

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

This file has been identified as malicious. 52 out of the 66 security vendors have flagged this file as malicious. The file also has a -285 community score, meaning the VirusTotal community agrees that it is malicious. The security vendors' analysis concludes that this file contains a trojan. The popular threat label is trojan.flagpro/fragtor and the threat category is listed as 'trojan'. It was used by the criminal group BlackTech to collect information on victims and execute commands in the victim's environment.

TTPs

Hijack Execution Flow

Tools

Encrypted data using DPAPI

**Network/host
artifacts**

C:\Users\<USER>\AppData\Local\Microsoft\PenWorkspac
e\DiscoverCacheData.dat

Domain names

gstatic.com

IP addresses

104.115.151.81

Hash values

MD5
287d612e29b71c90aa54947313810a25