Lab 1

Introduction to Incident Response

Mina Salehi

University of Maryland Baltimore County

CYBR 642 Introduction to Digital Forensics

Presented to: Gina Scaldaferri

02/05/2025

Introduction

In today's digital world, cybersecurity threats are increasingly widespread, making incident response crucial. This lab introduces incident response by simulating a real-world scenario, where students conduct analysis as an investigator. Through hands-on exercises, students will apply fundamental forensic techniques to assess system activity and identify potential threats. By engaging in this simulation, participants will develop essential skills for recognizing, analyzing, and responding to cybersecurity incidents.

Pre-Analysis

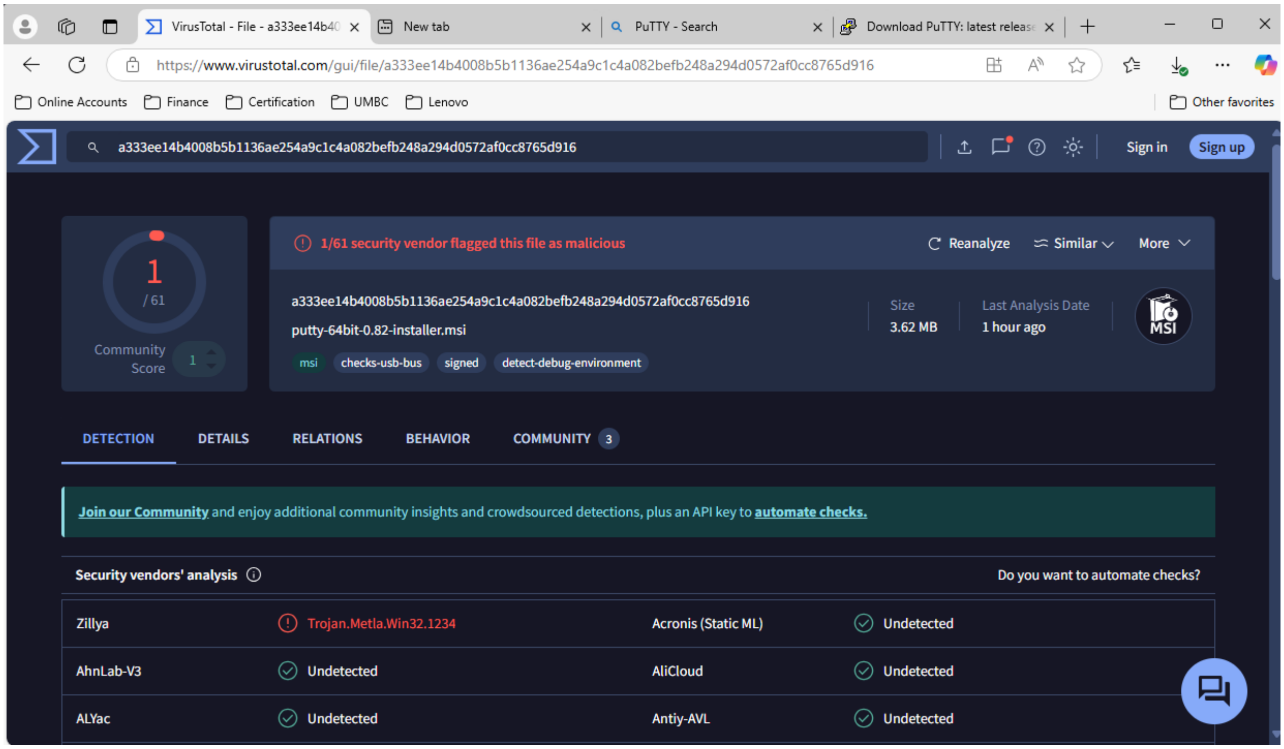
Computer forensics

Computer forensics applies scientific principles to the investigation and collection of digital evidence for legal cases. Like traditional forensics involves analyzing physical evidence like fingerprints or DNA, computer forensics focuses on retrieving data from electronic devices such as computers, networks, and storage systems.

Tatham, S. (2025, February 3). False-positive malware reports on PuTTY. Chiark Greenend. From https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/false-positive-malware.html

VirusTotal. (2025, February 3). False positive contacts. VirusTotal Documentation. From https://docs.virustotal.com/docs/false-positive-contacts

In this segment of the lab, I downloaded PuTTY from a reliable source, anticipating it to be free from vulnerabilities. Upon scanning the file with VirusTotal, the antivirus vendor Zillya identified it as containing "Trojan.Metla.Win32.1234." After conducting further research, I determined this to be a false positive. This experience underscores the importance of not solely relying on VirusTotal's results; additional investigation is essential. Notably, PuTTY's developers have acknowledged persistent false-positive reports from various antivirus programs, including Zillya. Therefore, it's advisable to consult official sources and community discussions when assessing potential threats.


