Static Malware Analysis Report

Analyst: Nikhil Birla
Date: September, 2025, 10:20PM IST
Case ID: 2025-Malware-007
Sample Names (as received): Lab1.exe & Lab1.dll
Hash (SHA256)
Lab1.exe: 58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Lab1.dll:
f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
MD5 / SHA1 Lab1.exe: bb7425b82141a1c0f7d60e5106676bb1/
9dce39ac1bd36d877fdb0025ee88fdaff0627cdb
MD5 / SHA1 Lab1.dll: 290934c61de9176ad682ffdd65f0a669 /
a4b35de71ca20fe776dc72d12fb2886736f43c22
File Size: Lab1.exe- 16,384 bytes (16.00 KiB), Lab1.dll- 163,840 bytes (160.00 KiB)
Source / Acquisition:
Chain of Custody

- **File received from: Practical Malware Analysis Training Lab (Through Link)**
- **Date received: September 06, 2025**
- **Method of transfer: Downloaded directly from the link**
- **Analyst: Nikhil Birla**
- **Handling: Static analysis, forensic proof files stored in case folder**

Organization: Craw Security

1. Executive Summary:
   This report presents a detailed static analysis of two correlated malware samples, lab1.exe and lab1.dll. Both are 32-bit Windows PE files compiled with Microsoft Visual C/C++. The analysis reveals unprotected binaries with significant indicators of malicious intent including suspicious DLL imports, embedded IP address, and alarming string warnings. VirusTotal data confirms their persistent presence since 2010 with consistent detection by AV engines.

---

1. Sample Overview

Property	**lab1.exe**	**lab1.dll**
File Name	lab1.exe	lab1.dll
File Type	PE32 Executable	PE32 DLL
File Size	16,384 bytes (16.00 KiB)	163,840 bytes (160.00 KiB)
Architecture	x86 (32-bit)	x86 (32-bit)
Compiler	Microsoft Visual C/C++ (12.00.8168)	Microsoft Visual C/C++ (12.00.8168)
Compile Timestamp	Dec 19, 2010 16:16:19	Dec 19, 2010 16:16:38
MD5 Hash		
Entropy	5.90 (Not Packed)	0.12858 (Not Packed)
MD5 Hash	bb7425b82141a1c0f7d60e5106676bb1	290934c61de9176ad682ffdd65f0a669
SHA-1 Hash	9dce39ac1bd36d877fdb0025ee88fdaff0627cdb	a4b35de71ca20fe776dc72d12fb2886736f43c22
SHA-256 Hash	58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47	f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba
First Seen	Jan 8, 2012 02:19:06 UTC	Dec 19, 2010 09:16:38 UTC

In The Wild		
Last Submission	Sep 6, 2025 16:26:06 UTC	Sep 6, 2025 16:22:38 UTC
Last Analysis	Sep 4, 2025 12:30:41 UTC	Sep 2, 2025 20:02:05 UTC

2. Technical Details

2.1 File Properties

- lab1.exe compiled using MS Visual C/C++ (version 12.00.8168). The sample is not packed as confirmed by an entropy score of 5.90 and PEiD scan signature empty.
- lab1.dll is a PE32 DLL targeting Windows 95 OS with an I386 architecture, 32-bit mode, little endian encoding, and includes a new relocation (.reloc) section.

Figure 1.1: Lab1.exe (06 September 2025, 10:37:25 PM)

