Challenge Questions

Q: What language is the binary written in?
A: Nim

Q: What is the architecture of this binary?
A: x86_64/amd64/64-bits

Q: Under what conditions can you get the binary to delete itself?
A:

- No internet or No cosmo.jpeg
- INetSim shut off while exfiltrating data
- Finish data exfiltration

Q: Does the binary persist? If so, how?
A: No persistence

Q: What is the first callback domain?
A: update[.]ec12-4-109-278-3-ubuntu20-04[.]local

Q: Under what conditions can you get the binary to exfiltrate data?
A: Internet connection + cosmo.jpeg

Q: What is the exfiltration domain?
A: cdn[.]altimiter[.]local

Q: How does exfiltration take place?
A:

- Initial callback domain successfully
- unpack passwrd.txt to %Public%
- encrypt cosmo.jpeg and exfiltrate data

Q: What URI is used to exfiltrate data?
A: http://cdn[.]altimiter[.]local/feed?post=[data]

Q: What type of data is exfiltrated (the file is cosmo.jpeg, but how exactly is the file's data transmitted?)
A: Data from cosmo.jpeg and encrypted using key stored in passwrd.txt

Q: What kind of encryption algorithm is in use?
A: RC4

Q: What key is used to encrypt the data?
A: SikoMode (passwrd.txt)

Q: What is the significance of houdini?
A: Delete itself from disk