RAT.Reverseshell.EXE

Sunday, July 02, 2023 11:40 AM

Static Analysis

Hashes

md5sum.exe c211704777e168a5151de79dc87ffac7
sha256sum.exe 481eae82ac4cd1a9cfadc026a628b18d7b4c54f50385d28c505fbcb3e999b8b0
sha1sum.exe 1f688b4872f8a740872b5cb6d58e2b9c7103143a

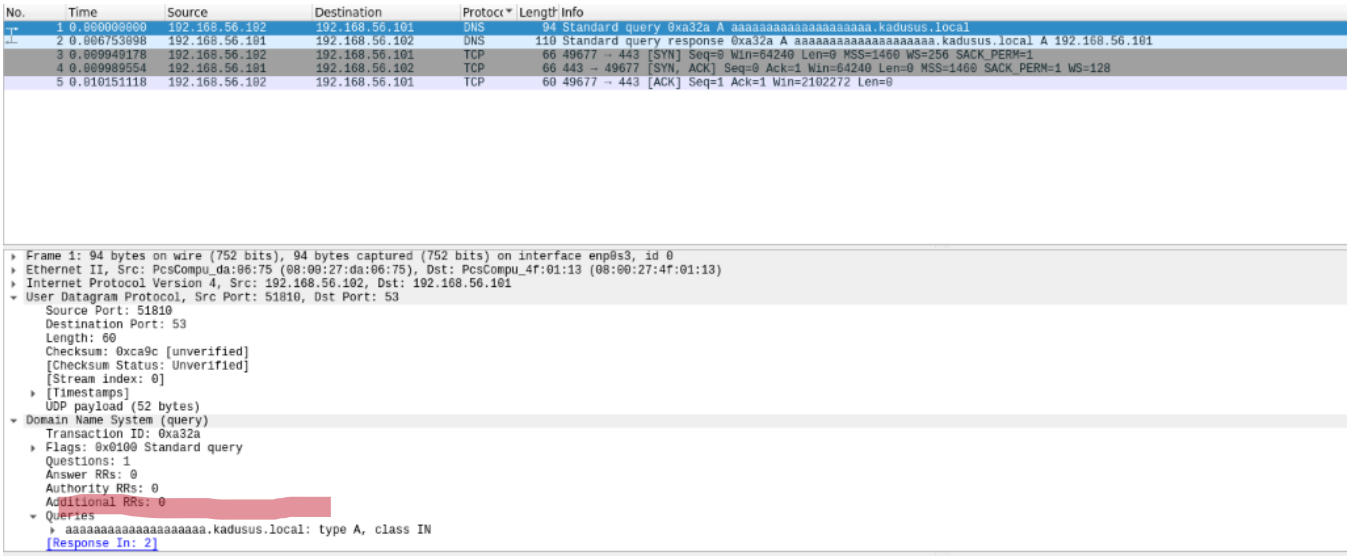
Floss/Strings

@cmd.exe /c
@exit
@.local
@iterators.nim(189, 11) `len(a) == L` the length of the seq changed while iterating over it
@kadusus

