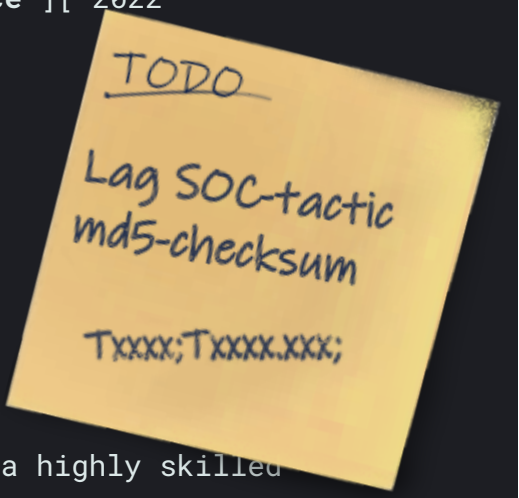

SECOPS
COMMAND
Cyber Defense



The threat actor

SecOpsCommand has been tracking what we assume is a highly skilled threat actor for some time. There are to our knowledge no other sightings to their existence than what has been detected by SecOpsCommand.

We have analysed some artefacts collected by our sensors. Among the artefacts there was a file collected from the user-space in Windows that we believe to be an internal log file from a second-stage tool - this as likely with low confidence.

From further analysis we can with high confidence conclude that the actor we call *FerRAT* has at least the following tooling in their arsenal:

] Command & Control [
Data Encoding https://attack.mitre.org/techniques/T1132/
Application Layer Protocol
https://attack.mitre.org/techniques/T1071/
Encrypted Channel: Symmetric Cryptography
https://attack.mitre.org/techniques/T1573/001/
Dynamic Resolution: Domain Generation Algorithms
https://attack.mitre.org/techniques/T1568/002/
SOC-tactic-ID: cc4d2d502cf8fb1cced8310a1985243f

] Execution [
System Services https://attack.mitre.org/techniques/T1569/
Command and Script Interpreter
https://attack.mitre.org/techniques/T1059/
SOC-tactic-ID: