Exploring the Malware Analysis Landscape for Forensic Investigation

Gursimran Kaur, Bharti Nagpal
Department of Computer Science & Engineering,
Ambedkar Institute of Advanced Communication Technology and Research,
Geeta Colony, Delhi, India
researchergursimran@yahoo.com, bhartinagpal24@yahoo.com

Abstract—The computer crime explosion in World Wide Web has increased in both commercial and personal areas. Study of poor users; provide valuable information in their system to their individual needs or for the efficient organization. Among the several attacking approaches like virus, worm, Trojan horse etc. to extract confidential data from particular victim system, this paper uses malware analysis of system to discover malware which extract confidential information from victim system. Malware poses a huge threat to society, which is heavily dependent on computer technology. Traces of malicious activity can be identified through digital forensics techniques. In this research we describe a generic and modular framework to present detection of malware attack & types of malware analysis technique based on existing approach. At the end we propose a Landscape to detect the malware in computer system for the help of computer forensic investigation.

Index Terms— Malware Analysis, Malware Detection, Forensic Investigation, Malware Investigation, Privacy.

1. Introduction

Nowadays internet is most emerging technology in the world. The use of system needs to follow some specific protocol that is given by our system provider. Many attackers try to exploit your security structure. Some get are successful in their effort and attack on our system by any malicious program. Malware is the malicious program which is harmful to computer system and network. Malware ambushes the confidential information in the system and misuses that information. It is used by the attacker to crack the CIA model property in the computer system and network.

In this paper, we discuss forensic investigation and investigating the malware. Many forensic investigators help us to investigate a system to detect that hacker/attacker who attempt to attack on the victim system. We represent secure malware investigation. It is hard to detect malware attack by forensic investigator's using specific tools. We detect malware attack in victim system and ensure that our investigation model will be very much effective.

We also explore landscape for forensic investigation on a system by malware analysis. The malware analysis is represented by investigation technique and we enhance the path of malware. We need to work on time monitoring collection, preprocessing and analysis various system metrics like use of system resources and CPU consumption, number of sent packets through the internet, number of running processes, then to detect malware attack and after analysis, we are able to detect an enhanced malware. This was further utilized with investigation of system representation through applying model to evaluate result.

The rest of this paper is arranged as follows: Section 2 gives an overview about the background and related work in the area of malware analysis and forensic investigation. In section 3 the details of the malware analysis and section 4 gives details of digital investigation. Section 5 results from our purposed model by applying malware detection technique. Finally, some conclusion and prospect are put forward in Section 6.

2. Background & Related Work

Generally speaking, computer forensics attempts to answer the question of who, what and how a security breach has occurred. The fidelity of the recorded information used in such analyses is highly dependent on how the data was collected in the first place. Malware Analysis, the art of analyzing malicious program on a victim system, has been dealt by several researchers using different approaches. Some researchers including [5] [6] have used classification algorithms for detecting web usage patterns. The authors [7] used similar upper approximation clustering technique on web transactions from web log data to extract the behavior pattern of user's page visits and order of occurrence of visits.

If you want to discover whether your website is being attacked, hack attempt identifier can help with that. Remember that just because an attack occurred doesn't mean it was successful, but it's still useful to know what you're up against [9].

3. Malware Analysis

Malware is nasty programs which are executed or replicated in the system and network form client host machine to server machine and propagate all networks. It infects the system by malicious code. Malware focus to compromise the system, Confidentiality, Integrity and Availability (CIA).

3.1 Life Cycle Of Malware

In the malware analysis the malware behavior can take place in various environments. This is categorized into four stages: Static, Mounted, Live and Network. It represents the natural progression of malware investigation in the four stages.

