جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Analysis of Crypto-Ransomware Using Network Traffic

Otasowie Owolafe*, and Aderonke F. Thompson

The Federal University of Technology Akure, Akure, Nigeria.

Received 24 Nov. 2021; Accepted 12 May. 2022; Available Online 01 June. 2022

Abstract

Ransomware is a form of malware attack that makes use of encryption to make information inaccessible for the motive of gathering a specified amount of payment. Many victims of this attack who couldn't recover their information from backups have been compelled to decide between losing the information or paying the sum requested by the attacker. This research shows some of the various samples of ransomware, the phases of attack, and the chance of recognizing ransomware by the network traffic patterns it generates. Traffic generated from the infected system was considered. Experimental results from the ransomware detection show that some certain ransomware is very noisy and generates noticeable traffic patterns. In light of traffic information gathered from ransomware, conceivable discovery thoughts could be investigated. The result of the analysis shows that some ransomware generates traffic that is different from normal network traffic. Also, the infection of the file server system shows that the length and time vary but after infection the time for the different samples of ransomware to carry out its encryption is constant.

I. Introduction

The enormous and unprecedented increase in computers, the internet, and applications has impacted our lifestyle, and these advancements have introduced several threats as well [10]. An example of these threats often called malware continuously causes harm to cyberspace [10]. These malware are developed to collect sensitive information, access private systems, or interrupt the operations of systems. Thus, cyber security has grown to be a major issue that pulls together many researchers, developers, and security personnel in proffering solutions. Since late when malware first occurred [7], adversaries have developed an improved version that keeps evolving and is capable of inflicting major damages to the system they attack. Viruses, Worms, Trojans, and ransomware are examples of malware types that have achieved wide prevalence in recent years.

Ransomware is a malware type that targets users' documents and related resources, takeover them and makes them impossible to access [1], [9]. It then demands a ransom to be paid by the victim in exchange for the hijacked data. This extortion is imposed by exploiting the victim's fear of losing valuable data, revealing sensitive information, or locking key resources. According to [11], ransomware first occurred in 1989 with a Denial-of-service attack when a Trojan called AIDS was released.

Keywords: Cybersecurity, Crypto-Mix, Crypto-Ransomware, Crypto-Shield, Message Block (SMB2), Network Traffic, Ransomware.

Production and hosting by NAUSS

* Corresponding Author: Otasowie Owolafe

Email: oiyare@futa.edu.ng

doi: 10.26735/JVUJ3498

Furthermore, the monetary benefit is the paramount factor that contributes to increasing the infection rate of ransomware by attracting many adversaries to building new variants of such programs.

Although ransomware can hit any file on the computer, ransomware often target specific file types [5] with the following extension .txt, .doc, .rft, ppt, .cbm, cpp, asm, .db, .db1, .dbx, .cgi, .dsw, .gzip, .zip, jpeg, .key, .mdb, .pgp, .pdf. [8].

The two types of ransomware are the locker and crypto-ransomware. The locker ransomware, as the name implies, locks the computer or device and demands a fee from the user to restore access to it. The locked computers will often be left with partial capabilities, such as only allowing the user to interact with the ransomware and pay the ransom. The other one is the crypto-ransomware that encrypts the victim's files thus making them inaccessible. This type of ransomware is designed to find and encode valuable data stored on the computer, making the data useless unless the user obtains the decryption key. In these two cases, users are forced to pay ransom to have access to the files. Therefore attacked files are useless until a ransom is paid and a decryption key is obtained. This research is aimed at identifying ways samples of crypto-ransomware occur in network traffic while comparing and analyzing some crypto-ransomware's behavior using network traffic technique.

II. Literature Review

Research has been carried out on how to identify and analyze ransomware. Since 1989, several internet security experts, interested scholars, and internet users have conducted relevant research on how this malware can be detected and prevented using different techniques.

