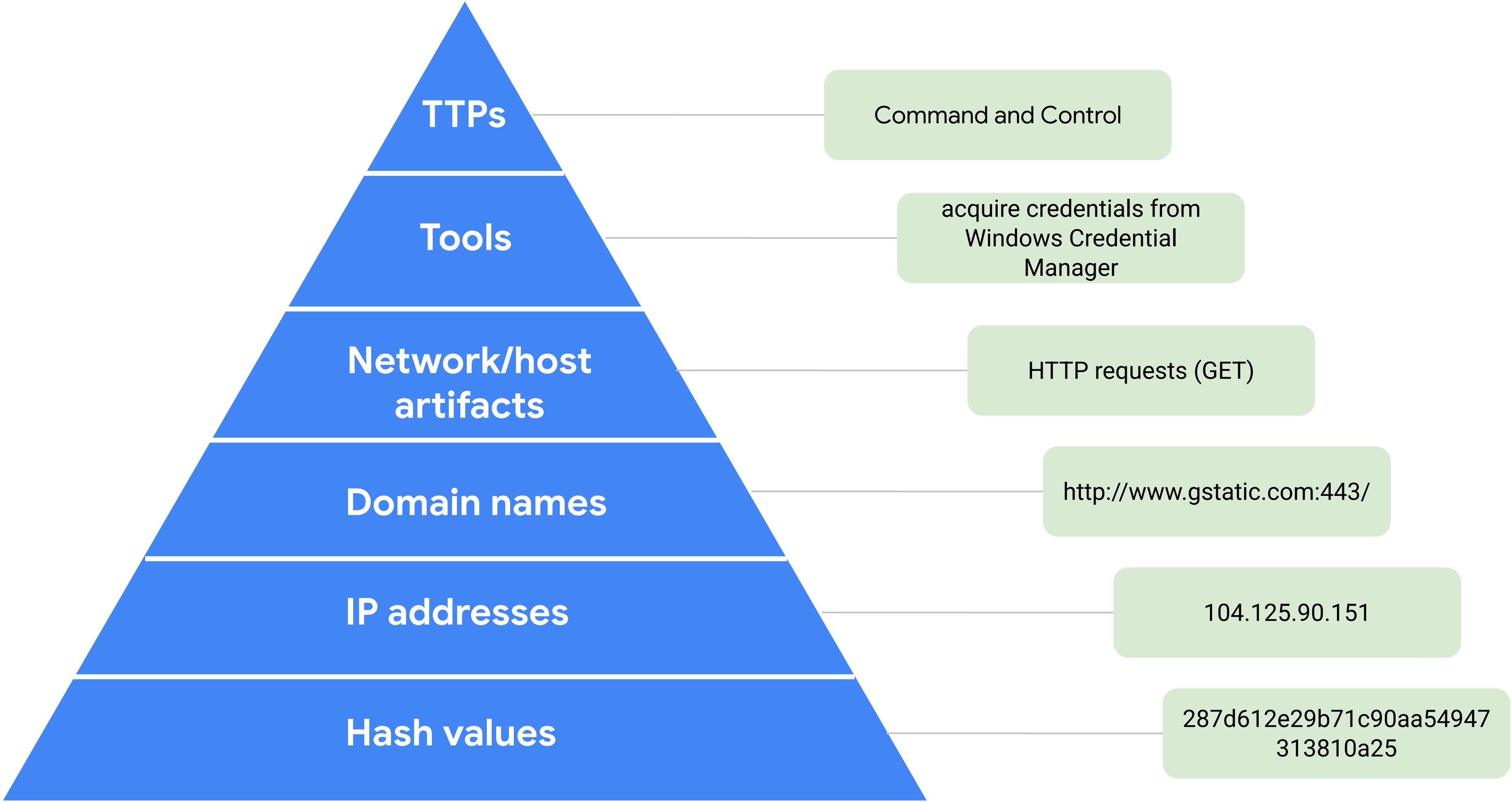
Has this file been identified as malicious? Explain why or why not.

The security team believes that this file is malicious. The SHA256 file hash was checked by searching the VirusTotal database. It has a very high number of positive malicious detections by vendors. It is described as a virus - Trojan. Additionally, the community score, which is "-236," indicates that many people have checked this file and confirmed its harmful nature
.



TTPs — Command and Control

Tools — acquire credentials from Windows Credential Manager

Network/host artifacts — HTTP requests (GET)

Domain names — http://www.gstatic.com:443/

IP addresses — 104.125.90.151

Hash values — 287d612e29b71c90aa54947313810a25