

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

Hash value obtained(54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) has been processed by VirusTotal website. Results show that nearly 60 vendors flagged this has value to be malicious, and the community score on this file is nearly -300. After further investigation we came to realization that file is trojan type of malware called flagpro.

TTPs

Defense Evasion

Tools

Input capture

**Network/host
artifacts**

HTTP request

Domain names

org.misecure.com/index.ht
ml

IP addresses

204.79.197.203:443

Hash values

54e6ea47eb04634d3e87f
d7787e2136ccfbcc80ade3
4f246a12cf93bab527f6b