[8] provided a comprehensive explanation of ransomware as "a category of malicious software which, when run, disables the functionality of a computer in some way. The ransomware program shows a message that asks for a payment to restore functionality. The malware, in effect, holds the computer ransom. They also explain ransomware when it disables computer functionality and later called it an "extortion racket" but specific information is lacking regarding the ransom paid for holding the computer ransom.

[9] developed an early warning system called CryptoDrop that alerts users of any suspicious file activity by focusing on detecting Ransomware, by-monitoring any change in user data in real-time. CryptoDrop can halt a process that appears to be tampering with a large amount of the user's data.

Automatic test packet generation proposed by [4] highlighted the working of the ATPG techniques for testing and debugging networks. This method generates a minimum number of dummy nodes or test packets to check every link in the network. The research was designed to detect and prevent ransomware by using automatic test packet generation (ATPG). In the system, two things were absorbed one is to prevent ransomware and the second is the detection of the ransomware and to recover the affected file or unblock the access control.

[3] worked on different ransomware, how they can be stopped and how their threat vectors work. It was started in the work that solving one ransomware doesn't solve the next incoming one. The research investigated six different ransomware that spread from 2016 to 2019, the encryption methods, the different threat vectors, infection spreading, and prevention methods. The results show that after the infection of ransomware, it encrypts the data instantaneously on the system.

III. System Design

This section offers a detailed analysis of the procedures and steps involved in carrying out analyzes of the crypto-ransomware samples used:

A. Overview of The Proposed System

The proposed system is designed to identify ransomware by the network traffic patterns it generates. Some experiments that have been carried out have shown that certain ransomware variants are very noisy and do create observable traffic patterns thus, this system takes into consideration the network patterns of this malware. For the ransomware to be generating network traffic, it must be installed or at least start to install. So the focus of the system is on traffic generated after an infection has occurred. Three devices were used to carry out ransomware identification using network traffic, a workstation (as shown in Fig. 1), a server, and a monitoring device (Wireshark).

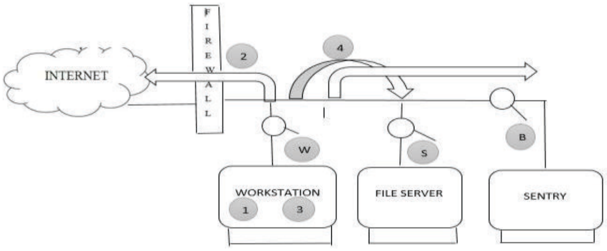

Fig. 1 Proposed System Architecture Adapted from Garvin (2019).

B. Capturing Ransomware Traffic

To have a good knowledge of ransomware traffic, there is need to be sure where to capture the packets is paramount. Once the traffic is captured, then traffic analysis can provide information on ransomware behavior. General network traffic capture is taken into consideration before ransomware traffic capture is performed.

1) Capturing Network Traffic

The proposed system in this research is built using Internet Protocol (IP) on wired ethernet-based networks. On these networks, common packet sniffers or network protocol analyzers include tcpdump, Wireshark, and Tshark. These tools allow for real-time analysis or can save traffic data to disk typically in the pcapng format. Considering the system proposed, packet sniffing was carried out only on a wired network. The simplest case of observing network traffic is on a computer to which login access is available. The analysis performed on captured traffic was done using Wireshark (which allows for efficient and productive traffic analysis).

2) Ransomware Traffic

In other to observe the ransomware traffic generated on a network, the network traffic was captured using Wireshark as depicted in the architecture shown in Fig. 1. To begin with, let's imagine a scenario of a successful phishing attack that resulted in executing ransomware on a workstation. For the ransomware to complete its work, it typically generates some network traffic. The first thing after the installation of ransomware is to contact the command-and-control (C&C) server to get further instructions or an encryption key.

C. Modelling and Simulation Tools

The tools used in carrying out the ransomware identification using network traffic simulation are GNS3, Wireshark, and virtual box.