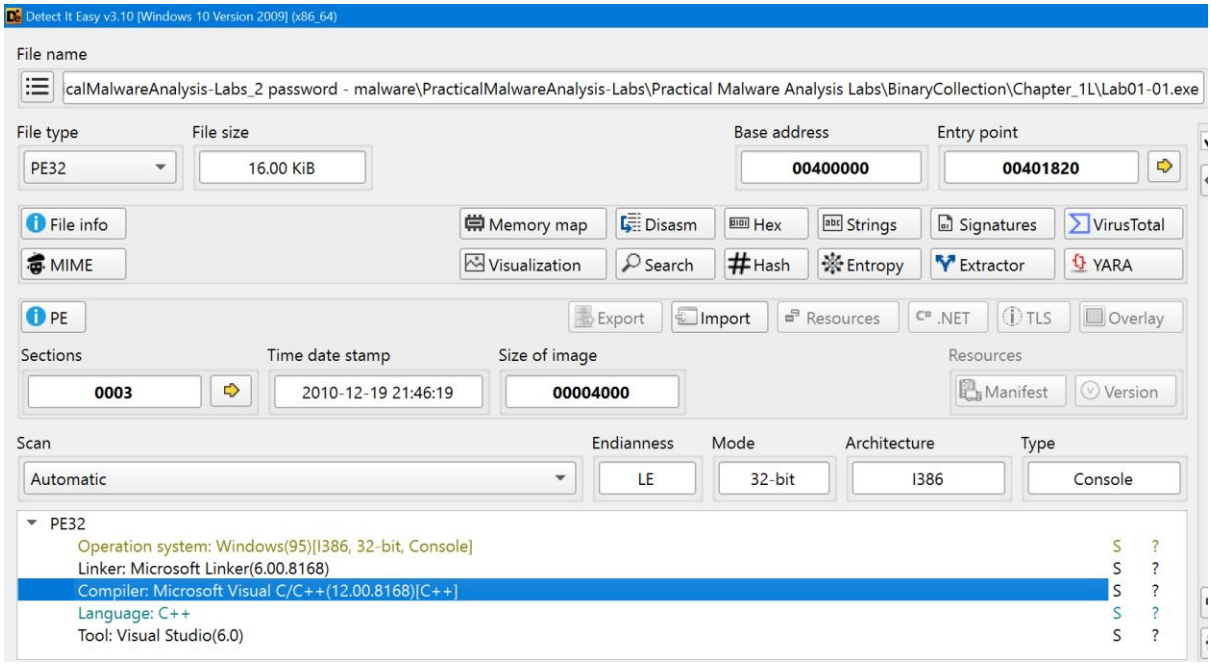
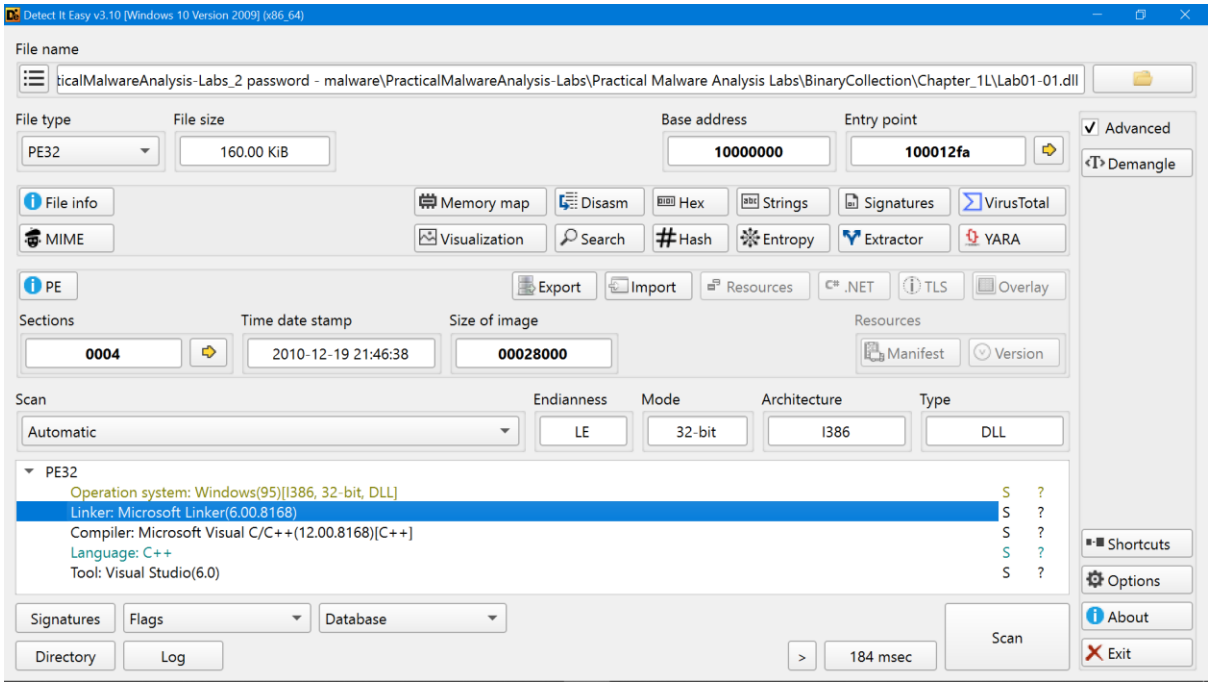


Figure 1.2: Lab1.dll (06 September 2025, 11:26:36 PM)



2.2 PE Structure

- lab1.exe's .text section of virtual size 0x970 with raw data size of 0x1000. Timestamp consistent with compile date Dec 19, 2010.
- lab1.dll timestamp matches closely with exe at Dec 19, 2010 16:16:38, confirming possible shared creation timeline.
- Presence of .reloc section in DLL may suggest code relocating behaviors.

