International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

A Review on Fileless Malware Analysis Techniques

Vala Khushali
ME in Computer Engineering(Cyber Security)
Gujarat Technological University
Ahmedabad, Gujarat

***Abstract*---Malware refers to any malicious code or program that is harmful to systems. It is a major threat to the security of information in computer systems. Some of the types of malware that are most commonly used are viruses, worms, Trojans, etc. Nowadays, the rise of a new malware known as fileless malware and its defensive strategies can be used to mitigate it. Fileless malware may be a class of malware that runs entirely in memory and leave as small of a footprint on the target host as possible. Fileless malware attack windows applications and system administration tools such as PowerShell and Windows Management Instrumentation (WMI) to execute and spread fileless malware. In this paper, various Fileless malware detection and mitigation techniques are discussed and clear some misconceptions of technical details of Fileless malware.**

Keywords---Fileless Malware; PowerShell; Registry Entry; Windows Management Instrumentation (WMI); Process Injection

I. INTRODUCTION

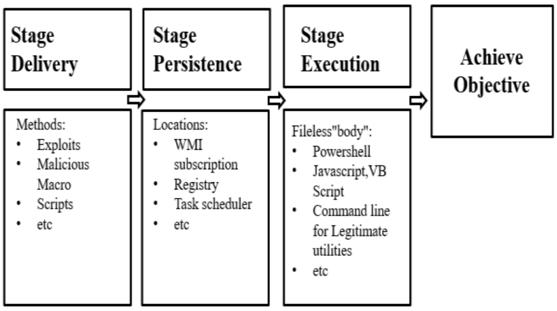
Malware is malicious software or a program to exploit the system and get the user's personal information. Malware of different names is given computer viruses, worms, Trojans, ransomware, scareware, spyware, cryptocurrency miners, adware, and other programs to exploit computer systems for harmful purposes [1]. The aim of such malware may be different in terms of its purpose of development, collecting personal data from its deciding systems.

Antivirus software is designed to detect, prevent, and take action to block or remove malicious software and its files from your computer. It will also scan your computer for behaviors that may signal the presence of new, unknown malware. Fileless malware is developed by the attackers during a way that it becomes very hard for antivirus to detect one. Fileless malware is written directly into memory on behalf of a file on a hard drive. After writing a malicious program or code to memory, the hacker sometimes attempts to gain persistence on the system. System administration tools like PowerShell and Windows Management Instrumentation (WMI) to execute and spread fileless malware [3].

Fileless Malware leaves no traces for antivirus software to detect so that making it very hard for antivirus software to detect fileless malware attacks, so discovering fileless malware attacks is a very challenging task for security analysts [3]. Because fileless malware does not require a file to be downloaded, it is truly difficult to prevent, detect, and remove.

- Fileless Malware Attack Life Cycle

Fileless Malware attacks can be mainly classified as attack life cycle following stages.



1. Lifecycle of Fileless Malware attack [3]

Stage 1. Fileless Delivery: Fileless attacks use social engineering to get users to click on a link and attachment in a phishing email. The malicious script, to hiding in flash on a website or in a document generated by an authorized application. Attackers use trusted applications because they want to ensure that traditional security monitoring technologies will not inspect any files or activities [3].

Stage 2. Fileless Persistence: Most fileless malware techniques are short-lived, attackers use several evasive techniques to achieve persistence. Storing malicious code in unusual locations associated with the operating system or common utilities, like Windows registry, WMI store, and SQL tables. Malicious Script direct passed as command line to PowerShell and stored in the registry and executed by OS Scheduler [3].

Stage 3. Malware Execution: When all the persistent mechanisms take place, the malware especially depends on the windows internals like PowerShell, JavaScript, and Macro Execution of the official documents and other legitimate resources of the windows executable [3].

II. LITURATURE SURVEY

Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis [1]

This paper mainly focuses on an overview of malware types and malware detection methods also discuss current malware analysis techniques. Detailed of malware detection methods such as the signature-based and heuristics-based, basically complete overview of malware detection. In the Detection process mainly two stages: analysis and detection.

- Malware Detection Methods

1. Signature Based Detection:

Currently available antivirus software use signature-based access. In process extracts a unique signature from captured malware file and use this signature to detect similar malware. A signature is a sequence of bytes or a file hash that easily identified specific malware. The main disadvantage of this detection is not difficult for attackers to change malware signature to evade detection by antivirus software. This is very effective and fast in the detection of known malware, but it is unable to capture newly released malware.

