Malware Analysis 101

What is malware analysis and how to respond to it?

Aditya Anand Follow
Sep 12 · 6 min read

I haven't been able to write any articles in the past few weeks as I was on a vacation for few days and I recently began studying regarding malware analysis. It was that field of CyberSec that always intrigued me but I always kept on procrastinating, convincing myself that it is way too hard and complex for someone like me. Last month I got lucky and was having conversation with an amazing french Infosec engineer Jo (telegram - @jiab77) when he explained me the basics of Malware Analysis and broke down the wall that I had created in my mind.

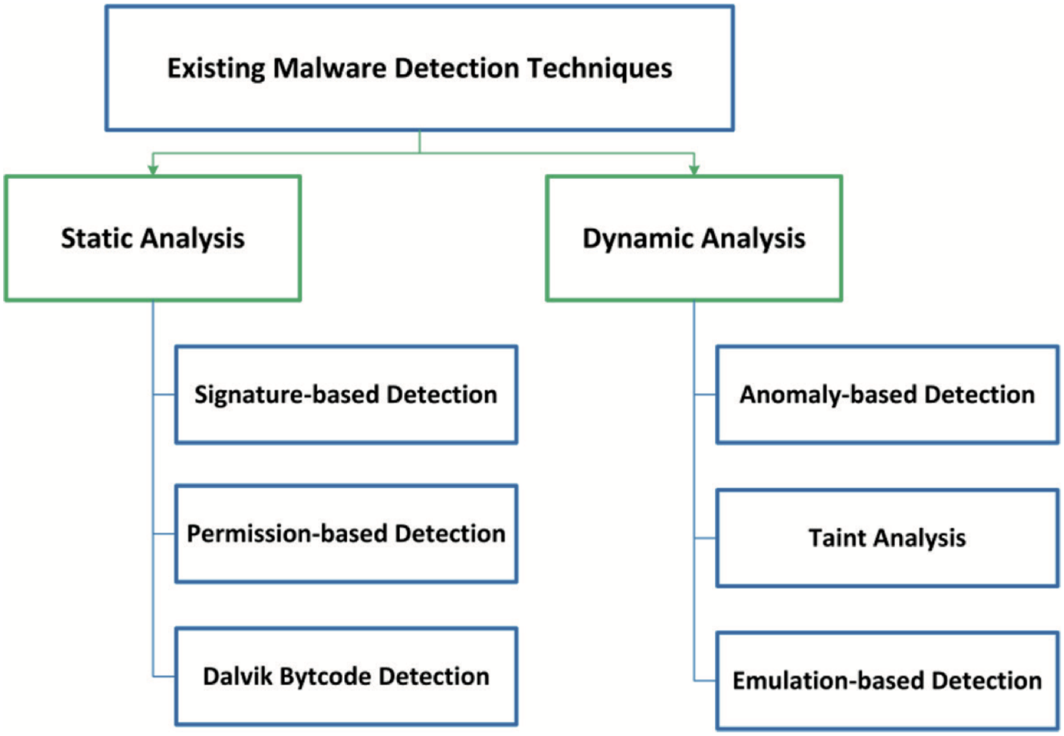
Let's begin!

Before we get into the depths of malware analysis let's understand what is a malware. Malware (malicious software) are programs or files that are designed as such to inflict harm to the computer and possibly to its user. There are various types of malware that are present in the big wide internet world of ours like viruses, worms, Trojan horses, ransomware and spyware. The malware can carry out various functions like stealing data, encrypting files, deleting data, altering files or even adding those systems to a huge botnet and monitor these systems without the user ever knowing that their computers are infected. The hackers mainly write these malware and carry out the attacks in two different methodology based on the attack surface, one being a mass attack where they write a malware that is supposed to take infect large masses for example the "WannaCry" and "NotPetya" ransomwares and the second one is targeted attacks where the attacker writes the malware designed for an extremely focused task, the infamous "Stuxnet" being one of such attacks.

Now that we have got the basic understanding of malware out of the way let’s dive into how we actually carry out malware analysis and what are the techniques utilised.

Malware Analysis Techniques

There are two different types of malware analysis techniques, one being static analysis and the other is dynamic analysis. Their names are self explanatory as to what it means but please let me explain it further. In layman terms static analysis entails all those examinations of the malware where you don’t actually execute the malware but try to figure out what the malware is trying to do. Dynamic analysis are all those examinations that you carry out when you actually execute the malware (do this in a sandboxed environment) and then try to figure out the functionality of the malware.