VirusTotal - File - a333ee14b40
New tab
PuTTY - Search
Download PuTTY: latest release
https://www.virustotal.com/gui/file/a333ee14b4008b5b1136ae254a9c1c4a082befb248a294d0572af0cc8765d916
Online Accounts
Finance
Certification
UMBC
Lenovo
Other favorites
Sign in
Sign up
Reanalyze
Similar
More
MSI

a333ee14b4008b5b1136ae254a9c1c4a082befb248a294d0572af0cc8765d916

1
/ 61
Community Score 1

1/61 security vendor flagged this file as malicious

a333ee14b4008b5b1136ae254a9c1c4a082befb248a294d0572af0cc8765d916
putty-64bit-0.82-installer.msi
msi checks-usb-bus signed detect-debug-environment

Size 3.62 MB
Last Analysis Date 1 hour ago

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 3

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Zillya	Trojan.Metla.Win32.1234	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected

Tatham, S. (2025, February 3). False-positive malware reports on PuTTY. Chiark Greenend.

https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/false-positive-malware.html

VirusTotal. (2025, February 3). False positive contacts. VirusTotal Documentation.

https://docs.virustotal.com/docs/false-positive-contacts

Analysis

What utility can be run on the Windows VM to monitor processes running on the system?

- Task Manager

What utility can be run on the Windows VM to monitor network connections on the system?

- Resource Monitor, Netstat, Wireshark

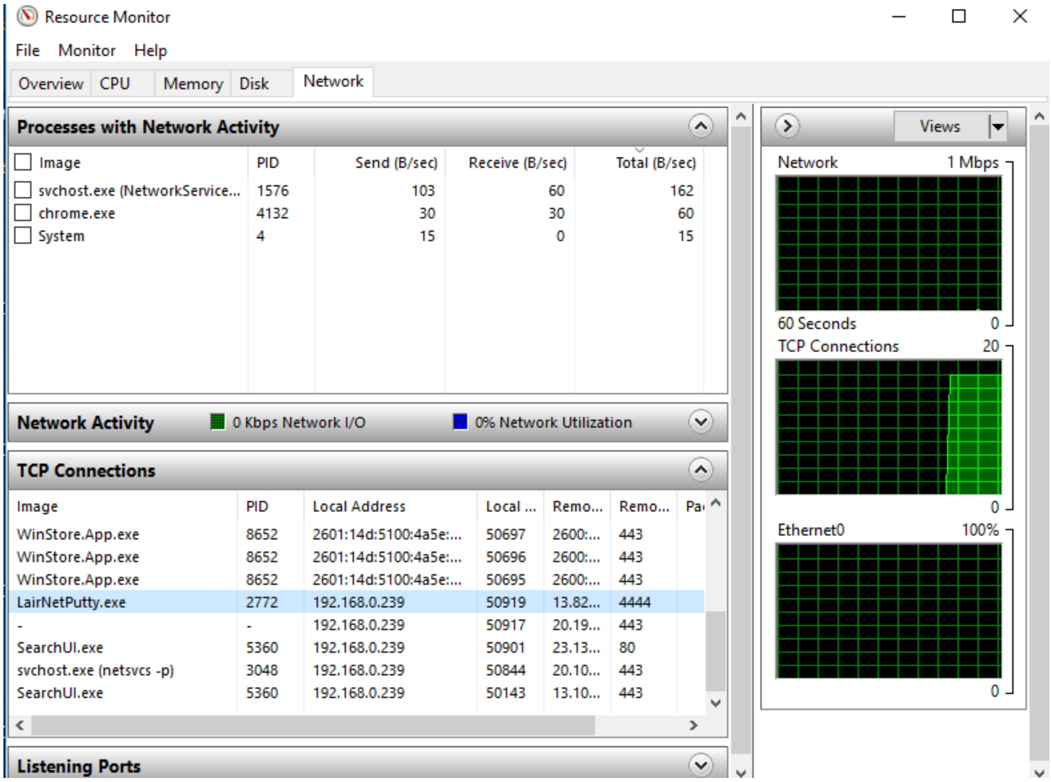
What application could you run on Windows to capture network traffic from the system?

- Wireshark, Microsoft Network Monitor

For this investigation, I will be using the Windows Task Manager a built-in tool within Windows that allows a user to note the Process and performance of the machine as items are run. I will also utilize Windows Resource Monitor, VirusTotal, PuTTY, and Netstat to identify malicious activities.

I began by assessing the system's baseline performance by accessing the Windows Task Manager. I observed that the CPU usage was initially between 2% and 7%. However, upon launching LairNet PuTTY, the CPU usage spiked to 25%. This significant increase suggests that the application may consume more system resources than expected. It's important to note that certain legitimate applications may cause temporary increases in CPU usage due to their operational requirements. Therefore, it's essential to consider the application's behavior and resource demands before concluding the presence of malicious activity.

