Detection of Windows Memory Anti Forensic Method

Mr. Nishith Khadadiya[1], Mr Gardas Naresh Kumar[2], Ms. Shweta Chawla[3]

[1] *Research Scholar, GTU PG School,Gujarat,India*
[2] *Course Co-Ordinator, CDAC ACTS, Maharashtra, India*
[3] *, Forensic Expert, CDAC ACTS, Maharashtra, India*

ABSTRACT

As the computer usage is expanding at an exponential rate, the crime rate is also increasing. Digital forensic comes into the existence so that detection of the crime should happen. As the investigators are getting smarter, criminals are also getting smarter and discover the methods which can disrupt or delay the forensic process which are also known as 'anti-forensic methods'. Here the author discusses about one such process which is used to counter the memory forensic method and also gives an approach to detect that method.

Keywords: - *Digital forensic, memory forensic, anti-forensic, windows forensic*

1. Introduction

Computers have turned into a fundamental piece of our regular daily existence. They are utilized as a part of each day of life and have made the life helpful for everybody. Be that as it may, diverse capacities of computer have additionally helped culprits with innovation that can be abused.
With far reaching utilization of Internet, the advanced crimes are additionally expanding step by step. So to do forensic analysis is necessary now a days. These days advanced forensic specialists need to deal with a major measure of information and the sum is always developing each day.[1]
Hostile to crime scene investigation has been risen in today's time with ad lobbed strategies and techniques to make the legal procedure somewhat harder and confused to protract the measurable procedure. The culprits are additionally utilizing the more intelligent approaches to wipe or limit their advanced follows with the goal that they can't get got. So that the legal specialists must be more intelligent and know about all the most recent hostile to scientific methods with the goal that they can likewise limit the impact done by apparatus or process which is utilized.

2. Introduction

Digital Forensics is the scientific process and methodology followed to identify, preserve, validate, analyze, interpret, and document any digital evidence derived from digital sources for the purpose of facilitating or understanding the sequence of events that led to any potentially criminal, unauthorized actions.
Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.
Computerized forensic is only the forensic of seized gadgets from crime scene to discover evidences to present to the court. So computerized forensic process is primarily used to gather advanced proof to display before the courtroom.

The forensic investigation is divided into several sub-branches like computer forensics, network forensics, forensic data analysis and mobile device forensics. The typical process encompasses the seizure, forensic imaging and analysis of media and then produce the report into collected evidence.

3 Memory Forensic

Memory forensics is unquestionably the most productive and intriguing point of digital forensics. Each operation performed by a OS or application brings about a few changes to the RAM. Besides, memory forensics gives phenomenal perceivability into the runtime condition of the framework, for example, which procedures were running, open system associations, and as of late executed orders [1]. One can remove these ancient rarities in a way that is totally autonomous of the framework you are exploring, diminishing the shot that malware or rootkits can meddle with your outcomes. Basic information frequently exists solely in memory, for example, plate encryption keys, memory-inhabitant infused code parts, confidentially visit messages, decoded email messages, and non-cacheable Internet history records.

4 Anti-Forensic

Anti-forensics are the counter-measures taken to frustrate forensic investigation and evade from it. The main aim of anti- forensic technique is to prevent any crime evidence from getting caught [2]. Digital forensics investigators Hilley and Sarah , defines Anti-Forensic as "attempts to negatively affect the existence, amount, and/or quality of evidence from a crime scene, or make the examination of evidence difficult or impossible to conduct."
Anti-forensic is something that makes life hard of digital investigator. Criminals utilize more brilliant ways and attempt to cover up or even crush the proofs to make examination hard. The primary point of anti-forensic methods are to keep any wrongdoing proof getting caught [7]

4.1 Anti-Forensic categorization

Anti-Forensic classifications are categorized based on different criteria:
On the attacked target, on the orientation of the attack, on the novelty of the techniques, or on its functionality. These techniques have been also divided into categories considering privacy aspects [9].

There are mainly four basic categories of Anti-forensics:
1. Data hiding
2. Artifact wipe
3. Trail obfuscation and
4. Attacks on the computer forensics process or tools.

Here author focuses on the process of attack against computer forensic process or tools and detect the windows platform based memory anti forensic process.

5 Memory Anti-Forensic method

This anti-forensic method mainly hides the arbitrary objects and traces from the memory while the dumping process is going on at operating system level.
The arbitrary objects which are hidden are processes, handles, threads, memory allocations and drivers.

In Windows the process is described by EPROCESS block and all the processes are linked in a doubly linked list structure [4]. So by arranging the next and previous pointers of a specific process block one can hide the process data associated with the malicious process and fool the forensic analyst.

Thread hiding is done by clearing the thread allocation. Each thread is denoted in the process by ETHREAD object and if one will see the structure of the EPROCESS block they can clearly see the ThreadListHead associated with the process block ETHREAD object also made of a doubly link list like EPROCESS block.

By deleting the process handle table completely remove the "Obtb" allocation also unlink the table from handle table list so seeing whether there are any object and any handles which are opened exclusively by target process. If found then it will remove those handle table entries and objects.

