CRYPTUS CYBER
SECURITY PVT. LTD.

Module Name:-

Malware Analysis

What is Malware ?

Malware : Malicious + Software

Software that is intended to harm. A software that disrupt or alter the normal operation of an electronic device. Electronic device could be anything either mobile phone or computers, tablets etc...

How it basically works: It infects a device or machine by tricking users nto clicking or installing a program (jo unko nhi krna chahiye tha). R jaise hi wo usko execute krte hai to several actions perform hote which comes under the category of

Effects of Malware

- khud ko replicate krna
- Apke keystrokes record krna or aapko pta bhi na chlna.
- Apko services ya files access krne se rok dena
- Apke browser ko ads se bhar dena.

Cryptocurrency Malware

How we get ourself into installing a Malware :

For the installation of malwares there are some techniques or we can say bait(chaara daalna) provided by hackers to make you click on such document or on a link or installing an executable software.

Types of Malwares:

Virus , Worms , Keyloggers , Ransomewares , Spywares (Trojans , Adwares) , Rootkits (ROOT + KIT) , Botnet, Robots in a Network.

VIRUS (Vital Information Resource Under Siege):

A piece of code which is capable of copying itself and typically has a devastating effect and it also require a human being for its implementation.

Viruses spread by reproducing and inserting themselves into programs, documents, or e-mail attachments. And they won't work untill unless we don't strike them or lead them to the phase of execution.

EG: Tera bit virus maker

FUD : Fully Undetectable

Chota packet badaa dhanamka...

infinite folder:

```
:loop
mkdir %random%
goto loop
```

```
:loop
```

Space consuming Virus:

mkdir hello

cd hello

echo " main saari jgh ko khtm kr dunga">> file.txt

goto loop

Shutdown Virus:

shutdown -s -t 10 -c "bye bye beta lg gye"

fork bomb :

%0|%0

Types of Viruses

Browser Hijacker (jo aapkoaapki sites pr multiple sites pr visit kraane ke baad pahuchaye)

File Infector (jo file ke saath chipak jaye r fr infect krta jaaye uske execution pr)

Polymorphic Virus (They are encrypted and change operations over time).

Macro(ek bde instruction ko chote sub instruction me baat deta hai) Virus

Boot Sector Virus

Memory Resident Virus (adiyal hota hai host program chla bhi jaaye tbhi bhi execute hota rehta hai)

etc etc ...

Worms:

A computer worm is self-replicating malware that duplicates itself to spread to uninfected computers. Worms often use parts of an operating system that are automatic and invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

Stuxnet : https://www.youtube.com/watch?v=7g0pi4J8auQ

Keyloggers

Recording your keystrokes that is whatever you typwe will be stored in a log file

Local Storage

Remote Storage

Eg: Ardamax Keylogger, Hooker.

Ransomwares : Beta loot lega aapko jis din gya aapke system pr.

Now the question is what is Malware Analysis ?

Malware analysis is the process of understanding the behavior and purpose of a suspicious file or URL. The output of the analysis aids in the detection and mitigation of the potential threat.

The key benefit of malware analysis is that it helps incident responders and security analysts:

- Pragmatically triage incidents by level of severity
- Uncover hidden indicators of compromise (IOCs) that should be blocked
- Improve the efficacy of IOC alerts and notifications
- Enrich context when threat hunting

Types of Malware Analysis

The analysis may be conducted in a manner that is static, dynamic or a hybrid of the two.

Static Analysis

Basic static analysis does not require that the code is actually run. Instead, static analysis examines the file for signs of malicious intent. It can be useful to identify malicious infrastructure, libraries or packed files.

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. In addition, tools like disassemblers and network analyzers can be used to observe the malware without actually running it in order to collect information on how the malware works.

However, since static analysis does not actually run the code, sophisticated malware can include malicious runtime behavior that can go undetected. For example, if a file generates a string that then downloads a malicious file based upon the dynamic string, it could go undetected by a basic static analysis. Enterprises have turned to dynamic analysis for a more complete understanding of the behavior of the file.

Dynamic 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.

The challenge with dynamic analysis is that adversaries are smart, and they know sandboxes are out there, so they have become very good at detecting them. To deceive a sandbox, adversaries hide code inside them that may remain dormant until certain conditions are met. Only then does the code run.

Hybrid Analysis (includes both of the techniques above)

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 basic 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.

For example, one of the things hybrid analysis does is apply static analysis to data generated by behavioral analysis – like when a piece of malicious code runs and generates some changes in memory. Dynamic analysis would detect that, and analysts would be alerted to circle back and perform basic static analysis on that memory dump. As a result, more IOCs would be generated and zero-day exploits would be exposed.

Malware Analysis Use Cases

Malware Detection

Adversaries are employing more sophisticated techniques to avoid traditional detection mechanisms. By providing deep behavioral analysis and by identifying shared code, malicious functionality or infrastructure, threats can be more effectively detected. In addition, an 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 Hunting

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.

