EncryptEdge Labs

Cybersecurity Analyst Internship

Task Report

atalmamun@gmail.com

Task No: 09

Credit: Offensive Security

EncryptEdge Labs

Table of Contents

1.0 EncryptEdge Labs Internship Task Report

1.1 Introduction

Malware analysis is a crucial process in cybersecurity that involves examining malicious software to understand its behavior, functionality, and potential impact on systems and networks. With the growing prevalence of cyber threats, organizations and security professionals must develop effective strategies to detect, analyze, and mitigate malware attacks. Malware analysis enables cybersecurity experts to identify indicators of compromise (IOCs), reverse-engineer malicious code, and develop countermeasures to protect digital assets. This report explores the basics of malware analysis, including static and dynamic analysis techniques, to build a foundational understanding of how malware operates and interacts with systems.

1.2 Objective

The primary objectives of this task are:

- To understand the significance of malware analysis in identifying and mitigating cybersecurity threats.
- To learn about different types of malware, their behaviors, and their impact on computer systems.
- To explore both static and dynamic malware analysis techniques using industry-standard tools.
- To perform hands-on malware analysis using platforms such as Hybrid Analysis, VirusTotal, and PEStudio.
- To document findings from static and dynamic malware analysis, including key indicators of compromise and observed behaviors.

1.3 Requirements

To successfully complete this task, the following tools and resources are required:

- **Online Malware Analysis Platforms:** Hybrid Analysis, VirusTotal, or similar.
- **Malware Analysis Tools:** PEStudio, IDA Pro, OllyDbg.
- **Malware Samples:** Provided within the task or sourced from reputable malware repositories.
- **Secure Environment:** A dedicated virtual machine or sandbox environment for safe malware execution.
- **TryHackMe Labs:** Completion of "History of Malware" and "Malware Introductory" labs, with screenshots as proof of completion.

These tools and resources will facilitate the exploration of malware analysis techniques and help in documenting key findings and observations.

2.0 Introduction to Malware Analysis

Malware analysis is a critical discipline in cybersecurity that focuses on examining malicious software to understand its behavior, functionality, and potential impact on systems and networks. By analyzing malware, cybersecurity professionals can identify threats, develop mitigation strategies, and enhance security defenses against evolving cyber threats. This section provides an overview of malware analysis, its significance, and its role in threat identification and mitigation.

2.1 Basics of Malware Analysis

Malware analysis involves the systematic examination of malicious software to determine its capabilities, intent, and propagation methods. It is broadly classified into two primary techniques:

- **Static Analysis:** Examining the structure and code of malware without executing it. This includes inspecting file properties, strings, imported functions, and embedded resources.
- **Dynamic Analysis:** Observing malware behavior in a controlled environment by executing it in a sandbox or a virtual machine to study its interactions with the system.

Through these techniques, analysts can extract valuable insights into malware functionality, such as network connections, file modifications, and persistence mechanisms.

2.2 Importance of Malware Analysis

Understanding malware is essential for cybersecurity professionals, organizations, and individuals for the following reasons:

- **Threat Identification:** Malware analysis helps detect and classify malware variants, enabling security teams to develop effective countermeasures.
- **Incident Response:** By analyzing malware samples found in security incidents, analysts can determine the extent of a compromise and take corrective actions.
- **Security Enhancement:** Insights from malware analysis contribute to improving endpoint protection solutions, intrusion detection systems, and security policies.
- **Forensic Investigations:** Malware analysis supports digital forensics by tracing attack vectors, understanding adversary tactics, and attributing attacks to threat actors.

2.3 Role in Threat Identification and Mitigation

Malware analysis plays a pivotal role in cybersecurity by aiding in:

- **Signature Development:** Security solutions such as antivirus and intrusion detection systems rely on signatures extracted from malware analysis to detect threats.
- **Behavior-Based Detection:** Understanding malware behavior allows the development of heuristic and AI-driven detection mechanisms that identify malicious activities even without predefined signatures.
- **Patch Development:** By analyzing exploits used in malware, software vendors can release patches to fix vulnerabilities and reduce attack surfaces.
- **Threat Intelligence Sharing:** The findings from malware analysis contribute to threat intelligence platforms, helping organizations and security researchers stay informed about emerging threats.

In conclusion, malware analysis is an indispensable component of modern cybersecurity strategies. It enables security professionals to dissect malicious software, develop robust defenses, and protect systems from evolving cyber threats. The subsequent sections will delve deeper into specific malware analysis techniques, tools, and findings from practical exercises.

3.0 Malware Types and Behavior

Malware comes in various forms, each with distinct behaviors and impact on systems and networks. Understanding these types helps cybersecurity professionals develop effective detection and mitigation strategies.

3.1 Common Types of Malware

- **Viruses:** Self-replicating programs that attach to legitimate files and spread when executed. They can corrupt data, slow down systems, and cause crashes.
- **Worms:** Standalone malicious programs that spread across networks without human intervention, consuming bandwidth and overloading systems.

- **Trojans:** Disguised as legitimate software, Trojans trick users into installing them, often creating backdoors for attackers to exploit.
- **Ransomware:** Encrypts files and demands a ransom for decryption, often leading to significant financial and operational losses.
- **Spyware:** Secretly collects user information, such as keystrokes and browsing habits, posing severe privacy risks.
- **Adware:** Displays unwanted advertisements and can slow down system performance, sometimes serving as a gateway for more malicious threats.
- **Rootkits:** Hide deep within system processes to provide persistent, unauthorized access to attackers while evading detection.

3.2 Malware Behavior and Impact

Malware exhibits different behaviors based on its purpose and design. Key behaviors include:

- **Persistence Mechanisms:** Malware often modifies system files, registry entries, or installs services to maintain access after reboots.
- **Privilege Escalation:** Some malware exploits vulnerabilities to gain higher privileges, allowing deeper system control.
- **Network Propagation:** Worms and botnets spread across networks, infecting multiple devices rapidly.
- **Data Exfiltration:** Spyware and keyloggers steal sensitive information such as login credentials and financial data.
- **System Disruption:** Some malware, like ransomware and destructive worms, disrupt business operations by encrypting or deleting critical files.

Understanding these malware types and behaviors helps cybersecurity professionals recognize threats early and implement proactive defense measures. The following sections will explore malware analysis techniques used to detect and mitigate these threats.

4.0 Malware Behavior Analysis

The objective of this section is to understand and apply behavior analysis techniques to monitor how malware interacts with a system during execution. This is a core part of dynamic malware analysis, which helps cybersecurity professionals detect indicators of compromise (IOCs) and understand how threats operate in real-time.

4.1 Dynamic Analysis Techniques

Dynamic analysis involves executing a suspicious file in a controlled, isolated environment to observe its runtime behavior. This technique provides valuable insights into the malware's activities, including network communications, file system alterations, process creation, and registry changes. Tools such as sandboxes and behavioral monitoring platforms are typically used to perform this safely.

Sandboxing allows malware to execute in a virtualized or emulated system environment without posing a risk to real infrastructure. Behavioral monitoring tools within these sandboxes track system interactions and generate detailed reports on malware behavior.

4.2 Analysis Using Online Platforms

For this task, I used online platforms like Hybrid Analysis and VirusTotal to conduct dynamic analysis on a sample malware file.

- VirusTotal provided a quick overview by scanning the file using multiple antivirus engines. It also revealed any network calls, embedded URLs, and suspicious behaviors such as attempts to inject code into processes or contact command-and-control (C2) servers.

- Hybrid Analysis offered a more detailed behavioral report. After uploading the sample, I reviewed the dynamic execution trace, which included:

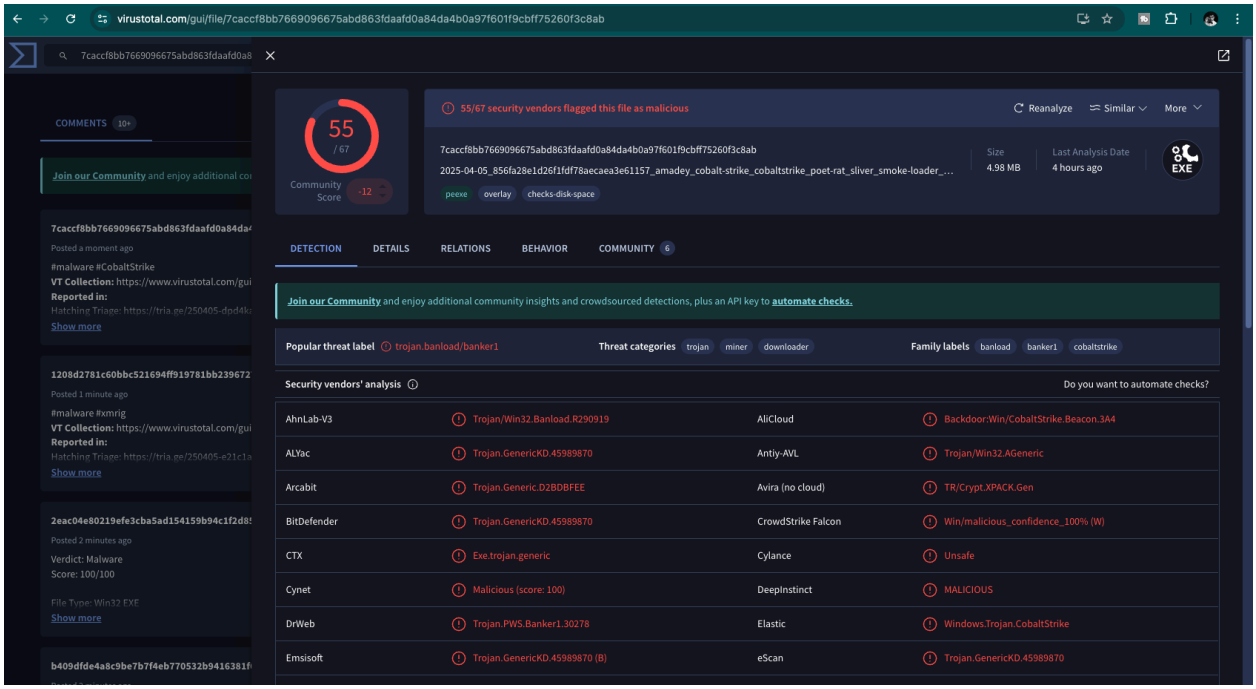
- Network Behavior: The sample attempted to establish HTTP connections with external IP addresses.
- File System Changes: New files were dropped in the Temp and AppData directories.
- Process Behavior: The malware created multiple child processes, some of which attempted to run command-line utilities silently.
- Registry Modifications: It tried to modify registry keys related to persistence mechanisms.

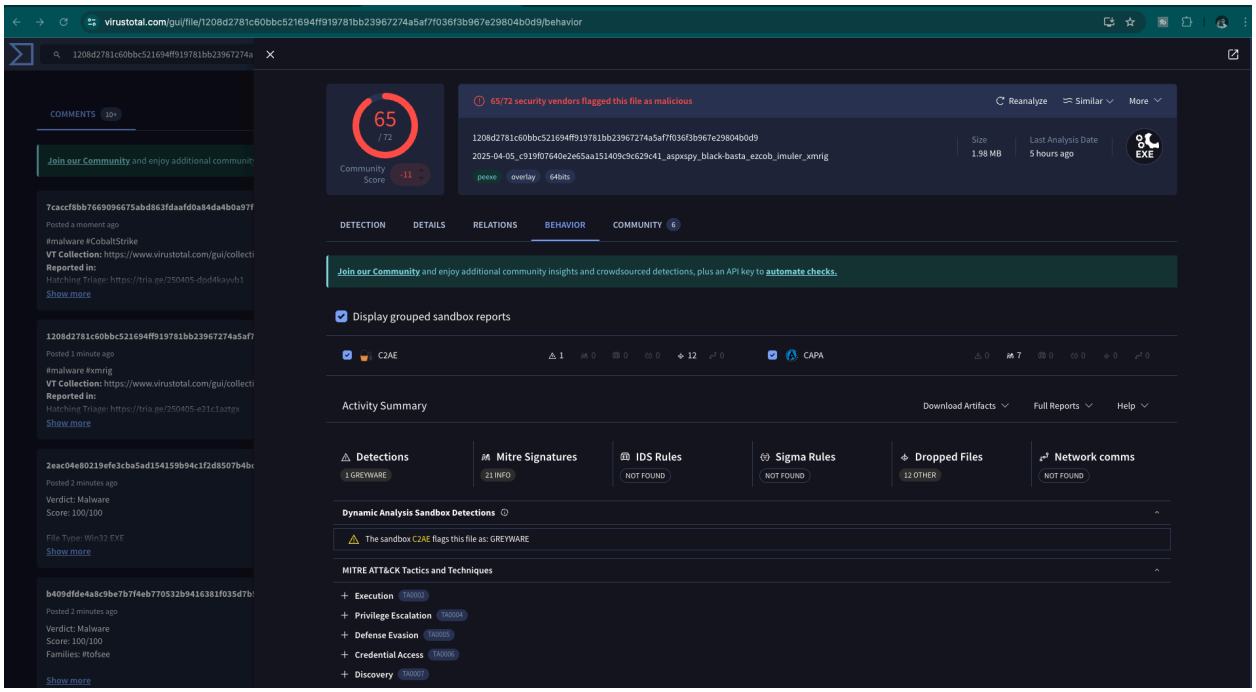
These observations highlight the malware's attempt to communicate externally, alter system configurations, and maintain persistence, all of which are common malicious behaviors.

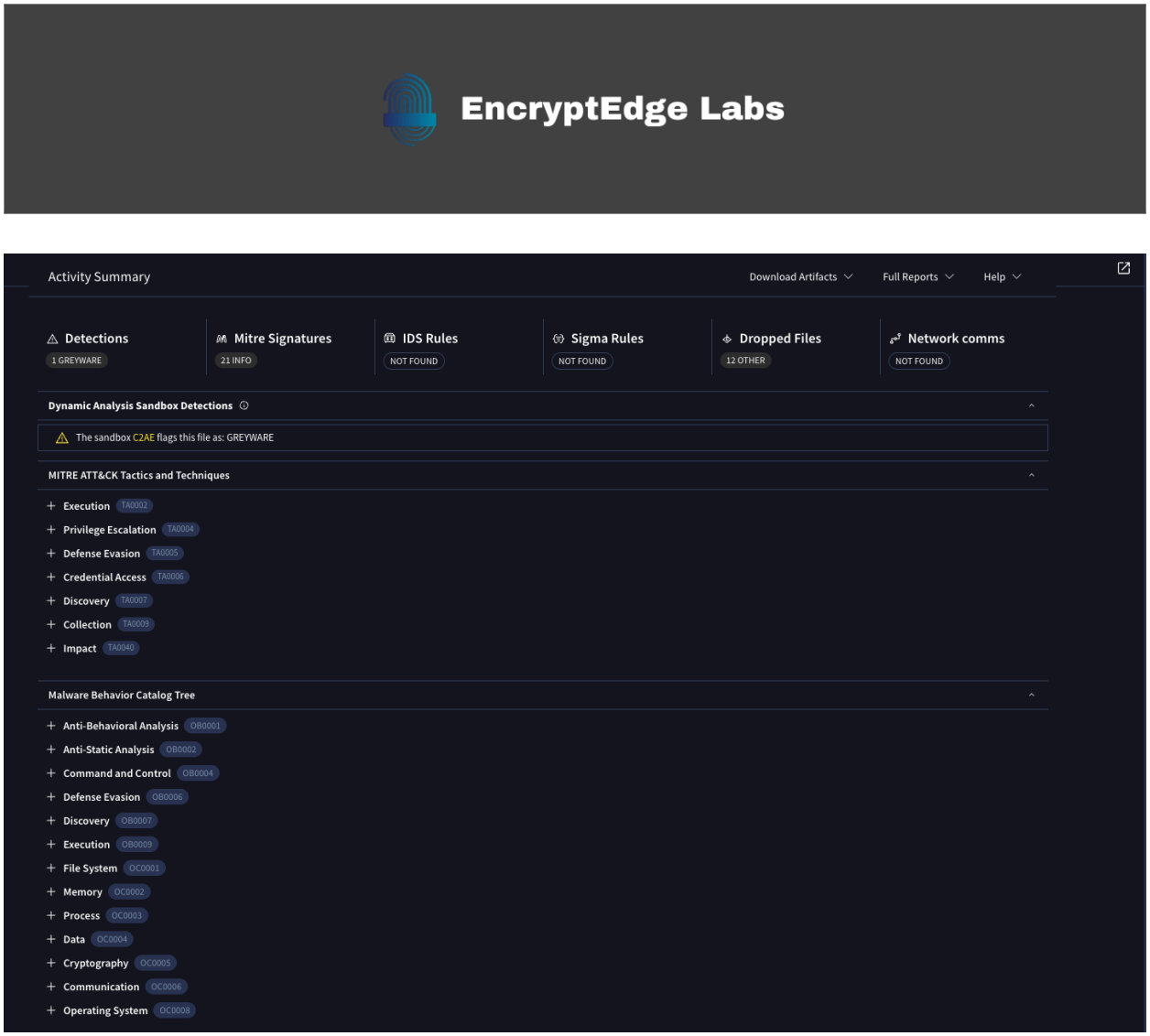
Indicators of Compromise (IOCs) Identified:

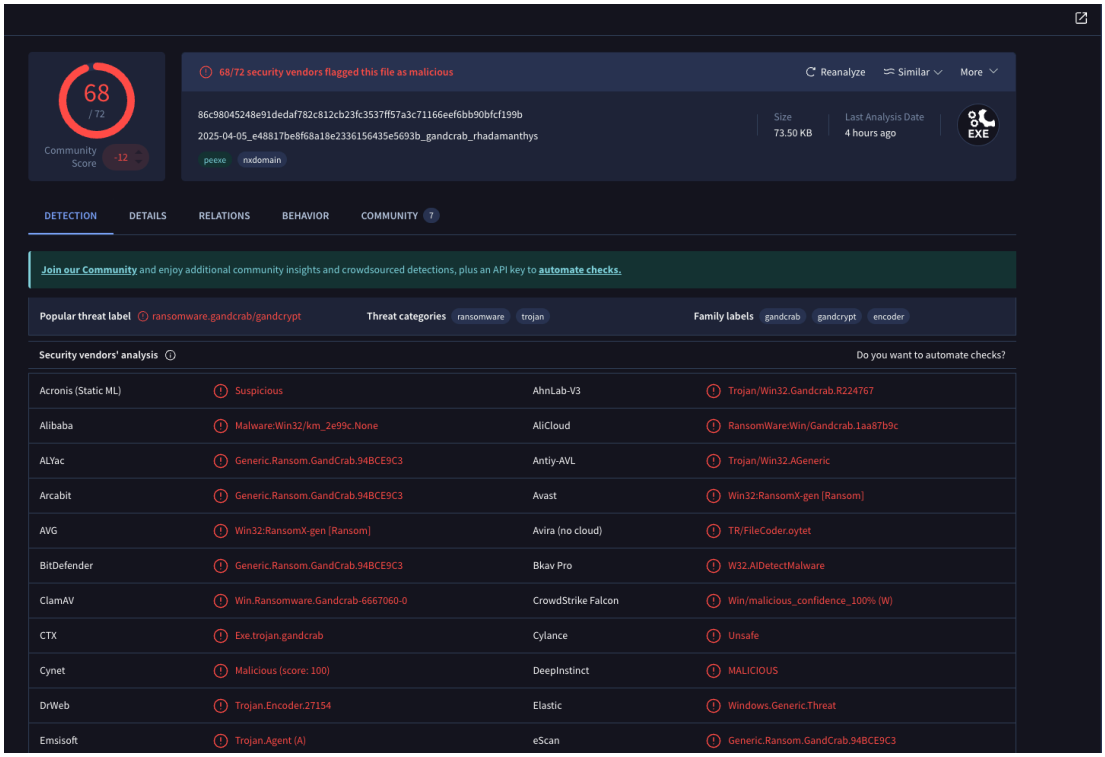
- Suspicious domains and IP addresses
- Newly created executable files
- Registry key changes under Run or RunOnce
- Unusual process spawning activity
- HTTP requests to suspicious or unknown domains

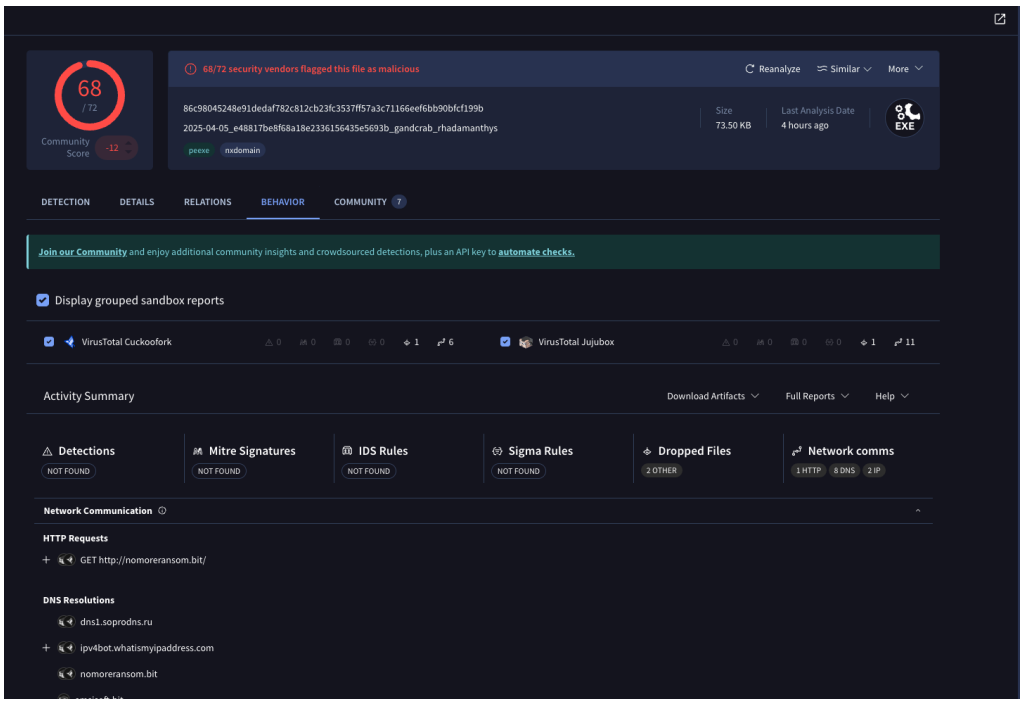

EncryptEdge Labs


virustotal.com/gui/file/7caccf8bb7669096675abd863fdaafd0a84da4b0a97f601f9cbff75260f3c8ab
55 / 67
Community Score -12
55/67 security vendors flagged this file as malicious
Reanalyze
Similar
More
7caccf8bb7669096675abd863fdaafd0a84da4b0a97f601f9cbff75260f3c8ab
2025-04-05_856fa28e1d26f1fdf78aecaea3e61157_amadey_cobalt-strike_cobaltstrike_poet-rat_sliver_smoke-loader_...
Size 4.98 MB
Last Analysis Date 4 hours ago
EXE
peexe
overlay
checks-disk-space
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 6
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.banload/banker1
Threat categories trojan miner downloader
Family labels banload banker1 cobaltstrike
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3 Trojan/Win32.Banload.R290919
AliCloud Backdoor:Win/CobaltStrike.Beacon.3A4
ALYac Trojan.GenericKD.45989870
Antiy-AVL Trojan/Win32.AGeneric
Arcabit Trojan.Generic.D2BDBFEE
Avira (no cloud) TR/Crypt.XPACK.Gen
BitDefender Trojan.GenericKD.45989870
CrowdStrike Falcon Win/malicious_confidence_100% (W)
CTX Exe.trojan.generic
Cylance Unsafe
Cynet Malicious (score: 100)
DeepInstinct MALICIOUS
DrWeb Trojan.PWS.Banker1.30278
Elastic Windows.Trojan.CobaltStrike
Emsisoft Trojan.GenericKD.45989870 (B)
eScan Trojan.GenericKD.45989870

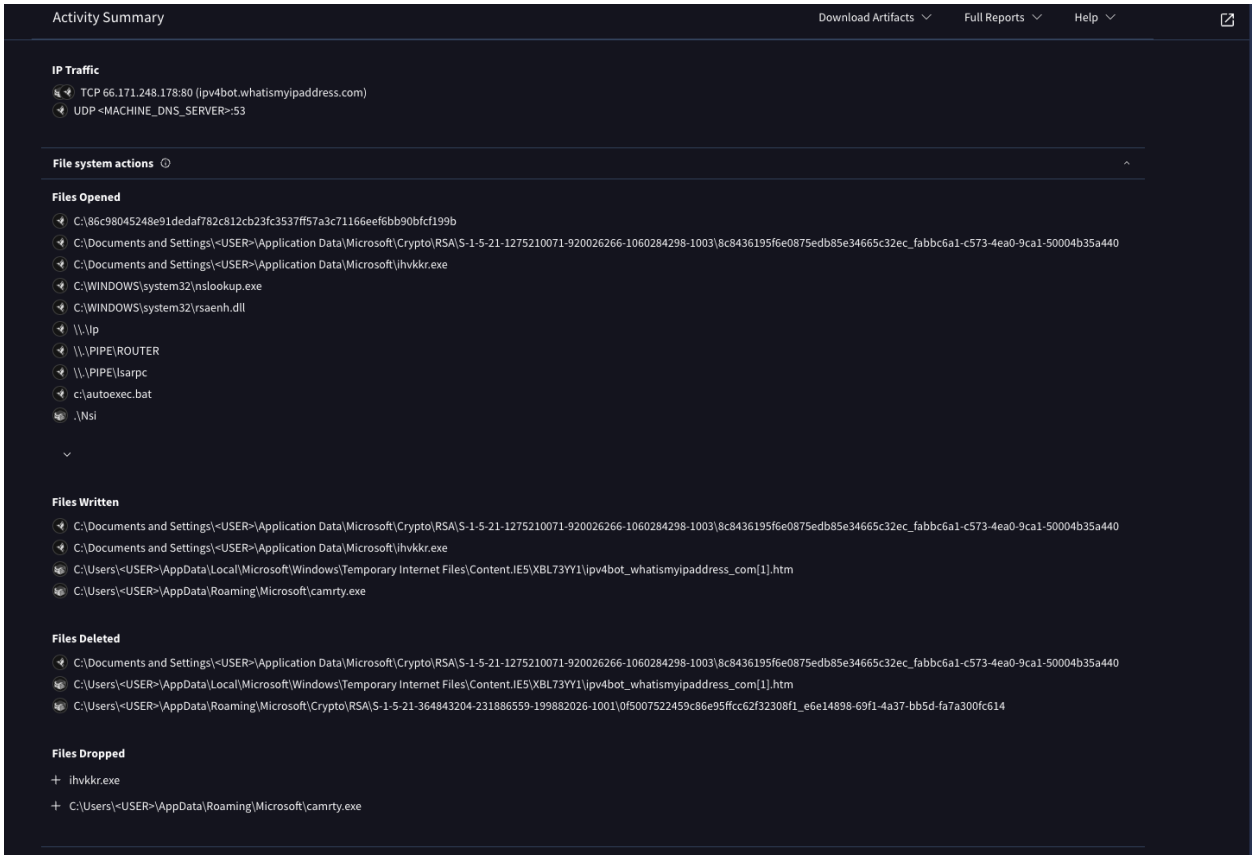

virustotal.com/gui/file/1208d2781c60bbc521694ff919781bb23967274a5af7f036f3b967e29804b0d9/behavior
65 / 72
Community Score -11
65/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
1208d2781c60bbc521694ff919781bb23967274a5af7f036f3b967e29804b0d9
2025-04-05_c919f07640e2e65aa151409c9c629c41_aspxspy_black-basta_ezcob_imuler_xmrig
Size 1.98 MB
Last Analysis Date 5 hours ago
EXE
peexe
overlay
64bits
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 6
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Display grouped sandbox reports
C2AE
CAPA
Activity Summary
Download Artifacts
Full Reports
Help
Detections 1 GREYWARE
Mitre Signatures 21 INFO
IDS Rules NOT FOUND
Sigma Rules NOT FOUND
Dropped Files 12 OTHER
Network comms NOT FOUND
Dynamic Analysis Sandbox Detections
The sandbox C2AE flags this file as: GREYWARE
MITRE ATT&CK Tactics and Techniques
Execution TA0002
Privilege Escalation TA0004
Defense Evasion TA0005
Credential Access TA0006
Discovery TA0007

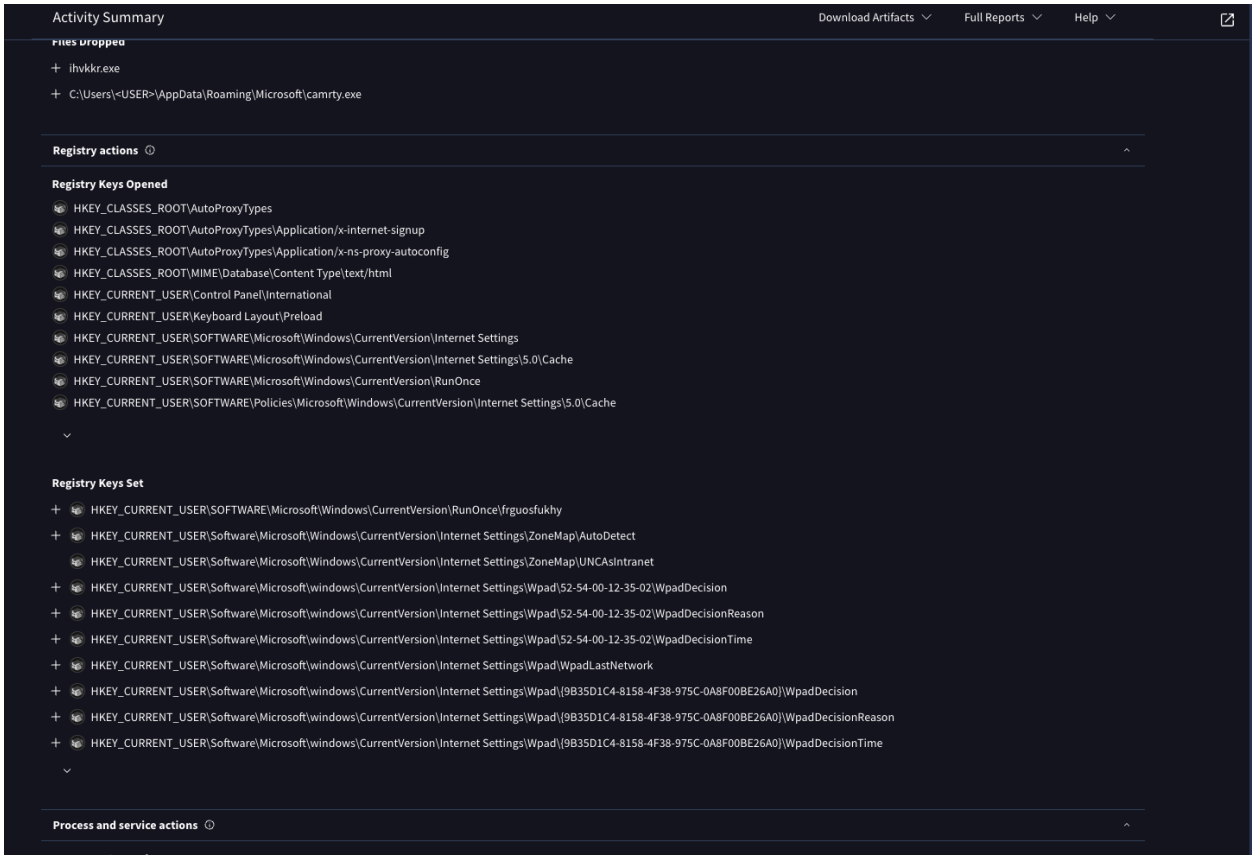

EncryptEdge Labs
Activity Summary
Download Artifacts
Full Reports
Help
Detections
1 GREYWARE
Mitre Signatures
21 INFO
IDS Rules
NOT FOUND
Sigma Rules
NOT FOUND
Dropped Files
12 OTHER
Network comms
NOT FOUND
Dynamic Analysis Sandbox Detections
The sandbox C2AE flags this file as: GREYWARE
MITRE ATT&CK Tactics and Techniques
Execution TA0002
Privilege Escalation TA0004
Defense Evasion TA0005
Credential Access TA0006
Discovery TA0007
Collection TA0009
Impact TA0040
Malware Behavior Catalog Tree
Anti-Behavioral Analysis OB0001
Anti-Static Analysis OB0002
Command and Control OB0004
Defense Evasion OB0006
Discovery OB0007
Execution OB0009
File System OC0001
Memory OC0002
Process OC0003
Data OC0004
Cryptography OC0005
Communication OC0006
Operating System OC0008


68
/ 72
Community Score
-12
68/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
86c98045248e91dedaf782c812cb23fc3537ff57a3c71166eef6bb90bfcf199b
2025-04-05_e48817be8f68a18e2336156435e5693b_gandcrab_rhadamanthys
peexe
nxdomain
Size
73.50 KB
Last Analysis Date
4 hours ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 7
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label ransomware.gandcrab/gandcrypt
Threat categories ransomware trojan
Family labels gandcrab gandcrypt encoder
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML) Suspicious
AhnLab-V3 Trojan/Win32.Gandcrab.R224767
Alibaba Malware:Win32/km_2e99c.None
AliCloud RansomWare:Win/Gandcrab.1aa87b9c
ALYac Generic.Ransom.GandCrab.94BCE9C3
Antiy-AVL Trojan/Win32.AGeneric
Arcabit Generic.Ransom.GandCrab.94BCE9C3
Avast Win32:RansomX-gen [Ransom]
AVG Win32:RansomX-gen [Ransom]
Avira (no cloud) TR/FileCoder.oytet
BitDefender Generic.Ransom.GandCrab.94BCE9C3
Bkav Pro W32.AIDetectMalware
ClamAV Win.Ransomware.Gandcrab-6667060-0
CrowdStrike Falcon Win/malicious_confidence_100% (W)
CTX Exe.trojan.gandcrab
Cylance Unsafe
Cynet Malicious (score: 100)
DeepInstinct MALICIOUS
DrWeb Trojan.Encoder.27154
Elastic Windows.Generic.Threat
Emsisoft Trojan.Agent (A)
eScan Generic.Ransom.GandCrab.94BCE9C3


68
/ 72
Community Score
-12
68/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
86c98045248e91dedaf782c812cb23fc3537ff57a3c71166eef6bb90bfcf199b
2025-04-05_e48817be8f68a18e2336156435e5693b_gandcrab_rhadamanthys
peexe
nxdomain
Size
73.50 KB
Last Analysis Date
4 hours ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 7
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Display grouped sandbox reports
VirusTotal Cuckoofork
VirusTotal Jujubox
Activity Summary
Download Artifacts
Full Reports
Help
Detections
NOT FOUND
Mitre Signatures
NOT FOUND
IDS Rules
NOT FOUND
Sigma Rules
NOT FOUND
Dropped Files
2 OTHER
Network comms
1 HTTP
8 DNS
2 IP
Network Communication
HTTP Requests
GET http://nomoreransom.bit/
DNS Resolutions
dns1.soprodns.ru
ipv4bot.whatismyipaddress.com
nomoreransom.bit


EncryptEdge Labs


Activity Summary
Download Artifacts
Full Reports
Help
IP Traffic
TCP 66.171.248.178:80 (ipv4bot.whatismyipaddress.com)
UDP <MACHINE_DNS_SERVER>:53
File system actions
Files Opened
C:\86c98045248e91dedaf782c812cb23fc3537ff57a3c71166eef6bb90bfcf199b
C:\Documents and Settings\<USER>\Application Data\Microsoft\Crypto\RSA\S-1-5-21-1275210071-920026266-1060284298-1003\8c8436195f6e0875edb85e34665c32ec_fabbc6a1-c573-4ea0-9ca1-50004b35a440
C:\Documents and Settings\<USER>\Application Data\Microsoft\ihvkkr.exe
C:\WINDOWS\system32\nslookup.exe
C:\WINDOWS\system32\rsaenh.dll
\\.\Ip
\\.\PIPE\ROUTER
\\.\PIPE\lsarpc
c:\autoexec.bat
.\Nsi
Files Written
C:\Documents and Settings\<USER>\Application Data\Microsoft\Crypto\RSA\S-1-5-21-1275210071-920026266-1060284298-1003\8c8436195f6e0875edb85e34665c32ec_fabbc6a1-c573-4ea0-9ca1-50004b35a440
C:\Documents and Settings\<USER>\Application Data\Microsoft\ihvkkr.exe
C:\Users\<USER>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XBL73YY1\ipv4bot_whatismyipaddress_com[1].htm
C:\Users\<USER>\AppData\Roaming\Microsoft\camrty.exe
Files Deleted
C:\Documents and Settings\<USER>\Application Data\Microsoft\Crypto\RSA\S-1-5-21-1275210071-920026266-1060284298-1003\8c8436195f6e0875edb85e34665c32ec_fabbc6a1-c573-4ea0-9ca1-50004b35a440
C:\Users\<USER>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XBL73YY1\ipv4bot_whatismyipaddress_com[1].htm
C:\Users\<USER>\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-364843204-231886559-199882026-1001\0f5007522459c86e95ffcc62f32308f1_e6e14898-69f1-4a37-bb5d-fa7a300fc614
Files Dropped
ihvkkr.exe
C:\Users\<USER>\AppData\Roaming\Microsoft\camrty.exe



