Types of Malware Analysis

Vijayabharathi (MT20ACS545)

Agenda

- What is Malware Analysis ?
- Types of Malware Analysis
  - Static Analysis
  - Dynamic Analysis
  - Hybrid Analysis
  - Reverse Engineering
- Malware Analysis Use Cases
- Demo

What is Malware Analysis ?

What is Malware ?

- Malware (malicious software) is a term used to describe any program or code that is created with the intent to do harm to a computer, network, or server.

- Malwares are used by the adversaries to get persistent access to a system.

- Once the malware takes control of the system with the purpose of communicating back to its original sender.

- The information it communicates may be sensitive data, intellectual property, captured keystrokes, images from a device’s camera, etc

Types of Malwares

- Virus (e.g. Mydoom, Melissa)
- Worms (e.g. Morris Worm, Stuxnet)
- Trojan horse (e.g. Emotet, Storm)
- Backdoor (e.g. ShadowPad, FinSpy)
- Root kit (e.g. Rovnix, Olmasco)
- Spyware (e.g. Pegasus, Gator)
- Adware (e.g. DeskAd, Fireball)
- Ransomware (e.g. Locky, WannaCry)
- Bots (e.g. Methbot, Mirai)

What is Malware Analysis ?

- Malware analysis is the process of understanding the behaviour and purpose of a suspicious file or URL.

- This is a study or process of determining the functionality, origin, impact of a given vulnerable file, program, URL.

- The output of the analysis aids in the detection and mitigation of the potential threat.

Purpose of Malware Analysis

- To determine the risk associated with a unknown file or URL.
- To identify the nature and functionalities of the malware.
- To know the repercussions of the malware attack.
- To understand the extent of malware infection.
- To prioritize the incidents by level of severity of threats.
- To uncover hidden indicators of compromise (IOCs) that should be blocked.
- To improve the efficacy of IOC alerts and notifications.
- To help the security analyst for enriching context of threat hunting.

Types of Malware Analysis

Types of Malware Analysis

- Static Analysis
- Dynamic Analysis
- Hybrid Analysis
- Reverse Engineering

Static Malware Analysis

- Static analysis examines the file for signs of malicious intent. It can be useful to identify malicious infrastructure, libraries or packed files.

- Static analysis does not require that the code is actually run. It’s identifying malwares based on signatures.

- Technical indicators are identified such as file names, hashes, strings such as IP addresses, domains, and file header data can be used to determine whether that file is malicious.

- Tools like disassemblers and network analysers can be used to observe the malware without actually running it in order to collect information on how the malware works.

Types of Malware Signatures

- Signature is a typical footprint or pattern associated with a malicious attack on a computer network or system.

- A Malware signature is a continuous sequence of bytes that is common for a certain malware sample. That means it’s contained within the malware or the infected file and not in unaffected files.

➢ Strict signatures
➢ Loose signatures
➢ Signature free

Dynamic Malware Analysis

- Dynamic malware analysis executes suspected malicious code in a safe environment called a sandbox.

- This closed system enables security professionals to watch the malware in action without the risk of letting it infect their system or escape into the enterprise network.

- Dynamic analysis provides threat hunters and incident responders with deeper visibility, allowing them to uncover the true nature of a threat. As a secondary benefit, automated sandboxing eliminates the time it would take to reverse engineer a file to discover the malicious code.

- To deceive a sandbox, adversaries hide code inside them that may remain dormant until certain conditions are met. They are using packers and crypters to save malwares from AV.

Malware Sandbox

- A sandbox is an isolated environment on a network that mimics end-user operating environments. Sandboxes are used to safely execute suspicious code without risking harm to the host device or network.

- Using a sandbox for malware detection provides another layer of protection against new security threats—zero-day (previously unseen) malware and stealthy attacks

- Sandbox environments provide a proactive layer of network security defense against new and Advanced Persistent Threats (APT).