Malware Research

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

Stages of Malware Analysis

Static Properties Analysis

Static properties include strings embedded in the malware code, header details, hashes, metadata, embedded resources, etc. This type of data may be all that is needed to create IOCs, and they can be acquired very quickly because there is no need to run the program in order to see them. Insights gathered during the static properties analysis can indicate whether a deeper investigation using more comprehensive techniques is necessary and determine which steps should be taken next.

Interactive Behavior Analysis

Behavioral analysis is used to observe and interact with a malware sample running in a lab. Analysts seek to understand the sample's registry, file system, process and network activities. They may also conduct memory forensics to learn how the malware uses memory. If the analysts suspect that the malware has a certain capability, they can set up a simulation to test their theory. Behavioral analysis requires a creative analyst with advanced skills. The process is

time-consuming and complicated and cannot be performed effectively without automated tools.

Fully Automated Analysis

Fully automated analysis quickly and simply assesses suspicious files. The analysis can determine potential repercussions if the malware were to infiltrate the network and then produce an easy-to-read report that provides fast answers for security teams. Fully automated analysis is the best way to process malware at scale.

Manual Code Reversing

In this stage, analysts reverse-engineer code using 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.

The World's Most Powerful Malware Sandbox

Security teams can use the CrowdStrike Falcon® Sandbox to understand sophisticated malware attacks and strengthen their defenses. Falcon Sandbox™ performs deep analyses of evasive and unknown threats, and enriches the results with threat intelligence.

Key Benefits Of Falcon Sandbox

Provides in-depth insight into all file, network and memory activity

Offers leading anti-sandbox detection technology

Generates intuitive reports with forensic data available on demand

Supports the MITRE ATT&CK® framework

Orchestrates workflows with an extensive application programming interface (API) and pre-built integrations

Detect Unknown Threats

Falcon Sandbox extracts more IOCs than any other competing sandbox solution by using a unique hybrid analysis technology to detect unknown and zero-day exploits. All data extracted from the hybrid analysis engine is processed automatically and integrated into Falcon Sandbox reports.

Falcon Sandbox has anti-evasion technology that includes state-of-the-art anti-sandbox detection. File monitoring runs in the kernel and cannot be observed by user-mode applications. There is no agent that can be easily identified by malware, and each release is continuously tested to ensure Falcon Sandbox is nearly undetectable, even by malware using the most sophisticated sandbox detection techniques. The environment can be customized by date/time, environmental variables, user behaviors and more.

Identify Related Threats

Know how to defend against an attack by understanding the adversary. Falcon Sandbox provides insights into who is behind a malware attack through the use of malware search a unique capability that determines whether a malware file is related to a larger campaign, malware family or threat actor. Falcon Sandbox will automatically search the largest malware search engine in the cybersecurity industry to find related samples and, within seconds, expand the analysis to include all files. This is important because it provides analysts with a deeper understanding of the attack and a larger set of IOCs that can be used to better protect the organization.

Achieve Complete Visibility

Uncover the full attack life cycle with in-depth insight into all file, network, memory and process activity. Analysts at every level gain access to easy-to-read reports that make them more effective in their roles. The reports provide practical guidance for threat prioritization and response, so IR teams can hunt threats and forensic teams can drill down into memory captures and stack traces for a deeper analysis. Falcon Sandbox analyzes over 40 different file types that include a wide variety of executables, document and image formats, and script and archive files, and it supports Windows, Linux and Android.

Respond Faster

Security teams are more effective and faster to respond thanks to Falcon Sandbox's easy-to-understand reports, actionable IOCs and seamless integration. Threat scoring and incident response summaries make immediate triage a reality, and reports enriched with information and IOCs from CrowdStrike Falcon MalQuery™ and CrowdStrike Falcon Intelligence™ provide the context needed to make faster, better decisions.

Falcon Sandbox integrates through an easy REST API, pre-built integrations, and support for indicator-sharing formats such as Structured Threat Information Expression™ (STIX), OpenIOC, Malware Attribute Enumeration and Characterization™ (MAEC), Malware Sharing Application Platform (MISP) and XML/JSON (Extensible Markup Language/JavaScript Object Notation). Results can be delivered with SIEMs, TIPs and orchestration systems.

Cloud or on-premises deployment is available. The cloud option provides immediate time-to-value and reduced infrastructure costs, while the on-premises option enables users to lock down and process samples solely within their environment. Both options provide a secure and scalable sandbox environment.

Automation

Falcon Sandbox uses a unique hybrid analysis technology that includes automatic detection and analysis of unknown threats. All data extracted from the hybrid analysis engine is processed automatically and integrated into the Falcon Sandbox reports. Automation enables Falcon Sandbox to process up to 25,000 files per month and create larger-scale distribution using load-balancing. Users retain control through the ability to customize settings and determine how malware is detonated.