2025-01-22 - TRAFFIC ANALYSIS EXERCISE ANSWERS

Link to the exercise:

- https://www.malware-traffic-analysis.net/2025/01/22/index.html

Links to some tutorials I've written that should help with this exercise:

- Wireshark Tutorial: Changing Your Column Display
- Wireshark Tutorial: Identifying Hosts and Users
- Wireshark Tutorial: Display Filter Expressions
- Wireshark Tutorial: Exporting Objects from a Pcap

ENVIRONMENT:

- LAN segment range: `10.1.17.0/24` (`10.1.17.0` through `10.1.17.255`)
- Domain: `bluemoontuesday.com`
- AD environment name: `BLUEMOONTUESDAY`
- Domain Controller: `10.1.17.2` – `WIN-GSH54QLW48D`
- LAN segment gateway: `10.1.17.1`
- LAN segment broadcast address: `10.1.17.255`

BACKGROUND:

You work as an analyst at a Security Operation Center (SOC). Someone contacts your team to report a coworker has downloaded a suspicious file after searching for Google Authenticator. The caller provides some information similar to social media posts at:

- https://www.linkedin.com/posts/unit42_2025-01-22-wednesday-a-malicious-ad-led-activity-7288213662329192450-ky3V/
- https://x.com/Unit42_Intel/status/1882448037030584611

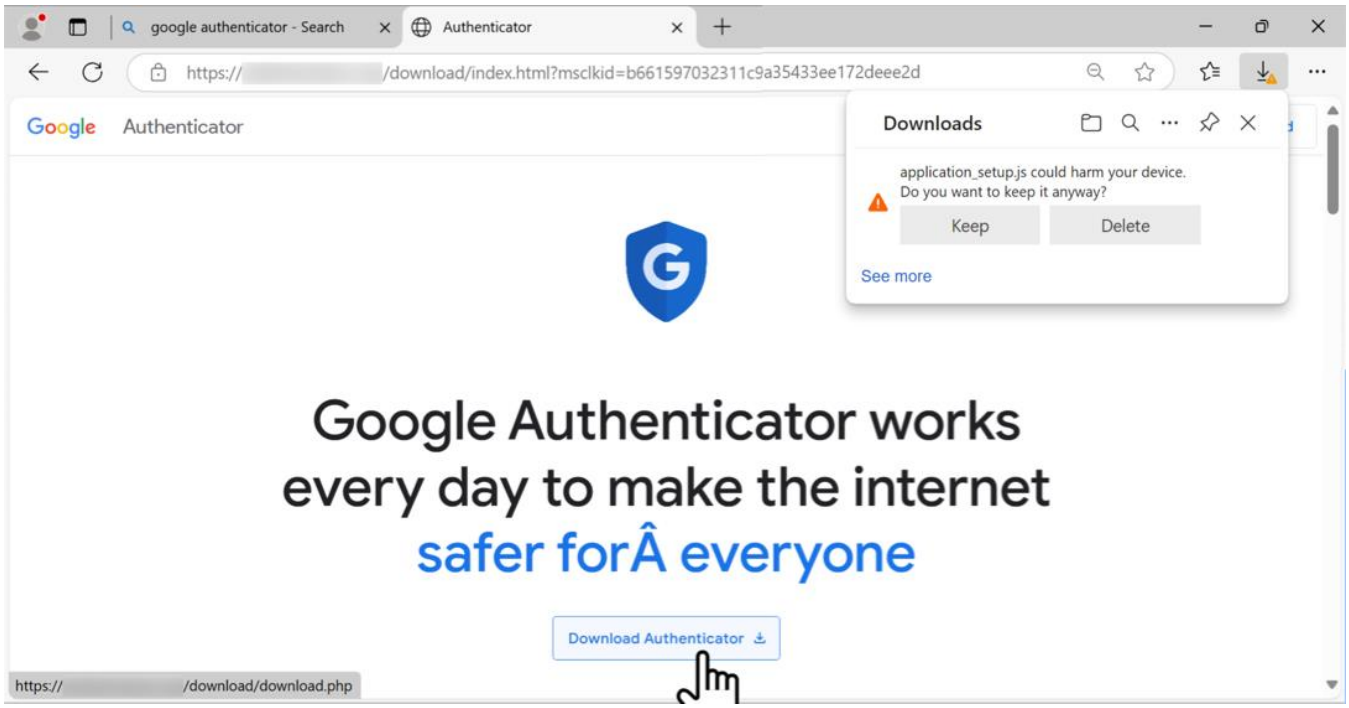
Based on the caller's initial information, you confirm there was an infection. You retrieve a pcap of the associated traffic. Reviewing the traffic, you find several indicators matching details from a Github page referenced in the above social media posts. After confirming an infection happened, you begin writing an incident report.

