

## Network Capture Task

WE Innovate

Prepared By Omar Hassan

You work as an analyst at a (SOC). Someone contacts your team to report a coworker has downloaded a suspicious file after searching for **Google Authenticator**.

- 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**

## 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?

- 
1. My first thought is to look into the conversation tab to get a summary or any clue about the IPs that we have. **Statistics > Conversations**

Ethernet · 7		IPv4 · 144		IPv6	TCP · 421	UDP · 346
Address A	Address B	Packets ▾		Bytes	S	
10.1.17.215	45.125.66.32	10,940		10 MB		
10.1.17.215	5.252.153.241	9,076		7 MB		
10.1.17.215	10.1.17.2	4,359		1 MB		
10.1.17.215	82.221.136.26	2,470		2 MB		
10.1.17.215	45.125.66.252	1,369		107 kB		
10.1.17.215	23.55.125.176	1,018		708 kB		

2. There is something going on with ip 10.1.17.215 which is in LAN segment range , therefore I will search for this specific IP and then filter using dns and search for 'google-' to see if there is an impersonation going on , fake google authenticator : **google-authenticator.burleson-appliance.net**.

1-Google Authenticator.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.1.17.215 && dns

Packet list String google- Find Cancel

Options: Narrow & Wide Case sensitive Backwards Multiple occurrences

No.	Time	Source	Destination	Protocol	Length	Info
38518	2857.750513	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0xc74b No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com
26924	1953.517250	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0xc78b No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com
17022	646.752626	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0xc7fa No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com
25108	1216.614587	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0xc850 No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com
37911	2629.814385	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0xc882 No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com
36786	2595.840616	10.1.17.2	10.1.17.215	DNS	196	Standard query response 0xc8bd HTTPS edge.microsoft.com CNAME edge-microsoft-com.dual-a-0036.a-msedge.net CNAME dual-a-0036.a
16530	624.927461	10.1.17.2	10.1.17.215	DNS	113	Standard query response 0xc90b A array804.prod.do.dsp.mp.microsoft.com A 52.175.242.182
25910	1503.553877	10.1.17.2	10.1.17.215	DNS	320	Standard query response 0xc985 A login.microsoftonline.com CNAME login.mso.msidentity.com CNAME ak.privatelink.msidentity.com
27308	2166.277019	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0xc9d9 No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com
31554	2431.326662	10.1.17.2	10.1.17.215	DNS	220	Standard query response 0xca05 HTTPS copilot.microsoft.com CNAME copilot-copilot-msft-com.trafficmanager.net CNAME copilot.mi
37902	2622.213195	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0xca2c No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com
36505	2594.996694	10.1.17.2	10.1.17.215	DNS	282	Standard query response 0xca35 HTTPS config.edge.skype.com CNAME config.edge.skype.com.trafficmanager.net CNAME 1-0007.config
38890	2941.361275	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0xca55 No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com
24003	1057.069876	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0xcb50 No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com
38978	2986.960435	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0xcc07 No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com
2329	38.250143	10.1.17.2	10.1.17.215	DNS	215	Standard query response 0xcc42 A google-authenticator.burleson-appliance.net A 104.21.64.1 A 104.21.48.1 A 104.21.32.1 A 104.
25622	1414.057269	10.1.17.2	10.1.17.215	DNS	148	Standard query response 0xcc50 No such name A ping3.dyngate.com SOA tv-ns1.teamviewer.com

google-authenticator.burleson-appliance.net

Did you intend to search across the file corpus?

11/94 security vendors flagged this domain as malicious

Community Score 11 / 94

google-authenticator.burleson-appliance.net

burleson-appliance.net

3. And then I managed to find another one , so probably there are more that malicious domain , notice the extra o ?

No.	Time	Source	Destination	Protocol	Length	Info
2365	38.863149	10.1.17.215	10.1.17.2	DNS	78	Standard query 0xe6f7 HTTPS authenticatoor.org
17812	722.767575	10.1.17.215	10.1.17.2	DNS	77	Standard query 0xe72f A ping3.dyngate.com
27355	2192.139970	10.1.17.215	10.1.17.2	DNS	131	Standard query 0xe756 SRV ldap.tco.Default-First-Site-Name.sites.dc.msd

authenticatoor.org

Did you intend to search across the file corpus?

