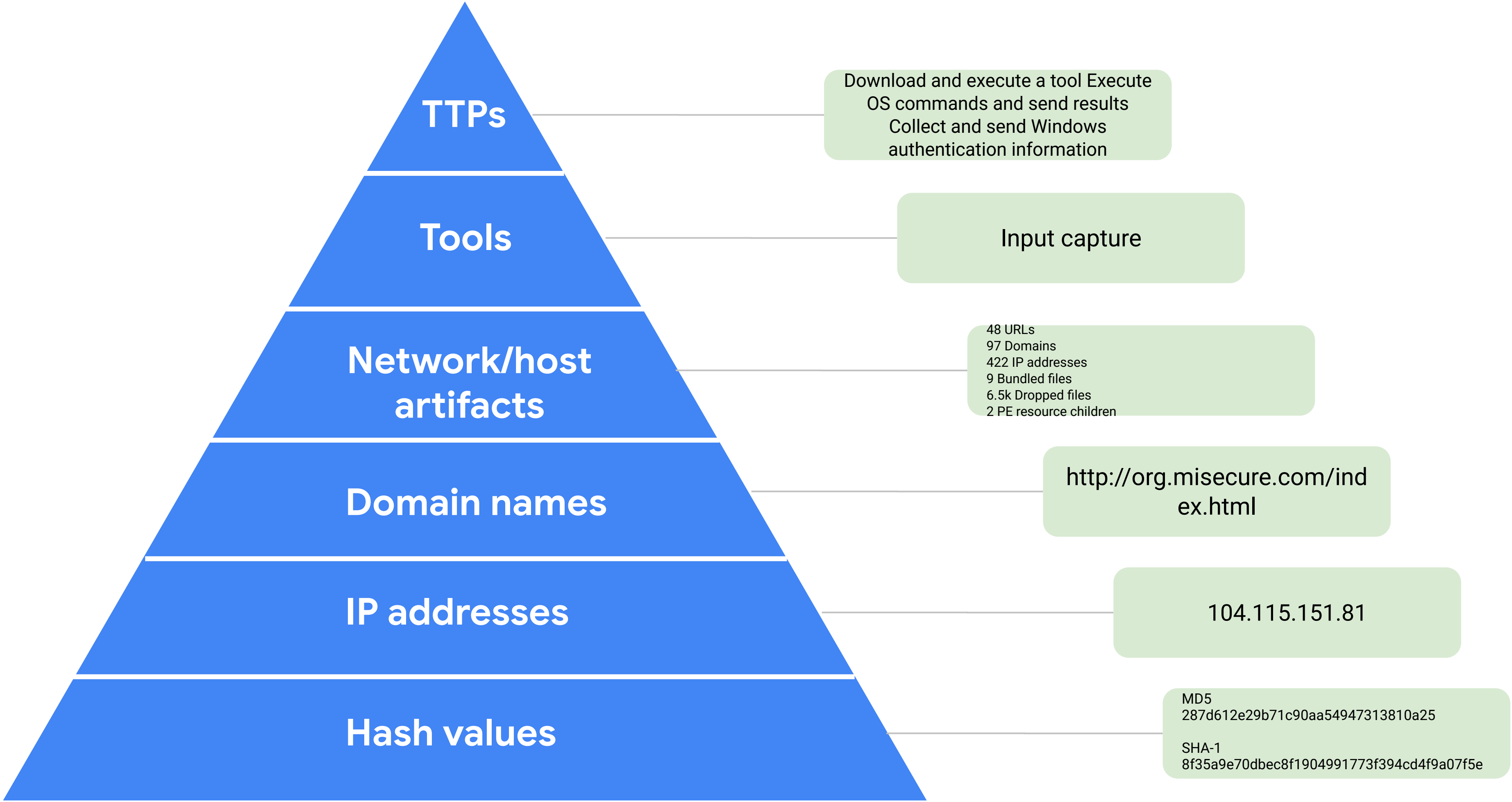
Has this file been identified as malicious? Explain why or why not.

This file has been flagged as a malicious trojan file, Flagpro. It has a high vendor’s ratio, very low community score and has been detected and flagged more than 10 times in security vendor’s analysis tab.



TTPs

Download and execute a tool Execute OS commands and send results Collect and send Windows authentication information

Tools

Input capture

Network/host artifacts

48 URLs
97 Domains
422 IP addresses
9 Bundled files
6.5k Dropped files
2 PE resource children

Domain names

http://org.misecure.com/index.html

IP addresses

104.115.151.81

Hash values

MD5
287d612e29b71c90aa54947313810a25

SHA-1
8f35a9e70dbec8f1904991773f394cd4f9a07f5e