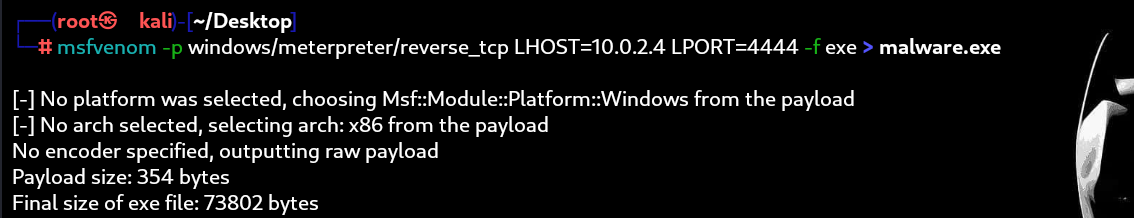
**Malware Analysis (Static and Dynamic)**

**Task(2)**

***Written by Vusal Isayev***

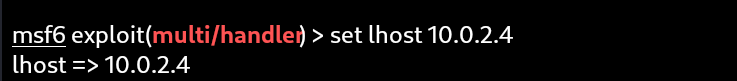
**1. Introduction** This report documents the process of creating and testing a Meterpreter payload for Windows using Metasploit. The objective is to generate a reverse TCP shell payload, configure a listener, and successfully establish a connection between the target and the attacking machine.

**2. Payload Creation** The payload was created using msfvenom with the following command:



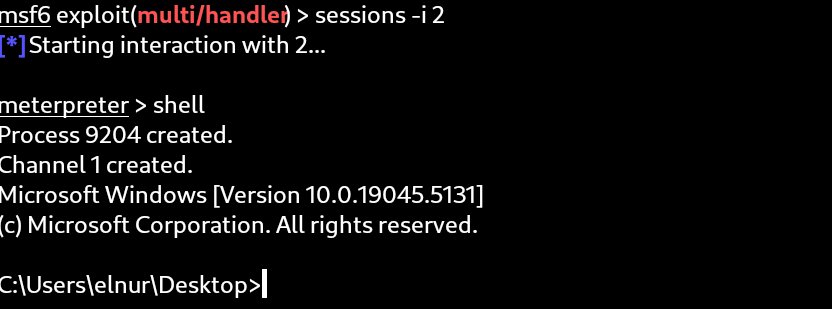
**3. Listener Setup** To receive the reverse shell connection, Metasploit’s multi/handler exploit module was configured as follows:





