JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Dynamic Study on The Implications of Windows Ransomware on Linux Operating System Using Wine-based Compatibility Layer

SUBMITTED BY

Shubham K Shirodkar
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY PART-I
INSTITUTE OF DISTANCE AND OPEN LEARNING IDOL BUILDING, VIDYANAGARI, SANTACRUZ (EAST), MUMBAI-400 098

Abstract: Linux is a free OS which uses the Linux kernel. Linux safety makes its users rarely use antivirus to prevent the threat. Linux runs on virtually every platform from mobile devices to supercomputers. As a result, attackers target the Linux infrastructure to launch ransomware attack so that they can recover greater ransom for data recovery. Ransomware is a type of malware designed to block access to a computer system until a payment is made. In this study, the security of the Linux operating system, which employs Wine as a compatibility layer, will be assessed. Then to find out if ransomware has a higher impact than malware samples in previous studies or not. From the 30 ransomware samples that can run on the Linux OS, the final results obtained show that 50% affect the file system,80% affect the registry, 50% affect the service, 60% affect the Process and 70% affect the Network. While overall there are 30% of samples that affect the five existing parameters. The findings demonstrate that ransomware has relatively high implications for existing parameters.

Introduction

Compared to other operating system Linux is free and open source that is easy to patch and repair so in terms of security it is safer of protecting the operating system from threatening attacks. The majority of ransomware attacks encrypt or infect Windows OS, however they are slowly making their way to Linux-powered computers. To decrypt data it demands ransom from the user otherwise the attacker threaten to make data in public [1]. Windows programs cannot run on Linux operating system. Since the instructions to be performed cannot be translated directly by Linux. To overcome this problem, Linux users must use a compatibility layer called as Wine.

Wine stands for "Wine Is Not an Emulator" .It is compatibility layer software by using this you can run Microsoft office on the Linux Operating system. However, according to research led by

Duncan titled "impact of running Windows Software using Wine" said that using wine Running Windows programs can pose a great security threat in Linux operating system.

The research describes used of 30 samples of Trojan, Spyware and Worms to study the impact of Ransomware on Linux operating system that uses compatibility layer Wine. 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]. These problems are the background of the writing of this study.

Methods

The method used for this research is the DRM (Design Research Methodology). The purpose of selecting this 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. The next stage is Descriptive Study, The aim is to create a thorough description in order to identify the aspects that must be taken into consideration in order to increase the task's effective and efficient clarity. The Third stage is perspective study, which aims to improve comprehension of the current situation and address the issues previously outlined. The final method used is static and dynamic analysis

In order to protect the host environment, analysis is done in a virtualized setting. Both the host's operating system and the guests' operating systems are running on Ubuntu 18.04. Ransomware is executed by the first guest, and the second guest keeps track of the first guest's network while the ransomware is running. The guest network settings is in host-only mode, which prevents the ransomware from communicating with the internet and restricts the network to the local environment.

Table 1. Hardware and software requirements.

Software Requirements	Hardware Requirements
Virtualization environment	
- Ubuntu 18.04 - Wine 4.0.3 - VirtualBox 6.0	- RAM 2 GB - CPU
Host environment	
- Linux 18.04	- RAM 8 GB - HDD 1 TB - Intel Core i5-8265U

Analysis

3.1. Static Analysis

Static analysis is a technique for examining the files without running it that may contain ransomware samples. In order to ensure that each sample is unique and never used more than once, the complete sample set is identified using this technique. The software used for analysis is HxD. it can identify file types, to check whether an executable sample is present or not. To ensure

that no sample is used more than once, the sample hash value is calculated using Hash Checker 4.0.8. In order to confirm whether the used file contains ransomware, VirusTotal is also used.

3.2. Dynamic Analysis

In the context of malware analysis, dynamic analysis is a technique for examining the system before and after the ransomware has been executed on it in order to analyse the impacts of malware functionalities on the system. Gnome System Monitor, QPS GUI-based Process monitor, InetSim, and Wireshark are the programs used in this. Here's how the analysis is carried out.

3.2.1. Simulate a server

A Linux-based programme called Inetsim mimics common internet services (such DNS, HTTP / HTTPS, etc.). The monitoring guest machine has INetSim installed; once connected, the ransomware will act as the service provider and record all communications.

3.2.2. Network Analysis.

Wireshark is used to record network traffic while INetSim is operating on the monitoring guest machine. It is possible to determine whether the ransomware connects with the C2 server after execution by running a service simulation.

3.2.3. Take the first registry snapshot

A tool called Regshot is used to compare two registry snapshots. We must capture two registry snapshots one before and one after the malware execution. In order to use Regshot to analyse malware. Wine must be used to run the programme since the Regshot utilised is Windows Regshot.

3.2.4. Running the ransomware

In a dynamic analysis, the ransomware that will be the subject of the research must be executed in order to study its behavior.

3.2.5. Analyze the modified file system

Procmon is used to track malicious file system alterations. Such as the timestamp, the name of the process that triggered the event, how the event operated.

3.2.6. Take the second registry snapshot

Take the second snapshot once more after the virus has been active for a while, and then compare the two to see what changes have occurred.

3.2.7. Monitor the process

Process Explorer is used to check the process to see if the ransomware starts a new process or terminates an existing one.

