Extracted Sections

Extracted Sections

To effectively gather data for digital forensics purposes, we need to focus on sections that provide actionable insights into the behavior, activities, and artifacts of potentially malicious software. These sections typically include:

1. **General Info** : This section provides high-level details about the file, such as its name, hash values (MD5, SHA1, SHA256), and any known threats. These details are crucial for identifying and categorizing the file, as well as correlating it with other samples in threat databases.
2. **Behavior Activities** : This section documents the actions performed by the software during analysis. It includes both malicious and suspicious activities, such as process creation, file manipulation, network connections, and registry modifications. These activities are key indicators of compromise (IOCs) that help forensic analysts understand the nature and intent of the software.
3. **Process Information** : Listing processes involved in the execution of the software helps identify potential entry points and lateral movements within the system. Understanding the relationships between processes can reveal how the malware propagates or communicates with other parts of the system.
4. **Registry Activity** : Changes to the Windows Registry can indicate persistence mechanisms used by malware to maintain control over the system. Monitoring these changes helps forensic analysts reconstruct the timeline of events and understand how the system was compromised.
5. **Files Activity** : This section details the files created, modified, or deleted by the software. It includes executable files, suspicious files, and dropped files, which are often used by malware to establish a foothold or execute malicious payloads. Analyzing these files can uncover additional evidence of malicious activity.
6. **Network Activity** : Network-related information, such as HTTP(S) requests, DNS queries, and connections, provides insight into communication patterns with external servers. This data helps determine whether the software is attempting to exfiltrate data, download additional payloads, or communicate with command-and-control (C2) servers.

By focusing on these sections, we ensure that the extracted data is directly applicable to digital forensics investigations. These sections collectively provide a comprehensive view of the software's behavior, artifacts, and potential impact on the system, enabling us to build a robust case for further analysis and remediation

Why I Did Not Extract Data from the Behavior Graph

After extracting data from the behavior graph, I found that it only contains a subset of the information already available in the **Process Information** section. Additionally, the graph is stored in SVG format, relying on extensive XML code to generate the visualization. This makes it complex to parse programmatically without adding significant value, as the key details are more efficiently accessible in structured sections of the report. Given these factors, scraping the behavior graph would be redundant and unnecessarily resource-intensive

Malware analysis Data-5544-J5823545.doc.zip Malicious activity | ANY.RUN - Malware Sandbox Online