1) Graphical Network Simulator (Gns3)

A graphical network simulator (GNS3) has the capability of emulating several network devices. GNS3 is an open-source software that simulates complex networks while being as close as possible to the way real networks works. To provide complete and accurate simulations, GNS3 uses the following emulators to run the very same operating systems as in real networks:

1. Dynamips: it is the well-known Cisco IOS emulator.
2. Virtual Box: it runs desktop and server operating systems.
3. Qemu: is a generic open-source machine emulator, it runs Cisco ASA, PIX, and IPS.

2) Wireshark

Wireshark is used for network troubleshooting, analysis, software and communications protocol development, and education. A network packet analyzer will try to capture network packets and display that packet data as detailed as possible. A network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter. Wireshark is cross-platform, using the Qt widget toolkit to implement its user interface, and using pcap to capture packets. Wireshark runs on Linux, MacOS, BSD, Solaris, and Microsoft Windows. Wireshark lets the user put network interface controllers into promiscuous mode so they can see all the traffic visible on that interface.

3) Virtual Box

Virtual box is a type of software that allows more than one operating system on one desktop. Virtual box supports cross-platform guests and hosts including Windows, Linux, Oracle Solaris, and Mac OS X. It is also a general-purpose full virtualizer for x86 hardware.

VI. System Simulation Process

The end product of this phase is a simulation that shows how a ransomware attack is being identified by using network traffic. To achieve the analysis of crypto-ransomware, seven types of crypto ransomware were used. They are revenge, crypto-shield, sage, cyber, crypto-mix, spora, and Locky ransomware. All these ransomware samples were gotten from Malware-Traffic-Analysis.net.

A. Modelling and Simulation Result

A diagrammatic representation of how the topology of the systems and devices used in GNS3 is shown in Fig. 2.

B. The Simulation Processes

The steps involved in the simulation are in the following process:

1. The first activity that was carried out during the course of simulating the identification of ransomware using network traffic was creating different operating systems on the virtual box. On the systems created, the different types of crypto-ransomware were installed. The ransomware samples were gotten from Malware-Traffic-Analysis.net.
2. On one of the systems (file server system), different forms of files were placed. This was done to allow the systems having the ransomware samples on the workstation to access them and also carry out the encryption process on the files.
3. The GNS3 simulator was then started to integrate the virtual box and connect the systems already created on the virtual box machine.
4. The systems and the router were configured by giving each system a distinct IP address. After that, all the devices in the topology were started.
5. Immediately after the devices were started on the GNS3 environment, the virtual box started to bring up the systems installed on it at the same time.
6. Different traffic was captured after the systems went up. On the GNS3 simulator, the sentry device was started (Wireshark). The first traffic that was captured was done before executing the various types of ransomware on the file-server system. The traffic generated was labeled Win Fig. 2.
7. The second traffic (B) was carried out to capture the traffic generated on the file server system immediately after the samples of the ransomware on the workstation gained access to the server and started its encryption.

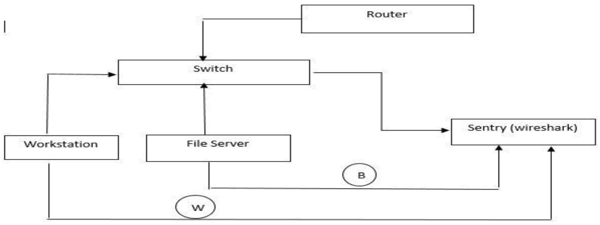

Fig. 2 Diagram Representing System and Device Topology

C. Analyzes of Ransomware Traffic

The analysis will focus on the identification of traffic patterns and not the creation of IDS signatures.

