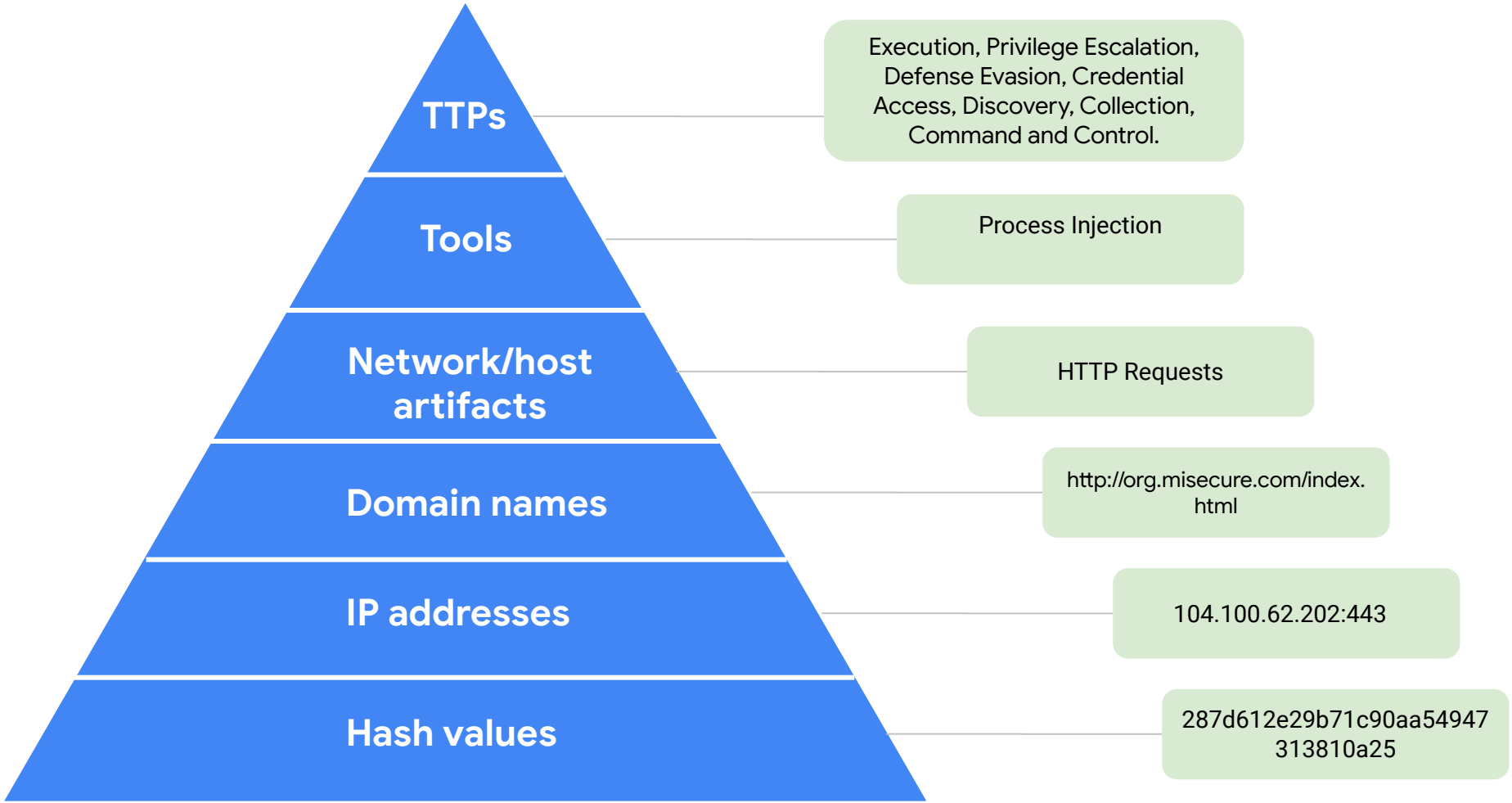
Has this file been identified as malicious? Explain why or why not.

The file hash has been reported as malicious by over 50 vendors. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Execution, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Collection, Command and Control.
Process Injection
HTTP Requests
http://org.misecure.com/index.html
104.100.62.202:443
287d612e29b71c90aa54947313810a25