CHAPTER 4

MALWARE PROTECTION FROM NEW AGE THREATS

4.1 ABSTRACT

Malicious software, more commonly known as Malware incessantly causes immense damage to end user's home computers, corporates systems, user mobile and handheld devices. Access to authorized data being denied and released only after ransom demand has been paid is one of the top security concerns of today. The new age of digital extortion in form of Ransomware is leading to loss of access to data, disruption of normal operations, financial losses to restore files and systems as well as impacts the reputation of organizations.. This chapter presents the proposed Malware mitigation solution as a possible viable solution against malware.

4.2 RANSOMWARE MITIGATION PROCESS

Malware mitigation process is implemented using virtual environments hosted on Cloud based systems using independent Windows 2008 Servers on VMware virtual machines running open source and commercial tools. The system involves use of VMware templates with last saved running version for quick redeployment. The system comprises of three stages which offer Malware Behavioral Analysis, Code Analysis and Reporting environments as illustrated in Figure 4.1 below.

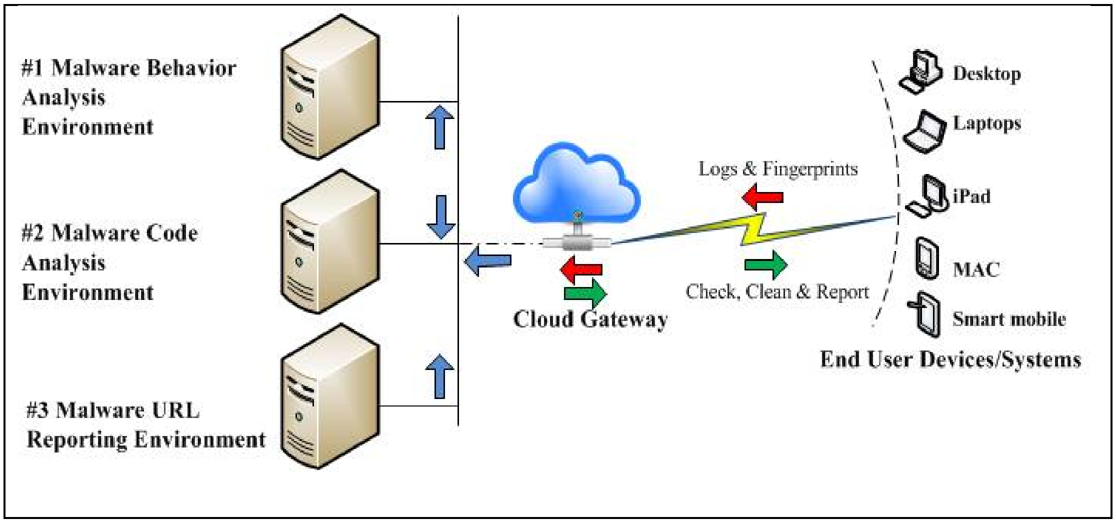
#1 Malware Behavior Analysis Environment
#2 Malware Code Analysis Environment
#3 Malware URL Reporting Environment
Cloud Gateway
Logs & Fingerprints
Check, Clean & Report
Desktop
Laptops
iPad
MAC
Smart mobile
End User Devices/Systems

Figure 4.1: Malware Detection Environments

Ransomware mitigation process to detect, block and remove is illustrated as follows:

- **Dynamic Analysis –** performs automated analysis of suspicious files which are scanned and analyzed for unique fingerprints and signatures or impact using tools as illustrated by Hughes, et al., (2014) and Zolkipli, et al. (2010) in which reports are produced at the end of analysis with information like registry keys used by malware, configuration changes done, device, file and network activity trends. However, automated scans do not necessarily provide detailed insight. These are signature based scans comparing and matching against a database of known malware signatures. Karbab, et al. (2016) presented fuzzy hashing fingerprints as an option for capturing malware static features against malware attacks and proposed use of emulation environment in order to extract the actual behavioral characteristics using fingerprinting as a novel solution.

- **Static Analysis –** is a manual analysis taking a deep insight at the malicious file's activities by looking at file headers, embedded resources, payload, hashes, signature and meta-data among host of other properties that are analyzed. Heuristic scans are done here that do not need a signature analysis. Rules and algorithms, commands which point to its malicious properties are evaluated to detect the malware. Anti-analysis trends in banking malware is proposed by Joseph, et al. (2016) in which reverse engineering process for six banking malware is analyzed and trends are presented for development of anti-analysis of malware.

