosts on the same local networks. Both protocols are allowed by default on Microsoft Vista machines and above. Ransomware and other malware were found to deploy these protocols to query for the host name which can be used to attack the host and the host domain. For this querying to be possible both NetBIOS and LLMNR should be permitted on the computer of the victim, and the firewall on the victim's device should enable traffic to the computer, both protocols by default utilizes ports UDP 137, UDP 138, TCP 139, TCP 5355, and UDP 5355. Some of the suspicious protocols are highlighted in Table.3.

*Table 4: Suspicious protocols*

<b>Virus</b>				<b>Ransomware</b>			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield- usb.exe	ZeusVM.ex e	Wannacr y.exe	Petrwrap.ex e	Satana.m em	TeslaCry pt.exe
TCP Port 80	TCP Port 80	UDP Port 80	TCP Port 80		TLSv1	TCP Port 80	TCP Port 80

#### ***4.2.4 External host communication.***

Like all other malware analyzed Scofield-usb was found to communicate with an external host but did not suggest contacting command and control server as in the case of ransomware. This was captured as in Fig.8.

Table 5: External Host communication

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield- usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.m em	TeslaCry pt.exe
Yes	Yes	Yes	Yes	Yes		Yes	Yes

Communicates with host for which no DNS query was performed (2 events)	
host	144.76.30.230
host	176.9.17.73

Figure 8: External Host communication

#### 4.2.5 Malicious URLs in process memory dump.

All analyzed Ransomware and other analyzed malware were found to dump a huge number of malicious URLs in the process memory Table.5, Fig.9 shows a number of these URLs which were captured during the dynamic analysis of scofield-usb.



Table 6: Malicious URLs in Process memory dump.

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield- usb.exe	ZeusVM.exe	Wannacry .exe	Petrwrap.ex e	Satana.me m	TeslaCryp t.exe
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Potentially malicious URLs were found in the process memory dump (50 out of 506 events)	
url	<a href="http://www.expedia.com/favicon.ico">http://www.expedia.com/favicon.ico</a>
url	<a href="http://uk.ask.com/favicon.ico">http://uk.ask.com/favicon.ico</a>
url	<a href="http://www.priceminister.com/">http://www.priceminister.com/</a>
url	<a href="http://www.iask.com/favicon.ico">http://www.iask.com/favicon.ico</a>
url	<a href="http://www.merlin.com.pl/favicon.ico">http://www.merlin.com.pl/favicon.ico</a>
url	<a href="http://www.cnet.com/favicon.ico">http://www.cnet.com/favicon.ico</a>
url	<a href="http://search.nifty.com/">http://search.nifty.com/</a>
url	<a href="http://ns.adobe.com/exif/1.0/">http://ns.adobe.com/exif/1.0/</a>
url	<a href="http://schemas.openxmlformats.org/wordprocessingml/2006/main">http://schemas.openxmlformats.org/wordprocessingml/2006/main</a>
url	<a href="http://www.etmall.com.tw/">http://www.etmall.com.tw/</a>
url	<a href="http://search.goo.ne.jp/">http://search.goo.ne.jp/</a>
url	<a href="http://fr.wikipedia.org/favicon.ico">http://fr.wikipedia.org/favicon.ico</a>
url	<a href="http://busca.estadao.com.br/favicon.ico">http://busca.estadao.com.br/favicon.ico</a>

Figure 9: Malicious URLs in Process memory dump.

#### 4.2.6 Private info from internet browser/ locate browser.

According to Etaber, Weir, & Alazab, 2015, financial botnets are threat to banking organizations, these malware deliberately perform financial fraud and steal important information from the client computers. ZueS botnet is an example of these malware. From this study all ransomware were found to steal browser private information while there were no analyzed malware that had the same behavior. This was recorded as shown in Table.6.

*Table 7: Steal private info from internet browser/ Locate browser*

<b>Virus</b>				<b>Ransomware</b>			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield- usb.exe	ZeusVM.ex e	Wannacr y.exe	Petrwrap.ex e	Satana.m em	TeslaCry pt.exe
No	No	No	No	Yes		Yes	Yes

#### **4.2.7 Use of 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 and also to aid in ransom payment as the bitcoin digital wallet of the recipient of the ransom cannot be traced (Ali, Murthy, & Kohun, 2016). Table.7 and Fig.10 shows that the WannaCry ransomware dumped TOR link in the memory to be used to connect to the control and command server through which demand for the ransom is to be made.

*Table 8: Use of Hidden Tor Browser*

<b>Virus</b>				<b>Ransomware</b>			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield- usb.exe	ZeusVM.ex e	Wannacr y.exe	Petrwrap.ex e	Satana.m em	TeslaCry pt.exe
No	No	No	No	Yes		No	Yes

* Found URLs related to Tor in process memory dump (e.g. onion services, Tor2Web, and Ransomware) (1 event)	
url	https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip

Figure 10: Use of Hidden Tor Browser

#### 4.2.8 Contacting Command and control server.

Ransomware and other malware were found to contact C&C server as summarized in Table.8, however, ransomware was seen to contact C&C server using secure protocols, this is a useful process since will facilitate the exchange of the cryptographic key securely. The exchange of cryptographically-generated key is done securely using Transport Layer Security Version-1 protocols. In the dynamic analysis of Petrwrap.exe ransomware, this behavior was captured in the analysis of traffic packets using Wireshark. The exchange of the key is shown in Fig.11.

Table 9: Contacting Command and control server

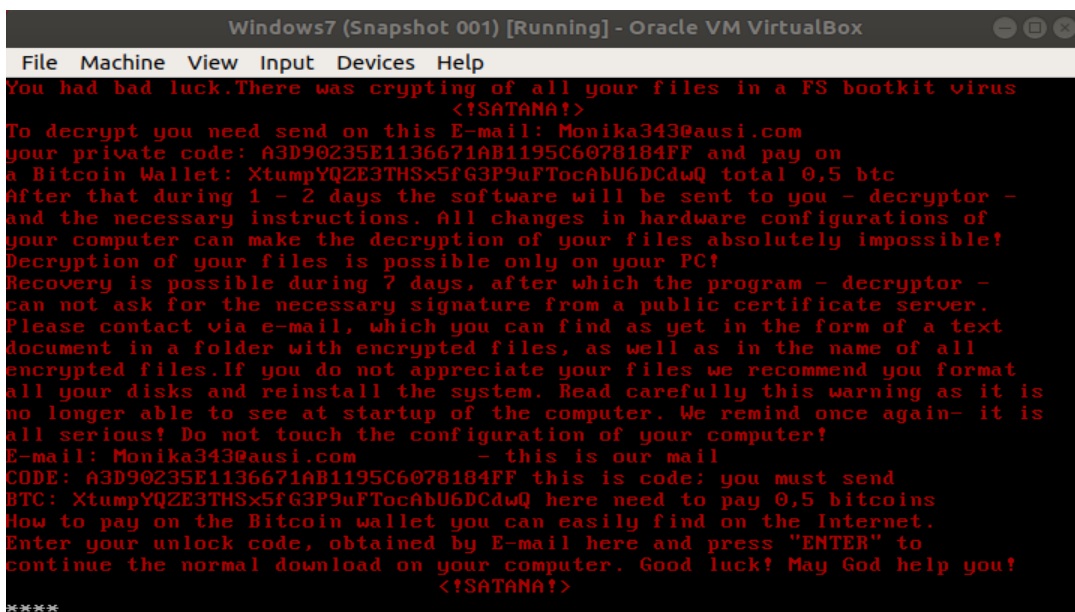
Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.m	TeslaCrypt.exe
Yes	Yes	No	No			No	Yes

No.	Time	Source	Destination	Protocol	Length	Info
170	23.991557	192.168.56.101	40.115.119.185	TLSv1	174	Client Hello
174	24.255366	40.115.119.185	192.168.56.101	TLSv1	1141	Server Hello, Certificate, Server Key Exchange, Server Hello Done
175	24.421221	192.168.56.101	40.115.119.185	TLSv1	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
176	24.750316	40.115.119.185	192.168.56.101	TLSv1	113	Change Cipher Spec, Encrypted Handshake Message

