A Review Paper on Detection and Analysis of Malware using Memory Forensics

[1]Khushbu Kalgude, [2]Chandresh Parekh,

[1]Master Scholar, [2]Faculty,
[1]Department of Cyber Security,
[1] Raksha Shakti University, Ahmedabad, India

Abstract: Over the years, technology has changed almost everything. Increasing use of technology so that increase the technical or digital crime. Now we are becoming familiar with identity theft, hacking, cyber fraud, phishing, malware or cyber criminals to get access to a very important information or simply cyber-crime. Digital Forensics is knowledge of investigating and recovering evidence from digital devices using different tools. It has become very essential to investigate and identify root of cyber-attack or fileless malware attack. One of the popular techniques of investigating is Memory Forensics, which refers to analysis of volatile data in computer's memory dump. Investigators conduct necessary memory forensics to investigate and identify attacks or malicious behaviours that are not easily detectable on hard drive.

Keywords **- Computer forensic, Memory Forensic, Volatile Memory, Fileless Malware**

I. INTRODUCTION

Digital Forensics is knowledge of investigating and recovering evidence from digital devices using different tools. With the enhancement of technology, the cybercrime rate has increased drastically. To control the effects of such crimes digital forensics has gained popularity in recent years. In today's world, the dependency on computers is growing widely. Government agencies and private companies are attempting to protect themselves from cyber-attacks with digital defence techniques like encryption, firewalls and heuristic or signature scanning, etc. Meanwhile, the number of attacks that include sensitive military data centers, targeting power grids and stealing trade secrets from both private and public organizations continues to increase.

This research examines the area of analysis malware using volatile memory forensics as an important source of digital forensic evidence for investigators. Memory Forensics play important role in investigating Cybercrime. "That is why memory forensics is becoming critical to the analysis of malware and its functions."

Increasing Crime

- Malware development
- Malware distribution
- Botnet
- Underground market for crime-ware

Challenges

- Whole Drive Encryption
- Live-Response
- Distributed evidence
    - File system
    - Volatile data
    - Application & Database Logs
    - Network device logs

A constant scene in the space of malware insistence is memory pictures. Memory real sciences is the bit of PC awful conduct scene examination that segregates a PCs memory dump in order to withdraw attestation of harmful development. It is getting notoriety in the terrible conduct scene examination coordinate by goodness of the wealth of information found in pictures, which, when showed up differently in association with the dimension of circles, are in a general sense smaller.It is especially valuable when a hazard wires stealth measures against plate authentic sciences. As passed on by Ligh, "Confirmation will no ifs ands or buts exist on memory by then on plate since all dangerous code must be stacked into memory to execute". There are two central stages in performing memory criminology. The principal form is the secures of memory, and it unites tying down a memory picture utilizing procurement instruments, for instance, Memoryze and WinPMEM . A usable memory picture is in like route passed on as episode dumps when a structure crash occurs. Regardless, crash dumps contain less information in the image when showed up unmistakably in association with grungy dumps.

After an image is gotten, it is blue down in the second time of memory criminology using instruments, for instance, Volatility and Rekall. The present test in memory terrible conduct scene examination is the nonattendance of robotization. Yara rules is the standard elective for robotized malware region in memory pictures. Regardless, similar to stamp perceiving proof, it requires the rules for a manual for be joined into enthusiasm to have the capacity to see that perspective. To automate malware prominent affirmation in memory pictures, we propose a heuristic approach reliant on malware collectibles found in memory pictures. In this paper, we talk around three old rarities that we separated and amassed models for, achieving a precision of up to 96%. The old rarities we investigated are library keys changed by the malware, imported DLLs, and called API limits. Anyway other malware-perceiving outdated rarities exist, for instance, coordinate development and metadata, they either don't for the most part exist in memory.

