INCIDENT REPORT OF MALWARE ATTACK FROM pcap (2025-01-22-traffic-analysis-exercise-pcap.zip) on malware-traffic-analysis.net

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 packet capture (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.

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**

TASK

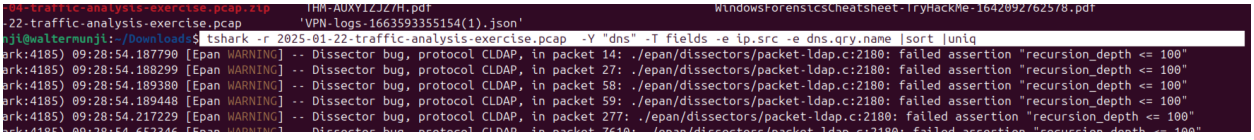
For this exercise, answer the following questions for your incident report:

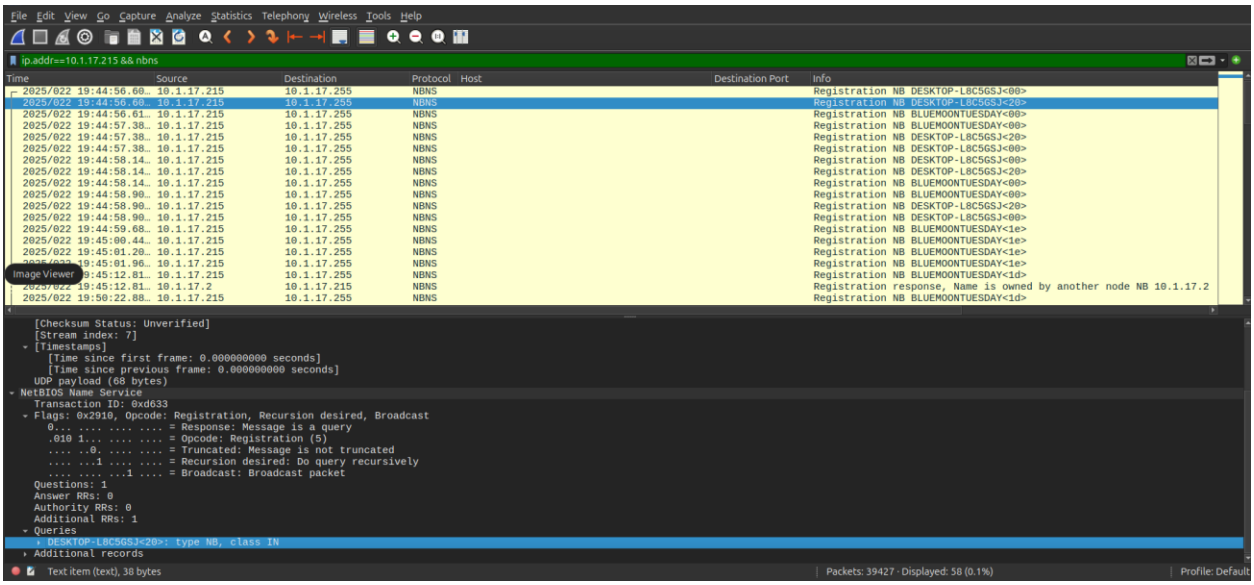
- What is the IP address of the infected Windows client?
- What is the mac address of the infected Windows client?
- What is the host name of the infected Windows client?
- What is the user account name from the infected Windows client?
- What is the likely domain name for the fake Google Authenticator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

Ip address of the desktop, desktop name and malicious site likely to be visited:

10[.]1[.]17[.]215, DESKTOP-L8C5GSJ

Malicious site visited: authenticatoor[.]org





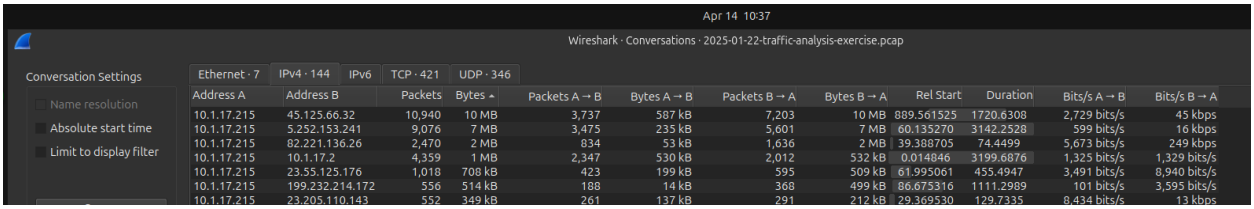
Suspicious communications (C2) with the host:

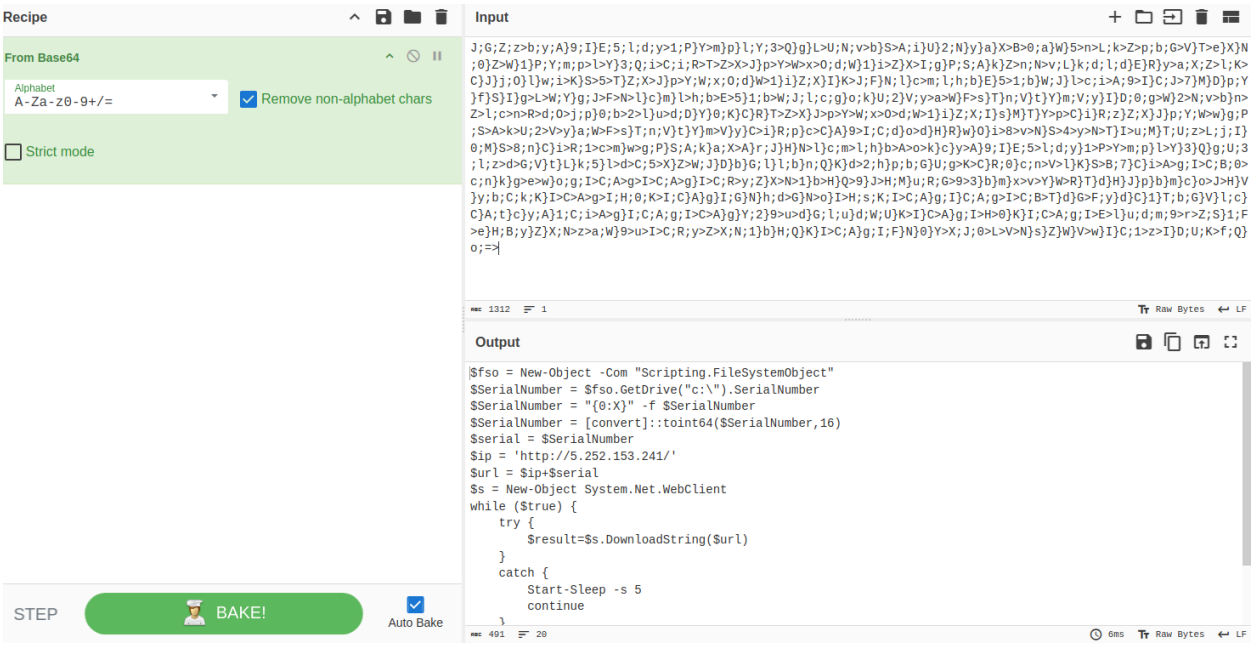
45[.]125[.]66[.]32 -sent many packets labeled as “application data”