Figure 11: Contacting Command and control server

#### 4.2.9 Locker Ransomware.

There are two types of ransomware namely locker and crypto locker. Locker ransomware work by barring users' computers through stopping them from logging in their computers and thereby exhibiting a message on the screen that give direction on the method to pay ransom for them to regain admission to their computers. During the dynamic analysis of ransomware Satana.mem was found to be a locker ransomware. The Fig.12 shows the message that was displayed on the screen after the binary was executed in the virtual Windows7.



```
Windows7 (Snapshot 001) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
You had bad luck. There was crypting of all your files in a FS bootkit virus
<!SATANA!>
To decrypt you need send on this E-mail: Monika343@ausi.com
your private code: A3D90235E1136671AB1195C6078184FF and pay on
a Bitcoin Wallet: XtumpYQZE3THSx5fG3P9uFTocAbU6DCdwQ total 0,5 btc
After that during 1 - 2 days the software will be sent to you - decryptor -
and the necessary instructions. All changes in hardware configurations of
your computer can make the decryption of your files absolutely impossible!
Decryption of your files is possible only on your PC!
Recovery is possible during 7 days, after which the program - decryptor -
can not ask for the necessary signature from a public certificate server.
Please contact via e-mail, which you can find as yet in the form of a text
document in a folder with encrypted files, as well as in the name of all
encrypted files. If you do not appreciate your files we recommend you format
all your disks and reinstall the system. Read carefully this warning as it is
no longer able to see at startup of the computer. We remind once again- it is
all serious! Do not touch the configuration of your computer!
E-mail: Monika343@ausi.com - this is our mail
CODE: A3D90235E1136671AB1195C6078184FF this is code; you must send
BTC: XtumpYQZE3THSx5fG3P9uFTocAbU6DCdwQ here need to pay 0,5 bitcoins
How to pay on the Bitcoin wallet you can easily find on the Internet.
Enter your unlock code, obtained by E-mail here and press "ENTER" to
continue the normal download on your computer. Good luck! May God help you!
<!SATANA!>
***
```

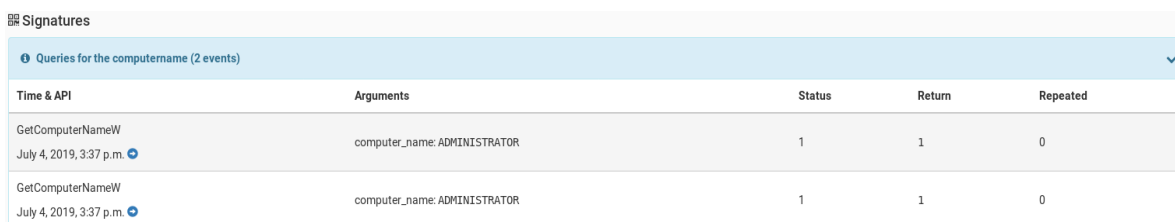
Figure 12: Locker Ransomware note

In this screenshot the victim is advised on the email to send the private code and the digital wallet where ransom should be paid in Bitcoin, the total amount of Bitcoin to be paid, and the amount of time the victim should wait before the decryptor is sent to them and any other instructions to be followed. This ransomware is a slight variation from the other analyzed ransomware, this is because it does not automate C&C server and instead gives an email address that should be used to send the key. However it depicted the usual behavior of other ransomware like writing potential ransom message, moving files which is indicative of ransomware file

encryption process and appending a new file extension which is also a strong indicator of ransomware file encryption process.

#### 4.2.10 Querying computer NetBIOS Name.

Virus was found to query the computer username Fig.13. GetComputerNameW function retrieves the NetBIOS name of the local computer. In the dynamic analysis results of Scofield-usb the return value was 1, this therefore shows that the virus was able to get the computer username (ADMINISTRATOR). The get GetComputerNameW function retrieves the NetBIOS name established at the system startup. This virus therefore will be activated every time the system startup.



Time & API	Arguments	Status	Return	Repeated
GetComputerNameW July 4, 2019, 3:37 p.m.	computer_name: ADMINISTRATOR	1	1	0
GetComputerNameW July 4, 2019, 3:37 p.m.	computer_name: ADMINISTRATOR	1	1	0

Figure 13: Querying computer NetBIOS Name

### 4.3 File Manipulation

Many known ransomware depends on file encryption, the most commonly file extensions that ransomware target include .doc, .docx, .xls, .xlsx, .ppt, .ppts, .pdf, .jpg, .jpeg, .png, .psd, .ai, .txt. Ransomware search for files with these extensions from hard drive and encrypt them. Some of the newer ransomware have been found to encrypt also network shared files making them a potentially dangerous variant for businesses in particular. Ransomware changes file name or path that make the computer and AV softwares overlook suspicious files. Dynamic analysis of ransomware and other malware results noted some few differences on file changes as a result of executing the binaries. Both ransomware and other malware were found to create new files. Ransomware unlike other malware, moved files, created word documents, dropped MIME files and also added file extension to the files committed to the HDD. Appending a new file extension make these files not accessible as there is no program associated with the new file extension that can open them.

### 4.3.1 Creating/ writing new files.

Both ransomware and other Malware create new files in the infected system as summarized in Table.9, during the analysis of ransomware and other malware, cuckoo sandbox captured the files being created in the system. Fig.14 was captured in the results of Scofield-usb.exe and was used to demonstrate this aspect of file being created in the infected system.

Table 10: Creating/ Writing new Files.

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield- usb.exe	ZeusVM.exe	Wannacry .exe	Petrwrap.exe	Satana.me m	TeslaCryp t.exe
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Time & API	Arguments	Status	Return	Repeated
July 4, 2019, 3:37 p.m.	dirpath: C:\Windows	1	10	0
July 4, 2019, 3:37 p.m.	create_disposition: 1 (FILE_OPEN) file_handle: 0x00000098 filepath: C:\Windows\Globalization\Sorting\sortdefault.nls desired_access: 0x80100000 (FILE_READ_ATTRIBUTES SYNCHRONIZE) file_attributes: 128 (FILE_ATTRIBUTE_NORMAL) filepath_j: \??\C:\Windows\Globalization\Sorting\sortdefault.nls create_options: 96 (FILE_NON_DIRECTORY_FILE FILE_SYNCHRONOUS_IO_NONALERT) status_info: 1 (FILE_OPENED) share_access: 1 (FILE_SHARE_READ)	1	0	0

Figure 14: Creating/ Writing new Files.

### 4.3.2 Deleting files.

WannaCry was found to delete a large number of files from the system which is a clear suggestion that it's actually a ransomware, wiper malware or system destruction malware. Fig.15 shows a sample of deleted files at 5174 in this dynamic malware analysis. None of the other malware was observed to depict this behavior, this is summarized in Table.10.

Table 11: Deleting Files

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.mem	TeslaCrypt.exe
No	No	No	No	Yes		Yes	Yes

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\pkjihgncpnkpnbcchdjjeoejaedia\8.2.0\_locales\ru\~SD8254.tmp
file	C:\Users\Symo\AppData\Local\Google\Chrome\User Data\Default\Extensions\felcaaldnbdnccimgdncolpebgiejap\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\pkedcjkdfgpdelpbcmbmeomcjbeemfm\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\anahminkiaainmarkoieifababaf\1.0.0\_locales\ru\~SDFEAD.tmp

Figure 15: Deleting Files

### 4.3.3 Moving files.

During the analysis of WannaCry binary a total of 4849 files were moved indicative of ransomware file encryption process, the appended 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. Fig.16 show the sample results

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\aNlTicnegY.pptx.WNCCRY flags: 2 oldfilepath_r: C:\Users\Administrator\Documents\aNlTicnegY.pptx.WNCCRY newfilepath: C:\Users\Administrator\Documents\aNlTicnegY.pptx.WNCCRY oldfilepath: C:\Users\Administrator\Documents\aNlTicnegY.pptx.WNCCRY	1	1	0	
MoveFileWithProgressW June 29, 2019, 12:45 a.m.	newfilepath_r: C:\Users\Administrator\Documents\aN5CLIKAEFwYELV.doc.WNCCRY flags: 2 oldfilepath_r: C:\Users\Administrator\Documents\aN5CLIKAEFwYELV.doc.WNCCRY newfilepath: C:\Users\Administrator\Documents\aN5CLIKAEFwYELV.doc.WNCCRY oldfilepath: C:\Users\Administrator\Documents\aN5CLIKAEFwYELV.doc.WNCCRY	1	1	0	
MoveFileWithProgressW June 29, 2019, 12:45 a.m.	newfilepath_r: C:\Users\Administrator\Documents\AVDQik0ctqKA.ppt.WNCCRY flags: 2 oldfilepath_r: C:\Users\Administrator\Documents\AVDQik0ctqKA.ppt.WNCCRY newfilepath: C:\Users\Administrator\Documents\AVDQik0ctqKA.ppt.WNCCRY oldfilepath: C:\Users\Administrator\Documents\AVDQik0ctqKA.ppt.WNCCRY	1	1	0	
MoveFileWithProgressW June 29, 2019, 12:45 a.m.	newfilepath_r: C:\Users\Administrator\Documents\BSz05TAznueXHF.rtf.WNCCRY flags: 2 oldfilepath_r: C:\Users\Administrator\Documents\BSz05TAznueXHF.rtf.WNCCRY newfilepath: C:\Users\Administrator\Documents\BSz05TAznueXHF.rtf.WNCCRY oldfilepath: C:\Users\Administrator\Documents\BSz05TAznueXHF.rtf.WNCCRY	1	1	0	
MoveFileWithProgressW June 29, 2019, 12:45 a.m.	newfilepath_r: C:\Users\Administrator\Documents\ByxyLXgJMEV.pptx.WNCCRY flags: 2 oldfilepath_r: C:\Users\Administrator\Documents\ByxyLXgJMEV.pptx.WNCCRY newfilepath: C:\Users\Administrator\Documents\ByxyLXgJMEV.pptx.WNCCRY oldfilepath: C:\Users\Administrator\Documents\ByxyLXgJMEV.pptx.WNCCRY	1	1	0	

Figure 16: Moving Files

### 4.3.4 Adding file extension.

Ransomware is known to append a file extension depending on the infecting ransomware, the new file extension appended to the user files make the files to be inaccessible. Fig.17 shows results captured by Cuckoo sandbox during the analysis of WannaCry ransomware. This screenshot shows a known WannaCry ransomware file extension .WNCCRY. All the files in the infected system with this extension have been encrypted and therefore inaccessible. Table.17 attests that all of the analyzed ransomware appended a new file extension, a behavior that was not observed with all other malwares.