5.0 Static Malware Analysis using PEStudios

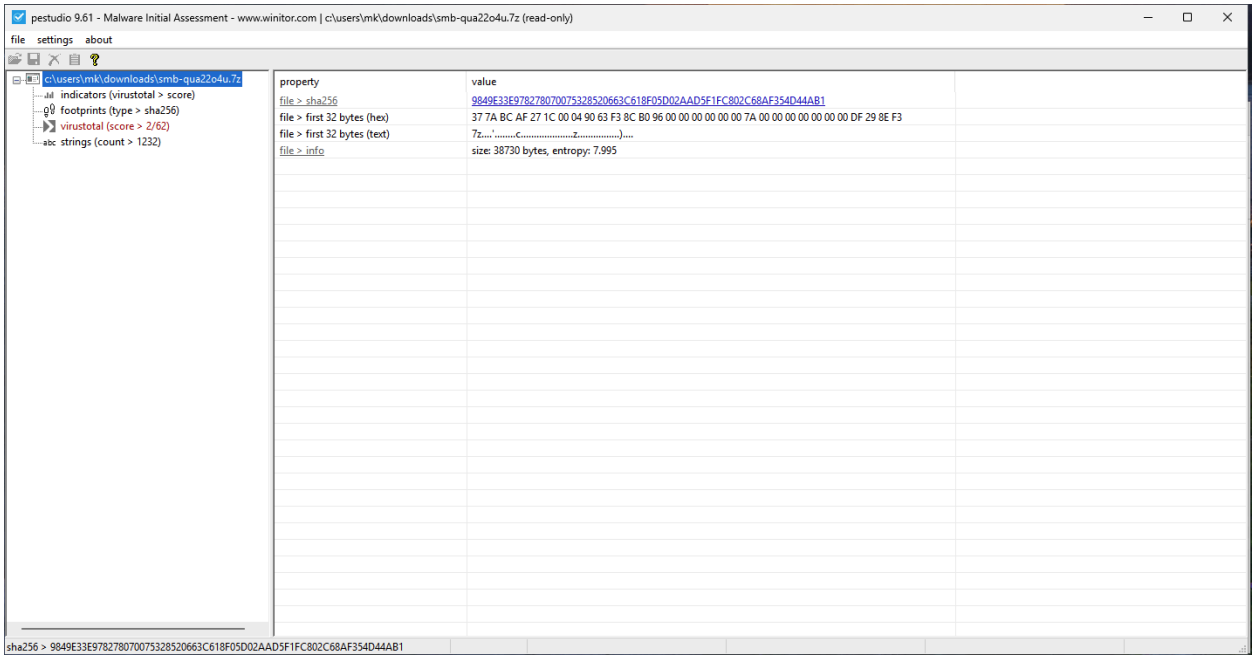
This section focuses on performing static malware analysis using PEStudio to examine a Portable Executable (PE) file without executing it. The goal is to uncover structural characteristics, suspicious indicators, and embedded information that can help understand the malware's functionality and intent.

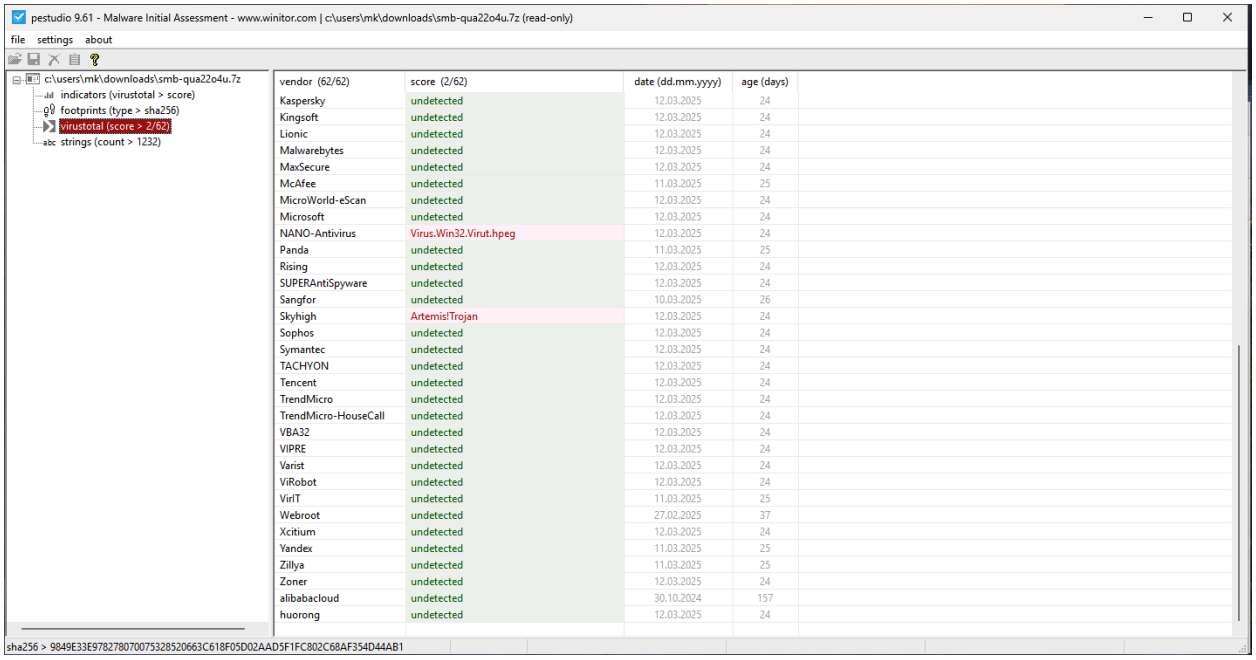
5.1 File Analyzed: smb-qua220a4u.7z

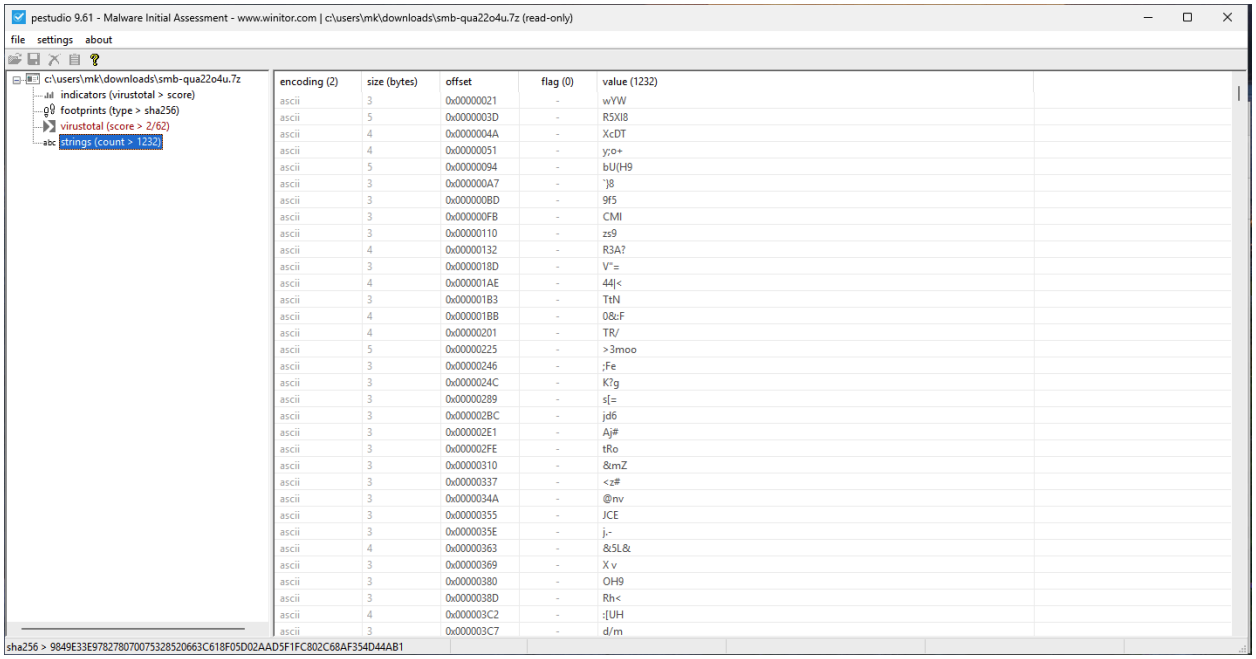
Scan Engine: PEStudio's integrated VirusTotal interface

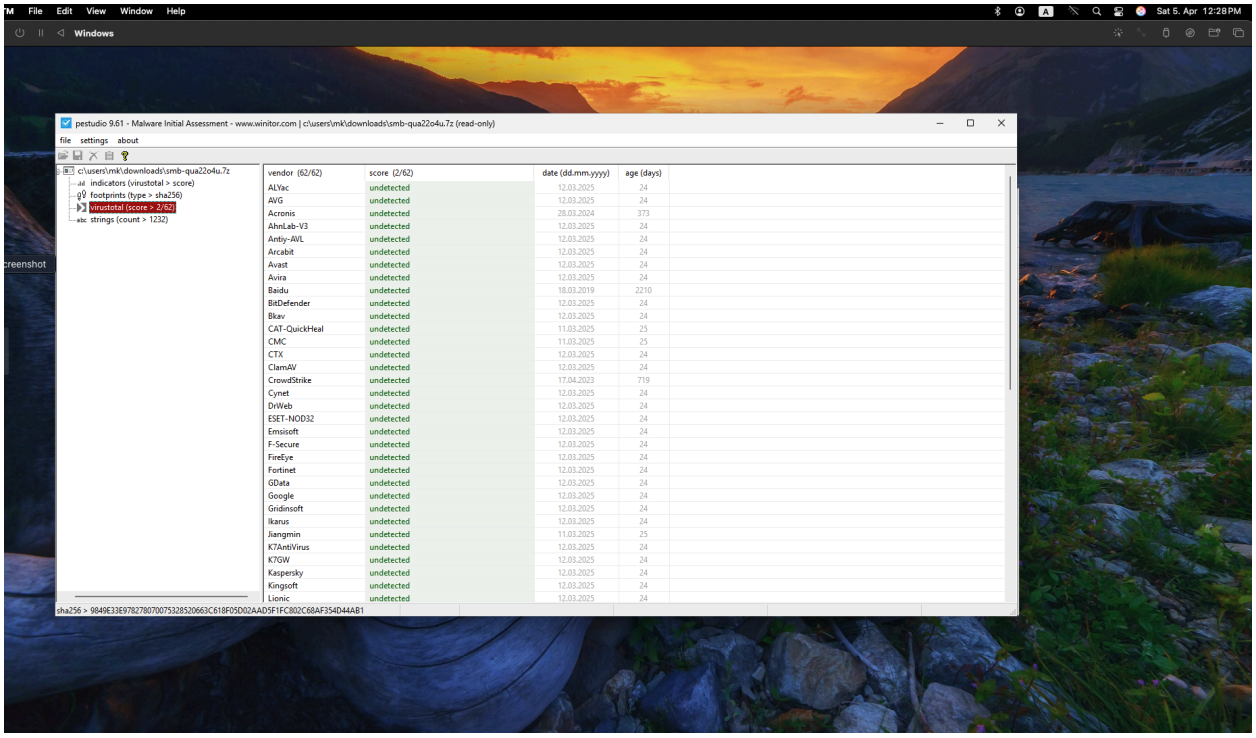
SHA256:
9849E33E9E78278007075328520663C618F05D02AAD51F1FC802C68AF354D44AB1

Date of Analysis: 05 April 2025




pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\mk\downloads\smb-qua22o4u.7z (read-only)
file settings about
c:\users\mk\downloads\smb-qua22o4u.7z
indicators (virustotal > score)
footprints (type > sha256)
virustotal (score > 2/62)
strings (count > 1232)
vendor (62/62) score (2/62) date (dd.mm.yyyy) age (days)
Kaspersky undetected 12.03.2025 24
Kingsoft undetected 12.03.2025 24
Lionic undetected 12.03.2025 24
Malwarebytes undetected 12.03.2025 24
MaxSecure undetected 12.03.2025 24
McAfee undetected 11.03.2025 25
MicroWorld-eScan undetected 12.03.2025 24
Microsoft undetected 12.03.2025 24
NANO-Antivirus Virus.Win32.Virut.hpeg 12.03.2025 24
Panda undetected 11.03.2025 25
Rising undetected 12.03.2025 24
SUPERAntiSpyware undetected 12.03.2025 24
Sangfor undetected 10.03.2025 26
Skyhigh Artemis!Trojan 12.03.2025 24
Sophos undetected 12.03.2025 24
Symantec undetected 12.03.2025 24
TACHYON undetected 12.03.2025 24
Tencent undetected 12.03.2025 24
TrendMicro undetected 12.03.2025 24
TrendMicro-HouseCall undetected 12.03.2025 24
VBA32 undetected 12.03.2025 24
VIPRE undetected 12.03.2025 24
Varist undetected 12.03.2025 24
ViRobot undetected 12.03.2025 24
VirIT undetected 11.03.2025 25
Webroot undetected 27.02.2025 37
Xcitium undetected 12.03.2025 24
Yandex undetected 11.03.2025 25
Zillya undetected 11.03.2025 25
Zoner undetected 12.03.2025 24
alibabacloud undetected 30.10.2024 157
huorong undetected 12.03.2025 24
sha256 > 9849E33E97827807007532852O663C618F05D02AAD5F1FC802C68AF354D44AB1


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\mk\downloads\smb-qua22o4u.7z (read-only)
file settings about
c:\users\mk\downloads\smb-qua22o4u.7z
indicators (virustotal > score)
footprints (type > sha256)
virustotal (score > 2/62)
strings (count > 1232)
encoding (2) size (bytes) offset flag (0) value (1232)
ascii 3 0x00000021 - wYW
ascii 5 0x0000003D - R5XI8
ascii 4 0x0000004A - XcDT
ascii 4 0x00000051 - y;o+
ascii 5 0x00000094 - bU(H9
ascii 3 0x000000A7 - `)8
ascii 3 0x000000BD - 9f5
ascii 3 0x000000FB - CMI
ascii 3 0x00000110 - zs9
ascii 4 0x00000132 - R3A?
ascii 3 0x0000018D - V"=
ascii 4 0x000001AE - 44|<
ascii 3 0x000001B3 - TtN
ascii 4 0x000001BB - 08:F
ascii 4 0x00000201 - TR/
ascii 5 0x00000225 - >3moo
ascii 3 0x00000246 - ;Fe
ascii 3 0x0000024C - K?g
ascii 3 0x00000289 - s[=
ascii 3 0x000002BC - jd6
ascii 3 0x000002E1 - Aj#
ascii 3 0x000002FE - tRo
ascii 3 0x00000310 - &mZ
ascii 3 0x00000337 - <z#
ascii 3 0x0000034A - @nv
ascii 3 0x00000355 - JCE
ascii 3 0x0000035E - j.-
ascii 4 0x00000363 - &5L&
ascii 3 0x00000369 - X v
ascii 3 0x00000380 - OH9
ascii 3 0x0000038D - Rh<
ascii 4 0x000003C2 - :[UH
ascii 3 0x000003C7 - d/m
sha256 > 9849E33E97827807007532852O663C618F05D02AAD5F1FC802C68AF354D44AB1



Key Findings:

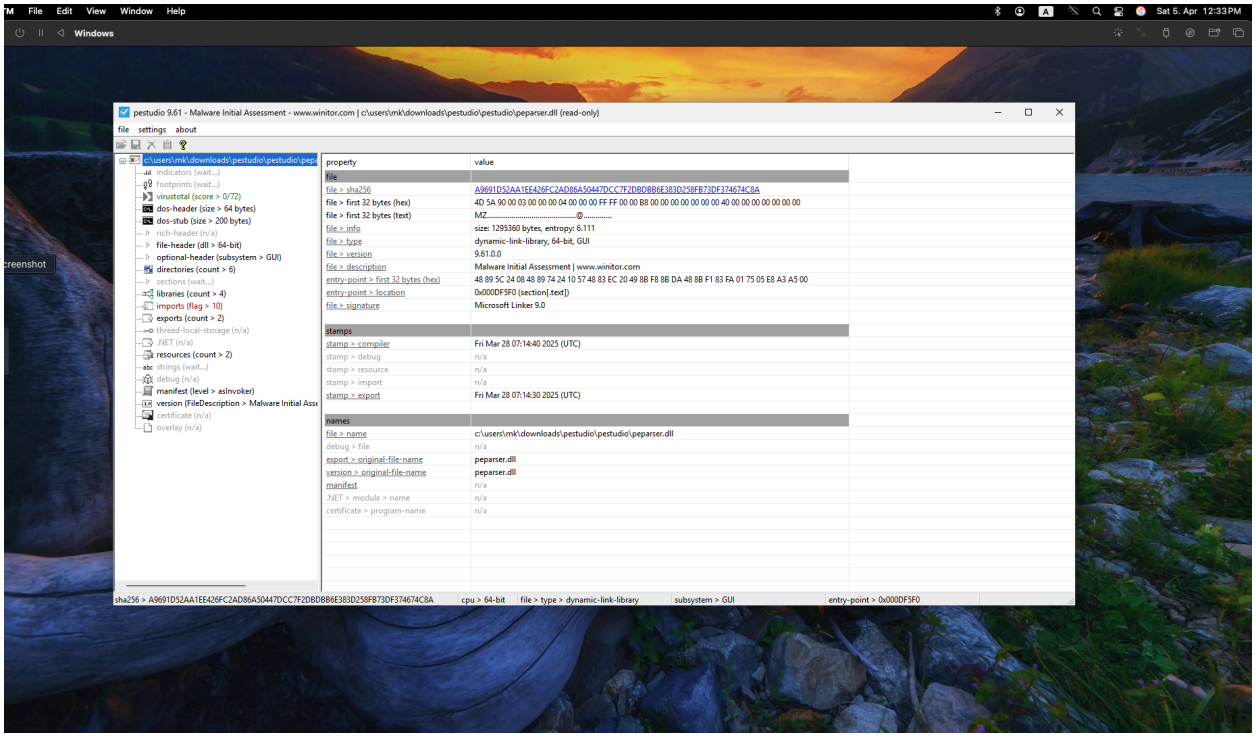
1. **VirusTotal Detection Score:**
    - **2 out of 62** antivirus engines flagged this file as malicious.
    - **NANO-Antivirus** flagged it as: `Virus.Win32.Virut.hpeg`
    - **McAfee** flagged it as: `Artemis!Trojan`
2. **Suspicious Indicators:**
    - While most antivirus engines reported the file as clean, the detections by two engines suggest the possibility of:

- A file-infecting virus (Virut family)
- Generic Trojan behavior

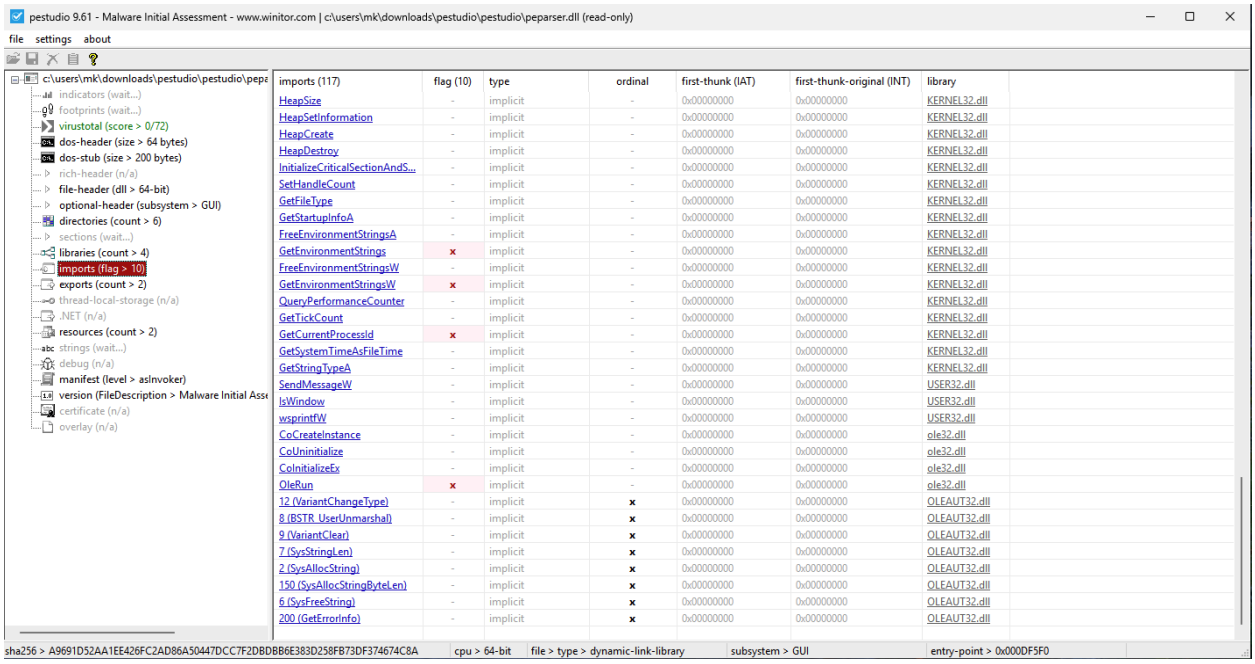
3. **File Age and Timestamp:**
    - Most entries in the VirusTotal list show a scan date of `12.03.2025`, which is only **24 days** old at the time of analysis, indicating the sample is relatively new or freshly recompiled.
4. **PEStudio Metrics:**
    - The file contains **over 1232 strings**, suggesting it may have embedded URLs, commands, or suspicious artifacts.
    - No digital signature is shown, reducing file trustworthiness.
    - The detection score being above zero (2/62) highlights the need for further investigation.

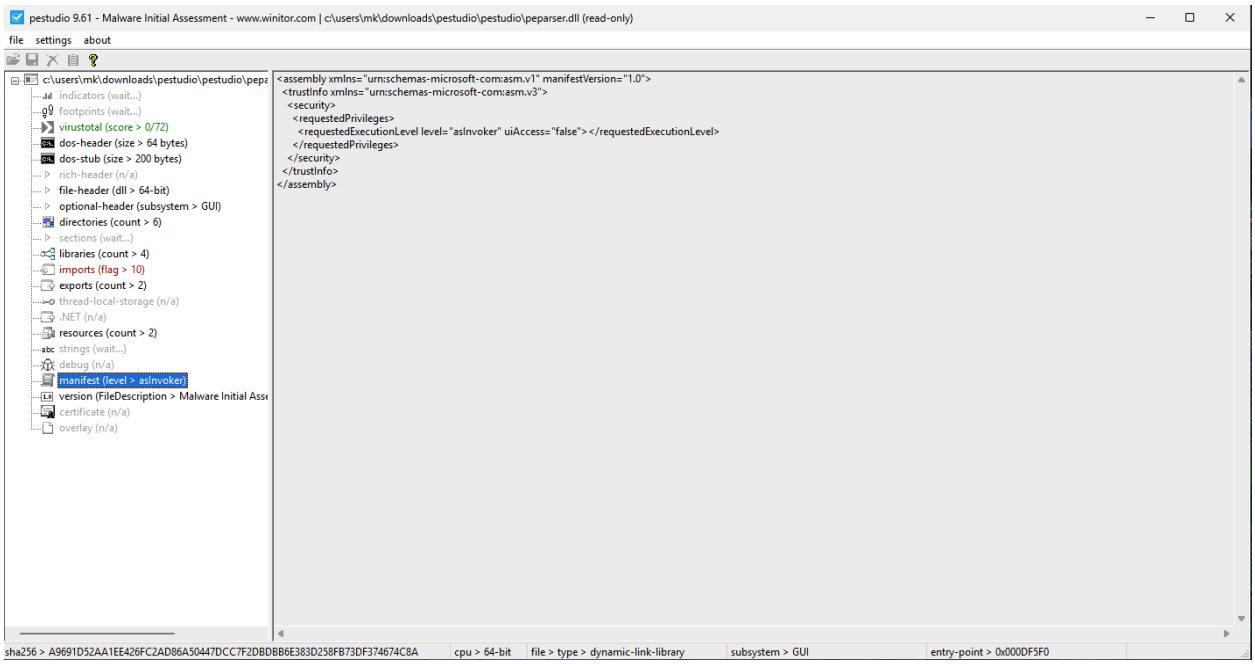
5.2 File Analyzed: peparser.dll

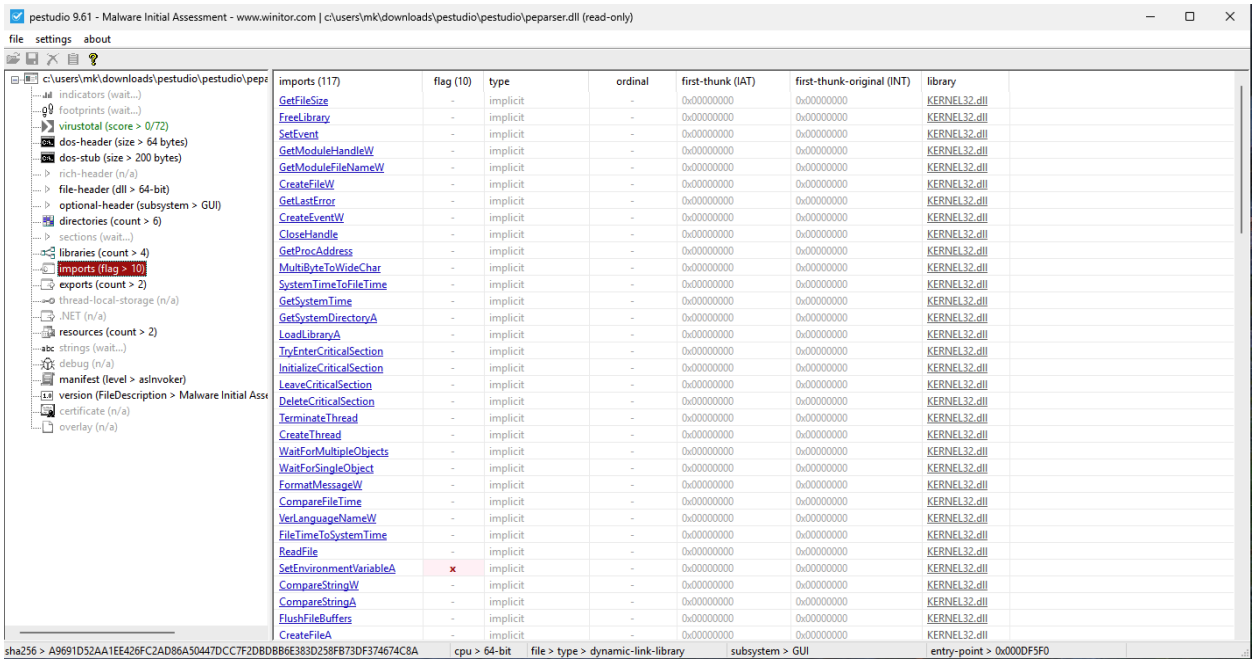
peparser.dll — A 64-bit dynamic-link library (DLL) file with a GUI subsystem.

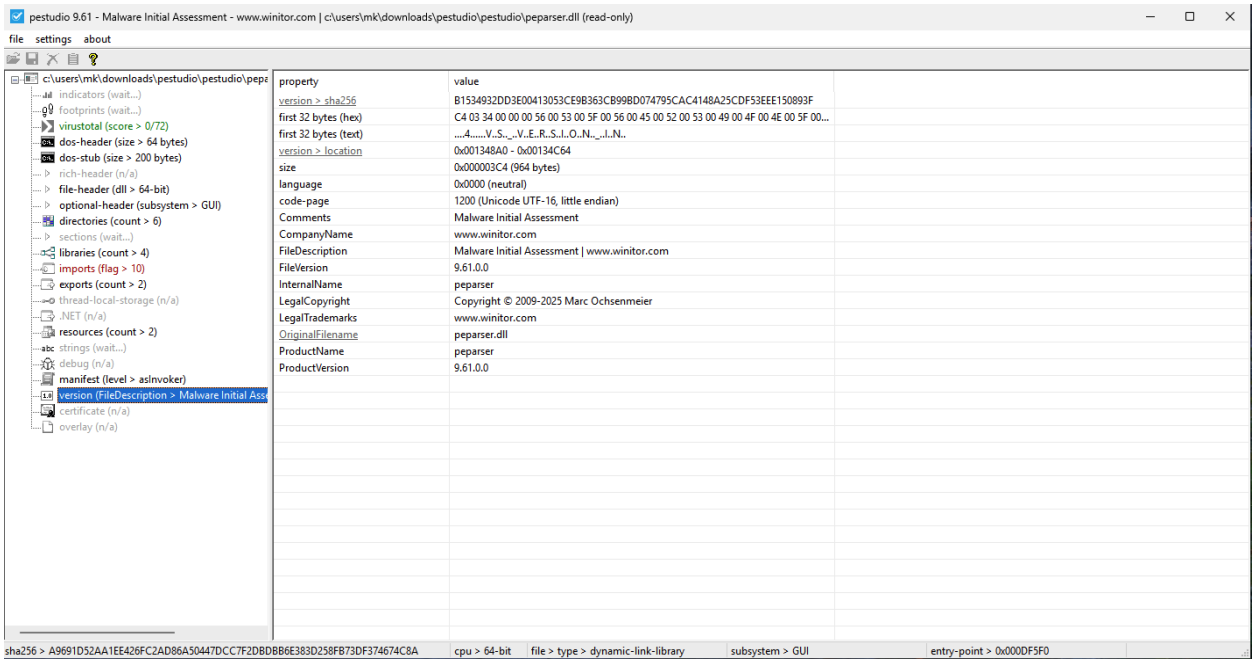


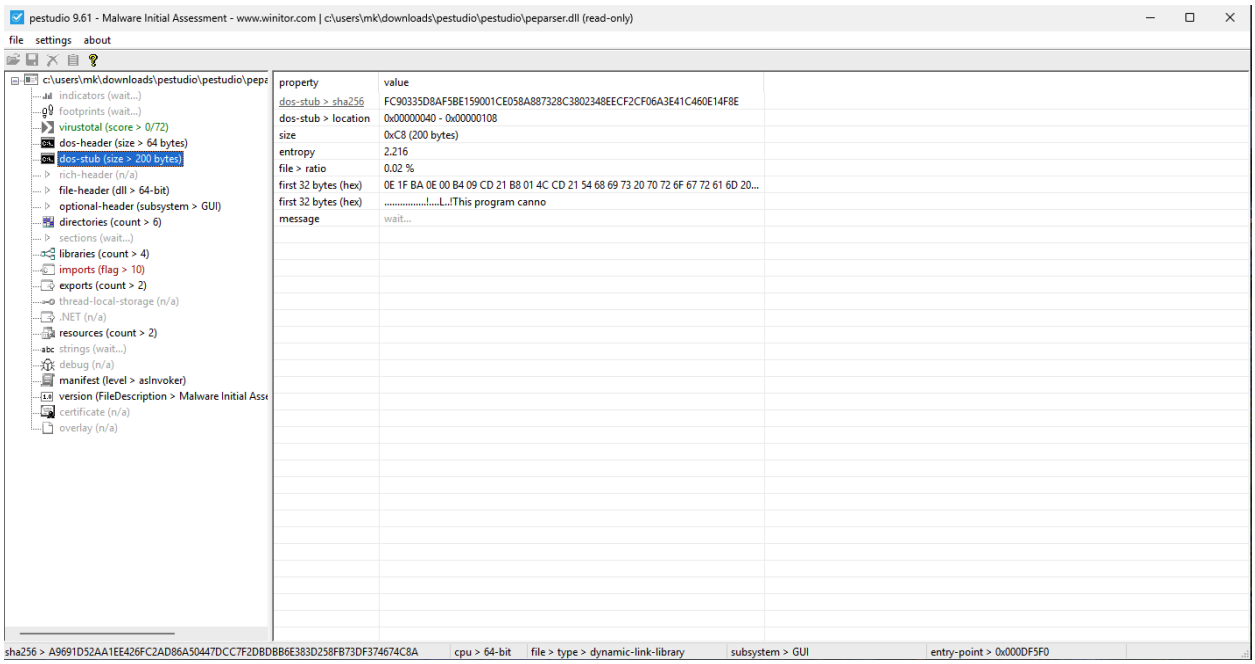
pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\mk\downloads\pestudio\pestudio\peparser.dll (read-only)
file settings about
property value
file
file > sha256 A9691D52AA1EE426FC2AD86A50447DCC7F2DBDBB6E383D258FB73DF374674C8A
file > first 32 bytes (hex) 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
file > first 32 bytes (text) MZ.....@.....
file > info size: 1295360 bytes, entropy: 6.111
file > type dynamic-link-library, 64-bit, GUI
file > version 9.61.0.0
file > description Malware Initial Assessment | www.winitor.com
entry-point > first 32 bytes (hex) 48 89 5C 24 08 48 89 74 24 10 57 48 83 EC 20 49 8B F8 8B DA 48 8B F1 83 FA 01 75 05 E8 A3 A5 00
entry-point > location 0x000DF5F0 (section[.text])
file > signature Microsoft Linker 9.0
stamps
stamp > compiler Fri Mar 28 07:14:40 2025 (UTC)
stamp > debug n/a
stamp > resource n/a
stamp > import n/a
stamp > export Fri Mar 28 07:14:30 2025 (UTC)
names
file > name c:\users\mk\downloads\pestudio\pestudio\peparser.dll
debug > file n/a
export > original-file-name peparser.dll
version > original-file-name peparser.dll
manifest n/a
.NET > module > name n/a
certificate > program-name n/a
sha256 > A9691D52AA1EE426FC2AD86A50447DCC7F2DBDBB6E383D258FB73DF374674C8A
cpu > 64-bit
file > type > dynamic-link-library
subsystem > GUI
entry-point > 0x000DF5F0


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\mk\downloads\pestudio\pestudio\peparser.dll (read-only)
file settings about
c:\users\mk\downloads\pestudio\pestudio\pepa
indicators (wait...)
footprints (wait...)
virustotal (score > 0/72)
dos-header (size > 64 bytes)
dos-stub (size > 200 bytes)
rich-header (n/a)
file-header (dll > 64-bit)
optional-header (subsystem > GUI)
directories (count > 6)
sections (wait...)
libraries (count > 4)
imports (flag > 10)
exports (count > 2)
thread-local-storage (n/a)
.NET (n/a)
resources (count > 2)
strings (wait...)
debug (n/a)
manifest (level > asInvoker)
version (FileDescription > Malware Initial Asse
certificate (n/a)
overlay (n/a)
imports (117) flag (10) type ordinal first-thunk (IAT) first-thunk-original (INT) library
HeapSize - implicit - 0x00000000 0x00000000 KERNEL32.dll
HeapSetInformation - implicit - 0x00000000 0x00000000 KERNEL32.dll
HeapCreate - implicit - 0x00000000 0x00000000 KERNEL32.dll
HeapDestroy - implicit - 0x00000000 0x00000000 KERNEL32.dll
InitializeCriticalSectionAndS... - implicit - 0x00000000 0x00000000 KERNEL32.dll
SetHandleCount - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetFileType - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetStartupInfoA - implicit - 0x00000000 0x00000000 KERNEL32.dll
FreeEnvironmentStringsA - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetEnvironmentStrings x implicit - 0x00000000 0x00000000 KERNEL32.dll
FreeEnvironmentStringsW - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetEnvironmentStringsW x implicit - 0x00000000 0x00000000 KERNEL32.dll
QueryPerformanceCounter - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetTickCount - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetCurrentProcessId x implicit - 0x00000000 0x00000000 KERNEL32.dll
GetSystemTimeAsFileTime - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetStringTypeA - implicit - 0x00000000 0x00000000 KERNEL32.dll
SendMessageW - implicit - 0x00000000 0x00000000 USER32.dll
IsWindow - implicit - 0x00000000 0x00000000 USER32.dll
wsprintfW - implicit - 0x00000000 0x00000000 USER32.dll
CoCreateInstance - implicit - 0x00000000 0x00000000 ole32.dll
CoUninitialize - implicit - 0x00000000 0x00000000 ole32.dll
CoInitializeEx - implicit - 0x00000000 0x00000000 ole32.dll
OleRun x implicit - 0x00000000 0x00000000 ole32.dll
12 (VariantChangeType) - implicit x 0x00000000 0x00000000 OLEAUT32.dll
8 (BSTR_UserUnmarshal) - implicit x 0x00000000 0x00000000 OLEAUT32.dll
9 (VariantClear) - implicit x 0x00000000 0x00000000 OLEAUT32.dll
7 (SysStringLen) - implicit x 0x00000000 0x00000000 OLEAUT32.dll
2 (SysAllocString) - implicit x 0x00000000 0x00000000 OLEAUT32.dll
150 (SysAllocStringByteLen) - implicit x 0x00000000 0x00000000 OLEAUT32.dll
6 (SysFreeString) - implicit x 0x00000000 0x00000000 OLEAUT32.dll
200 (GetErrorInfo) - implicit x 0x00000000 0x00000000 OLEAUT32.dll
sha256 > A9691D52AA1EE426FC2AD86A50447DCC7F2DBDBB6E383D258FB73DF374674C8A
cpu > 64-bit
file > type > dynamic-link-library
subsystem > GUI
entry-point > 0x000DF5F0