I utilized Windows Resource Monitor to observe system activity and noticed that upon launching LairNet PuTTY, the application established a connection to IP address 13.82.60.83 via port 4444. This IP address is registered to Microsoft Corporation. While connections to Microsoft IPs are generally legitimate, it's important to note that some malware can disguise their communications by connecting to reputable domains to avoid detection. Additionally, port 4444 is not a standard and is commonly associated with various malicious activities. For instance, some rootkits, backdoors, and Trojan horse software open and use port 4444 to eavesdrop on traffic and communications, for their own communications, and to exfiltrate data from compromised computers.



Processes with Network Activity

□ Image	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)
□ svchost.exe (NetworkService...	1576	103	60	162
□ chrome.exe	4132	30	30	60
□ System	4	15	0	15

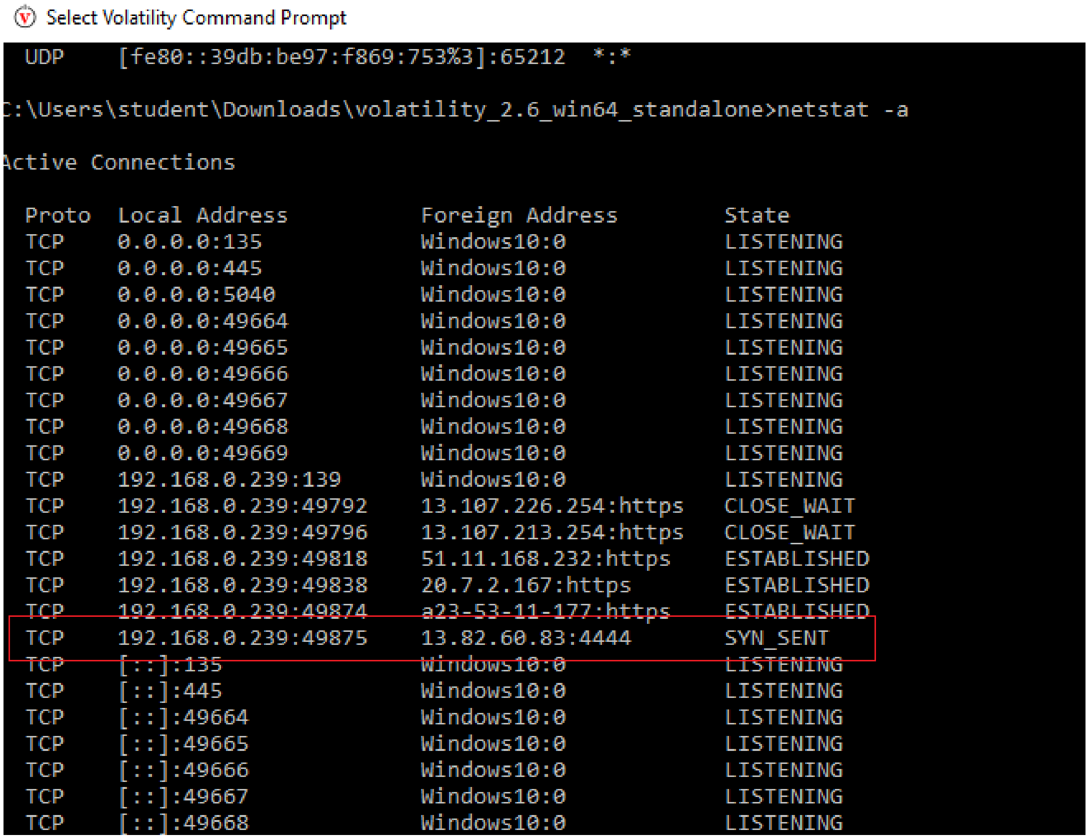
Network Activity 🟩 0 Kbps Network I/O 🟦 0% Network Utilization

TCP Connections

Image	PID	Local Address	Local ...	Remo...	Remo...	Pa
WinStore.App.exe	8652	2601:14d:5100:4a5e:...	50697	2600:...	443	
WinStore.App.exe	8652	2601:14d:5100:4a5e:...	50696	2600:...	443	
WinStore.App.exe	8652	2601:14d:5100:4a5e:...	50695	2600:...	443	
LairNetPutty.exe	2772	192.168.0.239	50919	13.82...	4444	
-	-	192.168.0.239	50917	20.19...	443	
SearchUI.exe	5360	192.168.0.239	50901	23.13...	80	
svchost.exe (netsvcs -p)	3048	192.168.0.239	50844	20.10...	443	
SearchUI.exe	5360	192.168.0.239	50143	13.10...	443	