Table 12: Adding file extension

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.mem	TeslaCrypt.exe
No	No	No	No	Yes	Yes	Yes	Yes

Append a known WannaCry ransomware file extension to files that have been encrypted (50 out of 3158 events)

file	C:\Users\Administrator\AppData\Local\Temp\6.WNCRYT
file	C:\Python26\tcl\tcl8.5\msgs\eu_es.msg.WNCRY
file	C:\Python26\Lib\email\test\data\msg_39.txt.WNCRYT
file	C:\Python27\tcl\tcl8.5\msgs\pt_br.msg.WNCRY
file	C:\Python26\tcl\tcl8.5\msgs\ar_jo.msg.WNCRY
file	C:\Python26\tcl\tcl8.5\msgs\eo.msg.WNCRY
file	C:\Python27\include\floatobject.h.WNCRY
file	C:\Python26\include\floatobject.h.WNCRY
file	C:\Users>All Users\Microsoft\User Account Pictures\Default Pictures\usertile39.bmp.WNCRYT
file	C:\Python27\tcl\tk8.5\images\logo100.gif.WNCRY
file	C:\Users\Administrator\AppData\Local\Temp\671.WNCRYT
file	C:\Python26\include\pymacconfig.h.WNCRY
file	C:\Python26\Lib\email\test\data\msg_38.txt.WNCRY
file	C:\Python27\tcl\tcl8.5\msgs\en_au.msg.WNCRY
file	C:\Users\Administrator\AppData\Local\Temp\167.WNCRYT
file	C:\Python27\Lib\email\test\data\msg_23.txt.WNCRYT

Figure 17: Adding file extension

### 4.3.5 Creating Office documents.

During the analysis of both ransomware and other malware, ransomware was found to create office documents, none of the other analyzed malware showed this behavior as summarized in Table.12. Ransomware are known to use stealth tactics in infecting systems, the main goal for the use of Microsoft office document is the utilization of the malicious macros that are implanted in the documents. This make going past installed antivirus and e-mail protection programs happen while they remain undetected.

Table 13: Creating Office documents

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.m	TeslaCrypt.exe
No	No	No	No	Yes		No	Yes

### 4.3.6 Dropping files mime types

Ransomware use a multipurpose internet mail extension to help browser to open the file with the appropriate extension and thereby encrypting the file content and appending the ransomware file extension. This was captured by Cuckoo sandbox during the dynamic analysis of Wannacry behavior. Fig.18 depicts this behavior.

Table 14: Dropping files Mime types

Drops 99 unknown file mime types indicative of ransomware writing encrypted files back to disk (50 out of 99 events)	
file	C:\Users\Administrator\AppData\Local\Temp\45.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\62.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\77.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\79.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\7.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\64.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\73.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\96.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\91.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\20.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\76.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\59.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\66.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\24.WNCRYT
file	C:\Users\Administrator\AppData\Local\Temp\36.WNCRYT

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.m	TeslaCrypt.exe
No	No	No	No	Yes		No	Yes

Figure 18: Dropping files Mime types

#### 4.3.7 Dropping executable files

Several techniques are used by cybercriminals to spread malware payloads, these techniques include using executable files, embedding malicious scripts, and programs that seems legitimate hence obscured from the installed antivirus. In this experimental study, we observed that, both

ransomware and other malware dropped executable files. Cybercriminals have advanced the tricks they use to spread .EXE files in malicious setups, malicious updates to unsuspecting victims and programs loaded with malicious binaries disguised as legitimate programs. The executable files are important in configuring the activities that will be done by malware

*Table 15: Dropping executable Files*

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.m	TeslaCrypt.exe
Yes	Yes	No	Yes	Yes		Yes	Yes

#### **4.4 Registry Manipulation**

Ransomware and other Malware make various changes in the registry that allow them to take control of the system, query regkey, create regkey and even generate cryptographic key.

##### ***4.4.1 Registry changes to make malware take control of the system.***

Ransomware and other malware affect systems by modifying or creating new entries in the system registry as shown in Table.15, which can be regarded as the database for all the operations on the computer system. These program changes are set to run every time the system starts and are designed to make malware have some control over the system and hence introduce new changes.

Table 16: Registry changes to make malware take control of the system

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.m	TeslaCrypt.exe
Yes	Yes	Yes	Yes	Yes		Yes	Yes

#### 4.4.2 Generating cryptographic key.

Ransomware were found to use windows APIs to generate a cryptographic key. Asymmetric key generation algorithm is deployed in generating a secure key meant to encrypt system files. The generated key is shared with C&C server. During the dynamic analysis of WannaCry captured in Fig.19, 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.

Table 17: Generating cryptographic key

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.m	TeslaCrypt.exe
No	No	No	No	Yes	Yes	Yes	

Time & API	Arguments	Status	Return	Repeated
CryptGenKey June 29, 2019, 12:45 a.m.	crypto_handle: 0x00041ff0 algorithm_identifier: 0x00000001 () flags: 134217729 provider_handle: 0x0003f0e0	1	1	0
CryptExportKey June 29, 2019, 12:45 a.m.	buffer: <INVALID_POINTER> crypto_handle: 0x00041ff0 flags: 0 crypto_export_handle: 0x00000000 blob_type: 6	1	1	0
CryptExportKey June 29, 2019, 12:45 a.m.	buffer: RSA2048... crypto_handle: 0x00041ff0 flags: 0 crypto_export_handle: 0x00000000 blob_type: 6	1	1	0
CryptExportKey June 29, 2019, 12:45 a.m.	buffer: RSA2048... crypto_handle: 0x00041ff0 flags: 0 crypto_export_handle: 0x00000000 blob_type: 7	1	1	0

Figure 19: Generating cryptographic key

#### 4.4.3 Querying and opening Regkey.

Ransomware and other malware make changes in the registry as indicated in Table.17 to help them take control of the system, Fig.20 captured in the results of Scofield-usb shows ransomware and other malware querying the system key value and opening it.

Table 18: Querying and opening Regkey

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacr.y.exe	Petrwrap.exe	Satana.mem	TeslaCrypt.exe
Yes	Yes	Yes	Yes			Yes	Yes

Time & API	Arguments	Status	Return	Repeated
NTOpenKey July 4, 2019, 3:37 p.m.	key_handle: 0x00000098 desired_access: 0x00020019 (READ_CONTROL) regkey: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale	1	0	0
NTQueryValueKey July 4, 2019, 3:37 p.m.	key_handle: 0x00000098 key_name: value: reg_type: 0 (REG_NONE) information_class: 1 (KeyValueFullInformation) regkey: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US		3221225524	0
NTOpenKey July 4, 2019, 3:37 p.m.	key_handle: 0x00000098 desired_access: 0x00020019 (READ_CONTROL) regkey: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale	1	0	0
NTQueryValueKey July 4, 2019, 3:37 p.m.	key_handle: 0x00000098 key_name: value: reg_type: 0 (REG_NONE) information_class: 1 (KeyValueFullInformation) regkey: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US		3221225524	0

Figure 20: Querying and opening Regkey

#### 4.4.4 Registry key interactions.

Ransomware makes major changes in the registry including deleting files, moving files, querying value entry for registry key, opening and closing key, and setting data and type of a specified value in the registry key. Fig.21 shows all these changes in the registry that were made by WannaCry ransomware.