12/94 security vendors flagged this domain as malicious

Community Score 12 / 94

authenticatoor.org

5. So therefore we can find that the infected host is indeed 10.1.17.215 and for the rest of the info I will use network miner for ease. (Everything is displayed about this host)

10.1.17.215 [DESKTOP-L8C5GSJ] [DESKTOP-L8C5GSJ.bluemoonuesday.com] [desktop-l8c5gsj] (Windows)

- IP: 10.1.17.215
- MAC: 00D0B7264A74
- NIC Vendor: Intel Corporation
- MAC Age: 2000-09-08
- Hostname: DESKTOP-L8C5GSJ, DESKTOP-L8C5GSJ.bluemoonuesday.com, desktop-l8c5gsj
- OS: Windows
- TTL: 128 (distance: 0)
- Latency: 0.142 ms
- Open TCP Ports:
- Sent: 16032 packets (2,470,879 Bytes)
- Received: 23013 packets (23,007,609 Bytes)
- Incoming sessions: 0
- Outgoing sessions: 405
- Host Details

6. We can also get the username with passwords too using the credentials tab

File Tools Help

Select a network adapter in the list ---

Hosts (311) Files (853) Images Messages Credentials (8) Sessions (491) DNS (1759) Parameters (15465) Keywords

☒ Include Cookies ☒ Include NTLM challenge-responses ☐ Mask Passwords

Enter a keyword filter ☐ Case sensitive ExactPhrase Any column Clear

Client	Server	Protocol	Username	Password
10.1.17.215 [DESKTOP-L8C5GSJ] [DESKTOP-L8C5GSJ.bl...	10.1.17.2 [win-gsh54qlw48d bluemoonuesday.com] [BLUE...	Kerberos	shutchenson	\$krb5pa\$18\$shutchenson\$BLUEMOO...
10.1.17.215 [DESKTOP-L8C5GSJ] [DESKTOP-L8C5GSJ.bl...	10.1.17.2 [win-gsh54qlw48d bluemoonuesday.com] [BLUE...	Kerberos	shutchenson	\$krb5asrep\$18\$BLUEMOONTUESDA...
10.1.17.215 [DESKTOP-L8C5GSJ] [DESKTOP-L8C5GSJ.bl...	10.1.17.2 [win-gsh54qlw48d bluemoonuesday.com] [BLUE...	Kerberos	BLUEMOONTUESDAY.COMhostdesktop-l8c5gsj bluemoo...	\$krb5pa\$18\$\$bluemoonuesday.com\$...
10.1.17.215 [DESKTOP-L8C5GSJ] [DESKTOP-L8C5GSJ.bl...	10.1.17.2 [win-gsh54qlw48d bluemoonuesday.com] [BLUE...	Kerberos	BLUEMOONTUESDAY.COMhostdesktop-l8c5gsj bluemoo...	\$krb5asrep\$18\$BLUEMOONTUESDA...
10.1.17.215 [DESKTOP-L8C5GSJ] [DESKTOP-L8C5GSJ.bl...	10.1.17.2 [win-gsh54qlw48d bluemoonuesday.com] [BLUE...	Kerberos	BLUEMOONTUESDAY.COMhostdesktop-l8c5gsj bluemoo...	\$krb5pa\$18\$\$BLUEMOONTUESDAY...
10.1.17.215 [DESKTOP-L8C5GSJ] [DESKTOP-L8C5GSJ.bl...	10.1.17.2 [win-gsh54qlw48d bluemoonuesday.com] [BLUE...	Kerberos	BLUEMOONTUESDAY.COMhostdesktop-l8c5gsj bluemoo...	\$krb5asrep\$18\$BLUEMOONTUESDA...
10.1.17.215 [DESKTOP-L8C5GSJ] [DESKTOP-L8C5GSJ.bl...	10.1.17.2 [win-gsh54qlw48d bluemoonuesday.com] [BLUE...	Kerberos	shutchenson	\$krb5pa\$18\$shutchenson\$BLUEMOO...
10.1.17.215 [DESKTOP-L8C5GSJ] [DESKTOP-L8C5GSJ.bl...	10.1.17.2 [win-gsh54qlw48d bluemoonuesday.com] [BLUE...	Kerberos	shutchenson	\$krb5asrep\$18\$BLUEMOONTUESDA...

