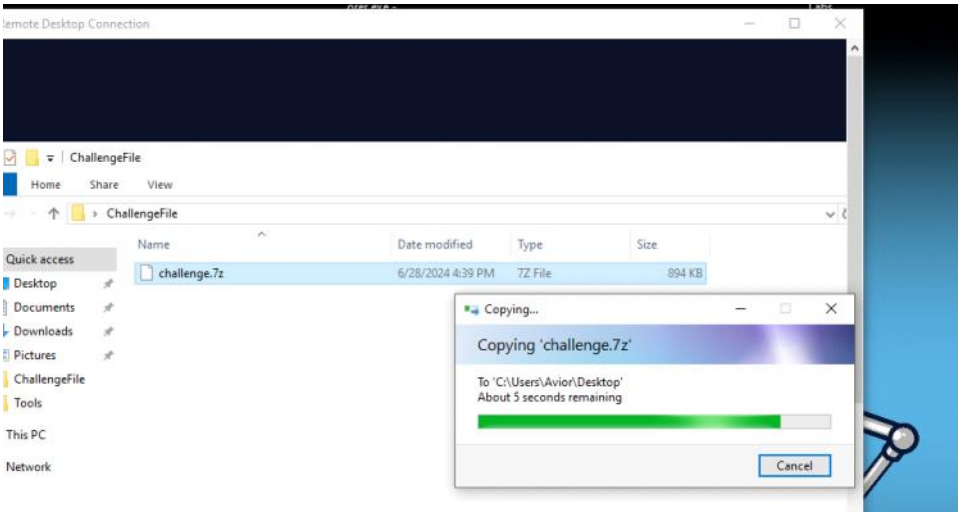
Avior Mostovski

Over the past few years, malware researchers have noticed a worrying trend: malicious groups are increasingly using Go, a powerful, easy-to-use, and platform-independent programming language, to create stealthy and resilient malware.

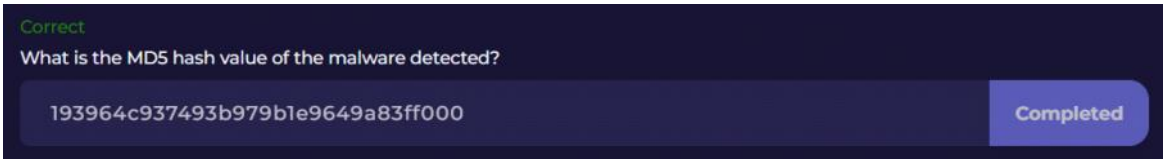
Unfortunately, a new strain of Golang malware has been detected on your organization's network.
Initial reports indicate that traditional antivirus solutions are struggling to detect this malware, which uses sophisticated evasion techniques.
Upon further investigation, it becomes clear that you need to understand Golang's subtleties.
You need to dissect the inner workings of this Golang malware, identify its capabilities, uncover its propagation methods, and analyze its functions.
File Location: C:\Users\LetsDefend\Desktop\ChallengeFile\challenge.7z