Dynamic Analysis

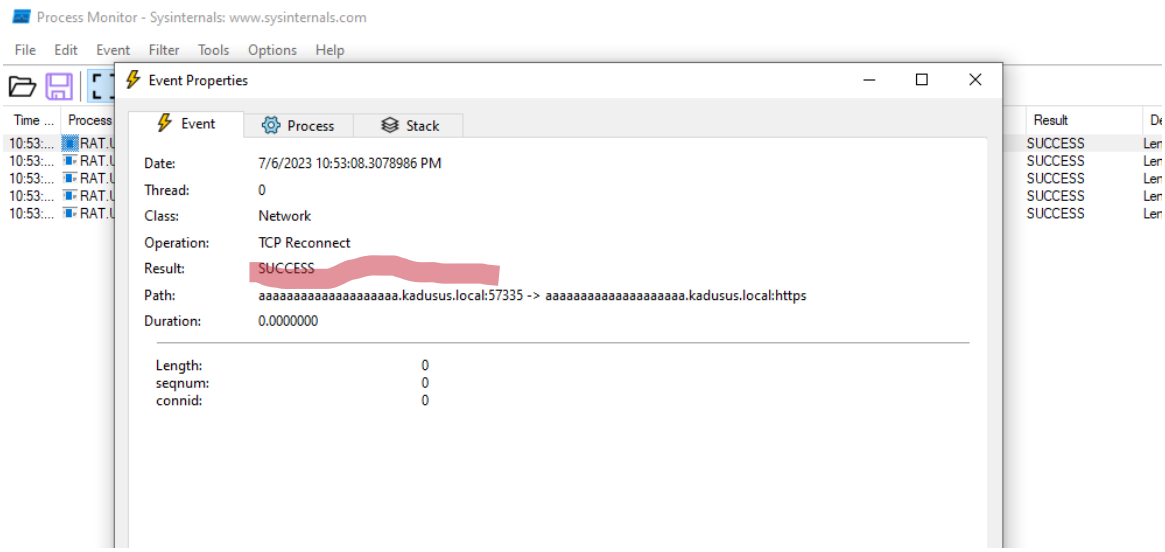
Network based Indicators

Creating a dns request



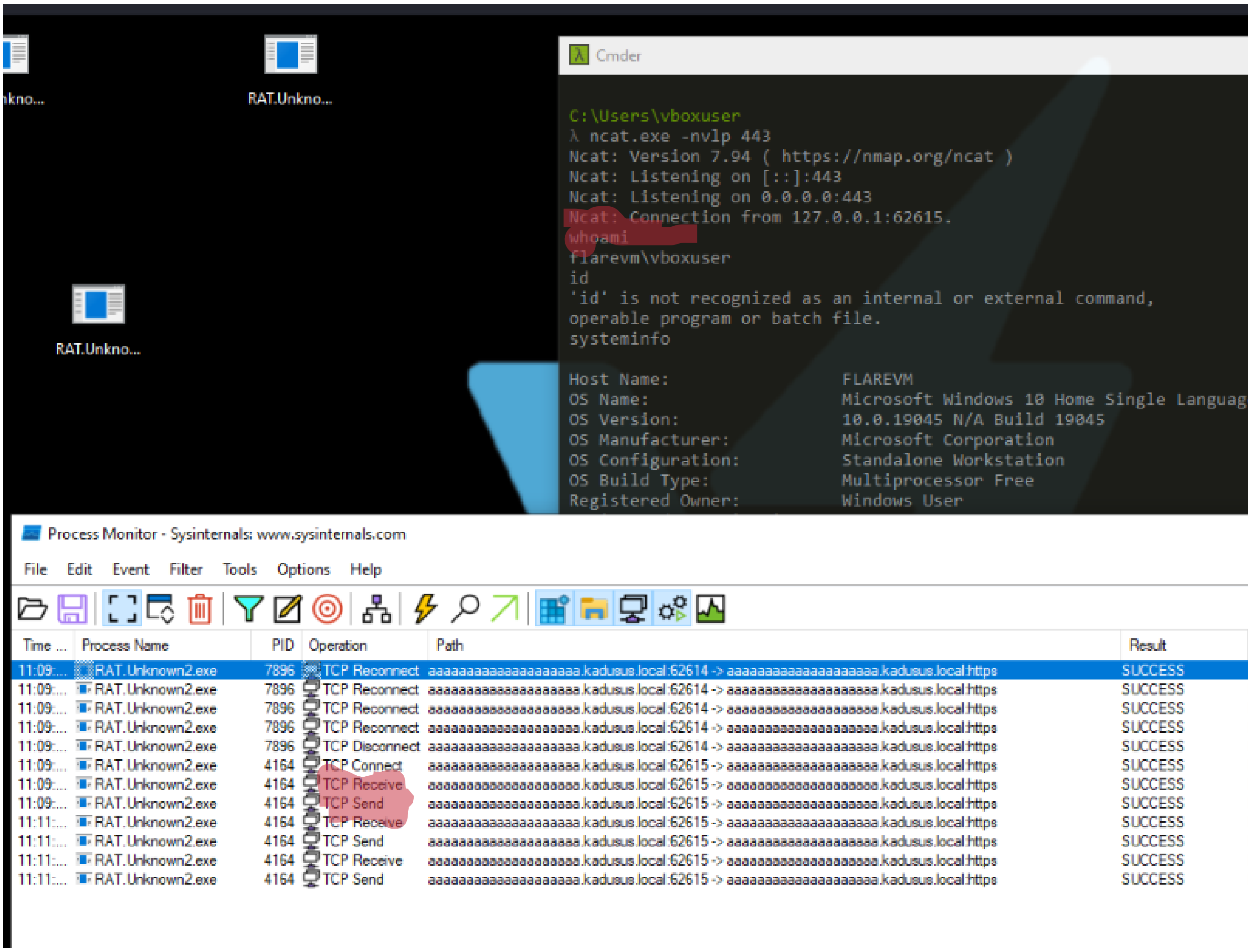
Host Based Indicators

DNS request
Requsting for aaaaaaaaaaaaaaaaaaa.kadusus.local



