

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

This hash file has been reported as malicious by 58 vendors as of now, and upon further investigation it has been discovered that this file is a trojan horse known as Flagpro, which has been associated with the BlackTech threat group.

TTPs

Command and control

Tools

Input capture

**Network/host
artifacts**

HTTP Requests

Domain names

org.misecure.com

IP addresses

103.193.149.26

Hash values

54e6ea47eb04634d3e87fd77
87e2136ccfbcc80ade34f246a
12cf93bab527f6b

