MALWARE ANALYSIS AND DETECTION USING MEMORY FORENSIC

Bansi Khilosiya
Student
Marwadi University
bansi.khilosiya105924@marwadiuniversity.ac.in

Kishan Makadiya
Assistant Professoe
Marwadi University
Kishan.makadiya@marwadieducation.edu.in

ABSTRACT

Malware harm to system, network, file-malware crime has used in cyber war , isolated malware depends on its symptoms ,and using malware cyber war has happened that depends on malware symptoms. After malware crime we could investigate malware footprint in memory such as advanced malware ,it's malware investigate using memory forensic via live and dead .if we could investigate malware in RAM and cache then live forensic and if we could find malware from hard disk. Then it is called dead forensics. Such a malware apt.rootkit, key- logger it is footprint we can Found Depends os we could find differ malware. There are four techniques of malware analysis: static malware analysis, dynamic malware analysis, advance static malware analysis, and advance dynamic malware analysis. After malware crime using memory but we could investigate malware footprint in memory depend on malware artifacts. Which has found only memory not anywhere in system such as a using file, network, client, server, application.

Keyword: Linux and Parrot OS, RAT Trojan Malware (Linux Malware) latest malware, live and dead forensics of memory.

1. INTRODUCTION

Malicious + Software = Malware, Malware Analysis and Memory forensic Have become a must have skill for fighting advanced malware, targeted attack, and security breaches. But what information has been stolen, how will this hurt to Business and this will only possible by investigation and forensics. A lot these answers might only be found through malware analysis and memory forensics. This forensics is used by security analysis to investigation sophisticated malware such as a root kit. Malware is harm to system, network, server, client, and file. While cyber warfare among countries has focused on Windows operating system so far, modern APT such as an advanced malware also aims at Mac OS X and other os also, Mac OS becomes no longer safe zone. Depends on malware or for symptoms of malware check we can use analysis tools using analysis all four techniques in analysis but after malware crime investigate malware footprint, but we could not found in system ,network and using file. Some advanced malware such as key logger ,apt, advanced persistent threat ,rootkit, we can found such malware footprint in memory if we could found in ram or cache then live forensic and if found

from hard disk then it' call dead forensic using differ OS such as Mac OS, parrot OS, windows, android, iOS, kali, cyber hawk, black-box.

2. OBJECTIVES

While we will do investigate after crime has happened and find malware footprint from memory not analysis only, it means memory forensic live as well dead both. With latest malware 2019 depends on os memory resident malware.

There are several types of malware:

- APT : advanced persistence threat
- key logger : data capture from key board
- rootkit : unauthorized access in kernel or memory and gather information
- adware : from advertisement gather information
- fileless : memory residence Malware
- downloader : from download link malware download and gather information
- spyware : replicate and gather information from victim
- RAT : remote access Trojan

There are four malware techniques to analysis of malware:

- Static analysis: via API calls static analysis has been done via API calls
- Dynamic analysis: via function calls dynamic analysis has been done.
- advanced static malware analysis: disassembler
- advanced dynamic malware analysis : Debugging

3. RESEARCHMETHODOLOGY

Which has malware find in memory it means symptoms of malware I have been take and take differ os parrot and compare between live and dead forensic with latest malware2019.

Which has malware find in memory it means symptoms of malware we will take and take differ os parrot and compare between live and dead forensic with latest malware2019.

Malware analysis using memory forensic, which has malware effect to memory cause all types of malware not effect to memory and we will take differ os parrot os with latest malware either 2019 or 2020. and compare between live and dead forensic using differ tool such as Lime and volatility.

Step 1: install free sweep game and make remote trojan access RAT and generate payload via meta sploit tool.

Step 2: using meta sploit tool and generate payload and spread malware to internet.

Step 3: gather information from victim system.

Step 4: live and dead forensics via time tool, volatility, wireshark.