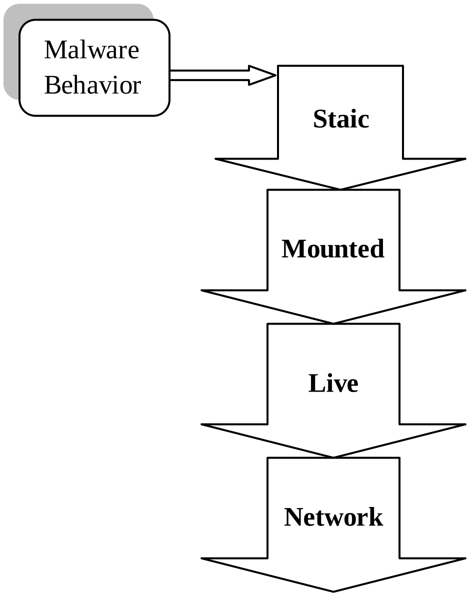

Fig. 1. Malware Analysis Life Cycle

i. **Static Analysis** takes place when the infected file is placed into a non-functioning environment and analyzed as raw data. The benefits that this has are that the virus cannot utilize any advanced techniques to evade detection and any unencrypted strings or headers can be easily identified

ii. **Mounted Analysis** involves mounting the file system on which the infected files are stored as a logical drive within the investigation machine. This has the advantage that the file can be viewed in its native environment, allowing for file and folder permissions and metadata to be more easily examined

iii. **Live Analysis** should occur within a sandboxed environment where the resources available can be strictly controlled. At this stage the infection can be set loose on a system and its effects monitored or controlled.

iv. **Network Analysis** stage looks at any network traffic associated with the infection. When viruses are created for profit they typically need to transfer information to be successful.

3.2 Categorization of Malware

Malware are categorized in many form. Some are given below [11]:

i. Computer Viruses

Computer virus is small, infectious and destructive software that can replicate itself and go on to infect other computers. A computer virus is usually executable software. Computer viruses can be contacted through downloads and various mode of email and instant messaging attachments. A virus then attaches itself to existing programs on the target computer. The main aim is to corrupt the computer system. Computer viruses can be removed by installing and running antivirus or antimalware programs.

ii. Worms

Similar to a computer virus, worms are infectious and self-replicating. However, Computer worms work with computer networks. The worm utilizes a computer network to send replicas of itself to connecting computers on that network. Computer worms can replicate to create volume and it poses a great threat to large computer networks. Computer worms can be removed using malware removal tools.

iii. Trojan horse

Trojan or a Trojan horse is a form of computer malware that can be installed on a computer system through deceptive means. The Trojan is presented to the user in a form of a free useful software or add-on. In all events, in the forefront installed, the Trojan horse gives access to hackers, who can then carry out their criminal operations on the target computer from a remote station. Trojan horses can be removed either manually or by using antivirus software programs.

iv. Adware

Adware is short for Advertisement-supported software. The program is designed to display advertisements on a computer system. However, some adware are dishonest and therefore can be classified as spyware - because that is what it does - spy on the computer user and also steal user sensitive information. Adware can also be removed using trusted spyware or malware removal tools.

v. Greyware

Greyware is a malicious software or code that is considered to fall in the "grey area" between normal software and a virus. Greyware is a term for which all other malicious or annoying software such as adware, spyware, trackware, and other malicious code and malicious shareware fall under.

vi. Crimeware

Crimeware is a form of malware created specifically to perpetrate crime on the Internet. The main aim of crimeware is to steal financial and confidential information such as credit card data and passwords and use this to access private online bank accounts or financial services - identity theft. Crimeware can be installed through social engineering and tricky manipulation of people which leads them to release their confidential information. This malware can also be installed through vulnerabilities in software applications or email attachments.

vii. Spyware

Spyware is a form of malware program installed secretly on a computer system that collects and sends information about its usage and other confidential and personal data to the developer in an unethical manner. A computer system can get infected with spyware through deceptive ways such as free online scanning, Internet add-ons or plugins, dubious websites and images or even through a search engine. Spyware can be removed using antispyware removal tools.

