**Introduction**

Malware or malicious software is used by cybercriminals to cause significant damage to the victim. It damages either the server, host system, or network. Cybercriminals include attackers, hackers, nation-states. The damage caused could disrupt normal operations of a computer, a network, steal important and confidential information stores, bypass access controls to gain access to confidential arenas. It can cause harm to the victims in unimaginable ways. The victims could be individuals, organizations, businesses, governments, and even important bodies working towards the improvement of the world.

A report states that around 200,000 malware samples are being caught every day. This in turn calls for a strong process that will detect any malicious content right at the start and help to put together a process that will avert the situation or be able to do significant damage control.

Malware analysis the process of detecting and mitigating any potential threat by any virus and enhance the security of any application, website, or server. Malware analysis is a key process that is undertaken by any company today to ensure they are safe and secure with regard to their information and keep themselves from any vulnerabilities.

## 1. ****What is Malware Analysis****

Malware analysis can be described as the process of understanding the behavior and purpose of a suspicious file or URL. The output of the process aids in detecting and mitigating any potential threat. Some key benefits that malware analysis offers are to the incident responders and security analysts.

* Assesses the damage from a security threat
* Identify the source of the attack
* Identify the vulnerability of the malware, its exploitation level, and preparation to patch accordingly.
* Practically break incidents by the level of security threat
* Reveal hidden indicators of compromise that need to be blocked
* Improve the efficiency of indicators of compromise, alert and notify
* Enrich any context when hunting for threat

## 2. ****Types of Malware Analysis****

Types of malware analysis include static, dynamic or a hybrid of the two.

The static analysis does not analyze the code when it is running. Instead, it examines files for malicious intent. This makes it useful to identify infrastructure, packed files, and libraries. Some technical indicators can be used to determine if the file is malicious. However, since it does not run the code, it is difficult to detect sophisticated malware.

Dynamic analysis executes any suspicious malicious code in a secure environment called a sandbox. It enables security professionals to watch the malware in action and not impacting the risk of infecting the system. It offers deeper visibility to reveal the true nature of the threat. It also reduces the time to rediscover a file with malicious code. Hackers and adversaries often hide code in a sandbox that will not run until some conditions are met.

The hybrid analysis is a combination of basic and dynamic techniques to provide the best of both approaches. It detects malicious codes and extracts more indicators of compromise. It can even help detect this in sophisticated malware.

## 3. ****Malware Analysis Stages****

**Malware analysis** s**teps** or stages involved are:

### A) **Static Properties Analysis**

This includes strings embedded in malware code which would be needed to create IOC’s and can be accessed quickly. There would be no need to run a program to see it. This is the first level that will determine if a deeper investigation is required or not. It will determine if further steps will be required.

### B) **Interactive Behavior Analysis**

This is used to examine a malware sample in a lab. It seeks to understand the registry, process, network activities, and file system. It conducts memory forensics to see how malware uses memory. If the malware is found to be suspicious, one can set up a simulation to test the theory. It is time-consuming and requires a creative analyst with advanced skills. It is more of an

### C) **Fully automated analysis**

Fully automated malware analysis simply assesses suspicious files and determines potential repercussions if they were to infect the network. It also produces a comprehensible report that will provide quick answers to security teams. It is a great way to process malware analysis on a large scale.

### D) **Manual Code Reversing**

Here analysts reverse the engineer code by using debuggers, disassemblers, specialized tools, and compilers to decode any encrypted data and determine the logic. It is a rare skill and executing it takes a lot of time. Several analysts tend to skip this step which results in losing a lot of valuable insights into the nature of the malware.

## 4. ****Malware Analysis Use Cases****

Malware analysis example or some common use cases are as follows:

* **Malware Detection**

By applying sophisticated techniques that provide deep behavioural analysis and identifying code, functionality threats can be easily detected. Output of malware analysis helps to extract IOC’s that can be fed into SEIM’s, intelligence platforms and orchestration tools to alert threats in future.

* **Threat alerts and Triage**

Malware analysis provides improved alerts early on in the attack life cycle. This helps teams to save time by sorting results and aiding technology.

* **Incident Response**

The goal of this is to provide root cause analysis, determine the impact and achieve success in remediation and recovery. It helps in the efficiency and effectiveness of the effort.

* **Threat hunting**

Threat hunters can use malware analysis as it exposes behaviour and facts like access to a port, domain or network connection.

* **Malware Research**

Malware researchers gain understanding of latest techniques, tools and other activities to perform malware analysis.

## 5. ****Importance of MA****

Malware includes virus, ransomware, rootkits, Trojan and a malware attack can adversely affect a business and its operations. Appropriate security measures must be put in place by businesses to malware analysis tools as an incident response plan that will chart a proper procedure to ensure there are the recovery time and reduced costs.

Whilst an incident response, malware analysis plays a vital role in aiding the security team to understand the extent of the incident along with identifying the hosts and systems that have been affected. With the help of the report generated from malware analysis, an organization can mitigate any vulnerabilities and prevent any additional compromises.

## ****Conclusion****

When there is a security threat and malware is the reason behind it, malware analysis comes into the picture and plays an integral role to create an incident response. It helps users know the required steps for recovery. It helps responders to understand the extent of the malware based incident and identify the hosts, servers, or systems affected. Malware analysis also generates actionable information that helps organizations to avert or mitigate risks that are generated by malware. It helps to prevent any additional compromise.