JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Product ID: AA24-290A

October 16, 2024

Co-Authored by:

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

AFP

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Iranian Cyber Actors' Brute Force and Credential Access Activity Compromises Critical Infrastructure Organizations

Summary

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Communications Security Establishment Canada (CSE), Australian Federal Police (AFP), and Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) are releasing this joint Cybersecurity Advisory to warn network defenders of Iranian cyber actors' use of brute force and other techniques to compromise organizations across multiple critical infrastructure sectors, including the healthcare and public health (HPH), government, information technology, engineering, and energy sectors. The actors likely aim to obtain credentials and information describing the victim's network that can then be sold to enable access to cybercriminals.

Since October 2023, Iranian actors have used brute force, such as password spraying, and multifactor authentication (MFA) 'push bombing' to compromise user accounts and obtain access to organizations. The actors frequently modified MFA registrations, enabling persistent access. The actors performed discovery on the compromised networks to obtain additional credentials and identify other information that could be used to gain additional points of access. The authoring agencies assess the Iranian actors sell

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.

this information on cybercriminal forums to actors who may use the information to conduct additional malicious activity.

This advisory provides the actors' tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs). The information is derived from FBI engagements with entities impacted by this malicious activity.

The authoring agencies recommend critical infrastructure organizations follow the guidance provided in the **Mitigations** section. At a minimum, organizations should ensure all accounts use strong passwords and register a second form of authentication.

For a downloadable list of IOCs, see:

- AA24-290A STIX XML (97KB)
- AA24-290A STIX JSON (82KB)

Technical Details

Note: This advisory uses the MITRE ATT&CK® for Matrix for Enterprise framework, version 15. See the **MITRE ATT&CK Tactics and Techniques** section in **Appendix A** for a table of the actors' activity mapped to MITRE ATT&CK tactics and techniques.

Overview of Activity

The actors likely conduct reconnaissance operations to gather victim identity [T1589] information. Once obtained, the actors gain persistent access to victim networks frequently via brute force [T1110]. After gaining access, the actors use a variety of techniques to further gather credentials, escalate privileges, and gain information about the entity's systems and network. The actors also move laterally and download information that could assist other actors with access and exploitation.

Initial Access and Persistence

The actors use valid user and group email accounts [T1078], frequently obtained via brute force such as password spraying [T1110.003] although other times via unknown methods, to obtain initial access to Microsoft 365, Azure [T1078.004], and Citrix systems [T1133]. In some cases where push notification-based MFA was enabled, the actors send MFA requests to legitimate users seeking acceptance of the request. This technique—bombarding users with mobile phone push notifications until the user either approves the request by accident or stops the notifications— is known as "MFA fatigue" or "push bombing" [T1621].

Once the threat actors gain access to an account, they frequently register their devices with MFA to protect their access to the environment via the valid account:

- In two confirmed compromises, the actors leveraged a compromised user's open registration for MFA [T1556.006] to register the actor's own device [T1098.005] to access the environment.
- In another confirmed compromise, the actors used a self-service password reset (SSPR) tool associated with a public facing Active Directory Federation Service (ADFS) to reset the accounts with expired passwords [T1484.002] and then registered MFA through Okta for compromised accounts without MFA already enabled [T1556] [T1556.006].

The actors frequently conduct their activity using a virtual private network (VPN) service [T1572]. Several of the IP addresses in the actors' malicious activity originate from exit nodes tied to the Private Internet Access VPN service.

Lateral Movement

The actors use Remote Desktop Protocol (RDP) for lateral movement [T1021.001]. In one instance, the actors used Microsoft Word to open PowerShell to launch the RDP binary `mstsc.exe` [T1202].

Credential Access

The actors likely use open-source tools and methodologies to gather more credentials. The actors performed Kerberos Service Principal Name (SPN) enumeration of several service accounts and received Kerberos tickets [T1558.003]. In one instance, the actors used the Active Directory (AD) Microsoft Graph Application Program Interface (API) PowerShell application likely to perform a directory dump of all AD accounts. Also, the actors imported the tool [T1105] `DomainPasswordSpray.ps1`, which is openly available on GitHub [T1588.002], likely to conduct password spraying. The actors also used the command `Cmdkey /list,` likely to display usernames and credentials [T1555].

Privilege Escalation

In one instance, the actors attempted impersonation of the domain controller, likely by exploiting Microsoft's Netlogon (also known as "Zerologon") privilege escalation vulnerability (CVE-2020-1472) [T1068].