Listening Ports

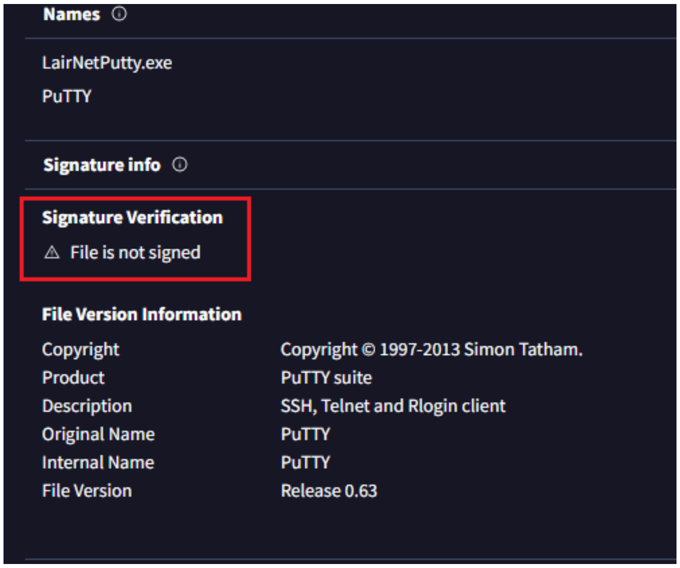
I also utilized Netstat command to examine active network connections and noticed that the state of the connection was listed as SYN_SENT. In TCP/IP protocol, a SYN_SENT state indicates that the client has sent a synchronization packet to initiate a connection and is waiting for a corresponding acknowledgment (SYB/ACK) from the server. The common cause could be the firewall blocking the client.



```
  UDP    [fe80::39db:be97:f869:753%3]:65212  *:*

:\Users\student\Downloads\volatility_2.6_win64_standalone>netstat -a

ctive Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Windows10:0            LISTENING
  TCP    0.0.0.0:445            Windows10:0            LISTENING
  TCP    0.0.0.0:5040           Windows10:0            LISTENING
  TCP    0.0.0.0:49664          Windows10:0            LISTENING
  TCP    0.0.0.0:49665          Windows10:0            LISTENING
  TCP    0.0.0.0:49666          Windows10:0            LISTENING
  TCP    0.0.0.0:49667          Windows10:0            LISTENING
  TCP    0.0.0.0:49668          Windows10:0            LISTENING
  TCP    0.0.0.0:49669          Windows10:0            LISTENING
  TCP    192.168.0.239:139      Windows10:0            LISTENING
  TCP    192.168.0.239:49792    13.107.226.254:https   CLOSE_WAIT
  TCP    192.168.0.239:49796    13.107.213.254:https   CLOSE_WAIT
  TCP    192.168.0.239:49818    51.11.168.232:https    ESTABLISHED
  TCP    192.168.0.239:49838    20.7.2.167:https       ESTABLISHED
  TCP    192.168.0.239:49874    a23-53-11-177:https    ESTABLISHED
  TCP    192.168.0.239:49875    13.82.60.83:4444       SYN_SENT
  TCP    [::]:135               Windows10:0            LISTENING
  TCP    [::]:445               Windows10:0            LISTENING
  TCP    [::]:49664             Windows10:0            LISTENING
  TCP    [::]:49665             Windows10:0            LISTENING
  TCP    [::]:49666             Windows10:0            LISTENING
  TCP    [::]:49667             Windows10:0            LISTENING
  TCP    [::]:49668             Windows10:0            LISTENING
```

I uploaded LairNet PuTTY to VirusTotal, where 61 security vendors flagged it as malicious. Notably, the file lacked valid or trusted digital signatures, which are essential for verifying the authenticity and integrity of software. The absence of a valid digital signature is a red flag, as legitimate software typically includes such signatures to confirm its source and integrity.

Comparing the hash values between the legitimate PuTTY and LairNet PuTTY revealed discrepancies. A mismatch in hash values suggests that the file may have been tampered with or is entirely different from the authentic version.



