Systematic Memory Forensic Analysis of Ransomware using Digital Forensic Tools

Paul Joseph, Vellore Institute of Technology, India
https://orcid.org/0000-0003-2897-212X
Jasmine Norman, Vellore Institute of Technology, India

ABSTRACT

Cybercrimes catastrophically caused great financial loss in the year 2018 as powerful obfuscated malware known as ransomware continued to be a continual threat to governments and organizations. Advanced malwares capable of system encryption with sophisticated obscure keys left organizations paying the ransom that hackers demand. Since every individual is vulnerable to this assault, cyber forensics play a vital role either in educating society or combating the attacks. As cyber forensics is classified into many subdomains, memory forensics is the domain that leads in curbing these types of attacks. This article gives insight on importance of memory forensics and provides widespread analysis on working of ransomware, recognizes the workflow, provides the ways to overcome this attack. Furthermore, this article implements user defined rules by integrating into powerful search tools known as YARA to detect and prevent the ransomware attacks.

KEYWORDS

Crypto Malware Analysis, Digital Forensics, DLL Injection, Malware Analysis, Memory Forensic Tools, RAM Forensics, Ransomware Analysis, Yara Tool

INTRODUCTION

Digital forensics (Beebe & Clark, 2005) is an assortment of multiple domains like multimedia forensics, Disk device forensics, Mobile forensics, database forensics, Memory forensics, Network forensics. Every area has its own techniques and tools. A few of the tools are multi-domain adjuvant and few of them are domain specific. Typically, forensics is a seven-stage process (Bem et al., 2008; Harichandrann et al., 2015). Generally, the word ‘memory’ in digital world makes people tend to contemplate on the magnetic storage devices; however, it alludes back to the silicon storage devices which might store volatile data (Amari, 2009; Grier & Richard, 2015). In relation to computers, primary memory is the memory that serves as a backbone of the system that loads and stores the data that is necessary to run the computer’s operating system. Once the system is online, regardless of the task a user performs, initially it is fetched into main memory, read and then executed. Random Access Memory contains enormous information like processes, user details and network details. Random access memory (RAM) holds evidence of user actions, malevolent processes and furtive behaviours implemented by malignant code. In the present forensics cases, it is even as vital to know memory structures as it is to know the disk and registry structures. Having in-depth proficiency of Windows memory internals permits the examiner to induce to the target information unequivocal to the necessities of the current case. Advanced malware and post-exploitation modules progressively employ self-defence procedures.
that fused more complex rootkits and anti-memory analysis mechanisms that decimate or debase the volatile information. Once the system is targeted either with an attack or with malware, by analysing the physical memory like RAM, the root cause might be found. This process in the digital world is termed as memory forensics.

Memory forensics is the area or domain that collects memory dumps from a compromised system and analyses the information (Digital Forensics Research Workshop (DFRWS), 2005; Stütgen & Cohen, 2013). The preliminary objective of this is often to perceive the attacks or source of attacks that has not left any traces on the target’s system. To analyse this shrouded data, some tools were designed and were advanced underneath three generations. The first-generation tools had constrained knowledge on the internal data structures and the operating systems. The second-generation tools were developed as an element of instructive research that supports all operating systems. One of them was volatility, that had set its own mark in memory forensics area due to its intensive support. The third generation, that is in progress, supports virtual machines memory dumps as well as platform independence. The reason why memory forensics became so crucial is because of its distinguished evidence stored in it (Vömel & Freiling, 2011). Since there is very less research done in this area, the authors attempted to give a thorough analysis of the same in the light of memory forensics. The rest of the paper deals with the Importance of Memory Forensics, its techniques and tools, Brief introduction on WannaCry ransomware with its design pursued by technical analysis, results and mitigation techniques followed by current trends and future directions. In this paper, memory forensics is studied with its background, issues, tools and practical implementation through a case study.

**IMPORTANCE OF MEMORY FORENSICS**

RAM contains a lot of information, which is very useful for forensics professionals. Memory forensics provides unprecedented visibility into the runtime state of the systems which consists of the following:

1. *Running processes at the time of acquisition*

   This will be useful for the examiners to comprehend what files are running at that time. Sometimes suspicious process and suspicious applications can be found. However, the concealed malware and rootkits cannot be discovered in this.

2. *Network Configuration*

   This information contains remote IP’s associated, port numbers, open ports list, compromised system communication with remote servers along with their IP’s, sites visited, wireless access points if connected any, WEP or WPA2 or wireless keys, cryptographic keys exchange information (public and private keys), some cookies and session id’s information which is very valuable.

3. *Credentials Configuration*

   This contains data like user id’s and passwords, number of instances the user has logged in, passwords of all accounts, ID’s and passwords of websites that the user visited, email passwords, social networking sites credentials etc. Based on the obtained passwords, emails, banking details can be traced out.

Metaheuristic-Based Hybrid Feature Selection Models
www.igi-global.com/chapter/metaheuristic-based-hybrid-feature-selection-models/187678?camid=4v1a

Comparative Analysis of EMD and VMD Algorithm in Speech Enhancement
www.igi-global.com/article/comparative-analysis-of-emd-and-vmd-algorithm-in-speech-enhancement/188780?camid=4v1a