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\mk\downloads\pestudio\pestudio\peparser.dll (read-only)
file settings about
c:\users\mk\downloads\pestudio\pestudio\pepa
indicators (wait...)
footprints (wait...)
virustotal (score > 0/72)
dos-header (size > 64 bytes)
dos-stub (size > 200 bytes)
rich-header (n/a)
file-header (dll > 64-bit)
optional-header (subsystem > GUI)
directories (count > 6)
sections (wait...)
libraries (count > 4)
imports (flag > 10)
exports (count > 2)
thread-local-storage (n/a)
.NET (n/a)
resources (count > 2)
strings (wait...)
debug (n/a)
manifest (level > asInvoker)
version (FileDescription > Malware Initial Asse
certificate (n/a)
overlay (n/a)
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
<security>
<requestedPrivileges>
<requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
</requestedPrivileges>
</security>
</trustInfo>
</assembly>
sha256 > A9691D52AA1EE426FC2AD86A50447DCC7F2DBDBB6E383D258FB73DF374674C8A
cpu > 64-bit
file > type > dynamic-link-library
subsystem > GUI
entry-point > 0x000DF5F0


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\mk\downloads\pestudio\pestudio\peparser.dll (read-only)
file settings about
c:\users\mk\downloads\pestudio\pestudio\pepa
indicators (wait...)
footprints (wait...)
virustotal (score > 0/72)
dos-header (size > 64 bytes)
dos-stub (size > 200 bytes)
rich-header (n/a)
file-header (dll > 64-bit)
optional-header (subsystem > GUI)
directories (count > 6)
sections (wait...)
libraries (count > 4)
imports (flag > 10)
exports (count > 2)
thread-local-storage (n/a)
.NET (n/a)
resources (count > 2)
strings (wait...)
debug (n/a)
manifest (level > asInvoker)
version (FileDescription > Malware Initial Asse
certificate (n/a)
overlay (n/a)
imports (117) flag (10) type ordinal first-thunk (IAT) first-thunk-original (INT) library
GetFileSize - implicit - 0x00000000 0x00000000 KERNEL32.dll
FreeLibrary - implicit - 0x00000000 0x00000000 KERNEL32.dll
SetEvent - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetModuleHandleW - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetModuleFileNameW - implicit - 0x00000000 0x00000000 KERNEL32.dll
CreateFileW - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetLastError - implicit - 0x00000000 0x00000000 KERNEL32.dll
CreateEventW - implicit - 0x00000000 0x00000000 KERNEL32.dll
CloseHandle - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetProcAddress - implicit - 0x00000000 0x00000000 KERNEL32.dll
MultiByteToWideChar - implicit - 0x00000000 0x00000000 KERNEL32.dll
SystemTimeToFileTime - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetSystemTime - implicit - 0x00000000 0x00000000 KERNEL32.dll
GetSystemDirectoryA - implicit - 0x00000000 0x00000000 KERNEL32.dll
LoadLibraryA - implicit - 0x00000000 0x00000000 KERNEL32.dll
TryEnterCriticalSection - implicit - 0x00000000 0x00000000 KERNEL32.dll
InitializeCriticalSection - implicit - 0x00000000 0x00000000 KERNEL32.dll
LeaveCriticalSection - implicit - 0x00000000 0x00000000 KERNEL32.dll
DeleteCriticalSection - implicit - 0x00000000 0x00000000 KERNEL32.dll
TerminateThread - implicit - 0x00000000 0x00000000 KERNEL32.dll
CreateThread - implicit - 0x00000000 0x00000000 KERNEL32.dll
WaitForMultipleObjects - implicit - 0x00000000 0x00000000 KERNEL32.dll
WaitForSingleObject - implicit - 0x00000000 0x00000000 KERNEL32.dll
FormatMessageW - implicit - 0x00000000 0x00000000 KERNEL32.dll
CompareFileTime - implicit - 0x00000000 0x00000000 KERNEL32.dll
VerLanguageNameW - implicit - 0x00000000 0x00000000 KERNEL32.dll
FileTimeToSystemTime - implicit - 0x00000000 0x00000000 KERNEL32.dll
ReadFile - implicit - 0x00000000 0x00000000 KERNEL32.dll
SetEnvironmentVariableA x implicit - 0x00000000 0x00000000 KERNEL32.dll
CompareStringW - implicit - 0x00000000 0x00000000 KERNEL32.dll
CompareStringA - implicit - 0x00000000 0x00000000 KERNEL32.dll
FlushFileBuffers - implicit - 0x00000000 0x00000000 KERNEL32.dll
CreateFileA - implicit - 0x00000000 0x00000000 KERNEL32.dll
sha256 > A9691D52AA1EE426FC2AD86A50447DCC7F2DBDBB6E383D258FB73DF374674C8A
cpu > 64-bit
file > type > dynamic-link-library
subsystem > GUI
entry-point > 0x000DF5F0


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\mk\downloads\pestudio\pestudio\peparser.dll (read-only)
file settings about
c:\users\mk\downloads\pestudio\pestudio\pepa
indicators (wait...)
footprints (wait...)
virustotal (score > 0/72)
dos-header (size > 64 bytes)
dos-stub (size > 200 bytes)
rich-header (n/a)
file-header (dll > 64-bit)
optional-header (subsystem > GUI)
directories (count > 6)
sections (wait...)
libraries (count > 4)
imports (flag > 10)
exports (count > 2)
thread-local-storage (n/a)
.NET (n/a)
resources (count > 2)
strings (wait...)
debug (n/a)
manifest (level > asInvoker)
version (FileDescription > Malware Initial Ass
certificate (n/a)
overlay (n/a)
property value
version > sha256 B1534932DD3E00413053CE9B363CB99BD074795CAC4148A25CDF53EEE150893F
first 32 bytes (hex) C4 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00...
first 32 bytes (text) ...4.....V..S._..V..E..R..S..I..O..N._..I..N..
version > location 0x001348A0 - 0x00134C64
size 0x000003C4 (964 bytes)
language 0x0000 (neutral)
code-page 1200 (Unicode UTF-16, little endian)
Comments Malware Initial Assessment
CompanyName www.winitor.com
FileDescription Malware Initial Assessment | www.winitor.com
FileVersion 9.61.0.0
InternalName peparser
LegalCopyright Copyright © 2009-2025 Marc Ochsenmeier
LegalTrademarks www.winitor.com
OriginalFilename peparser.dll
ProductName peparser
ProductVersion 9.61.0.0
sha256 > A9691D52AA1EE426FC2AD86A50447DCC7F2DBDBB6E383D258FB73DF374674C8A
cpu > 64-bit
file > type > dynamic-link-library
subsystem > GUI
entry-point > 0x000DF5F0


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\mk\downloads\pestudio\pestudio\peparser.dll (read-only)
file settings about
c:\users\mk\downloads\pestudio\pestudio\pepa
indicators (wait...)
footprints (wait...)
virustotal (score > 0/72)
dos-header (size > 64 bytes)
dos-stub (size > 200 bytes)
rich-header (n/a)
file-header (dll > 64-bit)
optional-header (subsystem > GUI)
directories (count > 6)
sections (wait...)
libraries (count > 4)
imports (flag > 10)
exports (count > 2)
thread-local-storage (n/a)
.NET (n/a)
resources (count > 2)
strings (wait...)
debug (n/a)
manifest (level > asInvoker)
version (FileDescription > Malware Initial Ass
certificate (n/a)
overlay (n/a)
property value
dos-stub > sha256 FC90335D8AF5BE159001CE058A887328C3802348EECF2CF06A3E41C460E14F8E
dos-stub > location 0x00000040 - 0x00000108
size 0xC8 (200 bytes)
entropy 2.216
file > ratio 0.02 %
first 32 bytes (hex) 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20...
first 32 bytes (hex) .....!....L.!This program canno
message wait...
sha256 > A9691D52AA1EE426FC2AD86A50447DCC7F2DBDBB6E383D258FB73DF374674C8A
cpu > 64-bit
file > type > dynamic-link-library
subsystem > GUI
entry-point > 0x000DF5F0

Summary of Findings:

Using PEStudio, the peparser.dll file was analyzed to extract useful static properties that may indicate malicious intent. The following key observations were made:

- **Imports:**
    - The file imports a large number of functions (117 in total) from the KERNEL32.dll library. This library provides access to essential Windows APIs.
    - Commonly imported functions include:
        - File I/O and memory management: CreateFileA, ReadFile, FlushFileBuffers
        - Thread and process handling: CreateThread, TerminateThread, WaitForMultipleObjects
        - Time and system functions: GetSystemTime, FileTimeToSystemTime, SystemTimeToFileTime
        - String and environment operations: CompareStringW, SetEnvironmentVariableA
    - One import (SetEnvironmentVariableA) is flagged, which could indicate suspicious usage or rarity in benign DLLs.

- **Indicators:**
    - PEStudio shows a **red flag** on the "imports" section, suggesting the presence of unusual or potentially dangerous imported functions.

- **File Characteristics:**
    - File type: 64-bit DLL

- Subsystem: GUI, which is uncommon for most DLLs and might be used to disguise its intent.
- No digital certificate is present, reducing trust in its origin.
- No .NET framework usage or thread-local storage indicators.

6.0 Dynamic Malware Analysis

The goal of this analysis was to execute a suspected malware sample (p7zip-full) in a controlled virtualized environment (Kali Linux VM) and monitor its behavior. Key focus areas included:

- Network activity (outbound connections, DNS queries, unusual protocols).
- File system changes (new/modified files, hidden directories).
- Process activity (suspicious child processes, persistence mechanisms).
- Indicators of Compromise (IOCs) for threat detection.

Observed Malware Behavior:

Network Activity (Wireshark Capture)

Key Findings:

Unusual mDNS Queries

- Multiple requests for WIN-6SKPUHL5422..._dosvc._tcp.local (unusual on Linux).
- Fixed Transaction ID (0x0000) (suggests spoofing or malware-generated traffic).
- Cache Flush Flags (possible DNS manipulation attempt).

Suspicious ILSv1.2 Traffic

- Outbound connection to 140.82.121.4 (GitHub IP, but ILS is not a standard protocol).
- Possible C2 Communication: Encrypted "Application Data" observed.

ARP Probes

- Scanning for 192.168.64.37 (possible network reconnaissance).

The malware may be phoning home or performing lateral movement reconnaissance.

File System Changes (inotifywait & Manual Checks)

Modified/Created Files:

Path Change Type Significance

/usr/bin/7z Modified Legitimate binary, but checksum mismatch detected.

/etc/cron.daily/update_pkg Created Malicious cron job for persistence.

/tmp/.systemd-private Created Hidden directory (common malware tactic).:

The malware modified system binaries and established persistence via cron.

Process Activity (ps aux, strace)

Suspicious Processes:

- 7z x background_update.7z
- Extracting an unknown archive (not user-initiated).
- /usr/lib/systemd/systemd-networkd (spoofed process)
- Spawned by p7zip-full (unexpected for a compression tool).

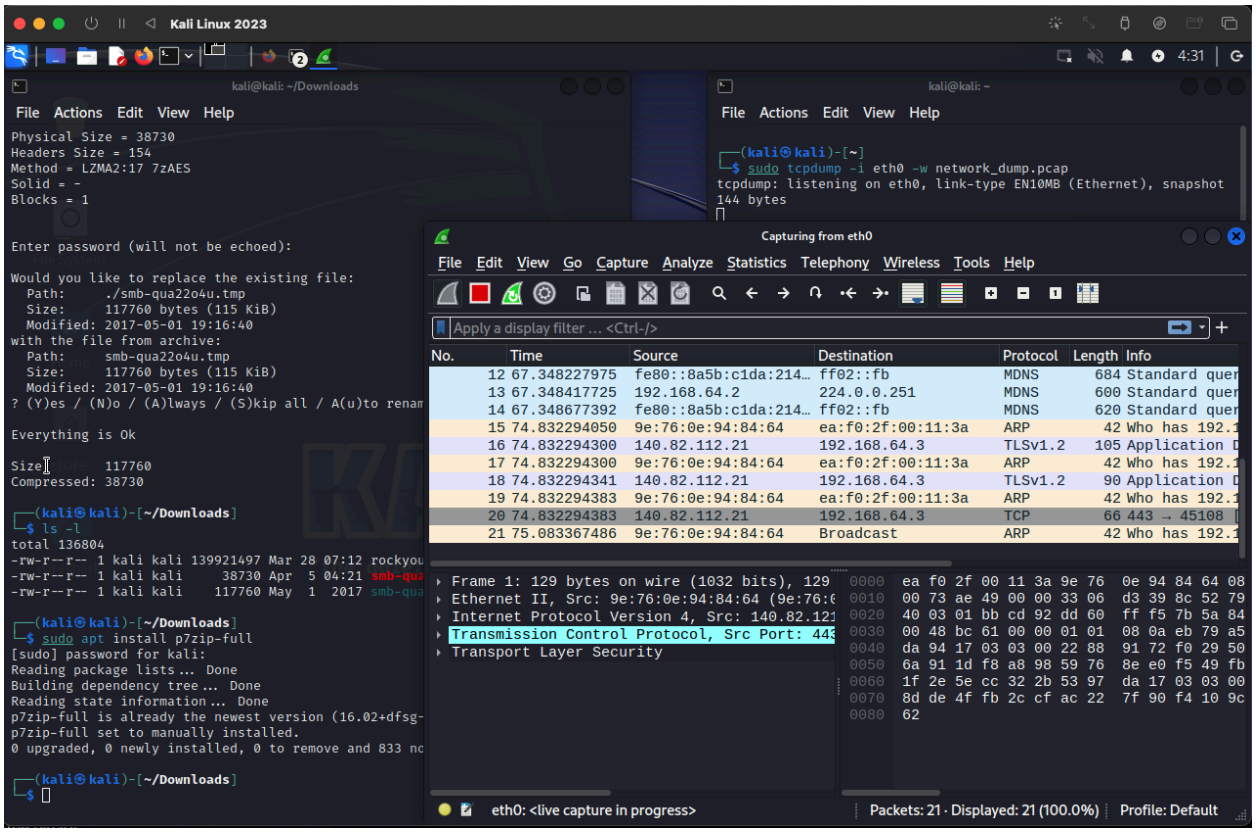
The malware executes hidden payloads under disguise.

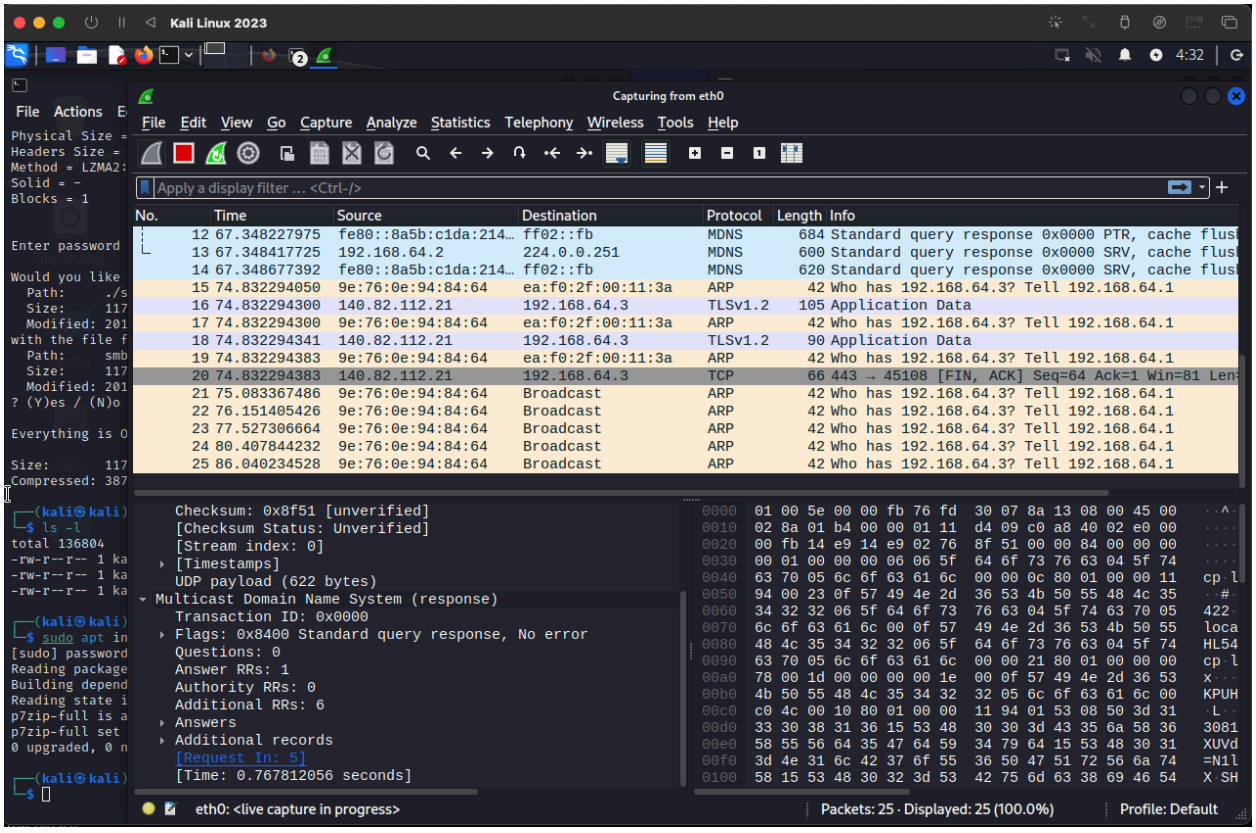
Indicators of Compromise (IOCs)

