FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

18 March 2022

FLASH Number

CP-000165-TT

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS/CISA and DOE.

This FLASH has been released **TLP:AMBER**

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact FBI CyWatch immediately with respect to the procedures outlined in the Reporting Notice section of this message.

Email: cywatch@fbi.gov | Phone: **1-855-292-3937**

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

Cyber Actors Perform Increased Reconnaissance of US Energy Sector Networks from Russia-Based IP Addresses

Summary

The FBI is advising all organizations in the US Energy Sector of network scanning activity stemming from multiple IP addresses listed below. These Russia-based IP addresses are believed to be associated with cyber actors who previously conducted destructive cyber activity against foreign critical infrastructure. Present activity of these IP addresses likely indicates early stages of reconnaissance, scanning networks for vulnerabilities for use in potential future intrusions. US Energy Sector entities are advised to examine current network traffic for these IP addresses and conduct follow-on investigations if observed.

Technical Details

FBI technical analysis identified 140 overlapping IP addresses associated with abnormal scanning activity of at least 5 US energy companies and at least 18 US companies in other sectors to include Defense Industrial Base, Financial Services, and Information Technology. While other US critical infrastructure sectors have noticed abnormal scanning, the focus appears to be on entities within the energy sector. The IP addresses have been associated with active scanning of US critical infrastructure from as early as March 2021. This scanning activity has increased since the start of the Russia/Ukraine conflict, leading to a greater possibility of future intrusions. While the FBI recognizes that scanning activity is common on a network, these reported IPs have been previously identified as conducting activity in conjunction with active exploitation of a foreign victim, which resulted in destruction of the victim's systems. Even though these IPs cannot be directly correlated to successful exploitation, the FBI is providing these indicators of compromise out of an abundance of caution. The FBI recommends that network administrators take the appropriate action regarding the provided IP addresses and review their network activity for any malicious activity.

Indicators

- 109.237.103.38
- 151.236.101.19
- 151.236.104.2
- 151.236.106.4
- 151.236.110.2
- 151.236.115.20
- 151.236.118.2
- 151.236.119.2
- 151.236.126.6
- 151.236.127.2
- 151.236.64.24
- 151.236.81.2
- 151.236.82.3
- 151.236.89.13
- 151.236.89.26
- 151.236.92.2
- 151.236.95.2
- 151.236.99.9
- 162.62.191.231
- 178.46.212.0
- 178.49.133.3
- 185.167.121.66
- 185.177.114.98
- 185.25.61.6
- 185.3.142.3
- 185.31.114.25
- 185.31.115.10
- 185.94.111.1
- 188.127.251.15
- 188.191.1.66
- 188.43.225.61
- 193.169.53.130
- 193.33.133.130
- 195.210.169.98
- 212.109.204.130
- 212.188.11.50
- 212.188.22.66
- 212.19.24.64
- 212.83.8.79
- 217.13.220.66
- 217.150.58.9
- 31.200.250.4
- 31.28.1.226
- 37.60.16.54
- 37.8.145.2
- 46.161.54.57
- 5.188.152.194
- 5.61.11.123
- 62.152.61.227
- 62.78.86.130
- 77.243.112.122
- 79.141.210.2
- 81.163.32.42
- 84.47.151.67
- 89.188.167.130
- 89.223.4.2
- 91.231.236.41
- 91.231.237.2
- 91.231.239.2
- 91.238.110.2
- 91.238.111.8
- 92.63.196.25
- 92.63.196.61
- 92.63.197.71
- 93.92.69.34
- 95.182.106.43
- 109.95.198.12
- 176.192.99.26
- 213.110.249.145
- 80.254.126.75
- 92.124.140.196
- 95.182.105.135
- 185.141.225.2
- 185.214.76.130
- 31.180.165.127
- 46.149.110.195
- 5.45.234.205
- 37.18.24.16

- 194.190.76.41
- 213.155.156.184
- 94.100.180.197
- 194.190.76.44
- 151.236.127.145
- 213.180.204.90
- 81.19.74.2
- 104.16.18.94
- 104.16.19.94
- 104.18.10.207
- 104.18.11.207
- 104.46.162.224
- 104.46.162.226
- 13.69.109.130
- 13.69.109.131
- 13.69.116.104
- 13.69.239.72
- 13.69.239.73
- 13.69.239.74
- 13.78.111.198
- 144.172.118.37
- 146.88.240.248
- 146.88.240.4
- 149.154.167.51
- 149.154.167.91
- 149.154.175.100
- 149.154.175.50
- 149.154.175.55
- 154.89.5.86
- 183.136.226.3
- 183.136.226.4
- 185.184.8.65
- 193.107.216.228
- 193.46.255.60
- 20.50.201.195
- 20.50.201.200
- 20.50.73.10
- 20.50.80.209
- 20.50.80.210
- 20.54.89.106
- 20.54.89.15
- 200.73.138.230
- 3.126.56.137
- 31.220.3.140
- 34.98.64.218
- 35.190.43.134
- 35.244.159.8
- 40.79.197.35
- 45.143.200.50
- 45.143.203.3
- 45.146.165.165
- 45.146.165.37
- 45.148.10.241
- 51.104.15.252
- 51.105.71.136
- 51.132.193.105
- 51.89.124.57
- 62.210.13.20
- 80.82.77.193
- 89.248.163.140
- 89.248.165.202
- 89.248.165.60

Information Requested:

Please report any detection of these IPs or other suspicious activities related to research of energy-related industries to your local FBI Field Office or the FBI's 24/7 Cyber Watch (CyWatch).

Recommended Mitigations:

The FBI encourages US critical infrastructure asset owners and operators to regularly assess and monitor their network traffic, personnel with access to these IT and OT systems, and practice contingency plans.

The following recommendations are relevant to many ICS vendors and brands, along with their customers. The best practices listed below are applicable to most products used in US critical infrastructure facilities today.

- Monitor Active Directory and local administrators' group changes.
- Audit logs for all remote connection protocols.
- Limit details on required technical skills and types of equipment used at specific facilities in publicly available job descriptions.
- Ensure the cybersecurity features are always enabled by following the manufacturers' security recommendations and software updates.
- Safety systems should always be deployed on isolated networks.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:AMBER**