Malware Reverse Engineering

Types of Malware Analysis

- There are three types of malware analysis that can be conducted:

- Static malware analysis
- Dynamic malware analysis
- Hybrid malware analysis

Static Malware Analysis

- Examines files for signs of malicious intent
- A basic static analysis does not require a malware code that is actually running
- It is useful for revealing malicious infrastructure, packed files, or libraries
- Technical indicators like file names, hashes, strings such as IP addresses, domains, and file header data are identified

Static Malware Analysis

- Various tools like disassemblers and network analyzers have the ability to observe the malware without running it

- These tools can gather information on how the particular malware works

- Since static malware analysis does not run the malware code, there can be malicious runtime behavior in some sophisticated malware, which can go undetected

Static Malware Analysis

- **Example :** a file that generates a string and downloads a malicious file depending on the dynamic string

- The malware could go undetected if a basic static malware analysis is used

- In these cases, dynamic analysis is more helpful in getting a complete understanding of the file behavior

Dynamic Malware Analysis

- A suspected malicious code is run in a safe environment called a sandbox

- This isolated VM is a closed system that allows security experts to observe the malware closely in action without the risk of system or network infection

- This technique provides deeper visibility of the threat and its true nature

Dynamic Malware Analysis

- Automated sandboxing, eliminates the time, which otherwise would have been spent for reverse engineering a file to discover a malicious code

- Dynamic analysis can be a challenge, especially against smart adversaries who know sandboxes will be used eventually

- So, as a form of deception, adversaries hide their code in a way that it remains dormant until specific conditions are met. The code will run only then.

Hybrid Malware Analysis

- We already know now that basic static analysis isn't reliable when the malware has a more sophisticated code, and sophisticated malware are sometimes, able to avoid detection by sandbox technology.

- Combining both types of malware analysis techniques offers the best of both approaches

- Hybrid analysis can detect hidden malicious code, and extract many more IOCs by statically and previously unseen code

Hybrid Malware Analysis

- It is capable of detecting unknown threats, even from the most sophisticated malware

- The hybrid analysis applies static analysis to the data that is generated by behavioral analysis

- Consider a piece of malicious code that runs and causes some changes in memory. The dynamic analysis will be able to detect that and Analysts will immediately know to perform static analysis on that memory dump. This will result in more Indicators of Compromise (IOC)s and exposed zero-day exploits.

Static Vs Dynamic Malware Analysis

- **Analysis**
- Static malware analysis analyzes a malware sample without executing it, eliminating the need for an analyst through each and every phase.

- It observes the behavior of the sample and determines its capability and the extent to which it can exert damage to the system

- Dynamic analysis, performs analysis using the behavior and actions of the malware sample, which means that it works during the execution of the code with proper monitoring.

Static Vs Dynamic Malware Analysis

- **Technique**
- Static analysis involves signature analysis of the malware binary file.

- The binary file has a unique identifier and can be reverse-engineered with the help of a disassembler such as IDA that converts the machine-executable code into assembly language code.

- Some of the techniques used in this type of malware analysis are virus scanning, packer detection, file fingerprinting, debugging, and memory dumping.

Static Vs Dynamic Malware Analysis

- **Technique**
- Dynamic analysis involves a sandbox environment so that analyzing the behavior of malware while running the program won't affect other systems.

- Commercial sandboxes replace manual analysis with automated analysis.

Static Vs Dynamic Malware Analysis

- **Approach**
- Static analysis has a signature-based approach when it comes to malware detection and analysis.
- The unique identifier in malware is a sequence of bytes.
- The signatures are scanned using different patterns.
- The antimalware programs that are signature-based are effective only against common malware.

