Static analysis:
sha256sum:
248D491F89A10EC3289EC4CA448B19384464329C442BAC395F680C4F3A345C8C

Md5sum: E925C3C5D8AB310DF586608885AEA0E7

46/75 vendors flagged this as malicious.
Trojan, Dropper

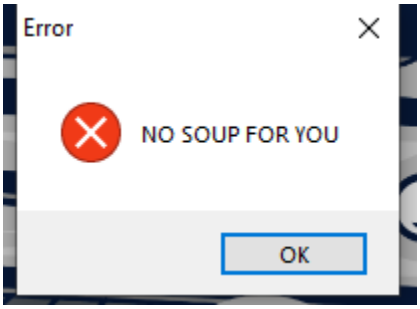
FLOSS:

- @Appdata\Roaming\Microsoft\Windows\Start Menu\ Programs\Startup

Dynamic analysis:

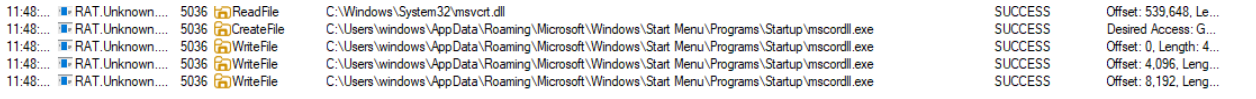
Initial Detonation:

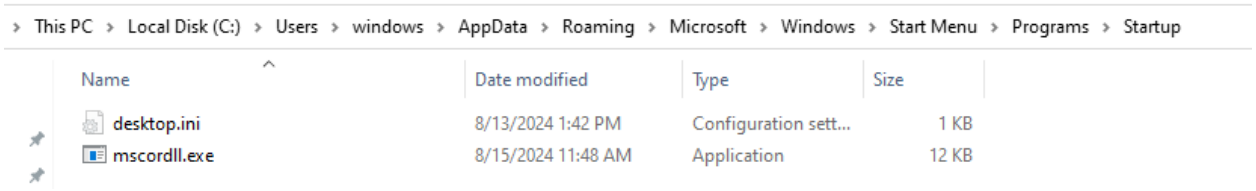
- If doesn't meet criteria (internet connection):
  - NO SOUP FOR YOU displays to screen



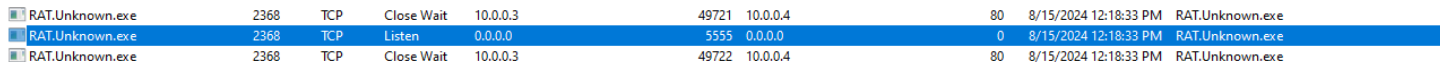
- If does:
  - Creates a file, likely for persistence, in Appdata\Roaming\Microsoft\Windows\Start menu\Programs\Startup\mscordll.exe

Host Indicators:

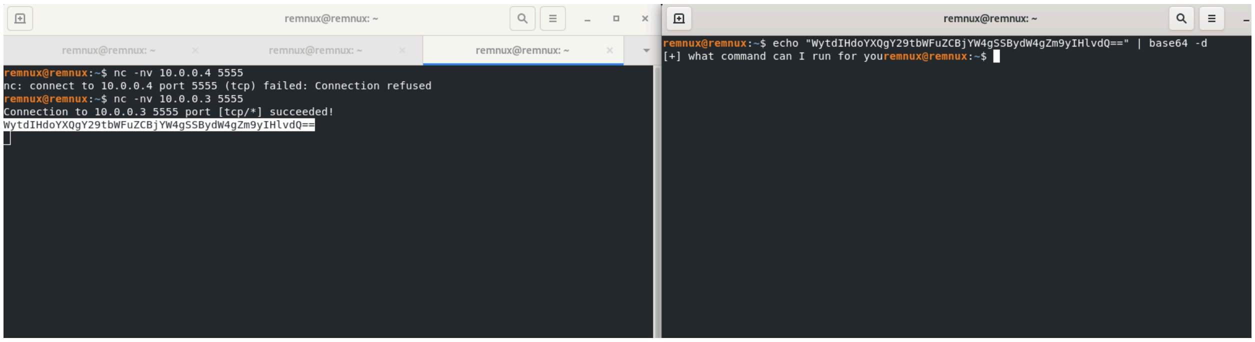




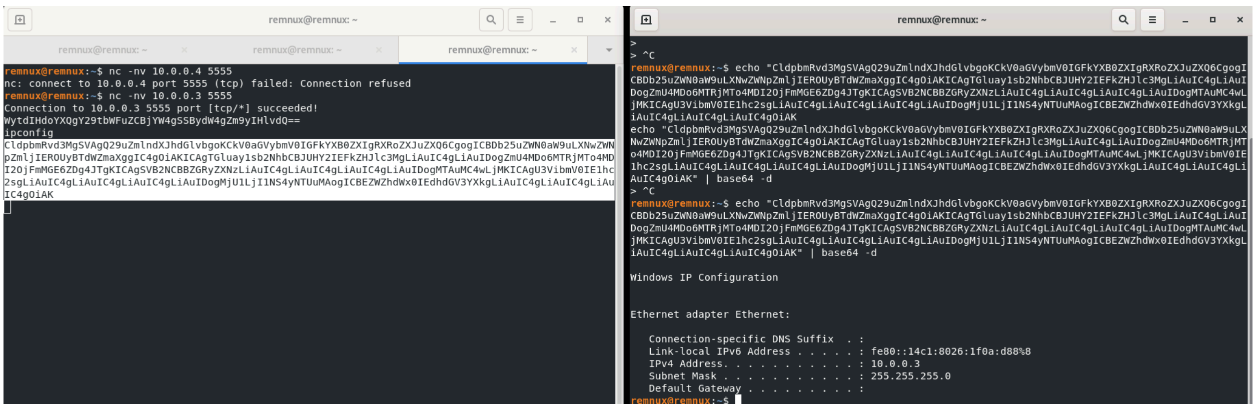
mscordll.exe tries to connect to the internet. Common way to create persistence



TCP socket in listening state on port 5555



Base64 encoded data from socket on TCP 5555



Command injection capability