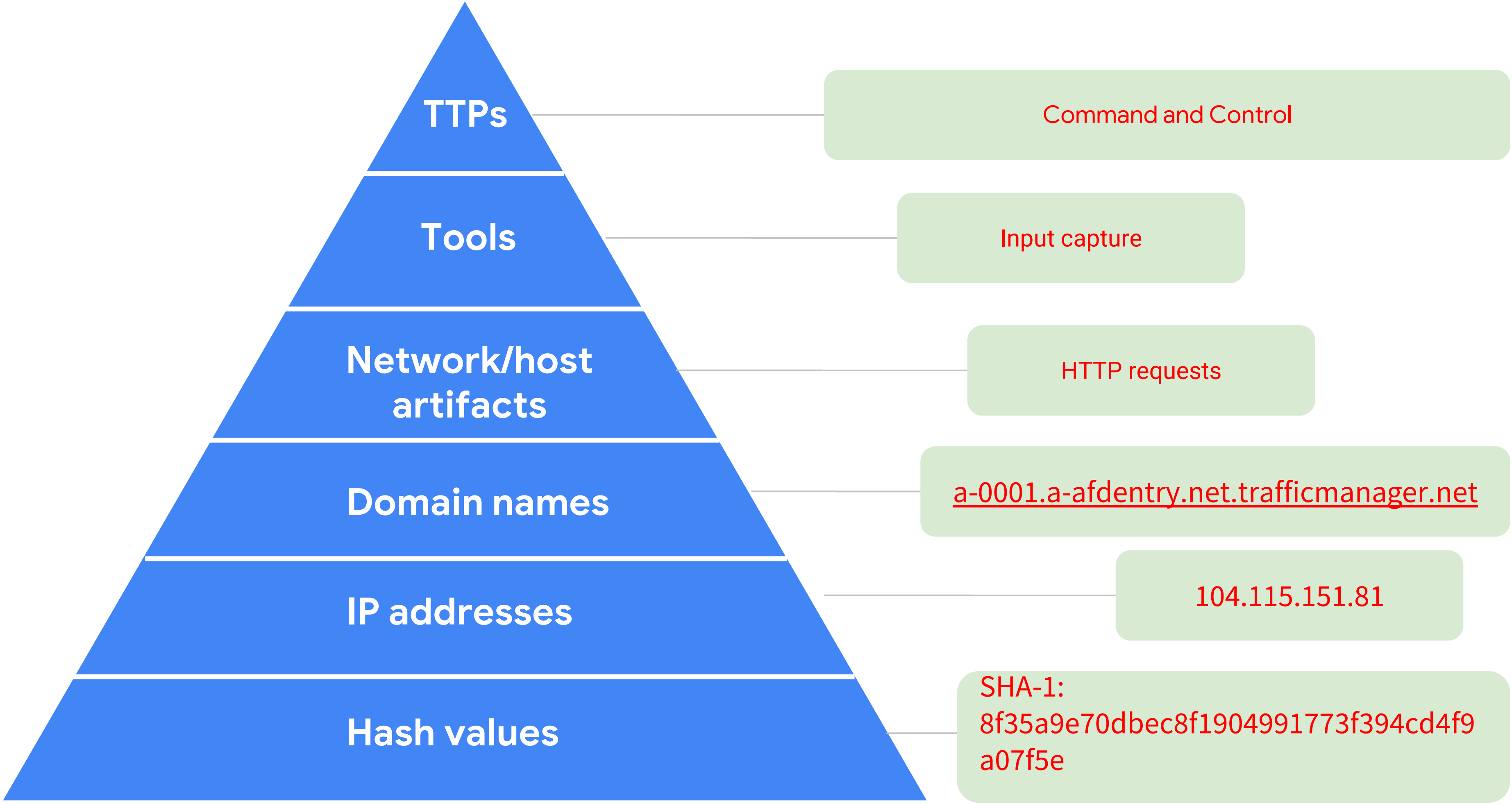
Has this file been identified as malicious? Explain why or why not.

Based on the investigation using Virustotal with the SHA256 file hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b), this file has been identified as malicious. Vendor’s ratio rated this at 59/73 and Community score marked it as -238. A file with a high number of vendor flags is more likely to be malicious and with a community score of minus is also most likely to be malicious. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech.



TTPs — Command and Control

Tools — Input capture

Network/host artifacts — HTTP requests

Domain names — a-0001.a-afdentry.net.trafficmanager.net

IP addresses — 104.115.151.81

Hash values — SHA-1: 8f35a9e70dbec8f1904991773f394cd4f9a07f5e