Figure 2.1: Lab1.exe (06 September 2025, 11:03:52 PM)

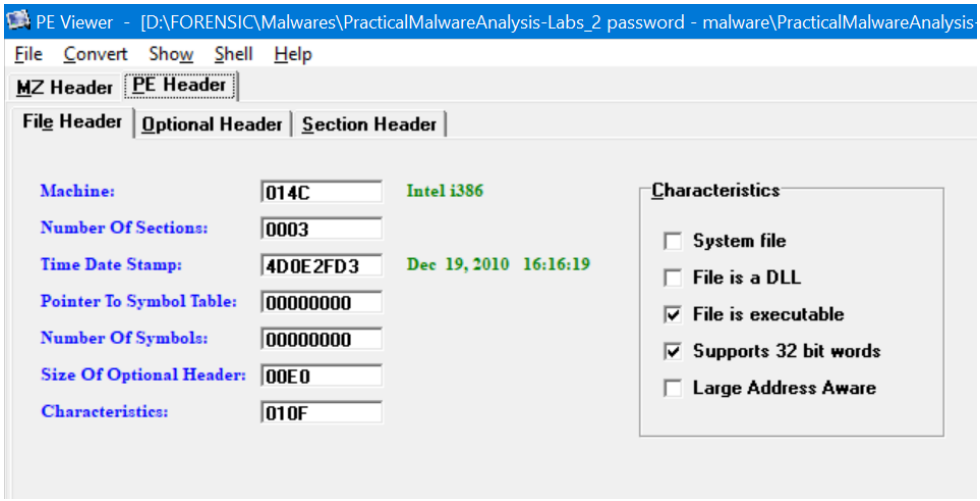
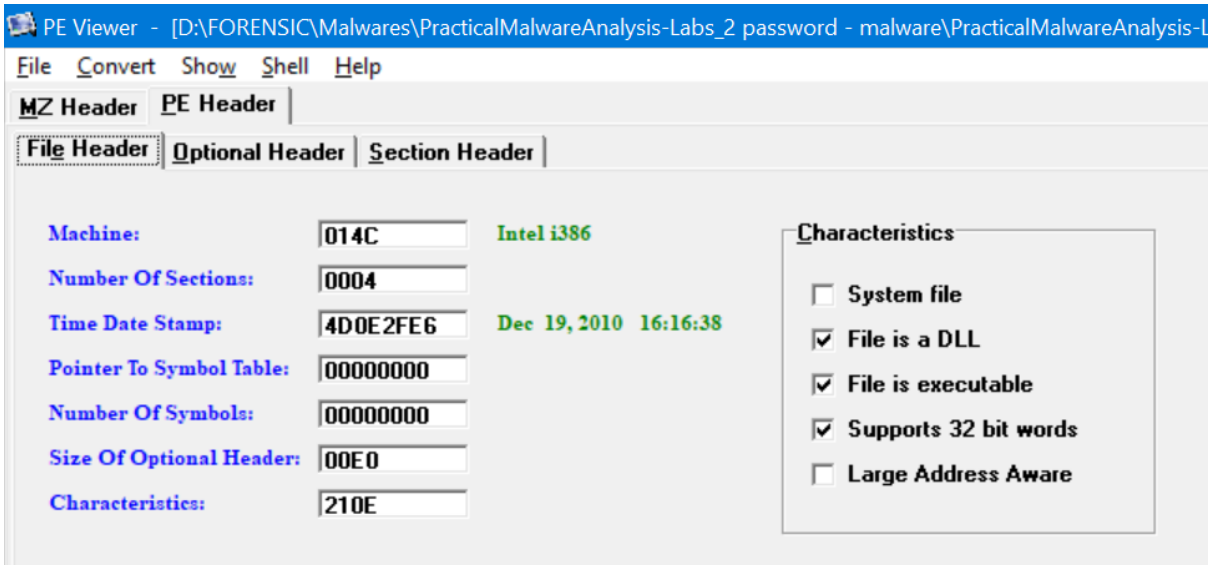