2. Heuristics Based Detection:

This is also known as an anomaly or behavior-based detection. In the detection process, the activities performed by malware in runtime analyzed a training phase. Below that, the file is labeled as a malicious file in the testing phase. The major disadvantage of behavior-based is considerable to false-positive rate and excessive monitoring time.

- Malware Analysis Techniques

1. Static Analysis

In this technique to analyzing the Portable Executable files without running them. A PE file needs to unpack and decompressed before analyzed. A dissembler tool can be useful like IDA pro and OlleyDbg that display assembly instructions, give information about the malware and extract patterns to identify the attacker.

2. Dynamic Analysis

In these techniques, suspicious files are executed and monitored in a controlled environment such as VM, emulator or simulator. It is also called behavior analysis.

Malware behavior normally when they detect such an environment and do not any malicious activities. Major advantage of dynamic analysis can detect known and unknown malware.

3. Hybrid Analysis

In these techniques, it gather Information about malware from static analysis and dynamic analysis. The main advantage of these techniques increases the ability to detect malicious programs correctly.

4. Memory Analysis

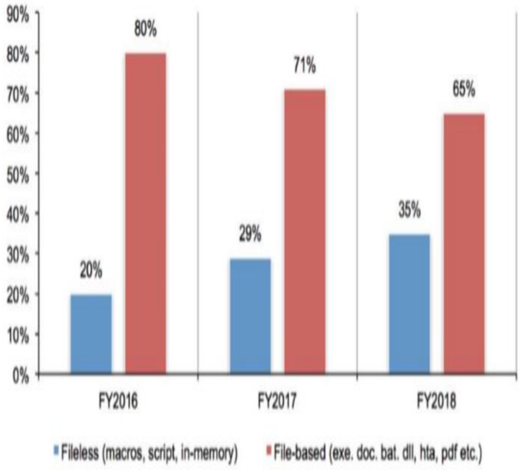
In current time it is a popular technique and also prove to be efficient and accurate in malware analysis. It can examine malware hooks and code outside the function normal scope. It uses a memory image to analyze information about running programs, operating system, and the general state of the computer. Memory forensic techniques can monitor malware behaviors such as API hooking, DLL injection and Hidden processes.

The Growth of Fileless Malware [2]

In current times, the rise of a new class of malware known as fileless malware. It is a class of malware that runs entirely in memory and to leave as small of a footprint on the target system. This new threat understand to clear up some misconceptions and identified assured characteristics that affect to this class of malware.

Fileless malware is also known as DLL injection, or memory injection attacks is a wide class of malicious attacks by attackers. All of the fileless attack is launched from an attacker's machine and injects itself into a memory of the victim system. This also looks like a traditional malware, except instead of trying to get itself installed on the target system. They count on a vulnerability in the computer at runtime to send code to the memory of the system through the network. In this paper, also analyze reports of fileless malware and the work of the industry leaders.

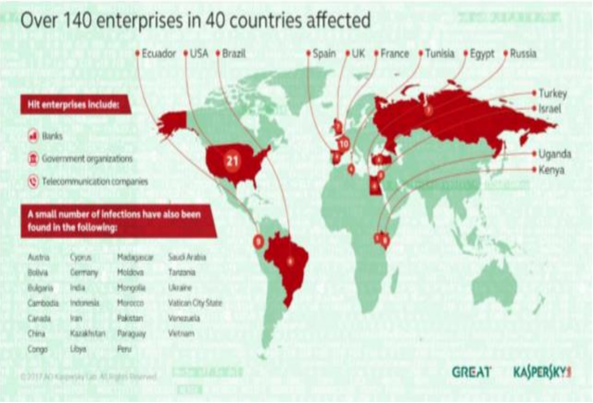
Fileless malware overlaps with another types of attack is called Living Off the Land in this attack attackers only utilize the software already on the machine to conduct attacks.



2. The growth of fileless and file-based attacks [2]

In this Fig.2 to indicate the shift away from file-based attacks into fileless malware attacks, with a graph of all attacks utilizing fileless techniques in 2018.

In February of 2017, researchers with Kaspersky Lab's Global Research and analysis team explained attacks on organizations around the world and the attackers used fileless malware hidden in memory of the affected servers. In fig. it was reported more than 140 enterprises in 40 countries were affected.



