A study on windows-based ransomware implications on linux operating system using compatibility layer wine based on dynamic analysis

Rycka Septiasari, Yogha Restu Pramadi*
Cyber Security Engineering, Department of Cyber Security, Politeknik Siber dan Sandi Negara, Bogor, Indonesia

rycka.septiasari@student.poltekssn.ac.id, *yogha.restu@poltekssn.ac.id

Abstract. Linux is an open source operating system that uses the Linux kernel. The security of Linux makes its users rarely use antivirus to prevent the threat of ransomware attacks. The purpose of this study is to assess the security of the Linux operating system that uses Wine as a compatibility layer against ransomware attacks. Then to determine whether ransomware has a higher impact than malware samples in previous studies or not. The methods used on the 30 samples are static analysis to identify samples, and dynamic analysis to determine the implications. From the 30 ransomware samples that can run on the Linux operating system, the results obtained show that 80% affect the registry, 50% affect the file system, 50% affect the service, 70% affect the Network and 60% affect the Process. While overall there are 30% of samples that affect the five existing parameters. The results show that ransomware has relatively high implications for existing parameters, inversely proportional to previous research.

1. Introduction
Linux is a free and open-source operating system that is easy to repair and patch so it is safer in terms of protecting the operating system from threatening attacks, compared to other operating systems [1]. Despite the security offered by Linux, Linux has not been able to meet all the needs of users who have to use Windows-based programs. Windows-based programs cannot run on Linux because the instructions to be executed cannot be translated directly by Linux. To overcome this, Linux users must use a compatibility layer, such as the Wine compatibility layer software. By using Wine, popular applications such as Microsoft Office can run on the Linux operating system. However, based on a research conducted by Duncan and Schreuders (2018) entitled "Security implications of running Windows software on a Linux system using Wine: a malware analysis study" stated that using Wine to run Windows programs can pose a serious security threat against Linux. Some of the malware samples used in the research can run successfully on the Linux operating system. This is certainly a threat to the security of individual and organizational data. The study used 30 samples of Trojan, Worm, Spyware, and Backdoor malware, but in that study, researchers did not use ransomware as an object of analysis, so it is unknown what are the implications that ransomware generates on Linux.
Ransomware is a major asset security threat. According to McAfee’s report, the percentage of ransomware attack growth in Q1 in 2019 reached 118% [2]. Most ransomware still targets Windows-based operating systems, which are the most commonly used operating systems on desktops and laptops [3]. These problems are the background of the writing of this study. The focus of this research is the study of the implications of ransomware on Linux operating systems that use a compatibility layer. The malware analysis technique used is dynamic analysis.

2. Method and Materials

2.1. Method

The method used in this research is the Design Research Methodology (DRM). The purpose of selecting DRM as the research methodology is to carry out a detailed approach so that it can help it can make the research designs to become more effective and efficient. The first stage is Research Classification, some indications that support the assumptions for formulating research objectives are collected to achieve the research objectives, here we are determined to measure the implication of Windows based ransomware on Linux that are using Wine. The next stage is Descriptive Study, the aim is to make a detailed description to determine which factors must be addressed in order to increase the clarification of the task effectively and efficiently. These factors are modification to the file system by the ransomware (such as encrypting files), malicious network activities (such as connection to C2 server), registry alteration, invoking malicious services, and spawning a malicious process (such as opening a ransom note window). Then the third stage is Perspective Study, to increase understanding of the existing situation to solve the problems that have been described previously. The analytical method used is static and dynamic analysis. Descriptive II (DS-II), this stage is the evaluation of the analysis conducted. Evaluation is done by measuring the results of the analysis.

