Evaluating the Effectiveness of Using a Modifiable Ransomware Simulation Tool

Patrick Collins
School of Design and Informatics
Abertay University
DUNDEE, DD1 1HG, UK

ABSTRACT

Context
Ransomware simulation tools are being created to safely simulate the behaviour of ransomware. By using these tools, you can test the security of a network against a ransomware attack. However, many of these tools are not simulating ransomware's behaviour effectively.

Aim
The aim of this project is to develop a ransomware simulation tool that has all of ransomware's features implemented which would be an accurate measurement of network/host security against a zero-day ransomware attack.

Method
Literature will be thoroughly reviewed from previous researchers to understand their attempts when creating a ransomware simulation tool and implementing its features. Research will also be carried out to find all of ransomware's features to be implemented. Once the tool is developed with all of these features implemented it, alongside existing solutions, will be evaluated using intrusion detection tool Snort/Yara to find the effectiveness of ransomware detection on a network.

Results
The project will identify if ransomware simulation tools are an effective and trustworthy measure of testing a network's security against a ransomware attack.

Conclusion
The current state and direction we are going in with ransomware simulators will be identified. If we are going in the wrong direction, then it could lead to further ransomware attacks occurring. If successful, this project will provide a guide for future developers on how to effectively design and implement a ransomware simulation tool. Finally, identifying if ransomware simulation tools are ineffective and should not be used or developed.

Keywords

Ransomware, simulation, tool, intrusion detection.

1. INTRODUCTION

Ransomware is a type of malicious software that encrypts personal data and extorts the user for payment of a decryption key to access their files again. If the ransom is not paid the data could be deleted or published online. In H1 of 2022 alone there were 236.1 million ransomware attacks (Statista.com, 2022). Ransomware is a persistent threat to the world and is showing no signs of giving up.

Currently, the only effective method to see ransomware in action is to run a live sample created by attackers for malicious intent and extortion. It can be very dangerous if the researcher does not set up their environment correctly before running the live ransomware.
Furthermore, the researcher always runs the risk of the ransomware sample escaping from its virtualized environment and infecting the host machine. The researcher may be attempting to analyse or demonstrate to others how ransomware behaves through running the live sample. Running the live sample could also be used for testing the security detection in place but will be very harmful if run on an important system/network.

Old samples of malware did not check if they were in a sandbox environment. This is not the case at the moment and going forward. Many malicious software now checks first if there is any virtualization/sandbox present, and if there is the harmful code is not executed (YUCEEL and Picus Labs, 2022). This will make it very difficult to run live samples for any reason in the future as the attackers are adapting to the methods researchers use to analyse their samples. We also have to adapt how the analysis and investigation is done.

This is why simulators are now being created to effectively test ransomware in a safe environment. There is no threat as no harmful live sample is being run. For ransomware simulators, it aims to behave like ransomware. However, many of these simulators aren't actually simulating how ransomware behaves effectively (PaloAlto, 2022). By playing it safe we run the risk of not being able to detect ransomware effectively and more infections and attacks will continue to happen.

It's the main aim of this project to develop a ransomware simulator that successfully combines all of ransomware's features into one tool without the false safety net that current simulators provide. If the simulation tool effectively covers all aspects of ransomware, then a user can be confident it will be an accurate measurement of their network/host security against a ransomware attack.

Furthermore, this project plans to enable the user to modify certain features of the ransomware simulation. Such as the encryption algorithm and file extension used for each simulation scenario. By doing so we can better simulate zero-day ransomware attacks and improve detection and security against them.

Finally, the project's effectiveness will be evaluated using a quantitative approach against other ransomware simulation tools using the detection tool Snort or Yara. Rules will be created to detect ransomware behavior on the network and system. The ransomware simulation tool created in this project and other existing tools will then be tested against these rules in Snort to gain data on the detection rate.

2. BACKGROUND

There have been many previous attempts at creating ransomware simulators. They all aim to simulate the behavior of ransomware to test the security and detection a network has in place. This has been done by either simulating the behavior of specific ransomware samples or testing main features of ransomware. These main features in current attempts can be found in Table 1 below.