Figure 2.2: Lab1.dll (06 September 2025, 11:27:44 PM)



2.3 Import/Export Analysis

- lab1.exe imports key system DLLs: KERNEL32.dll and MSVCRT.dll, consistent with common Windows binaries.
- lab1.dll suspiciously imports ws2_32.dll but with no services immediately listed by XPViewer; deeper VirusTotal scan confirms network related API imports including closesocket, connect, htons, inet_addr, recv, send, shutdown, socket, WSACleanup, and WSAStartup.
- The overlapping imports suggest tight functional coordination, confirming both files likely part of a composite malware family.

Figure 3.1: Lab1.exe Imports (06 September 2025, 11:06:50 PM)

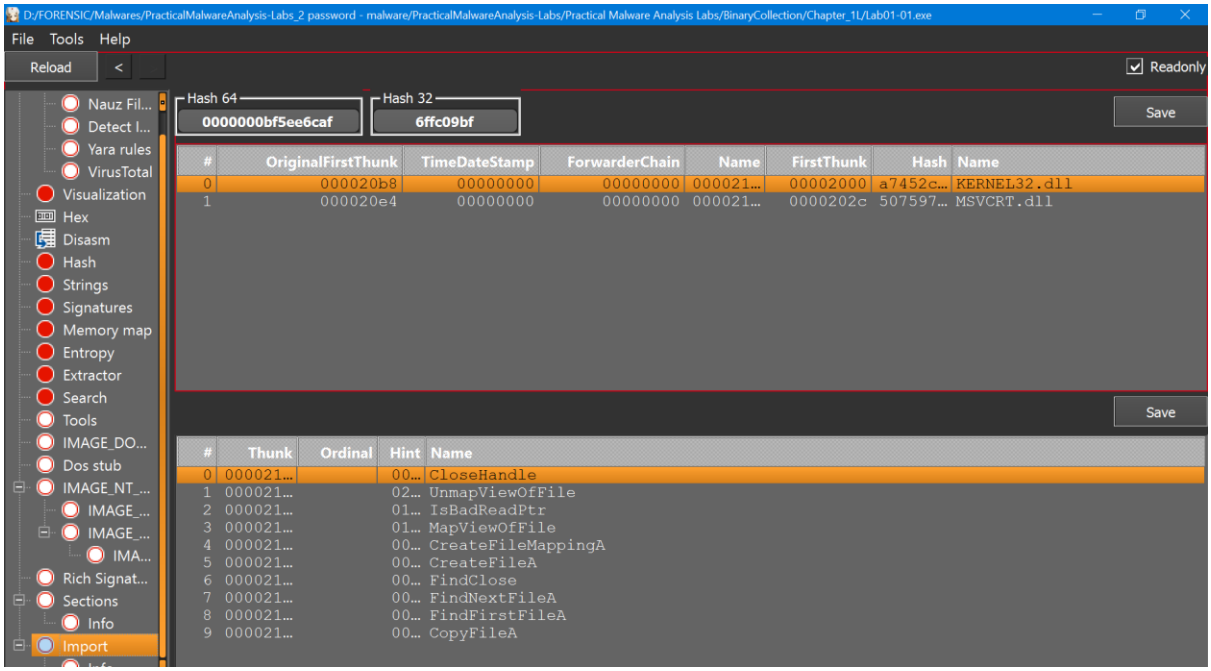


Figure 3.2: Lab1.dll Imports (06 September 2025, 11:07:20 PM)