2.2. Materials

Analysis is carried out in a virtualized environment in order to keep the host environment safe. The operating system used on the host is Ubuntu 18.04, and both guests also use Ubuntu 18.04. The first guest is used to run ransomware and the second guest is used to monitor the first guest network when the ransomware is running. The network configuration of the guests is set to Host-Only mode, so the ransomware cannot communicate with the internet and the network is limited to the environment. The two guests are set to static IP configurations, with the second guest’s network is set in promiscuous mode. The hardware and software used in the study are explained in Table 1.

| **Table 1. Hardware and software requirements.** |
|-----------------------------------------------|
| **Software Requirements** | **Hardware Requirements** |
| Virtualization environment | |
| - Ubuntu 18.04 | - RAM 2 GB |
| - Wine 4.0.3 | - CPU |
| - VirtualBox 6.0 | |
| Host environment | |
| - Linux 18.04 | - RAM 8 GB |
| | - HDD 1 TB |
| | - Intel Core i5-8265U |
3. Analysis

3.1. Static Analysis
Static analysis is a method of analyzing files that are suspected of ransomware samples without having to execute the file. This method is used to identify the entire samples so that all samples are different and no sample is used repeatedly. The software used for analysis is HxD. It can determine file types, so it can be seen whether the sample is executable or not. Hash Checker 4.0.8 is used to determine the sample hash value, so that no sample is used repeatedly. VirusTotal is also used to validate whether the file that is used is a ransomware malware.

3.2. Dynamic Analysis
Dynamic analysis in the context of malware analysis is a method of analyzing the effects of malware functions on a system by looking at the system before and after the ransomware is executed on the system. The software utilized here are Gnome System Monitor, Regshot for Linux, QPS GUI-based Process monitor, InetSim, and Wireshark. The analysis is carried out as follows:

3.2.1. Simulate a server. Inetsim is a Linux based software that simulates standard internet services (such as DNS, HTTP / HTTPS, etc.). INetSim is installed on the monitoring guest machine, the ransomware will connect to INetSim as the service provider and record the communications that occur.

3.2.2. Network Analysis. Network traffic is captured using Wireshark on the monitoring guest machine with INetSim running. By doing a service simulation, it can be seen if the ransomware communicates with the C2 server after it is executed or not.

3.2.3. Take the first registry snapshot. Regshot is a tool used to take and compare two registry snapshots. To use Regshot in analyzing malware, we need to take two snapshots of the registry, one before, and the other one after the execution of the malware. The Regshot used is Windows Regshot, so it is necessary to use Wine to run the software.

3.2.4. Running the ransomware. In dynamic analysis, the ransomware that is the object of analysis must be executed so that the behavior of the ransomware can be analyzed.

3.2.5. Analyze the modified file system. Malware file system alteration activity is monitored using Procmon. Procmon contains information about events that occur including the sequence number of events, the timestamp, the name of the process that caused the event, the operation of the event, the path used by the event, and the outcome of the event.

3.2.6. Take the second registry snapshot. After the malware has been running for some time, take the second snapshot again, and compare the two snapshots that have been made to identify the changes that occur.

3.2.7. Monitor the process. Process Explorer is used to check the process and determine whether the ransomware creates a new process or stops a process.

4. Result
The results of the dynamic analysis of 30 ransomware samples show that some samples have implications on existing parameters, while others do not. With details: as many as 50% (15 samples) affect the file system, 70% (20 samples) affect the network, 80% (24 samples) affect the registry, 50%
(16 samples) affect the service, 60% (18 samples) affect the process, and 30% (10 samples) affect all existing parameters. When compared with the results of research conducted by [4], the results show more implications for the operating system compared to previous studies where only 5 successful malware samples were run. The overall result is explained in Table 2.

Table 2. Overall analysis result.