viii. Keyloggers

Keyloggers are created to monitor user keystrokes and the information are logged and reported to the person or organization who installed them. Keyloggers may be used by organizations to monitor workers or employees activities. Keyloggers can also be used as a form of spyware to steal confidential information and commit identity theft.

ix. Hijackers

Hijacker is a form of malware that changes the browser setting of the user's computer and redirected to of the developers choice. The user is usually redirected to start pages and search pages for paid advertising. Hijackers may slow the computer and cause the browser to crash.

x. Rogue Security Software

Rogue security software is a form of malware that manipulates and scare people into buying a full version of fake application software. The fake software displays bogus scan reports and alerts, which are actually simulated to trick the user. The program takes over the whole computer system to prevent removal and in most cases block other applications including legitimate anti-malware programs from running.

4. Malware Investigation

Forensic science provides tools, techniques and scientifically proven method that can be used to acquire digital evidence. Digital forensics is a branch of computer science. It is defined as use of scientifically derived and proven method for digital evidence. Digital forensics is recovery and investigation digital evidence which is used in any criminal activity.

4.1 Malware Analysis Process via Digital Forensics Steps

In the organization if any crime happens with the help of malware in system then with the help of anti forensics investigation the crime can be checked by using some process. The forensics electronic crime investigation collects the digital evidence. By following these steps, an organization can recover from an incident with as little time and money lost to the business as possible, while also ensuring that the incident will not happen again. These following steps follow[8]:-

i. Identification – Indicators to identify an event and determine its type.

ii. Preparation – Preparing tools, techniques, search warrants, and monitoring authorizations and management support.

iii. Approach Strategy – Dynamically formulating an approach based on potential impact on bystanders and the specific technology in question. The goal of the strategy should be to maximize the collection of untainted evidence while minimizing impact to the victim.

iv. Preservation – Isolate, secure and preserve the state of physical and digital evidence. This includes preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius.

v. Collection – Record the physical scene and duplicate digital evidence using standardized and accepted procedures.

vi. Examination – In-depth systematic search of evidence relating to the suspected crime. This focuses on identifying and locating potential evidence, possibly within unconventional locations. Construct detailed documentation for analysis.

vii. Analysis – Determine significance, reconstruct fragments of data and draw conclusions based on evidence found. It may take several iterations of examination and analysis to support a crime theory. The distinction of analysis is that it may not require high technical skills to perform and thus more people can work on this case.

viii. Presentation – Summarize and provide explanation of conclusions. This should be written in a layperson’s terms using abstracted terminology. All abstracted terminology should reference the specific details.

ix. Returning Evidence – Ensuring physical and digital property is returned to proper owner as well as determining how and what criminal evidence must be removed. Again not an explicit forensics step, however any model that seizes evidence rarely addresses this aspect.

We also consider the legal/ethical procedure in the whole process of malware analysis and investigation.

4.2 Legal/Ethical Considerations

Consideration must be given to legal and ethical issues in the analysis of malware. From a legal perspective, Analysis of malware may require correct handling, preservation and presentation of evidence appropriate to a court of law. It may also include consideration of disclosure of private data that has been uncovered during the course of analysis. This private data could include, but not limited to, usernames, passwords, and personal Particulars such as date of birth, address, relationships and financial data such as credit card numbers or bank account details.

