BLUEMOONTUESDAY INC. – INCIDENT REPORT

Executive Summary

This report documents the analysis of a network capture file (PCAP) related to the download of a malicious file disguised as a Google Authenticator app from a fake website. My mission is to identify malicious activity, determine the involved entities, and recommend remediation actions.

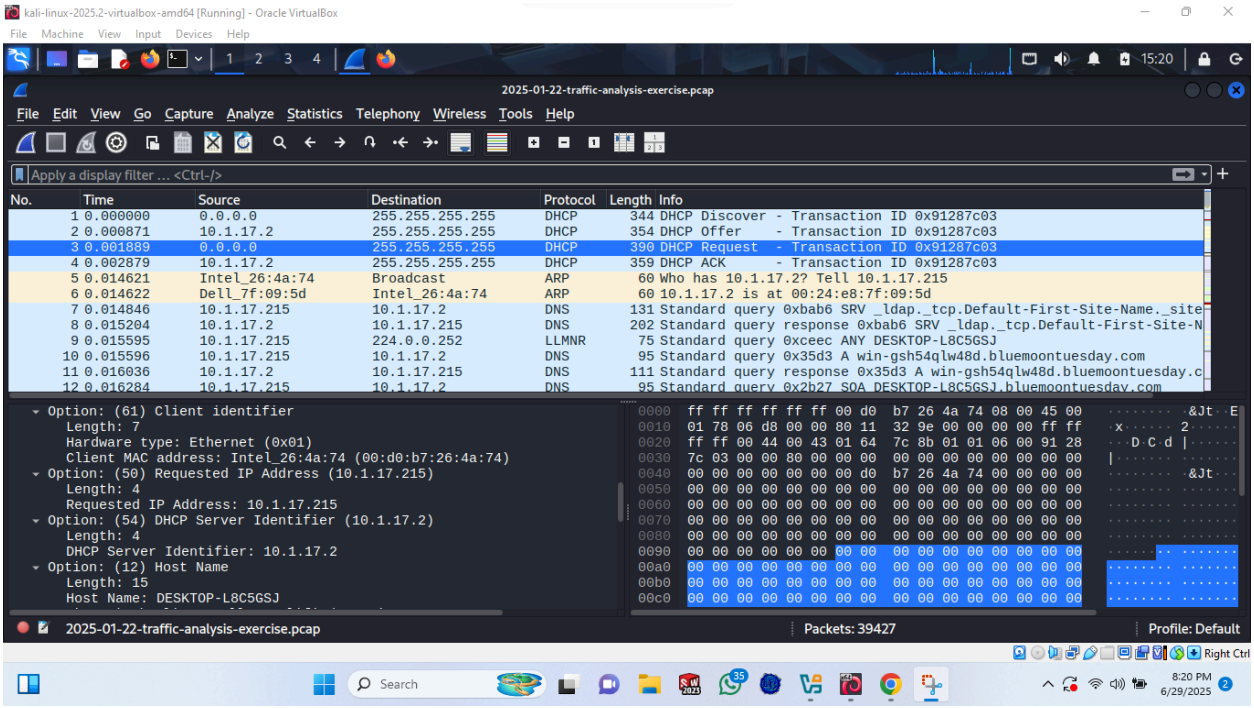
Timeline of Events

Time	Event	Details
2:09 PM	Phishing site accessed	Employee visits google-authenticator.blurlesoon-appliance.net hosted by (104.21.64.1).
2:10 PM	Connection to C2 servers established	Browser initiates connection to 82.221.136.26 and 5.252.153.241 causing the slower performance experienced by the employee.
2:11 PM	Malware download and opened	Executable named TeamViewer.exe is dropped to: C:\ProgramData\huo\TeamViewer.exe.
2:12 PM	Persistence established	PowerShell script creates a shortcut to the dropped TeamViewer.exe in the Windows Startup folder: TeamViewer.lnk.
2:13 PM	Anomaly detected	The employee suspects unusual behaviour of the system, like slower performance, Windows cmd opening which is likely to maintain its access, etc.
2:14 PM	Incident reported	SOC is notified and retrieves the PCAP file from the affected host.

