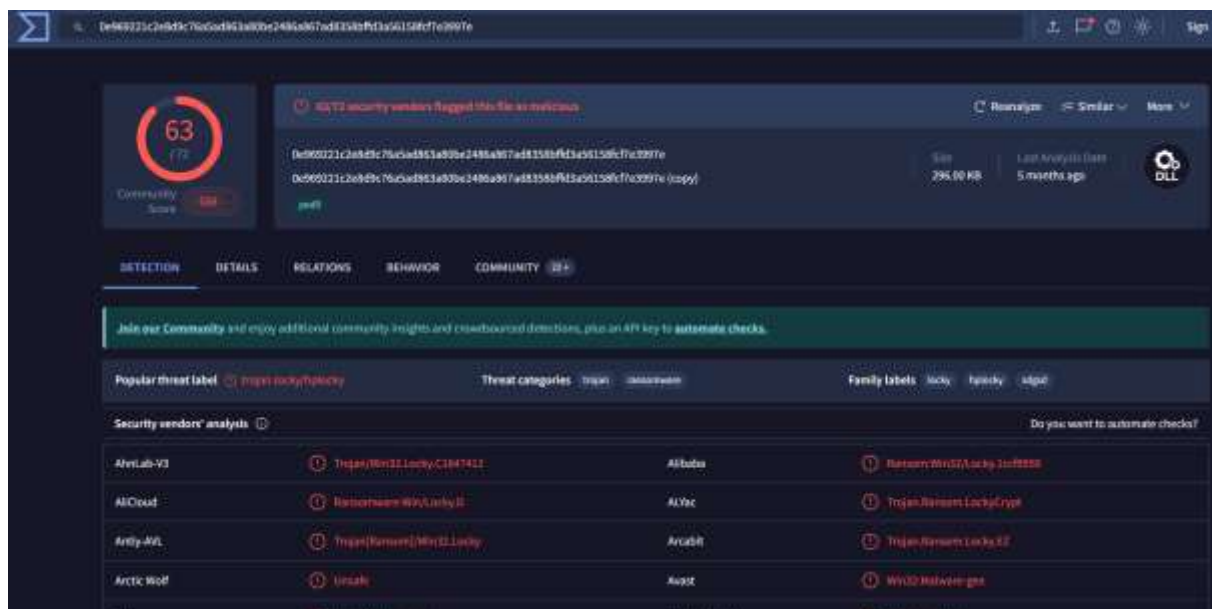


1. **Malware Name / Hash:** Trojan.GenericKD.3669885
2. **Malware Family:** Generic Trojan (possibly a loader/dropper variant)
3. **Platform:** Windows
4. **Architecture:** x86 (32-bit)
5. **Sample Information**
  - **MD5:** 3e9e79bce2df97b30e9f38289dc2f712
  - **SHA-1:** 6c34b79f83d50ad2c54e0481f08347db96cde417
  - **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



Vendor	Detection Name
BitDefender	Trojan.Ransom.Locky.EZ
CrowdStrike Falcon	Win/Malicious_confidence_100% (W)
Cyren	Malicious (score:100)
DrWeb	Trojan.GenericKD.3376
Emisoft	Trojan.Ransom.Locky.EZ (B)
ESET-NOD32	Win32/Hackbot.locky.D
GData	Win32.Trojan.Agent.5826
Gridinsoft (no cloud)	Ransom.Win32.Locky.cd31
Ikarus	Trojan.Ransom.Locky
ITAntivirus	Trojan (00495121)
Kaspersky	Trojan-Ransom.Win32.Locky.daw
Malwarebytes	Malware.M-KOD-493323
McAfee Scanner	T1187002112268
NANO-Antivirus	Trojan.Win32.locky.lockal
Panda	Trojan.Locky
ClamAV	Win.Trojan.Agent.161866
CTX	Detected
DeepInfect	Malicious
Elastic	Malicious (High Confidence)
eScan	Trojan.Ransom.Locky.EZ
Fortinet	W32/Generic.MP334476
Google	Detected
Huorong	Ransom.Locky.b
Jiangmin	Trojan.Locky.cd
K7GW	Trojan (00495121)
Look	Trojan.Win32.locky.lockal
MaxSecure	Trojan.Malware.225381720.sageon
Microsoft	Ransom.Win32.Locky.A
Palo Alto Networks	Generic.m
QuickHeal	Ransom.Trojan

## 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.