Software Reverse Engineering - CSI2107.2

Malware Defence White Paper Ransomware 2.0 behaviour and detection

Name: Marco CAVANI

Student Number: **10570027**

Contents

[Executive Summary 2](#_Toc118403048)

[Behaviour Analysis 2](#_Toc118403049)

[State-of-Art Detection Technique 3](#_Toc118403050)

[**EldeRan Live Detection** 4](#_Toc118403051)

[**RansomWall** 4](#_Toc118403052)

[**RansHunt** 5](#_Toc118403053)

[References: 7](#_Toc118403054)

# Executive Summary

Ransomware malware denies data access until the ransom is paid. Recent ransomware attacks victimised organizations such as Optus and Medibank raising public awareness in our society. New ransomware versions are not only blocking access to the system but duplicating the data allowing criminals to obtain a copy of the information. Data that can be used to blackmail the victims. In recent years, ransomware attacks have caused disruption and money lost to those impacted worldwide. National security should consider the battle against ransomware attacks a crucial point to maintain principles of justice. This document informs readers about the mechanisms behind Ransomware 2.0 and its capability to elude automated detection systems and enhance extortion mechanisms and discusses defensive strategies that can be adapted to mitigate the consequences. This paper outlines the importance of malware analysis and malware detection.

# Behaviour Analysis

Ransomware attacks are designed to lock and encrypt data within a target and in some instances allow criminals to obtain money from the victim who can then regain access to their computer system (Crandall, 2020). The payment request is made using a banner which is displayed on the encrypted computers, often in bitcoin as crypto money is unlikely to be trackable (Crandall, 2020). While the previous versions of the malware focused simply on locking the data and asking for money, ransomware 2.0 creates a hard copy of the data to be realised publicly in case the victim refuses to pay the ransom, exposing the target to a greater threat as those data are often sensitive information(Crandall, 2020). The newest attack techniques are often targeting specific companies and the executable is likely preponderated on the target allowing cybercriminals to conduct literal movements (Crandall, 2020). Ransomware 2.0 can potentially make a greater impact compared to its previous version as it maximises network intrusion and vulnerability exploitation to a grade that involves credential theft, network vulnerability detection, credential escalation and open port identification(Ahmed et al., 2022). This means threat actors are working closer than ever to disarm the exploited system. In fact, the more the victims have exposed to threats the better the chances for criminals of getting the ransom paid off. The criminal business model value data proportionally to money in a way that the more data are involved the greater will be the price for the victims(Bar-Yosef, 2010).

The involution of ransomware 2.0 is influenced by the progress of a new automated intrusion detection system capable of detecting and preventing the spread of the previous version of the virus. Antivirus software could easily detect the ransomware payload and stop further infections within the guarded system. Considering that, the 2.0 version have implemented technologies such as CAPTCHA which allows human interaction and deceive automated systems detection allowing criminals to deal with human and taking advantage of their behavioural mistakes such as clicking or downloading malicious code (Ahmed et al., 2022). The attack vectors define the entry point of the malware. Ransomware 2.0 can infect the system from a malicious website that trigs the user to download the executable into the system or from a malicious email that contains hidden malware(Mates, 2019)

# State-of-Art Detection Technique

Ransomware 2.0 can be prevented by implementing preventative measures and by following good practices related to human behaviours. Considering Ransomware attacks are now making literal movements is recommendable to have conventional security tools such as endpoint detection and response (EDR) that detect unusual activities and map malware activities after the attack. Such tools can provide information to analyse the malware behaviour but, they are inefficient in terms of stopping modern ransomware attacks (Crandall, 2020).

The primary detection of the malware in the early stage of the infection is the key to mitigating the impact of Ransomware 2.0. There are a few techniques to detect ransomware which are based on static and dynamic malware analysis. In dynamic analysis, the malware is executed and observed to define whether the file is malicious or not. Whereas in static analysis suspicious file components such as hashes, strings IP addresses, domains and file headers are analysed. Both static and dynamic analyses are generally performed using virtual machines and sandboxes to prevent any unwanted infection of the actual machine. Sandboxes are a dedicated environment where is possible to perform static and dynamic analysis safely with no risks of contamination (Anand, 2020).

## **EldeRan Live Detection**

EldeRan method allows the early detection of ransomware 2.0 by observing its behaviour which defer from normal software (Fernando et al., 2020). The EldeRan system monitors a sandbox (Cuckoo Sandbox) that defines the analysis of the malware in the following modules: Registry key, directory operation, file system operation, Windows API calls, dropped files and strings of the executable (Fernando et al., 2020). These modules are obtained through dynamic analysis except for strings which are gathered through static analysis (Sgandurra et al., 2016). The EldeRan system is using a machine learning approach for malware analysis to classify ransomware programs in their first stage of installation including unpinned versions of the malware. The Dynamic analysis can detect efficiently common behaviour among the different ransomware families (Sgandurra et al., 2016). The detection rate shown in a recent study almost is above 90% in both common and unpinned ransomware families (Ahmed et al., 2022).