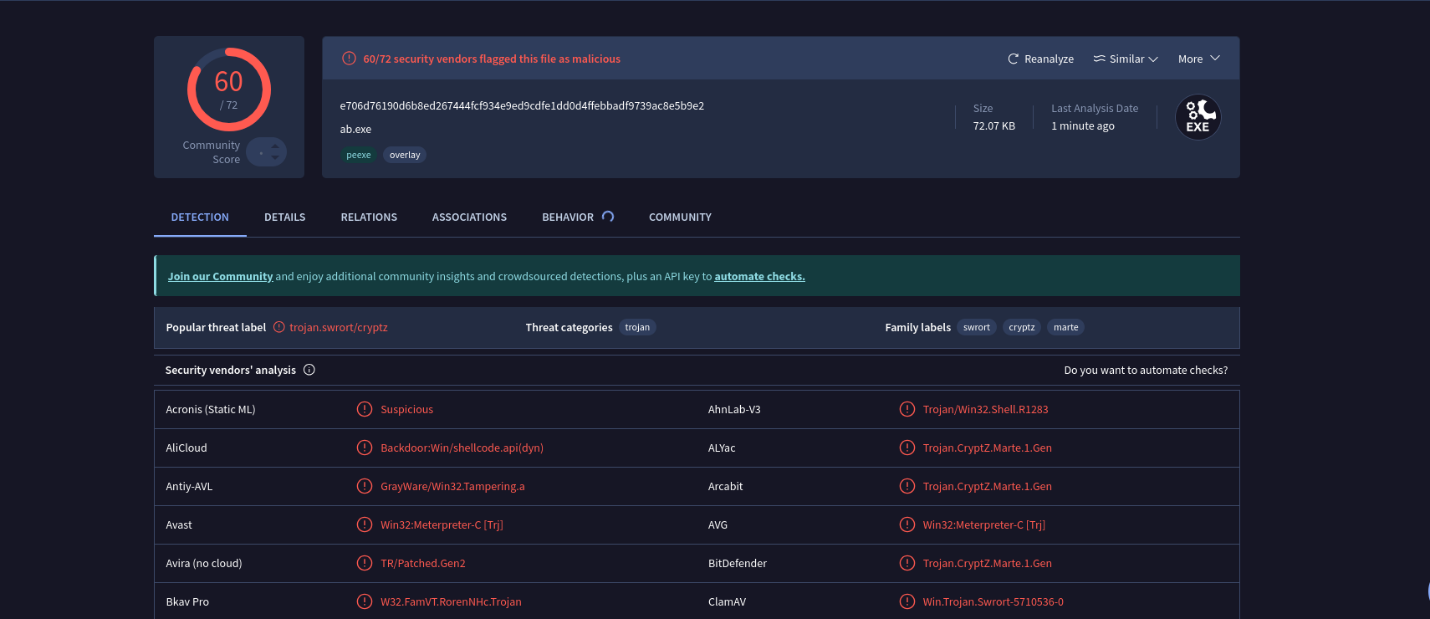
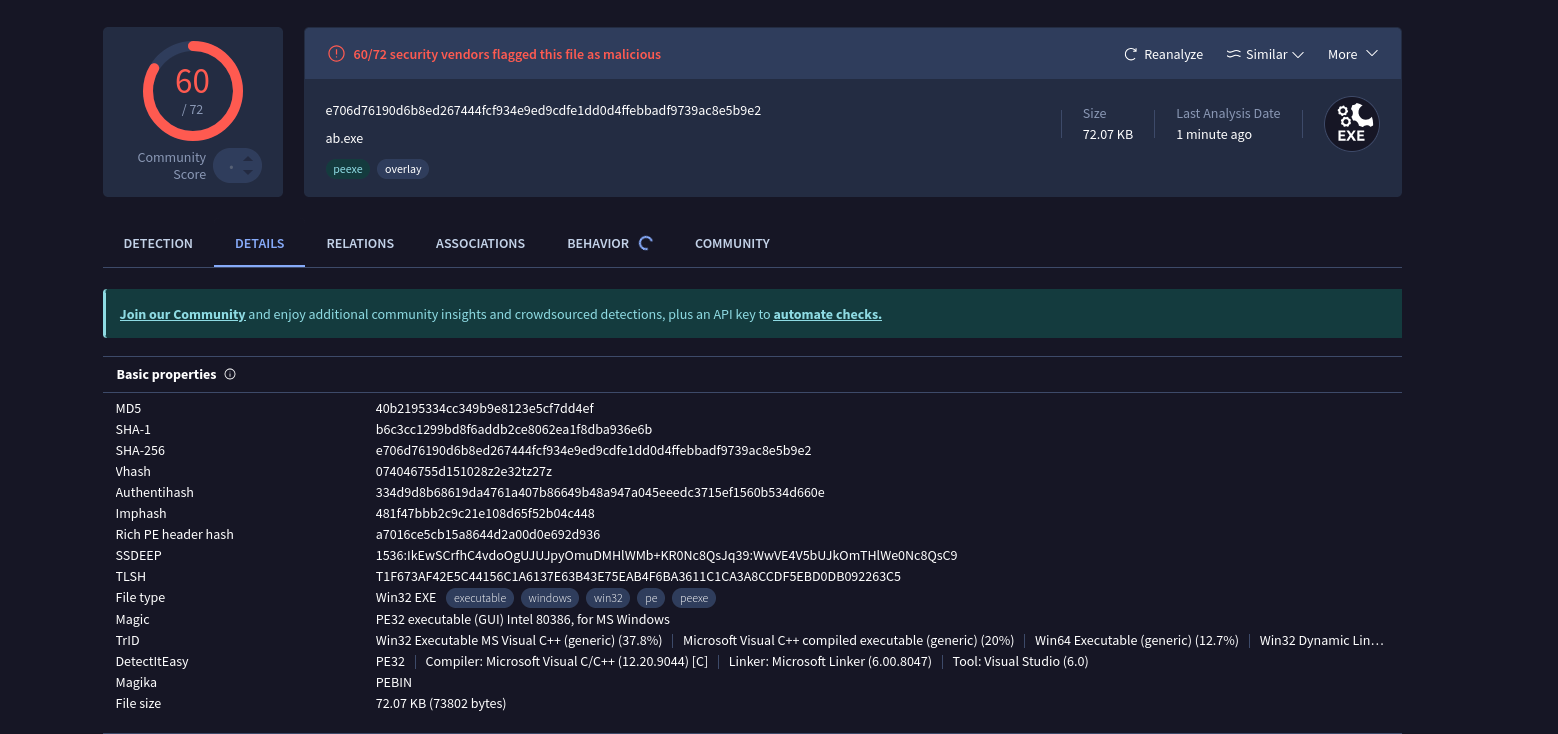
Now, after placing our malware file on the target machine, the shell will come to us automatically:



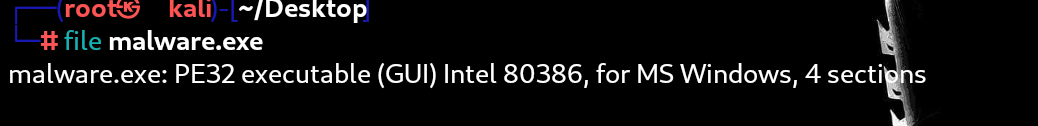


**Static analyze:**

I used **virustotal** for static analysis in the first turn:



After, I used ‘**file**’ command in my linux machine:



**Malware Analysis Report: ab.exe**

Overview

The file ab.exe was analyzed using VirusTotal, where 60 out of 72 security vendors flagged it as malicious. The analysis categorizes the file as a Trojan with labels such as trojan.swort/cryptz and Backdoor.Win/shellcode. The detection indicates that the file likely contains a backdoor, shellcode execution, and potential evasion mechanisms.

---

File Details

SHA-256: e706d76190d6bed267444fcf93e9ed9cfde1dd0d4ffebbafd9739ac8e5b9e2

MD5: 40b2195334cc349b9e8123e5cf7dd4ef

SHA-1: b6c3cc1299b8df6adb2ce8062a1fbdba936e6b

File Type: Win32 Executable (PE)

File Size: 72.07 KB (73802 bytes)

Compilation Tool: Microsoft Visual C++ (12.0.9044)

Detection Rate: 60/72

---

Threat Classification

Malware Type: Trojan, Backdoor

Common Labels by Security Vendors:

Backdoor.Win/shellcode.api(dyn)

Trojan.CryptZ.Marte.1.Gen

Win32:Meterpreter-C [Trj]

Win.Trojan.Swort-5710536-0

TR/Patched.Gen2

The presence of Meterpreter and shellcode-related signatures suggests that this file is likely designed for remote access and post-exploitation activities.

---

Behavioral Indicators

Key Observations:

Packed Executable: The presence of an overlay suggests possible packing or obfuscation.

Possible Shellcode Execution: Several detections refer to shellcode.api(dyn), indicating potential shellcode execution for evasion or privilege escalation.

Backdoor Functionality: Labels such as Win32:Meterpreter-C [Trj] and Backdoor.Win/shellcode.api(dyn) suggest that the executable may allow remote access/control.

---

Potential Impact

Unauthorized Remote Access: If executed, the file could establish a backdoor, allowing attackers to control the system remotely.

Data Exfiltration: Given its classification as a trojan, it could be used to steal sensitive information from the infected system.

Privilege Escalation & Evasion: The malware might deploy shellcode or inject itself into legitimate processes to avoid detection.

Recommended Actions

1. Isolate the Infected System: Prevent further compromise by disconnecting the affected machine from the network.

2. Conduct Static & Dynamic Analysis: Further analyze the malware in a controlled sandbox to observe its behavior.

3. Check for Persistence Mechanisms: Look for registry modifications, scheduled tasks, or startup entries related to ab.exe.

4. Remove the Malware: Use a trusted antivirus or manual removal by deleting suspicious files and terminating processes.

5. Monitor Network Traffic: Check for suspicious outbound connections, as backdoors often communicate with C2 (Command & Control) servers.

6. Review System Logs & Artifacts: Analyze event logs for unusual activity or unauthorized access attempts.

---

Conclusion

The file ab.exe is confirmed to be malicious based on the high detection rate and presence of Meterpreter, shellcode execution, and backdoor functionalities. It poses a severe threat, and immediate action should be taken to contain and analyze the malware further.

**Dynamic analyze:**

## **1. Overview**

The file malware(1).exe was executed in a controlled environment to observe its behavior. The analysis identified network connections, process interactions, and suspicious string patterns, indicating potential malicious activity.

## **2. Process Analysis**

* The executable malware(1).exe was running as a child process under cmd.exe, which is an indicator of potential command execution abuse.
* The parent process of cmd.exe was the analyzed malware, which suggests it may be executing system commands.
* conhost.exe was also running in relation to cmd.exe, which is commonly seen when command-line operations are being performed.

## **3. Strings Analysis**

* The malware contains standard headers, including .text, .rdata, .data, and .rsrc, which indicate it is a compiled binary.
* A notable string found is **"This program cannot be run in DOS mode."** which suggests it is a Windows PE (Portable Executable) file.
* Additional obfuscated strings, such as **random character sequences**, could indicate encryption or anti-analysis techniques.