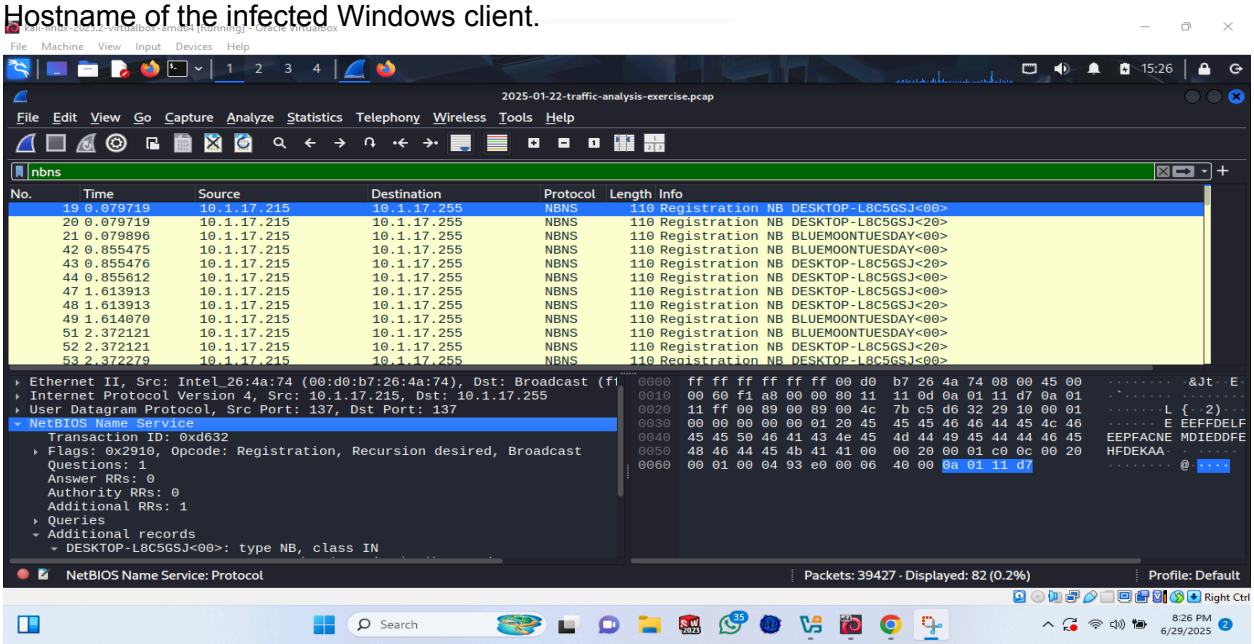
Host and User Details

Below are the details of the infected Windows client which includes its IP address, MAC address, hostname and its user account name. I take it a step further by identifying the domain name of the fake Google Authenticator Page and IP addresses most likely to be the Command and Control (C2) servers.

Looking at the first DHCP request object, we can find information on the infected Windows client.



Alternatively, filtering for NBNS traffic shows the correlating IP address, MAC address and Hostname of the infected Windows client.



