Malware Analysis Fundamentals BY P3NGU1N

How Malware Analysis Help SOC Analysts

🎯 How many zero-day vulnerabilities exist in Stuxnet? (Answer should be string)

ANSWER: four

🎯 Which company's industrial control systems is Stuxnet targeting?

ANSWER: siemens

Malware Definition and Malware Types

🎯 What is the name of the first worm malware to spread on the internet?

ANSWER: morris

🎯 What is the vulnerability code of the vulnerability used by Wannacry?

ANSWER: ms17-010

🎯 What is the name of the malware that was detected in December 2021, distributed through the Solarwinds Orion product and caused the hacking of many organizations such as FireEye?

ANSWER: Sunburst

What Should a Malware Analyst Know

🎯 Which encryption type ransomwares uses?

ANSWER: asymmetric

🎯 What is the encryption type frequently used by ransomware-type malware?

ANSWER: aes

🎯 What is the name of the software that compiles of the written codes?

ANSWER: compiler

🎯 According to Wikipedia, in what year did assembly language first appear?

ANSWER: 1947

🎯 What is the name of the software that translates machine code into assembly language?

ANSWER: disassembler

Dynamic Analysis Example Using AnyRun

🎯 (Access AnyRun report to answer this question) What is the email address that the malware connects to the mail server to steal data?

https://app.any.run/tasks/e4979ab7-3145-4121-a042-ea91d7e2c86b

ANSWER: logs@godforeu.com

🎯 (Access AnyRun report to answer this question) What is the password malware use while connecting to the mail server?

ANSWER: O8k#Pz4sk:w_

QUIZ:

🎯 **What is the type of malware that is used to control the device remotely?**

ANSWER: **RAT**

🎯 **What is the name given to programs that translate compiled code into assembly language?**

ANSWER: **Disassemblers**

🎯 **What is the type of malware that is increasing in popularity and encrypts the files on the victim device and demands ransom?**

ANSWER: **Ransomware**

🎯 **What is the name of the malware that has many 0day exploits and targets nuclear power plants that was on the agenda in 2010?**

ANSWER: **Stuxnet**

🎯 **What is the malware analysis method that allows to find the command and control center in a short time?**

ANSWER: **Dynamic Analysis**

🎯 **What is the name given to software that allows programs to be changed at runtime, to direct the flow of the code, to change the registers?**

ANSWER: **Debuggers**

🎯 **What is the function that automatically enables macro codes to be run when the Office document is opened?**

ANSWER: **Workbook_Open()**

🎯 **Which of the following is not a debugger?**

ANSWER: **Python**

🎯 **Which software enables encryption of the codes of the PE file to make static analysis difficult?**

ANSWER: **Packers**

🎯 **Which register is responsible for keeping the return values of functions in x86 architecture?**

ANSWER: **EAX**