Fileless cyberattacks: Analysis and classification

Cameron Noakes

February 2022

1 Sentence Overview

Analysis of 10 selected cyberattacks over the past five years where fileless attack techniques were used, the researchers propose a methodology for classifications based on the ATT&CK techniques and characteristics used in fileless cyberattacks followed by how the response time can be improved using the developed classification technique.

2 Introduction

The focus of the literature is fileless malware cyber attacks done by adversarial threat actors. The attackers develop fileless malware to bypass existing detection techniques and tools. To prepare for these attacks analysts are publishing analysis reports to help manage and better understand fileless malware.

The researchers outlined a key focus for their study for how despite the analysis of individual fileless malware, studies on fileless cyberattacks in their entirety still remain insufficient. There is a demand for literature examining such attacks.

3 Literature Review

They confirmed that, from a surveyed literature, among the malicious code collected, 10 percent were fileless cyberattacks, highlighting the new and hidden ways of cyber attacks currently.

Due to fileless cyber attacks being 10 percent this identifies how they are often uncommon and most likely do not have the necessary security mechanisms in place due to them not being as prevalent as other cyber attacks.

Kumar and sudhakar analysed seven fileless cyber attack samples and classified them based on persistent techniques outlined in ATT&CK.

4 Methodology

The researchers collected public fileless cyber attack samples (through Hybrid Analysis and GitHub) and then analyzed the techniques used through open source intelligence (OSINT), Cuckoo Sandbox was then used to extract the results from the OSINT.

The collected information was then used to map the fileless malware to ATT&CK techniques which then allowed scores and classifications to be made on the fileless malware cyber attacks.

Various namd fileless malware cyber attacks were listed such as Poweliks, WannaCry and Petya.

5 Cuckoo Sandbox Analysis

Cucko Sandbox uses a virtual environment to provide information on malware, it is an open source malware analysis system. The static analysis information refers to portable executable (PE) and resource information on the process (number of processes generated by the malicious code).

The number of 'file drops' refers to the number of files that malicious code installs or downloads on the computer.

6 Conclusion

Actual samples were obtained and analyzed using Cuckoo Sandbox. each fileless cyber attack ratio was identified and analyzed across three dimensions. Fileless cyberattacks were then classified into ATT&CK techniques.

7 What problem does this solve?

The outlined examined problem is that of fileless malware cyber attacks, due to their nature, are often difficult to identify and protect against, the literature explains these limitations and proposes a model to help with the cyber security of infrastructure.

8 How do they solve it?

the researchers propose a methodology for classifications based on the ATT&CK techniques and characteristics used in fileless cyberattacks followed by how the response time can be improved using their proposition.

9 How do they assess it?

There was no mention of evaluating the proposed system developed or an assessment to assess the end results from the proposed system.