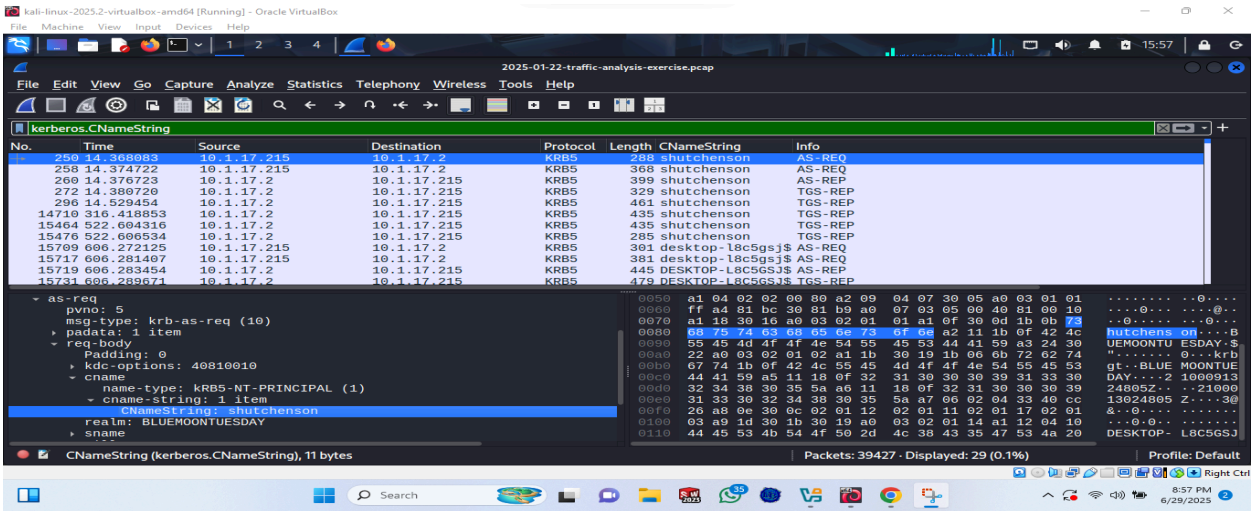
1. (10.1.17.215) is the IP address of the infected Windows client.

2. (00:d0:b7:26:4a:74) is the MAC address of the infected Windows client.

3. The hostname of the infected Windows client is DESKTOP-L8C5GSJ.

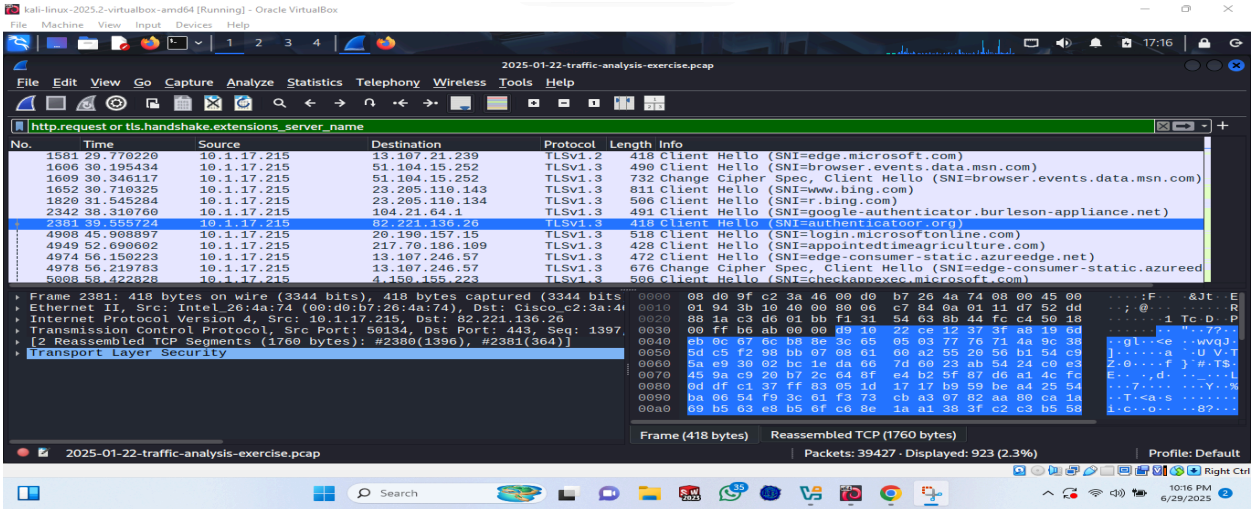
4. The user account name logged into the infected system is shutchenson.

   This was possible with “kerberos.CNameString”, I could filter for kerberos authentication traffic related to a specific user. I applied as a column for more visibility.