Operation	Time	Details	1	0	0
RegCreateKeyExW	June 29, 2019, 12:45 a.m.	regkey_r: Software\WanaCrypt0r base_handle: 0x00000002 key_handle: 0x00000064 class: options: 0 access: 0x02000000 disposition: 0 regkey: HKEY_LOCAL_MACHINE\Software\WanaCrypt0r			
RegSetValueExW	June 29, 2019, 12:45 a.m.	key_handle: 0x00000064 regkey_r: wd reg_type: 1 (REG_SZ) value: C:\Users\Administrator\AppData\Local\Temp regkey: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\WanaCrypt0r\wd	1	0	0
RegCloseKey	June 29, 2019, 12:45 a.m.	key_handle: 0x00000064	1	0	0
NIOpenKey	June 29, 2019, 12:45 a.m.	key_handle: 0x00000064 desired_access: 0x00000001 (0) regkey: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WRR	1	0	0
NIQueryValueKey	June 29, 2019, 12:45 a.m.	key_handle: 0x00000064 key_name: value: 1 reg_type: 4 (REG_DWORD) information_class: 2 (KeyValuePartialInformation) regkey: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WRR\Disable	1	0	0
RegOpenKeyExW	June 29, 2019, 12:45 a.m.	regkey_r: System\CurrentControlSet\Control\LSA\AccessProviders base_handle: 0x00000002 key_handle: 0x00000098 options: 0 access: 0x00020019 regkey: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\AccessProviders	1	0	0
RegOpenValueExW		key_handle: 0x00000098			

Figure 21: Registry key interactions

#### 4.4.5 Terminating processes.

During the analysis of ransomware and other malware in Cuckoo sandbox, most of the selected ransomware were found to terminate processes while none of the virus showed this behavior Table.19. Careful observation of processes using processes monitor and or task manager can give an indication of ransomware attack whenever there are various processes being terminated without user input.

Table 19: Terminating processes

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.m	TeslaCrypt.exe
No	No	No	No	Yes	Yes	No	Yes

#### 4.4.6 Encrypting data / Lock screen

The results of dynamically analyzing the ransomware and other malware showed that, ransomware either encrypt data or lock screen depending on the type of the ransomware, this behavior was not reported with other malware Table.19. Ransomware target a list of file extensions, which are majorly associated with database application, productivity, compressed archives, and multimedia file format. Whenever a ransomware encounter a file of interest, it first gain access to the file by opening it, read the content, use the generated key to encrypt the data in memory and transfer it to the malware working directory. The transferred file will bear the name which is a random number with a new file extension such that (<random number>.WNCRYT) hence changing the file format. The names of encrypted files are reverted to their original names but still appended a new file extension like .WNCRY and moved back to the original directory. The taskdl.exe is known to be launched by ransomware and periodically act to delete the remaining WINCRYT temporary files.



Table 20: Encrypting data / Lock screen

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.em	TeslaCrypt.exe
No	No	No	No	Yes		Yes	Yes

#### 4.4.7 Use of windows utility.

According to Hampton, Baig & Zeadally (2018), ransomware activities follow a particular pattern of behavior, these pattern include file identification, encryption of files, communication between infected system with the central server and the use of anonymizing network. The optimal way to scan and encrypt files is with system level calls facilitated by the Windows API's. The use of the Windows API by ransomware as shown in Table.20 simplify the work of a cyber-criminals since they are able to focus on the logic of developing ransomware code and thereafter use the pre-defined procedures to accomplish their attack process.

Table 21: Use of windows utility

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.em	TeslaCrypt.exe
				Yes		Yes	Yes

#### 4.4.8 Writing messages.

Ransomware write messages on the screen notifying the victim that data has been encrypted and therefore ransom should be paid to give access to the decryption key. This behavior was noted with ransomware and not with any of the analyzed computer virus, this difference between virus and ransomware is shown in Table.21.

Table 22: Writing messages

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.m	TeslaCrypt.exe
No	No	No		Yes		Yes	Yes

#### 4.4.9 Creating new/ injecting suspicious process.

During the analysis of selected ransomware and other malware, various processes were created in both ransomware and other malware as shown in Table.22 which carried out various tasks in the virtualized system registry and files, these created processes are executable. Icacls.exe, which is a command line utility, used to change Windows7 permissions in the New Technology File System. The Windows operating system file, Attrib.exe, located in the C:\Windows\System32 folder, gives privileges to alter or delete file attributes whereby files can be made read-only, archive system and or hidden. This process allows the WannaCry to change the file attributes by appending its files extension.

Table 23: Creating new/ injecting suspicious Process

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.m	TeslaCrypt.exe
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

**4.4.10 Anti-virtualization.**

Cyber-criminal has developed ransomware and other malware that have capability of detecting virtualization environment. This behavior makes it possible for all forms of malware not to execute as otherwise would have executed in an actual system. This behavior was stated in this study as one of the limitation. The antivirtualization behavior by both ransomware and other malware has been tabulated in Table.23.

Table 24: Anti-virtualization

Virus				Ransomware			
Older Trojan Asprox.exe	New Trojan Asprox.exe	Scofield-usb.exe	ZeusVM.exe	Wannacry.exe	Petrwrap.exe	Satana.m	TeslaCrypt.exe
No	Yes	No	Yes			Yes	Yes

## 4.5 Questionnaire Results and Discussions

From the research questions that are highlighted in the research design, this study pursued:

To analyze the data collected through questionnaires that were administered to IT professionals that practice in different industries, these questionnaires were majorly meant to collect data that was to inform on the prevalence of ransomware and other malware in Kenya. The administered questionnaire helped the researcher to focus on comparing ransomware and Virus, since virus ware found to be the malware that had infected majority of the respondents.

### 4.5.1 Ransomware threat

The researcher sought to establish whether various IT professional that participated in data collection have ever experienced a ransomware attack. The results of the findings is represented bellow in a bar graph. From 61 respondents 33 reported to have had a ransomware attack.

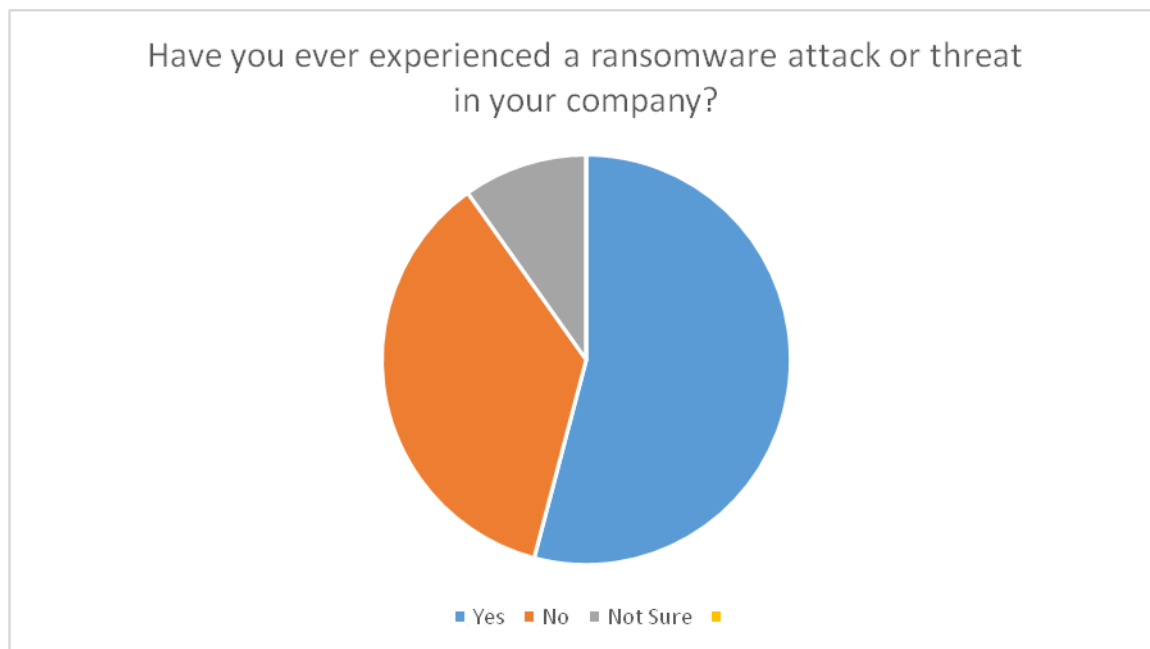


Figure 22: Have you ever encountered a ransomware attack or threat in your company?