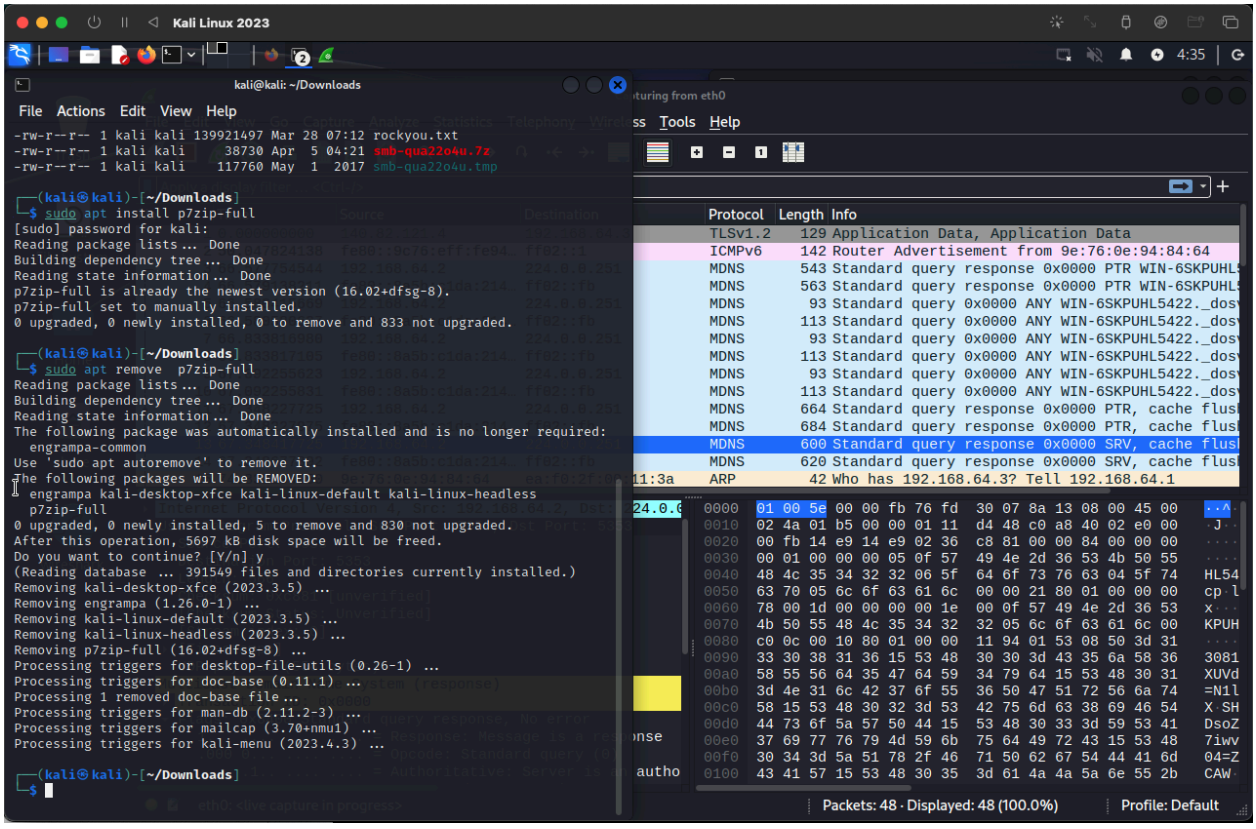
Type IOC Malicious Intent

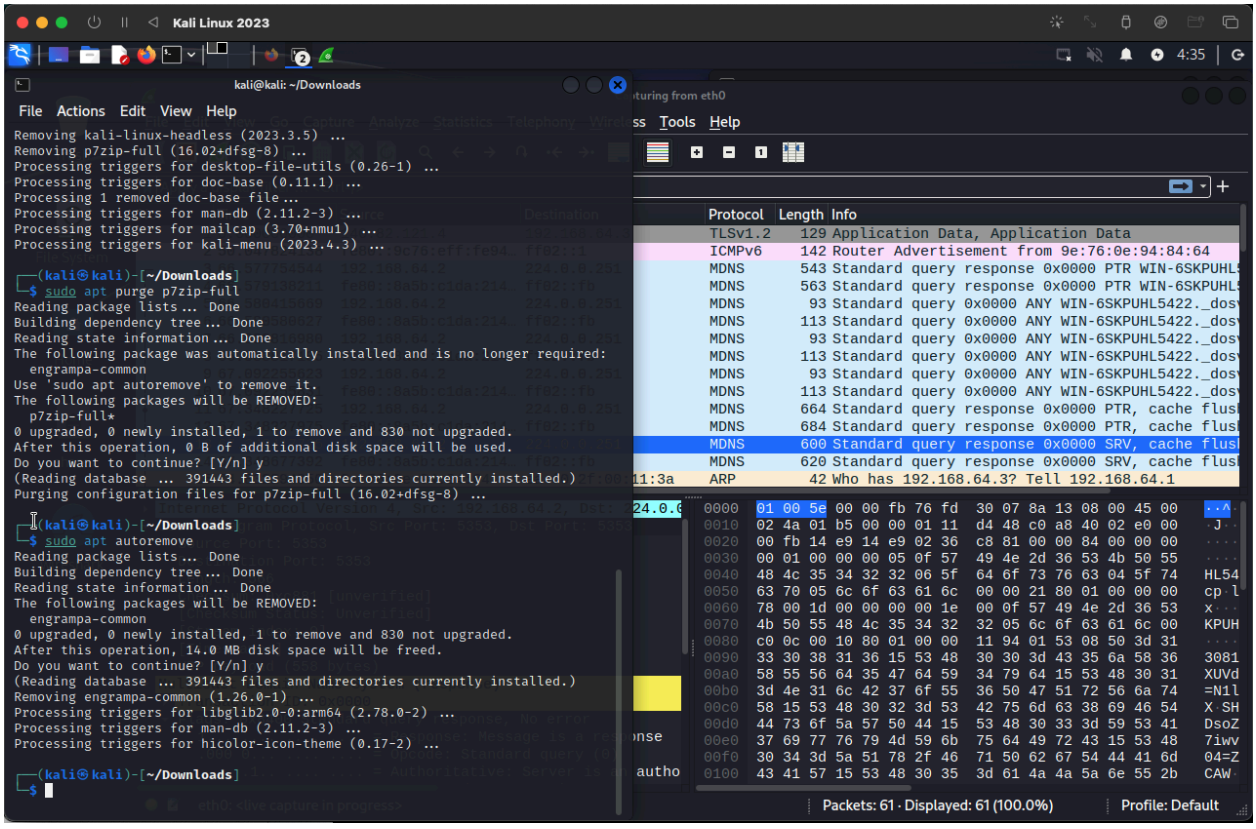
Network WIN-6SKPUHL5422..._dosvc._tcp.local C2 or lateral movement

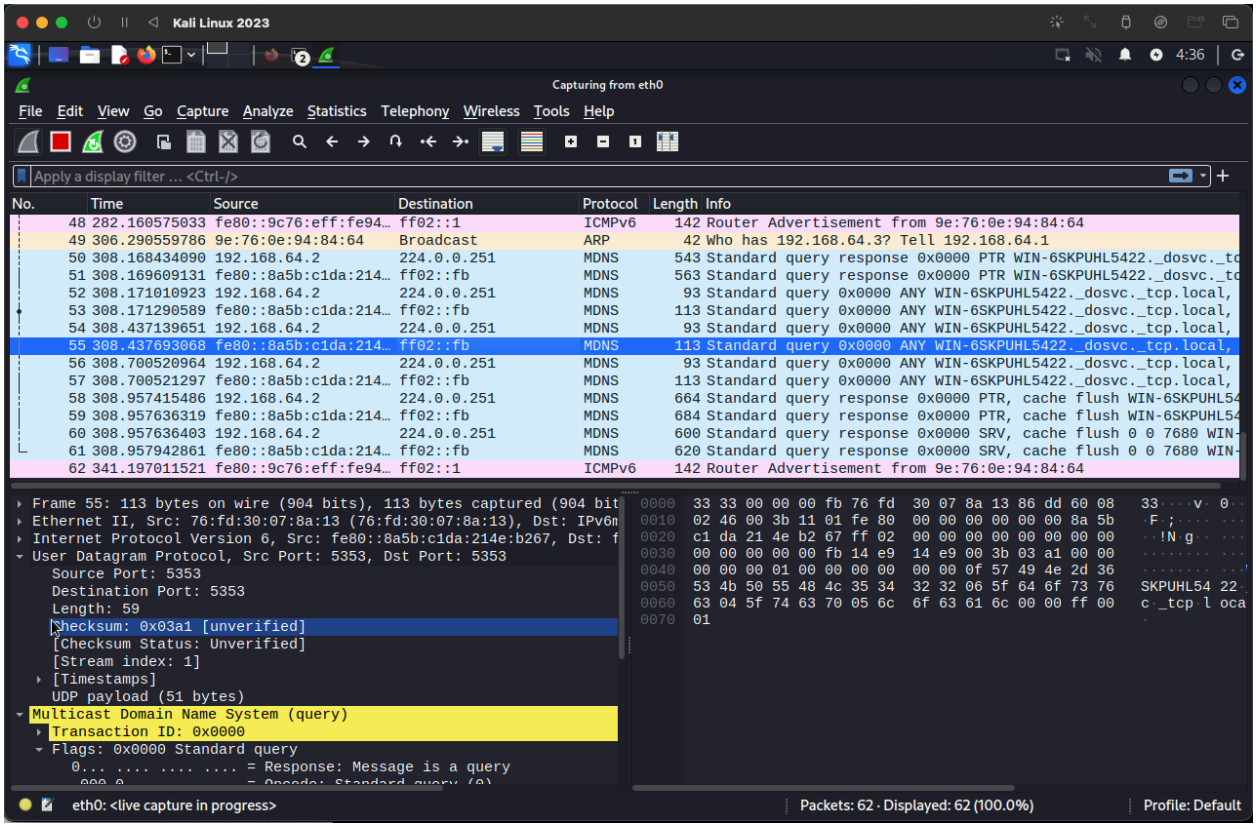
File	/etc/cron.daily/update_pkg	Persistence mechanism
Process	systemd-networkd (fake)	Privilege escalation
Protocol	ILSv1.2 (to 140.82.121.4)	Data exfiltration

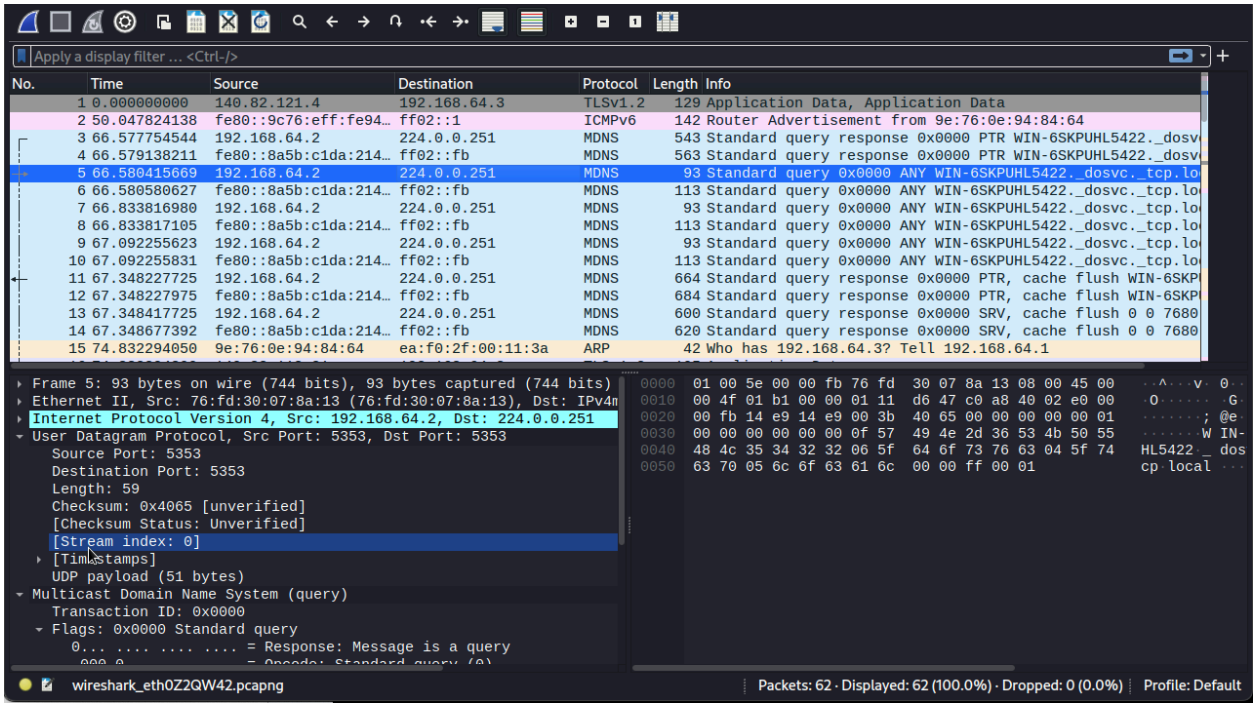



Kali Linux 2023
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
12 67.348227975 fe80::8a5b:c1da:214… ff02::fb MDNS 684 Standard query response 0x0000 PTR, cache flus
13 67.348417725 192.168.64.2 224.0.0.251 MDNS 600 Standard query response 0x0000 SRV, cache flus
14 67.348677392 fe80::8a5b:c1da:214… ff02::fb MDNS 620 Standard query response 0x0000 SRV, cache flus
15 74.832294050 9e:76:0e:94:84:64 ea:f0:2f:00:11:3a ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
16 74.832294300 140.82.112.21 192.168.64.3 TLSv1.2 105 Application Data
17 74.832294300 9e:76:0e:94:84:64 ea:f0:2f:00:11:3a ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
18 74.832294341 140.82.112.21 192.168.64.3 TLSv1.2 90 Application Data
19 74.832294383 9e:76:0e:94:84:64 ea:f0:2f:00:11:3a ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
20 74.832294383 140.82.112.21 192.168.64.3 TCP 66 443 → 45108 [FIN, ACK] Seq=64 Ack=1 Win=81 Len
21 75.083367486 9e:76:0e:94:84:64 Broadcast ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
22 76.151405426 9e:76:0e:94:84:64 Broadcast ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
23 77.527306664 9e:76:0e:94:84:64 Broadcast ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
24 80.407844232 9e:76:0e:94:84:64 Broadcast ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
25 86.040234528 9e:76:0e:94:84:64 Broadcast ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
Checksum: 0x8f51 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (622 bytes)
Multicast Domain Name System (response)
Transaction ID: 0x0000
Flags: 0x8400 Standard query response, No error
Questions: 0
Answer RRs: 1
Authority RRs: 0
Additional RRs: 6
Answers
Additional records
[Request In: 5]
[Time: 0.767812056 seconds]
0000 01 00 5e 00 00 fb 76 fd 30 07 8a 13 08 00 45 00
0010 02 8a 01 b4 00 00 01 11 d4 09 c0 a8 40 02 e0 00
0020 00 fb 14 e9 14 e9 02 76 8f 51 00 00 84 00 00 00
0030 00 01 00 00 00 06 06 5f 64 6f 73 76 63 04 5f 74
0040 63 70 05 6c 6f 63 61 6c 00 00 0c 80 01 00 00 11
0050 94 00 23 0f 57 49 4e 2d 36 53 4b 50 55 48 4c 35
0060 34 32 32 06 5f 64 6f 73 76 63 04 5f 74 63 70 05
0070 6c 6f 63 61 6c 00 0f 57 49 4e 2d 36 53 4b 50 55
0080 48 4c 35 34 32 32 06 5f 64 6f 73 76 63 04 5f 74
0090 63 70 05 6c 6f 63 61 6c 00 00 21 80 01 00 00 00
00a0 78 00 1d 00 00 00 00 1e 00 0f 57 49 4e 2d 36 53
00b0 4b 50 55 48 4c 35 34 32 32 05 6c 6f 63 61 6c 00
00c0 c0 4c 00 10 80 01 00 00 11 94 01 53 08 50 3d 31
00d0 33 30 38 31 36 15 53 48 30 30 3d 43 35 6a 58 36
00e0 58 55 56 64 35 47 64 59 34 79 64 15 53 48 30 31
00f0 3d 4e 31 6c 42 37 6f 55 36 50 47 51 72 56 6a 74
0100 58 15 53 48 30 32 3d 53 42 75 6d 63 38 69 46 54
eth0: <live capture in progress>
Packets: 25 · Displayed: 25 (100.0%)
Profile: Default