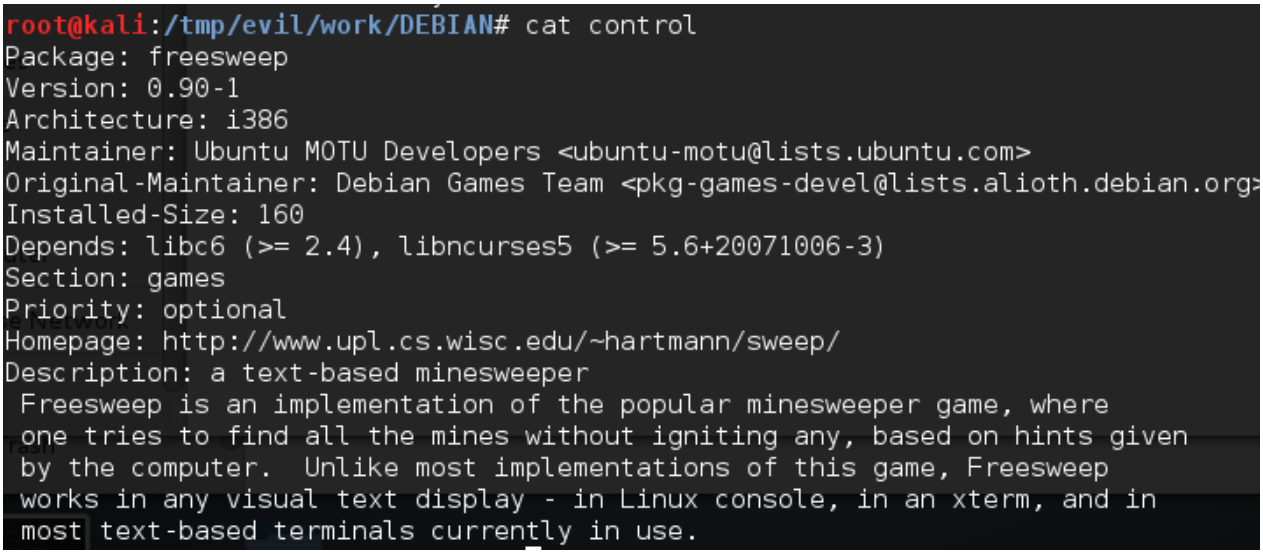

Figure 1: install game

```
root@kali:/tmp/evil/work/DEBIAN# cat postinst
#! /bin/sh
# postinst script for freesweep

set -e

scores=/var/games/sweeptimes
if [ ! -e $scores ] ; then
  touch $scores
  chown root:games $scores
  chmod 0664 $scores
fi

# Automatically added by dh_installmenu
if [ "$1" = "configure" ] && [ -x "`which update-menus 2>/dev/null`" ]; then
        update-menus
fi
# End automatically added section


exit 0
```

Figure 2: Postinst

Figure 3.3: generate payload

```
root@kali:~# msfvenom -a x86 --platform linux -p linux/x86/shell/reverse_tcp LHO
ST=172.21.42.106 LPORT=443 -b "\x00" -f elf -o /tmp/evil/work/usr/games/freeswee
p_scores
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 98 (iteration=0)
x86/shikata_ga_nai chosen with final size 98
Payload size: 98 bytes
Saved as: /tmp/evil/work/usr/games/freesweep_scores
```

Figure 3.4: start reverse handler

```
root@kali:/# msfconsole -q -x "use exploit/multi/handler;set payload linux/x86/s
hell/reverse_tcp;set LHOST 172.21.42.106;set LPORT 443;run;exit -y"
[-] Failed to connect to the database: could not connect to server: Connection r
efused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?

payload => linux/x86/shell/reverse_tcp
LHOST => 172.21.42.106
LPORT => 443
[*] Started reverse handler on 172.21.42.106:443
[*] Starting the payload handler...
```

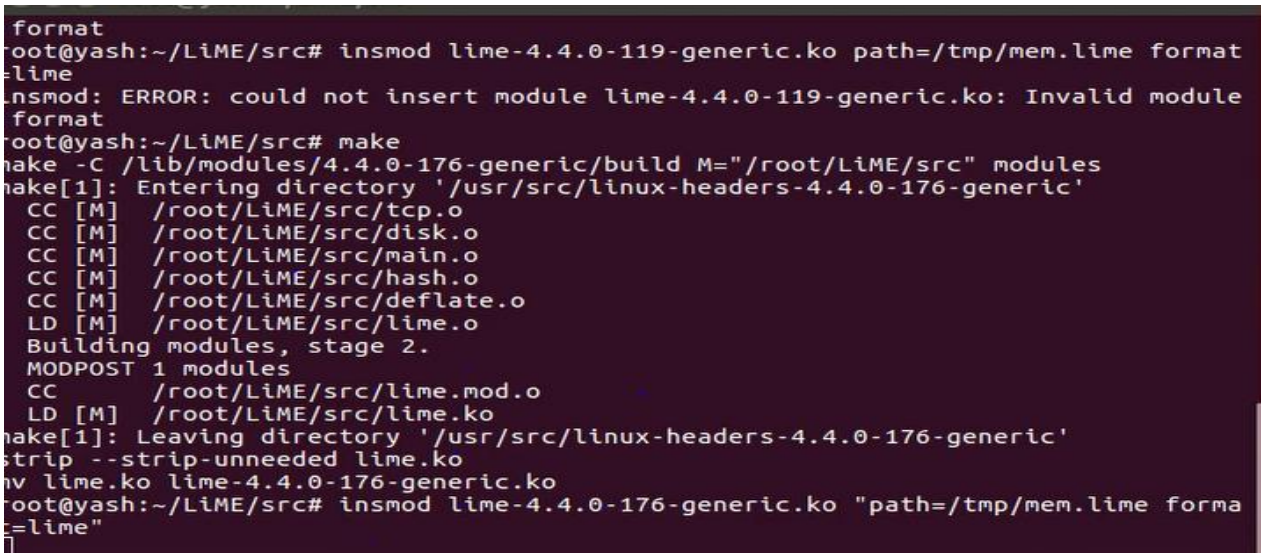

Figure 3.4: Memory Forensics using LiME tool

Malware Forensics:

We could analysis of malware via machine learning, forensics, and four malware analysis techniques.

Here we have did via forensics from memory live and dead forensics. If we have did gather data from RAM or cache, it is live forensics because data temporarily stored in RAM and cache. If we have did gather information from hard disk, then it is dead forensics. Because all the information stored in hard disk. And it is all about called artifacts of memory.

Investigation and find evidence

- Memory forensic: live and dead.
- Live forensic: Cache and RAM
- Dead forensic: Hard disk

Malware enter via source:

- File: exe file,.dll file, .bat file
- application and software: malicious code
- network through: Ransomware, adware downloader
- google forms, google link

4. LITERATUREREVIEW

4.1 Detect mac objective-C malware using memory forensics:

In this Paper forensic tool use Mac OS and detect objective -c malware for Mac OS malware analysis using memory forensic using volatility tool. So, in this they had detected Objective c detective malware. Objective malware is sophisticated malware. Using APIs, they had did active malicious

activity and gather information using sophisticated malware. And using Forensic tool volatility in Mac OS analysis and detect malware and criminal how crime had did that investigate.

4.2 Advanced Malware Analysis through Memory Forensic Technique:

Static analysis method has been complex method. Here in this paper use windows OS Here use static analysis and dynamic analysis and memory forensic all three method use in this paper. They have taken 200 malware samples. They have shown malware 40 malware Out of 200. VM ware, Virtual Box, Cuckoo sandbox, Volatility tool, IDA pro, Wireshark, Virus Total are the required tool for analysis. Some tool volatility for forensic purpose, Ida pro is for static analysis tool use, cuckoo sandbox is use for dynamic analysis. Many malware Trojan, RAT, Ransomware.

4.3 GPU-assisted malware effect using memory forensics:

In this paper GPU effect malware use. Here in this paper GPU-assisted malware detect. GPU assisted malware Symptoms to perform malicious activity and still information. They had used lime tool for forensic. Here window OS used and for forensic anti – forensic techniques use. GPU driver manage the kernel. Here they had never considered either malicious hardware or code JUST modified of the graphics card's Firmware.