### 4.5.2 Ransomware attack mitigations.

There are various ways of mitigating against a malware attack, the researcher sought to know the varied ways that the respondents used to mitigate on the attack. From the data collected from the

61 respondents, 17 of the respondents said they recovered data from an off-site backup, 10 of the respondents said to have formatted all the devices that were infected, only 2 of the respondents resulted to paying the ransom. This data was summarized in a bar graph as shown below

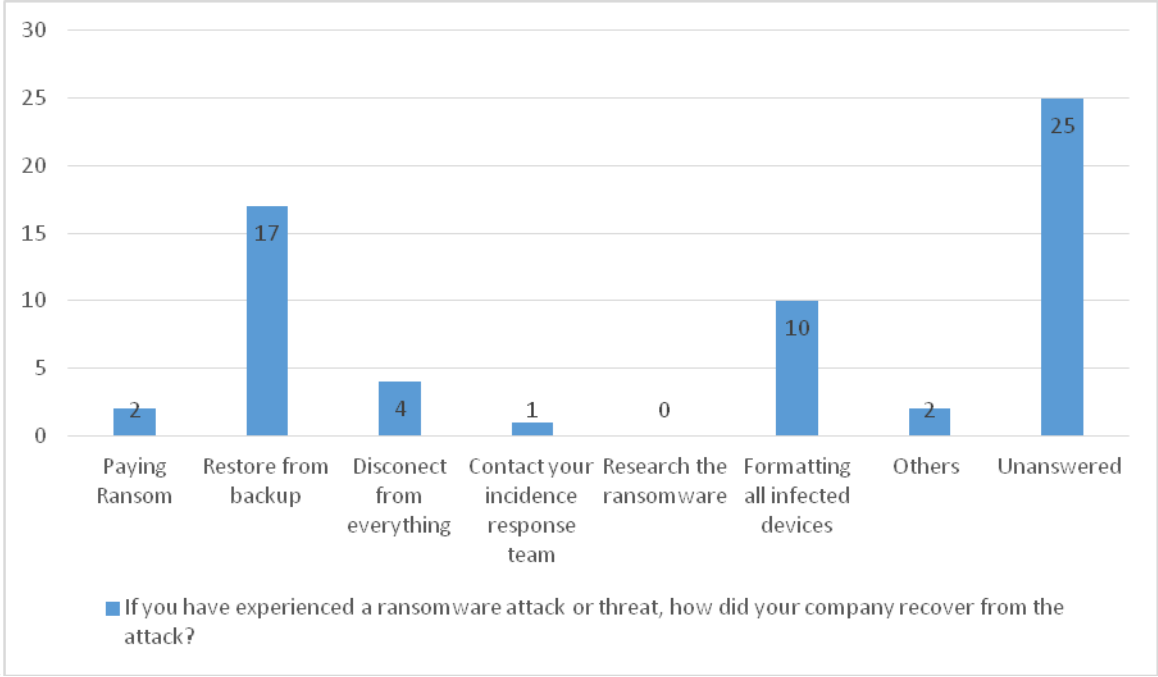
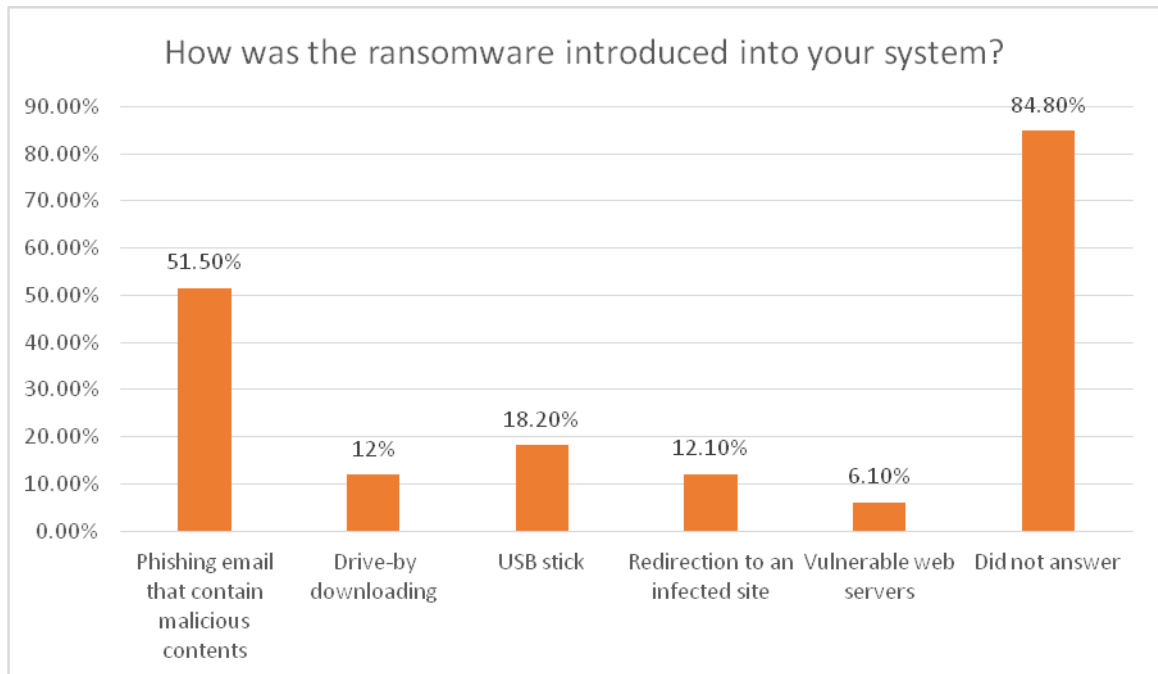


Figure 23: If you have ever experienced a ransomware attack or threat, how did your company recover from the attack?

**4.5.3 Ransomware distribution**

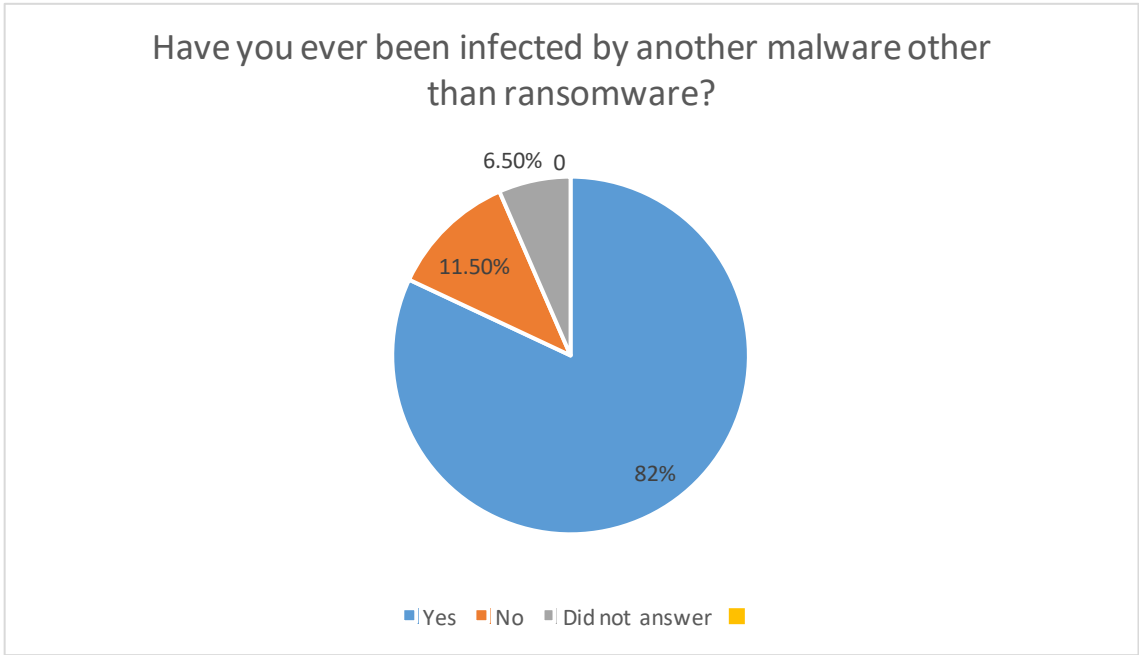
Malware can be introduced in a system using various means. The researcher was interested in knowing the common means of malware introduction into system. Whereas only 33 of the total respondents answered this question since they are the one who has reported an attack or ransomware threat, 51.5% associated their attack or threat to a phishing email that contained malicious attachment, USB stick was reported by 18.2% of the respondents as the source of discovered ransomware, and only 12.1% of respondents reported drive-by downloading and redirection to an infected site as the source of ransomware previously infected their systems. The results of this data was presented in a bar graph as shown below.



