

Static analysis:

sha256sum:
248D491F89A10EC3289EC4CA448B19384464329C442BAC395F680C4F3A345C8C

Md5sum: E925C3C5D8AB310DF586608885AEA0E7

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

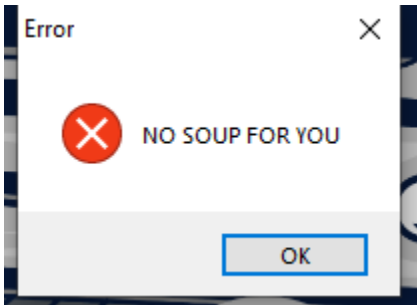
FLOSS:

- @AppdataRoaming\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:

11:48:...	RAT.Unknown.exe	5036	ReadFile	C:\Windows\System32\msvcr.dll	SUCCESS	Offset: 539,648, Le...
11:48:...	RAT.Unknown.exe	5036	CreateFile	C:\Users\windows\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mscordll.exe	SUCCESS	Desired Access: G...
11:48:...	RAT.Unknown.exe	5036	WriteFile	C:\Users\windows\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mscordll.exe	SUCCESS	Offset: 0, Length: 4...
11:48:...	RAT.Unknown.exe	5036	WriteFile	C:\Users\windows\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mscordll.exe	SUCCESS	Offset: 4,096, Leng...
11:48:...	RAT.Unknown.exe	5036	WriteFile	C:\Users\windows\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\mscordll.exe	SUCCESS	Offset: 8,192, Leng...

> This PC > Local Disk (C:) > Users > windows > AppData > Roaming > Microsoft > Windows > Start Menu > Programs > Startup

Name	Date modified	Type	Size
desktop.ini	8/13/2024 1:42 PM	Configuration sett...	1 KB
mscordll.exe	8/15/2024 11:48 AM	Application	12 KB

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

RAT.Unknown.exe	2368	TCP	Close Wait	10.0.0.3	49721	10.0.0.4	80	8/15/2024 12:18:33 PM	RAT.Unknown.exe
RAT.Unknown.exe	2368	TCP	Listen	0.0.0.0	5555	0.0.0.0	0	8/15/2024 12:18:33 PM	RAT.Unknown.exe
RAT.Unknown.exe	2368	TCP	Close Wait	10.0.0.3	49722	10.0.0.4	80	8/15/2024 12:18:33 PM	RAT.Unknown.exe

TCP socket in listening state on port 5555

