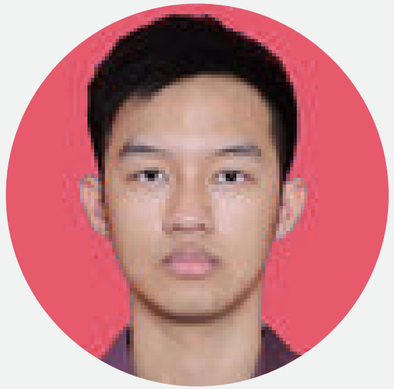
ANGGOTA KELOMPOK

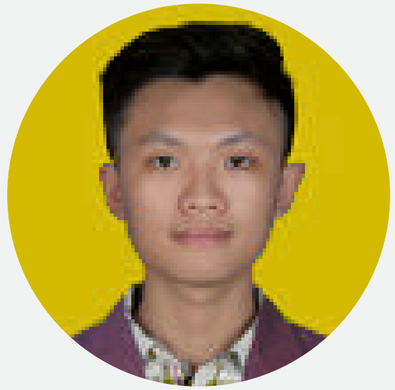
CHRISTINA
2502004235



HUGO
2501997016

MADE
2502005723

JONATHAN
2501986611



MAX
2502011360

Computer Forensic | Apache Log Analysis

THE IMPORTANCE OF VOLATILE

- Fileless malware is a type of malware that does not rely on files to infect a system, making it difficult to detect using traditional antivirus software.
- Volatile memory analysis can help detect fileless malware by examining the contents of a system's memory.
- Volatile memory analysis can also be useful in detecting other advanced threats, such as rootkits and advanced persistent threats (APTs).
- These types of threats are designed to evade detection and can be difficult to identify using traditional security tools.
- By analyzing volatile memory, security researchers can gain insights into the behavior of these threats and develop more effective strategies for detecting and mitigating them.
- Overall, volatile memory analysis is a critical tool in the fight against advanced threats and highlights the need for continued research and development in this area.

The Challenges with Collecting and Analyzing Volatile Memory

Page-smearing

Page-smearing refers to a situation where the data from one process gets mixed with another process in the memory space. This kind of technique can be used by Malware to hide code and data from forensics tools and render an inaccurate and more complex reconstruction of the original data.

Slow Performance

While acquiring volatile memory, the data will constantly change as the data is being read and written. Thus, makes the process of acquisition much slower to not disrupt the system or destroy the evidence. Other factors that might affect performance might be the size of the volatile memory and the complexity of volatile memory.

Storage Costs

Collecting volatile memory can also be a challenge because volatile memory tends to be much larger than other memory and certainly will be more expensive.

Subversion from Malware

Malware can be designed to subvert or tamper the volatile memory collection process where it will actively attempt to detect and subvert if there is an attempt to acquire memory.

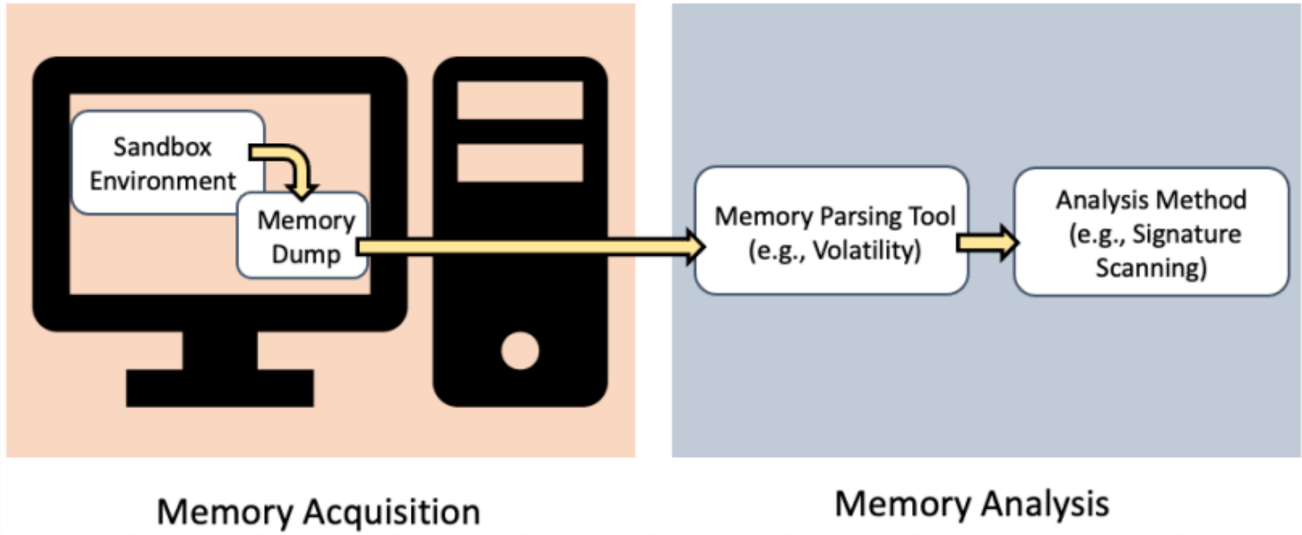
TOOLS AND TECHNIQUES

Memory Acquisition

Memory dump techniques are used to create a snapshot of the volatile memory of a system

Memory Analysis

Memory analysis tools are used to parse memory dumps making it easier to analyze volatile data



MEMORY ACQUISITIONS TOOLS

Different tools are used for different access levels, types and conditions. So be sure to use the right tools for the right circumstances

Kernel Level

Kernel Drivers:
Pmem
LiME
ProcDump

Debuggers:
GNU Project Debugger
WinDbg
Visual Studio

Hypervisor Level

VMWare
LibVMI
Hypersleuth
Vis

System Management Level

SmmBackdoor

Asynchronous Device Level

Direct Memory Access:
PCILeech
Inception

Hardware Thread Control Block:
Snipsnap

MEMORY ANALYSIS TOOLS & TECHNIQUE

Scanning Methods:

- Signature Scanning:
  - Looks to match the signatures of known malware with the contents
- Heuristic Scanning:
  - Detects threats using algorithms to look for malicious commands or instructions

The two open sourced tools commonly used for memory dump analysis are:

- Volatility
- Rekall

Dynamic Analysis:

Analysis done in a virtual environment to record malicious behaviors/characteristics through it's volatile memory. The two ways to setup a virtual environment are:

- Virtualized Environments
- Software Emulators

Sandbox Tools like *AnyRun, FireEye, JoeSecurity* and many more are used to help dynamic analysis.

Machine Learning Approach

ML has shown promising results for a wide variety of domains. This includes it's approach for malware detection within Volatile memories.

VARIOUS TECHNIQUES IN VOTILE MEMORY

Memory dump techniques

Memory dump techniques are used to create a snapshot of the volatile memory of a system

Parsing memory dumps

Parsing memory dumps involves analyzing the memory snapshot to extract useful information

Machine learning

type of artificial intelligence that involves training algorithms to recognize patterns in data.

Overall, the strengths and weaknesses of different tools and techniques need to be considered when conducting volatile memory analysis. Combining different approaches can help improve accuracy and effectiveness.