- **Cloud Services –** is using IaaS to build virtualized environment, record and analyze behavior of malicious files and predict the next action or occurrence event. This is a real-time protection and system are updated several times a day to mitigate zero-day attack vectors. The system integrates with antivirus engines with a lightweight agent running on user devices (laptops, desktops or mobiles) to monitor any deviation or new files in the user devices. Xiaobao, et al. (2016) presented a novel method for detecting mobile applications infected by malware by using a scheme named locality sensitive hashing. Their proposed approach constructed new signatures from constituent malware blocks to construct malware variants and compared the approach with existing projects.

4.3 PROPOSED MALWARE MITIGATION SOLUTION

The design and implementation of the Malware mitigation solution is illustrated in this section and the malware mitigation solution process is illustrated in Figure 4.2 below.

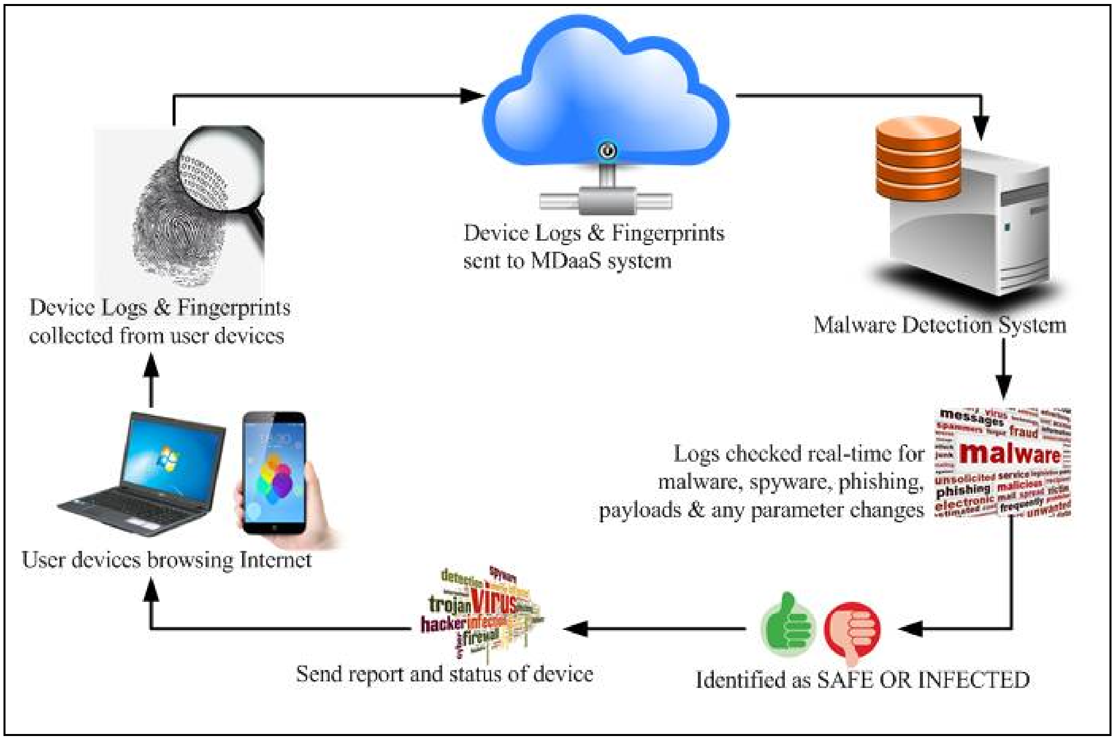
Device Logs & Fingerprints
sent to MDaaS system
Device Logs & Fingerprints
collected from user devices
Malware Detection System
Logs checked real-time for
malware, spyware, phishing,
payloads & any parameter changes
malware
User devices browsing Internet
trojan
virus
hacker
firewall
Send report and status of device
Identified as SAFE OR INFECTED

Figure 4.2: Malware Detection Process

The malware detection service environments are implemented using virtual machines running VMware Servers with Windows 2008 Server hosts in three lab environments over the Internet. End user devices are initially scanned, snapshot is taken and compared against existing template for malware. If found clean, a lightweight agent is installed on Windows and Android devices, running on the end user system as a service.

