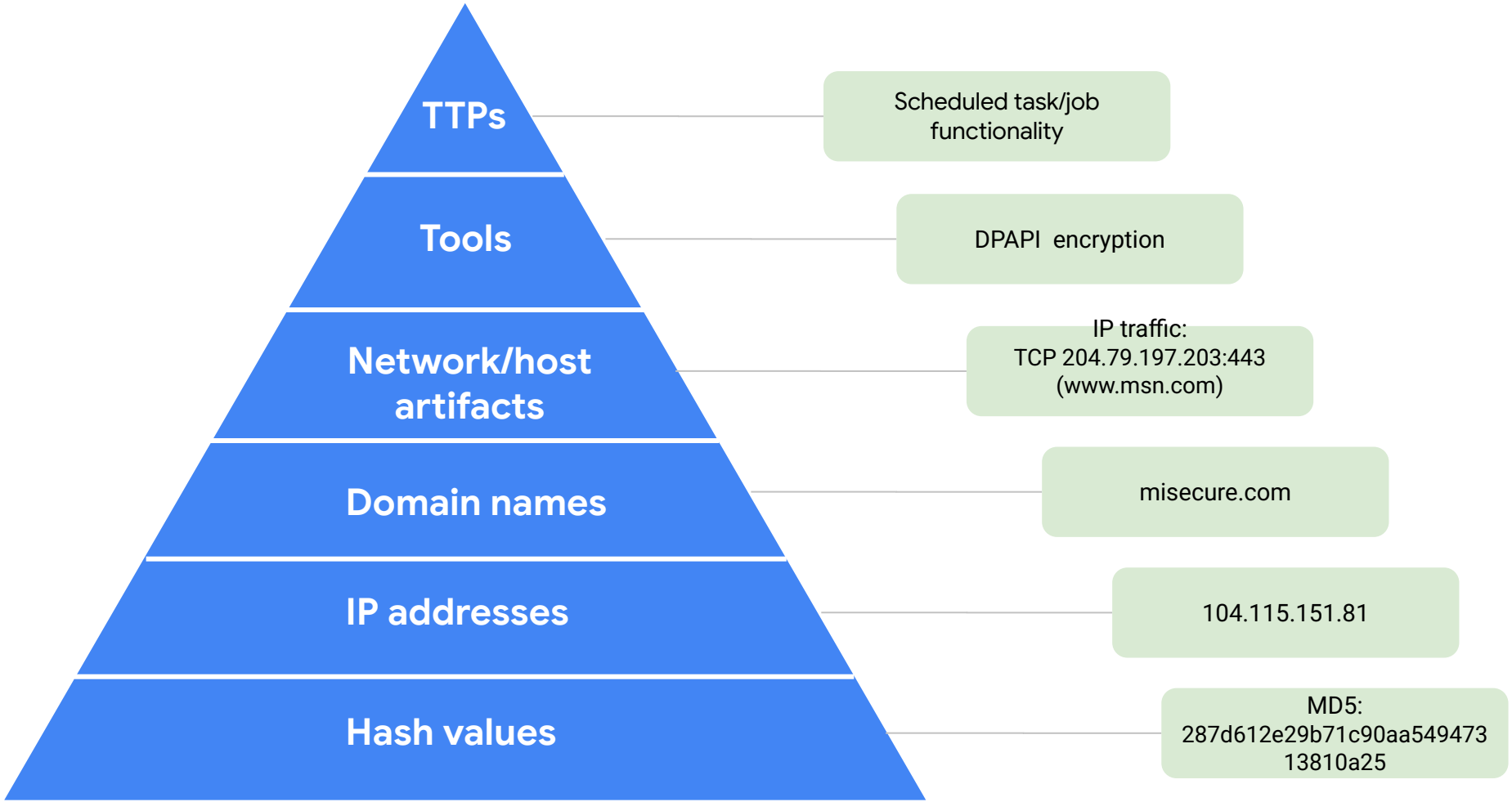
Has this file been identified as malicious? Explain why or why not.

The file was identified as malicious. The vendors' ratio is a high 58/71 with the community score of -221 as well. More than half of the security vendors in the detection tab of the report have flagged it as malicious because of the data exfiltration behavior.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Scheduled task/job functionality
DPAPI encryption
IP traffic: TCP 204.79.197.203:443 (www.msn.com)
misecure.com
104.115.151.81
MD5: 287d612e29b71c90aa549473 13810a25