Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X Vol.6 No.2, 2017, pp.36-39
@The Research Publication, www.trp.org.in

AUMFOR: Automated Memory Forensics for Malware Analysis

Parag H. Rughani[1] and Vimal Rughani[2]
[1]Assistant Professor, Gujarat Forensic Sciences University, Gandhinagar, Gujarat, India
[2]CEO, Virtual Reality Systems, Gandhinagar, Gujarat, India
E-Mail: parag.rughani@gmail.com

Abstract **- Day by day cyber crimes and attacks are growing exponentially, every year companies in worldwide lose billions of dollars due to cyber attacks. It has became very essential to investigate and indentify root of cyber 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 do not leave easily detectable tracks on hard drive data. There are varieties of tools available for RAM analysis including Volatility, which currently dominates open source RAM forensic tools. However, use of volatility requires knowledge of command line tool and dynamic as well as static malware analysis; it becomes very complex and tedious process. The work mentioned in document is aimed to help forensic investigators and researchers by providing GUI based Tool for Automated Memory Forensics (AUMFOR). AUMFOR do perform all complex and tedious work automatically, it also analyzes and gives final accurate reports about possibilities of use of malware in committing a crime.**

Keywords**: Memory Forensics, Live Memory Forensics, Volatile Memory Analysis, Malware Analysis, Forensic RAM Analysis, Volatility GUI, Automated Memory Forensics**

I. INTRODUCTION

Nowadays Cyber attacks are sophisticated, so Memory Forensics play important role in investigating Cyber crime. "That is why memory forensics is becoming critical to the analysis of malware and its functions... The attackers used every conceivable anti-forensic technique; demonstrating how no malware files are needed for the successful exfiltration of data from a network, and how the use of legitimate and open source utilities makes attribution almost impossible." as quoted by Sergey Golovanov, principal security researcher at Kaspersky Lab [1]. Memory Forensics can provide unique insights into runtime system activities, including open network connections and recently executed commands or processes. In many cases, critical data pertaining to attacks or threats will exist solely in system memory – examples include network connections, account credentials, chat messages, encryption keys, running processes, injected code fragments, and internet history which are non-cacheable. Any program – malicious or otherwise – must be loaded in memory in order to execute, making memory forensics critical for identifying otherwise obfuscated attacks.

Considering importance of Memory Forensics, it becomes very important for Forensic Investigator to have expertise in understanding how malware work and how they can be identified from the live memory image or RAM dump. Unfortunately, Digital Investigators frequently lack the training or experience to take advantage of the volatile artefacts found in physical memory. Volatile memory contains valuable information about the runtime state of the system, provides the ability to link artefacts from traditional forensic analysis (network, file system, registry), and provides the ability to ascertain investigative leads that have been unbeknownst to most analysts. Though, there are many commercial and existing live forensic tools available, but none of them feature automated analysis.

The work mentioned in this paper is inspired to provide a Graphical User Interface and automation of basic steps. The tool derived from the work is made user friendly to ease extraction and analysis of malware from RAM dump. The biggest advantage of this tool is, user does not need to remember commands, their syntaxes or even when to use which command. This is very handy for those who do not prefer to work on command line utilities because they avoid remembering commands. The proposed solution called AUMFOR – Automated Memory Forensic is GUI based Tool for helping Forensic Investigator by performing all complex and tedious work automatically, it also analyzes and gives final accurate reports about possibilities of use of malware in committing a crime.

II. RELATED WORK

Forensic Investigators, Experts and Companies are working from many years in automating analysis process to ease their work. Except forensic aspects as discussed in this paper, there are many open source sandboxes available like cuckoo[2] which provides automation in malware analysis process. Also Michael Bailey, et. al. proposed automated classification and analysis of Internet Malware in their work[3]. Manuel Egele, et. al. discussed various sandboxes and automated malware analysis tools in their survey[4].

But for Automated Memory Forensic very little work is done. Tomer Teller, et. al. proposed a solution based on cuckoo, Volatility and IDA[5] in their paper at Blackhat [6], but it heavily depends on Cuckoo. Also Logen, Höfken and Schuba provided a GUI based solution as an extension to Volatility in their paper [7], though work proposed by them performs few basic tasks automatically, While another tool eVOLe developed by James Habben[8] is web based tool,

but that tool ask image profile at time of execution, which indicates that user are required to run Volatility separately to get profile and work become tedious. Further eVOLe GUI doesn't provide complete Malware Analysis. To overcome all such issues, AUMFOR is proposed in next section. It does all necessary process Automated for Memory Forensic and Malware Analysis with user friendly GUI.

