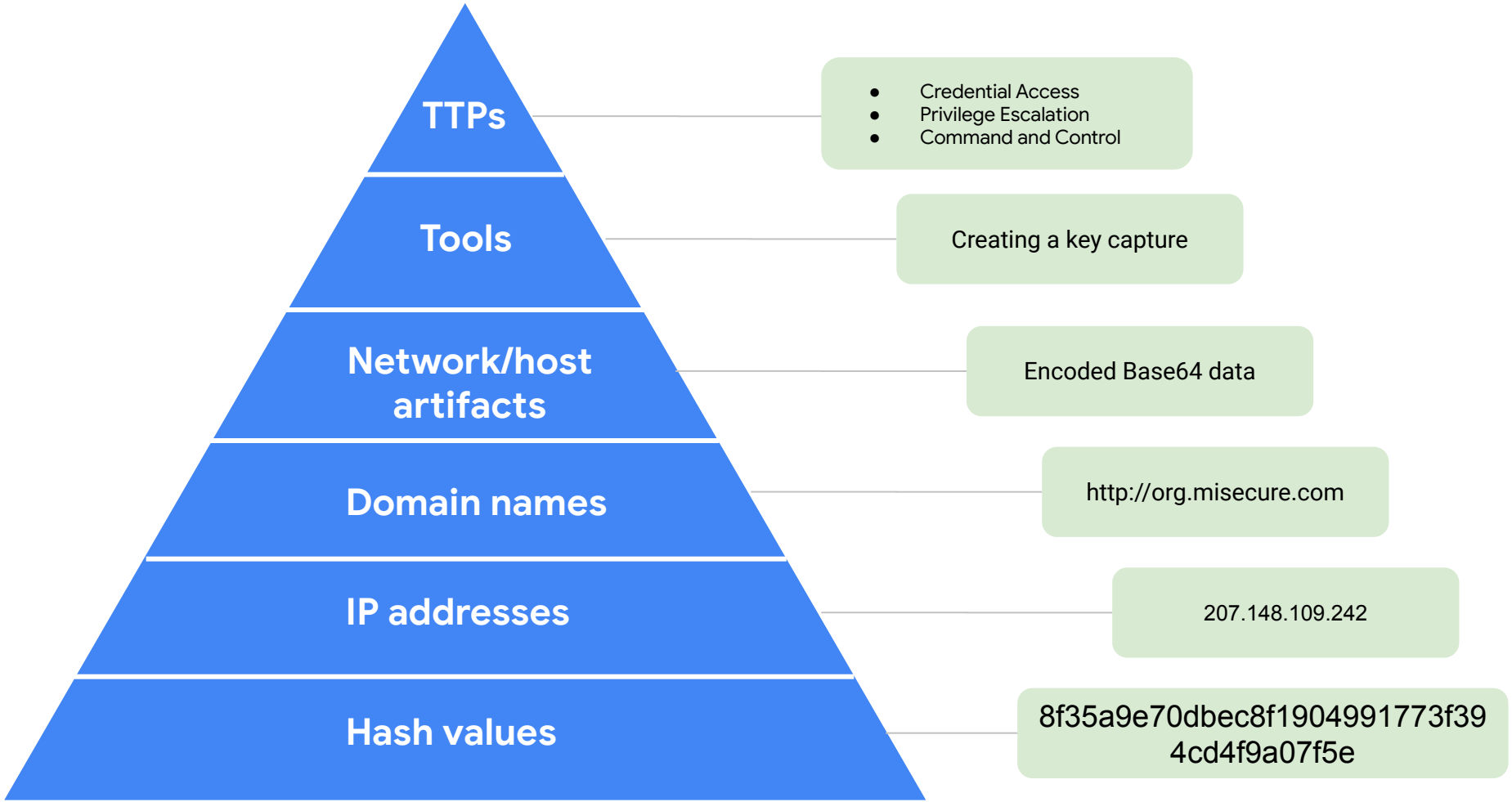
Has this file been identified as malicious? Explain why or why not.

Based on analysis of the hash using TotalVirus, it is shown that the file has been identified as malicious. A high vendor's ratio as over 50 vendors reported the file as being malicious and very negative Community score suggests that the file is very likely to be malicious. Under the Detection tab, many security vendors has flagged the file as malicious. Upon reading community reports/comments, the malware is listed under the trojan threat category under the name Flagpro, commonly used by the threat actor BlackTech.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Credential Access
Privilege Escalation
Command and Control
Creating a key capture
Encoded Base64 data
http://org.misecure.com
207.148.109.242
8f35a9e70dbec8f1904991773f39 4cd4f9a07f5e