Malware and Malware Analysis

Md Sameull Islam

Department of Computer Science

American International University-Bangladesh

Dhaka, Bangladesh

soykot.ch@gmail.com

Khandakar Anim Hassan Adnan

Department of Computer Science

American International University-Bangladesh

Dhaka, Bangladesh

khandakar.adnan21@gmail.com

***Abstract*—Now a days the most serious threat on internet is malware. Malware word comes from two words. If malware word is splitted, "mal" can come from malicious and "ware" can come from software. That means, malware is a "Malicious Software". It is also a software or program or file that is a serious threat for a computer. It is generally designed by cybercriminals. There are many types of malware. Different types of malware has the different types of mechanism but their work principle is same. Malware can work in variety of way or perform different functionality like as delete computer data, stealing computer data, encrypt data of computer and many kinds of functionality. Malware attacks are increasing day by day so it is high time to do malware analysis to know the types, nature and mechanism of malware. There are two kinds of methods for malware analysis such as "Static Analysis" and "Dynamic Analysis". This paper shows the overview of different types of malware and also analysis of malware.**

Keywords—malware, types of malware, malware analysis, static analysis, dynamically analysis.

I. INTRODUCTION

Malware is a type of software that is threat for a computer network. It is different than any other software that has the power to open out itself to the system network. It is not able to be detected and also ruin the infected system and system network. The machine performance goes down and that is cause a devastation of the network. When a computer is infected by malware then it is no longer to usable and sometimes malware can delete the important data of a computer. Sometimes by using malware cybercriminals can hijack computer data and at times cybercriminals can encrypt the computer data and they offer the user to give money to them for decrypting those data.

This paper is arranged as the ensue Section 2 gives the background of your research ; Section 3 organize the research questions ; Section 4 shows the analysis ; Section 5 concludes this research paper.

II. RELATED BACKGROUND

To gather data for this research paper we seek other research paper in google scholar. We discuss classification of malware and malware analysis in this paper. We also gather data from many digital libraries by helping of google scholar. Some data of this paper collect from many other websites and blog. Finally, we try to describe the possibility that is proposed.

III. RESEARCH QUESTION

There are many forms of malware. All the malwares have the same target and that is to interrupt the computer system. Now we can describe the classification of malware. And we can also discuss about the each malware mechanism and functionality. Generally, there are seven kinds of malwares. These are-

1. Virus
2. Worm
3. Backdoor
4. Trojan horse
5. User-level Rootkit

6. Kernel-level Rootkit
7. Blended Malware

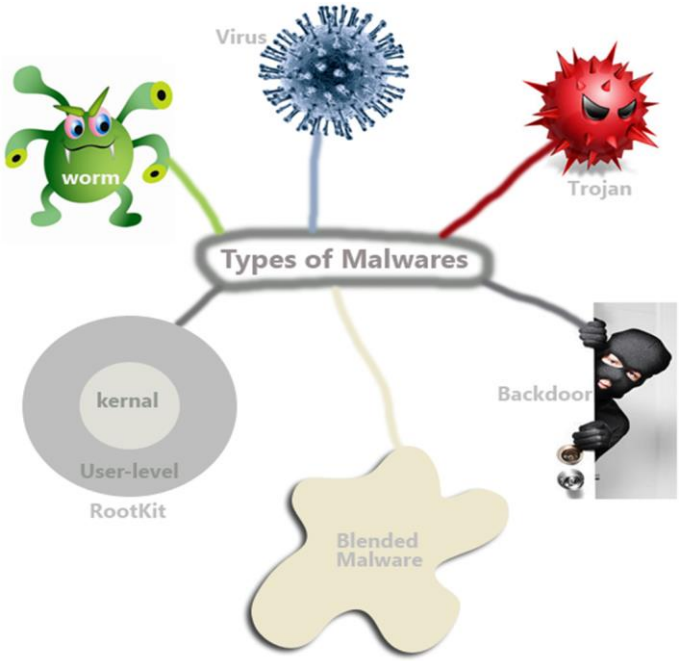

Figure-1: Types of Malware [1]

Virus: Virus can clone itself and attach with another program. This type of program is known as host because it assigns viruses itself. Viruses are activated when the user is in contact with the host program. Viruses cannot update themselves. It is updated by its creator.

Worm: Worm is also self-cloning codes as like virus. The main dissimilarity between worm and virus is that worm is activated without user interaction. Some worms are updated themselves. Systems and applications are attacked by the worms and infected systems and applications have well recognized vulnerabilities.