Network Indicators and C2 Communication

The domain name of the fake Google Authenticator page is google-authenticator.blurleson-appliance.net with an ip address of “104.21.64.1”. While “82.221.136.26” is likely a C2 server misspelt as “authenticatoor” to evade detection.



The IP addresses of the Command and Control (C2) servers for this infection

From the network traffic, I identified 2 IP addresses as likely Command and Control (C2) servers based on distinct patterns:

- 82.221.136.26
  Domain name is authenticatoor.org to evade detection.This suggests its involvement in luring victims and potentially coordinating further malicious actions.

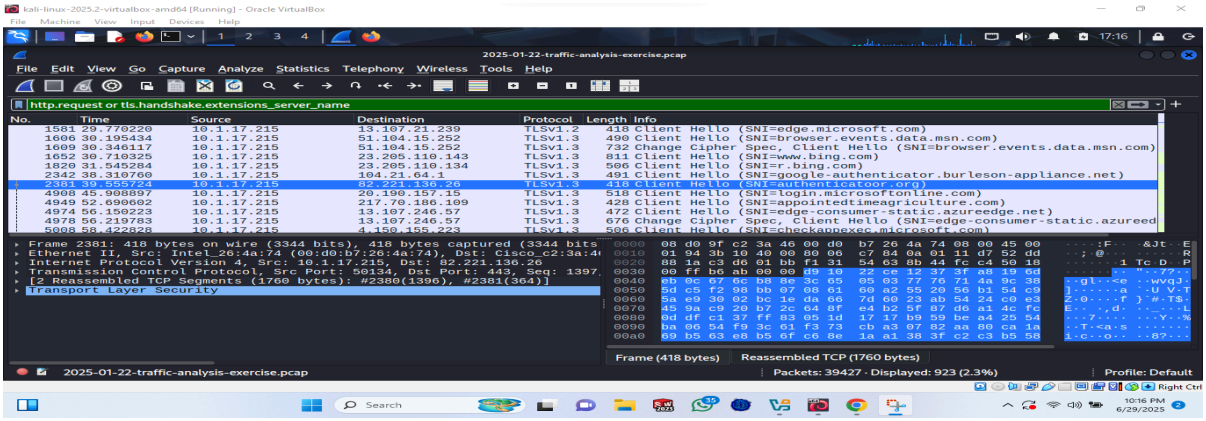
- 5.252.153.241
  The role of this IP address in distributing the payload, downloading the malware and maintaining persistence is a strong indicator of its malicious role.

Analysis Walkthrough
LAN SEGMENT DETAILS FROM THE PCAP

- LAN segment range: 10.1.17.0/24 (10.1.17.0 through 10.1.17.255)
- Domain: bluemoontuesday.com
- Active Directory (AD) domain controller: 10.1.17.2 - WIN-GSH54QLW48D
- AD environment name: BLUEMOONTUESDAY
- LAN segment gateway: 10.1.17.1
- LAN segment broadcast address: 10.1.17.255