Table 1 – Ransomware's Main Features

Feature	Simulation Purpose
Backup/Exfiltration	Backup of the user data before encryption to hold for ransom.
Encryption	Lock the user out of their personal data.
Ransom Note	All ransomware samples leave a ransom note to the victim with details on what has occurred.
Replication	Spreading the simulation scenario to multiple machines.
Decryption	Once the scenario has finished the data is decrypted and can be accessed.

However, most of these tools are not effectively simulating the ransomware behavior. An investigation by Yoni Allon and PaoloAlto Networks on a few of these attempts show the current understanding is not clear. Some attempts are getting it right whilst others are not a good measure for ransomware detection/prevention at all (Yoni Allon, 2022). This investigation highlights that it's important to get the simulation scenario correct.

2.1 Encryption

One of the most popular ransomware simulation tools is from KnowBe4's "RanSim" (KnowBe4, 2022). Unfortunately this tool, and many others, is not open source so it's unclear exactly how the tool is simulating the scenario. However, to simulate the ransomware encryption feature, files are downloaded from the internet and then encrypted.

One flaw, that most of the current attempts have, is not encrypting any amount of existing files and instead creating/downloading a few files from the simulation tool itself and using those files for the simulation. A real ransomware attack will encrypt already existing files on the computer system. Some ransomware simulation tools have got this feature right, such as "Infection Monkey" (Akamai, 2022).

2.2 Scenario modification

Current simulation tools do not have the option to modify certain aspects of the ransomware simulation that may prove valuable if allowed to do so. Instead most tools force the simulation of an already existing ransomware sample that has its own uniqueness. The downside to attempting to keep up with the newest ransomware sample created is that the prevention measures put in place to detect and combat that specific type of ransomware becomes obsolete once another ransomware sample is released with its own uniqueness. If we allow the user to modify the file extension used for the encrypted files in each simulation scenario, we can better simulate zero-day ransomware attacks and improve detection and security against them.

2.3 Visuals

Moreover, there is no visual aspect of the current simulation scenarios. The disadvantage of not having visuals in the scenario is the user cannot see the ransomware simulation in action. The simulation scenario runs and, for the tools that have this feature, the user gets a generated report on how secure their network is. It would be beneficial if the ransomware simulation were to fully play out in a safe environment to also help improve the user's understanding of a ransomware attack scenario.

2.4 Not covering all ransomware features

The simulation tools currently available specialise in one or more aspects of a ransomware attack but not all. For example, "RanSim" simulates the encryption and decryption of data on the system but not the data exfiltration or ransomware replication. To effectively test the network security against a ransomware attack you may have to run a few of these tools to be confident you are protected by all of the features of ransomware. Although, you cannot be confident the results are accurate. As mentioned previously, this project hopes to continue with the direction of current simulation tools and attempt to implement all features into one tool. Some missing features are shown in Table 2 below.

Table 2 – Missing Features of current simulation tools

Missing Feature	Reason
User Lockout	Locker ransomware blocks user control on the system disabling the peripherals until the ransom is paid.
Modifying the Master Boot Record (MBR)	Newer strains of ransomware are also editing the MBR on top of encrypting user files.
Ransomware Pop-Up window	Many ransomware samples have a pop-up window once run.
Timer	A timer displays how long the user has to pay the ransom before data deletion/publication.

The project will attempt to implement all of these features in the least harmful way possible as to not damage the system. If this is not possible those features will have to be dropped as the project progresses.

3. METHOD

Before carrying out the project, literature will be thoroughly reviewed from previous researchers to understand their attempts when creating a ransomware simulation tool and implementing its features. Furthermore, research will be carried out on the best safe method to implement all of the ransomware features previously mentioned and the extra features discovered from the research.

3.1 Project development

The ransomware simulation tool will be created with the programming language C++. The decision for using this programming language is due to being a popular choice for the current ransomware samples created for malicious intent and extortion. A great analysis done by S. Alzahrani, Y. Xiao and W. Sun on “An Analysis of Conti Ransomware Leaked Source Codes” shows this recent strain was developed using C++ (S. Alzahrani, Y. Xiao and W. Sun, 2022). The project therefore should be possible and successful if following the methods actual ransomware uses.