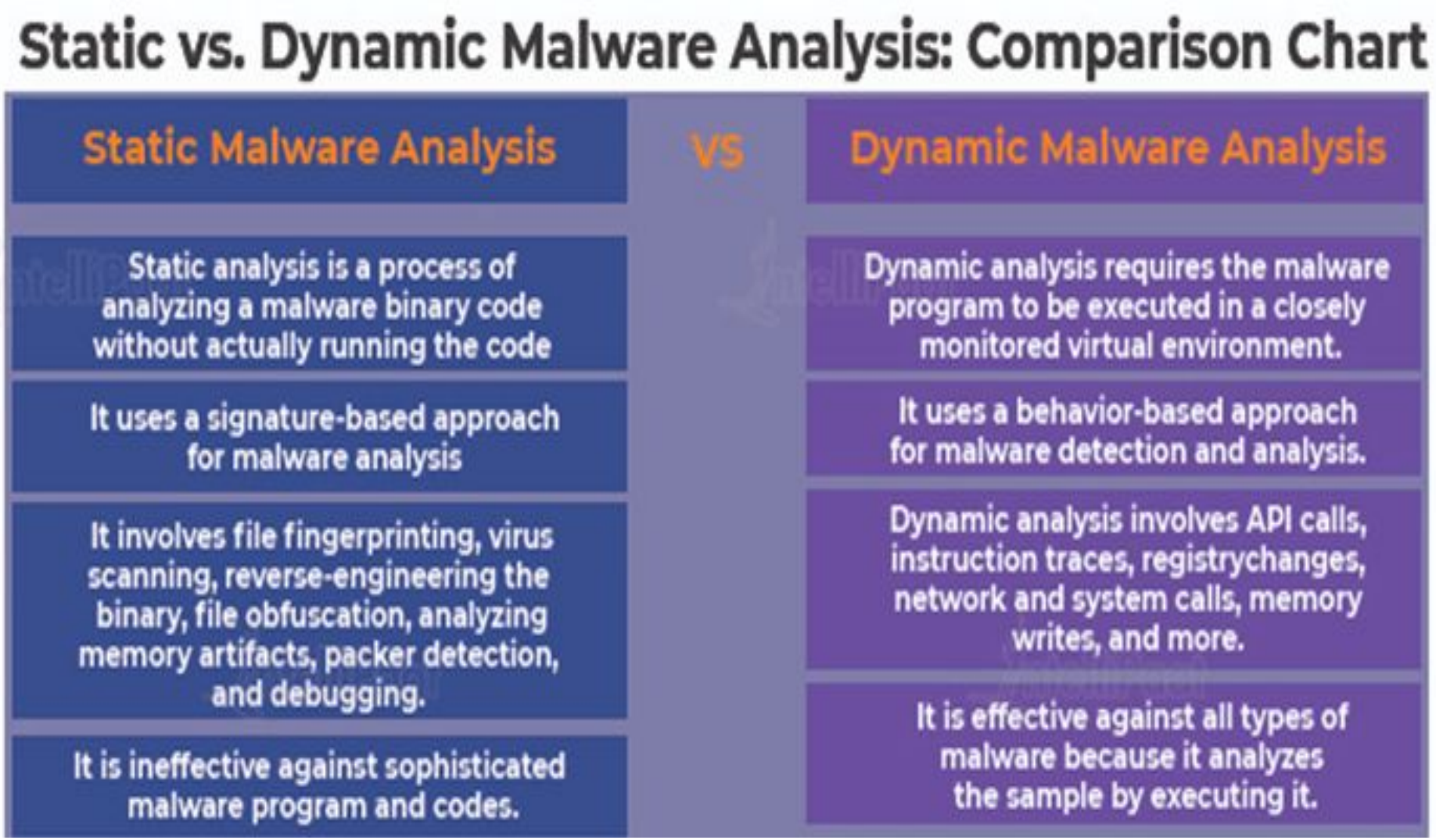
Static Vs Dynamic Malware Analysis

- **Approach**
- These are ineffective when it comes to sophisticated and advanced malware. This is where dynamic malware analysis comes into the picture.

- The dynamic analysis doesn’t have a signature-based approach. Instead, it uses a behavior-based approach that determines the functionality of the malware.

- It involves studying the actions performed by the malware.

Static Vs Dynamic Malware Analysis



Malware Analysis Use Cases

- **Malware Detection**
- More and more sophisticated techniques are being used by adversaries to evade traditional detection mechanisms.

- Threats can be more effectively detected through deep behavioral analysis by identifying shared code, malicious functionality, or infrastructure.

- Additionally, malware analysis results in the extraction of IOCs.

Malware Analysis Use Cases

- **Malware Detection**
- These IOCs can then be fed into threat intelligence platforms (TIPs), SEIMs, and security orchestration tools for alerting teams to related threats in the future.

Malware Analysis Use Cases

- **Threat Hunting**
- Threat hunters can use the behavior and artifacts that are exposed by malware analysis to find similar activities, like accessing a particular network connection, domain, or port.

- Searching firewall, proxy logs, or SIEM data can help find similar threats.

Malware Analysis Use Cases

- **Threat Alerts and Triage**
- The outputs of malware analysis offer higher-fidelity alerts early in the attack life cycle thus saving time by triaging the results of these alerts.

- **Incident Response (IR)**
- The objective of the IR team is to perform root cause analysis, determine the impact, and successfully offer remediation and recovery solutions.

- Malware analysis helps in the efficacy of this effort.

Malware Analysis Use Cases

- **Malware Research**
- All industry and academic malware researchers apply malware analysis to achieve insights on the latest techniques, tools, and exploits used by adversaries.