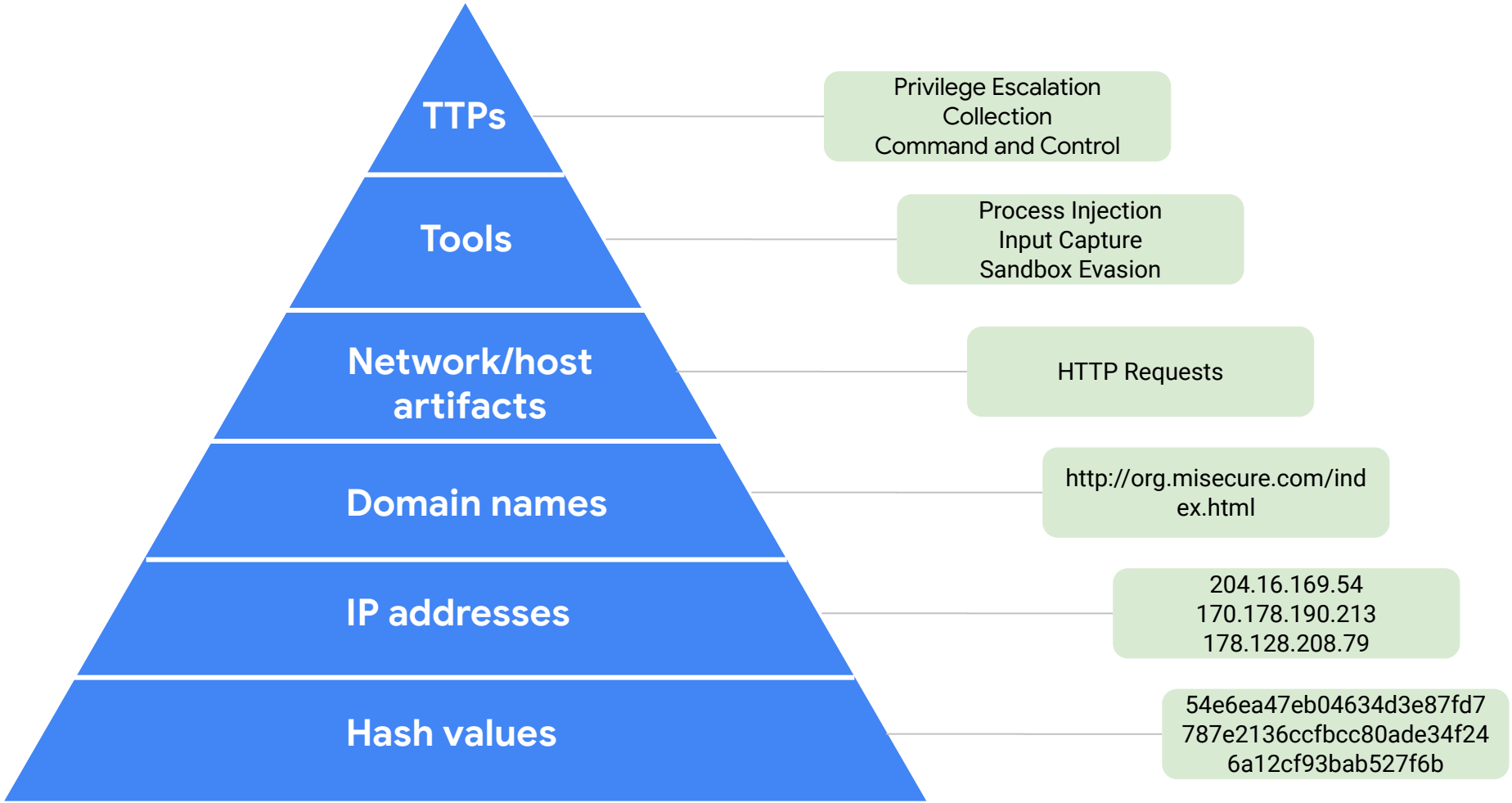
Has this file been identified as malicious? Explain why or why not.

-Hashsum => 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
-When activated, several unauthorized files were downloaded, triggering the IDS
-When the hash of the program was search for in VirusTotal.com, it declared it to be a malicious file by both vendors and the community.

>57 total vendors have the file marked as a malicious file, known as a “Trojan”
>The files hash has been marked by the name “flagpro”
>Appears to have the ability to:
-Input capture
-Process Injection
-Virtualization/Sandbox Evasion
-Steal Web Session Cookies
-Masquerading

File should be considered dangerous, isolate the infected system and consult the incident response playbook.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Privilege Escalation
Collection
Command and Control
Process Injection
Input Capture
Sandbox Evasion
HTTP Requests
http://org.misecure.com/index.html
204.16.169.54
170.178.190.213
178.128.208.79
54e6ea47eb04634d3e87fd7
787e2136ccfbcc80ade34f24
6a12cf93bab527f6b