

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

When scanned with virustotal the file has been identified as malicious file and was flagged by 59 out of 72 vendors as harmful.

There were multiple signs of trojans called Flagpro usually used by advanced threat actor BlackTech. And also has code to make backdoors in the system so that the attacker can maintain prolong access to the device.

TTPs

Execution, Persistent,
Privilege escalation

Tools

Input capture

**Network/host
artifacts**

HTTP Requests

Domain names

org.misecure.com

IP addresses

04.115.151.81

Hash values

287d612e29b71c90a
a54947313810a25