Names ⓘ

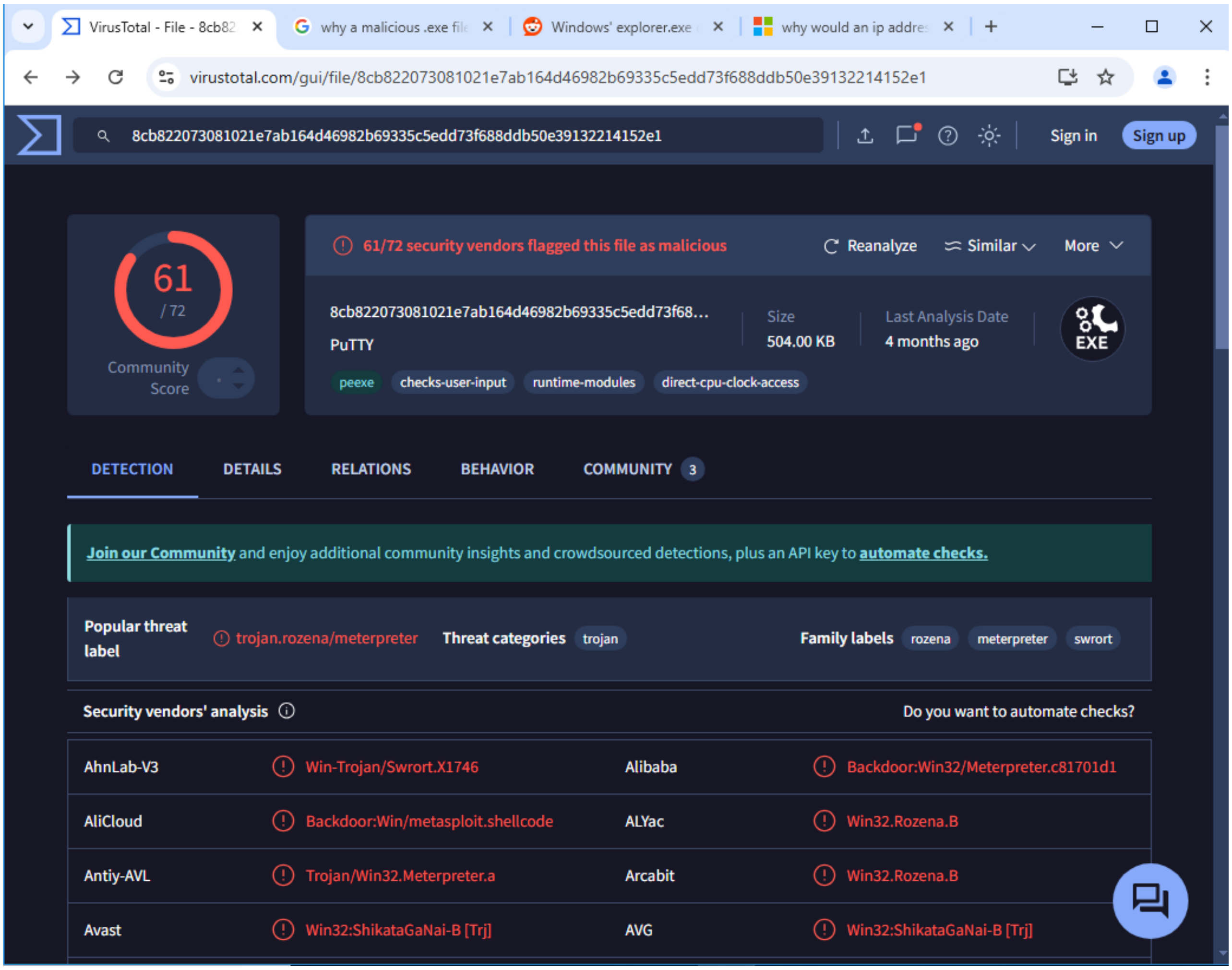
LairNetPutty.exe
PuTTY

Signature info ⓘ

Signature Verification
⚠ File is not signed

File Version Information

Copyright	Copyright © 1997-2013 Simon Tatham.
Product	PuTTY suite
Description	SSH, Telnet and Rlogin client
Original Name	PuTTY
Internal Name	PuTTY
File Version	Release 0.63



virustotal.com/gui/file/8cb822073081021e7ab164d46982b69335c5edd73f688ddb50e39132214152e1

