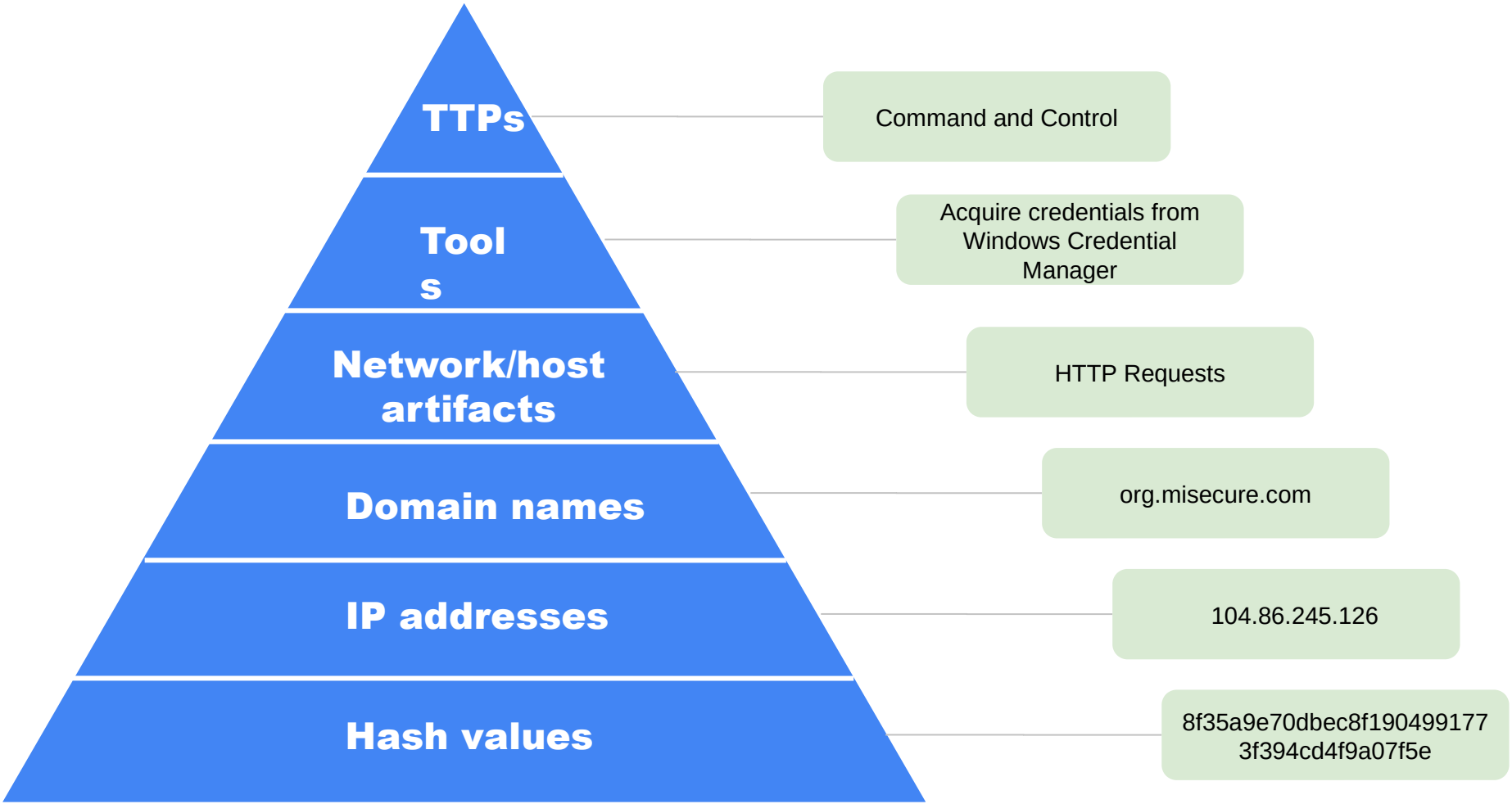
Malware Incident Analysis Report

The file hash has been identified as malicious by more than 50 vendors. Further analysis reveals that this file hash corresponds to the malware known as Flagpro, which is frequently utilized by the advanced threat actor group BlackTech.


TTPs
Tool
s
Network/host
artifacts
Domain names
IP addresses
Hash values
Command and Control
Acquire credentials from
Windows Credential
Manager
HTTP Requests
org.misecure.com
104.86.245.126
8f35a9e70dbec8f190499177
3f394cd4f9a07f5e