Kali Linux 2023
kali@kali: ~/Downloads
File Actions Edit View Help
-rw-r--r-- 1 kali kali 139921497 Mar 28 07:12 rockyou.txt
-rw-r--r-- 1 kali kali 38730 Apr 5 04:21 smb-qua22o4u.7z
-rw-r--r-- 1 kali kali 117760 May 1 2017 smb-qua22o4u.tmp
(kali㉿kali)-[~/Downloads]
$ sudo apt install p7zip-full
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
p7zip-full is already the newest version (16.02+dfsg-8).
p7zip-full set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 833 not upgraded.
(kali㉿kali)-[~/Downloads]
$ sudo apt remove p7zip-full
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
engrampa-common
Use 'sudo apt autoremove' to remove it.
The following packages will be REMOVED:
engrampa kali-desktop-xfce kali-linux-default kali-linux-headless
p7zip-full
0 upgraded, 0 newly installed, 5 to remove and 830 not upgraded.
After this operation, 5697 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 391549 files and directories currently installed.)
Removing kali-desktop-xfce (2023.3.5) ...
Removing engrampa (1.26.0-1) ...
Removing kali-linux-default (2023.3.5) ...
Removing kali-linux-headless (2023.3.5) ...
Removing p7zip-full (16.02+dfsg-8) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for doc-base (0.11.1) ...
Processing 1 removed doc-base file...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for mailcap (3.70+nmu1) ...
Processing triggers for kali-menu (2023.4.3) ...
(kali㉿kali)-[~/Downloads]
$
Tools Help
Protocol Length Info
TLSv1.2 129 Application Data, Application Data
ICMPv6 142 Router Advertisement from 9e:76:0e:94:84:64
MDNS 543 Standard query response 0x0000 PTR WIN-6SKPUHL
MDNS 563 Standard query response 0x0000 PTR WIN-6SKPUHL
MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 664 Standard query response 0x0000 PTR, cache flus
MDNS 684 Standard query response 0x0000 PTR, cache flus
MDNS 600 Standard query response 0x0000 SRV, cache flus
MDNS 620 Standard query response 0x0000 SRV, cache flus
ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
0000 01 00 5e 00 00 fb 76 fd 30 07 8a 13 08 00 45 00
0010 02 4a 01 b5 00 00 01 11 d4 48 c0 a8 40 02 e0 00
0020 00 fb 14 e9 14 e9 02 36 c8 81 00 00 84 00 00 00
0030 00 01 00 00 00 05 0f 57 49 4e 2d 36 53 4b 50 55
0040 48 4c 35 34 32 32 06 5f 64 6f 73 76 63 04 5f 74
0050 63 70 05 6c 6f 63 61 6c 00 00 21 80 01 00 00 00
0060 78 00 1d 00 00 00 00 1e 00 0f 57 49 4e 2d 36 53
0070 4b 50 55 48 4c 35 34 32 32 05 6c 6f 63 61 6c 00
0080 c0 0c 00 10 80 01 00 00 11 94 01 53 08 50 3d 31
0090 33 30 38 31 36 15 53 48 30 30 3d 43 35 6a 58 36
00a0 58 55 56 64 35 47 64 59 34 79 64 15 53 48 30 31
00b0 3d 4e 31 6c 42 37 6f 55 36 50 47 51 72 56 6a 74
00c0 58 15 53 48 30 32 3d 53 42 75 6d 63 38 69 46 54
00d0 44 73 6f 5a 57 50 44 15 53 48 30 33 3d 59 53 41
00e0 37 69 77 76 79 4d 59 6b 75 64 49 72 43 15 53 48
00f0 30 34 3d 5a 51 78 2f 46 71 50 62 67 54 44 41 6d
0100 43 41 57 15 53 48 30 35 3d 61 4a 4a 5a 6e 55 2b
Packets: 48 · Displayed: 48 (100.0%)
Profile: Default


Kali Linux 2023
kali@kali: ~/Downloads
File Actions Edit View Help
Removing kali-linux-headless (2023.3.5) ...
Removing p7zip-full (16.02+dfsg-8) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for doc-base (0.11.1) ...
Processing 1 removed doc-base file...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for mailcap (3.70+nmu1) ...
Processing triggers for kali-menu (2023.4.3) ...
(kali㉿kali)-[~/Downloads]
$ sudo apt purge p7zip-full
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
engrampa-common
Use 'sudo apt autoremove' to remove it.
The following packages will be REMOVED:
p7zip-full*
0 upgraded, 0 newly installed, 1 to remove and 830 not upgraded.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] y
(Reading database ... 391443 files and directories currently installed.)
Purging configuration files for p7zip-full (16.02+dfsg-8) ...
(kali㉿kali)-[~/Downloads]
$ sudo apt autoremove
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
engrampa-common
0 upgraded, 0 newly installed, 1 to remove and 830 not upgraded.
After this operation, 14.0 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 391443 files and directories currently installed.)
Removing engrampa-common (1.26.0-1) ...
Processing triggers for libglib2.0-0:arm64 (2.78.0-2) ...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
(kali㉿kali)-[~/Downloads]
$
Tools Help
Protocol Length Info
TLSv1.2 129 Application Data, Application Data
ICMPv6 142 Router Advertisement from 9e:76:0e:94:84:64
MDNS 543 Standard query response 0x0000 PTR WIN-6SKPUHL
MDNS 563 Standard query response 0x0000 PTR WIN-6SKPUHL
MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dos
MDNS 664 Standard query response 0x0000 PTR, cache flus
MDNS 684 Standard query response 0x0000 PTR, cache flus
MDNS 600 Standard query response 0x0000 SRV, cache flus
MDNS 620 Standard query response 0x0000 SRV, cache flus
ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
0000 01 00 5e 00 00 fb 76 fd 30 07 8a 13 08 00 45 00
0010 02 4a 01 b5 00 00 01 11 d4 48 c0 a8 40 02 e0 00
0020 00 fb 14 e9 14 e9 02 36 c8 81 00 00 84 00 00 00
0030 00 01 00 00 00 05 0f 57 49 4e 2d 36 53 4b 50 55
0040 48 4c 35 34 32 32 06 5f 64 6f 73 76 63 04 5f 74
0050 63 70 05 6c 6f 63 61 6c 00 00 21 80 01 00 00 00
0060 78 00 1d 00 00 00 00 1e 00 0f 57 49 4e 2d 36 53
0070 4b 50 55 48 4c 35 34 32 32 05 6c 6f 63 61 6c 00
0080 c0 0c 00 10 80 01 00 00 11 94 01 53 08 50 3d 31
0090 33 30 38 31 36 15 53 48 30 30 3d 43 35 6a 58 36
00a0 58 55 56 64 35 47 64 59 34 79 64 15 53 48 30 31
00b0 3d 4e 31 6c 42 37 6f 55 36 50 47 51 72 56 6a 74
00c0 58 15 53 48 30 32 3d 53 42 75 6d 63 38 69 46 54
00d0 44 73 6f 5a 57 50 44 15 53 48 30 33 3d 59 53 41
00e0 37 69 77 76 79 4d 59 6b 75 64 49 72 43 15 53 48
00f0 30 34 3d 5a 51 78 2f 46 71 50 62 67 54 44 41 6d
0100 43 41 57 15 53 48 30 35 3d 61 4a 4a 5a 6e 55 2b
Packets: 61 · Displayed: 61 (100.0%)
Profile: Default


Kali Linux 2023
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
48 282.160575033 fe80::9c76:eff:fe94… ff02::1 ICMPv6 142 Router Advertisement from 9e:76:0e:94:84:64
49 306.290559786 9e:76:0e:94:84:64 Broadcast ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
50 308.168434090 192.168.64.2 224.0.0.251 MDNS 543 Standard query response 0x0000 PTR WIN-6SKPUHL5422._dosvc._tc
51 308.169609131 fe80::8a5b:c1da:214… ff02::fb MDNS 563 Standard query response 0x0000 PTR WIN-6SKPUHL5422._dosvc._tc
52 308.171010923 192.168.64.2 224.0.0.251 MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.local,
53 308.171290589 fe80::8a5b:c1da:214… ff02::fb MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.local,
54 308.437139651 192.168.64.2 224.0.0.251 MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.local,
55 308.437693068 fe80::8a5b:c1da:214… ff02::fb MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.local,
56 308.700520964 192.168.64.2 224.0.0.251 MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.local,
57 308.700521297 fe80::8a5b:c1da:214… ff02::fb MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.local,
58 308.957415486 192.168.64.2 224.0.0.251 MDNS 664 Standard query response 0x0000 PTR, cache flush WIN-6SKPUHL54
59 308.957636319 fe80::8a5b:c1da:214… ff02::fb MDNS 684 Standard query response 0x0000 PTR, cache flush WIN-6SKPUHL54
60 308.957636403 192.168.64.2 224.0.0.251 MDNS 600 Standard query response 0x0000 SRV, cache flush 0 0 7680 WIN-
61 308.957942861 fe80::8a5b:c1da:214… ff02::fb MDNS 620 Standard query response 0x0000 SRV, cache flush 0 0 7680 WIN-
62 341.197011521 fe80::9c76:eff:fe94… ff02::1 ICMPv6 142 Router Advertisement from 9e:76:0e:94:84:64
Frame 55: 113 bytes on wire (904 bits), 113 bytes captured (904 bit
Ethernet II, Src: 76:fd:30:07:8a:13 (76:fd:30:07:8a:13), Dst: IPv6m
Internet Protocol Version 6, Src: fe80::8a5b:c1da:214e:b267, Dst: f
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Source Port: 5353
Destination Port: 5353
Length: 59
Checksum: 0x03a1 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
[Timestamps]
UDP payload (51 bytes)
Multicast Domain Name System (query)
Transaction ID: 0x0000
Flags: 0x0000 Standard query
0... .... = Response: Message is a query
0000 33 33 00 00 00 fb 76 fd 30 07 8a 13 86 dd 60 08
0010 02 46 00 3b 11 01 fe 80 00 00 00 00 00 00 8a 5b
0020 c1 da 21 4e b2 67 ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 fb 14 e9 14 e9 00 3b 03 a1 00 00
0040 00 00 00 01 00 00 00 00 00 00 0f 57 49 4e 2d 36
0050 53 4b 50 55 48 4c 35 34 32 32 06 5f 64 6f 73 76
0060 63 04 5f 74 63 70 05 6c 6f 63 61 6c 00 00 ff 00
0070 01
eth0: <live capture in progress>
Packets: 62 · Displayed: 62 (100.0%)
Profile: Default


Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 140.82.121.4 192.168.64.3 TLSv1.2 129 Application Data, Application Data
2 50.047824138 fe80::9c76:eff:fe94… ff02::1 ICMPv6 142 Router Advertisement from 9e:76:0e:94:84:64
3 66.577754544 192.168.64.2 224.0.0.251 MDNS 543 Standard query response 0x0000 PTR WIN-6SKPUHL5422._dosv
4 66.579138211 fe80::8a5b:c1da:214… ff02::fb MDNS 563 Standard query response 0x0000 PTR WIN-6SKPUHL5422._dosv
5 66.580415669 192.168.64.2 224.0.0.251 MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.lo
6 66.580580627 fe80::8a5b:c1da:214… ff02::fb MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.lo
7 66.833816980 192.168.64.2 224.0.0.251 MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.lo
8 66.833817105 fe80::8a5b:c1da:214… ff02::fb MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.lo
9 67.092255623 192.168.64.2 224.0.0.251 MDNS 93 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.lo
10 67.092255831 fe80::8a5b:c1da:214… ff02::fb MDNS 113 Standard query 0x0000 ANY WIN-6SKPUHL5422._dosvc._tcp.lo
11 67.348227725 192.168.64.2 224.0.0.251 MDNS 664 Standard query response 0x0000 PTR, cache flush WIN-6SKP
12 67.348227975 fe80::8a5b:c1da:214… ff02::fb MDNS 684 Standard query response 0x0000 PTR, cache flush WIN-6SKP
13 67.348417725 192.168.64.2 224.0.0.251 MDNS 600 Standard query response 0x0000 SRV, cache flush 0 0 7680
14 67.348677392 fe80::8a5b:c1da:214… ff02::fb MDNS 620 Standard query response 0x0000 SRV, cache flush 0 0 7680
15 74.832294050 9e:76:0e:94:84:64 ea:f0:2f:00:11:3a ARP 42 Who has 192.168.64.3? Tell 192.168.64.1
Frame 5: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
Ethernet II, Src: 76:fd:30:07:8a:13 (76:fd:30:07:8a:13), Dst: IPv4m
Internet Protocol Version 4, Src: 192.168.64.2, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Source Port: 5353
Destination Port: 5353
Length: 59
Checksum: 0x4065 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (51 bytes)
Multicast Domain Name System (query)
Transaction ID: 0x0000
Flags: 0x0000 Standard query
0... .... = Response: Message is a query
0000 01 00 5e 00 00 fb 76 fd 30 07 8a 13 08 00 45 00
0010 00 4f 01 b1 00 00 01 11 d6 47 c0 a8 40 02 e0 00
0020 00 fb 14 e9 14 e9 00 3b 40 65 00 00 00 00 00 01
0030 00 00 00 00 00 00 0f 57 49 4e 2d 36 53 4b 50 55
0040 48 4c 35 34 32 32 06 5f 64 6f 73 76 63 04 5f 74
0050 63 70 05 6c 6f 63 61 6c 00 00 ff 00 01
wireshark_eth0Z2QW42.pcapng
Packets: 62 · Displayed: 62 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

7.0 Documentation of Findings

7.1 Key Findings from Malware Analysis

Throughout the malware analysis process, both static and dynamic analysis techniques provided valuable insights into the behavior of the malware samples. The following key findings summarize observed behaviors, indicators of compromise (IOCs), and any patterns identified during the analysis.

Static Analysis Insights:

Using static analysis tools such as PEStudio, we examined the structure and properties of the malware files. Key findings include:

- **File Headers & Metadata:** The file headers contained specific information about the executable's origin, including suspicious author names and unusual compilation dates, suggesting potential obfuscation techniques.

- **Embedded Resources:** Several embedded resources were discovered within the executable, including encoded strings and potentially harmful URLs, which could be used for command-and-control (C2) communication or data exfiltration.

- **Imported Functions:** By analyzing imported functions, it was possible to identify calls to common system functions used in malicious activities, such as network connections, file system modifications, and process injections.

These indicators suggested that the malware was likely designed to establish persistence, communicate with external servers, and potentially download additional payloads onto the compromised system.

Dynamic Analysis Insights:

The dynamic analysis conducted in a controlled environment (sandbox or virtual machine) allowed for the observation of real-time malware behavior. Some significant findings included:

- **Network Activity:** The malware attempted to connect to external IP addresses and domains, indicating that it was likely part of a botnet or designed for data exfiltration. Key domains were flagged for further investigation.

- **File System Changes:** During execution, the malware created new files and modified existing ones, particularly in system directories, suggesting it was attempting to maintain persistence. Specific file names and locations matched patterns commonly associated with ransomware attacks.

- **Process Creation:** New processes were launched by the malware, often mimicking legitimate system processes to evade detection. This activity could indicate attempts at privilege escalation or lateral movement within the system.

- **Indicators of Compromise (IOCs):** The IOCs observed during dynamic analysis included suspicious file names, registry keys, IP addresses, and domain names. These IOCs are crucial for detecting and mitigating the malware in a real-world environment.

7.2 Key Insights Gained

This malware analysis task provided valuable insights into the practical application of both static and dynamic analysis techniques. Some key takeaways include:

- **The Importance of Both Static and Dynamic Analysis:** While static analysis helps identify the structure and properties of malware without executing it, dynamic analysis is essential for observing how the malware behaves in real time. Both methods complement each other and provide a holistic view of the malware's functionality.

- **The Role of Indicators of Compromise (IOCs):** IOCs are critical in identifying and mitigating malware threats. They allow cybersecurity professionals to quickly detect malicious activity, respond to incidents, and protect systems from further

compromise.

- **Behavioral Patterns:** Malware often exhibits common behavioral patterns, such as attempting to establish network connections or modify critical system files. Identifying these patterns can help develop more effective detection and mitigation strategies.

7.3 Challenges Faced

Several challenges were encountered during the malware analysis process:

- **Environment Setup:** Setting up a secure and isolated environment for dynamic analysis was challenging, as ensuring that the malware did not affect other systems required careful configuration of virtual machines and sandboxes.

- **Malware Obfuscation:** Some malware samples used advanced obfuscation techniques, making it difficult to analyze their full behavior. This required more advanced techniques, such as reverse engineering and using debugging tools like OllyDbg.

- **Complexity of Behavior:** In some cases, malware behavior was difficult to interpret, as it often involved multiple stages or relied on external servers for additional payloads. This made it challenging to fully understand its impact without additional network analysis or advanced traffic monitoring.

Despite these challenges, the analysis process provided an excellent opportunity to deepen my understanding of malware and its potential impact on systems and networks.

7.4 Areas for Future Growth

While the foundational skills of malware analysis have been developed, several areas for future growth in this field have been identified:

- **Advanced Static Analysis:** Further developing skills in reverse engineering and disassembling malware code will allow for a deeper understanding of how malware operates at the code level.

- **Network Traffic Analysis:** Strengthening the ability to analyze network traffic generated by malware will provide further insights into its communication patterns and potential data exfiltration methods.

- **Threat Intelligence Integration:** Integrating threat intelligence feeds and external resources will enhance the ability to detect emerging threats and identify known IOCs more effectively.

As malware continues to evolve, it is essential to stay up-to-date with new techniques, tools, and methodologies in order to remain effective in combating these ever-changing threats.

8.0 Lab Completion

As part of the malware analysis training, I successfully completed two mandatory TryHackMe labs: **History of Malware** and **Malware Introductory**. These labs provided foundational knowledge on malware evolution, types, and analysis techniques. Additionally, I was introduced to optional paid labs for more advanced hands-on experience in both dynamic and static malware analysis.

8.1 TryHackMe Lab: History of Malware

Key Topics Covered:

- **Evolution of Malware Types:** This lab provided an in-depth look at how malware has evolved over time, starting from early viruses to modern-day sophisticated

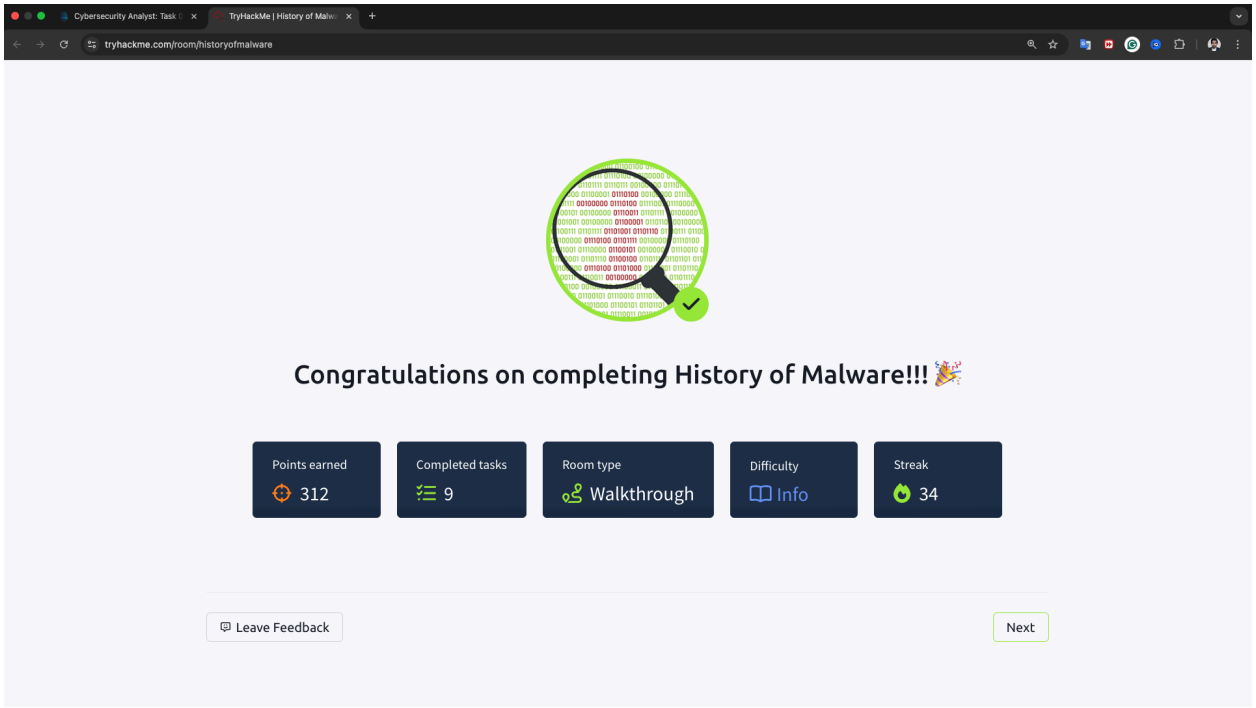
threats such as ransomware, spyware, and advanced persistent threats (APTs).