45[.]125[.]66[.]252 --sent many packets labeled as “application data” -

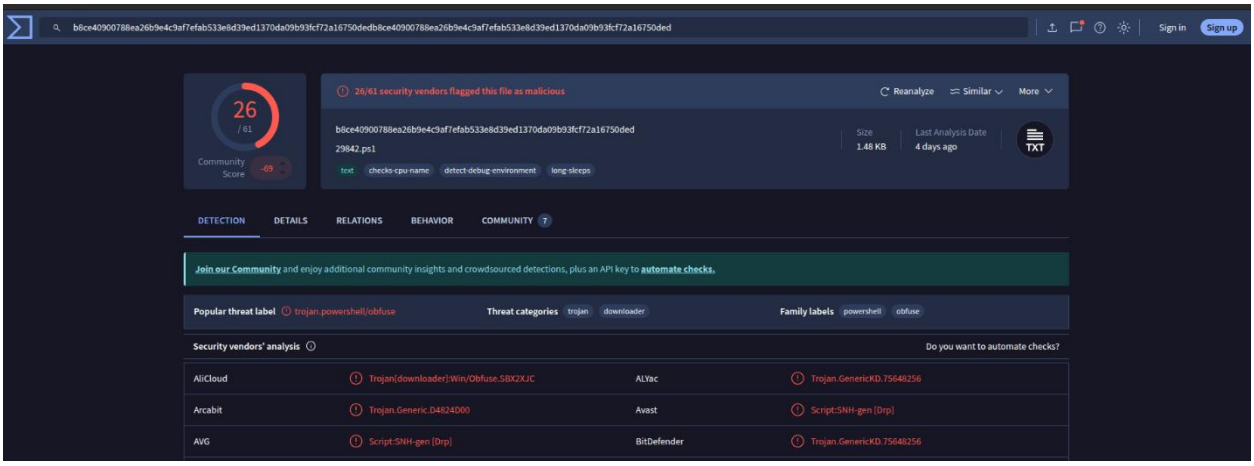
82[.]221[.]136[.]26 – Ip address of the malicious website

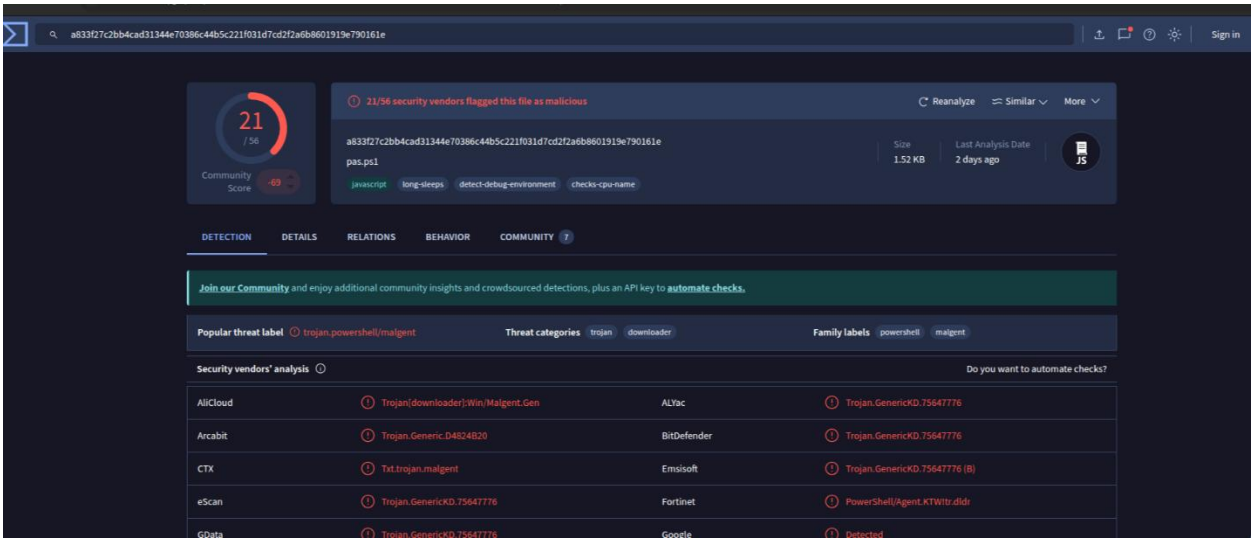
5[.]252[.]153[.]241 - Sent malicious PowerShell script in base64 encoding plus other portable executable files