III. PROPOSED TOOL

The work is done to help Digital Forensic Investigator, who are assumed not be expert malware analysts but are needed to have some mechanism by which they can easily identify presence of any malware in the RAM dump.

The proposed tool called and now onward refered as AUMFOR is a web based GUI for performing Memory Forensics related complex and tedious work Automated. GUI of AUMFOR is developed in Django[9], python based web framework, to perform Memory Forensics. AUMFOR utilized and extended Volatility[10] open source python framework for Memory Forensic, while performing Automation Process AUMFOR uses Django Rest Framework[11], system level threads and Jquery.

Forensic Investigators have to perform very minimal steps to get analyzed report of Memory Forensic from AUMFOR. AUMFOR expect only one zipped file of RAM dump which is supposed to be analyzed. AUMFOR provides file browser window for uploading RAM. Once dump is uploaded into AUMFOR, it will start executing different complex processes automatically in background; user will get live status update on processes which are being executed.

First Automatic process AUMFOR does is, it extracts zip file of dump and put valid dump on proper place for next execution step. Next step is to identify image information of dump which will give details about Operating Systems. AUMFOR will identify information like Profile (Volatility refer as architecture of Operating System), service pack details, basic kernel details, etc. All these image information will be utilized while performing all other commands.

Once having dump image information and profile related details, AUMFOR starts exploring and analyzing dump's processes. Process plays a crucial role in identifying malware related attacks. Most of the malware including ransomware are network based and work as botnet. These malware mostly need to connect to their origin developer or control centre to execute next command or to send important or confidential information.

To accomplish such communication, malware uses open IP address with port. Liming Cai, et. al. mentioned importance of this point by stating "We must access the computer system's physical memory to find more important information, such as the intruder's IP address, information about the running malicious programs, processes, worms, Trojans and so on in their paper[12]. To identify such open IP and Port, AUMFOR will analyze Network Connections for given dump. It will give all possible and necessary details to you for identifying malicious IP or port. So if any such IP or port found, we can easily link with associated process. It is important to note that above mentioned process may become difficult for regular Forensic Investigators, if they do manual malware check for each IP, port and process. AUMFOR plays very important role by performing above mentioned process automatically.

After identifying malicious Process, next important task is to dig more on that process and identify executables, DLLs, Threads and Handles used by that Process. It is very important here to understand that suspicious executable of process which initiated the communication, was running when RAM was captured hence; it was loaded on RAM dump.

To get executables, DLLS, Thread and Handles, AUMFOR will utilize its intelligence and capture all necessary details relevant to each process while analyzing dump and its process. AUMFOR provides download feature for process, so Forensic Investigators can experiment with suspicious executables or Process in isolated environment or they can send to advance malware research centre for further investigation.

For windows system, Registry is a goldmine of forensics artefacts that can be utilized during investigations, incident response handling, and malware analysis. Registry appears as unified tree, but is made of distinct hives. In automated process of analyzing dump, AUMFOR also collects information related to Registry hives, so that can be investigated further.

In addition to above mentioned features, AUMFOR provides feature of scanning individual process file for viruses, worms, Trojans and all kinds of malwares. AUMFOR utilizes VirusToal[13] to accomplish scan process. AUMFOR does all background stuff for scanning process and generates final report of that.

AUMFOR is smart umbrella which covers up and automates all necessary steps and process of Memory Forensic to help Digital Forensic Investigator. Users will get quick and accurate results without knowing complexity and tediousness of tasks. AUMFOR is available for Windows and Linux and it supports memory dump from Windows Linux and Mac.

IV. METHODOLOGY

After getting the files, one can install the tool with minimal steps and commands. Once installed, the tool can be launched using the command aumfor. Following screens show details of the tool with important features.

