Ethical Hacking Implementation for Lime Worm Ransomware Detection

Nagham A Sultan1, Karam H Thanoon2, Omar A Ibrahim3
1,3 Computer Science Department, University Of Mosul, Mosul, Iraq
2 Software Department, University Of Mosul, Mosul, Iraq
naghamajeel@uomosul.edu.iq1, karamhatim@uomosul.edu.iq2,
dr.omar.aldabbagh@uomosul.edu.iq3

Abstract. Nowadays, computer worms become one of the most dangerous types of malwares threats. Computer worms have evolved during the time with sophisticated forms such as crypto type ransomware. Lime worm is one of these worm kinds. The researchers apply this worm on real environment in lab (ethically and for education purposes) and this paper presents the capabilities of this worm. This paper also presents static analysis by applying many tools, which are used to obtain the key information of lime worm. This paper discovers that applying static analysis on this type of worms is very effective and accurate. The obtained key information are used to develop a software for detecting lime worm and the ability to erase it.

1. Introduction
Nowadays, computer worms threat is considered as one of the main profit scheme for cyber criminals to earn money and one key of threats to the Internet users. Computer worm was growth recently and emerged into multiple forms such as ransomware. This evolution result is a new types of ransomware which combines the usage of vulnerable points with worm such as spreading mechanisms to propagate in local networks and internet. [1]

Therefore, from the research perspective, worms require a huge study to analyze its features and behavior which construct an important field to enter malware analysis tools. This paper presents here the capabilities of the lime worm by executing it and applies it in practical (ethically) in a lab. The paper performs a compressive static analysis of this malware. This analysis results are used to detect the worm and can be used to design and implement software to worm detection and mitigation mechanisms .In addition to the ability of detection and the way to deal with this kind of threat, the presented techniques are applicable also in the cases of other worms with characteristics similar to lime. [1]

2. Background
The Basics of computer worms (one type of malwares) are standalone malicious code that can copy itself and infect additional computers by spreading through a network[2]. These worms can do different tasks. These tasks could be for ransomware, leak information, remote desktop control …etc.

Lime is a worm that built as a client-server model, it is especially a ransomware-type discovered by malware security researcher. Lime worm (client) after its execution (in victim side), sends an acknowledge to the server. At server side, the malicious guy can do many tasks like: monitoring the victim computer, full control …etc.

One of the most dangerous tasks that can do the server by utilizing this worm is encrypting the private files of the victim. Lime encrypts most data and appends filenames with the "Lime" extension (e.g., "ABC.jpg" is renamed "ABC.jpg.Lime"). Once files are encrypted, they become unusable. After
successfully encrypting data, Lime places two files on the desktop: 1) ":BackGround.png" [also set as the desktop wallpaper], and; 2) ":Decryptor.exe" [opens a file decryption tool]. The new files contain ransom-demand messages that inform victims of the encryption and encourage them to pay a ransom of $100 (in Bitcoins) in exchange for file decryption. The lifecycle of modern ransomware typically consists of four stages: distribution, infection, communications, file search, file encryption, and ransom demand [3].

3. Related Work
David at el [4] shows six vital static features. These features are extracted from the structure of the executable segments codes. These features were used to classify files as benign or malware. The features are file information, size of the image, header size, file alignment, section alignment, and addition to compilation time.

Wang at el [5] presented a SVM method for detecting the malware. New PE malware can be detected using this method. The paper uses static analysis. After extracting the selected PE features, these features are used for training the SVM classifier. Depending on trained SVM method, PE file can be classified as malicious or benign.

A. Kumar at el [6] paper presented an integrated method of both kinds of analyzing which are static and dynamic. The paper also showed that machine learning for the results of these analysis can increase the accuracy to detect the malware.

4. Malware Analysis
This section will discussed the benefits and goals of malware analysis, then impact on analysis types for malware, static analysis and dynamic analysis.

