## Reporting Hash to VirusTotal

The file hash (SHA256 file hash:

**54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b**) has been reported as malicious by over 50 vendors (see <u>Results</u>). Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech.

## Indicators of compromise (IoCs) in Pyramid of Pain **TTPs** Command and Control **Tools** Input capture Network/host **HTTP Requests** artifacts org.misecure.com **Domain names IP addresses** 207.148.109.242 287d612e29b71c90aa54947 Hash values 313810a25