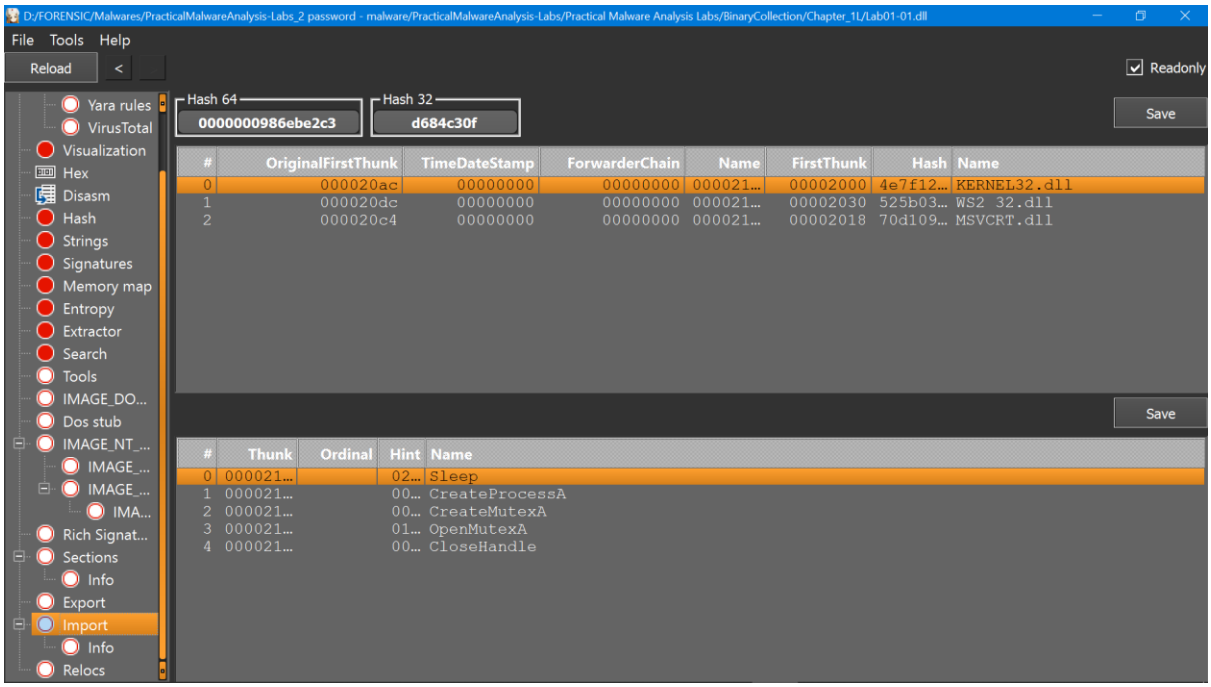
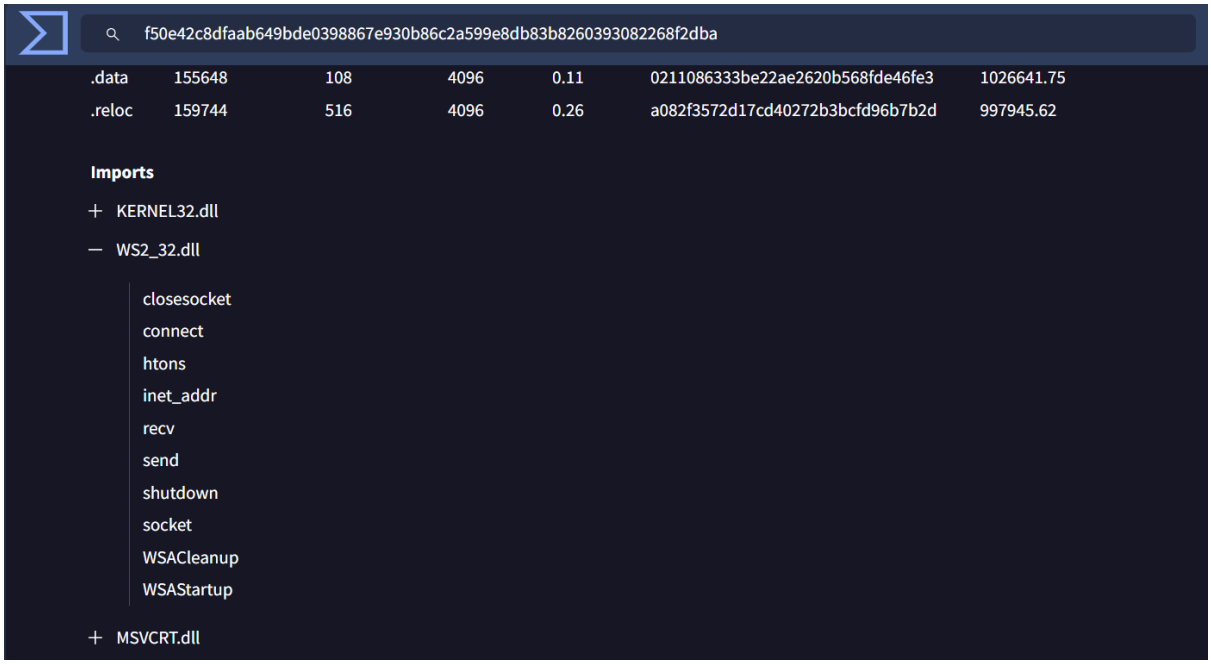