- Detect Unknown Threats
- Identify Related Threats
- Achieve Complete Visibility
- Respond Faster
- Automation

Hybrid Malware Analysis

- Basic static analysis isn’t a reliable way to detect sophisticated malicious code, and sophisticated malware can sometimes hide from the presence of sandbox technology.

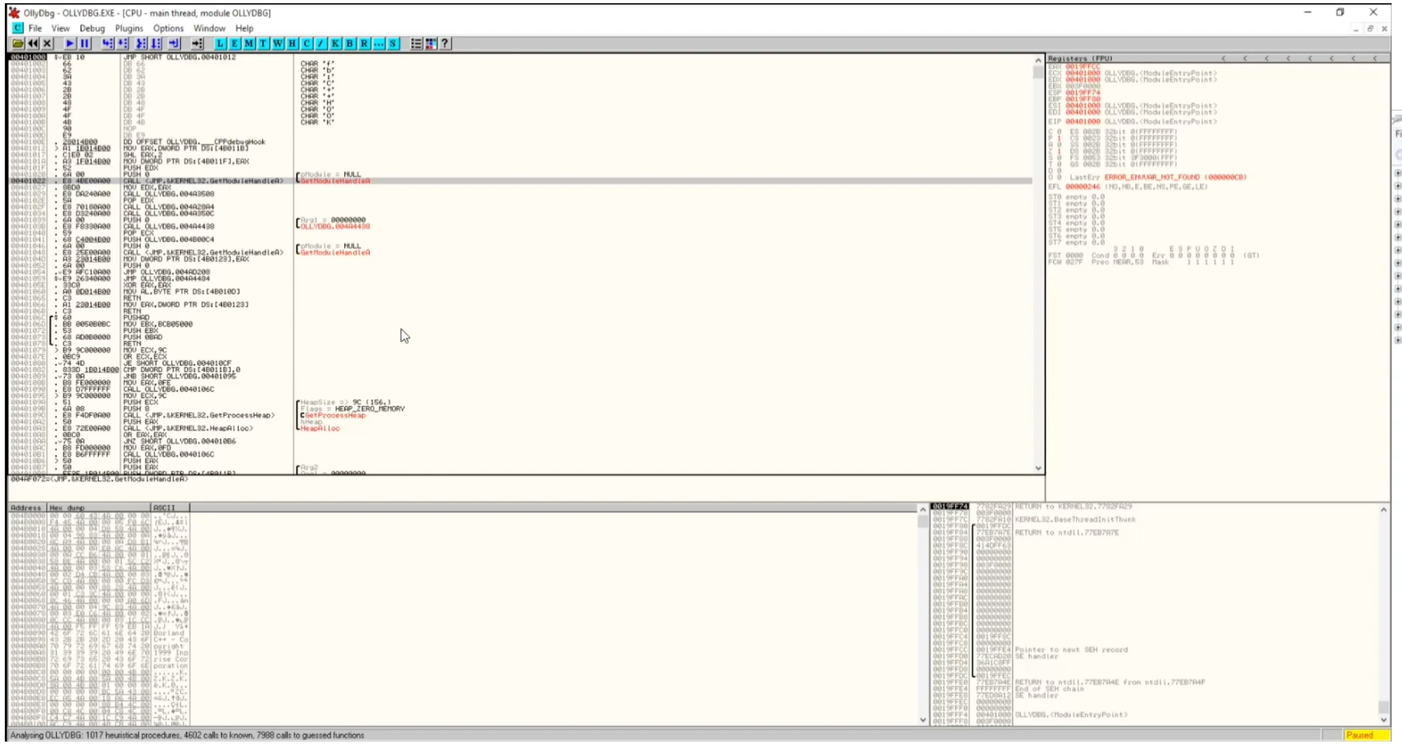
- By combining static and dynamic analysis techniques, hybrid analysis provide security team the best of both approaches – primarily because it can detect malicious code that is trying to hide, and then can extract many more indicators of compromise (IOCs) by statically and previously unseen code.