## **RansomWall**

RansomWall is a security system made of five layers of protection against ransomware attacks used for real-time detection, RansomWall is intended for the windows operating system (OP) and uses sandboxes dynamic analysis future to base the behavioural analysis on executable files. Each layer is characterised by a specific functionality (Shaukat and Ribeiro, 2018).

The first layer is characterised by the static analysis engine that provides information extrapolated from the binary code such as strings, hashes, entropy and packed components, headers details, embedded resources etc. This phase is performed before the execution. The second phase is defined by the trap layer which keeps track of any malicious behaviour performed by the program. The third phase is characterised by the dynamic analysis which is used to analyse the behaviour of the program during the execution followed by the file backup phase and the machine learning layers (Shaukat and Ribeiro, 2018). The file backup layer can create a copy of the files manipulated by the malware. During this stage, If the machine learning intelligence classified the file as malicious the processes are killed and the file is repristinated (Shaukat and Ribeiro, 2018). However, this layer is effective on the previous ransomware version but not the 2.0 version (Ahmed et al., 2022). The machine learning layer takes the trap layer and the outcome of both the static and dynamic analysis layers to classify the program as Ransomware or Goodware (Ahmed et al., 2022). This system shows only 1.2% false negatives (Shaukat and Ribeiro, 2018).

## **RansHunt**

RansHunt is a framework used in malware analysis that base its analysis on machine learning principle. In fact, this framework has been designed using 21 different families of ransomware and can identify prevalent characteristics of the malware by combining this information with precision. A recent study has demonstrated a high precision detection rate of 97.1% low false-positive rate of 2.1% (Hasan and Rahman, 2017) proving its efficiency in detecting malware (Hasan and Rahman, 2017). This tool has margins to improve following its nature based on machine learning principles and is considered a promising tool for detecting ransomware 2.0 and future version of the malware (Ahmed et al., 2022). RansHunt shows promising results to detect ransomware which is similar to ransomware 2.0 but with the ability to propagate across the network. These ransomworms are most likely to increase in the future. Once again, the importance of machine learning in malware analysis to discover present and future ransomware families has remarkably found its place in tools like RansHunt which most likely be used in the future to discover new patterns and variations of ransomware (Ahmed et al., 2022).

The state-of-art detection technic of Ransome 2.0 has found its complexity in defining the initial entry point which can be divided into two main vectors

Assuming that ransomware 2.0 entry points scenarios can be similar but different each time, it is likely to imagine scenarios but hard to define the exact entry point.

# References:

1. Ahmed, Mohiuddin, et al. “Ransomware 2.0: An Emerging Threat to National Security.” *Australian Journal of Defence and Strategic Studies*, vol. 4, no. 1, July 2022, 10.51174/ajdss.0401/emqh2521. Accessed 21 Aug. 2022.
2. Anand, Aditya. “Malware Analysis 101 - Sandboxing.” *Medium*, 13 Jan. 2020, infosecwriteups.com/malware-analysis-101-sandboxing-746a06432334. Accessed 3 Nov. 2022.
3. Bar-Yosef, Noa. “An inside Look at Hacker Business Models | SecurityWeek.com.” *Www.securityweek.com*, 19 Oct. 2010, [www.securityweek.com/inside-look-hacker-business-models](http://www.securityweek.com/inside-look-hacker-business-models).
4. Crandall, Carolyn. “Derailing Ransomware 2.0 Requires a Little Trickery | 2020-09-16 | Security Magazine.” *Www.securitymagazine.com*, 16 Sept. 2020, [www.securitymagazine.com/articles/93303-derailing-ransomware-20-requires-a-little-trickery](http://www.securitymagazine.com/articles/93303-derailing-ransomware-20-requires-a-little-trickery).
5. Fernando, Damien Warren, et al. “A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques.” *IoT*, vol. 1, no. 2, 15 Dec. 2020, pp. 551–604, 10.3390/iot1020030. Accessed 27 Jan. 2021.
6. Hasan, Md Mahbub, and Md. Mahbubur Rahman. “RansHunt: A Support Vector Machines Based Ransomware Analysis Framework with Integrated Feature Set.” *2017 20th International Conference of Computer and Information Technology (ICCIT)*, Dec. 2017, 10.1109/iccitechn.2017.8281835. Accessed 27 Oct. 2022.
7. Mates, Amanda. “Incident Response Ransomware Series - Part 2.” *TrustedSec*, 30 Oct. 2019, www.trustedsec.com/blog/incident-response-ransomware-series-part-2/. Accessed 3 Nov. 2022.
8. Sgandurra, Daniele, et al. “Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection.” *ArXiv:1609.03020 [Cs]*, 10 Sept. 2016, arxiv.org/abs/1609.03020.
9. Shaukat, Saiyed Kashif, and Vinay J. Ribeiro. “RansomWall: A Layered Defense System against Cryptographic Ransomware Attacks Using Machine Learning.” *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*, Jan. 2018, 10.1109/comsnets.2018.8328219. Accessed 11 Sept. 2019.