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

Yes, as previously mentioned before we can assume that the SHA256 hash provided in VirusTotal Scan can be considered malicious due to many alarming flags.

- The community score is quite high, which sits at a score of -216
- We can also mention that the VirusTotal Score is 60/73 which indicates a high possibility of being malicious
- We can also determine that it is a malicious file due to VirusTotal indications of containing Malware, Trojan and Backdoors
- We can also find that the Threat categories are considered “trojan”
- Upon looking further, we have found that the file download was supposed to be a excel spreadsheet file however, the file type was a Win32 EXE which is an executable file
- (Relations tab) - We are able to see some of the behaviors using provided sandbox tests (MITRE ATT&CK) (Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Collection, Command and Control)
- File reported as malicious by over 50 vendors, filehash known as malware Flagpro (commonly used by advanced threat actor BlackTech)