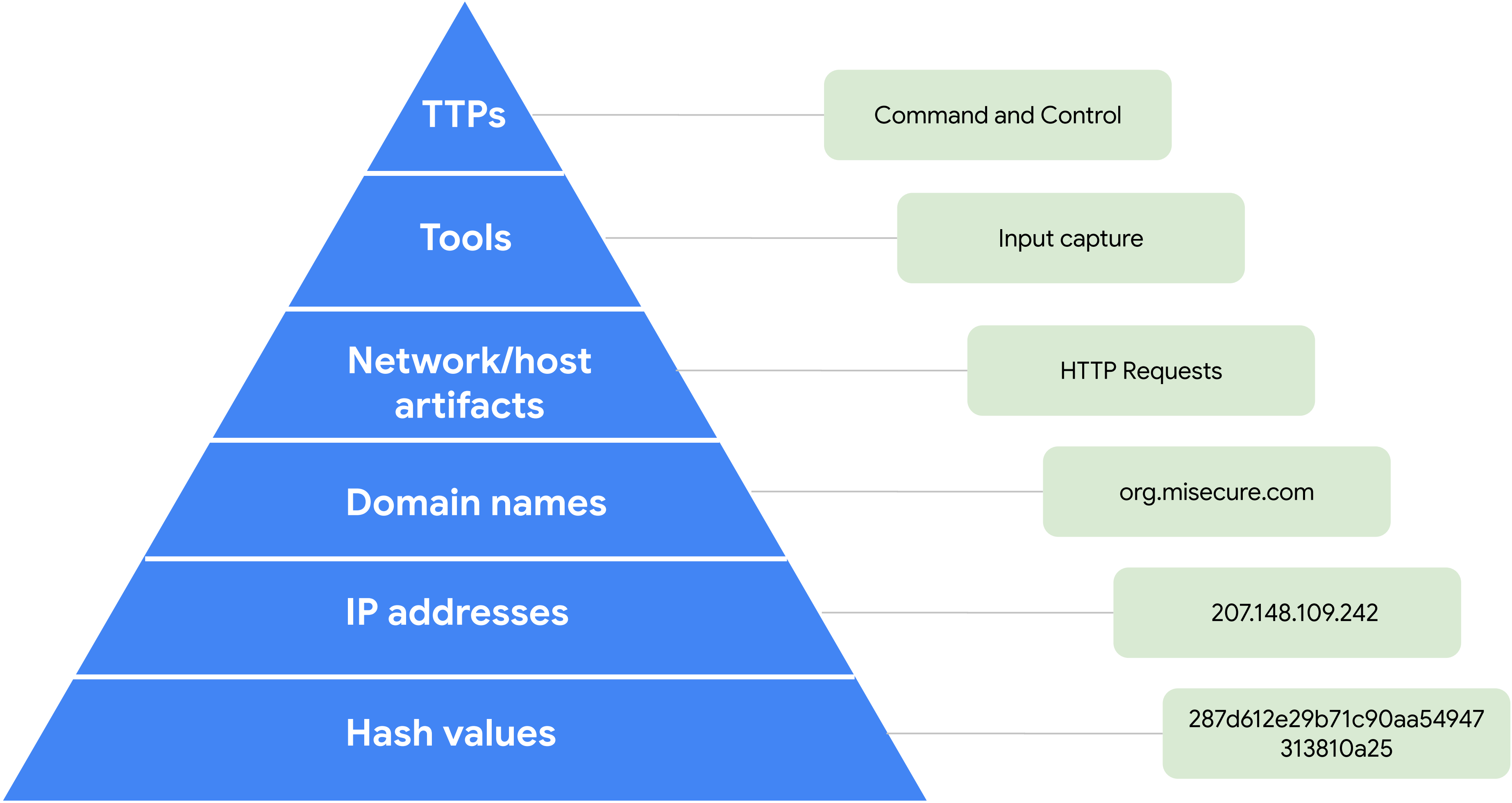
Malicious File Identified as Flagpro Malware Linked to APT Group BlackTech

The file hash has been flagged as malicious by over 50 security vendors. Further analysis reveals that it corresponds to Flagpro, a known malware strain frequently leveraged by the advanced persistent threat (APT) group BlackTech, recognized for its targeted and stealthy cyber operations.



TTPs

Command and Control

Tools

Input capture

Network/host artifacts

HTTP Requests

Domain names

org.misecure.com

IP addresses

207.148.109.242

Hash values

287d612e29b71c90aa54947
313810a25