Introduction to Malware Analysis

Malware Analysis

What is Malware?

(malicious software)-Malware is any software that was written to causes damage to data, devices, computer, or network—such as viruses, trojan horses, worms, rootkits, ransomware, scareware, and spyware.

How we get the the malware?

-Clicking on phishing email link or opening malicious email attachment (90% of attacks)

--Bundled in Free Software Programs

-Removable Media

-Malvertising

-Peer to peer applications

EXAMPLE OF GETTING ATTCACKED.

KCB finds EMOT malware on 10 PCs

IT team cleans, reformats and reconfigures.

Is this the final step?

YES or NO?

Malware Analysis

Is this the final step?

NO

After malware is found, you need to know

- Did an attacker implant a rootkit or trojan on your systems?
- Is the attacker really gone?
- What did the attacker steal or add? What was exfiltrated out?
- How did the attack get in?

What is Malware Analysis?

It's the process of dissecting malware to understand and learn:

- How it works
- How to identify it
- How to defeat or eliminate it
- potential repercussions of a given malware.

Malware Analysis

Goals of Malware Analysis?

It's the process of dissecting malware to understand and learn:

- Exactly what happened
- Ensure you've located all infected machines and files
- How to measure and contain the damage
- Find signatures for intrusion detection systems

- Antivirus scanning

  ***Challenge*:**Malware can easily change its signature and fool the antivirus)
- Hashes
- A file's strings, functions, and headers

Two types malware analysis methods:

Static Analysis and Dynamic Analysis (Behavioural Analysis)

1.Static Analysis- static analysis-analyse the malware without running it/executing it.Here you will not be bothered about viewing the actual code or instructions.

EXAMINE THE CHARACTERISTICS OF MALWARE WITHOUT EXECUTING IT.

Malware Analysis

In Static Analysis you can use:

- Antivirus scanning

  ***Challenge*:**Malware can easily change its signature and fool the antivirus)
- Hashes
- A file’s strings, functions, and headers

Malware Analysis

2. **Dynamic Analysis** - dynamic analysis-analyse the malware while executing or/running it in a controlled environment like a sandbox.

- Run the malware and monitor its effect
- Use a virtual machine and take snapshots
- Tools: RegShot, Process Monitor, Process Hacker, CaptureBAT
- RAM Analysis: Redline and Volatility

SANDBOXES

- Cuckoo sandbox;
- Sandboxie: https://www.sandboxie.com
- Shade Sandbox: https://www.shadesandbox.com
- Toolwiz Time Freeze: http://www.toolwiz.com
- Shadow Defender: https://www.shadowdefender.com
- Create a virtual machine of the OS of your choice
- Virtualbox: https://www.virtualbox.org
- VMWare: https://www.vmware.com

Malware Analysis

What is a sandbox

- A sandbox is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third parties, suppliers, untrusted users and untrusted websites
- What Sandbox does is basically does is **Isolates** the file before sending it out or recieiving it. Analyses the file. Checks its behaviour. Ensures that there is no insecure links or backdoor. any external links, checks where the links connect to.

Goal of a sandbox

- Goal of a sandbox is to Allow you to test unkown software/files without damaging the host OS/other end devices.
- Prevents ‘suspected file” in a normal setup NGFW at the perimeter. Send suspicios files to the Sandbox for further analysis.

--→ **NB:In malware analyses, we use sandboxing.**

We will isolate the suspicious file (suspected malware) for analysis.