All memory allocations are described by the VAD which are simple kernel level structures which describes memory ranges allocated by any process. These VAD's are organized in tree structure and root which is known as VadRoot is stored inside the EPROCESS block. So by traversing the entire tree and delete the descriptor and checks whether those points to private memory of the process and unlink entire allocation [8]
By hiding the driver by unlinking the driver entry, loaded data table entry from PsLoadedModuleList and "MmLd" allocation and deletes driver image from memory.

6 Detection Method

In Windows there is an environment called Windows GUI subsystem is there which is outermost container in Windows GUI subsystem which represents a user's logon environment. When a user logon, session object is created and a unique session ID is denoted.

Session object contains a process list that are associated with the session. So scan for session object to find interesting information regarding the processes. For that the responsible object is __MM_SESSION_SPACE

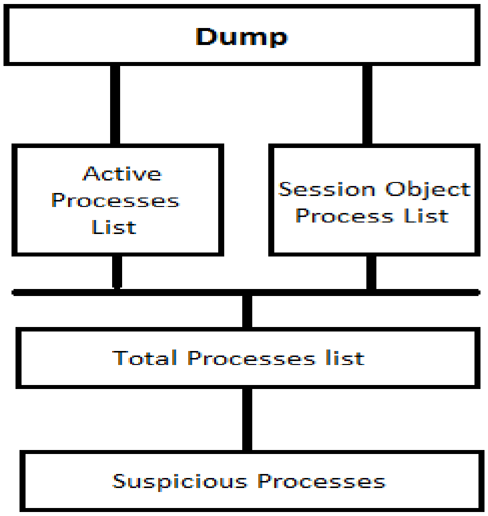

Fig. 1 Malicious process detection from session object

This object contains the details regarding the processes which are associated with the session so one can find the processes associated with it.

Also the other thing is that by scanning the registry entries one can get the recently opened file details associated with the session so it is also like a gold mine for the forensic researcher. So scanning the user assist registry keys, one can get the details regarding the process which are hidden by the above described methods.

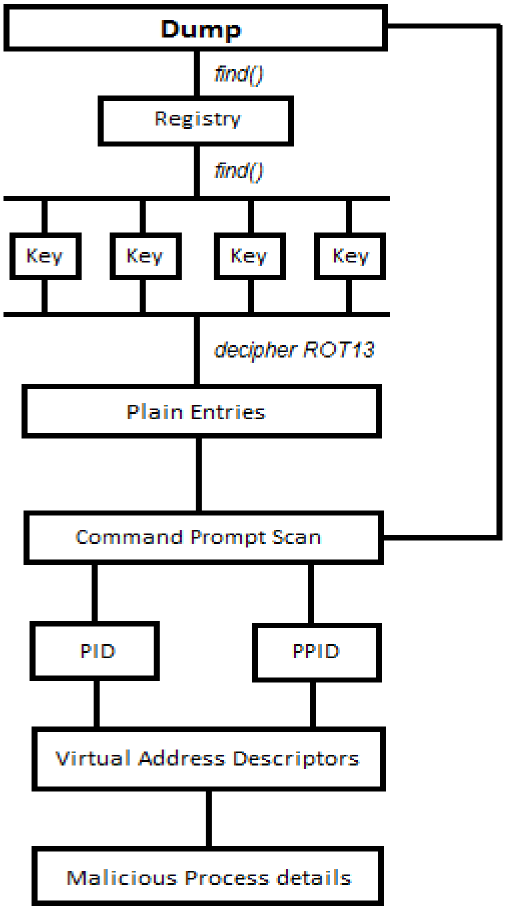

Fig. 2 Malicious process detection from registry keys

7 Conclusion

Now a days criminals are using smarter ways to evade or hamper the forensic process above mentioned process and many open source tools also available for spoiling the memory forensic process so detection of these activities is a must. This detection technique will help forensic analyst to understand that there is some manipulation to the system and one will not carried away in wrong direction so it will ultimately save the time which is an important aspect of the forensic process.

6. REFERENCES

[1] Palmer Gary. A road map for digital forensic research. In Digital Forensics Research Workshop, 2001.

[2] Kamal Dahbur and Bassil Mohammad. The anti-forensic challenge. In Proceedings of the 2011 International Conference on Intelligent Web-Services and Applications, ACM

[3] Foster, I., Kesselman, C.: The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann, San Francisco (1999)

[4] Michael Hale Ligh, Andrew Case, Jamie Levy, and Aaron Walters. The art of memory forensics: detecting malware and threats in windows, linux, and mac memory. John Wiley & Sons, 2014.

[5] Anu Jain and Gurpal Singh Chhabra. Anti-forensics techniques: an analytical review. In Contemporary Computing (IC3), 2014 Seventh International Conference on, pages 412{418. IEEE, 2014.

[6] Stuart McClure, Joel Scambray, and George Kurtz. HACKING EXPOSED FIFTH EDITION: NETWORK SECURITY SECRETS & SOLUTIONS. McGraw- Hill/Osborne, 2005.

[7] M Russinovich. Inside windows nt disk defragmentation. Mar, 6:1{7, 1997.

[8] Luka Milkovich. Defeating windows memory forensics. URL https://events.ccc.
de/congress/2012/Fahrplan/events/5301.en.html.

[9] Gary C Kessler. Anti-forensics and the digital investigator. In Australian Digital
Forensics Conference, page 1, 2007.

IJARIIE