II. Memory Forensic

Memory forensic is a part of Computer Forensic or Digital Forensic. Memory forensic means analysis of volatile data in a computer’s memory dump, using a memory image to determine information about running programs, the OS, and the overall state of a computer. It contains valuable forensics data in memory dump about the system before an incident occur. RAM data that can be used to identify the occurrence of incident and other key details about incident. Memory Forensics deals with collecting data from system memory (e.g., system registers, cache, RAM) in raw form and carving the data from the raw dump. The memory must be analysed for forensic information.

Three Methodology of Forensic:

1) **Acquisition:**

Acquisition is the act or process of gathering information and evidence. Starting, a gear make blocker is set up between the verification and the target drive to ensure that no adjustment to the principal evidence is possible at whatever point in the midst of the acquiring. We simply use sanitized (or clearly perfect) drives to secure confirmation. We moreover support hard drive encryption as an extra layer of security and comfort for our clients. Using industry-standard programming, an aggregate and indistinct 'logical picture' of each hard drive or other mechanized storing contraption is made.

The business standard MD5 and SHA-1 cryptographic hash limits are used to process hash regards (unique automated identifiers) for each limit contraption that is imaged. This system ensures our gathering that the forensically spared image of the source hard drive is checked as being undefined to the first. If the anchoring is coordinated adjacent, appropriate notes, photos, depictions of the scene, information concerning the systems under investigation and any additional essential information are taken with the accumulated verification.

2) **Authentication:**

To guarantee that the data acquired from a computer is a correct duplicate, it must be authenticated. Authentication is a process of ensuring that the acquired evidence is the same as the data that was originally seized. The legitimate check of mechanized chronicles has transformed into a fundamental bit of intuitive media logical examination, and has been of essential massiveness and regard both on a basic level investigate and sensible applications.The advance of the academic research in video criminological affirmation was portrayed.

Starting now and into the foreseeable future, sensible procedures for video criminological approval were researched and discussed in the reason for examinations on video metadata, substance, associated sounds and camcorder legitimate distinctive evidence. Finally, achievable game plans and future examples of rational video legitimate affirmation were shortened. Our work would provide sensible guidance to related monitors and experts in future case examinations and theoretical research.

3) **Analysis:**

Analysis is the process of examining and evaluating information. When examining computer files, it is vital that they aren't modified in any way. Forensic data analysis means scientific data analysis used for legal disputes. Using forensic data analysis ensures that legal disputes can be resolved by an unbiased, scientific methodology. This in turn helps enforcement of laws and regulations and aids public health.

Types of Memory Forensic:

1) Volatile Memory

Live data means Volatile data. Volatile data generally stays in RAM which would be lost if computer is turned off or restarted. The volatile data that can be recovered is date and time, running processes, network connections, network status, logged on users, doc files, email ids and login credentials, chatting messages, email messages, login credentials for social networking site, other accounts with login credentials, encryption keys, etc.