## **4. Network Activity**

* The malware established a **TCP connection to 10.0.2.4:4444**.
* The connection is in an **ESTABLISHED** state, suggesting active communication with a remote host.
* Port **4444** is commonly used for reverse shells, which is a strong indication of remote control functionality.

## **5. System Modifications & Execution Context**

* The malware was executed from C:\Users\elnur\Desktop\ under the user **ELBURUSUN\_KOMPU\elnur**.
* It utilized C:\Windows\SysWOW64\cmd.exe to execute system commands, indicating potential privilege escalation or persistence mechanisms.
* DEP (Data Execution Prevention) is enabled, but Stack Protection is disabled, which may expose vulnerabilities.

## **6. Suspicious Indicators**

* **Process Execution**: The malware spawns cmd.exe, which is a common method used by malicious software to execute commands.
* **Network Communication**: The established connection to an external IP on port 4444 suggests possible command-and-control (C2) activity.
* **Strings**: The presence of potentially encoded or obfuscated strings raises concerns about evasion techniques.

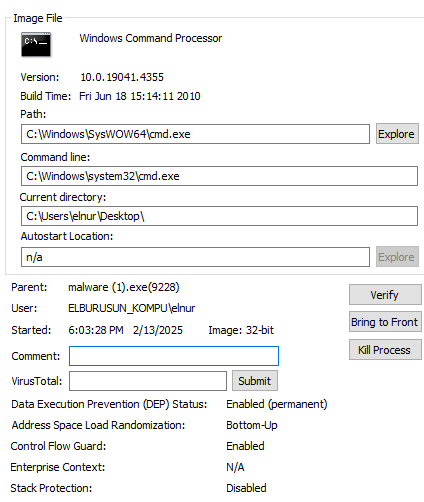
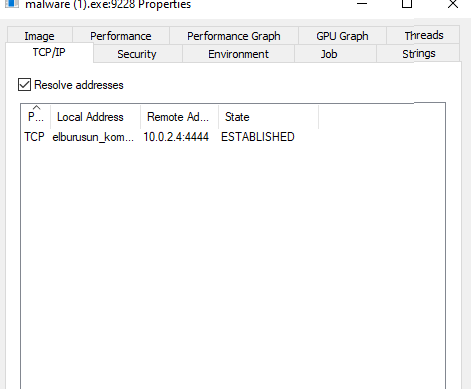
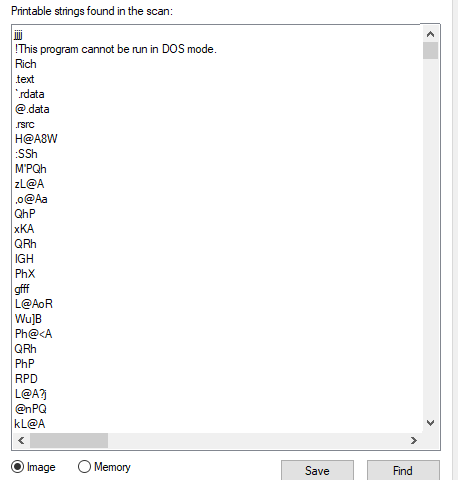
## **7. Conclusion & Recommendations**

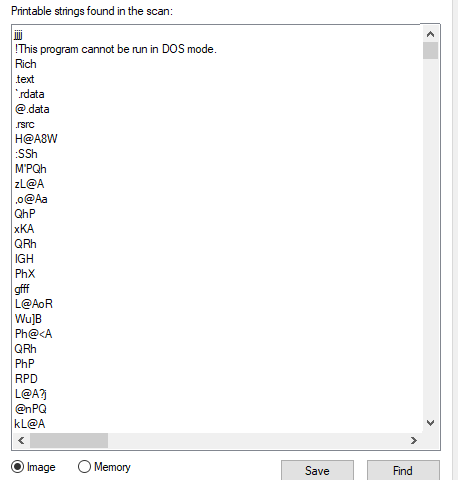
The observed behavior strongly suggests that malware(1).exe is a potentially harmful executable, likely associated with remote administration, command execution, or data exfiltration.