*Figure 24: How was the ransomware introduced into your system?*

#### **4.5.4 Other types of malware that are not ransomware.**

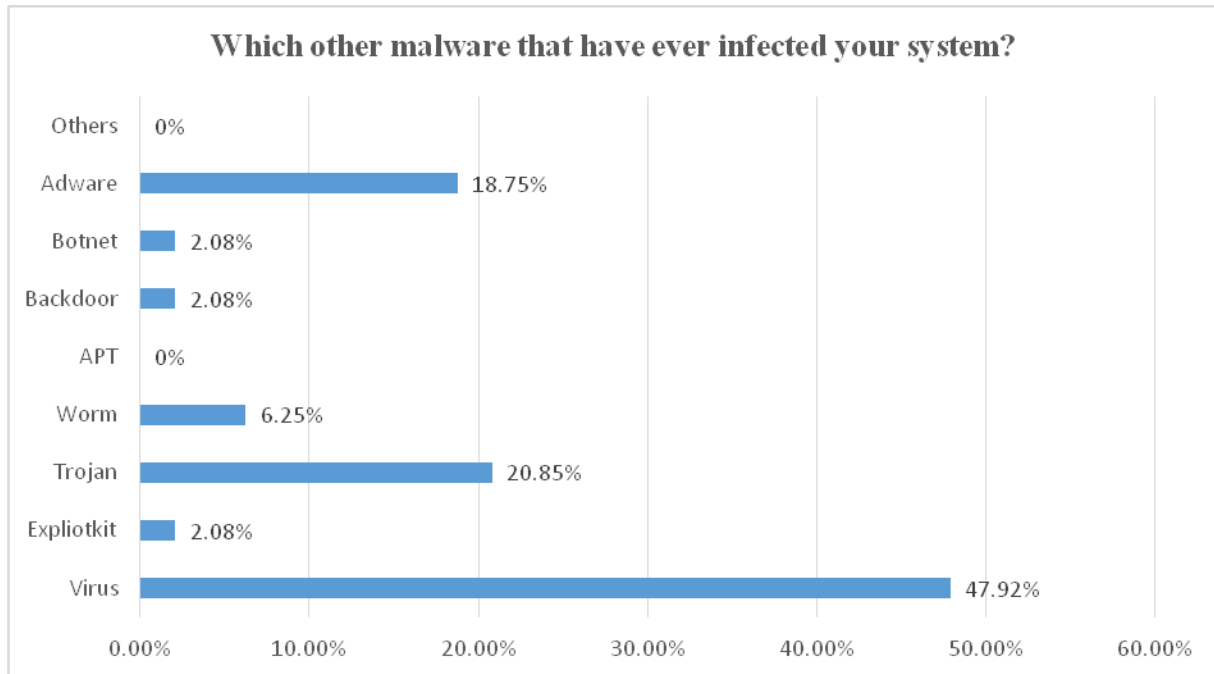
There are various types of malware that are programmed to infect a computer system, therefore, researcher sought to know whether the respondents have ever been infected by other types of malware. From 61 respondents that participated in the survey, 82% of the respondents said to have been infected by virus previously, 11% of the respondents said they have never been infected by other types of malware other than ransomware and only 7% of the respondents said they were not sure.



*Figure 25: Have you ever been infected by another malware other than ransomware?*

**4.5.5 Types of malware other than ransomware.**

Various types of malware have been found in the wild, For the researcher to be able to narrow down on the most common malware that was to be used for comparison with the ransomware, he sought to establish the most common malware that had infected respondents previously. Viruses were found to have infected most of the respondents as 47.92% reported to have been previously infected by virus. Therefore, the researcher focused on comparing ransomware and viruses in this experimental study. The result of this finding was presented in a bar graph as shown below.

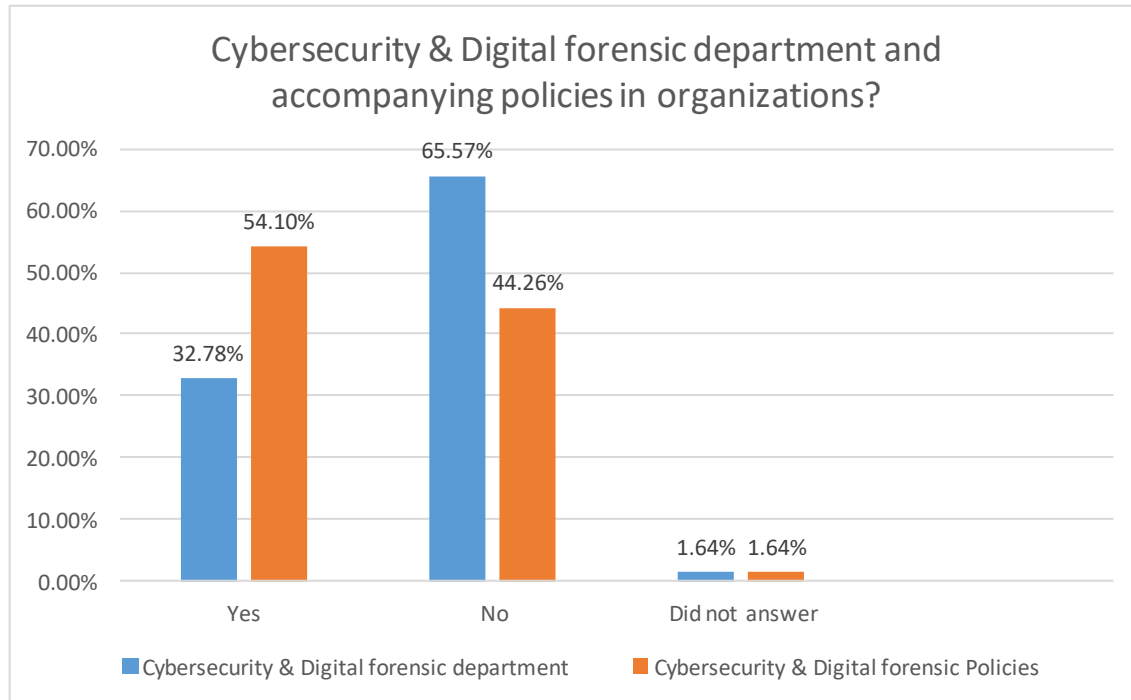


*Figure 26: Which other malware that have ever infected your system?*

#### ***4.5.6 Cybersecurity & Digital Forensic Department And Accompanying Policies In Organizations?***

For the purpose of establishing how various organizations are prepared in securing their data against any form of cyber threat, the researcher pursued to establish whether various organizations have cyber security policies and computer forensics and cyber security departments. From 61 respondents, 33 said yes they have cyber security policies in place, 27 respondents said no and only 1 was not sure. Researcher also established that, from the 61 respondents only 20 said they have a computer forensic and cyber security department, 40 said they do not have and only one was not sure. These findings were presented in a bar graph as shown below.





*Figure 27: Cybersecurity & Digital forensic department and accompanying policies in organizations?*

#### **4.6 Ransomware and Other Malware Look Up In Virus Total Results**

According to Ali, Murthy, & Kohun, (2016), 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. The sampled ransomware and other malware were all submitted to Virus Total which is a website that puts together many AV 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 AV may have missed or to verify any False positive that might have been realized. Cuckoo sandbox is used in Virus Total for dynamic analysis. According to Ali, Murthy, & Kohun, (2016) 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.

The binaries used in this dynamic analysis were all uploaded to the Virus Total with the sole purpose of comparing the detection rate of both ransomware and other malware by the aggregate Av in the Virus Total. The finding of the detection rate are as tabulated bellow;