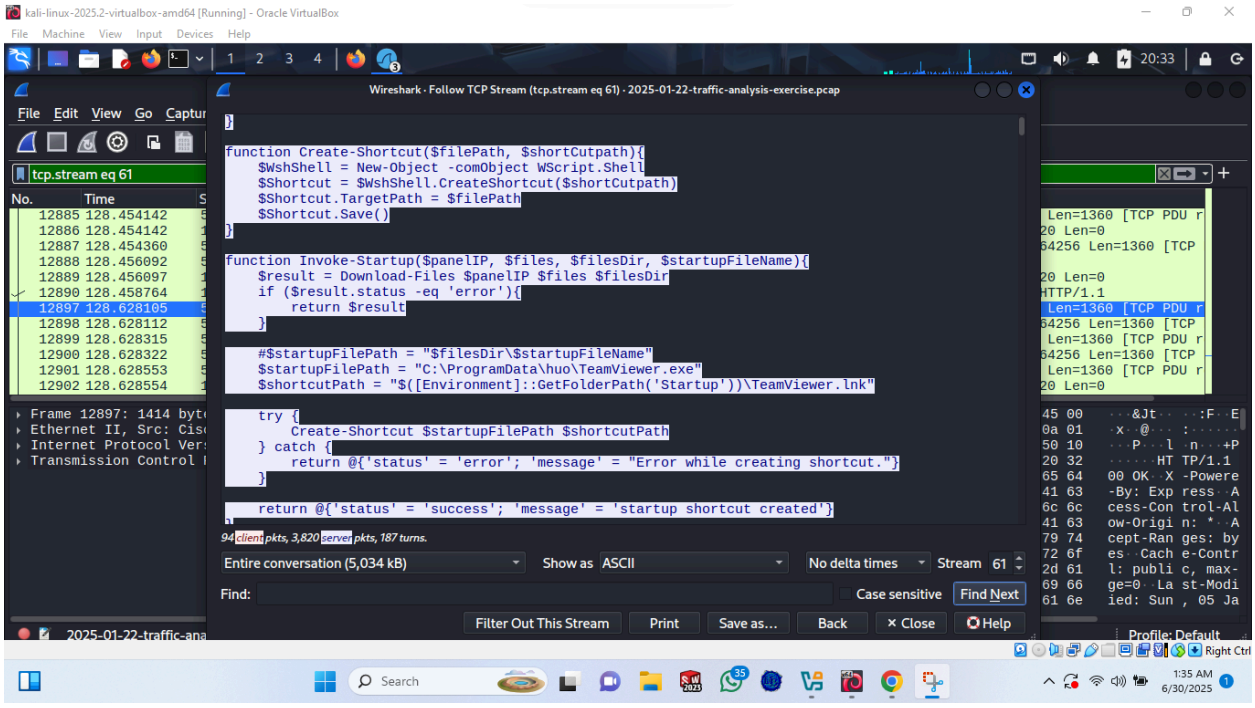
1. Initial DNS Request to Malicious Domain

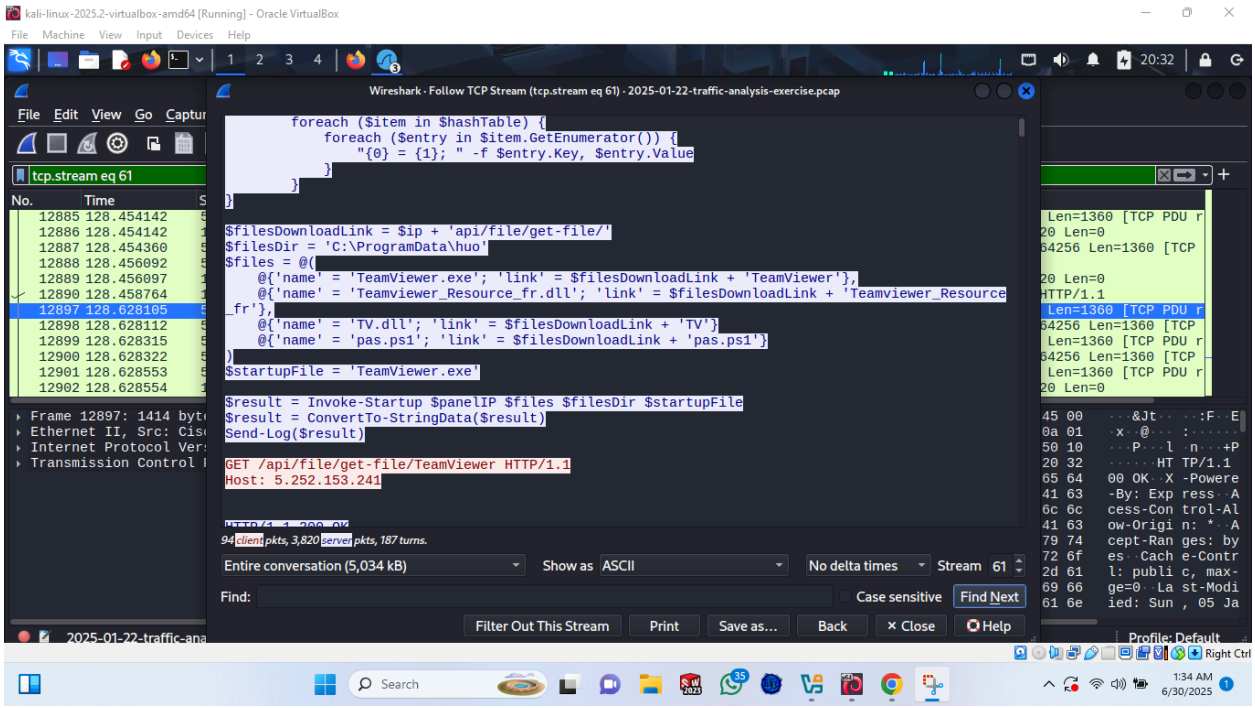
The analysis of the screenshot below shows the system connection to the phishing site and C2 server that is totally encrypted in the TLSv1.3.