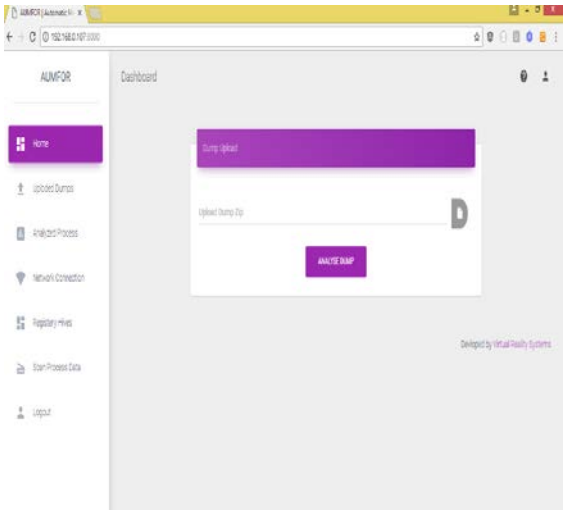

Fig.1 Upload zipped file of Dump

User can upload zip file using browse button shown in following screen. As the dump size may be in GBs, users are required to submit it by compressing into a zip file.After selecting the file, once user clicks on Analyze Dump button, AumFor will start analzing dump and will update user with real time status of execution.

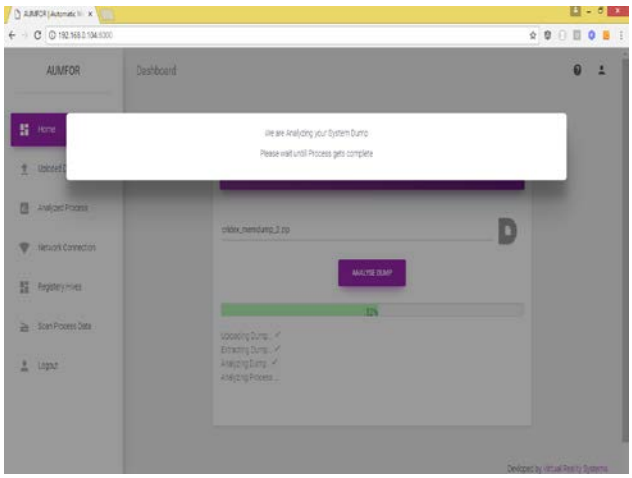

Fig.2 Uploaded Dump is being analyzed in AUMFOR

The process may take long time based on file size. As it does all the routine tasks in background the user has to wait till it finished the process. However, it may seem taking more time, but that is required ony once. As soon as intial analysis gets over, it saves lots of time compared to which it consumes in analysis.

After successful analysis, the tool diverts user to the dashboard. Default screen of dashboard shows list of processes with relevant details like threds, handles and dlls associated with each process.

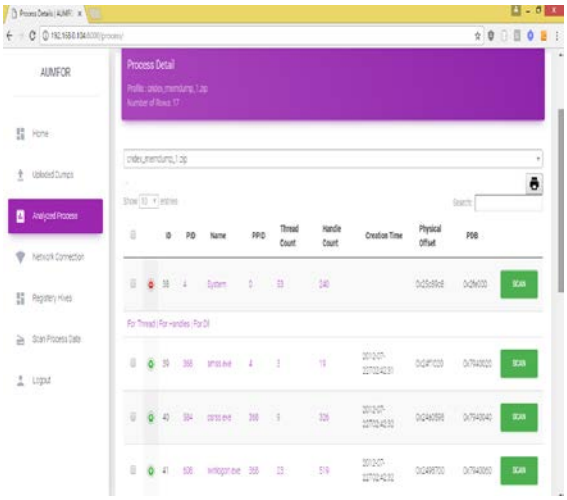

Fig.3Details of Process, its Threads, Handles and DLL listed on screen.

From the perspective of malware analysis, suspicious process can be analyzed by clicking on scan button. It will scan individual process for virus, worms, Trojan and all possible malware. When you click on scan button, it will query the process to VirusTotal and will generate detailed report.

