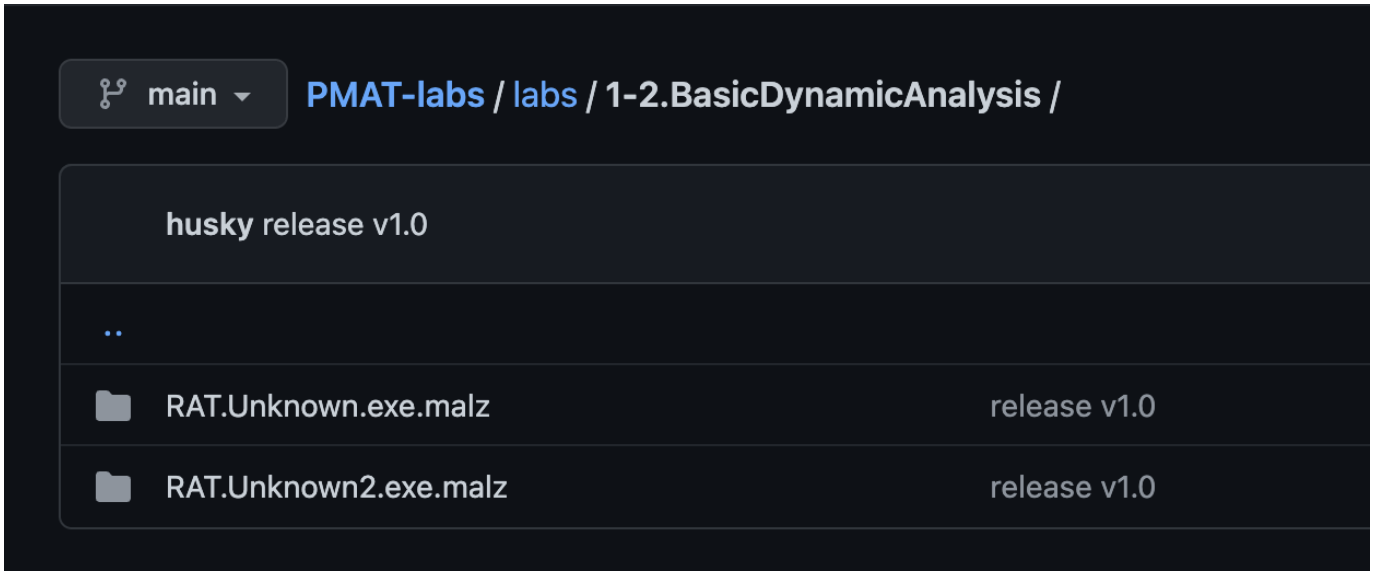
1-2. Basic Dynamic Analysis

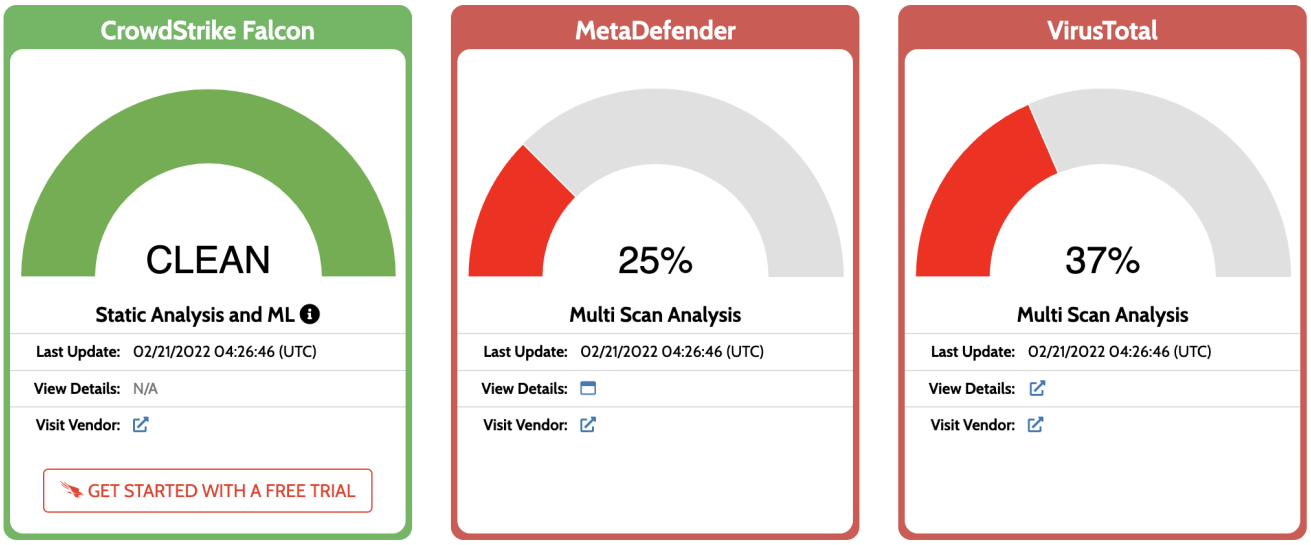
In this section let's talk about the basic dynamic analysis of the malware samples.

> Raher than using our custom lab we will be using any.run/hybrid analysis for quick analysis.