4.1. The Goals of Malware Analysis
The goal of malware analysis procedure is to supply the information required to distinguish the effects of the malware besides the ability to build a software for discovering or even deleting that malware. This needs to find exactly what a specific suspect executing file can do, how to discover it on the network, and how to know the degree of its damage[7]. Both host-based malware and network malware signatures can be obtained by analysis. While host based signatures (indicators) can be used to find the malicious code on victim computers which effect on files or specific changes to the registry, Network signatures can be identified to find the malicious code by observing the traffic of network. So, without analyzing the malware, the analyzer can get the Network signatures. Getting the signatures and the behavior of malwares are the goal for the analyzer.

4.2. Malware Analysis Techniques
Common techniques are used to analyze many different malwares. The executable malware cannot be directly recognized by human. Instead, the analyzer has to use many different tools and even tricks to find the required information. Two main techniques are used for analysis:

4.2.1. Static Analysis
In this type, the analyzer does not execute the suspicious file. Instead, the analyzer performs the analysis on the structure bases of the executable file. These files have many static attributes specially those related to memory compactness.

4.2.2. Dynamic Analysis
In this type, the analyzer executes the malware file in a dynamic prepared control environment and observes the malware behavior. Of course, the malware will try to get more privileged from operating system and will try to make a change in the registry. The analyzer put an agent in this environment that logs the malware behavior. Unfortunately, some malwares
have intelligence that detect the malware are executed in virtual environment and then change its behavior.

5. Malware Detection Technique
There are two basic categories of detection techniques: misuse and anomaly detections. In the first type, the systems are using specific signatures to find known attacks. This type of technique has an advantage which is the high accuracy in detecting the well-known attacks. Unfortunately, this technique cannot detect new types of attacks that do not have their patterns. While latter one, study the normal behavior activities and any event that out of this area is considered as malicious. Thus, this technique can detect new types of malwares. Unfortunately, anomaly detection can generate more false alarms [8].

6. Case study: Lime worm
Lime ransomware was a client server worm that work on specific port on computer network and the spearred over the internet without user knowledge, it is a remote access control worm, so the attacker can manage victim computer from his own computer over the internet. Lime worm has the ability to do the following malicious activities on victim machine:

6.1. Ransomware: Lime worm has the ability to encrypt victim files using encryption algorithms, then the attacker ask for money from victim user, this can be done by manipulating with bit coin addresses to gain profit with very difficult foot printing.

6.2. Remote Desktop: Lime worm can monitor every event in victim computer using remote desktop ability. The worm can not only monitor events, it can even have full control on the remote computer such as:
- Run a file on victim computer.
- Restart victim computer.
- Shutdown victim computer.
- Update the worm that’s infecting victim computer.
- Steal passwords from victim computer.
The attacker can determine window size and quality of remote desktop operation during monitoring all actions done by user who use victim machine.

6.3. Gathering information: The type of attack used by Lime worm has the ability to get all system information about the victim computer like:
- User: include (computer name, user name, worm id,…etc.).
- Windows: include (windows name, windows version, windows architecture, windows product key).
- Specification: include (machine type, Cpu name, Gpu name …etc.).

And also information about the worm in victim computer such as country, IP address, installation date, ransomware status and others. In addition to USB spread capability of the worm over USB ports to increase the probability of infection and to enlarge attacker malicious network activity. This paper focuses on static analysis of worm using varies tools and behavior analysis using ethical hacking in order to design and implement detection program on users computers.

Lime worm v0.5.8D was downloaded for using it in real implementation in lab ,to achieve ethical hacking by create a worm then use it to infect other computer in our lab (ethically ) for educational purpose and to study the effects of this worm activities. Lime worm server was shown in figure 1.
7. Worm analysis

In this section, static analysis of Lime worm was done in several manners using several tools of malware static analysis. Many samples of Lime worms was created by researchers using Lime builder in Lime worm server v0.5.8D, after build operation is done, a malware Lime worm ransomware was created as (sample.exe) which will be analyzed in our paper. Static analysis was done using varies methods and useful tools of analysis in order to gain maximum amount of information about the worm to use it later for detection process in the final part of the work.

The methods which are used for static analysis are:

1. Hash code:
The first step in malware static analysis is compute hash function for the malware. Hash my files tool was used to find multiple types of hash code of Lime worm (MD5, SH1, SHA256). The obtained results described in figure 2 that explained all information about the file (sample.exe).