8cb822073081021e7ab164d46982b69335c5edd73f688ddb50e39132214152e1

61 / 72 Community Score

ⓘ 61/72 security vendors flagged this file as malicious

8cb822073081021e7ab164d46982b69335c5edd73f68...
PuTTY

Size 504.00 KB

Last Analysis Date 4 months ago

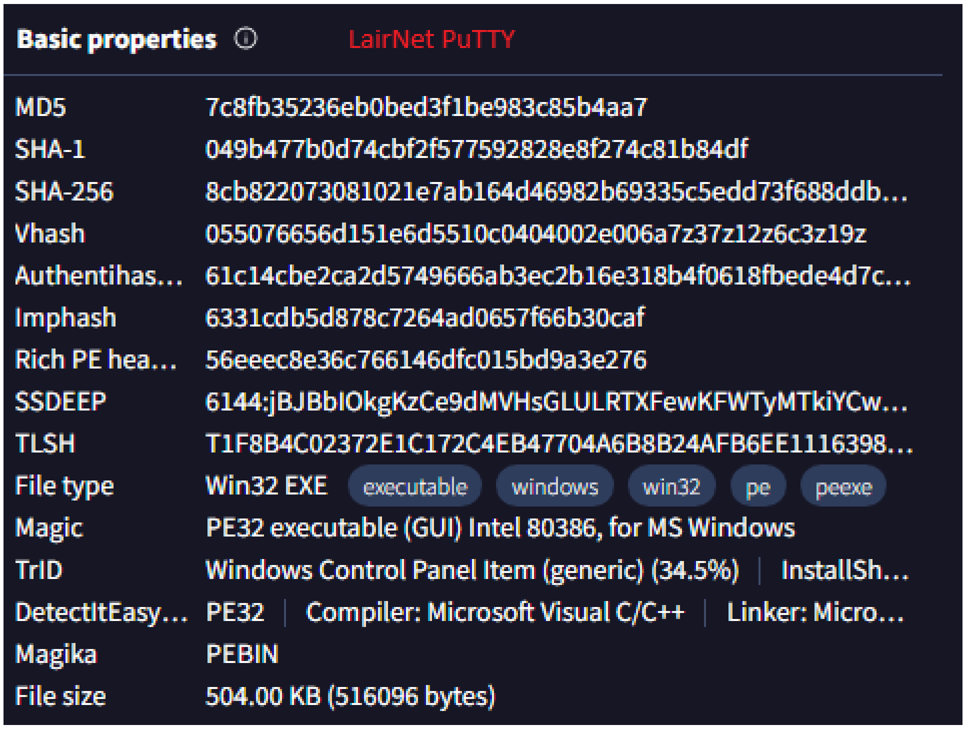
peexe checks-user-input runtime-modules direct-cpu-clock-access

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Popular threat label ⓘ trojan.rozena/meterpreter **Threat categories** trojan **Family labels** rozena meterpreter swrort

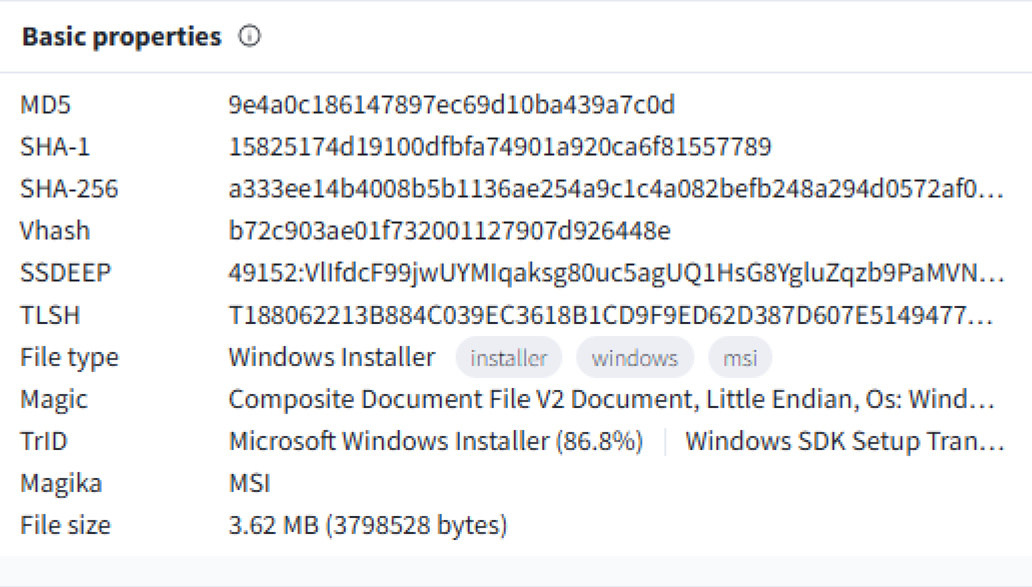
Security vendors' analysis ⓘ Do you want to automate checks?

AhnLab-V3	ⓘ Win-Trojan/Swrort.X1746	Alibaba	ⓘ Backdoor:Win32/Meterpreter.c81701d1
AliCloud	ⓘ Backdoor:Win/metasploit.shellcode	ALYac	ⓘ Win32.Rozena.B
Antiy-AVL	ⓘ Trojan/Win32.Meterpreter.a	Arcabit	ⓘ Win32.Rozena.B
Avast	ⓘ Win32:ShikataGaNai-B [Trj]	AVG	ⓘ Win32:ShikataGaNai-B [Trj]



