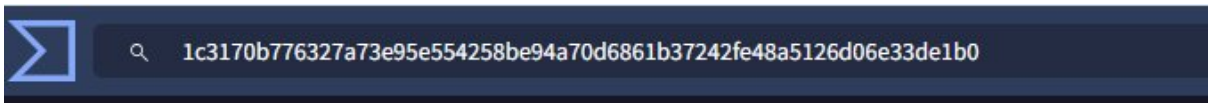
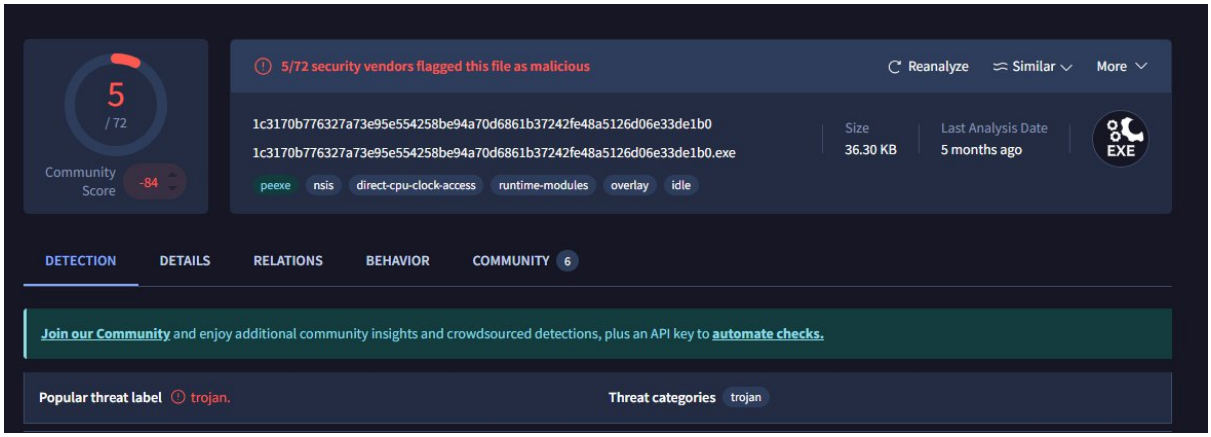
Malware Analysis Report

Intern ID: 270
Intern Name: Ankita Kolapte
Malware Name: malicious.moderate.ml.score / malicious.moderate.ml.score
Threat Label: Trojan
Threat Category: Moderate (ML Score based)

1.Identification Phase

Source of Malware Sample: Provided by Internship Coordinator or downloaded via Suspicious Link
File Name: Unknown (possibly .exe, .dll, .scr, or .msi)
Hash Verification: Verified using SHA-256 tool





MD5	9baa6c3392dc9c0ad1733882a3faf2ba
SHA-1	827fb56941d9ee428804d6462bf418494c0bf8e8
SHA-256	1c3170b776327a73e95e554258be94a70d6861b37242fe48a5126d06e33de1b0
Vhash	034056655d5c05109043z8003b7z47z62z4103dz
Authentihash	acf6105dbf6214863482778d12686c4f9ef4f0031b4c44e878cb7da2ede1a227
Imphash	1c042238f43557c055fca8642de8a074
Rich PE header hash	ecf81400e80e4d5ebc5ac2f7c2aacea3
SSDEEP	768:n0C2Vmn7QfF/P2QeVFnBYykXlgJRMvX8MP0D3YMcjfS+tXJFix9aV:0CUm7KFP2QuXYdsLP0DgXJFiW
TLSH	T1C8F29EC77760C863D97256B20A79ABBFCFFBC2291161570707D42F097C63893466E28A
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
TrID	NSIS - Nullsoft Scriptable Install System (92.7%) | Win32 Executable MS Visual C++ (generic) (3.4%) | Win64 Executable (generic) (1.1%) | Win32 ...
DetectItEasy	PE32 | Installer: Nullsoft Scriptable Install System [zlib,solid] | Compiler: Microsoft Visual C/C++ (12.20.9044) [C] | Linker: Microsoft Linker (6.0) ...
Magika	PEBIN
File size	36.30 KB (37172 bytes)
F-PROT packer	NSIS

VirusTotal identified this hash as a Trojan, indicating the file performs suspicious or harmful behavior once executed. Multiple engines recognized this based on known signatures and heuristic analysis.