1) Revenge Ransomware Traffic

The filename on the server system changed in the following way:

123.Txt=943F78AB5E5DB16CB5CA73C9240B-01DE.REVENGE

TABLE I
Traffic Generated by Revenge Ransomware

NO	TIME	SOURCE	DESTINATION	PROTOCOL	LENGTH	INFO
58	11.111720	169.254.57.130	169.254.259.62	SMB2	458	Close Request, File: 123.txt
59	11.1112698	169.254.259.62	169.254.57.130	SMB2	450	Create Request, File: 123.txt
60	11.113070	169.254.57.130	169.254.250.62	SMB2	146	Read Request, Len:3 Off:0 File: 123.txt
61	11.113720	169.254.250.62	169.254.57.130	SMB2	182	Close Request, File: 123.txt
62	11.114301	169.254.57.130	169.254.250.62	SMB2	374	Create Request, File: 123.txt

2) Crypto-Shield Ransomware Traffic

The file name on the file server system changed in the following way:

123 = .txt GKG.[R_SP@INDIA.COM].ID[9C7D375B607C01B2].CRYPTOSHIELD.

Table II shows some of the noticeable traffic generated on the file server system by Crypto-Shield ransomware:

TABLE II
Traffic Generated by Crypto-shield Ransomware

NO	TIME	SOURCE	DESTINATION	PROTOCOL	LENGTH	INFO
41	1.792205	169.254.57.130	169.254.250.62	SMB2	138	Create Reques File: 123.txt; SetInfo Request FILE_INFO/SMB 2_FILE_BASIC_INFO
42	1.792579	169.254.250.62	169.254.57.130	SMB2	162	Close Request File: 123.txt
43	1.793079	169.254.57.130	169.254.250.62	SMB2	186	Create Request File: 123.txt
44	1.793470	169.254.250.62	169.254.57.130	SMB2	146	Read Request Len:3 Off:0 File: 123.txt
46	1.794977	169.254.250.62	169.254.57.130	SMB2	374	Close Response

3) Crypto-Mix Ransomware

The filename on the file server system changed in the following way:

123 = .txt ID[9C7D375B607C01B2].RDMK.

Table III shows some of the noticeable traffic generated on the file server system by Crypto-mix ransomware:

TABLE III
Traffic Generated by Crypto-mix Ransomware

NO	TIME	SOURCE	DESTINATION	PROTOCOL	LENGTH	INFO
57	12.395397	169.254.207.95	169.254.250.62	SMB2	110	Create request File: 123.txt
58	12.454162	169.254.250.62	169.254.207.95	SMB2	110	Close request File :123.txt
59	12.457086	169.254.207.95	169.254.250.62	SMB2	110	Create request File: 123.txt
60	12.202649	169.254.250.62	169.254.207.95	SMB2	110	Close request File :123.txt
61	12.203238	169.254.207.95	169.254.250.62	SMB2	110	Create request File: 123.txt

4) CYBER RANSOMWARE

The filename on the file server system changed in the following way:

123 = .txtN-2V7JgmIB.abf4.

Table IV shows some of the noticeable traffic generated on the file server system by Cyber ransomware:

TABLE IV
Traffic Generated by Cyber Ransomware

NO	TIME	SOURCE	DESTINATION	PROTOCOL	LENGTH	INFO
1464	10.862327	169.254.250.62	169.254.207.95	SMB2	42	Create request File: 123.txt
1465	10.865168	169.254.207.95	169.254.250.62	SMB2	42	Close request File :123.txt
1466	10.866163	169.254.250.62	169.254.207.95	SMB2	62	Create request File: 123.txt
1467	10.868077	169.254.207.95	169.254.250.62	SMB2	42	Close request File :123.txt
1468	10.869246	169.254.250.62	169.254.207.95	SMB2	42	Create request File: 123.txt

5) Sage Ransomware

The filename on the file server system changed in the following way:

123 = .txt GKGID[9C7D375B607C01B2].SWF.