Basic properties LairNet PuTTY

MD5	7c8fb35236eb0bed3f1be983c85b4aa7
SHA-1	049b477b0d74cbf2f577592828e8f274c81b84df
SHA-256	8cb822073081021e7ab164d46982b69335c5edd73f688ddb…
Vhash	055076656d151e6d5510c0404002e006a7z37z12z6c3z19z
Authentihas…	61c14cbe2ca2d5749666ab3ec2b16e318b4f0618fbede4d7c…
Imphash	6331cdb5d878c7264ad0657f66b30caf
Rich PE hea…	56eeec8e36c766146dfc015bd9a3e276
SSDEEP	6144:jBJBblOkgKzCe9dMVHsGLULRTXFewKFWTyMTkiYCw…
TLSH	T1F8B4C02372E1C172C4EB47704A6B8B24AFB6EE1116398…
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Windows Control Panel Item (generic) (34.5%) | InstallSh…
DetectItEasy…	PE32 | Compiler: Microsoft Visual C/C++ | Linker: Micro…
Magika	PEBIN
File size	504.00 KB (516096 bytes)



Basic properties

MD5	9e4a0c186147897ec69d10ba439a7c0d
SHA-1	15825174d19100dfbfa74901a920ca6f81557789
SHA-256	a333ee14b4008b5b1136ae254a9c1c4a082befb248a294d0572af0…
Vhash	b72c903ae01f732001127907d926448e
SSDEEP	49152:VlIfdcF99jwUYMIqaksg80uc5agUQ1HsG8YgluZqzb9PaMVN…
TLSH	T188062213B884C039EC3618B1CD9F9ED62D387D607E5149477…
File type	Windows Installer installer windows msi
Magic	Composite Document File V2 Document, Little Endian, Os: Wind…
TrID	Microsoft Windows Installer (86.8%) | Windows SDK Setup Tran…
Magika	MSI
File size	3.62 MB (3798528 bytes)

Conclusions

A comprehensive analysis of LairNet PuTTY has revealed several security concerns. The investigation began with an assessment using Windows Task Manager and Resource Monitor. An unusual spike in CPU usage and a suspicious network connection to port 4444 were detected. Considering port 4444 is commonly associated with backdoors and malware, closer examination was necessary.

To verify the integrity of the executable, VirusTotal was utilized, revealing that 61 security vendors flagged LairNet PuTTY as malicious. Additionally, a comparison of hash values between the legitimate PuTTY and LairNet PuTTY confirmed a discrepancy, indicating that the file had been tampered with. Furthermore, the absence of a valid digital signature raised another red flag, as legitimate software typically includes such signatures to verify authenticity.

Network analysis using Netstat revealed that the connection remained in the SYN_SENT state, which can be indicative of firewall blockage. Since malware often attempts to establish unauthorized network communications, persistent SYN_SENT states can serve as potential indicators of compromise.

Given these findings, immediate remediation steps should be taken to prevent further system compromise and mitigate security risks:

1. Immediate Removal of LairNet PuTTY: Uninstall and delete all instances of LairNet PuTTY from the affected system.

2. Use Windows Defender, Malwarebytes, or another trusted antivirus tool to perform a full system scan and remove any residual malware.

3. Verify and Secure Other Systems: Check all other computers on the network to ensure they have not been infected or compromised.

4. Reinstall a Clean Version of PuTTY: Download the legitimate version of PuTTY only from its official website (https://www.chiark.greenend.org.uk/~sgtatham/putty/).
5. Verify the hash values and digital signatures before installation to ensure the file's authenticity.
6. Review and update firewall rules and policies to prevent unauthorized outbound connections.
7. Use Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) to detect unusual network activity.
8. Implement a strict policy against downloading and installing unauthorized or free software from untrusted sources.
9. Require employees to use only approved software repositories and verify digital signatures before installation.
10. Educate users on cybersecurity best practices.
11. Conduct regular security audits to detect unauthorized software or network anomalies.
12. Enable automatic updates for security tools and operating systems.

By implementing these remediation steps, organizations can mitigate security risks, prevent similar incidents, and strengthen overall cybersecurity posture. This case highlights the importance of multi-layered security defenses, secure software acquisition, and proper incident response planning.

Glossary

CPU (Central Processing Unit) -The CPU is the primary component of a computer that processes instructions and performs calculations necessary for running programs and system operations. It is often referred to as the "brain" of the computer and is responsible for executing tasks efficiently (Stallings, 2020).

False Positive - A false positive in cybersecurity occurs when a security tool incorrectly identifies a benign file or activity as malicious. This can happen with antivirus software, intrusion detection systems, or malware analysis platforms like VirusTotal, leading to unnecessary security alerts or system disruptions (Scarfone & Mell, 2007).

Intrusion Detection System (IDS) - An Intrusion Detection System (IDS) is a security solution that monitors network traffic or system activity for suspicious behavior and potential threats. (Scarfone & Mell, 2007).