From <https://app.letsdefend.io/challenge/golang-ransomware>

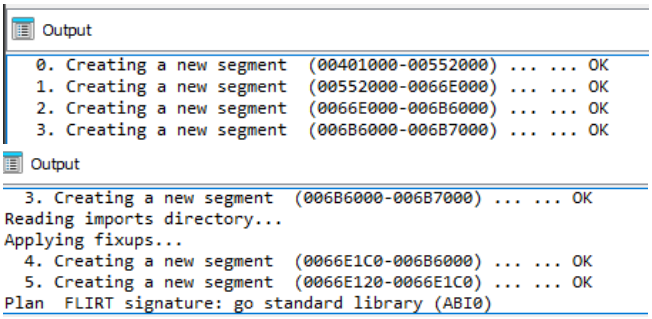


I will be using both IDA and Cutter

1. What is the MD5 hash value of the malware detected?



2. How many sections are present in this sample?

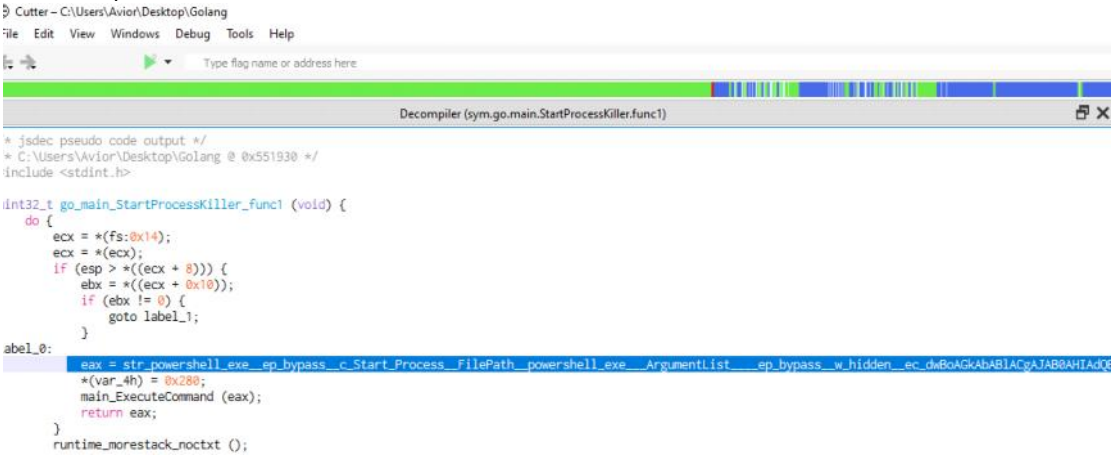