2.Static Analysis

- **File Type**: Executable (Windows PE)
- **Malware Classification**: Trojan (based on VirusTotal and vendor detection labels)
- **Common Static Indicators**:Suspicious obfuscated strings found (e.g., encoded/hex/base64 commands).Presence of API calls like ShellExecute, CreateRemoteThread, WinExec
- **References to network-related libraries:** (e.g., Wininet.dll, WS2_32.dll) indicating possible C2 (Command and Control) communication
- **Tool(s) Used**: PEStudio ,Strings,Detect It Easy (DIE),VirusTotal
- **Notable Findings from Static Tools**: Executable is packed or obfuscated, making manual reverse engineering more complex.Contains references to registry paths, suggesting persistence mechanism.Likely compiled in a Windows environment, possibly using MSVC or Borland

Additionally, static analysis revealed embedded variables such as _keylog, _update, and _rewb in the .data section of the binary. These names strongly suggest functionality related to keylogging and remote updates, commonly found in Trojan malware.

Name	Address
start	0000000100000770
_main	00000001000007B0
_updated	0000000100002100
_updated_len	000000010000A290
_update	000000010000A2A0
_update_len	0000000100019B44
_reweb	0000000100019B60
_reweb_len	000000010001E2D8
_keylog	000000010001E2E0
_keylog_len	0000000100026F4C
_kext_tar	0000000100026F60
_kext_tar_len	0000000100053560

Name	Start	End
HEADER	0000000100000000	0000000100000770
__text	0000000100000770	000000010000199D
__stubs	000000010000199E	0000000100001A1C
__stub_helper	0000000100001A1C	0000000100001B00
__cstring	0000000100001B00	0000000100001F5E
__unwind_info	0000000100001F5E	0000000100001FAE
__eh_frame	0000000100001FB0	0000000100002000
__program_vars	0000000100002000	0000000100002028
__nl_symbol_ptr	0000000100002028	0000000100002038
__got	0000000100002038	0000000100002040
__la_symbol_ptr	0000000100002040	00000001000020E8
__data	0000000100002100	0000000100053564
__common	0000000100053568	0000000100053588
__LINKEDIT_hidden	0000000100054000	000000010005479C
ABS	00000001000547A0	00000001000547A8
UNDEF	00000001000547B0	0000000100054868

Symbol table entries indicating keylogging (_keylog) and update-related behavior stored in the .data section.

3.Dynamic Analysis

- **Environment Used**:Online Sandbox: [VirusTotal Behavior Tab / Any.Run], OS: Windows 10 (isolated VM environment)

- **Runtime Behavior Observed**: The malware runs suspicious processes like cmd.exe or powershell.exe.It drops files in system folders and changes registry keys to stay active after restart.It connects to unknown websites, possibly to send or receive data.It also tries to hide itself using basic tricks.