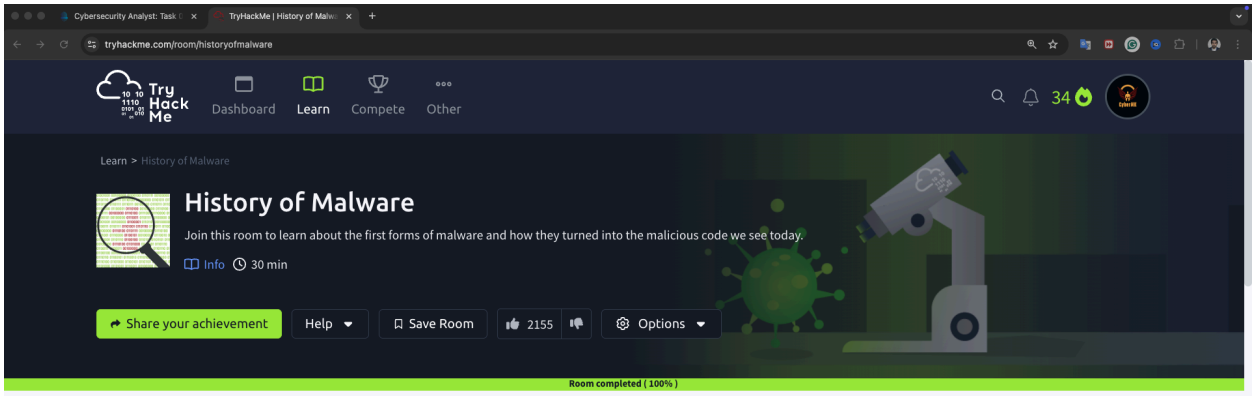
- **Examples of Historical Malware:** The lab covered several landmark malware examples, including the Morris Worm, MyDoom, and Stuxnet, highlighting their impact on cybersecurity.

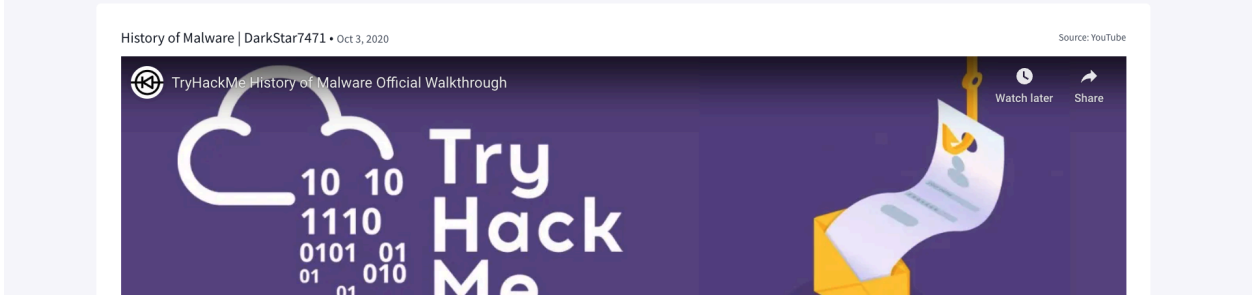
- **Characteristics of Different Malware Types:** The lab helped identify key characteristics that distinguish various types of malware, such as their propagation methods, targets, and the damage they can cause.

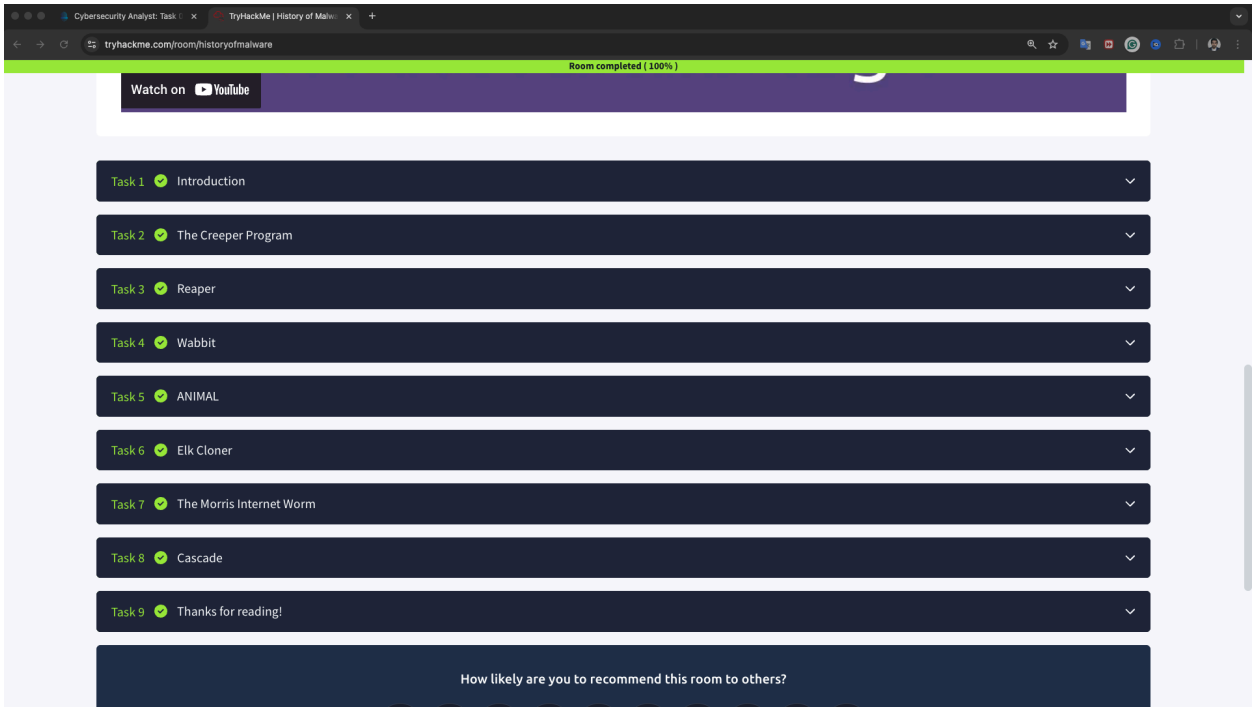
By completing this lab, I gained a deeper understanding of how malware has progressed, and the lessons learned from historical incidents have shaped the development of modern cybersecurity defense mechanisms.

Screenshots:




tryhackme.com/room/historyofmalware
Try Hack Me
Dashboard
Learn
Compete
Other
34
Learn > History of Malware
History of Malware
Join this room to learn about the first forms of malware and how they turned into the malicious code we see today.
Info
30 min
Share your achievement
Help
Save Room
2155
Options
Room completed (100%)


History of Malware | DarkStar7471 • Oct 3, 2020
Source: YouTube
TryHackMe History of Malware Official Walkthrough
Watch later
Share
Try Hack Me


tryhackme.com/room/historyofmalware
Room completed (100%)
Watch on YouTube
Task 1 Introduction
Task 2 The Creeper Program
Task 3 Reaper
Task 4 Wabbit
Task 5 ANIMAL
Task 6 Elk Cloner
Task 7 The Morris Internet Worm
Task 8 Cascade
Task 9 Thanks for reading!
How likely are you to recommend this room to others?

8.2 TryHackMe Lab: Malware Introductory

Key Topics Covered:

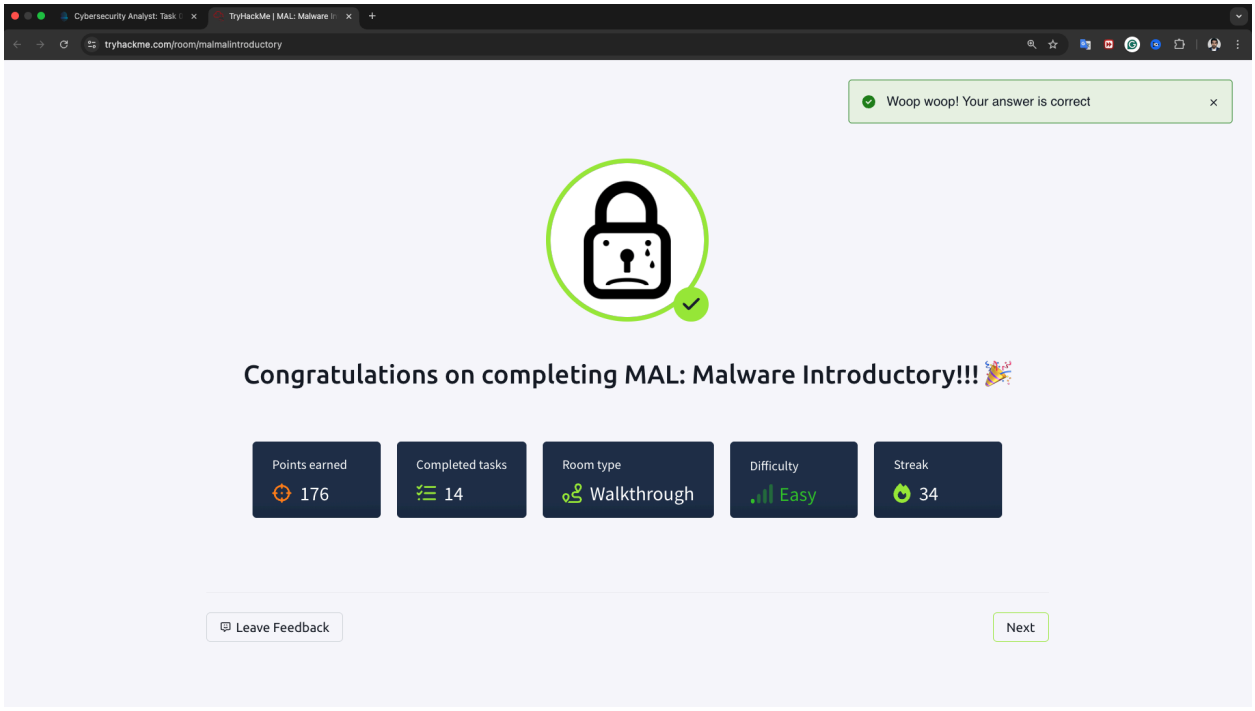
- **Basic Introduction to Malware:** This lab introduced the fundamental concepts of malware, its purpose, and the general techniques used by attackers to compromise systems.

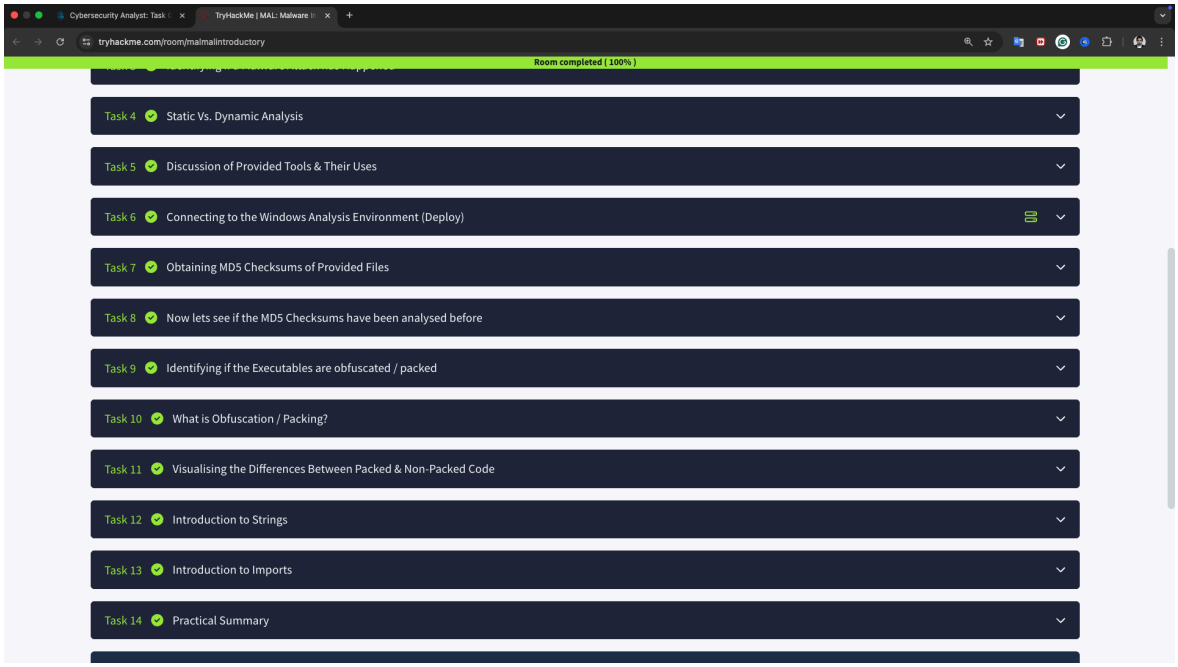
- **Types of Malware:** The lab provided an overview of different malware categories, including viruses, worms, Trojans, and ransomware, and examined their behaviors and effects on infected systems.

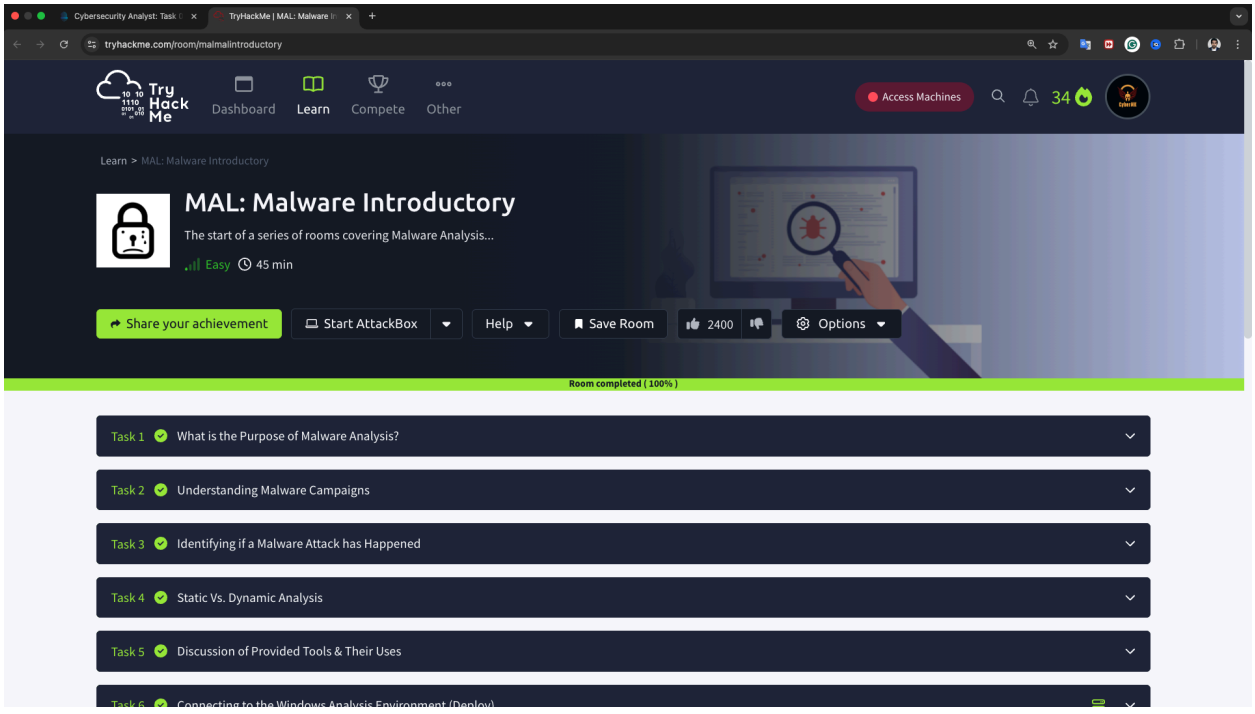
- **Simple Analysis Techniques:** I learned basic malware analysis techniques, including identifying common malware behaviors such as file modifications, registry changes, and network communications. This lab served as a stepping stone into more advanced analysis techniques.

The **Malware Introductory** lab provided a solid foundation for understanding the core concepts of malware, enabling me to approach more complex analysis tasks with confidence.

Screenshots:




tryhackme.com/room/malmalintroductory
Room completed (100%)
Task 4 Static Vs. Dynamic Analysis
Task 5 Discussion of Provided Tools & Their Uses
Task 6 Connecting to the Windows Analysis Environment (Deploy)
Task 7 Obtaining MD5 Checksums of Provided Files
Task 8 Now lets see if the MD5 Checksums have been analysed before
Task 9 Identifying if the Executables are obfuscated / packed
Task 10 What is Obfuscation / Packing?
Task 11 Visualising the Differences Between Packed & Non-Packed Code
Task 12 Introduction to Strings
Task 13 Introduction to Imports
Task 14 Practical Summary


tryhackme.com/room/malmalintroductory
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
34
Learn > MAL: Malware Introductory
MAL: Malware Introductory
The start of a series of rooms covering Malware Analysis...
Easy
45 min
Share your achievement
Start AttackBox
Help
Save Room
2400
Options
Room completed (100%)
Task 1 What is the Purpose of Malware Analysis?
Task 2 Understanding Malware Campaigns
Task 3 Identifying if a Malware Attack has Happened
Task 4 Static Vs. Dynamic Analysis
Task 5 Discussion of Provided Tools & Their Uses

he goal of this analysis was to execute a suspected malware sample (`p7zip-full`) in a controlled virtualized environment (Kali Linux VM

This Internship Task report was developed on [April, 05, 2025]

By:

atalmamun@gmail.com