Intrusion Prevention System (IPS) - An Intrusion Prevention System (IPS) is an advanced security mechanism that not only detects but also actively prevents and blocks malicious activities in real-time. Unlike IDS, which only generates alerts, IPS can take automated actions such as dropping malicious packets, blocking IP addresses, or terminating suspicious connections (Bace & Mell, 2001).

IP Address - An IP (Internet Protocol) address is a numerical label assigned to devices connected to a network that enables communication between them, and it serves as a unique identifier for devices on the internet or local networks (Kurose & Ross, 2021).

Netstat - Netstat (Network Statistics) is a command-line utility used to display active network connections, listening ports, and routing tables on a computer. It is commonly used for network diagnostics, troubleshooting, and detecting unauthorized connections (Tanenbaum & Wetherall, 2011).

Port - A port is a logical communication endpoint used in networking to distinguish different types of traffic on a system. Ports are identified by numbers (e.g., port 80 for HTTP, port 443 for HTTPS) and enable multiple applications to communicate over a single network connection (Comer, 2018).

PuTTY - PuTTY is an open-source terminal emulator that supports SSH, Telnet, and other network protocols. It is widely used for securely connecting to remote servers, executing commands, and managing network devices (Tatham, 2023).

Trojan Horse - A Trojan horse is a type of malware that disguises itself as legitimate software to trick users into installing it. Once executed, it can perform malicious activities such as stealing sensitive data, creating backdoors, or spreading other malware (Baker, 2022).

VirusTotal - VirusTotal is an online malware scanning and threat intelligence platform that aggregates results from multiple antivirus engines and security tools. It is commonly used to analyze suspicious files and URLs to detect potential threats (Google, 2024).

Wireshark - Wireshark is an open-source packet analyzer used for network traffic analysis and troubleshooting. It allows users to capture and inspect packets in real-time, making it a valuable tool for cybersecurity professionals and network administrators (Orebaugh et al., 2007).

Reference

Ashraf, K. (n.d.). *Advanced log analysis*. KARIM ASHRAF SPACE. Retrieved February 5, 2025, from https://karim-ashraf.gitbook.io/karim_ashraf_space/writeups/advanced-log-analysis

Castro, J. (2017, August 5). What means SYN_SENT status in a socket? *Devsys*. Medium. From https://medium.com/devsys/what-means-syn-sent-status-in-a-socket-5ea03eaf6ca9

Comer, D. E. (2018). *Computer networks and internets* (6th ed.). Pearson.

CrowdStrike. (n.d.). *What is a Trojan? Understanding how Trojans work in cybersecurity*. CrowdStrike. from https://www.crowdstrike.com/en-us/cybersecurity-101/malware/trojans/

CrowdStrike. *Incident response: How organizations can effectively respond to cyber incidents*. CrowdStrike. from https://www.crowdstrike.com/en-us/cybersecurity-101/incident-response/

Geer, D. (2017, April 24). Securing risky network ports. *CSO Online*. From https://www.csoonline.com/article/561301/securing-risky-network-ports.html

Google. (2024). *VirusTotal documentation*. Retrieved February 5, 2025, from https://www.virustotal.com

Mckay, D. (2021, January 8). Why are some network ports risky, and how do you secure them? *How-To Geek*. From https://www.howtogeek.com/devops/why-are-some-ports-risky-and-how-do-you-secure-them/

Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson.

Karunsubramanian, K. (2015, December 1). What is SYN_SENT socket status? *Karunsubramanian.com*. From https://karunsubramanian.com/network/what-is-syn_sent-socket-status/

MalwareTips. (n.d.). *How to fix high CPU usage at 100% without any running programs.* Retrieved [2023, March 27], from https://malwaretips.com/blogs/fix-high-cpu-usage-at-100-without-any-running-programs/

Orebaugh, A., Ramirez, G., Burke, J., & Morris, L. (2007). *Wireshark & Ethereal network protocol analyzer toolkit*. Syngress.

Red Canary. (2019, February 12). Catch me if you code: How to detect process masquerading. *Red Canary*. From https://redcanary.com/blog/threat-detection/process-masquerading/

Rouse, M. (n.d.). *Computer forensics.* TechTarget. Retrieved [date], from https://www.techtarget.com/searchsecurity/definition/computer-forensics

Scarfone, K., Mell, P., & Souppaya, M. (2007). *Guide to intrusion detection and prevention systems (IDPS)*. National Institute of Standards and Technology (NIST). From https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

SOCRadar. (2022, Jan 27). What is network port? *SOCRadar® Cyber Intelligence Inc.* Retrieved from https://socradar.io/what-is-network-port/

Stallings, W. (2020). *Computer organization and architecture* (11th ed.). Pearson.

Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer networks* (5th ed.). Pearson.

Tatham, S. (2023). *PuTTY documentation*. Retrieved February 5, 2025, from https://www.chiark.greenend.org.uk/~sgtatham/putty/