3. The hidden-malware enterprise attacks: victim geography [2]

An Approach to Detect Fileless Malware and Defend its Evasive mechanisms[3]

Recently many different types of malware have been increasingly trying to unnoticed by antivirus software and attack the system. One of the malware is fileless malware. It is leaving no trace after its execution. So, Author discussed

Malware Evasion techniques, Categories of fileless malware, Fileless malware detection, and mitigation.

- Categories of Fileless Malware

1. *RAM resident Fileless malware*

Most of the antivirus solutions checks are done when a new process starts and processes are already running on the system are choose unsuspicious for the antivirus solutions. So, it does not choose any event if malware not creating anything on the disk. Fileless malware occupy and run in RAM has more persistence when compared to other malware.

2. Script Based Fileless malware

Scripts is a popular attack vector for compromising a system. The main advantage of developing script-based malware is to exploit the vulnerabilities of the present in the MS Office, Windows applications and Windows PowerShell.

- Malware Evasion Techniques

1. *Malicious Documents*

Mostly document download by the adversary supplies and email attachment. Document script abilities to launching programs and downloading malicious code and run directly in the memory of the endpoint as part of the fileless infection.

2. *Malicious Scripts*

Microsoft Windows includes script interpreters for PowerShell, VBScript, batch files and JavaScript. To run these scripts use powershell.exe, script.exe, cmd.exe, and mshta.exe. So, the scripts that run directly on Microsoft Windows.

3. *Living off the Land*

Living off the Land in this attack attackers only utilize the software already on the machine to conduct attacks. Once the malicious code can interact with local programs so starting the infection with a document, and misuse the OS to download malicious artifacts, launch malicious programs and scripts, and steal data.

4. *Malicious Code in Memory*

Memory is volatile and dynamic and gives an opportunity to malware changes in its shape and operate the blind spot of antivirus and similar technologies. When attacker starts executing malicious code on the endpoint, the adversary can unpack malware into memory without saving artifacts to the file system.

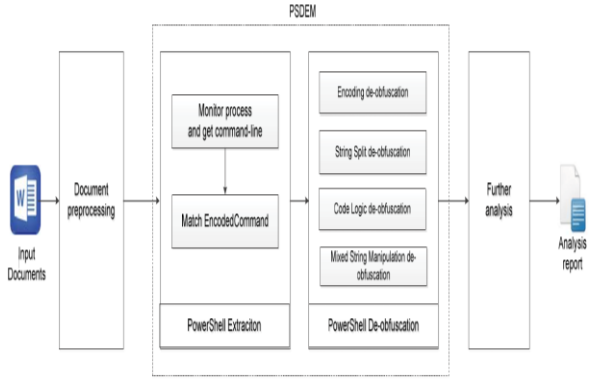
Fileless Malware Detection is finding a new approach to the executable in the system. In the detection process also use traditional approaches like Sandboxing, execution emulation using tools such as ProcMon, Yara, and heuristics-based.

Fileless Malware useful some Mitigation points:

- ➢ Perform OS patches and updates periodically.
- ➢ Restrict the PowerShell usage policy to restricted access to run the scripts through windows policy.
- ➢ Perform Behavior-based analysis.
- ➢ Periodically check the recent patches for vulnerabilities in the application and security checks frequently.

PSDEM: A Feasible De-Obfuscation Method for Malicious PowerShell Detection [2]

In this paper, the author proposes a de-obfuscation method of PowerShell called PSDEM. Mostly attacker uses PowerShell malware arrives via spam email, using a combination of Microsoft Word documents to infect victims with its deadly payload. In PSDEM method has two layers de-obfuscation to get original PowerShell scripts. The first layer is extracting PowerShell scripts from the obfuscated document code. The second layer is de-obfuscation scripts including encoding, string manipulation, and code logic obfuscation. PSDEM increases the efficiency and accuracy rate for analyzing malicious PowerShell scripts in word documents.


PSDEM
Input Documents
Document preprocessing
Monitor process and get command-line
Match EncodedCommand
PowerShell Extraciton
Encoding de-obfuscation
String Split de-obfuscation
Code Logic de-obfuscation
Mixed String Manipulation de-obfuscation
PowerShell De-obfuscation
Further analysis
Analysis report

4. Overall structure of the tool PSDEM [4]

In this fig, the complete structure of the tool of PSDEM. The tool has four main steps:

1. *Document Pre-processing*

Each of Word 2007-2016 document is a ZIP archive.so, use the signature of ZIP to identify OOXML files. This tool provides a complete environment for malicious documents.