Existing Malware Detection Techniques
Static Analysis
Dynamic Analysis
Signature-based Detection
Permission-based Detection
Dalvik Bytcode Detection
Anomaly-based Detection
Taint Analysis
Emulation-based Detection

Source : Android Application Security Scanning Process - Iman Almomani and Mamdouh Alenezi

These can be further divided into four categories.

i) *Basic Static Analysis*

- Basic static analysis consists of examining the executable file without viewing the actual instructions.
- Basic static analysis can confirm whether a file is malicious, provide information about its functionality
- Sometimes provide information that will allow you to produce simple network signatures.
- Its straightforward & quick, but it's largely ineffective against

sophisticated malware & can miss important behaviours.

ii) Basic Dynamic Analysis

- Basic dynamic analysis techniques involve running the malware and observing its behavior on the system in order to remove the infection, produce effective signatures, or both.
- Before executing the malware, you must set up an environment that will allow you to study the running malware without risk of damage to your system or network.
- Basic dynamic analysis techniques can be used by most people without deep programming knowledge, but they won't be effective with all malware and can miss important functionality.

iii) Advanced Static Analysis

- Consists of reverse-engineering the malware's internals by loading the executable into a disassembler and looking at the program instructions in order to discover what the program does.
- Instructions are executed by the CPU, so advanced static analysis tells you exactly what the program does.
- However, it has a steeper learning curve than basic static analysis and requires specialised knowledge of disassembly, code constructs, and Windows operating system concepts.

iv) Advanced Dynamic Analysis

- It uses a debugger to examine the internal state of a running malicious executable.
- Advanced dynamic analysis techniques provide another way to extract detailed information from an executable.
- These techniques are most useful when you're trying to obtain information that is difficult to gather with the other techniques.

I am planning to write further articles explaining in depth about these techniques and how to perform them in the most optimised way possible.

Three Golden Rule

Malware analysis has its own three golden rules that you should definitely keep in mind while carrying out your examination of these programs to enhance your productivity and not fall for the attackers trap.

i) *First*

- Don't get too caught up in the details. Most malware programs are large and complex, and you can't possibly understand every detail.
- Focus instead on the key features. When you run into difficult and

complex sections, try to get a general overview before you get stuck in the weeds.

ii) *Second*

- Remember that different tools and approaches are available for different jobs. There is no one approach.
- Every situation is different, and the various tools and techniques that you'll learn will have similar and sometimes overlapping functionality.
- If you're not having luck with one tool, try another. If you get stuck, don't spend too long on any one issue; move on to something else.
- Try analysing the malware from a different angle, or just try a different approach.

iii) *Third*

- Remember that malware analysis is like a cat-and-mouse game.
- As new malware analysis techniques are developed, malware authors respond with new techniques to thwart analysis.
- To succeed as a malware analyst, you must be able to recognise, understand, & defeat these techniques, and respond to changes in the art of malware analysis.

Now that we know the golden rules of malware analysis and what malware are, let's now have a bird view perspective on things we need to do when we encounter a malware on your system or on our network.

What to do in a Malware Attack?

The purpose of malware analysis is usually to provide the information you need to respond to a network intrusion. Our goals will typically be to determine exactly what happened & ensure that we have located all infected machines & files.

- When analysing suspected malware, your goal will typically be to determine exactly :-

i) what a particular suspect binary can do

ii) how to detect it on your network

iii) how to measure and contain its damage.

After identifying which files require full analysis, we need to develop signatures to detect malware infections on our network.

- *Host-based signatures*, or indicators, are used to detect malicious code on victim computers.

Malware indicators focus on what the malware does to a system, not on the characteristics of the malware itself

- *Network signatures* are used to detect malicious code by monitoring net- work traffic.

Network signatures can be created without malware analysis, but signatures created with the help of malware analysis are usually far more effective.

The final objective is always to figure out exactly how the malware works and what are the functions that it is trying to execute when present on the system.

> *P.S. Here is an image that will give you a basic outlook of Malware Analysis. I will try to cover these topics in my upcoming articles.*

Source : BSides Austin 2015 and Malware Analysis Training by Adam Kujawa

If you enjoyed it please do clap & let’s collaborate. Get, Set, Hack!

Website : aditya12anand.com | Donate : paypal.me/aditya12anand

Telegram : https://t.me/aditya12anand

Twitter : twitter.com/aditya12anand

LinkedIn : linkedin.com/in/aditya12anand/

E-mail : aditya12anand@protonmail.com

· · ·

Follow Infosec Write-ups for more such awesome write-ups.

InfoSec Write-ups

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to

medium.com