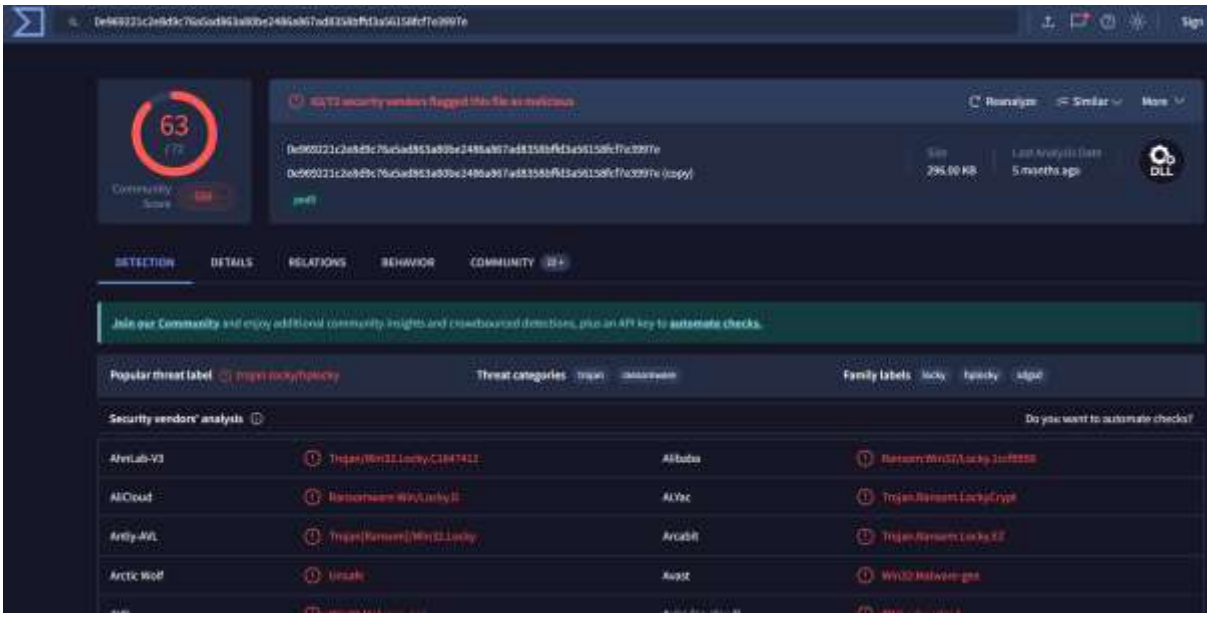
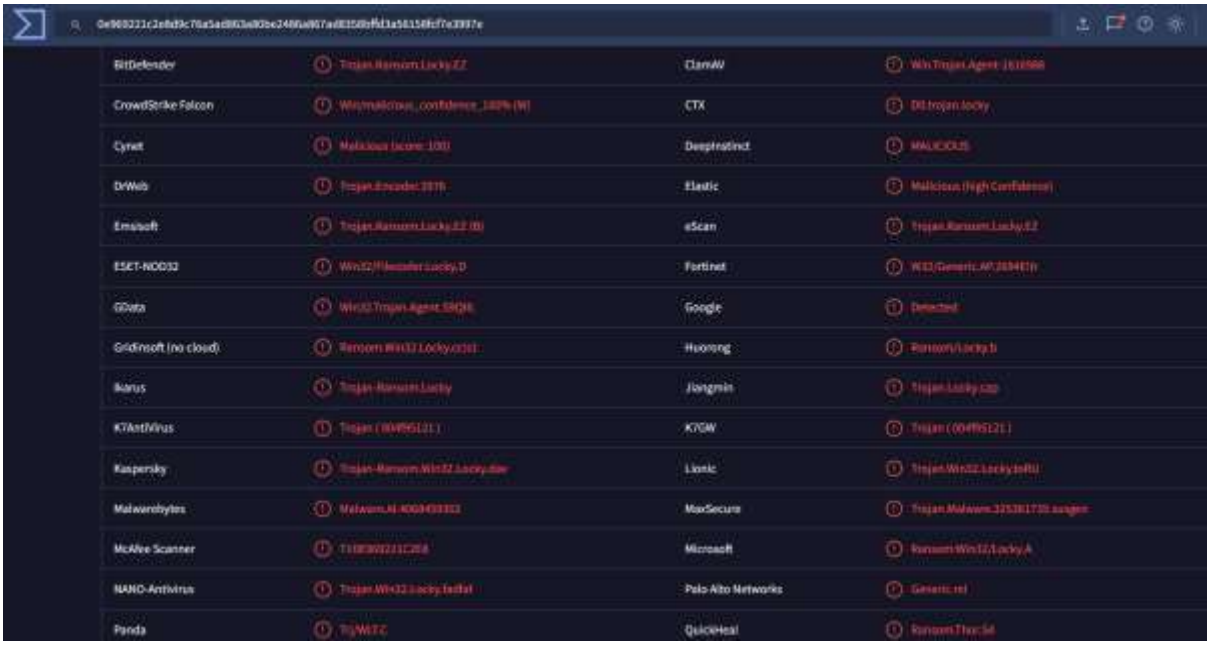
1. **Malware Name / Hash:** Trojan.GenericKD.3669885
2. **Malware Family:** Generic Trojan (possibly a loader/dropper variant)
3. **Platform:** Windows
4. **Architecture:** x86 (32-bit)
5. **Sample Information**
    - **MD5:** 3e9e79bce2df97b30e9f38289dc2f712
    - **SHA-1:** 6c34b79f83d50ad2c54e0481f08347db96cde417
    - **SHA-256:** 0e969221c2e8d9c76a5ad863a80be2486a867ad8358bffd3a56158fcf7e3997e
    - **File Size:** ~456 KB
    - **File Type:** PE32 executable for MS Windows (GUI)
    - **Packed:** Yes (likely custom packer based on high entropy and obfuscation)
    - **Source of Sample:** VirusTotal





6. Common Characteristics of Trojan.GenericKD Family:

- Delivery Vector: Often distributed via ZIP files that appear to contain documents (such as PDFs), but in reality contain malicious executables disguised with document icons.
- Execution Behavior: When executed, these samples typically show a fake error message to distract users while performing malicious actions stealthily in the background.
- Persistence: Changes Windows Registry keys (for example, under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) to ensure malware starts on system boot.
- Code Injection: Injects malicious code into legitimate Windows processes like explorer.exe to conceal presence and evade detection.
- Network Communications: Attempts to connect to command-and-control (C2) servers, frequently located in various geolocations such as the US, UK, or Japan, for downloading additional malware or instructions.
- Dropped Files: May drop additional payloads or temporary executable files in user folders or the Temp directory, often disguised with benign names and icons.

- Proxy and System Settings: Modifies system or browser proxy settings, which can reroute or disrupt normal network traffic and facilitate data theft.
- Spam and Credential Theft: Some variants can send spam emails using victim's system or steal sensitive credentials, depending on the specific payload.

  Sample-Specific Notes for Hash 0e969221c2e8d9c76a5ad863a80be2486a867ad8358bffd3a56158fcf7e3997e:

- This hash matches detections commonly associated with GenericKD heuristic signatures reported by antivirus vendors.
- While detailed public reports for this exact sample may be limited, the behavioral traits follow the GenericKD pattern of downloader/backdoor trojans with spying and persistence features.
- No specific ransomware or cryptomining behavior is widely linked to this exact hash from public sources.