2. *PowerShell Extraction*

This tool uses the PSDEM method to get PowerShell from Word documents. When monitors the process,

to make documents open completely and catch the command line of the powershell.exe process.

3. *PowerShell De-obfuscation*

PSDEM has used obfuscation methods such as Encoding obfuscation, String Split obfuscation, Code Logic obfuscation, Mixed String Manipulation obfuscation. The tool takes different actions and gets original scripts once the regex designed according to the features of different obfuscation methods matches successfully.

1. *Further Analysis*

The tool has got original PowerShell scripts in Word documents. So, attack to easily understand now. The scripts are used downloader, visit malicious websites and saving payload in the folder called temp. The scripts .exe file has downloaded in the backstage. The tool will extract the payload and URLs to analyze.

III. LITERATURE REVIEW AT GLANCE

Sr. No.	Title of Paper	Major Contribution	Further extension
I.	A Survey on Malware Analysis Techniques:	Explain Malware types, Detection methods,	Memory Analysis gives detailed

	Static, Dynamic, Hybrid and Memory Analysis[1]	Analysis techniques.	analysis of Malware.
II.	The Growth of Fileless Malware[4]	Clear up some misconceptions and identify certain characteristics that belong to this class of malware.	Software endpoint solution that performs automatic behavioural analysis of a computer system and could detect and stop Fileless malware from loaded into Memory.
III.	An Approach to Detect Fileless Malware and Defend its Evasive mechanisms[3]	Technical details of Fileless malware on various Fileless malware detection and mitigation techniques.	Behavioural analysis allows efficient detection of fileless threats on execution stage.
IV.	PSDEM: A Feasible De-Obfuscation Method for Malicious PowerShell Detection[6]	Design an automatic de-obfuscation and analysis tool for malicious PowerShell scripts in Word documents based on PSDEM.	Macro Security concerns.

IV. CONCLUSION

Fileless Malware is the real and critical threat that should be known and understood by all computer users. Malware that runs entirely in memory and to leave as small of a footprint on the target system. Different detection techniques to be used to overcome the effect of fileless malware. Fileless malware attacks directly windows applications and system administration tools such as PowerShell and Windows Management Instrumentation (WMI) to exploit and spread fileless malware. PSDEM tool used to detect malicious document run in PowerShell. It would be much better if the software has an endpoint solution that performs automatic behavioral analysis of a computer system and detect and stop fileless malware from loaded into memory.

REFERENCES

[1] Rami Sihwail, Khairuddin Omar, K. A. Z. Ariffin "A Survey on Malware Analysis Techniques: Static, Dynamic, Hybrid and Memory Analysis " *International Journal on Advance Science Engineering Information Technology,* Vol.8 (2018) No. 4-2 ISSN: 2088-5334

[2] Alain Alzuri, David Andrade, Yadelis Nunez Escobar, and Brian M. Zamora, Member, IEEE "The Growth of Fileless Malware "

[3] Sanjay B N, Rakshith D C , Akash R B, Dr.Vinay V Hegde "An Approach to Detect Fileless Malware and Defend its Evasive mechanisms" *3rd IEEE International Conference on Computational Systems and Information Technology for Sustainable Solutions* 2018

[4] Chao Liu, Bin Xia, Min Yu, Yunzheng Liu, "PSDEM: A Feasible De-Obfuscation Method for Malicious PowerShell Detection" *IEEE Symposium on Computers and Communications* (ISCC)2018

[5] Buddy Tancio "Hunting for Ghosts in Fileless Attacks" *SANS Institute 2019 Information Security Reading Room*

[6] Aru Okereke Eze and Chiaghana Chukwunonso E "Malware Analysis and Mitigation in Information Preservation" *IOSR Journal of Computer Engineering (IOSR-JCE)* e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 4, Ver. I (Jul - Aug 2018), PP 53-62 www.iosrjournals.org

[7] Ekta Gandotra, Divya Bansal, Sanjeev Sofat "Malware Analysis and Classification: A Survey" *Journal of Information Security, 2014, 5, 56-64*

[8] Liu, D., Wang, H., and Stavrou, A, "Detecting malicious javascript in pdf through document instrumentation," *in Proc. of the 44th Annual Int. Conf. on Dependable Systems and Networks*, 2014, pp. 100-111.

[9] Endpoint Security Trends and the Rising Threat of Fileless Malware Attacks. (2017, November 23). Retrieved from https://www.hipaajournal.com/endpoint-security-trends-filelessmalware-attacks/