4.4 AUMFOR: Automated Memory Forensics for Malware Analysis:

In this paper use AUMFOR is GUI memory forensic tool. Here they had did forensic in volatile memory RAM or cache that is why here used live forensic. AUMFOR tool is used for window and Linux OS. Here they had developed AUMFOR tool based on python language. Volatility tool is for live forensic OS malware memory forensic. This tool has benefit is no need commands. AUMFOR - Automated Memory Forensic tool is use for forensic investigator by performing all work itself.

4.5 Automated malware detection using artefacts in Forensic memory images:

Here in this paper cuckoo sandbox is use for automatic malware analysis. Using registry, APIs call, DLLS. Machine learning also use. Here they have taken memory dump. They have detected malware automatically Using CuckooSandbox.

4.6 Malware Detect using Artifacts of Memory dump and Dynamic Analysis:

Here in this paper for malware analysis using dynamic malware analysis. Using volatility tool and cuckoo sandbox they have detected and analysis of malware with machine learning. Using API call, DLL, Registry feature they have detected Malware. Adware, Ransom ware, Key logger, Downloader and Backdoor such malware found.

4.7 Android Malware Analysis Based On Memory Forensics:

In this paper they have taken android malware dynamic analysis and memory forensic techniques. They have found malicious malware using Trojan application such as backdoor. In this paper APKANALYZER is used for memory forensic tool for android. Ukatemi SHIELD is for analysis purpose of Android application. They are use Lime tool for capture memory images.

4.8 Review of Mobile Malware Forensic:

Here in this paper take mobile device for analysis of malware. Here they have taken mobile device for analysis of malware using forensic. Android and IOS mobile used for mobile forensics. Malware such as backdoor, viruses, worms, Trojans and spyware, botnet. They have taken Open Source Android Forensics (OSAF) tool for mobile forensic. They have OSAF tool for taken malware investigate with android application.

4.9 Rootkit detection using memory forensics:

MASHKA is physical tool used for rootkit detection. Malware Analysis System for Hidden Knotty Anomalies (MASHKA) is used for forensic purpose and this tool is anti-forensics tool. In this paper how to detect kernel level rootkit from the memory and also analysis of anti-root kit tools. Here in this paper they have taken window OS. They have taken Volatile memory dump it means live forensics.

4.10 Malware Analysis survey using Static, Dynamic, Hybrid and Memory Analysis:

Here in this paper they have used static malware analysis, dynamic malware analysis and analysis of memory .They have taken several malware such as virus, worms, Trojan, spyware, root kit, ransom ware, adware, botnet. In this paper they have taken static analysis using API calls, opcode and in dynamic analysis using function call and function parameter. And memory analysis using memory analysis using DLL, Registry key, and network connection. In this paper they have used two type of malware detection method one is the signature-based detection and second is Heuristic-based Detection.

4.11 Smartphone Volatile live Memory forensics:

Here in this paper they have taken mobile device IOS and Android. And they have done live forensic in volatile memory. They had taken This all are parameter such as a Contacts list, emails, messages, downloaded confidential documents from email attachment via malware of mobile android and IOS mobile. They have done comparison between android and IOS Device with raw volatile memory it is live forensic.

4.12 Malware analysis using Memory forensic via virtual machine introspection tool:

In this paper VM Introspection Tool is used for forensics. Using this tool, they had done Forensic. This tool is used for both live forensic and dead forensic of malware. Due to malware cyber-attack Happened therefore they has developed tool for forensic purpose. First, they had run vulnerable software and run malware exploit and write to memory and target to VM. Third task is read to memory VM. And last one is run to tools for observation of Event.

4.13 Detection Automatic Analysis and identify using Malware Processes in Forensics via DLLs.

In This paper they had done forensic using DLL dynamic link Libraries .malware forensic collect evidence and data recovery using Volatility tool. In this paper they had recovered how to restore processes, system registry, network Information and files that all the information Recovered from memory. Cause forensics it means live and dead forensics and investigate, find evidence, recovered data this all are we have to check while we will forensics.

4.14 Detecting Malware and Root kit via Memory Forensics

In this paper they had taken malware and rootkit for detection. That malware is effect to memory. And steal information of victim. They had used VMI Virtual machine introspection. VMI system is used for detecting hidden process.