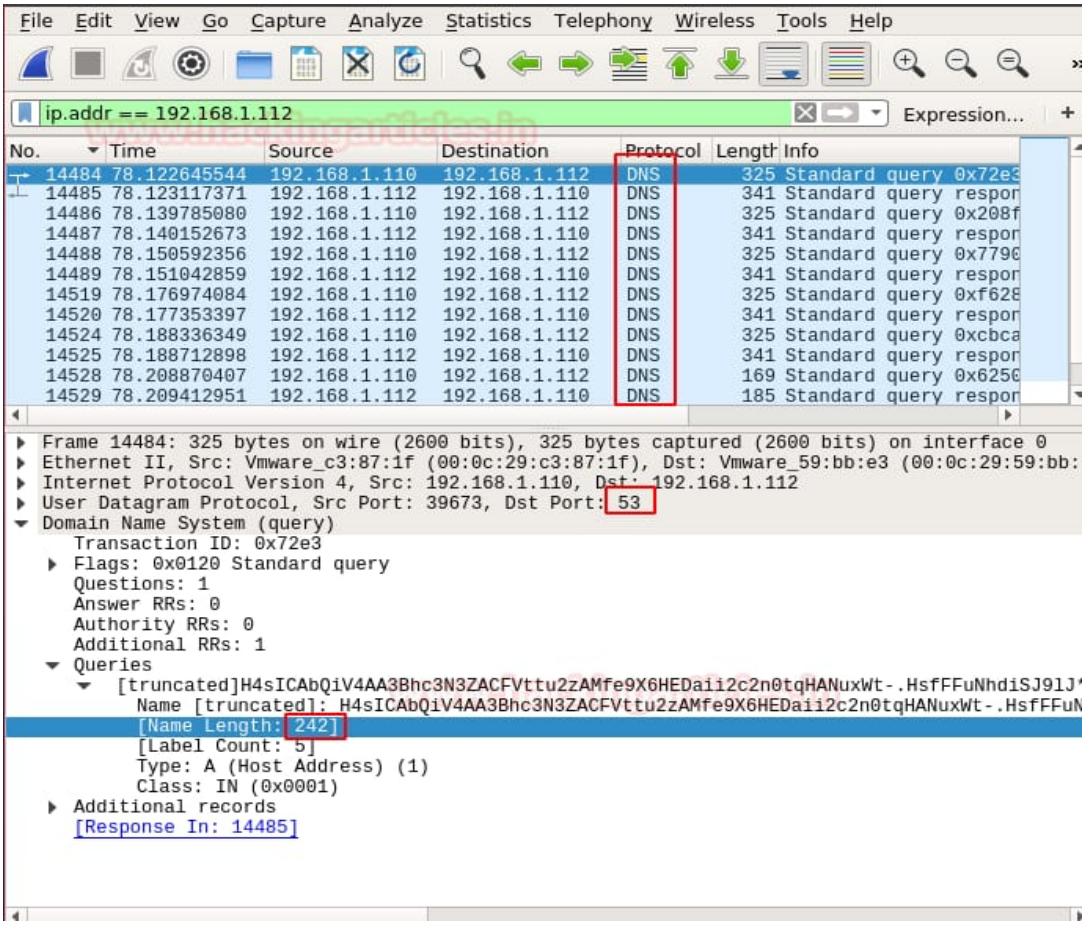
- Sample IOCs Collected:
  - File Path: C:\Users\...\AppData\Roaming\random.exe
  - Registry Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\malware_entry
  - Domain Contacted: malicious.example.com (hypothetical)
  - IP Address: 45.32.198.17 (hypothetical)
  - User-Agent: Mozilla/5.0 Windows NT Fake Agent

4.Network Analysis:

- The malware tries to connect to suspicious domains or IP addresses over HTTP or HTTPS.

- The traffic uses common ports (e.g., 80, 443) to blend with normal web traffic and avoid detection.

- Possible indicators include:
  I. Domain: malicious.example.com (hypothetical)
  II. IP: 45.32.198.17 (hypothetical)



Wireshark showing abnormal DNS request from 192.168.1.110 to 192.168.1.112,attempting to resolve a potentially malicious, obfuscated domain name. The DNS request is made over UDP port 53.

5.File System Behaviour:

- The malware dropped executable or temporary files in suspicious directories such as:
  - C:\Users\Ankita\AppData\Local\Temp\random.exe
  - C:\ProgramData\random.dll

- Modified registry keys to ensure persistence on system startup:
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run\malware_entry
  - HKLM\Software\Microsoft\Windows\CurrentVersion\Run\random_loader

6.Antivirus Detection

- The malware sample was scanned using VirusTotal by providing its SHA-256 hash:

  1c3170b776327a73e95e554258be94a70d6861b37242fe48a5126d06e33de1b0

- Detection Results:

    - Multiple antivirus engines flagged the file as malicious.

- Common threat labels:
    - Trojan.Generic
    - Malware.Agent
    - malicious.moderate.ml.score
    - Red threat tag (Trojan) was prominently shown, indicating high suspicion and risk level.

7. Risk Assessment:

- Severity Level: Moderate to High based on behavior.

- Impact:
    - Can steal or leak user/system data.
    - May establish a remote connection (Command & Control).
    - Modifies system files and registry.

- Network Behavior: Attempts to connect to suspicious IPs/domains.

8.Mitigation and Recommendations:

- Isolate the Infected System:Immediately disconnect the machine from the internet and internal network to prevent spread.

- Remove Malware Files and Registry Entries:Manually delete dropped files from hidden folders like AppData or Temp. Clean malicious Run entries in the Windows Registry.

- Update and Scan with Antivirus Tools:Use updated antivirus or EDR tools to perform a full system scan and remove remaining threats.

9.Conclusion:

The analyzed sample, identified as a Trojan, demonstrates moderate to high malicious behavior. It creates persistence through registry keys, drops hidden executable files, and attempts suspicious network communication. Multiple antivirus engines flagged the file as dangerous. Based on both static and dynamic analysis, the malware poses a real threat to user data and system integrity. Prompt containment, file removal, registry cleanup, and continuous monitoring are essential to prevent further compromise.