مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Iranian Cyber Actors' Brute Force and Credential Access Activity

Tracking #:432316405

Date:17-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed recent activities by Iranian cyber actors targeting critical infrastructure organizations through brute force attacks and credential access techniques.

TECHNICAL DETAILS:

Iranian cyber actors have been observed conducting reconnaissance to gather victim identity information, followed by gaining persistent access through brute force techniques. They utilize compromised accounts to explore networks further, escalating privileges and downloading sensitive data. Since October 2023, these actors have employed tactics such as password spraying and multifactor authentication (MFA) push bombing to compromise user accounts across various sectors, including healthcare, government, and energy. The goal is to obtain sensitive credentials and network information, which are then sold on cybercriminal forums for malicious purposes.

Initial Access Techniques:

- **Brute Force Attacks**: Techniques such as password spraying allow actors to gain access to Microsoft 365 and Azure environments.
- **MFA Push Bombing**: This method involves bombarding users with MFA requests until they inadvertently approve a request.

Lateral Movement:

The actors leverage Remote Desktop Protocol (RDP) for lateral movement within networks, often utilizing legitimate tools like Microsoft Word to execute malicious commands.

Credential Access:

The use of open-source tools enables actors to gather additional credentials through methods like Kerberos Service Principal Name enumeration and password spraying.

Detection Strategies:

Organizations should implement the following detection strategies:

- Monitor for "impossible logins" where user credentials are accessed from geographically distant locations.
- Identify unusual MFA registrations from unfamiliar devices.
- Look for signs of credential dumping or suspicious privileged account activity.

Indicators of Compromise:

- Investigate IP Addresses: Before blocking, verify the legitimacy of the IP addresses by checking historical activity.
- Analyze Activity: If positive hits are found for these IPs, assess whether the activities correspond with known TTPs of Iranian cyber actors.
- Dynamic Nature of IPs: Cyber actors are known to change their IP addresses often, sometimes daily. This makes it crucial for defenders to understand the context before acting.
- VPN Utilization: Many of the listed IP addresses are associated with VPN services, which means they can be used by various legitimate users, not just malicious actors.

IP Address	Date Range		
95.181.234.12	01/30/2024	to	02-07-24
95.181.234.25	01/30/2024	to	02-07-24
173.239.232.20	10-06-23	to	12/19/2023
172.98.71.191	10/15/2023	to	11/27/2023
102.129.235.127	10/21/2023	to	10/22/2023
188.126.94.60	10/22/2023	to	01-12-24
149.40.50.45	10/26/2023		
181.214.166.59	10/26/2023		
212.102.39.212	10/26/2023		
149.57.16.134	10/26/2023	to	10/27/2023
149.57.16.137	10/26/2023	to	10/27/2023
102.129.235.186	10/29/2023	to	11-08-23
46.246.8.138	10/31/2023	to	01/26/2024
149.57.16.160	11-08-23		
149.57.16.37	11-08-23		
46.246.8.137	11/17/2023	to	01/25/2024
212.102.57.29	11/19/2023	to	01/17/2024
46.246.8.82	11/22/2023	to	01/28/2024
95.181.234.15	11/26/2023	to	02-07-24
45.88.97.225	11/27/2023	to	02-11-24
84.239.45.17	12-04-23	to	12-07-23
46.246.8.104	12-07-23	to	02-07-24
37.46.113.206	12-07-23		
46.246.3.186	12-07-23	to	12-09-23
46.246.8.141	12-07-23	to	02-10-24
46.246.8.17	12-09-23	to	01-09-24
37.19.197.182	12/15/2023		
154.16.192.38	12/25/2023	to	01/24/2024
102.165.16.127	12/27/2023	to	01/28/2024
46.246.8.47	12/29/2023	to	01/29/2024
46.246.3.225	12/30/2023	to	02-06-24
46.246.3.226	12/31/2023	to	02-03-24
46.246.3.240	12/31/2023	to	02-06-24
191.101.217.10	01-05-24		
102.129.153.182	01-08-24		
46.246.3.196	01-08-24		
102.129.152.60	01-09-24		
156.146.60.74	01-10-24		
191.96.227.113	01-10-24		
191.96.227.122	01-10-24		
181.214.166.132	01-11-24		
188.126.94.57	01-11-24	to	01/13/2024
154.6.13.144	01/13/2024	to	01/24/2024
154.6.13.151	01/13/2024	to	01/28/2024
188.126.94.166	01/15/2024		
89.149.38.204	01/18/2024		

46.246.8.67	01/20/2024		
46.246.8.53	01/22/2024		
154.16.192.37	01/24/2024		
191.96.150.14	01/24/2024		
191.96.150.96	01/24/2024		
46.246.8.10	01/24/2024		
84.239.25.13	01/24/2024		
154.6.13.139	01/26/2024		
191.96.106.33	01/26/2024		
191.96.227.159	01/26/2024		
149.57.16.150	01/27/2024		
191.96.150.21	01/27/2024		
46.246.8.84	01/27/2024		
95.181.235.8	01/27/2024		
191.96.227.102	01/27/2024	to	01/28/2024
46.246.122.185	01/28/2024		
146.70.102.3	01/29/2024	to	01/30/2024
46.246.3.233	01/30/2024	to	02/15/2024
46.246.3.239	01/30/2024	to	02/15/2024
188.126.89.35	02-03-24		
46.246.3.223	02-03-24		
46.246.3.245	02-05-24	to	02-06-24
191.96.150.50	02-09-24		

Hashes	
1F96D15B26416B2C7043EE7172357AF3AFBB002A	Associated with malicious activity
3D3CDF7CFC881678FEBCAFB26AE423FE5AA4EFEC	Associated with malicious activity

RECOMMENDATIONS:

- **Implement Strong Password Policies**: Ensure all accounts utilize strong, unique passwords that meet NIST guidelines.
- **Adopt Phishing-Resistant MFA**: Transition to MFA solutions that are resistant to phishing attacks.
- **Monitor Authentication Logs**: Regularly review logs for unusual login attempts and patterns indicative of credential misuse.
- **Conduct Cybersecurity Training**: Provide training for employees on recognizing MFA fatigue and suspicious login behaviors.
- **Review IT Helpdesk Protocols**: Ensure that password management procedures align with security policies to prevent common password usage.
- **Validate Security Controls**: Regularly test and validate security measures against the MITRE ATT&CK framework to assess effectiveness.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.
The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a