The important note here that must be taken into account is that hash code is unique and it will vary every time attacker make any changes to the attribute of the file such as time and size and any other characteristic of the file.

2. Online analysis:
The obtained hash code from (1) was tested online initially to know this file is malware or not using online tool “virus total” as shown in figure 3, which accept a hash function of any file then compare it with its malware database to decide if the file is malicious or not. But when the hash code of the file
(sample .exe) was entered, the result becomes as: “No matches found”, Which mean that the file is not malicious.

![Hash search in virus total database](image1)

**Figure 3:** Hash search in virus total database

This result was expected because hash function differ every time you build a malware, to overcome this the hash function must computed and tested for the persistence process that is called run when the worm run in the victim machine. Another way to use online analysis in useful manner is to upload the file (sample.exe) to “virus total” online tool, which will analyze the file using multiple antivirus engines and gives how many antivirus engine was able to detect that this file malicious as shown in figure 4 and which antivirus decide that file is benign as shown in figure 5.

![Antivirus engines which detect file as malicious](image2)

**Figure 4:** Antivirus engines which detect file as malicious
Although this information are useful but it is still insufficient, to have the ability to design and implement an active detection program tool for this type of malware.

3. PeStudio tool:
To get more deep analysis of lime worm, PeStudio tool version 9.00 was used to analyze the malware (sample.exe). This tool gives a precise important information about the file, like file header with description if file run in dos mode or in windows and gives indicators about suspicious details founded in file like DLL file, finally this tool gives information about all strings exists in this PE with warning about some strings that is may be used for hacking purpose.

One of the most important information gotten from PeStudio are indicators which presented in figure 6. This figure explain that there are 4 urgent indicators in this file, some related with black list strings in the file, others for URL that this file will referred to when executed.

While figure 7 below shows and explain the strings used into (sample.exe) and classified it as blacklist strings and give hints for some strings with all string values. Lime worm has 24 black list strings in their file with 31 hints about other string from total 458 string exist in worm file.
Ethical hacking process is to done hacking with knowledge of victim in ethical way using professional manner, it is also to study and find risks and vulnerabilities of specific malware and give some suggestion to improve it. This process will be very useful and helpful for malware analyst to extract information to use it in next step which is detection process implementation for Lime worm in this paper. To perform the real analysis, ethical hacking was implemented in a lab using two laptop computers, one computer for server which Lime worm 0.5.8D must be downloaded and install on it, after infection, attacker will control all victim computers which infected with this worm through this computer, then the attacker have the ability to do all types of malicious activities on victim computer. The other computer (Laptop) is the victim computer which will be infected and study worm behavior on it.

In order to implement ethical hacking, first a worm file must be created at server computer using Lime worm server 0.5.8D, an important thing must be taken into account is next steps are for educational purpose only, So anyone must do not try to run it on his computer and any damage happened from try to check it ,the researchers are not responsible of it.

First step is run Lime worm .exe, then a window displayed on the screen ask attacker to specify port number as shown in figure 8. Port number 8989 was selected then when ok button pressed another window appears ask for password from attacker to enter to main server window of Lime worm.

Figure 7: Black list and hint strings in lime

Figure 8: Select port number
Then builder tab was selected to create worm (shown in figure 9) used to infect victim computer in ethical hacking process. In builder the first text box ask attacker to enter a “Paste bin raw URL” which must attacker get it to ensure that worm will connect with server after infection completed in victim computer. The attacker must visit “Pastebin .com” in order to resolve its public IP address (real IP) to equivalent URL to use it in Lime worm builder.

Figure 9: Lime worm Builder

Lime builder window permit to attacker to select some of other characteristics such as bitcoin URL and USB spread capability of the worm. Later attacker can select an icon for its worm created to ensure and add some obfuscation properties to the created file. Finally by select “Build” button by attacker, the server display message explains that worm creator was not responsible for any action or damage caused by using this software. After agreement and select YES, a worm file “worm .exe” will created and ready for infect users’ computers.