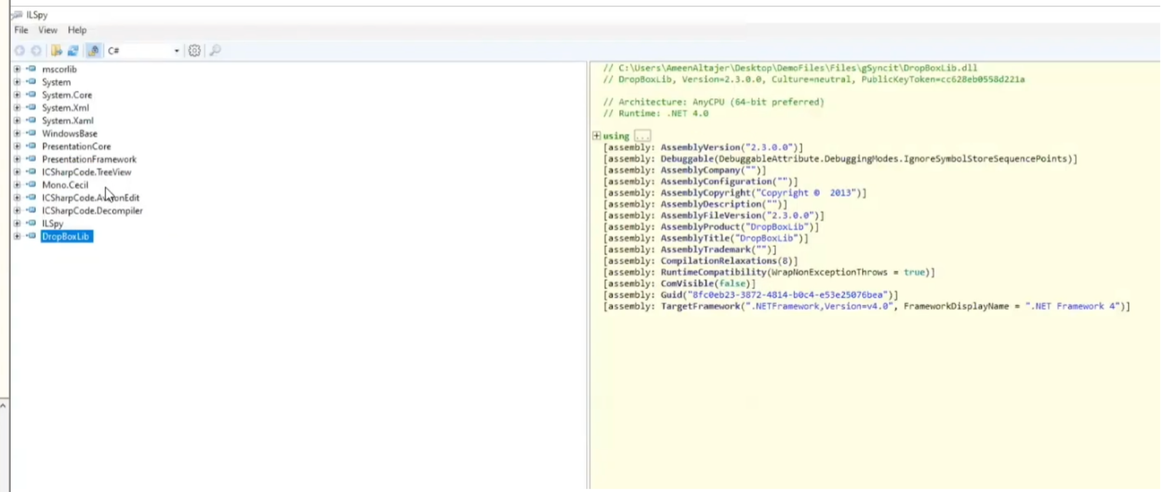
- Hybrid analysis helps detect unknown threats, even those from the most sophisticated malware even zero-day exploits would be exposed.

Reverse Engineering

- Reverse Engineering – “ Taking things apart to understand how they work “
- Dissect the software to understand how it works and understand the intention behind it.
- In this type, analysts will use debuggers, disassemblers, compilers and specialized tools to decode encrypted data, determine the logic behind the malware algorithm and understand any hidden capabilities that the malware has not yet exhibited.
- Code reversing is a rare skill, and executing code reversals takes a great deal of time. For these reasons, malware investigations often skip this step and therefore miss out on a lot of valuable insights into the nature of the malware.

Reverse Engineering





https://youtu.be/RnbLCI-_UzQ

Malware Analysis Use cases

Malware Detection

- Malware detection is a process of identifying malware by doing deep behavioral analysis and by identifying shared code, malicious functionality or infrastructure, threats can be more effectively detected.

- Output of malware analysis is the extraction of IOCs. The IOCs may then be fed into SEIMs, threat intelligence platforms (TIPs) and security orchestration tools to aid in alerting teams to related threats in the future.

Threat Alerts and Incident Response

- Malware analysis solutions provide higher-fidelity alerts earlier in the attack life cycle. Therefore, teams can save time by prioritizing the results of these alerts over other technologies.

- The goal of the incident response (IR) team is to provide root cause analysis, determine impact and succeed in remediation and recovery.

- The malware analysis process aids in the efficiency and effectiveness of this effort.

Threat Hunting and Malware Research

- Malware analysis can expose behavior and artifacts that threat hunters can use to find similar activity, such as access to a particular network connection, port or domain.

- By searching firewall and proxy logs or SIEM data, teams can use this data to find similar threats.

- Academic or industry malware researchers perform malware analysis to gain an understanding of the latest techniques, exploits and tools used by adversaries.

Demo

Thank you...!