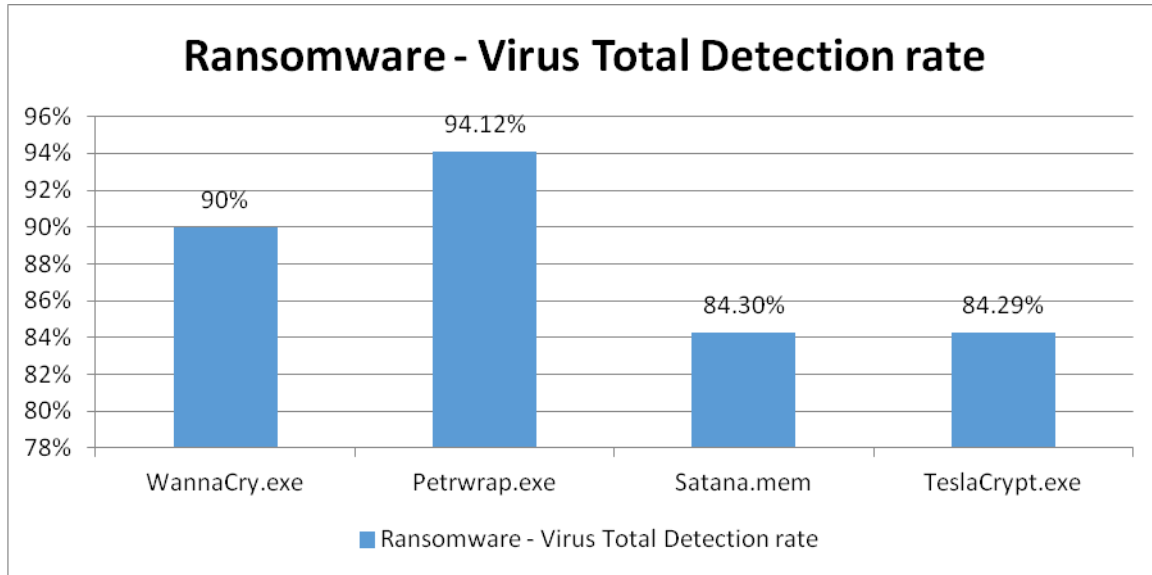


Figure 28: Ransomware and other malware look up in Virus total detection rate

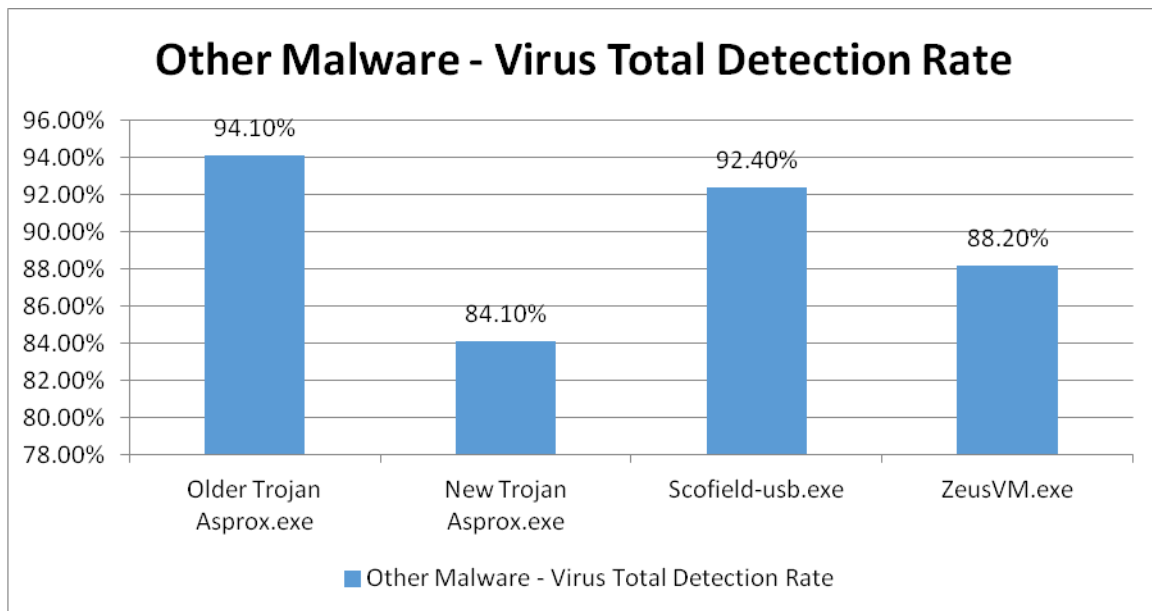


Figure 29: Ransomware and other malware look up in Virus total detection rate

## 5. CHAPTER FIVE

### CONCLUSION AND RECOMENDATION

Ransomware unlike other malware was seen to download Windows API's to be utilized in generating cryptographic key, after encrypting the user data the ransomware then export the key to C&C server, the private key will be supplied only after the ransom has been paid. Data encryption is a resource intensive activity, careful observation of heightened computational power demand above usually normal can signal a ransomware attack, and therefore you can be able to catch ransomware mid-encryption. However, encryption happen in the background and therefore necessitating a system that can be able to monitor system activities in real time like performance monitor in Windows operating system and notify the user of any changes in CPU usage.

Ransomware contact command and control server using secure protocols, TLSv1. This communication facilitates the exchange of generated cryptographic key in the registry between the infected host and command and control server. Private Key is retained in the server and the public key is stored in the infected host. After ransom has been paid the server will automatically send the decryption key that will be used to decrypt the encrypted data.

Dynamic analysis of Ransomware and other malware showed that; Both ransomware and malware rely on NetBIOS, which is an obsolete protocols and LLNMR protocols to resolve host name which help in facilitating communication between hosts on the same network. These protocols are used by ransomware and other malware because of the inherent trust the target computer respond to the attacker with a hashed network credentials and thereby authenticating into it. Both protocols uses port UDP 137, UDP 138, TCP 137, TCP 5355 & UDP 5355 by default.

Ransomware was found to either rely on either downloading Tor network that is meant to enable anonymous communication between the host and the command and control server, or using secure protocols like TLSv1 to share the generated cryptographic key in the registry.

Ransomware has spread throughout the world, from the analysis of data collected using the questionnaire, different companies in Kenya has also been affected by ransomware. 54.1% of the sampled population reported to have experienced ransomware attack or threat in their companies and only 36.1% reported as not having any ransomware attack or threat in their companies. Other forms of malware were also reported to have affected most of the companies, 82% of the sampled population reported to have been affected by other forms of malware. Restoring data from the backup was the most common method for safeguarding business continuity as 82% of the respondents reported to have relied on data backup, only 3.28% of the sampled population reported to have paid ransom to recover their data.

Ransomware was found to download Windows API's which in turn are used to generate cryptographic key, the generated key is then shared with C&C sever in an encrypted message on a secure network. Machine learning algorithm can be used to trace pattern of API's calls which can be analyzed by comparing with the known malware databases, this can help in classification of ransomware pattern of API calls and thereby be deployed to raise an alarm whenever such pattern is matched. Monitoring windows download API's which are not initiated by the computer user can help signal a ransomware attack and thereby be stopped midway.

Ransomware was found to download Tor network, this is an anonymity network that works by redirecting internet traffic through a relay composed of seven thousand servers worldwide and hence concealing the source of the traffic. Careful observation of network traffic geared toward checking for any possible Tor network download can signal an impending ransomware attack and thereby stopping it midway. This can also be achieved by flagging any communication between the host and the torproject.org.

Ransomware was found to delete and move files in large volumes, this was not realized during the analysis of other malware, appending a new file extension was also a factor that was only observed during the dynamic analysis of ransomware. These two activities contribute to the heightened demand for the computer resources. Careful observation of file movement and change of files extension in large volumes can signal a ransomware attack and thereby stopping an attack before the data is encrypted.

There are various AV that are in the market that are used to safeguard the user's systems. Analysis of sampled ransomware and other malware results after they were submitted to Virus Total showed that the conventional AV's aggregated in the Virus Total could detect Ransomware and categorize it as a malicious program. Ransomware were reported to score an average detection rate of 89.5% against other malware that reported 89.7% detection rate.

Literature has reviewed different methods that can be used as best practice that can be used to secure systems against ransomware and other malware attack.

The research project sought to obtain results that determined the distinctive features of ransomware that were not the same with other form of malware that affect computer system, this was done by using Cuckoo sandbox which is an open source automated malware analysis tool and thereby comparing the results. The research also sought to know the prevalence of ransomware and other malware in Kenya, a structured online questionnaire was distributed and respondents were requested to fill the questionnaire from which the collected data was analyzed to give the necessary conclusion.

With the advancement in technology so do the advancement in cyber-attack, ransomware unlike other form of malware have been greatly automated and therefore posing a challenge to cyber security and even to cyber forensic specialist. Therefore being cyber secure and safeguarding a company asset remain to be a very important aspect towards achieving cyber security resilience.

Ransomware was seen to share a lot of traits with other malware, ransomware however, had a common trait that was found to be only associated with ransomware and not other malware, these specific traits form a good basis that can be used to profile ransomware and therefore develop working system that can help get rid of ransomware before an attack occur.

Careful observation of network traffic and unusually high demand for computer resources are a good indicators of a possible ransomware attack. Companies and individuals with critical information should have an offsite backup site, this will help them resume their normal operations within the shortest time possible in case of an attack. Patching AV is a very important factor that can help protect computers from both ransomware and other malware, also keeping all

the computers up to date with the recent security updates and other software updates can greatly help the risk of an attack.

For future research, the recommendation is to develop 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.

## References

1. Symantec Internet Security Threat Report – Trends for July – December 2017. Retrieved 25<sup>th</sup> May 2017, from: [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_exec\\_summary\\_internet\\_security\\_threat\\_report\\_xiii\\_04-2008.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf)
2. <https://en.wikipedia.org/wiki/Malware>
3. Evolution of malware-malware trends. Microsoft security intelligence report. Retrieved 25<sup>th</sup> May 2017, from: [https://www.microsoft.com/security/sir/story/default.aspx#!10year\\_malware](https://www.microsoft.com/security/sir/story/default.aspx#!10year_malware)
4. <http://www.pctools.com/security-news/what-is-antivirus-software/>
5. <https://www.howtogeek.com/125650/htg-explains-how-antivirus-software-works/>
6. Premium Content/E-Handbooks January 2017, retrieved 26<sup>th</sup> May 2017, from [http://www.computerweekly.com/ehandbook/Focus-Securing-for-the-future?Offer=mn\\_ah032717CPWKBANR\\_Welcome-ad\\_Security-EMEA\\_Focus-Securing-for-the-future&utm\\_source=ComputerWeekly&utm\\_medium=AD&utm\\_campaign=HOUSE-Banner-Mar2717&utm\\_content=Welcome-ad\\_Securit](http://www.computerweekly.com/ehandbook/Focus-Securing-for-the-future?Offer=mn_ah032717CPWKBANR_Welcome-ad_Security-EMEA_Focus-Securing-for-the-future&utm_source=ComputerWeekly&utm_medium=AD&utm_campaign=HOUSE-Banner-Mar2717&utm_content=Welcome-ad_Securit)
7. Cloudsec- Little known facts about Ransomware 2016, retrieved 27<sup>th</sup> May 2017, from <https://www.cloudsec.com/2016/08/05/little-known-facts-ransomware/>
8. Wall, D. S. (2015). Dis-organised crime: Towards a distributed model of the organization of cybercrime. *The European Review of Organised Crime*, 2(2).
9. Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.
10. Oates, B. J. (2005). *Researching information systems and computing*. Sage.
11. <https://explorable.com/statistical-sampling-techniques>
12. <https://advisory.ey.com/cybersecurity/should-you-pay-the-ransom>
13. <https://iapp.org/news/a/bitcoins-strategic-place-in-ransomware/>
14. Zavarisky, P., & Lindskog, D. (2016). Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, 94, 465-472.

