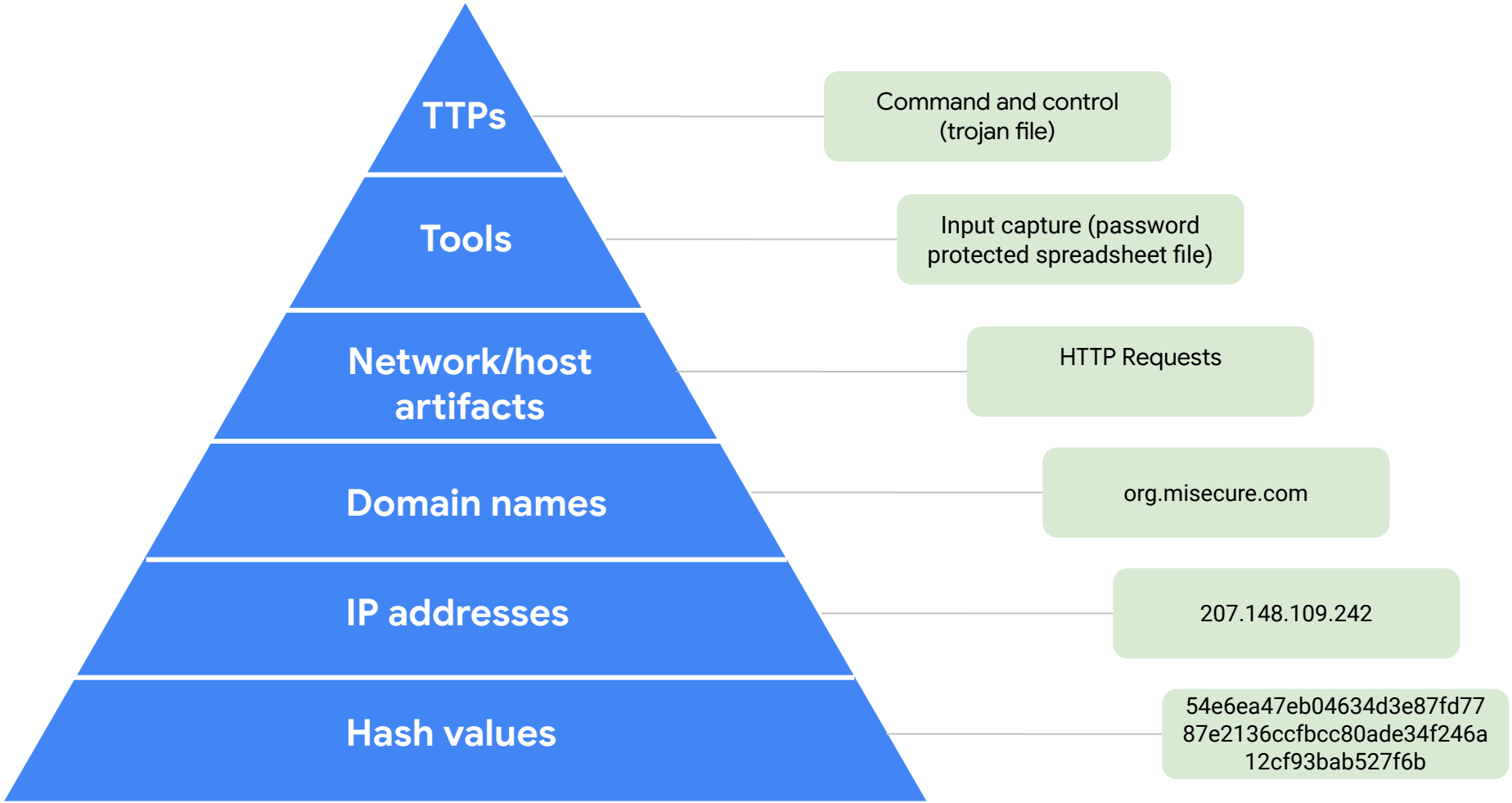
Has this file been identified as malicious? Explain why or why not.

Yes, this file has been identified as malicious.

The VirusTotal report provides strong evidence of the file's malicious nature, supported by several key findings:

1. **Vendor Detection Ratio**: The file was flagged by 58 out of 71 security vendors, a high detection rate that strongly indicates it is associated with known malware or malicious behaviors. When the majority of reputable security vendors identify a file as a threat, it is typically a reliable indication of its malicious intent.
2. **Community Score**: The community score is -217, which reflects a highly negative assessment from the VirusTotal user community. This score suggests that other analysts and users have encountered harmful activity related to this file and have flagged it accordingly.
3. **Detection Details**: In the **Detection** tab, multiple vendors listed specific malware signatures and behaviors linked to the file. This further supports the conclusion that the file contains harmful payloads or performs actions typically associated with malware, such as unauthorized file creation, data exfiltration, or system compromise.

Given these indicators—a high vendor detection ratio, a significantly negative community score, and specific malicious behaviors detected—the file is conclusively identified as malicious. Immediate action, such as quarantining the file and investigating any potentially impacted systems, is recommended to mitigate further risk.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Command and control (trojan file)
Input capture (password protected spreadsheet file)
HTTP Requests
org.misecure.com
207.148.109.242
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b