Table V shows some of the noticeable traffic generated on the file server system by sageransomw are:

TABLE V
Traffic Generated by Sage Ransomware

NO	TIME	SOURCE	DESTINATION	PROTOCOL	LENGTH	INFO
161	9.057	169.254.250.62	169.254.207.95	SMB2	228	Create request File: 123.txt
162	9.085935	169.254.207.95	169.254.250.62	SMB2	162	Close request File :123.txt
163	9.098424	169.254.250.62	169.254.207.95	SMB2	228	Create request File: 123.txt
164	9.158901	169.254.207.95	169.254.250.62	SMB2	220	Close request File :123.txt
165	9.160866	169.254.250.62	169.254.207.95	SMB2	339	Create request File: 123.txt

Considering the different tables shown, it could be deduced that some ransomware generated traffic that is different from normal network traffic. The first noticeable characteristic of these various forms of ransomware is that they occur on the Server Message Block protocol (SMB2). SMB2 protocol is an application layer protocol that allows for the sharing of folders, printers, and serial ports within a given network. It is the protocol that is commonly used by ransomware on windows operating systems platforms because they are more vulnerable to the attack.

Some ransomware variants were tested that either did not successfully run or only encrypted files and generated no noteworthy network traffic. These included the Locker and Spora ransomware. In these cases, it was concluded that the operating system somehow detected and stopped the infection even though Windows Defender was disabled. Therefore, a time–length graph showing the behaviour of the file-server system before and after the ransomware infections is shown below:

From Fig. 3 and 4, the graph before ransomware infection of the file server system shows that the length and time yvary but on the graph after infection the time for the different samples of ransomware to carry out its encryption is constant. More so, Fig. 5 and 6 show the length and time it takes each ransomware sample to carry out its encryption.

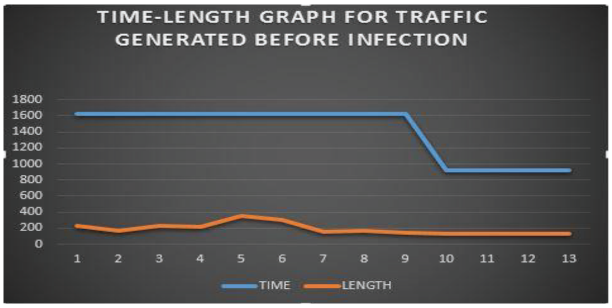

Fig. 3 Graph Showing the Time-length Relationship of File Server System before Ransomware Infection.

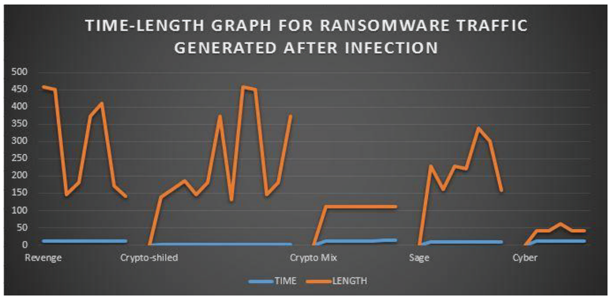

Fig. 4 Graph Showing the Time-length Relationship of file server System after Ransomware Infection.

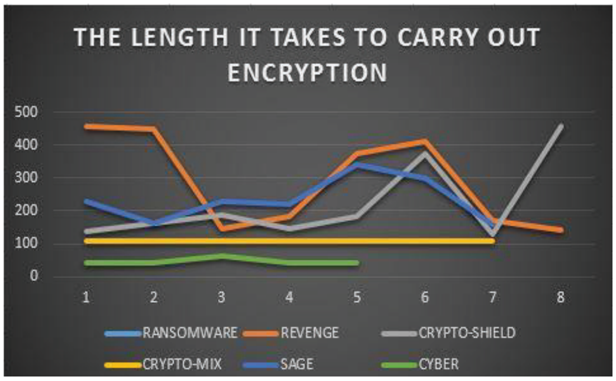

Fig. 5 Graph Showing the Length it takes to carry out encryption on a file server System.

