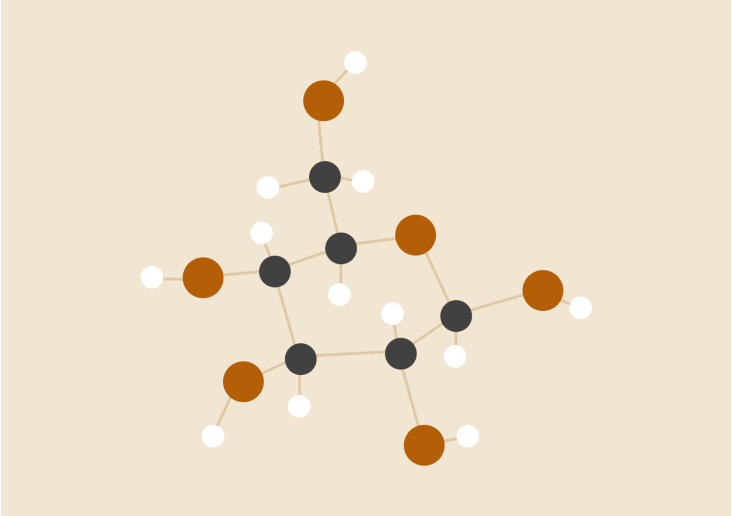
Malware Analysis

Vibe Stealer : White Mamba



INTRODUCTION

My friend recently told me he's become a *"vibe coder"*. Apparently, with the help of LLMs, he's now able to write and ship malware faster than ever. He even joked about starting his own *Malware-as-a-Service (MaaS)* operation.

He told me LLMs generate clean, high-level code that follows best practices, making it easy for him to pack it into a binary and deploy it. He sent me a sample of his latest creation and asked me to take a look.

He also claimed he already tested it on a victim, and *“it worked like a charm.”*
He insisted I check out what the victim was doing at the time of the infection and his browsing history .

Malware sample :

Malware sample : stc2_clean.exe

Tasks :

- Understand how the malware works
- Analyze how it communicates with the Command & Control (C2) server
- Figure out how data is exfiltrates
- Investigate the first victim's data (**only the first victim is relevant for this challenge**)
- Assemble the flag: it’s split into **three parts** across the challenge

Note : this is not really needed to solve the challenge all you need is to find the flag

DATA: use those as base and answer in detailed manner

Questions	Answer
Sha256 hash	
Malware Tags	
packer	
C2	
Data exfiltration	
Flag	nexus{}