What is malware analysis? How are the steps taken?

What is malware analysis? In what situations do we need to conduct malware analysis? How is the malware analysis process implemented?

Malware (malware), sometimes called malicious software, malware or malware or malicious software, is a type of system software created by hackers or vandals to harmful to computer systems, software, so what is malware analysis? In what situations do we need to conduct malware analysis? How is the malware analysis process implemented? We will find out later.

1. Alarming statistics on the situation of network security in our country in the first half of 2019

Malware was born to destroy the system

Malware / malware

1. Malware analysis
2. Cases need to implement malware analysis process
    1. Computer security
    2. Research on malware
    3. Extracting system attack traces (Indicators of Compromise)
3. 4 main stages in the malware analysis process
    1. Automatic analysis
    2. Analysis of malicious properties
    3. Interactive characterization / behavioral analysis
    4. Reverse encryption

Malware analysis

Malware analysis is a process that involves studying and understanding how a particular malware works, as well as how it can affect an operating system, target program. As we all know, each malware has different code, so their functions are not the same and extremely diverse. However, after all, the main purpose of these malware is not outside the possession of information, data from the infected device without the permission or authorization of specific users.

1. Detection of security vulnerabilities affects all Bluetooth versions

Cases need to implement malware analysis process

Computer security

Malware analysis helps determine whether the system is actually infected with malicious code

One of the cases where it is necessary to deploy malware analysis processes is to determine if an organization is actually infected with malware, if so, what kind of malicious code it is and how does it affect the system? From the knowledge gained during the analysis, security experts will make the most appropriate response action, minimizing mistakes that can cause serious damage to the system.

1. What is email encryption? Why does it play an important role in email security?

Research on malware

Yes, malware research is a vast, complex task, and malware analysis is a sub-process that constitutes this task. Knowing the specific characteristics and ways of malware is one of the best defense measures against them. In particular, the malicious analysis process will give security experts the most optimal understanding of the nature of a malicious program, as well as solutions that they can deploy to ensure capabilities. most proactive protection.

Extracting system attack traces (Indicators of Compromise)

Indicator of Compromise (IoC) is the data clue that shows the traces of an unauthorized intrusion that remain on the system. These data may include logs, retained emails, IP addresses after downloading data, or md5 values ?? of malicious codes.

Finding a data clue shows that the traces of an illegal intrusion play a very important role

Software solution providers will have to conduct malware analysis on a local scale to find any new clues, which can help an organization take effective measures to protect itself. more effective before potential attacks.

1. Discover the new malicious code, automatically record the victim's screen when they watch 'adult movies'

4 main stages in the malware analysis process

To understand what malware analysis is, it is important to understand the 4 essential stages in a typical malware analysis process, including:

Automatic analysis

If you find a suspicious program appearing on your organization's intranet system, the quickest and easiest way to determine if it is a security threat is to use programs. Automatic security analysis. They can quickly find out the true functions and purposes of a potential malware. Although this is not the most comprehensive solution, it is easiest to deploy and at the same time take the least time.

1. What is data exfiltration? How to prevent this dangerous behavior?

Analysis of malicious properties

A careful analysis and analysis of the static properties of malware will give security experts a more detailed view of the potential of malicious code, as well as the damage it can cause in practice. . In addition, you do not need to

worry about the risks that may occur in analyzing code attributes because this process does not require launching a malicious program.

This step will provide basic indicators of system attack traces.

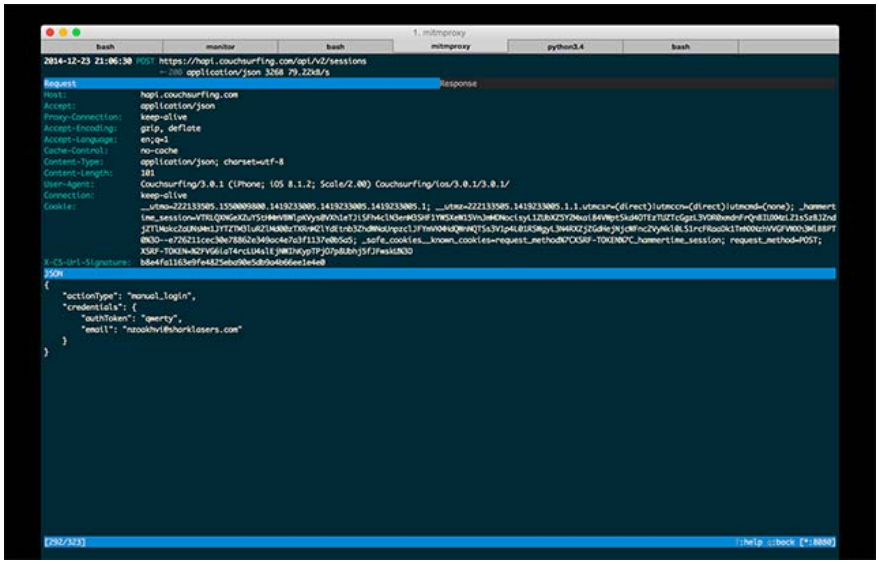
Interactive characterization / behavioral analysis

At this stage, you must put the malware in an isolated test environment, allowing you to safely observe malicious activity. The information needed during this period will serve as an important factor, supporting security experts in establishing and deploying automated tools to detect and prevent malicious code. More, easier.

Reverse encryption

The final and most important step in the entire malware analysis process. The most comprehensive way to understand a malware is to reverse its code manually. Reverse encryption provides the most detailed knowledge of malware, what it can do, along with the measures that an organization can take to protect its system from the harms that malicious code.

1. Overview of building enterprise security detection and response system



The most comprehensive way to understand a malware is to reverse its code manually

The above is basic information about the concept, the process of analyzing malware as well as the way to implement it. Wish you build a tight and secure security system!

You finished reading the article "**What is malware analysis? How are the steps taken?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.