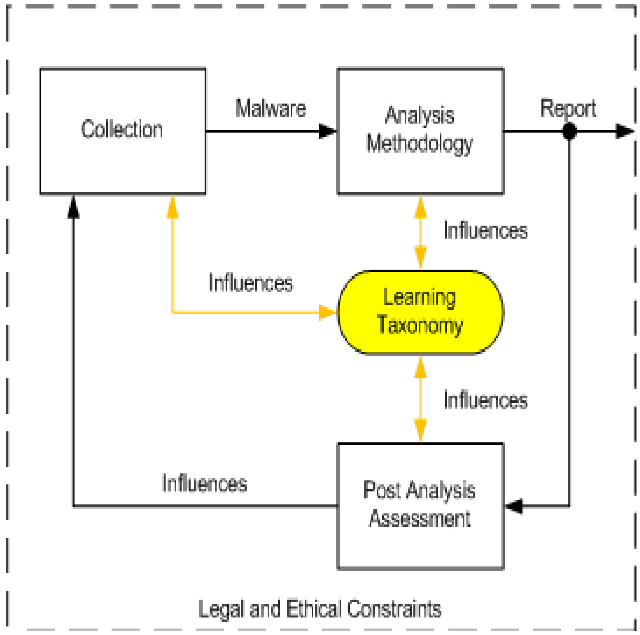

Fig. 2. Legal/Ethical Considerations

Furthermore, there is an ethical consideration to ensure that the analysis process is secure and that the spread of malware is not a possibility. Also in the case of extraction or identification of a particular new malware, the responsible sharing of this knowledge is also a matter for ethical consideration.

5. Exploring The Malware Analysis Landscape For Forensic Investigation

Here, we propose a model for investigating the given victim system through malware analysis. By examining malware by our model, we can easily detect when and how many times our system was attacked by hacker/attacker.

The security model is design to detect the malware on the system firstly system is design to protecting itself. The system application is identify their permission that govern the right and law to their data and interface at the installation time in the organization.

To overcome the limitation we purpose the light weight malware detection system. The malware is basically consumption of CPU memory, resources and suspicious activity on their hands. To detect the malware basically use the real time monitoring collection, preprocessing and analysis various system metrics like as use system resources and CPU consumption, number of sent packets through the Wi-Fi, number of running processes.

Collection and preprocessing, the system is sent for analysis by matrix Explore the various units, namely the processor, each specializing in their own employment malicious behavior detection and threat assessment (TA) to generate. In this, according to weight, generates the alert indication report. All malware, weight already stores in the database in this process compare the weight which is store in the database (fig.3). All threat has different weights warm weight is not similar virus weight. According to weight if it is not match then indicate the alarm. Some unwanted action, performed by the malware Automatic actions, include among others: uninstalling an application, killing a process, disconnecting all radios, encrypting data, changing firewall policies and more. A manual action can be uninstalling an application subject to user consent. Manual action can be uninstalling an application subject to user consent.

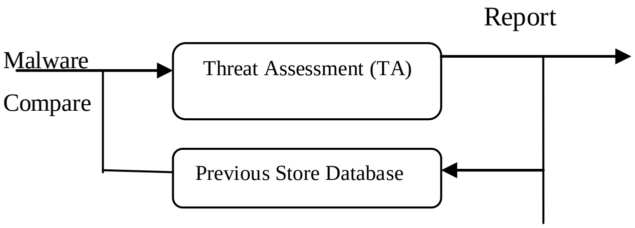

Fig. 3. Threat Weight Unit

The security model is categories into four components: Graphical User Interface (GUI), Feature Extractors, Processors and Main Service.

i. **Feature Extractors:** The Feature Extractors communicate with various components of the system framework, including the kernel and the Application Framework layer in order to collect feature metrics, while the Feature Manager triggers the Feature Extractors and requests new feature measurements every pre-defined time interval. In addition, the Feature Manager may apply some pre-processing on the raw features that are collected by the Feature Extractors.

ii. **Processor Unit:** An analysis and find a processor unit. It is preferred that the processor will which is basically a pluggable external components can be installed as provided Established the United Nations. Feature vectors of the service is their role, they analyze Risk assessment and risk load the output unit. Each processor Expose the advanced configuration screen. Rule-based processor knowledge based, may be Or classifiers / anomaly detection, machine learning method employed.

iii. **Threat Weighting Unit:** The risk weight of all active units (TWU) analysis results Processor and an added algorithm (much like voting, distribution applies etc. In order to balance a final decision

