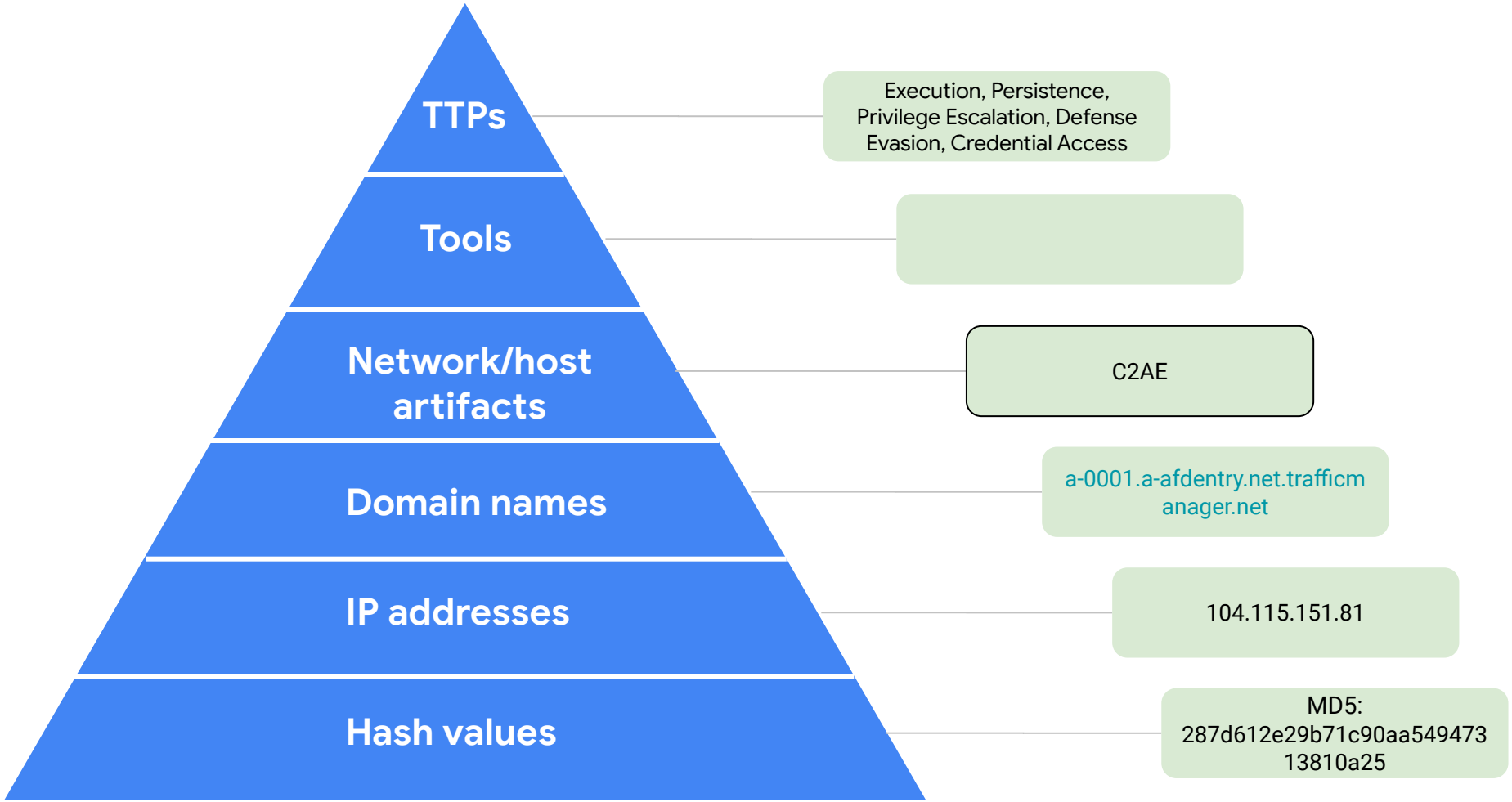
Has this file been identified as malicious? Explain why or why not.

61/73 security vendors and 3 sandboxes flagged this file as malicious. Therefore, this file is malicious.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access
C2AE
a-0001.a-afdentry.net.trafficmanager.net
104.115.151.81
MD5: 287d612e29b71c90aa54947313810a25