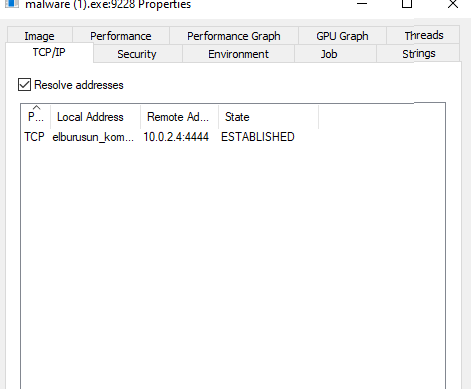
### **Recommendations:**

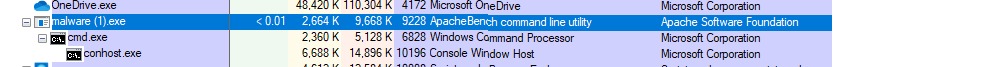
1. **Immediate Quarantine:** Remove or isolate the file from the system.
2. **Network Monitoring:** Block connections to **10.0.2.4** and monitor for additional suspicious outbound traffic.
3. **Forensic Analysis:** Investigate system logs to determine any additional compromise.
4. **System Scan:** Perform a full system scan with updated antivirus/endpoint security software.
5. **User Awareness:** Inform the user and restrict privileges if necessary.

This report provides initial findings. A deeper reverse engineering analysis may be required to determine the full capabilities of this malware.









## **1. Overview**

The analysis was conducted on an executable file named **malware (1).exe**. The sample was executed in a controlled environment, and its behavior was monitored using various analysis tools. The findings indicate potentially malicious activity, including network communication, process creation, and execution of system commands.

## **2. Process Behavior**

* **Parent Process:** malware (1).exe
* **Spawned Processes:**
  + cmd.exe (C:\Windows\System32\cmd.exe)
  + conhost.exe (Console Window Host)
* The malware executed the Windows Command Processor (cmd.exe), which is often indicative of command execution, potentially for malicious purposes such as downloading additional payloads or modifying system settings.
* **Autostart Behavior:** No direct evidence of persistence mechanisms was observed in the process properties.

## **3. Network Activity**

* **Observed Connection:**
  + **Local Address:** elburusun\_komp
  + **Remote Address:** 10.0.2.4:4444
  + **Protocol:** TCP
  + **State:** ESTABLISHED
* The malware established a network connection to 10.0.2.4 on port 4444, which is a commonly used port for reverse shells or remote access tools (RATs). This indicates potential remote control or exfiltration behavior.
* **HTTP Requests Observed:**
  + The malware made HTTP requests to 10.0.2.4, including a request for malware.exe.
  + Other HTTP traffic includes requests for favicon.ico and msdownload/update/v3/static/trustedr/en/authrootstl.cab, possibly to bypass security checks.
* **Packet Analysis (Wireshark Findings):**
  + The captured packets show GET requests to 10.0.2.4/malware.exe.
  + The user-agent string in the requests suggests the use of a common browser, potentially to masquerade as legitimate traffic.
  + Encapsulation via Ethernet and TCP indicates standard HTTP communication.

## **4. Strings Analysis**

* **Extracted Strings:**
  + "This program cannot be run in DOS mode" (Standard PE header indicator)
  + .text, .rdata, .data, .rsrc (Common PE sections)
  + Various unreadable characters, possibly obfuscated strings.
  + Potentially suspicious function calls or encoded data.
* **Potential Indicators:**
  + The presence of encrypted or encoded strings suggests that the malware may use obfuscation techniques to evade detection.

## **5. Indicators of Compromise (IoCs)**

* **Processes:**
  + malware (1).exe (Suspicious behavior, process spawning)
  + cmd.exe execution without user interaction
  + conhost.exe launched by malware (1).exe
* **Network:**
  + TCP connection to 10.0.2.4:4444
  + HTTP request to /malware.exe
  + Use of potentially deceptive user-agent strings
* **File Behavior:**
  + No observed file modification, but execution behavior suggests possible payload download.

## **6. Conclusion & Recommendations**

### **Conclusion:**

The analyzed executable (malware (1).exe) demonstrates behavior consistent with malware:

* Establishes a remote connection (10.0.2.4:4444), possibly for command-and-control (C2) communication.
* Makes HTTP requests for additional payloads (malware.exe).
* Executes system commands via cmd.exe.
* Contains obfuscated or encrypted strings, suggesting evasion techniques.

### **Recommendations:**

* **Immediate Actions:**
  + Block network traffic to 10.0.2.4:4444 and monitor for similar connections.
  + Terminate and remove the malicious process and any downloaded files.
  + Perform memory forensics to extract additional details about its execution.
* **Long-Term Actions:**
  + Deploy endpoint detection and response (EDR) solutions.
  + Monitor for unauthorized command-line activity.
  + Conduct further static analysis to identify obfuscated payloads.
  + Implement firewall rules to block suspicious outbound connections.

This concludes the dynamic analysis report. Further forensic investigation is recommended to determine the full scope of the threat.