4.15 Formality: Automated Forensic Malware Analysis using volatility:

Here in this paper they had taken volatility tool for investigate using memory forensic. And they had investigated in RAM memory its live forensic .in this paper for steal information they had inject

ransomware, and botnet. They had taken RAM Dump form RAM Memory that was live forensics.in this paper they had taken 5 various malware samples.

5.ANALYSISPART

Table 1: ANALYSIS

Basic Static analysis	Basic dynamic analysis	Advance static analysis	Advance dynamic analysis	Forensics
API CALLS Opcode	Function call Function parameter Information traces	Disassembler using IDA Analysis of the linked libraries	Debugging Analysis on registry	DLL Registry Network connection.
PEview PEid Md5deep Virus total	COMODO ANUBIS Virtual box	Bintext Ida pro	OlldbgRegshot	Volatility Lime GRR Remnux

6. FINDINGS

Using static and dynamic tool we could not did forensic, for forensic we should be take differ tool such as volatility, Lime tool, GRR for live and dead forensic. And also find latest malware depends on os.cause depends on OS. We could find malware according to malware symptoms. And also check which malware effect to in memory is. And we will find evidence from memory. Here there are some tools for forensics purpose:

- Meta sploit tool

  Here we have used meta-sploit tool to generate payload and spread malware into internet and gather information from victim.

- lime tool

  It is use for live forensics. This tool is use for live forensics.

- volatility tool

  It is use for forensics purpose, but this tool is convert into readable format.

- wireshark tool

  This tool is use for also forensics purpose.

  Two techniques for gather information from kernel and memory via rootkit

There are two techniques of hooking:

- IAT hooking
  Malware harm to system using two techniques (1) IAT hooking and (2) inline hooking.

- Inline hooking:
  They both techniques IAT and inline hooking use gather data from kernel and memory.

Table 6.1: FINDINGS PARAMETERS

Sr. No.	OS	Malware analysis techniques	Techniques for malware detection	Analysis tool	Forensics tool
1	Window	Static malware analysis	machine learning	IDA Pro	Lime
2	MAC	Dynamic malware analysis	forensics	Cuckoo sand box.	Volatility
3	IoS	Dynamic malware analysis	Via four Malware analysis techniques	PEid	Wireshark
4	Android	Static malware analysis		PEview	
5	Linux				
6	Parrot				

6.2 Diagram of Malware Analysis using memory Forensics:

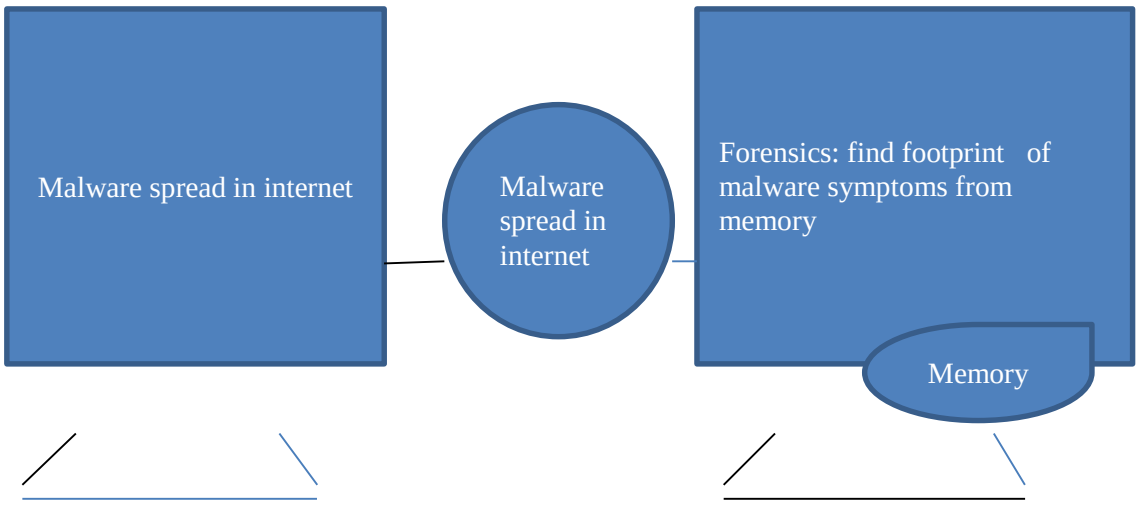

Figure 6.2 : how to malware spread in internet and Forensics via memory

7. CONCLUSION:

We have conclude we can find malware in memory but after attack and crime and we can find malware evidence and footprint in memory-investigation(memory forensic)-via using different method and tool of malware analysis and memory forensic for both and use different os for research work.