2. Confirmation of Second C2 server

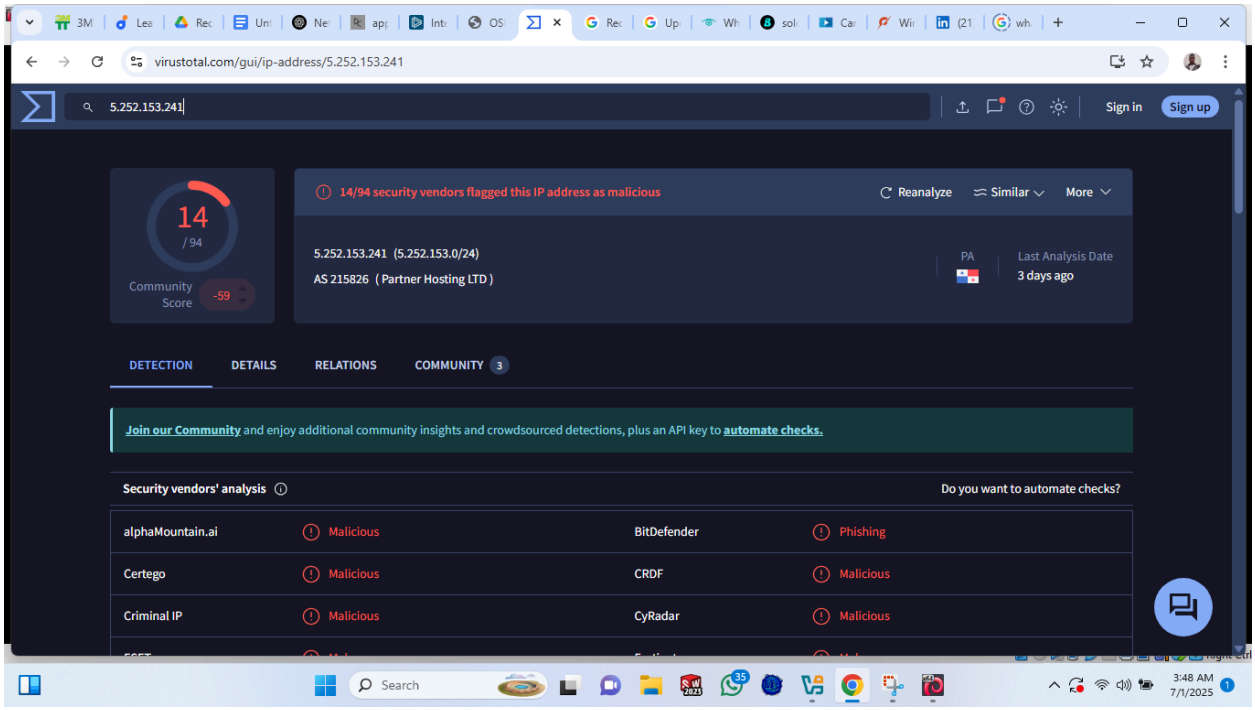
This analyzed portion of the script is designed to ensure persistence on the system by creating a startup shortcut for a downloaded file. This functionality is implemented within the ‘Invoke-Startup’ function, which downloads the required malware and stores it in created shortcuts thereby maintaining access gained through the startup.





