**RAT.Unknown2.exe**

**Static Analysis**

* File hashes do not return any results on VirusTotal so we can infer this is custom malware
* Not too many interesting strings however, we did see strings such as socket, closeSocket, writefile so we can infer the malware is attempting to make a network connection and may be writing a file to the host machine.
* There were also not too many interesting API calls some were in the “flagged” column of PEStudio but nothing that really stood out

**Dynamic Analysis**

**Table

Description automatically generated with medium confidence**

**DNS callout** to the aaaaaaaaaaaaaaaaaa.kedusus.local domain

Using procmon and ncat we can see this malware has reverse shell capabilities

Graphical user interface, text, application

Description automatically generated