| No | Ransomware name | Hash | File | System | Network | Registry | Services | Process | Overall |
|----|-----------------|------|------|--------|---------|----------|----------|---------|---------|
| 1  | Wannacry        | f42d29367786af1b8919a9d0fbed1d3f | No   | Yes   | No      | No       | Yes      | No       | No      |
| 2  | Wannacry2       | 6085cb00e4e434711530c95e58c38c11f | No   | Yes   | No      | No       | Yes      | No       | No      |
| 3  | Sodinokibi      | a0f4b1f97277e396b13933877c7992d | No   | Yes   | No      | Yes      | No       | Yes      | No      |
| 4  | Jsworm          | c669320897f2e124307e2e8ae2e9206d | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 5  | PwndLocker      | 16a29314e8563135b1866036a6f0f3e8 | No   | Yes   | Yes     | Yes      | No       | Yes      | No      |
| 6  | Ragnar Locker   | 6171000983c8396d167e0da9b9b49ba | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 7  | GermanWiper     | 36cdec427554d482900b57188ace3a8a9a7 | No   | Yes   | No      | No       | Yes      | No       | Yes     |
| 8  | Pjx             | 5dc438d8e9ab91c0c20b1d9e82a481d0 | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 9  | Epoblock        | 8b08c16d1f37e09a9bb90b2b1b67d67 | No   | Yes   | No      | No       | No       | No       | No      |
| 10 | TFlower         | 3c32934e3b9b66ab9319a3b9d909be | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 11 | PureLocker      | 527468a4053d4e142dd247965f9e1e94c | No   | Yes   | No      | No       | No       | No       | No      |
| 12 | Snake           | 3d1ceef32ba0c39c757f3ce517ef82a | No   | No    | No      | No       | No       | Yes      | No      |
| 13 | HorseDeal       | 716c302a250f742fe935b3c2b3ca4a | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 14 | Mailto          | d60d91c245707f0af4281602ac19e97 | No   | Yes   | No      | No       | No       | No       | No      |
| 15 | Cerber          | 8bb6c16d137e09a80b02b1b67d67 | No   | No    | No      | No       | No       | Yes      | No      |
| 16 | CLOP            | 8752a052a75239b86b0da1d483dd7 | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | No      |
| 17 | Coronavirus      | ec517204f0c7a980d13781b1afa94ad | No   | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 18 | ERIS            | 7fde8ce9802a8b6f426244e61524b69 | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 19 | Maze            | 21a563958b73d453ad91e2511855c | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 20 | Nefilim         | 890539c405672016c90d7a3c5743ee | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 21 | Delphimorix     | c04f3a5c97bb993b51e9d3ea68c309f | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 22 | Jencrypt        | 0f2ade94c6b3d35295d77f5d4a968c2 | No   | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 23 | LockerGoga      | c1152069f6be5663f758f343b38f8ea | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 24 | Xcry            | d60d91c245707f0af4281602ac19e97 | No   | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 25 | GarrantyDecrypt | 96f48973ce17363939e95f2b009c2a1 | Yes  | No    | Yes     | Yes      | Yes      | Yes      | No      |
| 26 | 01001           | 78cb258e6916e0d2287010bf5b0211 | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 27 | Scroboscop      | 1efaa7a7a6f99d04faa44c7f0c30909 | Yes  | Yes   | Yes     | Yes      | Yes      | Yes      | Yes     |
| 28 | T1 Happy         | 64f11aeef1f211e74a3f8f151e456d55 | No   | No    | No      | No       | No       | No       | No      |
| 29 | Argus           | 668983ef223a390f4b81a4d7cdd7b | No   | No    | No      | No       | No       | No       | No      |
| 30 | Anatova         | 9d8445d4800ee1715b183f647261aa | No   | No    | No      | No       | No       | No       | No      |

This research also provides the fact that files in the etc directory are not encrypted, but files outside the etc are encrypted, it is because we need root privileges to be able to access the etc directory.

5. Recommendation

The recommendations for Linux operating system users who use Wine to run Windows-based applications are expected to be one of the references that could prevent malware attacks that occur due to running executable files using Wine. The following are recommendations that can be used as a reference for Linux users to keep the system safe when using Wine:
5.1. Use an application from the repository or download the application from the official site.
On Linux operating systems, a software is downloaded and installed through a repository. But if the required software is not in the repository, then inevitably we would have to download it through a browser whose security is not known. On the other hand, the software available on the repository has been approved by Linux, which means that security is guaranteed. With devices that download and install softwares from other sources. Try to only install software that are available in the repository [5].

5.2. Use an Antivirus
If forced to download and install software that is not from a repository, it must be ensured that the software is free of viruses. One of the most common methods to determine whether the software is a malware or not is to use an antivirus. Some antivirus that can be used on Linux are ClamAV [6], Sophos [7], Firetools [8], and Rootkit Hunter [9] [10].