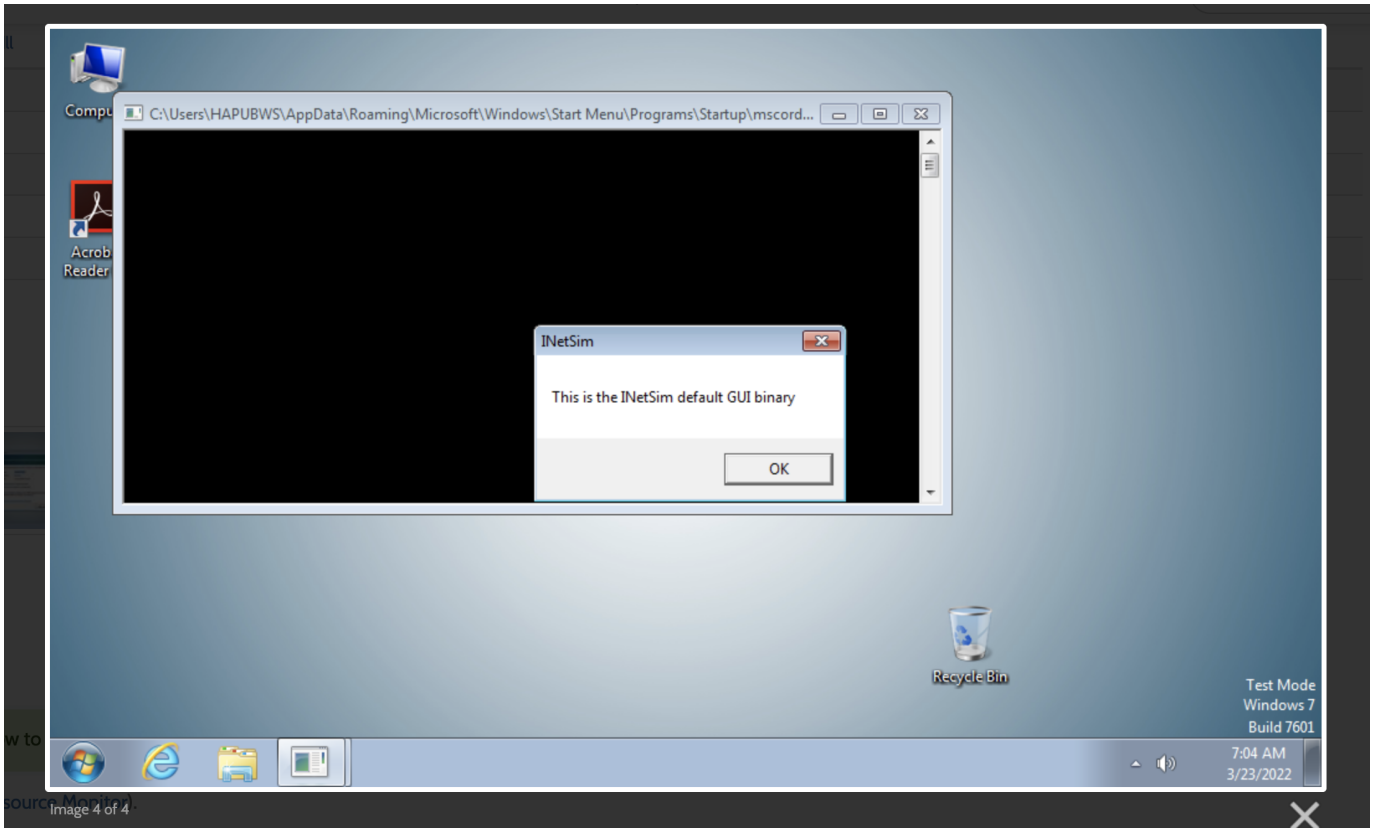


> https://github.com/HuskyHacks/PMAT-labs/tree/main/labs/1-2.BasicDynamicAnalysis/RAT.Unknown.exe.malz

So, let's upload the sample on Hybrid Analysis and check what it greets us with.



It is confirmed that the executable is malicious indeed. Also, we are greeted with a message box which says that this is an INetSim default GUI Binary.



Which also makes a request to the following domain (Possible Network Based Indicators)

DNS Requests

Login to Download DNS Requests (CSV)

Domain
serv1.ec2-102-95-13-2-ubuntu.local

Host based indicators include the dropped files, their locations, registry edits etc.

Installation/Persistence

Connects to LPC ports

details "mscordll.exe" connecting to "\ThemeApiPort"
source API Call
relevance 1/10

Dropped files

details "mscordll.exe.bin" has type "PE32 executable (console) Intel 80386 (stripped to external PDB) for MS Windows"
"mscordll.exe" has type "PE32 executable (console) Intel 80386 (stripped to external PDB) for MS Windows"
source Extracted File
relevance 3/10

Touches files in the Windows directory

details "RAT.Unknown.exe" touched file "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\mscordll.exe"
"RAT.Unknown.exe" touched file "%APPDATA%\Microsoft\Windows\Cookies"
source API Call
relevance 7/10

Detailed Analysis is provided by Hybrid Analysis which can be looked at the following URL..

> https://www.hybrid-analysis.com/sample/248d491f89a10ec3289ec4ca448b19384464329c442bac395f680c4f3a345c8c/623ac40656257745b114d302

Similarly, we can perform the analysis on the second file as well.

Follow Me

Twitter: https://twitter.com/deFr0ggy

GitHub: https://github.com/deFr0ggy

LinkedIn: https://linkedin.com/in/kamransaifullah