

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

The file hash has been reported as malicious by over 50 vendors. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech.

TTPs

Command and Control

Tools

Input capture

**Network/host
artifacts**

HTTP Requests

Domain names

org.misecure.com

IP addresses

104.115.151.81

Hash values

287d612e29b71c90aa549473
13810a25