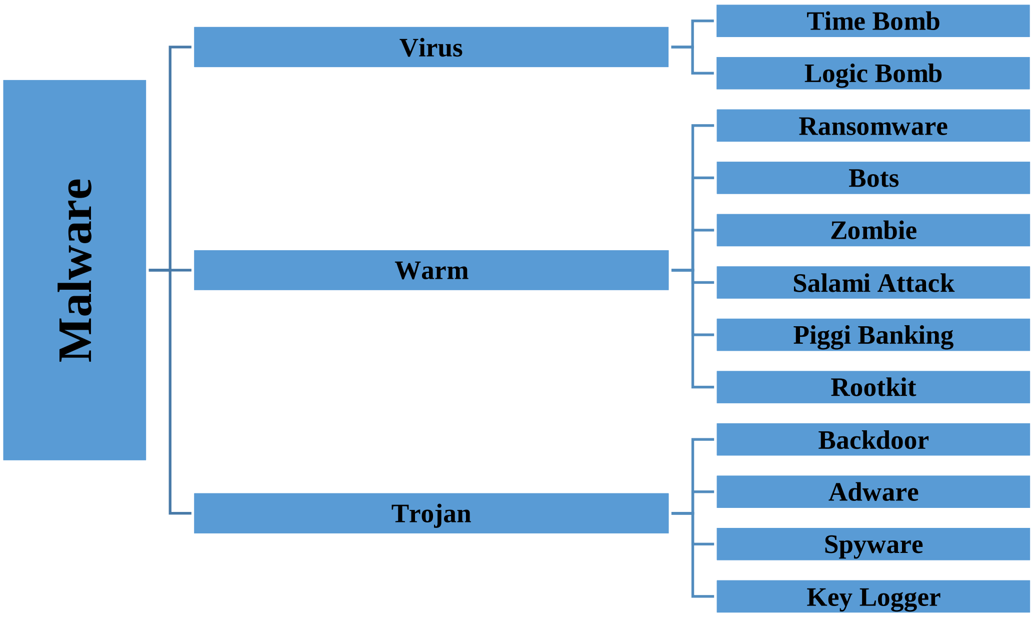
2) Non-Volatile Memory

A Non-Volatile memory (generally called a middle dump or system dump) is a delineation catch of PC memory data from an unequivocal minute. A memory dump can contain gainful legitimate sciences data about the state of the system before a scene, for instance, a mishap or security exchange off. Memory dumps contain RAM data that can be used to recognize the purpose behind a scene and other key bits of knowledge concerning what happened.

III. MALWARE

Malware is contractionary of malicious software or scripting code intentionally or Deliberately designed damage to a computer, server or computer network. Any program or file that is harmful to a computer user. Malware does the damage after it is established or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software.

Different Malware types:



(Fig. 1: Different types of Malware)

1) Virus

Virus is a program written to enter to your computer and damage/alter your files/data. A virus might corrupt or delete data on your computer. Viruses can also replicate themselves. A computer Virus is more dangerous than a computer worm as it makes changes or deletes your files while worms only replicates itself without making changes to your files/data. Viruses can enter to your computer as an attachment of images, greeting, or audio / video files. Viruses also enters through downloads on the Internet. They can be hidden in a free/trial softwares or other files that you download.

So before you download anything from internet be sure about it first. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, such as running an infected program to keep it going.

2) Warm

Worms are malicious tasks that make copies of themselves again and again on the area drive, compose shares, etc. The primary purpose behind the worm is to copy itself again and again. It doesn't hurt any data/record on the PC. As opposed to a disease, it doesn't need to affix itself to an ebb and flow program. Worms spread by abusing vulnerabilities in working structures as a result of its replication nature it takes a huge amount of room in the hard drive and eats up more cpu uses which therefore makes the pc too moderate in like manner exhausts more framework information exchange limit.

3) Trojan

A Trojan horse is not a virus. It is a destructive program that looks as a genuine application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans also open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.

Fileless Malware

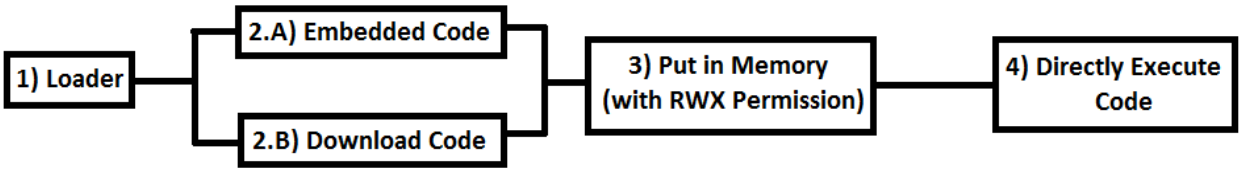
Fileless Malware is malware category. **“Fileless malware** is a variant of computer related malicious software that exists exclusively as a computer memory-based artefact i.e. in RAM. It does not write any part of its activity to the computer's hard drive meaning that it's very resistant to existing Anti-computer forensic strategies that incorporate file-based whitelisting, signature detection, hardware verification, pattern-analysis, time-stamping, etc., and leaves very little by way of evidence that could be used by digital forensic investigators to identify illegitimate activity.