Backdoor: Backdoor is also a program. It has the power to bypass a system security. Cybercriminals installs it in a computer by type of program can be found in compromised system. Cybercriminals installs this type of program in compromised system to get remote control of the system.

Trojan horse: Trojan horse is one kind of malicious program. It has the power to appear like a legal program. This kind of malware observes the user activity and hijack user important data and also activate backdoor for cybercriminals. When a user downloads software from an open source it may be a Trojan horse program.

User-level Rootkit: This is another kind of malicious program. It can change the operating system equipment from user to user. Cybercriminals apply this sort of program to get access administrative or root level privilege. It always conceal itself prom the process list and change the operating system equipment.

Kernel-level Rootkit: Kernel-level rootkit is another kind of malware. It changes the operating system kernel level program. By this, it seizes the system calls. Even it do this type of changes remain hidden from the user. It is so troublesome to detect kernel-level rootkit program.

Blended Malware: This kind of malware has property of several types of malware. This type of program can be installed as a Trojan horse and works like viruses, worm and also activates backdoor for the cybercriminals in the hunting machine.

Now we will discuss about malware analysis. There are two types of methods for malware analysis. These are-

1. Static Analysis
2. Dynamic Analysis

Now we will discuss each of the analysis.

Static Analysis: Static malware analysis is a method

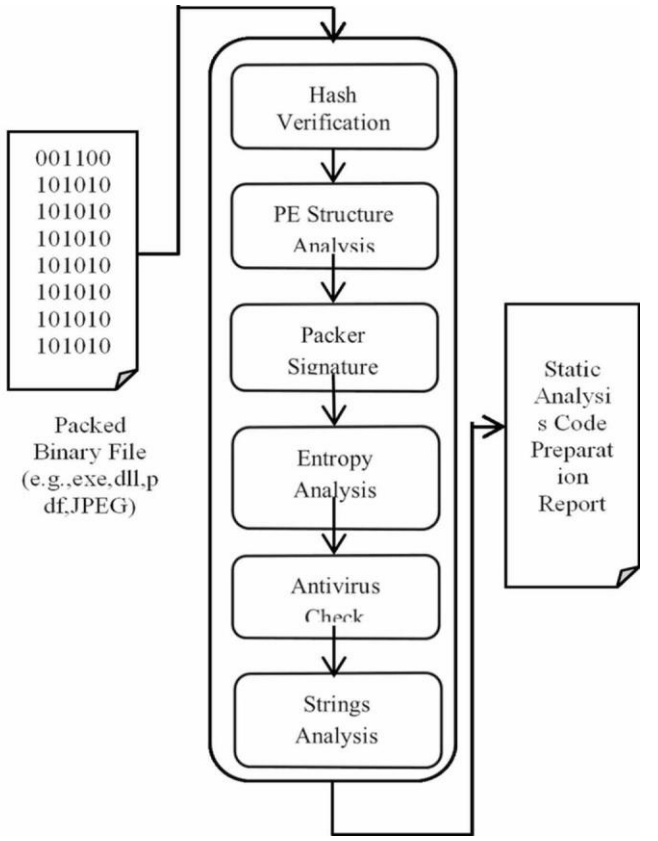

Figure-2: Structure of Static Malware Analysis [2]

to explore the malware binary file without any execution the code. It is generally accomplished by realizing the subscription of the binary code file and which is single identical for the binary code file and then calculating the cryptographic hash code of the file to realize the all equipment. [3]

Then the binary file is reverse-engineered by sending the file to a disassembler. Then the machine readable code can be transformed to an assembly code which is well recognized by the human being. Finally, the analyzer analyzes the assembly code and realizes the nature of the malware. [3]

Dynamic Analysis: This is another method to analyze the malware nature.