Result

The research of 30 ransomware samples revealed that certain samples had an impact on the parameters that are currently in use, while others did not. With specifics: up to 50% (15 samples) have an impact on the file system, 70% (20 samples) the network, 80% (24 samples) the registry, 50% (16 samples) the service, 60% (18 samples) the process, and 30% (10 samples) have an impact on all currently used parameters. The findings have more ramifications for the operating system when compared to earlier experiments where only five successful malware samples were executed,

The overall result is explained in below Table

No	Ransomware name	Hash	File System	Network	Registry	Services	Process	Overall
1	Wannacry	f42d29367786af1b8919a9d0cbedfd3f	No	No	Yes	No	No	No
2	Wannacry2	0805cb0e64e34711530c95e58e38c11f	No	Yes	No	No	No	No
3	Sodinokibi	af04b1f978277e936b13933877c7992d	No	Yes	Yes	No	Yes	No
4	Jsworm	c669320b97f2c124307c3e8ae2e9206d	Yes	Yes	Yes	Yes	Yes	Yes
5	PwndLocker	16a29314e8563135b18668036a6f63c8	No	Yes	Yes	Yes	Yes	No
6	Ragnar_Locker	6171000983cf3896d167e0d8aa9b94ba	Yes	Yes	Yes	Yes	Yes	Yes
7	GermanWiper	36ccd442755d482900b57188ae3a89a7	No	Yes	Yes	No	Yes	No
8	Pjx	5dc438c8c9ab91ccadba1de82ab481d9	Yes	Yes	Yes	Yes	Yes	Yes
9	Epoblock	8b6bc16fd137c09a08b02bbe1bb7d670	No	Yes	Yes	No	No	No
10	TFlower	53c923d4e39b966ab951f9a3b9d090be	Yes	Yes	Yes	Yes	Yes	Yes
11	PureLocker	527468a4053dc142dd479659cf2fc94c	No	Yes	No	No	No	No
12	Snake	3d1cc4ef33bad0e39c757fce317ef82a	No	No	No	No	Yes	No
13	HorseDeal	716c502ba250f742fc935b3cb223ca4a	Yes	Yes	Yes	Yes	Yes	Yes
14	Mailto	d60d91c24570770af42816602ac19c97	No	Yes	Yes	No	No	No
15	Cerber	8b6bc16fd137c09a08b02bbe1bb7d670	No	No	Yes	No	No	No
16	CLOP	8752a7a052ba75239b86b0da1d483dd7	Yes	Yes	Yes	Yes	No	No
17	Coronavirus	ec517204fbcf7a980d137b116afa946d	No	Yes	Yes	No	No	No
18	ERIS	7fd8fc98d8028afb6426244e61524b69	Yes	Yes	Yes	Yes	Yes	Yes
19	Maze	21a563f958b73d453ad91e251b11855c	Yes	Yes	Yes	Yes	Yes	Yes
20	Nefilim	8f90539c405672016c0dec7ac3574eea	Yes	Yes	Yes	Yes	Yes	Yes
21	Delphimorix	cb411fa5c97bb993b51c9ddeaa8c804f	Yes	No	Yes	Yes	Yes	No
22	Iencrypt	02ade94c4b5bd3295d775a6d48a968c2	No	Yes	Yes	No	No	No
23	LockerGoga	e11502659f6b5c5bd9f78f534bc38fea	Yes	Yes	Yes	Yes	Yes	Yes
24	Xcry	7475713df82b2a81b2d32715a94c2b63	Yes	No	Yes	Yes	Yes	No
25	GarrantyDecrypt	96f48973c173639ce9b5f28b006c92a1	Yes	No	Yes	Yes	Yes	No
26	010001	78cb258a691efde0d2287010bff3b211	Yes	Yes	Yes	Yes	Yes	Yes
27	Scroboscop	1efaa77a6f99d04effa4dc710c3909f0	Yes	No	Yes	Yes	Yes	No
28	T1 Happy	64f11aee7f21ec74a3f8f518e45c6d55	No	No	No	No	No	No
29	Argus	668983cf8223a398f4b8a1a4d7cddb7a	No	No	No	No	No	No
30	Anatova	9d844d5480eec1715b18e3f6472618aa	No	No	No	No	No	No
		Total	**15**	**20**	**24**	**16**	**18**	**10**

Conclusion

In this study, 30 ransomware samples were analyzed. A static analysis was used to identify each sample, and a dynamic analysis was done to determine the effects that Windows-based ransomware had on Linux, which uses the Wine compatibility layer. The results show that the ransomware sample had a relatively high negative impact on Linux users who use Wine to run Windows applications, with the specifics of 15 samples (50%) successfully affecting the file system, 20 samples (70%) successfully affecting the network, 24 samples (80%) successfully affecting the registry, 16 samples (50%) successfully affecting the service, 18 samples (60%) effectively influencing the process,

The findings of the study and the recommendations made are increases to boost knowledge and awareness among Linux users who use Wine to execute Windows-based programs.

Reference:

[1] "Ransomware Attack: Recover Data after Attack in Linux Operating System" Retrieved from **https://www.jetir.org/view?paper=JETIR2304718**

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

[3] "What is Wine" Retrieved from **https://www.winehq.org/**

[4] "Wine Software" Retrieved from **https://en.wikipedia.org/wiki/Wine_(software)**