The worm file “worm .exe” was copied to a flash disk memory and pasted on victim computer on our lab. Later this file is run on victim computer which will result a connection between server and victim computer, attacker will find a row of information explain that there is a victim computer connected with it with information about country and IP address and other about victim computer.

Finally, by right click on this victim computer by attacker as explain in figure 10, attacker has fully control on victim machine and he can implement any malicious activity on victim computer which explained previously in this paper.

Figure 10: Attacker control after victim infection
When select remote desktop, the attacker will see victim computer screen on his computer screen. So, attacker can monitor every event done by victim user on his infected computer which made the attacker be able to steal sensitive information from victim computer such as passwords and license key. In addition, the attacker can select ransom to encrypt files on victim machine and ask for money to decrypt it later.

After study, the implementation of worm on victim computer for many times making many experiments on it, and monitor files and folders created in the windows operating system of the victim machine. Researchers are found that Lime worm file when executed, it was creating a child process called “Lime.exe” stored at the location (path): “C:\users\.....\appdata\roaming\my folder” which is created and run when worm is executed. From this point of view and depend on all information collected from all types and tools of analysis used in this paper, now researchers are able to switch to final step which is detection of lime worm on users computers. It is worth noting that ethical hacking process implementation is considered as dynamic analysis because the malware was run at victim machine and researchers are able to monitor and find every events effect on victim machine.

9. Worm Detection
Lime worm ransomware detection program was designed depending on all information gathering through analysis steps, which have been done in this research. Now, it is time to say that every notice and piece of information has been very useful in detection phase. The detection program done using visual C# programming language, which its main window was shown in figure 11.

![Figure 11: Lime worm program detection window](image)

System button will check the operating system of user’s computers, then decide if that computer has lime worm through message box, or user’s computer was clean from this worm.

10. Conclusion
The researchers deal with real effects of the lime worm by executing it in a real lab. This is due to that some worms are changed their behavior when using under virtual machines. The paper presents that Static analysis for this worm is very useful and can get the key information which can be used later for detecting that dangerous worm. This type of analysis got accurate results for detection that type of worms. The analysis is performed by using different tools. Every tool was used for specific purposes. Although the same tools can be used for similar worms, another worms need more sophisticated tools.
This work can be a core for building database for malware signatures and developing a software uses that database for detecting many malware files.

11. Future work
This type of analysis can be applied for other types of malware. The researchers can also use more tools and find the capabilities for each one. Another type of analysis (dynamic) can also be used to discover the effects of many malwares on the computer resourced and how these malware are spreading.

12. Acknowledgment
Special thanks to University of Mosul and the computer Science Dept. for their Supporting us and provide computer laboratories.

References
[1] Maxat O, Vassilios V., et.al, 2018, "Static and dynamic analysis of WannaCry ransomware", in Proc. IEICE Inform. and Commun. Technol. Forum ICTF 2018, Graz, Austria.,
[2] Asmaa H., sunds A,, 2013, "design monitoring tool for Mosul university network to detect computer worms", alrafidain journal, Vol 10.
[3] Akbanov M, Vassilakis V, Logothetis MD., 2019, "analysis of infection, persistence, recovery, prevention and propagation mechanisms", J Telecommun Inf Technol. pp:113-124.
[4] David, B., Filiol, E., & Gallienne, K., 2017, "Structural analysis of binary executable headers for malware detection optimization", Journal of Computer Virology and Hacking Techniques, 13(2), 87-93.
[5] Wang, T., Wu, C., & Hsieh, C. , 2009, “Detecting unknown malicious executables using portable executable headers”. In INC, IMS and IDC, 2009. NCM09. Fifth International Joint Conference on (pp. 278-284). IEEE.
[6] Jain, A., & Singh, A., 2017, “Integrated Malware analysis using machine learning”. In 2017 2nd International Conference on Telecommunication and Networks (TEL-NET) (pp. 1- 8). IEEE.
[7] Chandan K., Lalitha B., 2017, "International Journal of Information Security and Privacy", Volume 11 Issue 4, Pages 47-64.
[8] Muhammad I, Muhammad H., Maliha I., 2019, "Static and Dynamic Malware Analysis Using Machine Learning", 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST).