Malware Analysis: Tools and Techniques

Rakesh Singh Kunwar
Raksha Shakti University
Ahmadabad, India, +919409369262
rakesh.singh.kunwar@gmail.com

Priyanka Sharma
Raksha Shakti University
Ahmadabad, India, +917874703993
ps.it@rsu.ac.in

ABSTRACT

Malicious code is a serious issue which regularly threatens the security of computer systems and act as a challenging task for cyber security& Information security personals. Malicious code is named differently according to their specification such as virus, worm, Trojan, Rootkit, spam etc. Risk factor due to malwares increases exponentially with the advancement in technology. Malware analysis is divided into code (static) analysis, behavioral (dynamic) analysis. It depends upon the investigator to use the different tools and techniques for analysis. Static analysis is first line of defense against malware which is composed of malware detector and scanners. With the advancement in technology, Malware developer uses different kind of techniques to maintain its source code hide from these detectors or scanner to find out hash value, finding strings, pattern matching etc. to identify the malware. Whereas, malware analyst decompress the packed file into unpacked file & investigate obfuscated malwares. In this paper, we try to investigate the different tool and techniques used in malware over practical working malwares.

CCS Concepts

Security and privacy → Malware and its mitigation

Keywords

Static Malware analysis, Dynamic Malware analysis, Threats, Security, Sandbox.

1. INTRODUCTION

Malware is any program or file which is harmful to a computer. It is mainly design to disrupt any computer operations, act as intruder to gather sensitive information, unauthorized private access to computer system or displaying undesirable advertisement. They are defined by their malicious intent because they act as a threat to the availability of the internet, integrity of internet hosts and the privacy of the internet users. Malwares may be stealthy, intended to snip information or scout the computer users for an extended period without legislative user.

Malwares comes in widespread range of variations like Virus, Worms, Trojan-horse. Rootkit, Backdoor, Key loggers, Ransomware, Botnet, Spyware, Adware etc.

Any malware may reveal the characteristics of multiple classes. Fig.1. shows the different types of viruses based on their classification:

1. Adware:. The least risky and most money-spinning Malware. It access the users system and displays ads on your computer.
2. Spyware: Spyware is a software that use to spies intentionally tracking the users internet activities in order to send advertising (Adware) back to the system[1].
3. Virus: A virus is ainfectious program or code that attaches itself to another piece of software, and then reproduces itself when that software is run. Most often this is spread by sharing software or files between computers [2].
4. Worm: It is a type of program which replicates itself and destroys all data and files on the computer. It does not alter files but silently resides in active memory and duplicates itself. Worms intend only to “eat” the system operating files and data files until the drive is empty.

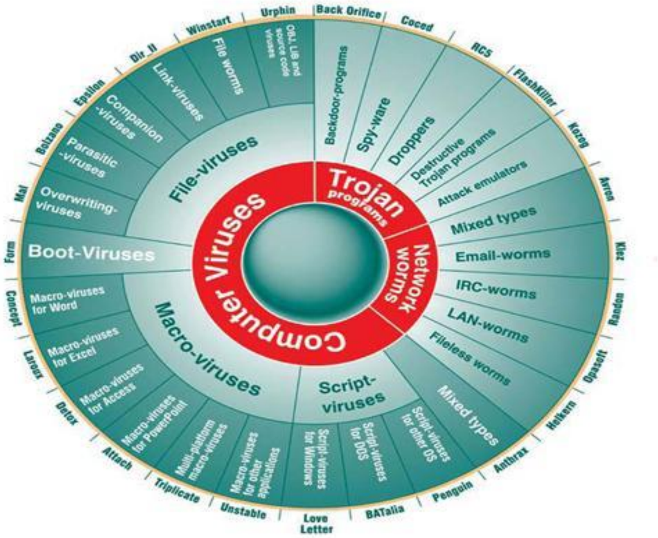

Figure 1. Classification of viruses, Trojan and Network worms [3].

5. Trojan: It is the most dangerous Malware which is written with the purpose of discovering your crucial information unauthorized access of computer’s system resources, and in larger systems creating a “denial-of-service attack ”[4].

ICTCS '16, March 04-05, 2016, Udaipur, India
© 2016 ACM. ISBN 978-1-4503-3962-9/16/03…$15.00
DOI: http://dx.doi.org/10.1145/2905055.2905361

6. Rootkit: It is a type of malicious software which is the hardest in all other Malware to detect and therefore to remove; it activate each time when the system boot up. It is hard to detect because it activates before the system operating system has completely booted up.
7. Backdoors: It is a method often secret much the same as Trojans or worms, except that they open a “backdoor” onto a computer which quietly providing a network connection for hackers or other Malware to enter or for viruses or SPAM to be sent.
8. **Keyloggers:** It is a type of spy software which have capability to records everything which is type on PC in order to capture log-in names, passwords, and other sensitive information and send it on to the source of the key logging program..
9. **Ransomware:** This type of malware restricts the user to access its infected computer system or mobile devices. Attacker encrypt the whole data and then block the device, in order to remove the restriction it demands the user to pay a ransom. The major problem is even after payment of ransomware to unlock the system, the system is unlocked, but it is not free of it locking out again.
10. **Botnet:** It is much similar to backdoor, it allows the attacker to access the infected system, but all system which are infected by the same botnet receive the same commands from a single command and control server.

The motivation behind the developing of malware is depend on different motives, sometimes the malware developer create it as a hobby which is not concern with financial matter but still damage in terms of data and cost. But financially motivated cyber crime only keep profit motive in their mind. Criminals make malware and other nasty software to make money.

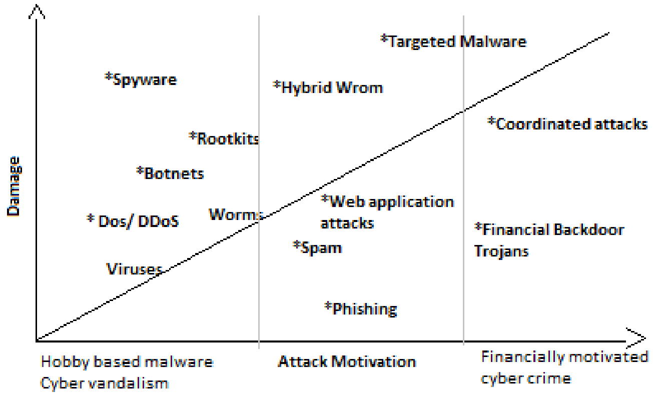

Figure 2. Attack vectors with their motivation [5].

2 MALWARE THREAT EVOLUTION :

With the significant growth in the volume and technical capabilities of cyberattacks. The conditions are persuasive to ignore . From last few year threats are evolved like a classic arms race, each time criminals develop new malwares to attacks, the security industry responding with new defenses and new techniques and so on.

The dark side of internet or “dark web” continuously fueling this race, making easy for criminals to share latest techniques and they learn from each other. There are some statistics taken from the McAfee Labs Threats Report which clearly show the evolution of Malware.

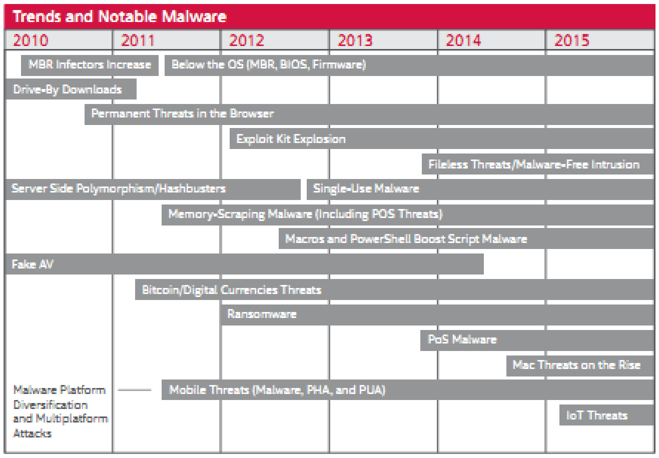

Figure 3. Trends and Notable Malware raises in specific years [6].

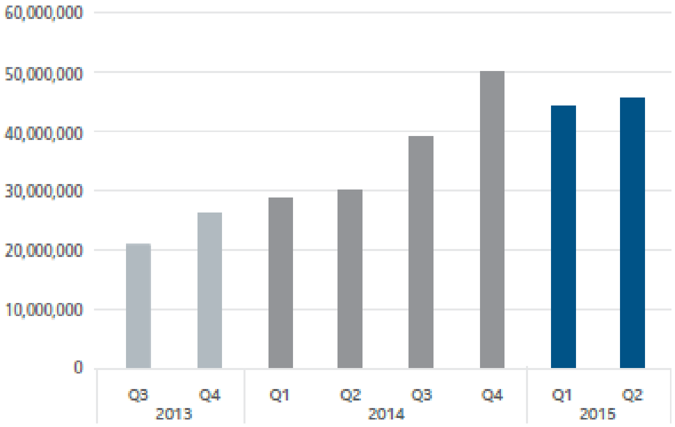

Figure.4. New Malwares created from 2013-Q3 to 2015-Q2 [6].

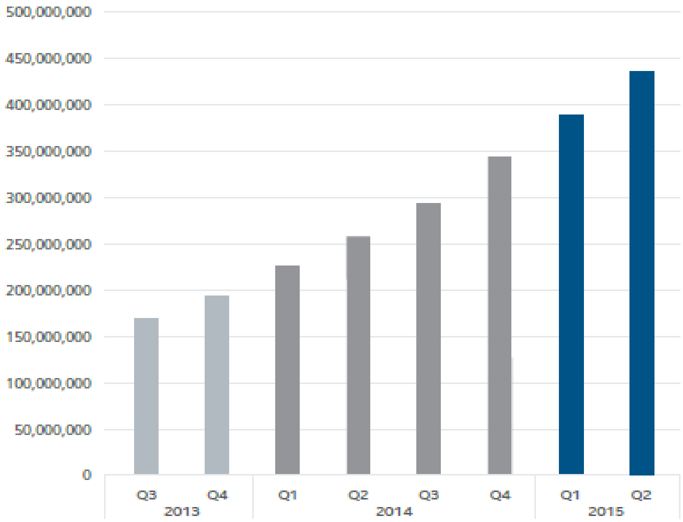

Figure.5. Total malware created from 2013-Q3 to 2015-Q2 [6].

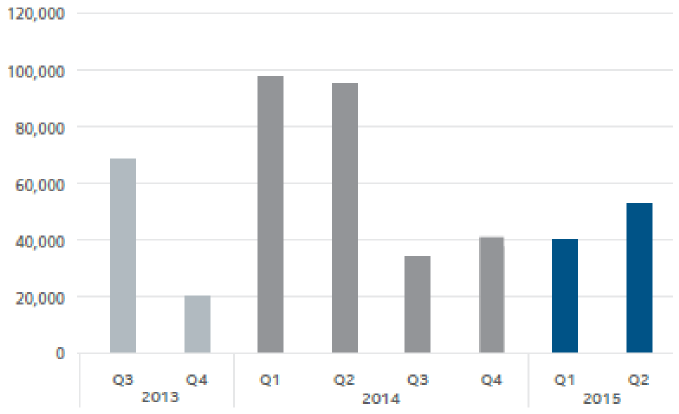

Figure.6. Total New Rootkit malware created from 2013-Q3 to 2015-Q2 [6].

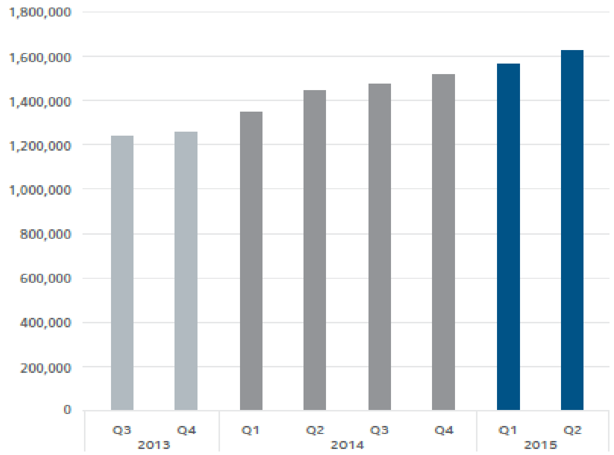

Figure.7. Total Rootkit malware created from 2013-Q3 to 2015-Q2 [6].

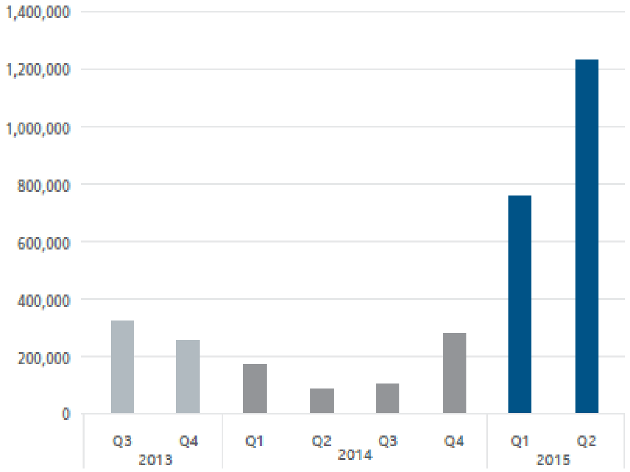

Figure.8. Total New Ransomware malware created from 2013-Q3 to 2015-Q2 [6].

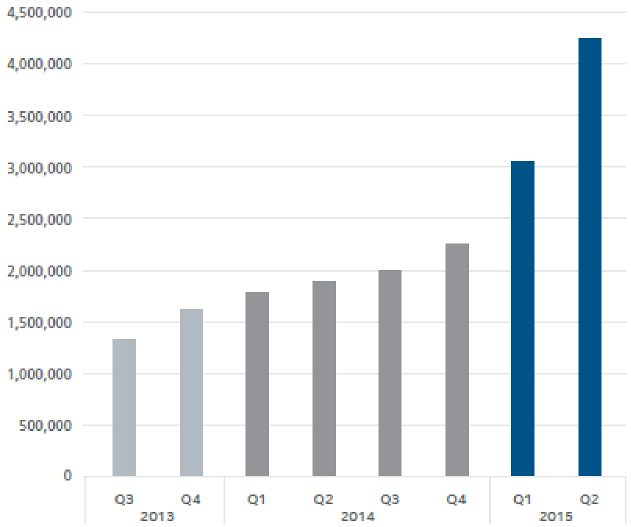

Figure.9. Total Ransomware malware created from 2013-Q3 to 2015-Q2 [6].

3 MALWARE ANALYSIS AND TOOLS:

Malware analysis is a process to determine the process and functionality of a particular malware .i.e. How it behaves and what is actual working?. This is important step to develop effective detection techniques for malicious code. Malware Analysis is basically are of two types code (static) analysis, behavioral (dynamic) analysis.

3.1 Static Malware Analysis:

Static malware analysis is used to examining the executable file without viewing the real instructions. It provides the information regarding functionality and sometime simple network signatures. Static analysis also consists of reverse-engineering of the malwares. In it executable file of malware is loaded in disassemble and program instructions are analyzed to understand the working.

Tools:

- VirusTotal: Its is a service which analyzes suspicious files and URLs and provide facility to quickly detect the viruses, worms, Trojans and all other viruses detected by antivirus engines.
- PE(Portable Executable) Analysis tools

    i. PEview [7].

    ii. FileAlyzer [8].

    iii. CFF Explorer [9]

    iv. PEstudio [10]

    V. Exeinfo PE [11]

- Dependancy Walker program. [12]
- Resource Hacker [13]
- IDA Pro: Interactive Disassemble Professional is an extremely powerful disassemble distributed by Hex-Rays [14].

3.2 Dynamic Malware Analysis:

This analysis technique involve to executing the malware and observing its behavior on the system in the controlled environment. It is used to analyze the infection process and producing effective signature. Dynamic malware analysis uses a debugger to examine the internal state of a running malicious file. This technique is used to find out the detail in more depth which requires specialized knowledge of disassembly, code constructs and windows operating system concepts.