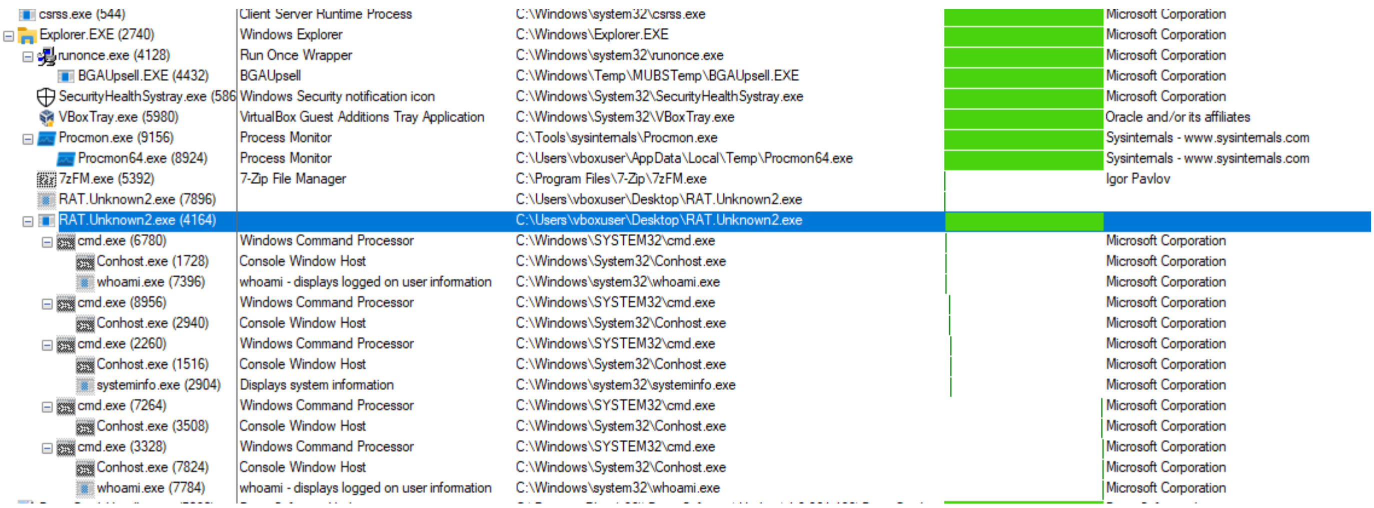
Reverse Shell capability

At port 443



Process tree

Have cmd.exe as child of this malware



In last we can say that this EXE have capability of revershell connection and command injection at port 443