7. Now the remaining question “What are the IP addresses used for C2 servers for this infection?” I suspect those two because they are out of the LAN and have the most packets but we will do further investigation.

Wireshark · Conversations · 1-Google Authenticator.pcap

Conversation Settings

Ethernet · 7 IPv4 · 144 IPv6 TCP · 421 UDP · 346

Name resolution	Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s
	10.1.17.215	45.125.66.32	10,940	10 MB	95	3,737	587 kB	7,203	10 MB	889.561525	1720.6308	272
	10.1.17.215	5.252.153.241	9,076	7 MB	34	3,475	235 kB	5,601	7 MB	60.135270	3142.2528	59

8. I inspect both IPs and find some suspicious commands in the query using http filter & ip.addr

ip.addr== 5.252.153.241 && http						
No.	Time	Source	Destination	Protocol	Length	Info
39370	3170.494838	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39377	3176.097646	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39386	3181.340731	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39397	3186.535218	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39404	3191.727993	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39413	3196.921867	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
39424	3202.128240	10.1.17.215	5.252.153.241	HTTP	103	GET /1517096937 HTTP/1.1
13677	129.210334	10.1.17.215	5.252.153.241	HTTP	176	GET /1517096937?k=message%20=%20startup%20shortcut%20created;%20%20status%20=%20success; HTTP/1.1
19292	881.889559	10.1.17.215	5.252.153.241	HTTP	174	GET /1517096937?k=script:%20RunRH,%20status:%20OK,%20message:%20PS%20process%20started HTTP/1.1
28335	2413.352160	10.1.17.215	5.252.153.241	HTTP	174	GET /1517096937?k=script:%20RunRH,%20status:%20OK,%20message:%20PS%20process%20started HTTP/1.1
33356	2577.662979	10.1.17.215	5.252.153.241	HTTP	174	GET /1517096937?k=script:%20RunRH,%20status:%20OK,%20message:%20PS%20process%20started HTTP/1.1
5031	60.297799	10.1.17.215	5.252.153.241	HTTP	371	GET /api/file/get-file/264872 HTTP/1.1
5063	62.145732	10.1.17.215	5.252.153.241	HTTP	144	GET /api/file/get-file/29842.ps1 HTTP/1.1
13643	128.827817	10.1.17.215	5.252.153.241	HTTP	113	GET /api/file/get-file/TV HTTP/1.1
8002	124.998139	10.1.17.215	5.252.153.241	HTTP	121	GET /api/file/get-file/TeamViewer HTTP/1.1
12890	128.458764	10.1.17.215	5.252.153.241	HTTP	133	GET /api/file/get-file/TeamViewer_Resource_fr HTTP/1.1
13671	128.984576	10.1.17.215	5.252.153.241	HTTP	118	GET /api/file/get-file/pas.ps1 HTTP/1.1
5033	60.464642	5.252.153.241	10.1.17.215	HTTP	819	HTTP/1.1 200 OK
5071	62.309349	5.252.153.241	10.1.17.215	HTTP	555	HTTP/1.1 200 OK
8000	124.958915	5.252.153.241	10.1.17.215	HTTP	444	HTTP/1.1 200 OK

9. There are a lot of suspicious things especially the highlighted packet therefore **5.252.153.241 is a suspicious c2.**