Furthermore, a very simple proof of concept ransomware simulation tool had been created by A. Adamov and A. Carlsson on their experiment “Reinforcement Learning for Anti-Ransomware Testing”. The tool created was very limited only changing the file extension, encrypting in Base64. Whilst created for a different purpose, they concluded that the results looked promising, even for the limited features used (A. Adamov and A. Carlsson, 2020). This creates confidence that the simulation tool created in this project may be even more effective due to the extra features to be implemented.

Finally, the ransomware simulation tool will attempt to implement all of the ransomware features, as discussed previously in Figure 1 and Figure 2 plus any more discovered through the research stage of the project. Each feature implemented will be split up and have to be run individually. The decision for doing this is to avoid the sample becoming a live sample that may harm the system.

3.2 Ransomware detection

After the simulation tool has been created it will be evaluated against the intrusion detection tool Snort or Yara. Snort/Yara is an effective method to detect ransomware as seen by M. Satheesh Kumar, Jalel Ben-Othman and K.G. Srinivasagan’s work on “An Investigation on Wannacry Ransomware and its Detection”(M. Satheesh Kumar, Jalel Ben-Othman & K.G. Srinivasagan, 2018).

3.3 Evaluation

A quantitative approach will be used for the evaluation. The evaluation will be on the effectiveness of each ransomware simulation tool. The data will be collected by using the Intrusion Detection tool Snort or Yara (Depending on which detection tool is better suited as the project progresses).

Rules will be created to detect the ransomware behavior of each tool on the network and system. The ransomware simulation tool created in this project and other existing tools will then be tested against these rules to find the detection rate of each tool.

Once the data has been collected from the various ransomware simulation tools, it will then be evaluated to find the effectiveness of each tool to be detected by an Intrusion Detection System. This will display which of the tools is effectively simulating a real zero-day ransomware attack on a network and/or computer system. The tool with a high detection rate will allow the user to be confident that running that tool on their network is a trustworthy assessment of their security against a ransomware attack.

4. Summary

It’s important to carry out this project to know the current state and direction we are going in with ransomware simulators. If we are going in the wrong direction, then any individual who decides to deploy these simulation scenarios to test their security will be given a false security assessment and critical flaws in the network security will be overlooked leading to more ransomware attacks to occur.

If successful, this project will provide a guide for future developers on how to effectively design and implement a ransomware simulation tool. Hopefully improving upon the one developed in this project. The project will also identify if the idea of a ransomware simulation tool itself is flawed and should not be used or continued to be developed in the future.

5. REFERENCES

A. Adamov and A. Carlsson, 2020, Reinforcement Learning for Anti-Ransomware Testing, IEEE East-West Design & Test Symposium (EWDTS), pp. 1-5, doi: 10.1109/EWDTS50664.2020.9225141.

Akamai, 2022. *Ransomware simulation*. [online] techdocs.akamai.com. Available at: <https://techdocs.akamai.com/infection-monkey/docs/ransomware-simulation> [Accessed 4 October 2022].

Knowbe4.com, 2022. *Ransomware Simulator: Testing Tool for Malware | KnowBe4*. [online] Available at: <https://www.knowbe4.com/ransomware-simulator> [Accessed 3 October 2022].

M. Satheesh Kumar, J. Ben-Othman and K. G. Srinivasagan, 2018, An Investigation on Wannacry Ransomware and its Detection, IEEE Symposium on Computers and Communications (ISCC), pp. 1-6, doi: 10.1109/ISCC.2018.8538354.

Statista. 2022. *Number of ransomware attacks per year 2022 | Statista*. [online] Available at: <https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/> [Accessed 25 September 2022].

S. Alzahrani, Y. Xiao and W. Sun, 2022, An Analysis of Conti Ransomware Leaked Source Codes, in IEEE Access, vol. 10, pp. 100178-100193, doi: 10.1109/ACCESS.2022.3207757.

Yoni Allon, 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 September 2022].

YUCEEL, H. and Picus Labs, 2022. *Virtualization/Sandbox Evasion - How Attackers Avoid Malware Analysis*. [online] Picussecurity.com. Available at: <https://www.picussecurity.com/resource/virtualization/sandbox-evasion-how-attackers-avoid-malware-analysis> [Accessed 27 September 2022].