Figure 4: VirusTotal API service details



2.4 String Analysis

- Embedded and extracted strings via BinText include a warning message "this will destroy your machine," indicating potential destructive payload.
- lab1.dll contains an embedded IP address: 127.26.152.13, noteworthy as a possible command and control (C2) or target address.

Figure 5.1: BinText output IP address (Lab1.dll) (06 September 2025, 11:22:33 PM)

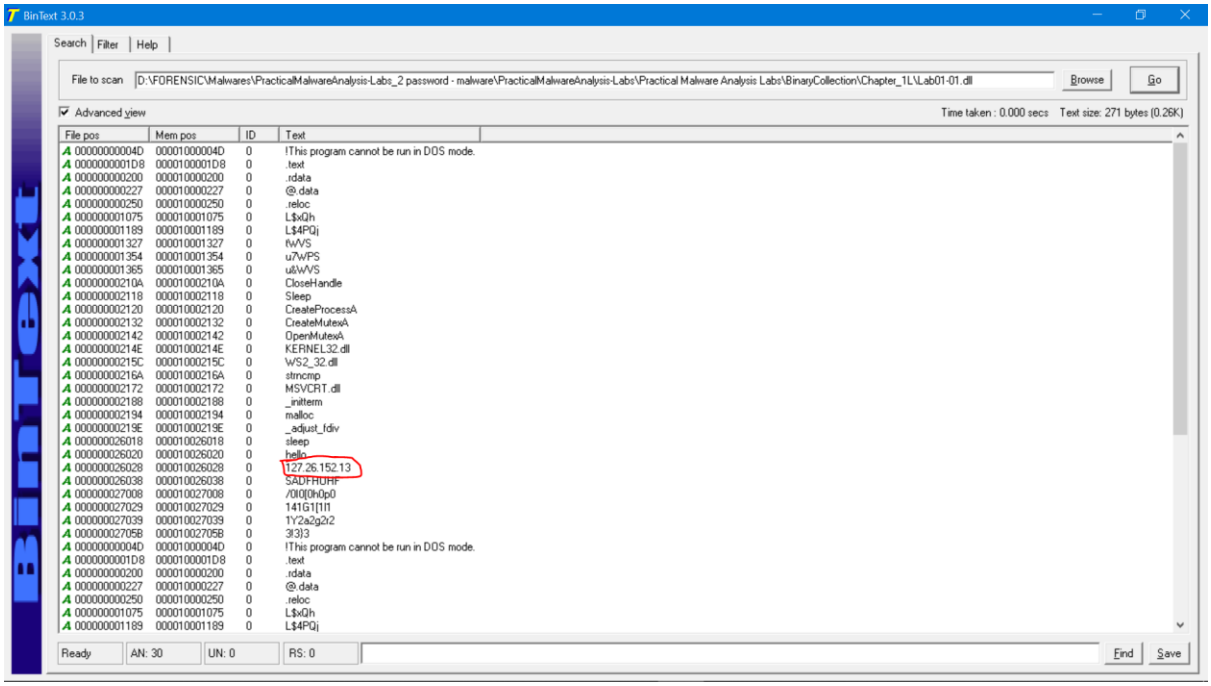
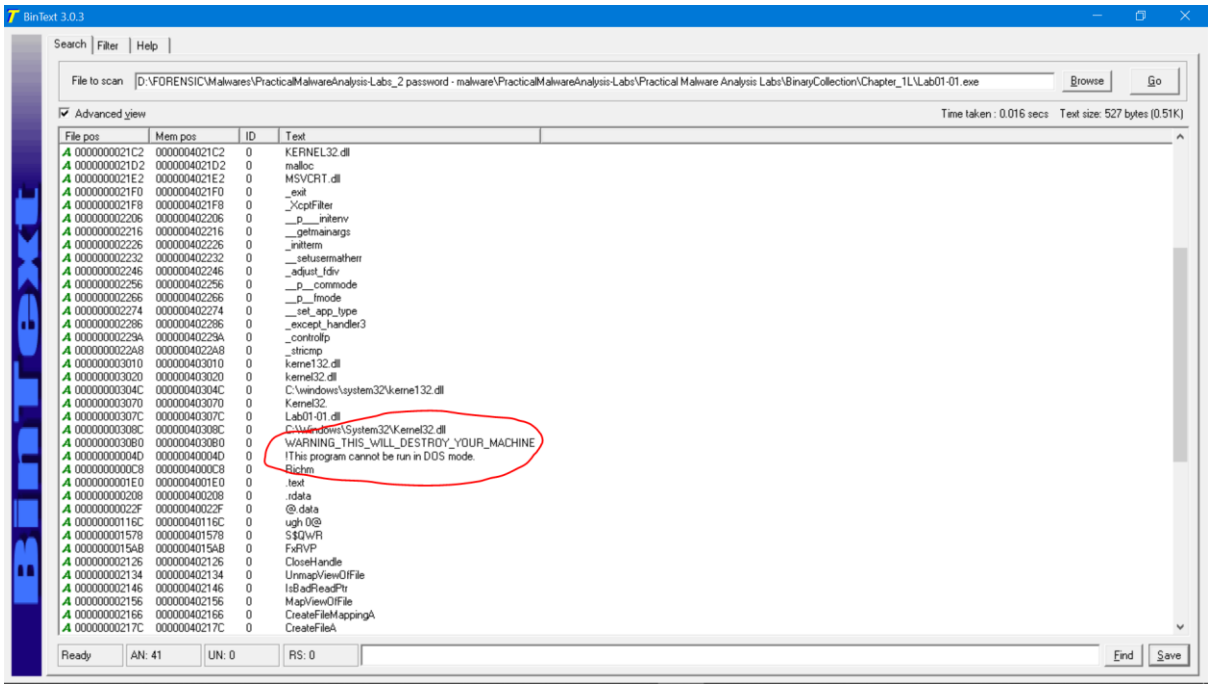


