Abertay University

Evaluating the Effectiveness of Using a Modifiable Ransomware Simulation Tool

Patrick Collins

BSc (Hons) Ethical Hacking

Introduction

Ransomware is one of the most prominent and successful threats facing computer security today. It is malicious software that's aim is to encrypt important information and extort the victim for payment to decrypt their files.

This is why ransomware simulation tools are now being created to test the systems security and detection against a ransomware attack in a safe and effective manner. There is no risk to the company or the individual running the tool. The idea behind each tool is to behave like ransomware as best as possible. However, many of these simulation tools aren't actually simulating how ransomware behaves effectively (Allon, 2022).

Aim

It's the main aim of this project to develop a ransomware simulation tool that will encrypt existing user data and enable the user to modify certain features of the ransomware simulation. Such as the file extension used for each simulation scenario and the directory that gets encrypted.

Objectives to achieve this aim:

- Undertake an extensive literature review on the project area.
- Develop a ransomware simulation tool for a Windows environment.
- Implement features behaving as close to ransomware as possible, whilst still being safe to run.
- Give the User ability to modify each scenario.
- Compare the final project against RanSim.

Research Question:

Are ransomware simulation tools an effective measure to accurately assess security against a ransomware attack?

Method

Setting Up Host-Only Virtual AD Network

Before any development could begin the researcher set up an isolated virtual network using virtual machines in VMWare. The network was set up to mimic an actual company network with Active Directory configured, multiple Windows 10 Machines, a Windows Server 2009 and a pfSense firewall.

Snort Setup

Snort was set up using the pfSense firewall VM. Snort community ruleset was installed to detect ransomware activity. Snort was then set to monitor the private network.

MoChara

Development then began on the ransomware simulation tool called "MoChara". The researcher programmed the tool using Microsoft Visual Studio 2022 in C++20.

The cryptography used in the project for encryption/decryption was from the library **CryptoPP** 8.7 (Dai, 2021).

AES 256 in Galois/Counter Mode (**GCM**) **mode** symmetric encryption is the encryption algorithm used to encrypt each file. GCM is authenticated encryption and was chosen as it is a more secure encryption method checking for any modification of the encrypted files before decrypting.

Multiple features were successfully implemented including **Selecting a Folder, Encryption, Ransom note, Decryption, Modifying MoChara**.

KnowBe4's RanSim V2.2.1.3

The researcher downloaded another ransomware simulation testing tool from KnowBe4 called "RanSim" (Knowbe4, 2023). The executable was transferred onto the private network. The researcher ran the setup wizard and fully installed the tool.

Results

The project was evaluated by gathering quantitative data on MoChara on the encryption/decryption feature to test its performance. A python script was created to check the Shannon Scale entropy of a file. If a file is higher than 5 from 0-10 then it has been properly encrypted.

The researcher calculated the entropy of each file before and after encryption had occurred. Figure 1 below show the **average** entropy of a file **before** encryption was **4.56**.

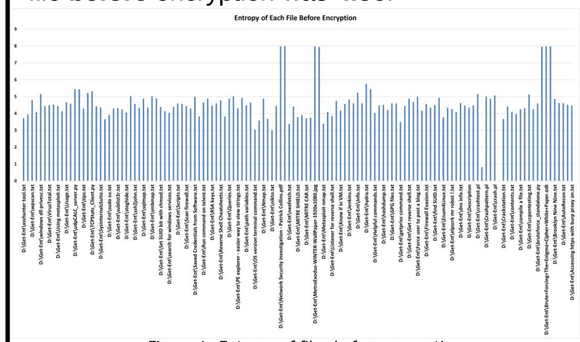

Figure 1: Entropy of files before encryption.

Figure 2 below shows the **average** entropy of a file **after** encryption was **6.68**.

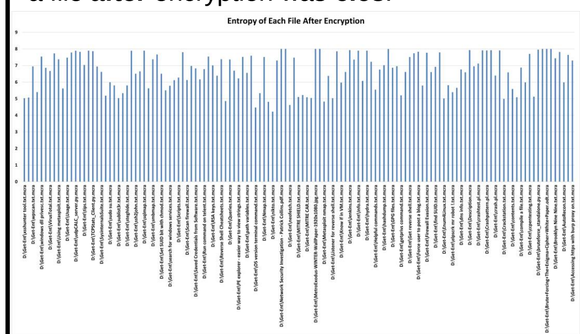

Figure 2: Entropy of files after encryption.

KnowBe4's **RanSim** was evaluated on its ransomware features and the statistical graphs generated at end of each simulation. After three simulations **no file encryption occurred** although a report showed the system vulnerable to 22/23 ransomware types.

Snort did not have any alerts for ransomware activity after running both simulation tools.

Discussion

Overall, MoChara has met all aims identified in this project to develop a ransomware simulation tool. It successfully uses encryption algorithms and libraries that real world ransomware uses. Real ransomware behaviour is deployed encrypting existing files and the entire directory that was chosen. Files are appended with a file extension that the User chooses. It achieves all of this whilst still being safe demonstrating that it is possible to remove the safety net.

With MoChara you can also notice the simulation scenario playing out in real-time improving visuals and understanding for the User. It is a step in the right direction for ransomware simulation tools.

One major weakness identified was the Intrusion Detection tool Snort not detecting any ransomware activity from either ransomware simulation tool.

It is still very unclear how RanSim is simulating a ransomware attack as the most important main features of ransomware do not appear to be occurring at all despite the vulnerable report generated.

Conclusion

Overall, the project was a success with ransomware simulation tools showing a promising method to test the security against a ransomware attack in a safe manner. However, a lot of work is needed to reach the point of fully simulating unknown ransomware behaviour and to do so safely.

Future work includes implementing more ransomware features and instead using an EDR solution to detect and evaluate the tools.

References

Allon, Y, 2022. Ransomware Simulators - Reality or a Bluff? - Palo Alto Networks Blog. [online] Palo Alto Networks Blog. Available at: <https://www.paloaltonetworks.com/blog/security-operations/ransomware-simulators-reality-or-a-bluff/> [Accessed 25 May 2023].

Dai, W, 2021, Crypto++® Library 8.7, Crypto++ Library 8.7 | Free C++ Class Library of Cryptographic Schemes. Available at: <https://www.cryptopp.com/> [Accessed: 25 May 2023].

Knowbe4, 2023. Ransomware Simulator: Testing Tool for Malware | KnowBe4. [online] Available at: <https://www.knowbe4.com/ransomware-simulator> [Accessed 25 May 2023].