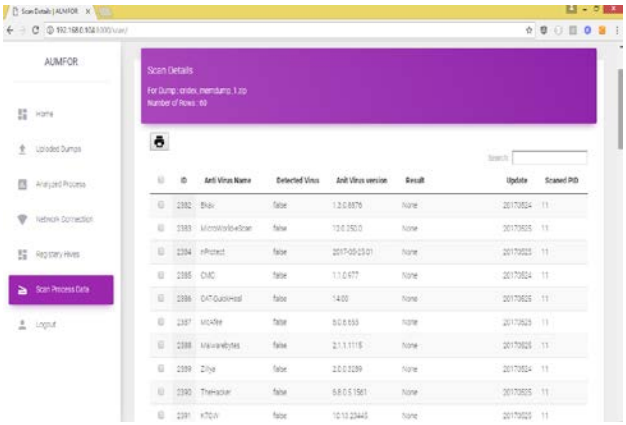

Fig.4 support network and registry analysis

Apart from the process analysis, AUMFOR is designed to support network and registry analysis. The biggest advantage of this tool is it's user friendliness.

V. CONCLUSION

Outcome of this work (AUMFOR) will provide GUI based fully Automated Memory Forensic Tool. It will help Digital Forensic Investigators in analyzing live memory dump with Automation, Accuracy and User Friendly GUI. AUMFOR has been tested with different sample dumps and it gave accurate result for all the samples. AUMFOR will help in reducing investigation time and cost.

VI. FUTURE SCOPE

Though, AUMFOR perform all necessary actions for Automated Memory Forensic, there are still scope of enhancement. The tool can be further extended to include more aspect of malware analysis and Behavioral Analysis for Malware with help of Machine Learning. Organisations face millions of threats each day, so it would be impossible for threat researchers to analyse and categorise them all. As each threat is analysed by the machine, it learns and improves. This not only helps protect organisations now, but compiles this valuable data for use in predictive analytics: Sourced by Hal Lonas, CTO of webroot [14]. Also quoted by Mike Paquette, VP of Products at Prelert, argue that machine learning is cybersecurity's answer to detecting advanced breaches [15].

If one can develop solution which combines Machine Learning and AUMFOR, it will be great solution. It will help Forensic Investigators to indentify Patterns and Behaviours of malware, so they can prevent future cyber attack.

ACKNOWLEDGEMENT

We acknowledge the assistance provided by developers from Virtual Reality Systems in implementing some of the features of this tool.

REFERENCES

[1] Sergey Golovanov, principal security researcher at Kaspersky Lab, as quoted by TechRepublic

[2] Cuckoo Sandbox – A malware Analysis system https://www.cuckoosandbox.org

[3] Michael Bailey, Jon Oberheide, Jon Andersen, Z. Morley Mao, Farnam Jahanian, Jose Nazario, "Automated Classification and Analysis of Internet Malware" in Recent Advances in Intrusion Detection, Vol.4637 of the series Lecture Notes in Computer Science. Pp. 178-197, 2007.

[4] Manuel Egele, Theodoor Scholte, Engin Kirda and Christopher Kruegel, "A Survey on Automated Dynamic Malware Analysis Techniques and Tools" *in the ACM Computing Surveys*, Vol.44 ,Issue 2, Article No. 6, pp. 1–49, 2012.

[5] IDA - Multi-processor disassembler and debugger, https://www.hex-rays.com/products/ida/

[6] Tomer Teller, Adi Hayon, "Enhancing Automated Malware Analysis Machines with Memory Analysis" , Blackhat Arsenal , pp. 1-5, 2014.

[7] Steffen Logen, Hans Höfken, Marko Schuba, "Simplifying RAM Forensics - A GUI and Extensions for the Volatility Framework", *in the Seventh International Conference on Availability, Reliability and Security* (ARES),,pp. 620 – 624, 2012.

[8] eVOLve by JamesHabben, https://github.com/ James Habben/ evolve

[9] Django – A python based web framework https:// www.djangoproject.com/

[10] Volatility – A python based open source memory forensic http://www.volatilityfoundation.org/

[11] Django Rest Framework – Django - Python based toolkit for building Web API's http://www.django-rest-framework.org/

[12] Liming Cai, Jing Sha ,Wei Qian, "Study on Forensic Analysis of Physical Memory" *in the proceedings of 2nd International Symposium on Computer, Communication, Control and Automation (3CA 2013)*, pp. 221-224, 2013.

[13] VirusTotal - facilitates the quick detection of viruses, worms, trojans, and all kinds of malware, https://virustotal.com/

[14] Web reference of source: http://www.information-age.com/importance-creating-cyber-security-culture-123465778/

[15] Web reference of source : http://insidebigdata.com/2015/12 /11/ machine-learning-is-cybersecuritys-answer-to-detecting-advanced-breaches/