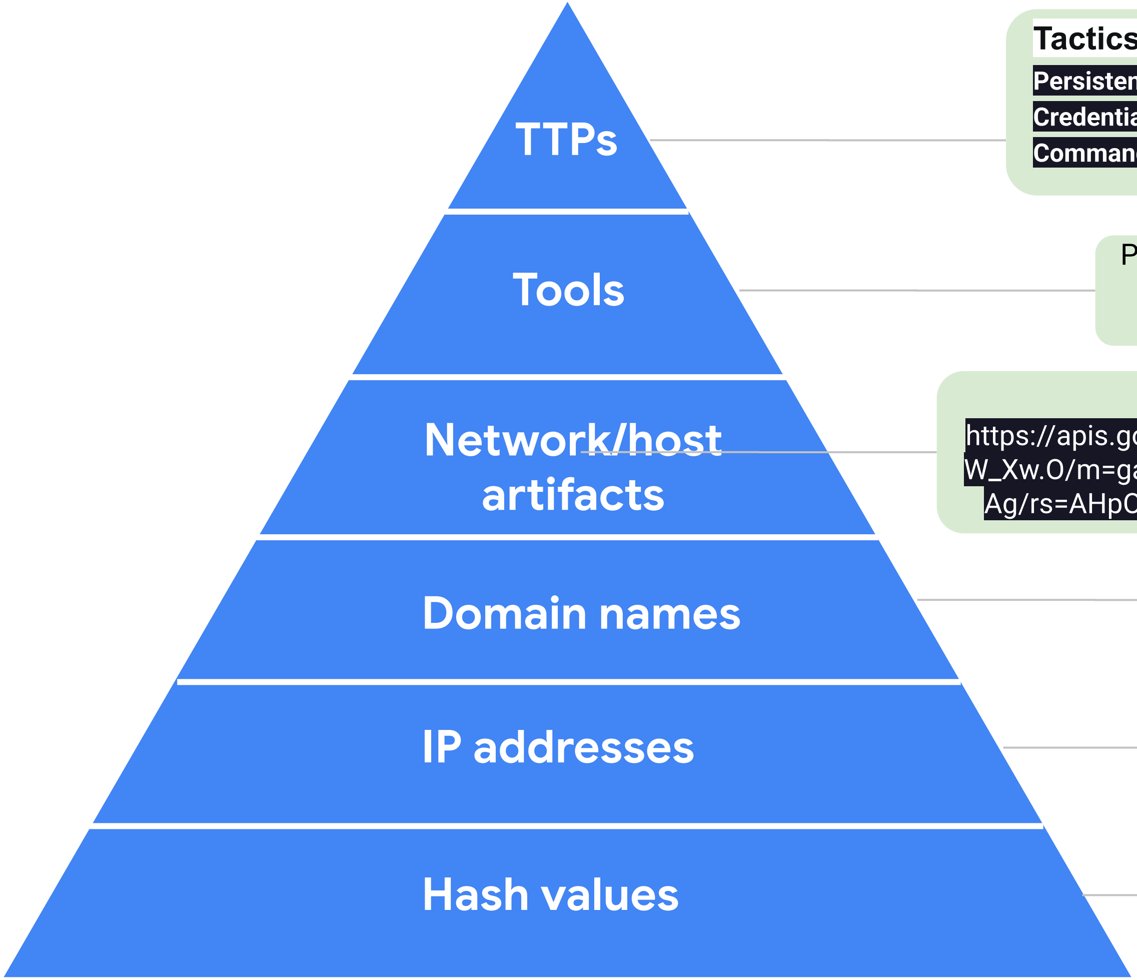
Has this file been identified as malicious? Explain why or why not.

The hash file has been seen to be malicious and has affected over 50+ vendors. The malicious file that the virus came from is also under named called Flagpro, which can be traced back to a group of people called BlackTech



Tactics, techniques, and procedures : ExecutionTA0002, **Persistence**TA0003, **Privilege Escalation**TA0004, **Defense Evasion**TA0005, **Credential Access**TA0006, **Discovery**TA0007, **Collection**TA0009, **Command and Control**TA0011, **Impact**TA0040

Possible tools: Input Capture and creating automating viruses

Get Requests: GET https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.MGCxJbnW_Xw.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/am=AAAg/rs=AHpOoo9xa4htLEVH9xe6c4ToUehtTaLWvA/cb=gapi.loaded_0

org.misecure.com

TCP 204.79.197.203:443 (www.msn.com)

MD5; 287d612e29b71c90aa54947313810a25