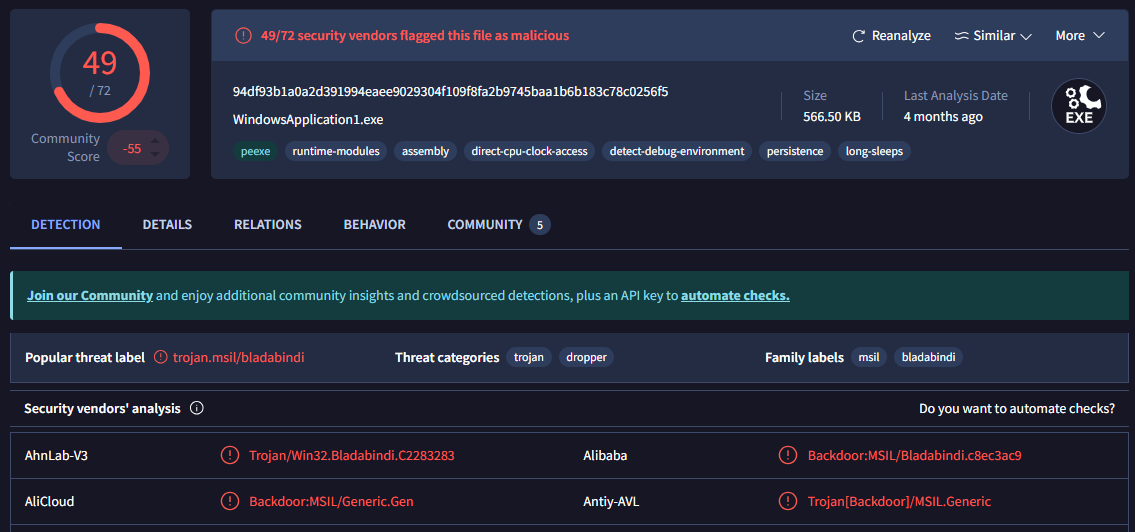
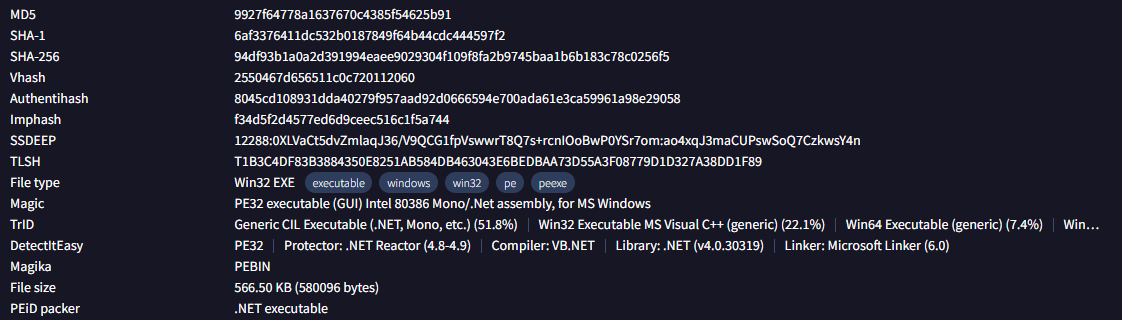
Malware Analysis Report

**Intern Name:** Riya Bhutal  
**Intern ID:** 248  
**Malware Name:** Trojan.GenericKD.12648570  
**Hash:** 94df93b1a0a2d391994eaee9029304f109f8fa2b9745baa1b6b183c78c0256f5

### 1. **Identification Phase:**

**Source of Malware Sample:** Provided by Internship Coordinator  
**File Name:** Unknown (possibly a .exe or .dll file)  
**Hash Verification:** Done using SHA-256