The main snapshot vectors considered from the end point devices are Host file, Auto-creation of any file or executables, emails being sent in a short durations or any changes or modifications in registry keys of system. This agent is tasked for sending the device snapshots to the malware monitoring system for tracking any changes to the system OS, Registry, Processes or critical Files. This agent sends the updated (malicious) files from the user devices to the test bed environment for analysis, detection and blocking.

For detection purposes, malware executing the payload to make changes in user systems and files are taken into account. Tests are performed on isolated system environments and three environments are implemented as having virtual machines with malware tools. The servers are commissioned and decommissioned each time a new malware analysis is completed. This is done in order to avoid any chance of the malware polymorphic features getting into action and potentially infecting the analysis servers, leaking data or payload to other systems, contacting the attacker for new action to perform or even upgrading themselves.

#1 Malware Behavior Analysis Environment

The first environment is configured for Malware Behavior Analysis, with server snapshots taken before and after receiving malware payload files. Logs are pulled from user devices and checked for any malware infection or device configuration and changes are analyzed here using tools which are described as follows:

- Process Monitor with Proc DOT tool determines the manner in which malware infects and the processes then interacts with the system, OS, Files and Registry.
- Wireshark sniffer for Network Bandwidth Monitoring and observing the malware payload attempts to contact the attacker, DNS or other external sources (P2P servers) for engaging bot traffic and trying to download the payload binaries or java scripts.
- Process Explorer and Process Hacker tools to observe malware behavior processes like opening of new ports, contacting attacker IP addresses.
- Lightweight agent combined with Regshot tool to take user system and device snapshots

#2 Malware Code Analysis Environment

The second environment is setup with Malware Code Analysis tools analyzing instructions in their assembly code and memory dumps from memory with the below mentioned tools described as follows:

- IDA Pro tool used as disassembler to parse Windows OS executable files
- Scylla Memory Dump tool for obtaining code from system memory. This is a novel way of code analysis since executable payload instructions are mostly encoded and extracted in RAM only during execution time.

#3 Malware Reporting Environment

This environment acts as the reporting system for Internet, analyzing Web URL proactively for sites hosting malware code or payloads. This also checks the user system and devices taking snapshots for before and after analysis comparing them and presenting the report. The tools required for this environment are presented as follows:

- MalWr, Threat Expert tools for automated behavior analysis of payload executables.

- Web Inspector MxToolKit for real time threat assessment and reputation of Web URL hosting suspected malware payloads and codes.

- Process Monitor with ProcDOT helps analyze processes read-write, update or delete registry entries. This helps ascertain the manner in which malware attempts their actions and begins the attack.

- File system and Registry analyzes, collecting the user data and checks for malware. Here dynamic analysis method is preformed to observe the malicious code behavior.

4.4 PERFORMANCE ANALYSIS

The proposed malware detection system displays certain advantages over existing systems, these are presented as follows.

- Malware scanning offered in form of a Cloud service over the Internet has inherent advantage of using pay-as-you-use services running over virtual platforms, global coverage, not having to worry about any in house breach over the local network infecting users and IT servers alike.

- Use of Virtual machines and Cloud infrastructure offers the advantage of not being limited by hardware or computing power, thus ensuring highly scalable setup and providing the antimalware services over long periods of time, while indexing huge databases and malware logs.

- This service can be further customized for end users by providing them the ability to upload and update logs/executables or even grab image of the infected systems. The geek users can be offered a virtual test bed to perform their own lab analysis.

- Yet another advantage with this system is the ability to inform each user as soon as a new malicious payload is detected, this benefits from the experience of others.

- This Malware mitigation system can be modified to offer specific payload blocking for different customers even as other customers of that very application program are able to access them and even benefit from experience of the infected customers. This model also helps in saving costs by promoting the BYOD concept.

The results obtained for malware detection system clearly point towards the proposed Malware detection system being better with such a solution as illustrated in Figure 4.3.