15. Takafumi, R., Yutaka, I., Pingguo, H., Takanori, M., Hitoshi, O., Yuichiro, T., & Hitoshi, W. (2017). Effect of stabilization control by viscosity in remote robot system. *IEICE Technical Report; IEICE Tech. Rep.*, 117(217), 25-30.
16. Gupta, J. N. (2009). *Handbook of research on information security and assurance*. S. K. Sharma (Ed.). Information Science Reference.
17. Microsoft Malware Protection Centre. Retrieved 23<sup>rd</sup> March 2017, from <https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx>
18. Solanki, N., & Sharma, N. (2019). Malware Analysis: Types & Tools. *International Journal of Engineering Science*, 22664.
19. Ransomware research data summary 2018; Retrieved from <https://go.sentinelone.com/rs/327-mnm87/images/ransomware%20research%20data%20summary%202018.pdf>
20. <https://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service>
21. [https://en.wikipedia.org/wiki/Public-key\\_cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography)
22. <https://www.malwarebytes.com/malware/>
23. Ray, A., & Nath, A. (2016). Introduction to Malware and Malware Analysis: A brief overview. *International Journal*, 4(10).
24. Szor, P. (2005). *The Art of Computer Virus Research and Defense: ART COMP VIRUS RES DEFENSE \_p1*. Pearson Education.
25. Director, T. T., Hawes, J., Director, A. S. T., Grooten, M., Executive, S., Sketchley, A., & Gracey, T. (2013). TARGETED ATTACKS: WHAT'S IN STORE?.
26. Rajput, T. S. (2017). Evolving Threat Agents: Ransomware and their Variants. *International Journal of Computer Applications*, 164(7), 28-34.
27. Andronio, N., Zanero, S., & Maggi, F. (2015, November). Heldroid: Dissecting and detecting mobile ransomware. In *International Symposium on Recent Advances in Intrusion Detection* (pp. 382-404). Springer, Cham.
28. Koshy, P., Koshy, D., & McDaniel, P. (2014, March). An analysis of anonymity in bitcoin using p2p network traffic. In *International Conference on Financial Cryptography and Data Security* (pp. 469-485). Springer, Berlin, Heidelberg.



29. Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks* (pp. 197-223). Springer, New York, NY.
30. Popoola, S. I., Ojewande, S. O., Sweetwilliams, F. O., John, S. N., & Atayero, A. A. (2017). Ransomware: Current Trend, Challenges, and Research Directions.
31. Wanjala, M. Y., & Jacob, N. M. (2018). Review of Viruses and Antivirus patterns. *Global Journal of Computer Science and Technology*.
32. Hampton, N., & Baig, Z. A. (2015). Ransomware: Emergence of the cyber-extortion menace.
33. Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (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.
34. Choi, K. S., Scott, T. M., & LeClair, D. P. (2016). Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. *International Journal of Forensic Science & Pathology*.
35. Nieuwenhuizen, D. (2017). A behavioural-based approach to ransomware detection. *Whitepaper. MWR Labs Whitepaper*.
36. Cabaj, K., Gregorczyk, M., Mazurczyk, W., Nowakowski, P., & Żórawski, P. (2018, August). SDN-based Mitigation of Scanning Attacks for the 5G Internet of Radio Light System. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (p. 49). ACM.
37. <https://www.zdnet.com/article/ransomware-attack-how-a-nuisance-became-a-global-threat/>
38. O'Murchu, L., & Gutierrez, F. P. (2015). The evolution of the fileless click-fraud malware Poweliks. *Symantec Corp*.
39. [https://en.wikipedia.org/wiki/Microsoft\\_CryptoAPI](https://en.wikipedia.org/wiki/Microsoft_CryptoAPI)
40. Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5).
41. <https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-getcomputernamew>
42. <https://www.solvusoft.com/en/errors/blue-screen-errors/microsoft-corporation/windows-operating-system/bug-check-0x7-invalid-software-interrupt/>

43. <http://www.informit.com/articles/article.aspx?p=130690&seqNum=11>
44. <https://www.crowe.com/cybersecurity-watch/netbios-llmnr-giving-away-credentials>
45. <https://www.comparitech.com/blog/information-security/ransomware-removal-handbook/>
46. Morgan, K. (1970). Sample size determination using Krejcie and Morgan table.
47. Etaher, N., Weir, G. R., & Alazab, M. (2015, August). From zeus to zitmo: Trends in banking malware. In *2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, pp. 1386-1391). IEEE.
48. <https://sensorstechforum.com/popular-windows-file-types-used-malware-2018/>
49. Mbol, F., Robert, J. M., & Sadighian, A. (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.
50. Diffie, W. (1988). The first ten years of public-key cryptography. *Proceedings of the IEEE*, 76(5), 560-577.
51. Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. *Information Systems Security*, 16(4), 195-202.
52. Han, J. W., Hoe, O. J., Wing, J. S., & Brohi, S. N. (2017, December). A Conceptual Security Approach with Awareness Strategy and Implementation Policy to Eliminate Ransomware. In *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence* (pp. 222-226). ACM.
53. Salvi, M. H. U., & Kerkar, M. R. V. (2016). Ransomware: A cyber extortion. *Asian Journal For Convergence In Technology (AJCT)*, 2.
54. Zavorsky, P., & Lindskog, D. (2016). Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, 94, 465-472.
55. Mbol, F., Robert, J. M., & Sadighian, A. (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.
56. Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (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.

**57.**Ali, A., Murthy, R., & Kohun, F. (2016). Recovering from the nightmare of ransomware-how savvy users get hit with viruses and malware: a personal case study. *Issues in Information Systems, 17*(4).

## Appendices

### Appendix1: Questionnaire

1. To find out the prevalence of ransomware and other malware in Kenya.

Questions.

a) Have you ever experienced a ransomware attack?

If Yes

How did you mitigate on the attack

- Paying Ransom
- Recovering data from an off-site backup
- Discarding the whole data and formatting the system.

2. have you ever been infected by another malware other than ransomware.

■ YES

■ NO

if YES

➤ Which one

➤ How did you mitigate on the attack?

- Recovering data from an off-site backup
- Scanning and cleaning using antivirus
- Discarding the whole data and formatting the system
- Ignoring

3. How was the malware introduced into your system

- Download from the internet disguised as a legitimate file attachment
- infected USB-stick
- Clicking on an infected Link

4. Do you have a computer forensic and Cybersecurity department in your organization.

5. Which malware analysis tool do you use in your organization if any, either open source or proprietary source.

6. Do you have a Cybersecurity policy in your organization.

## Appendix 2: Questionnaire Responses

QUESTIONS	RESPONSE RATE	
1 Have you ever experienced a ransomware attack or threat in your company?	YES	33
	NO	22
	NOT SURE	6
2 if your answer is YES in Q1 above : How did your company recover from the attack?	paying ransom	2
	restore from backup	17
	disconnect from everything	4
	enact your incidence response plan	1
	research the ransomware	0
	formatting all infected devices	10
	other(specify)	2
	answered	25
3 how was the ransomware introduced in to your system	phishing email that contain malicious attachments	17
	Drive-by downloading	4
	USB stick	6
	redirection to an infected site	4
	vulnerable web servers	3
	Did not answer	27
4 have you ever been infected by another malware other than ransomware?	YES	50
	NO	7
	Did not answer	4
5 if your answer in Q4 above is YES: Which one?	virus	23
	exploitkit	1
	trojan	10
	worm	3
	APT	0
	backdoor	1
	botnet	1
	adware	9
other(specify)		
6 do you have a cyber security and digital forensic department in your organization?	YES	20
	NO	40
	DID NOT ANSWER	1
7 do you have a cyber-security policy in your organization?	YES	33
	NO	27
	DID NOT ANSWER	1