5.3. Keep the software up to date
Update the software regularly to keep the system safe. By updating periodically, it can be ensured that the software has the latest security patches to avoid threatening attacks [5].

5.4. Install a Firewall
A firewall is a software or hardware-based network security system that controls the incoming and outgoing network traffic based on established rules [11]. A firewall is one of the important tools to protect hosts from attacks coming from untrusted networks [12]. A firewall builds a barrier between a secure internal network and an insecure external network. Linux users can also use a host-based firewall which is a software-based firewall. A Host-based firewall is easier to use because it is simpler and can be run on the system itself. Examples of host-based firewalls include IPCop (www.ipcop.org), pfSense (www.pfsense.org), and Zentyal Community (www.zentyal.com) [11].

5.5. Using Sandbox
Unsafe internet content must be run in a restricted environment, so that it does not affect other systems. Sandbox is an important security technique that runs untrusted content in an isolated environment [13]. Some sandbox applications available for Linux include Flatpak, FireJail, Qubes OS and SnapCraft.

6. Conclusion
In this study, an analysis of 30 ransomware samples was performed with a static analysis first to identify the sample, then dynamic analysis aimed to find out the implications caused by Windows-based ransomware against Linux that runs on the Wine compatibility layer. The results indicate that the ransomware sample showed a relatively high negative impact on Linux based operating system users that run Windows applications using Wine, with the details of 15 samples (50%) successfully affected the file system, 20 samples (70%) successfully affected the network, 24 samples (80%) affected the registry, 16 samples (50%) affected the service, 18 samples (60%) influences the process, and 10 samples (30%) that successfully affect all five parameters in their entirety.

This is inversely proportional to previous research which states that the success rate of malware running on the Linux operating system is relatively low. The research results and recommendations given are expected to increase the understanding and awareness of the Linux operating system users that use Wine when running Windows-based applications.
References

[1] N. Barkakati, Linux All In One Desk Reference For Dummies 2nd Edition, Indiana: Wiley Publishing, 2006.

[2] McAfee, "McAfee Labs Threats Report," McAfee, 2019.

[3] Symantec, "Internet Security Threat Report," Symantec Corporation, Mountain View, 2019.

[4] R. Duncan and Z. C. Schreuders, "Security implications of running windows software on a Linux system using Wine: a malware analysis study," *Journal of Computer Virology and Hacking Techniques*, 2018.

[5] M. Yaswinski, M. Chowdhury and J. Mike, "Linux Security: A Survey," in *IEEE International Conference on Electro Information Technology (EIT)*, Stroudsburg, 2019.

[6] ClamAv, "ClamAV® is an open source antivirus engine for detecting trojans, viruses, malware & other malicious threats.," 2020. [Online]. Available: https://www.clamav.net/.

[7] Sophos, "Antivirus for Linux," 2020. [Online]. Available: https://www.sophos.com/en-us/products/free-tools/sophos-antivirus-for-linux.aspx.

[8] Firejailtools, "Firetools a firejail graphical user interface," [Online]. Available: https://firejailtools.wordpress.com/.

[9] Monika, P. Zavarsky and D. Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization," *The 2nd International Workshop on Future Information Security, Privacy & Forensics for Complex Systems (FISP)*, pp. 465-472, 2016.

[10] T. Gallo and A. Liska, Ransomware Defending Against Digital Extortion, USA: O'Reilly, 2017.

[11] D. Sampaio and J. Bernardino, "Evaluation of Firewall Open Source Software," *International Conference on Web Information Systems and Technologies (WEBIST 2017)*, pp. 356 - 362, 2017.

[12] J. Fruhinger, "What is WannaCry ransomware, how does it infect, and who was responsible?," 30 Agustus 2018. [Online]. Available: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.

[13] Z. Wan, D. Lo, X. Xia and L. Cai, "Practical and effective sandboxing for Linux containers," *Empirical Software Engineering*, 2019.