3. Confirm of C2 servers using VirusTotal

The two probable IP addresses which are likely to be C2 servers were scanned and confirmed on VirusTotal to be malicious in nature. Though IP address 82.221.136.26 is not properly flagged due to its complete encryption, it remains an unknown threat.



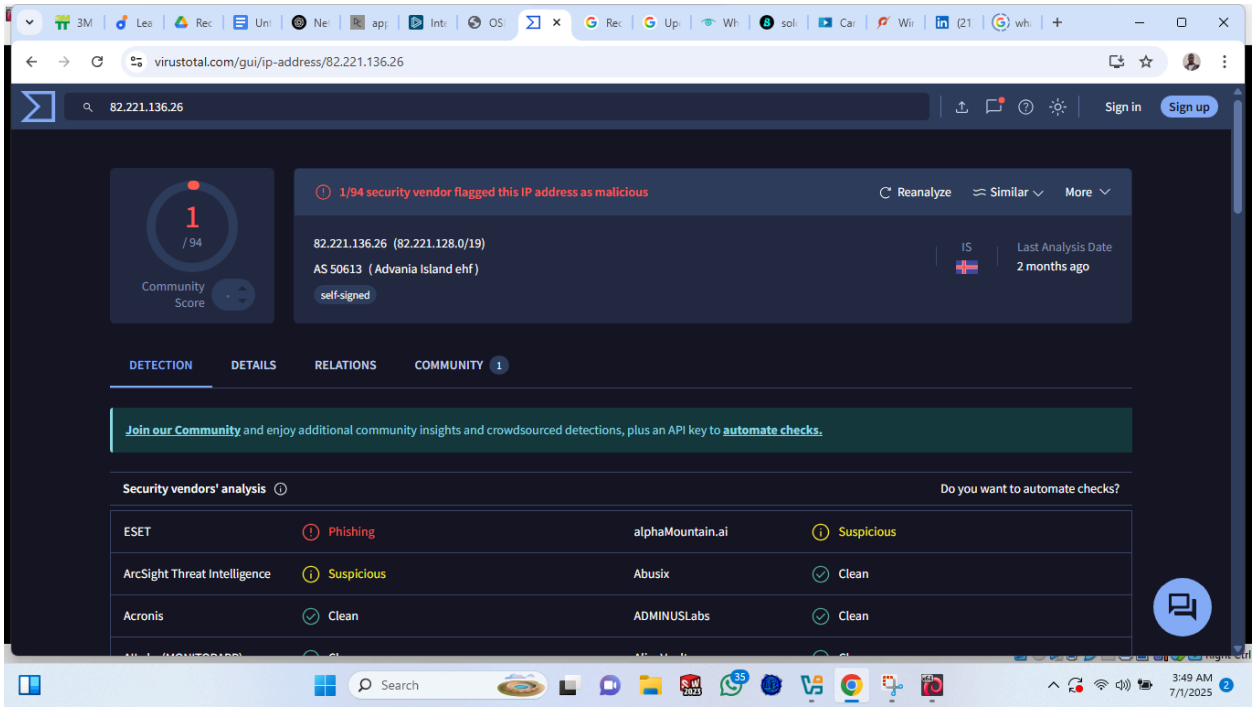


Table of Indicator of Compromise

Type	Value
Phishing	IP address ● 104.21.64.1 Domain name ● google-authenticator.blurleson-appliance.net
C2 Servers	IP addresses ● 82.221.136.26 ● 5.252.153.241

Remediation

1. Immediately isolate the infected host from the network.
2. Block the following IOCs at the firewall and DNS levels:
    - 104.21.64.1
    - 82.221.136.26
    - 5.252.153.241
3. Scan all endpoints for related activity.
4. Deploy threat detection rules to alert on similar domain names and TLS behaviour.
5. Monitor event logs of all employees.
6. Engage the employees on active and passive phishing awareness training.