TASK:

For this exercise, answer the following questions for your incident report:

- What is the IP address of the infected Windows client?
- What is the mac address of the infected Windows client?
- What is the host name of the infected Windows client?
- What is the user account name from the infected Windows client?
- What is the likely domain name for the fake Google Authenticator page?
- What are the IP addresses used for C2 servers for this infection?

2025-01-22 - TRAFFIC ANALYSIS EXERCISE ANSWERS



Shown above: Screenshot of the fake Google Authenticator page in a web browser.

ANSWERS:

Victim Details:

- IP address: `10.1.17.215`
- Host name: `DESKTOP-L8C5GSJ`
- MAC address: `00:d0:b7:26:4a:74`
- Windows user account name: `shutchenson`

Probable fake software site for initial malware download:

- `authenticatoor.org`

Time	Dst	port	Host	Info
2025-01-22 19:45:28	23.205.110.134	443	r.bing.com	Client Hello
2025-01-22 19:45:34	104.21.64.1	443	google-authenticator.burleson-appliance.net	Client Hello
2025-01-22 19:45:36	82.221.136.26	443	authenticatoor.org	Client Hello
2025-01-22 19:45:42	20.190.157.15	443	login.microsoftonline.com	Client Hello
2025-01-22 19:45:49	217.70.186.109	443	appointedtimeagriculture.com	Client Hello
2025-01-22 19:45:52	13.107.246.57	443	edge-consumer-static.azureedge.net	Client Hello
2025-01-22 19:45:52	13.107.246.57	443	edge-consumer-static.azureedge.net	Change Ciphe
2025-01-22 19:45:54	4.150.155.223	443	checkappexec.microsoft.com	Client Hello
2025-01-22 19:45:56	5.252.153.241	80	5.252.153.241	GET /api/fi
2025-01-22 19:45:58	23.55.125.176	443	azure.microsoft.com	Client Hello
2025-01-22 19:45:58	5.252.153.241	80	5.252.153.241	GET /api/fi
2025-01-22 19:45:58	5.252.153.241	80	5.252.153.241	GET /151709
2025-01-22 19:45:59	23.55.125.176	443	azure.microsoft.com	Client Hello

Shown above: traffic showing the redirect domain and the final software download page.

2025-01-22 - TRAFFIC ANALYSIS EXERCISE ANSWERS

IP addresses used for C2 traffic:

- 5.252.153.241
- 45.125.66.32
- 45.125.66.252

More details on the post infection traffic are at:

- https://github.com/PaloAltoNetworks/Unit42-timely-threat-intel/blob/main/2025-01-22-IOCs-for-malware-from-fake-Microsoft-Teams-site.txt

The infection documented in the above Github page is from a different fake software site, and the post-infection check-in URLs have a different number because this is a different infected Windows host. Otherwise, all of the post-infection traffic is the same.

That Github page also has file SHA256 hashes for files sent during the infection that you can export from the pcap. This is also information you could add to an incident report.

I'm not sure what this malware is called, but it's clearly malicious.