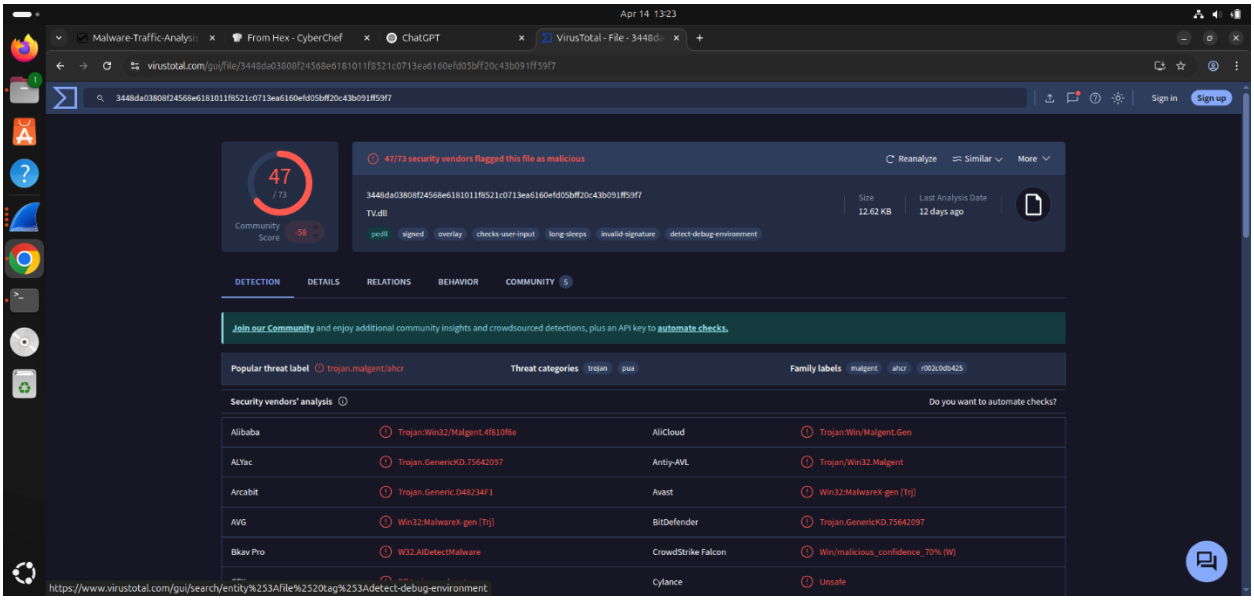





```
waltermunji@waltermunji:~/Documents$ ls
'1517096937%3fk=script%3a%20RunRH,%20status%3a%20OK,%20message%3a%20PS%20process%20started'   connecttest.txt  'index.php%3fid=&subid=qIOuKk7U'  TeamViewer
 29842.ps1                                                                                    index.php         ProcessMAU.txt                   TV
waltermunji@waltermunji:~/Documents$ file 29842.ps1
29842.ps1: ASCII text, with very long lines (1512), with no line terminators
waltermunji@waltermunji:~/Documents$ sha256sum 29842.ps1
b8ce40900788ea26b9e4c9af7efab533e8d39ed1370da09b93fcf72a16750ded  29842.ps1
waltermunji@waltermunji:~/Documents$ file TV
TV: PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows, 10 sections
waltermunji@waltermunji:~/Documents$ sha256sum TV
3448da03808f24568e6181011f8521c0713ea6160efd05bff20c43b091ff59f7  TV
waltermunji@waltermunji:~/Documents$ file TeamViewer
TeamViewer: PE32 executable (GUI) Intel 80386, for MS Windows, 5 sections
waltermunji@waltermunji:~/Documents$ sha256sum TeamViewer
904280f20d697d876ab90a1b74c0f22a83b859e8b0519cb411fda26f1642f53e  TeamViewer
waltermunji@waltermunji:~/Documents$
```