Via malware crime it would be not possible to recover the data. So, via malware crime not possible to recovery. May be some time it will possibly find other techniques and find tools .via modern anti -techniques perhaps it will possible to recovery data. And use Apple brand OS such a MAC and IOS OS for further research work. And take latest malware.

8. REFERENCES

[1] Case, A., & Richard, G. (2016). Detecting objective-C malware through memory forensics. *Digital Investigation, 18*, S3- S10. doi: 10.1016/j.diin.2016.04.017

[2] Rathnayaka, C., &Jamdagni, A. (2017). An Efficient Approach for Advanced Malware Analysis Using Memory Forensic Technique. *2017 IEEE Trustcom/Bigdatase/ICESS*. doi:10.1109/trustcom/bigdatase/icess.2017.365

[3] Balzarotti, D., Di Pietro, R., &Villani, A. (2020). The impact of GPU-assisted malware on memory forensics: A case study. Retrieved 9 February 2020

[4] Igor Korkin, Ivan Nesterov (2014), Applying memory forensics to Rootkit detection.

Retrieved 9 February 2020.

[5] Mosli, R., Li, R., Yuan, B., & Pan, Y. (2016). Automated malware detection using artifacts in forensic memory images. *2016 IEEE Symposium on Technologies for Homeland Security (HST)*. doi:10.1109/ths.2016.7568881

[6] Sihwail, R., Omar, K., ZainolAriffin, K., & Al Afghani, S. (2019). Malware Detection Approach Based on Artifacts in Memory Image and Dynamic Analysis. *Applied Sciences*, *9*(18), 3680. Doi: 10.3390/app9183680

[7] Andr´as Gazdag and Levente Butty´an, Android malware analysis based on memory forensic. Retrieved 9 February 2020.

[8] Ahmet Efe, Aysenur Dalmis (2019), Reiew of mobile malware forensic. Retrieved 9 February 2020.

[9] Korkin, I., &Nesterov, I. (2020). Applying Memory Forensics to Rootkit Detection. Retrieved 9 February 2020, from https://commons.erau.edu/adfsl/2014/wednesday/1/

[10] Sihwail, R., Omar, K., &ZainolAriffin, K. (2018). A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(4- 2), 1662. Doi: 10.18517/ijaseit.8.4-2.6827

[11] Thing, V., & Chua, Z. (2013). Smartphone Volatile Memory Acquisition for Security Analysis and Forensics Investigation. *Security and Privacy Protection in Information Processing Systems*, 217-230. Doi: 10.1007/978-3- 642-39218-4_17

[12] Tien, C., Liao, J., Chang, S., &Kuo, S. (2017). Memory forensics using virtual machine introspection for Malware analysis. *2017 IEEE Conference on Dependable and Secure Computing*. Doi: 10.1109/desec.2017.8073871

[13] Duan, Y., Fu, X., Luo, B., Wang, Z., Shi, J., & Du, X. (2015). Detective: Automatically identify and analyze malware processes in forensic scenarios via DLLs. *2015 IEEE International Conference on Communications (ICC)*. Doi: 10.1109/icc.2015.7249229

[14] Hua, Q., & Zhang, Y. (2015). Detecting Malware and Rootkit via Memory Forensics. *2015 International Conference on Computer Science and Mechanical Automation (CSMA)*. Doi: 10.1109/csma.2015.25

[15] H. Rughani, p. (2020). ForMaLity: Automated FORensicMAlware Analysis using VolatiLITY - PDF Free Download. Retrieved 9 February 2020, from http://docplayer.net/100192184-Formality-automated-forensic-malware-analysis- using-volatility.html