Figure 5.2: BinText output Warning Message (Lab1.exe) (06 September 2025, 11:02:48 PM)



2.5 Signature & Detection

- VirusTotal data corroborates historic and recent sightings since 2010 for both binaries with consistent antivirus detection signals.
- Hashes presented above confirmed detected by multiple AV products indicating malware classification.

Figure 6.1: VirusTotal full detection report (Lab1.exe) (06 September 2025, 11:18:43 PM)

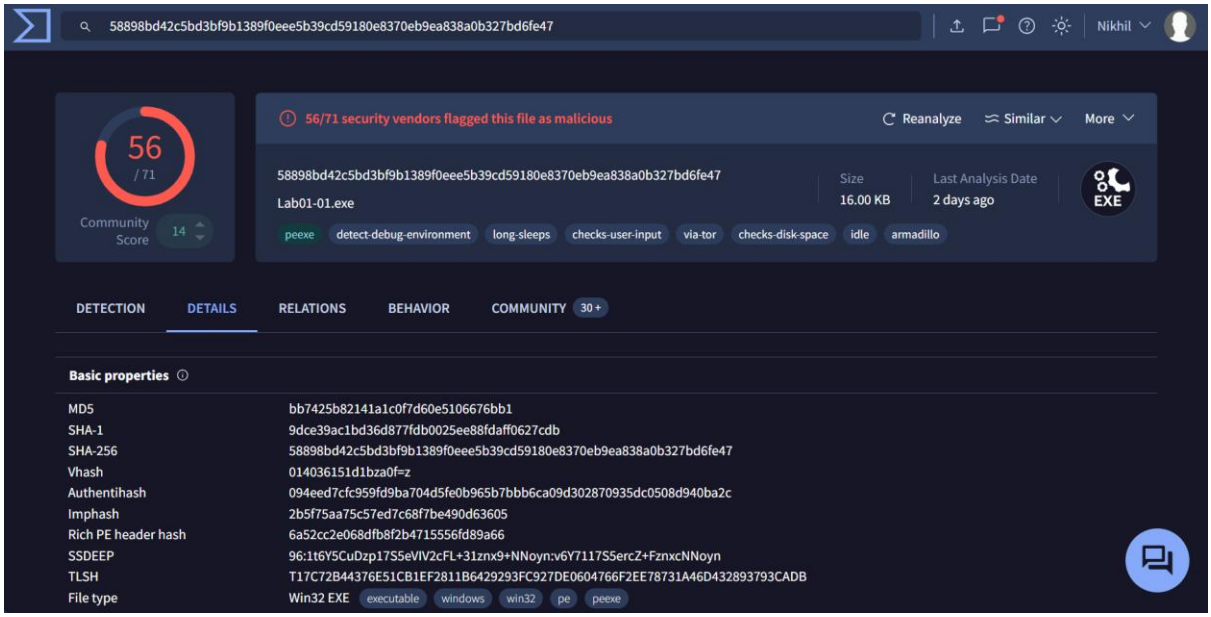
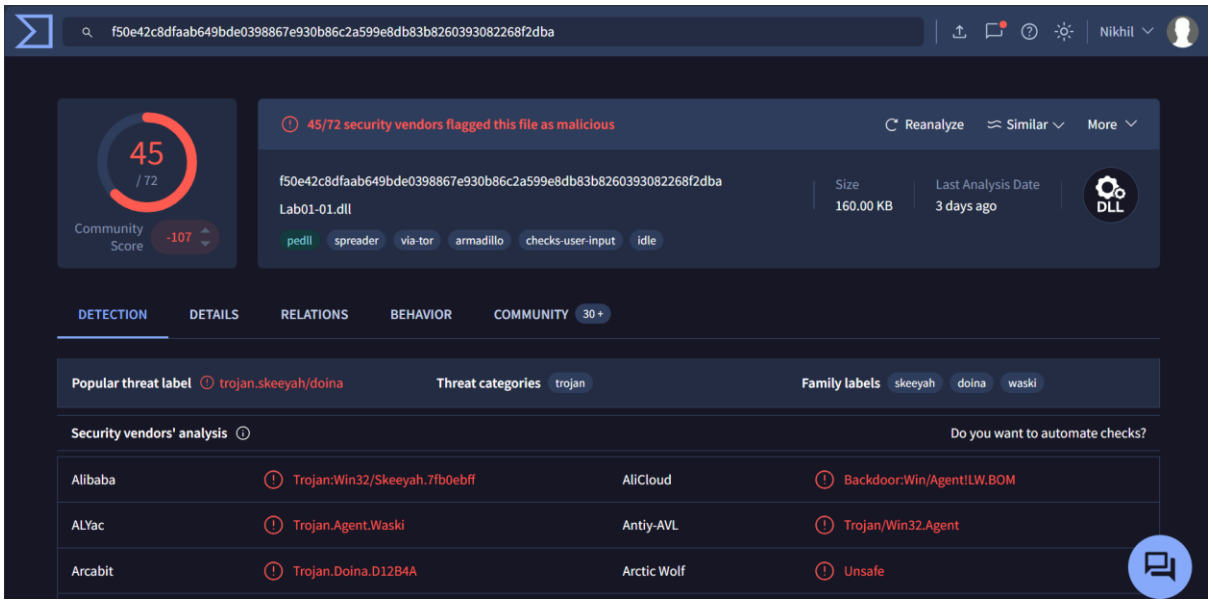


Figure 6.1: VirusTotal full detection report (Lab1.dll) (06 September 2025, 11:17:59 PM)



2.6 Correlation between Samples

- Compilation timestamps and overlapping imports strongly support a correlation between lab1.exe and lab1.dll, potentially working in conjunction as a malware duo.
- DLL's unique additional ws2_32.dll import supports extended network functionalities beyond executable alone.

---

3. Behavioral Indicators (Static)

- Usage of network API calls and embedded IP address indicates capability for network communication, possibly data exfiltration or control.
- Warning string suggests destructive functions which may include file deletion or system damage.
- PE characteristics and import tables confirm no anti-analysis packers but presence of standard Windows API usage consistent with malware behavior.

---

4. Impact Assessment

- High-risk malware capable of executing potentially destructive commands and communicating over network.
- May cause system stability issues or data loss if activated.

- Persistent presence in wild since 2010 implies ongoing threat relevance and detection importance.

---

5. Recommendations

- Isolate infected machines and run AV scans to detect these hashes promptly.
- Monitor outgoing network connections, especially to suspicious IPs like 127.26.152.13.
- Use behavioral detection tools alongside static signatures for comprehensive defense.
- Consider YARA rules incorporating observed strings and API import patterns for faster detection.