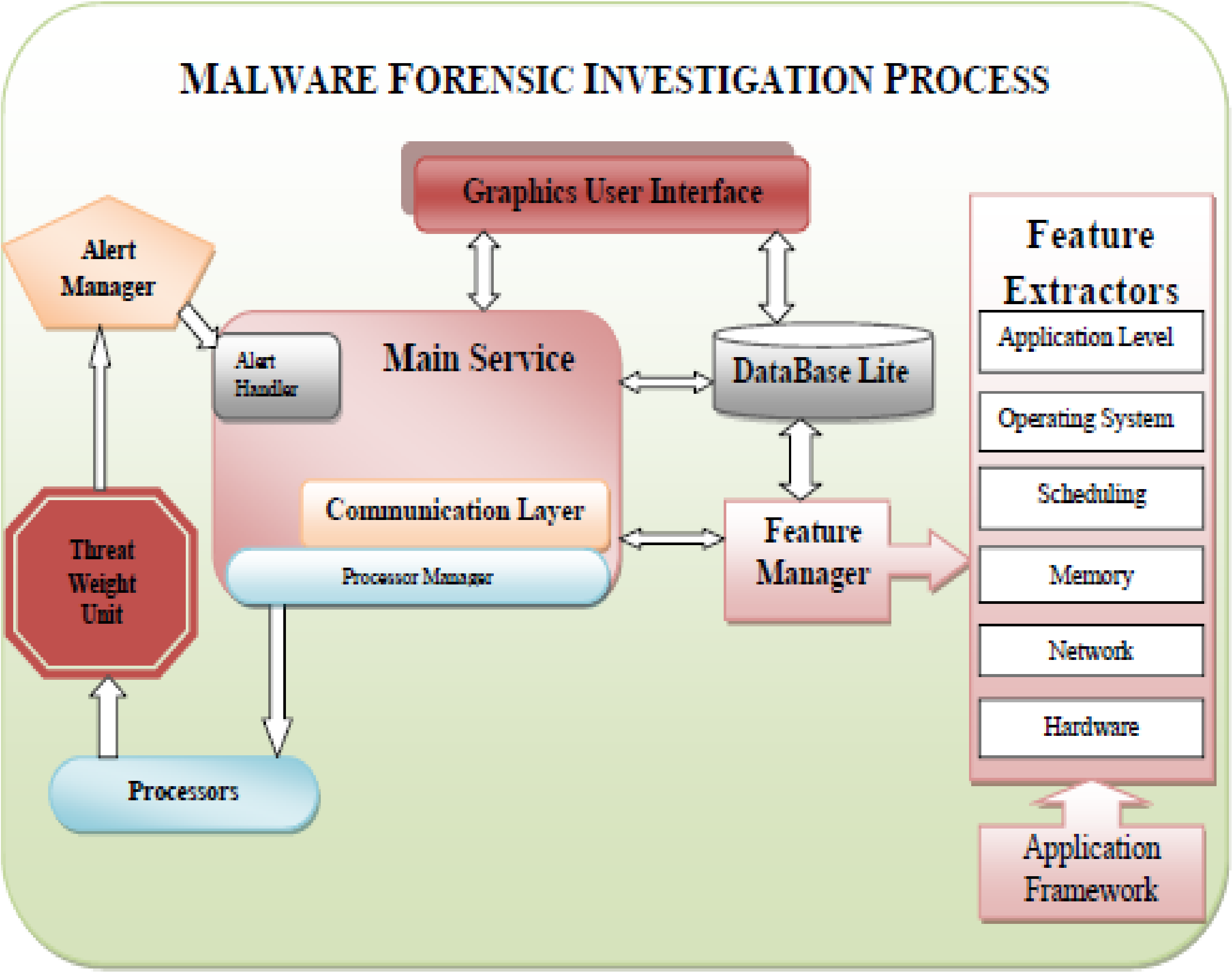

Fig. 4. Malware Analysis Landscape for Forensic Investigation

about the device to achieve a coherent Infection levels. Alert manager is produced final ranking TWU. In order to implement the so-smoothing function can provide a more constantly vigilant and avoid false alarm instantly. Examples of such functions Average and leaky - bucket can be mounted. Infection levels is simplified Compared with pre-set minimum and maximum thresholds.