Tools [15][16]:

- FileMon & RegMon.
- Process Monitor or procmon.
- Process Explorer
- ApateDNS
- Netcat
- Wireshark
- INetSim
- Ollydbg
- Sandboxes[17]:

  It is a security mechanism for executing untrusted malicious programs in safe environment. Using it provide a environment in which “real” physical systems are safe. It comprise virtualized environments in such a manner that ensure that the malware being tested will function normally. e.g:

  - Norman Sandbox
  - GFI Sandbox
  - Anubis
  - Malwr
  - Joe Sandbox
  - CWSandbox
  - ThreatExpert
  - BitBlaze
  - Cuckoo
  - IObit Cloud
  - ViCheck
  - Comodo MA

4. CONCLUSION

Malwares are acting as serious threats to the internet and computer systems. Malware developers are continuing updating and implementing new techniques to hide their malicious code. Coding is much easier and faster than detecting and analyzing the malware. Even dynamic malware analysis is times and resource intensive. So, It is necessary to counter the tradeoff between detection of malwares and analysis speed. So, In this paper we spot various tools regarding static and dynamic analysis which are used in the field of malware analysis.

5. REFERENCES

[1] K. Macharia, "How to Protect Your Device From Malware", http://allafrica.com/, 2016. [Online]. Available: http://allafrica .com/stories/201408260879.html. [Accessed: 09- Feb- 2016].

[2] J. Lad, "Basics of Cyber Security", http://www.slideshare.net/, 2014. [Online]. Available: http://www.slideshare.net/Jigarlad 050/basics-of-cyber-security. [Accessed: 11- Feb- 2016].

[3] A. Kriti,”Types of Malware”,http://www.foxtrot.in/types-of-malware/, 2015. [Online]. Available [Accessed:10- Feb- 2016].

[4] B. Hooper, "A Windows Upgrade, And Virus Definitions", http://islandconnectionnews.com/, 2015. [Online]. Available: http://islandconnectionnews.com/a-windows-upgrade-and-virus-definitions/. [Accessed: 09- Feb- 2016].

[5] S. Curry and A. Williams, "The Economics of Cybercrime and the Law of Malware Probability", http://www.slideshare.net/, 2010. [Online]. Available: http://www.slideshare.net/ RSA SecurityDivisionofEMC/cybercrime-and-malware-probability. [Accessed: 11- Feb- 2016].

[6] http://www.mcafee.com, "McAfee Labs Threats Report", 2014. [Online]. Available: http://www.mcafee.com/us/resources/ reports/rp-quarterly-threat-q3-2014.pdf. [Accessed: 10- Feb-2016].

[7] http://wjradburn.com/software/, "PEView", 2016. [Online]. Available: http://wjradburn.com/software/. [Accessed: 11- Feb-2016].

[8] https://www.safer-networking.org, "FileAlyzer", 2016. [Online].Available: https://www.safer-networking.org/products /filealyze/. [Accessed: 11- Feb- 2016].

[9] http://www.ntcore.com, "CFF Explorer", 2016. [Online]. Available: http://www.ntcore.com/exsuite.php. [Accessed: 12-Feb- 2016].

[10] https://www.winitor.com/, "pestudio", 2016. [Online]. Available: https://www.winitor.com/. [Accessed: 12- Feb-2016].

[11] http://exeinfo.atwebpages.com/, "Exeinfo PE by A.S.L", 2016. [Online]. Available: http://exeinfo.atwebpages.com/. [Accessed: 12- Feb- 2016].

[12] www.dependencywalker.com/, "Dependancy Walker", 2016. [Online]. Available: http://www.dependencywalker.com/. [Accessed: 11- Feb- 2016].

[13] A. johnson's, http://www.angusj.com, 2016. [Online]. Available: http://www.angusj.com/resourcehacker/. [Accessed: 12- Feb- 2016].

[14] http://www.hex-rays.com/idapro/idasownfreeware.htm

[15] https://zeltser.com, "Free Automated Malware Analysis Sandboxes and Services", 2016. [Online]. Available: https://zeltser.com/automated-malware-analysis/. [Accessed: 12- Feb- 2016].

[16] https://github.com, "awesome-malware-analysis", 2016. [Online]. Available: https://github.com/rshipp/awesome-malware-analysis. [Accessed: 12- Feb- 2016].

[17] H. Kromer, "Choosing the best Sandbox for malware analysis", http://kromer.pl, 2016. [Online]. Available: http://kromer.pl/malware-analysis/choosing-th-best-sandbox-for-malware-analysis/. [Accessed: 12- Feb- 2016].