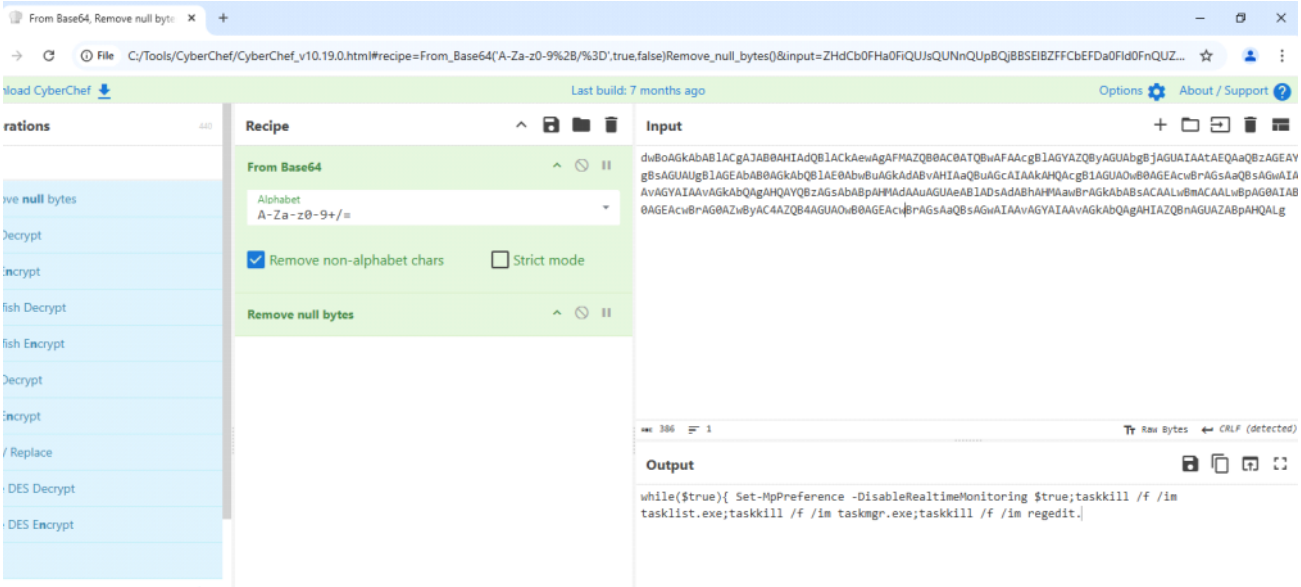
0 - 5 Sections
So we get 6 sections

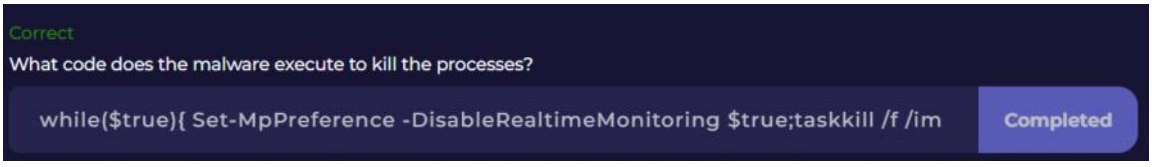
3. What code does the malware execute to kill the processes?

Search for ProcessKiller functions:

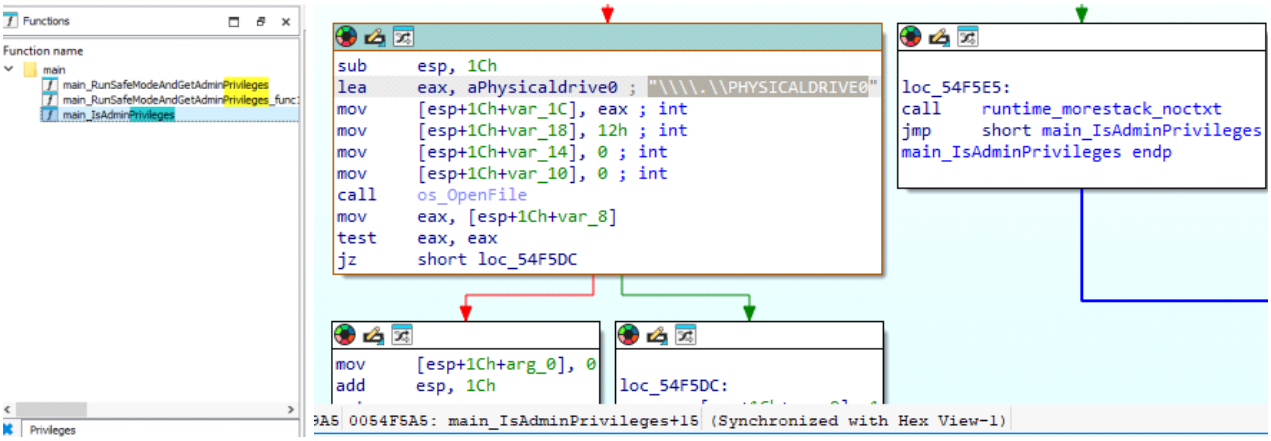
There is a powershell encoded with Base64 command:

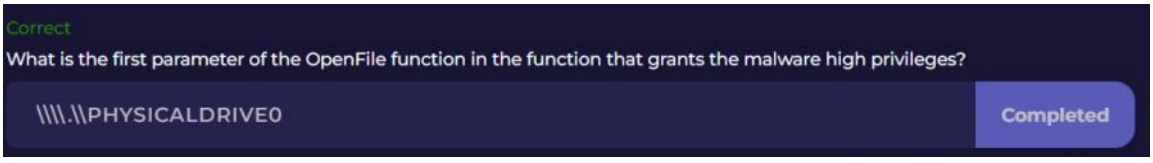




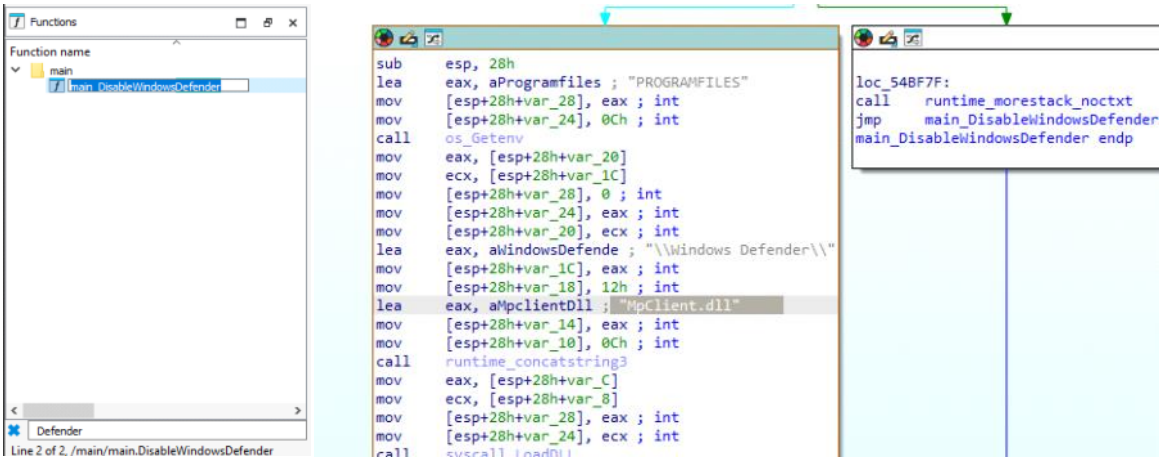


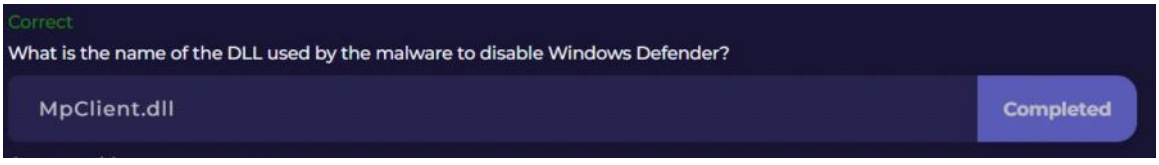
4. What is the first parameter of the OpenFile function in the function that grants the malware high privileges?