How to fileless malware work:

The code for fileless malware is not stored in a file nor installed on the victim’s machine. Fileless malware loads directly into memory as system commands and run immediately. Often it will continue to run until the host device is powered down-putting a computer into standby mode won’t kill of the malware. The vast majority of fileless malware targets windows computers.

Current scenario in Fileless Malwre

- 2014-2015: Duqu 2.0
- 2016: PowerSniff, PowerWare
- 2017: POSHSPY
- 2018: PowerShell attack



(Fig. 2: Fileless attack’s typical infection Chain)

PowerShell Fileless Malware attack

Development by Microsoft. Windows Powershell is a task-based command-line shell and scripting language designed especially for system administration. Built on the .Net framework. **PowerShell** is an attacker's tool of choice for conducting fileless malware **attacks**. **PowerShell** is a powerful scripting language that provide unprecedented access to a machine's inner core, including unrestricted access to Windows APIs.

- Automation engine
- Command-line shell
- Scripting language

Reasons to attack on PowerShell

- ➢ PowerShell’s capabilities allow you to simplify and automate tedious and repetitive tasks by creating scripts and combining multiple commands together.
- ➢ It is the Microsoft standard for automation and Most Microsoft products will eventually use it. Many GUIs are PowerShell front ends.
- ➢ You can use PowerShell commands to manage your domains.

IV. MOTIVATION

Over the years, technology has changed almost everything. Increasing use of technology so that increase the technical or digital crime. Now we are becoming familiar with identity theft, hacking, cyber fraud, phishing, malware or cyber criminals to get access to a very important information or simply it’s one of the cyber-crime. The digital evidences are mostly found in crime-scene. Cyber forensic experts help us to prevent from cyber-crime. The application of investigation and analysis techniques to retrieve information from a computing device that is suitable for presentation in s court of law.

V. CONCLUSION AND FUTURE WORK

I conclude that now a day’s increase PowerShell Fileless malware attack in volatile memory forensic. so that I will try how to prevent and detect PowerShell attack in volatile memory using some tools. These review paper related to basic introduction about memory forensic and fileless malware.

VI. REFERENCES

Websites :

[1] https://www.dfrws.org/sites/default/files/session-files/prescurrent_cyber_investigation_challenges_in_digital_forensics.pdf
[2] bfa925a872.pdf" \h https://pdfs.semanticscholar.org/f140/f3bdb657f4dcfbfd4bf0183524bfa925a872.pdf
[3] https://www.coe.int/en/web/octopus/blog/-/blogs/live-data-forensics-or-why-volatile-data-can-be-crucial-for-your-cases/
[4] https://www.geeksforgeeks.org/types-computer-memory-ram-rom/
[5] https://www.quora.com/What-is-the-basic-difference-between-volatile-and-non-volatile
[6] https://www.darkreading.com/attacks-breaches/the-5-challenges-of-detecting-fileless-malware-attacks/a/d-id/1332557
[7] https://www.darkreading.com/endpoint/fileless-attacks-jump-94--in-first-half-of-2018/d/d-id/1332686
[8] https://www.google.com/search?ei=pKbYW5aRKZi6vwT1YuoBA&q=what+is+raw+data&oq=what+is+raw+data&gs_l=psy-ab.3..0l10.114793.115720.0.116447.3.3.0.0.0.0.344.603.2-1j1.2.0....0...1.1.64.psy-ab..1.2.602....0.XddCNP8WyHU
[9] https://zeltser.com/fileless-malware-beyond-buzzword/
[10] https://threatpost.com/threatlist-ransomware-attacks-down-fileless-malware-up-in-2018/136962/
[11] https://betanews.com/2018/08/28/fileless-malware-rises/
[12] https://www.peerlyst.com/posts/how-to-detect-advanced-volatile-threats-avt-and-fileless-malware-chiheb-chebbi

Papers :

1) Volatile Memory Forensics : A Legal Perspective
2) AUMFOR : Automated Memory Forensics for Malware Analysis
3) Memory Forensics : Tools Comparison
4) Live Memory Forensic Analysis