b8ce40900788ea26b9e4c9af7efab533e8d39ed1370da09b93fcf72a16750dedb8ce40900788ea26b9e4c9af7efab533e8d39ed1370da09b93fcf72a16750ded
Sign in
Sign up
26
/ 61
Community Score
-69
26/61 security vendors flagged this file as malicious
Reanalyze
Similar
More
b8ce40900788ea26b9e4c9af7efab533e8d39ed1370da09b93fcf72a16750ded
29842.ps1
text
checks-cpu-name
detect-debug-environment
long-sleeps
Size
1.48 KB
Last Analysis Date
4 days ago
TXT
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 7
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.powershell/obfuse
Threat categories trojan downloader
Family labels powershell obfuse
Security vendors' analysis
Do you want to automate checks?
AliCloud
Trojan[downloader]:Win/Obfuse.SBX2XJC
ALYac
Trojan.GenericKD.75648256
Arcabit
Trojan.Generic.D4824D00
Avast
Script:SNH-gen [Drp]
AVG
Script:SNH-gen [Drp]
BitDefender
Trojan.GenericKD.75648256


a833f27c2bb4cad31344e70386c44b5c221f031d7cd2f2a6b8601919e790161e
Sign in
21
/ 56
Community Score
-69
21/56 security vendors flagged this file as malicious
Reanalyze
Similar
More
a833f27c2bb4cad31344e70386c44b5c221f031d7cd2f2a6b8601919e790161e
pas.ps1
javascript
long-sleeps
detect-debug-environment
checks-cpu-name
Size
1.52 KB
Last Analysis Date
2 days ago
JS
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 7
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.powershell/malgent
Threat categories trojan downloader
Family labels powershell malgent
Security vendors' analysis
Do you want to automate checks?
AliCloud
Trojan[downloader]:Win/Malgent.Gen
ALYac
Trojan.GenericKD.75647776
Arcabit
Trojan.Generic.D4824B20
BitDefender
Trojan.GenericKD.75647776
CTX
Txt.trojan.malgent
Emsisoft
Trojan.GenericKD.75647776 (B)
eScan
Trojan.GenericKD.75647776
Fortinet
PowerShell/Agent.KTW!tr.dldr
GData
Trojan.GenericKD.75647776
Google
Detected


Apr 14 13:23
Malware-Traffic-Analysis
From Hex - CyberChef
ChatGPT
VirusTotal - File - 3448da
virustotal.com/gui/file/3448da03808f24568e6181011f8521c0713ea6160efd05bff20c43b091ff59f7
3448da03808f24568e6181011f8521c0713ea6160efd05bff20c43b091ff59f7
Sign in
Sign up
47
/ 73
Community Score
-58
47/73 security vendors flagged this file as malicious
Reanalyze
Similar
More
3448da03808f24568e6181011f8521c0713ea6160efd05bff20c43b091ff59f7
TV.dll
pedll
signed
overlay
checks-user-input
long-sleeps
invalid-signature
detect-debug-environment
Size
12.62 KB
Last Analysis Date
12 days ago
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 5
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.malgent/ahcr
Threat categories trojan pua
Family labels malgent ahcr r002c0db425
Security vendors' analysis
Do you want to automate checks?
Alibaba
Trojan:Win32/Malgent.4f810f6e
AliCloud
Trojan:Win/Malgent.Gen
ALYac
Trojan.GenericKD.75642097
Antiy-AVL
Trojan/Win32.Malgent
Arcabit
Trojan.Generic.D48234F1
Avast
Win32:MalwareX-gen [Trj]
AVG
Win32:MalwareX-gen [Trj]
BitDefender
Trojan.GenericKD.75642097
Bkav Pro
W32.AIDetectMalware
CrowdStrike Falcon
Win/malicious_confidence_70% (W)
Cylance
Unsafe
https://www.virustotal.com/gui/search/entity%253Afile%2520tag%253Adetect-debug-environment