iv. **The Main Agent Service**: The most important component is the main agent service. The service Convenience stores, synchronized malware detection and warning process. Agent Service facilities to manage the flow of new samples to detect the request, sending Processor, the new sample matrix and the final recommendation Alert Manager. Loggers are the debugging options for calibration of the offer and experiment with detection algorithms. Configuration Manager to manage Agent configuration (activating the processor, as an active feature extractors, Warning threshold, activating users, temporary gap sample detection mode Configuration, etc.). Warning as a result of an action handler can be sent Warning (for example, the visual alert information bar, the sending application uninstalling SMS or email, device lock, holds any communication through the notification Channels). Processor Manager / unregisters processor, and active/Register Processor deactivates. Manger agent operation Mode changes Based on the desired configuration and operation mode. The active/ Inactive processors and feature extractors. Changing the operation mode a full security mode and normal

v. mode is initiated as a result of Changes in the level of available resources (CPU, network).

vi. **Graphical User Interface:** The final component is the graphical user interface provides the user with this means the agent parameters to Configure, enable / disable (for practical use only), visual warnings, and the data collected explore the scene. With the help of digital forensics we investigate the system digital parts and collect the digital evidence by using digital forensics steps.

6. Conclusion And Future Work

This paper describes Landscape to analysis malware in victim system for forensic investigation. Data loss can be occurred due to malware. By analyze we identify the malware activities on the system. We propose a model for forensic investigation through threat weight unit. To this end, the detecting attack must be linked with security related technology in system navigation. Here, we get the investigation result by applying this model.

In future, we plan to implement this Landscape with algorithm and mathematical solution. In addition to it, we plan to evaluate this model against real and synthetic datasets.

Acknowledgment

We are grateful to Dr. Vishal Bhatnagar (Associate Professor, Ambedkar Institute of Communication Technologies and Research), & Mr. Gulshan Shrivastava (Assistant Professor, Dronacharya College of Engineering. Gr. Noida, U.P.) for taking time to read carefully drafts of this paper and provide us with valuable comments.

The authors are also grateful for thoughtful comments from reviewers who improved the content of the paper.

References

[1] Kaur, G., Nagpal, B. "Malware Analysis & its Application to Digital Forensic" International Journal on Computer Science and Engineering (IJCSE), Vol. 4, No. 04, Pp.622-626, 2012.

[2] Daryabar, F., Dehghantanha, A., Broujerdi, H. G. "Investigation of Malware Defence and Detection Techniques", International Journal of Digital Information and Wireless Communications (IJDIWC) 1(3): 682- 687 The Society of Digital Information and Wireless Communications, 2012.

[3] http://en.wikipedia.org seen on March 2012.

[4] Malin, C. H., Casey, E., Aquilina, J. M.,"Malware Forensics: Investigating and Analyzing Malicious Code", Syngress, 2008.

[5] Farmer, D. Venema, W., Forensic Discovery, Addison Wesley Professional, 2004.

[6] Jacob, G. Debar, H. & Filiol, E., "Behavioral detection of malware: From a survey towards an established taxonomy", Journal in Computer Virology, 4, 251–266, 2008.

[7] R. Richardson., "CSI Computer Crime & Security Survey", Computer Security Institute. Available online at: http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf seen on Feb., 2012.

[8] Shrivastava, G., Sharma, K., Dwivedi A.: Forensic Computing Models: Technical Overview, CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 207–216, 2012.