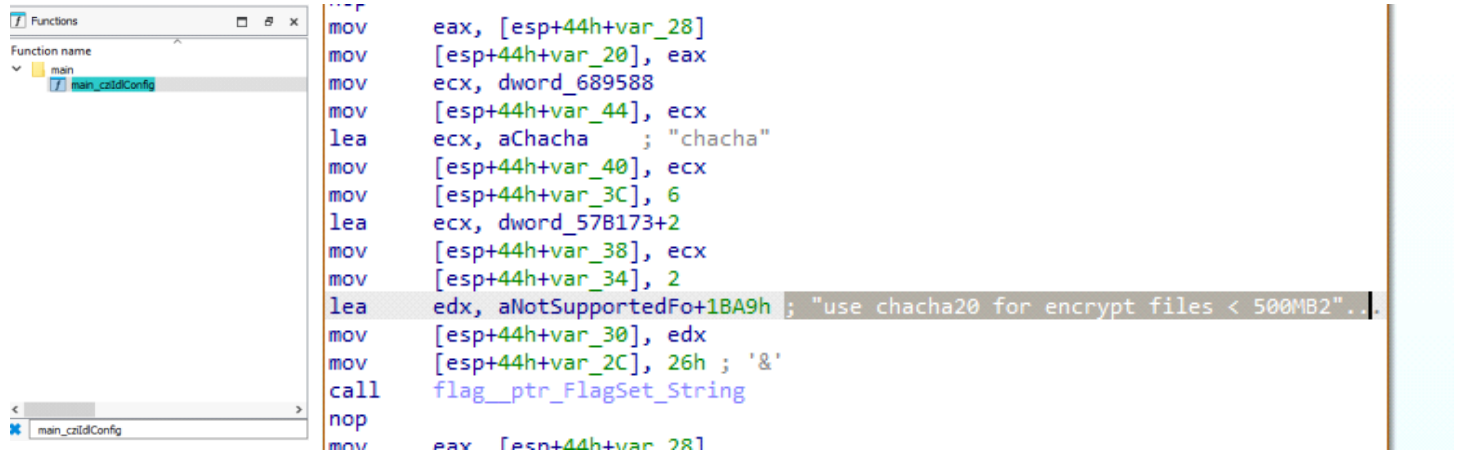


5. What is the name of the DLL used by the malware to disable Windows Defender?





6. What is the decryption flag used by the malware?

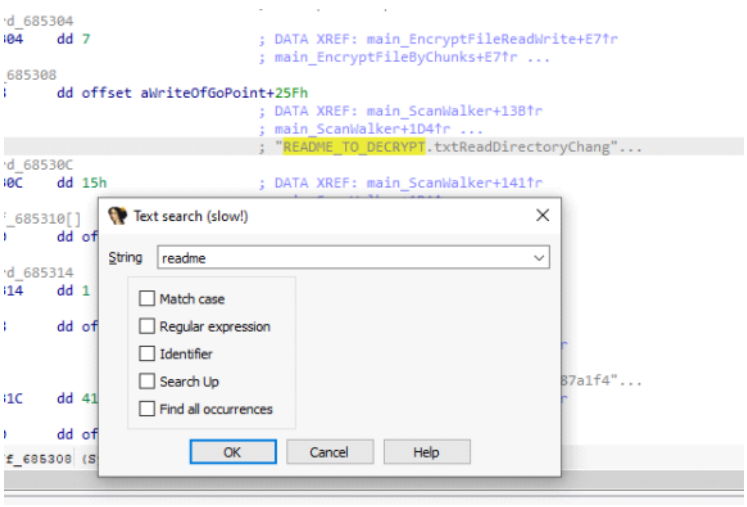


Correct

What is the decryption flag used by the malware?