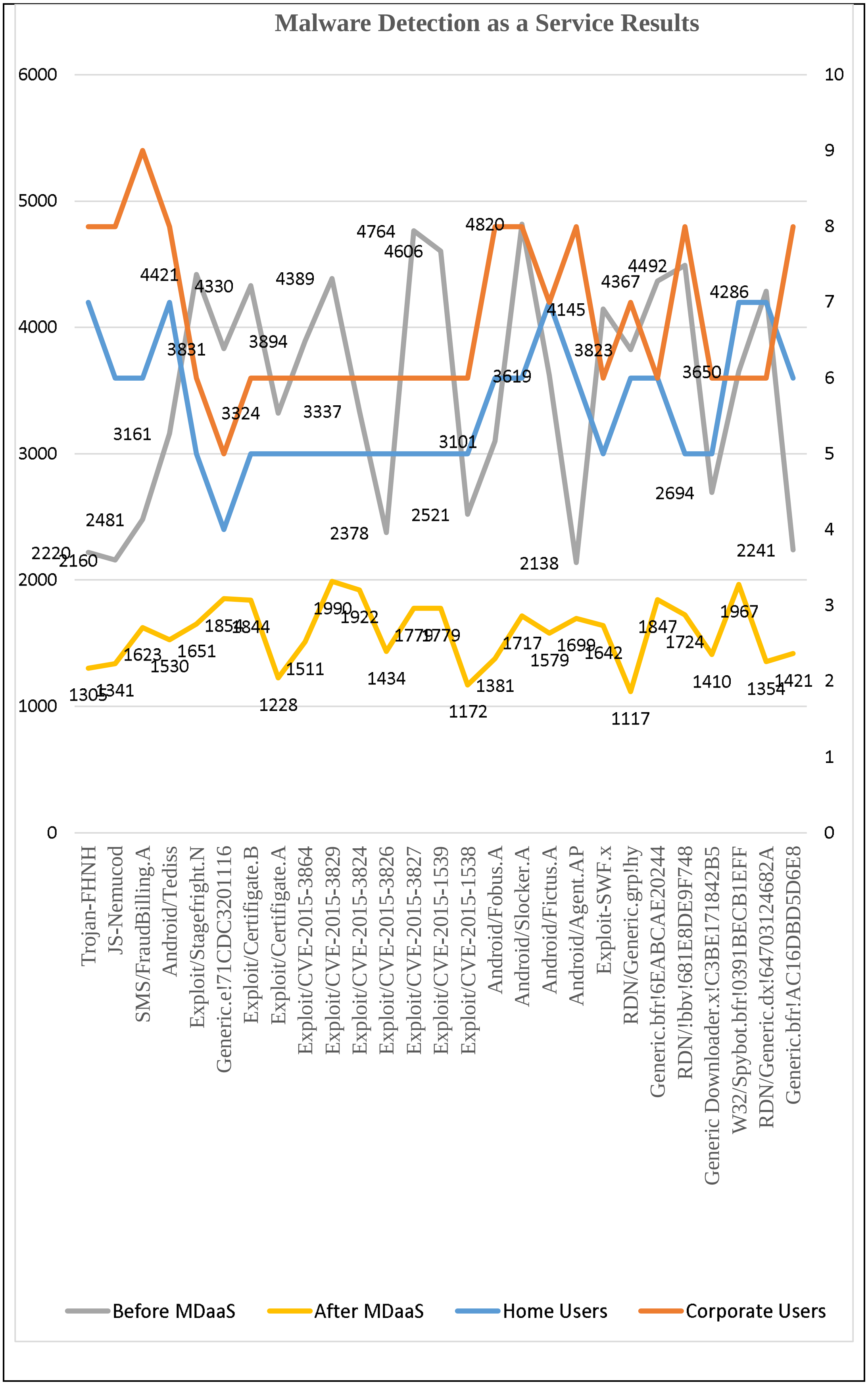

Figure 4.3: Malware Detection as a Service Results

CHAPTER SUMMARY

Malware detection using Cloud based services as the mitigation solution for malware detection as a service is an upcoming area of research. The proposed Cloud based malware mitigation solution for corporates and home users is implemented in this chapter using three phase environmental setup. The results obtained point to the proposed solution delivering far better results as compared to alternative solutions and options proposed by other authors like Hughes, et al., (2014), Zolkipli, et al. (2010), Karbab, et al. (2016), Joseph, et al. (2016) and Xiaobao, et al. (2016).

Since DDoS and Ransomware impacts user data by compromising on its privacy as well as data theft issues, there is an urgent need towards encryption for data security by using secure algorithms for network devices like Routers, Switches, Virtual Private Networks and Application Servers. User information and data more often than not, travels across unsecure Internet for Cloud based consumers. Securing this data in motion to ensure any unauthorized access is taking place has gained the highest priority for service providers. In the next chapter, the author analyzes cryptographic algorithms for encryption and encoding techniques which should be used in Cloud services for network devices and Cloud applications which require encryption for different protocols and functions.