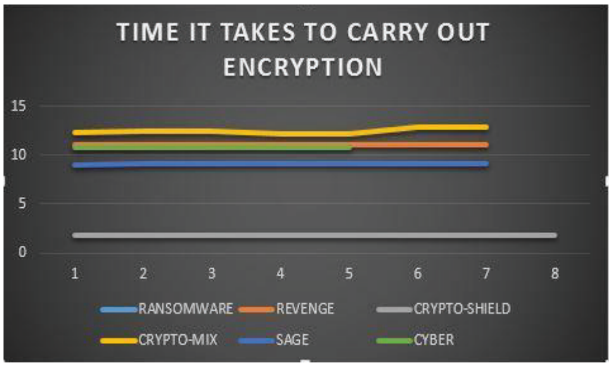

Fig. 6 Graph Showing the Time it takes to carry out encryption on file server System.

From Fig. 6, the time it takes to carry out encryption by the samples of crypto-ransomware is at a constant rate. Comparing this with Fig. 4, we can see that the time plotted also correlates with the one shown in Fig. 6. Hence, it can be concluded that some variants of crypto-ransomware carry out their encryption using constant time.

V. Conclusion

Ransomware has been and will continue to be a serious threat to organizations of all sizes. Improved detection would help system users quickly contain and eradicate ransomware on an infected system. This research access the possibility of ransomware detection by looking for post-install network traffic patterns. This approach unfortunately does not help detect ransomware variants that only attack the local file system. However, identification of ransomware using network traffic could adequately serve as a yardstick for detecting ransomware even though it is not a preventive technique for ransomware.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors declare that they have no conflict of interest.

References

[1] N. Androino, S. Zanero, and F. Maggi, “HELDROID: Dissecting and Detecting Mobile Ransomware,” in *Int. Symp. Recent Adv. Intrusion Detect.*, in Research in Attacks, Intrusions, and Defenses, H. Bos, F. Monrose, and G. Blanc Eds., in Lecture Notes in Computer Science, vol. 9404, 2015, doi: 10.1007/978-3-319-26362-5_18.

[2] G. Hull, H. John, and B. Arief, “Ransomware deployment methods and analysis: views from a predictive model and human responses,” *Crime Sci.*, vol. 8, no. 2, 2019, doi: 10.1186/s40163-019-0097-9.

[3] C. Greinsmark, “Ransomware,” B.S. thesis, Fac. Nat. Sci., Kristianstad Univ., Kristianstad, Sweden, 2020.

[4] H. Chen, J. Su, L. Qiao, Y. Zhang, and Q. Xin, “Malware

Collusion Attack Against Machine Learning-Based Methods: Issues and Countermeasures," in *Int. Conf. Cloud Comput. Secur.*, in Cloud Computing and Security, X. Sun, Z. Pan, and E. Bertino, Eds., in Lecture Notes in Computer Science, vol. 11067, 2018, doi: 10.1007/978-3-030-00018-9_41.

[5] X. Luo and Q. Liao, "Awareness Education as the Key to Ransomware Prevention," *Inf. Syst. Secur.*, vol. 16, no. 4, pp. 195-202, Sept. 19, 2007, doi: 10.1080/10658980701576412.

[6] V. Mathane and P.V. Lakshmi, "Predictive Analysis of Ransomware Attacks using Context-aware AI in IoT Systems," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 4, 2021, doi: 10.14569/IJACSA.2021.0120432.

[7] N. Milosevic, "History of malware," *Digit. Forensics Mag.*, Issue. 16, pp. 58-66, Aug. 2013.

[8] G. O'Gorman and G. McDonald, "Ransomware: A Growing Menace," Symantec Corporation, CA, USA, 2012. [Online].Available: https://www.01net.it/whitepaper_library/Symantec_Ransomware_Growing_Menace.pdf

[9] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," *2016 IEEE 36th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2016, pp. 303-312, doi: 10.1109/ICDCS.2016.46.

[10] L. Xue, and G. Sun, "Design and implementation of a malware detection system based on network behavior," *Secur. Commun. Netw.*, vol. 8, no. 3, pp. 459-470, June 2014, doi: 10.1002/sec.993.

[11] A. L. Young, and M. Yung, "Cryptovirology: the birth, neglect, and explosion of ransomware," *Commun. ACM*, vol. 60, no. 7, pp. 24-26, July 2017, doi: 10.1145/3097347.