chacha — Completed

7. What is the file name of the ransomware note?

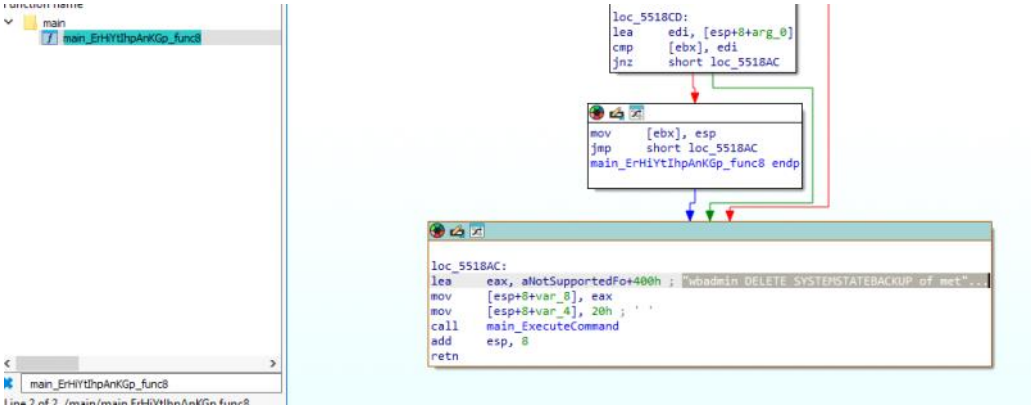


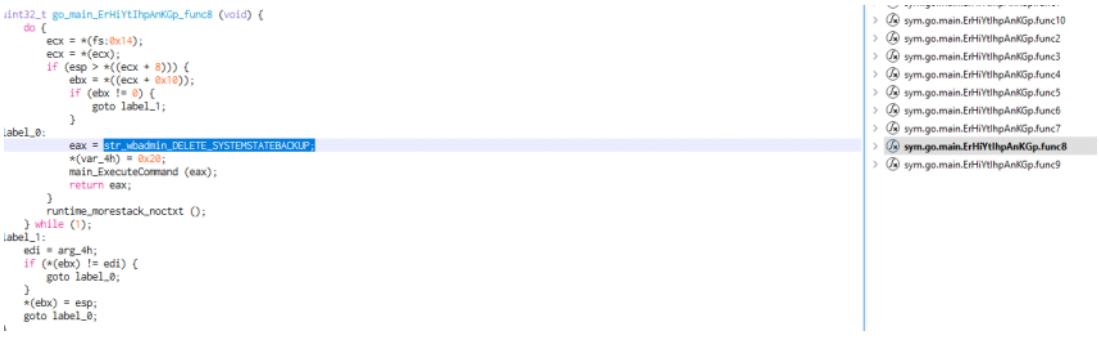
Correct

What is the file name of the ransomware note?

README_TO_DECRYPT.txt — Completed

8. What command can be executed by the "main_ErHiYtIhpAnKGp_func8" function?



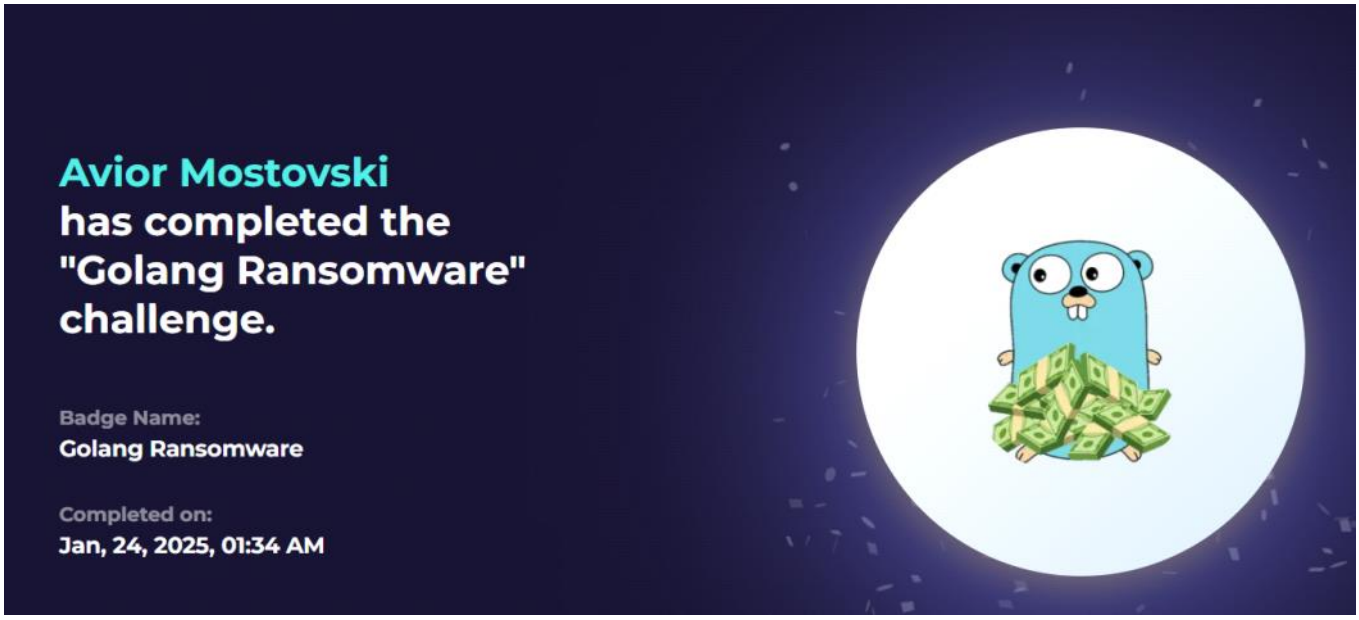


Correct

What command can be executed by the "main_ErHiYtIhpAnKGp_func8" function?

wbadmin DELETE SYSTEMSTATEBACKUP — Completed


Golang Ransomware
You've gained a new badge!


Avior Mostovski
has completed the
"Golang Ransomware"
challenge.
Badge Name:
Golang Ransomware
Completed on:
Jan, 24, 2025, 01:34 AM