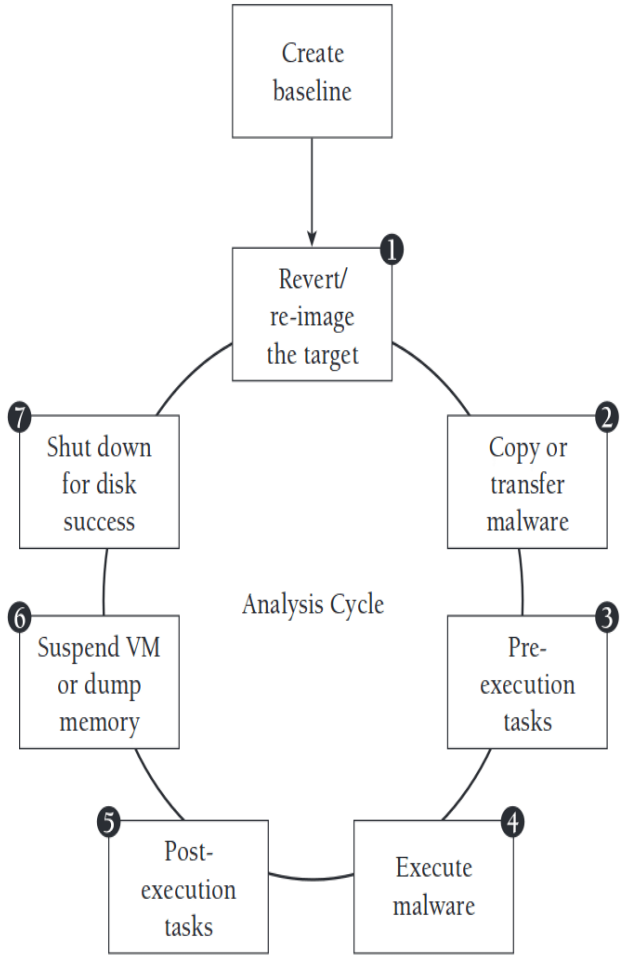

Figure-3: Structure of Dynamic Malware Analysis[4]

In this method, malware natures are analyzed by installing malware program in a virtual machine. Then the analyzer observes the malware functionality that how to change the machine condition by the effect of the malware. Finally, the analyzer takes a decision about the malware mechanism and its functionality. [3]

There are some key differences between Static analysis and Dynamic analysis. And these differences are given below-

Table-1: Static Analysis vs Dynamic Analysis

Static Analysis	Dynamic Analysis
Static analysis is done by using malware binary file without any execution.	Dynamic analysis is done by installing malware program in a virtual machine.
It uses Subscription-based malware analysis.	It uses Functioning-based malware analysis.
It is useless in opposition to sophisticated malware program and code.	It is efficient for all types of malware for analysis.

[3]

IV. ANALYSIS

Static based detection is the most extensively used in anti-virus technique. This type of anti-virus must sustain an assortment signatures of known as malware and an assortment can be updated if a new threats are revealed.

Dynamic based detection concentrates on the functionality that's are performed by malware during the execution. In this detection there are two phases such as training phase and testing phase. In training phase the malware file will be analyzed. In the testing or monitoring phase an execution file is classified as it is malware.

Static analysis is useless for some .exe files because it cannot get the binary code file. It is also useless for the corrupted file scanning. But the dynamic analysis is efficient for all types of malware analysis. In this method analyzer also see the current situation if machine is infected by malwares. And analyzer also see the live malware's functionality performing and how the machine can fall a risk situation in attacking situation. So dynamic analysis is better between the two methods of analysis.

If computer users follow some tools and techniques, they may be protected from malwares and these are-

- User should keep operating system up to date.
- User should use a firewall.
- User should not download or install software from unknown source.
- User may use any anti-virus software.
- User should secure the network.
- User should aware and think before clicking any link.
- User should not use any open Wi-Fi network.

V. CONCLUSION

Now we reached at the end of our paper. In this paper we discuss about malware, classification of malware and malware analysis. Malware is a harmful program. There are many types of malware. But generally there are seven kinds of malware. We have discussed about that. After the analysis of malware is discussed. There are two methods for analyze the malware. Finally one line can be said that, in present situation all the user of internet should aware all-time about the malware and know elaborately about malware nature, mechanism and functionality.

REFERENCES

[1] Definition of 7 Types of Malware

https://securitywing.com/definition-of-7-types-of-malware/

[2] Structure of static malware analysis

https://www.researchgate.net/figure/Structure-of-static-malware-analysis_fig2_332215777

[3] Difference Between Static Malware Analysis and Dynamic Malware Analysis

http://www.differencebetween.net/technology/difference-between-static-malware-analysis-and-dynamic-malware-analysis/?fbclid=IwAR0PCZ-jRcYVg4jLvvpENTUhx4VzIqCik97ZSfksQd2p2WNRMgQiUAR9d0c#ixzz5vW1wea3W

[4] Dynamic malware analysis

https://www.researchgate.net/figure/Dynamic-malware-analysis-34_fig1_316446553