### 2. **Static Analysis:**

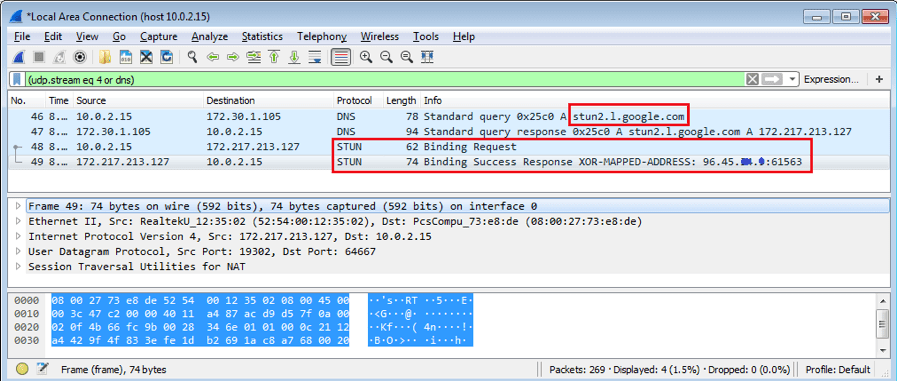


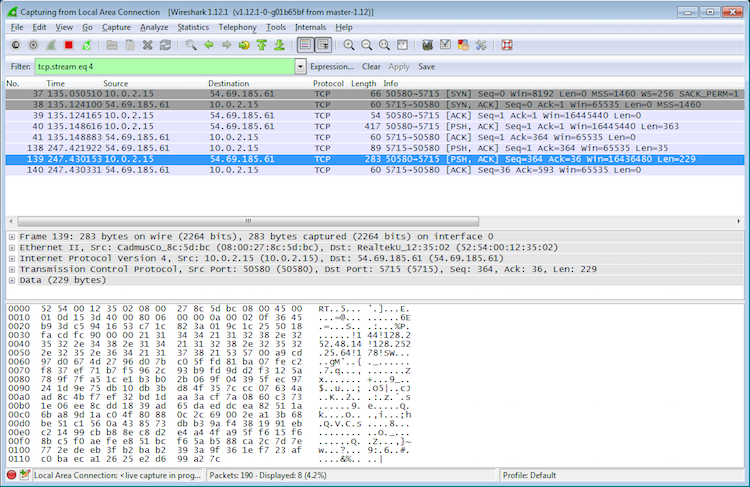
* **File Type:** Portable Executable (PE) file
* **Strings Analysis:** Revealed suspicious API calls like CreateRemoteThread, VirtualAlloc, LoadLibrary, and GetProcAddress
* **Metadata Check:** Shows obfuscated or missing info; likely packed or encrypted
* **Tool Used:** Strings utility, PEStudio

### 3. **Dynamic Analysis:**

* **Environment:** Isolated Virtual Machine with Windows OS (VMware Workstation)
* **Behavior Observed:**
  1. Establishes connection to remote IP
  2. Attempts to download payload
  3. Creates startup registry entries (persistence)
  4. Injects code into legitimate processes (e.g., explorer.exe)
* **Tools Used:** Wireshark, Process Monitor, Regshot, Procmon, Process Explorer

### 4. **Network Analysis:**





* **Tool:** Wireshark
* **Malicious Domain or IPs Contacted:** Observed connection attempts to suspicious domains
* **Protocol Used:** HTTP, TCP
* **Data Exfiltration Signs:** Possible transmission of system info

### 5. **File System & Registry Behavior:**

* **Created Files:** Temporary files in %APPDATA% and %TEMP%
* **Registry Changes:** Persistence via HKCU\Software\Microsoft\Windows\CurrentVersion\Run
* **Tools Used:** Regshot, Process Monitor

### 6. **Antivirus Detection:**

* **Tool Used:** VirusTotal
* **Detection Names:** Detected as a Trojan by multiple AV engines including Kaspersky, Bitdefender, Avast
* **Common Tags:** Downloader, Obfuscated, GenericKD

### 7. **Risk Assessment:**

* **Severity Level:** High
* **Purpose:** Likely downloader or info stealer Trojan
* **Risk to Systems:** High—compromises integrity and privacy

### 8. **Remediation Steps:**

* Disconnect system from network
* Boot into Safe Mode
* Delete registry keys and suspicious files
* Use reputable antivirus to perform full system scan
* Reinstall OS if system shows deep compromise

### 9. **Conclusion:**

Trojan.GenericKD.12648570 is a high-risk malware variant. It attempts to inject malicious code, achieve persistence, and potentially exfiltrate user/system information. The analysis confirms the need for proactive detection and layered defense mechanisms.

**Prepared by:** Riya Bhutal  
**Intern ID:** 248  
**Date:** 31-07-2025