Discovery

The actors leverage living off the land (LOTL) to gain knowledge about the target systems and internal networks. The actors used the following Windows command-line tools to gather information about domain controllers [T1018], trusted domains [T1482], lists of domain administrators, and enterprise administrators [T1087.002] [T1069.002] [T1069.003]:

- `Nltest /dclist`
- `Nltest /domain_trusts`
- `Nltest /domain_trusts/all_trusts`
- `Net group "Enterprise admins" /domain`
- `Net group "Domain admins" /domain`

Next, the actors used the following Lightweight Directory Access Protocol (LDAP) query in PowerShell [T1059.001] to search the AD for computer display names, operating systems, descriptions, and distinguished names [T1082].

```
$i=0
$D=
[System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDom
ain()
$L='LDAP://' . $D
$D = [ADSI]$L
```

```
$Date = $((Get-Date).AddDays(-90).ToFileTime())
$str =
'(&(objectcategory=computer)(operatingSystem=*serv*)(|(lastlogon
>='+$Date+')(lastlogontimestamp>='+$Date+')))'
$s = [adsisearcher]$str
$s.searchRoot = $L.$D.distinguishedName
$s.PropertiesToLoad.Add('cn') > $Null
$s.PropertiesToLoad.Add('operatingsystem') > $Null
$s.PropertiesToLoad.Add('description') > $Null
$s.PropertiesToLoad.Add('distinguishedName') > $Null
Foreach ($CA in $s.FindAll()) {
      Write-Host $CA.Properties.Item('cn')
      $CA.Properties.Item('operatingsystem')
      $CA. Properties.Item('description')
      $CA.Properties.Item('distinguishedName')
      $i++
}
Write-host Total servers: $i
```

Command and Control

On one occasion, using `msedge.exe,` the actors likely made outbound connections to Cobalt Strike Beacon command and control (C2) infrastructure [T1071.001].

Exfiltration and Collection

In a couple instances, while logged in to victim accounts, the actors downloaded files related to gaining remote access to the organization and to the organization's inventory [T1005], likely exfiltrating the files to further persist in the victim network or to sell the information online.

Detection

To detect brute force activity, the authoring agencies recommend reviewing authentication logs for system and application login failures of valid accounts and looking for multiple, failed authentication attempts across all accounts.

To detect the use of compromised credentials in combination with virtual infrastructure, the authoring agencies recommend the following steps:

- Look for "impossible logins," such as suspicious logins with changing usernames, user agent strings, and IP address combinations or logins where IP addresses do not align to the user's expected geographic location.
- Look for one IP used for multiple accounts, excluding expected logins.
- Look for "impossible travel." Impossible travel occurs when a user logs in from multiple IP addresses with significant geographic distance (i.e., a person could not realistically travel between the geographic locations of the two IP addresses during the period between the logins). **Note:** Implementing this detection opportunity can result in false positives if legitimate users apply VPN solutions before connecting into networks.

- Look for MFA registrations with MFA in unexpected locales or from unfamiliar devices.
- Look for processes and program execution command-line arguments that may indicate credential dumping, especially attempts to access or copy the `ntds.dit` file from a domain controller.
- Look for suspicious privileged account use after resetting passwords or applying user account mitigations.
- Look for unusual activity in typically dormant accounts.
- Look for unusual user agent strings, such as strings not typically associated with normal user activity, which may indicate bot activity.

Mitigations

The authoring agencies recommend organizations implement the mitigations below to improve organizations' cybersecurity posture based on the actors' TTPs described in this advisory. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA. The CPGs, which are organized to align to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, are a subset of cybersecurity practices, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people. These voluntary CPGs strive to help small- and medium-sized organizations kick-start their cybersecurity efforts by prioritizing investment in a limited number of essential actions with high-impact security outcomes. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

- Review IT helpdesk password management related to initial passwords, password resets for user lockouts, and shared accounts. IT helpdesk password procedures may not align to company policy for user verification or password strength, creating a security gap. Avoid common passwords (e.g. "Spring2024" or "Password123!").
- Disable user accounts and access to organizational resources for departing staff [CPG 2.D]. Disabling accounts can minimize system exposure, removing options actors can leverage for entry into the system. Similarly, create new user accounts as close as possible to an employee's start date.
- Implement phishing-resistant MFA [CPG 2.H]. See CISA's resources Phishing-Resistant Multifactor Authentication and More than a Password for additional information on strengthening user credentials.
- Continuously review MFA settings to ensure coverage over all active, internet-facing protocols to ensure no exploitable services are exposed [CPG 2.W].
- Provide basic cybersecurity training to users [CPG 2.I] covering concepts such as:
  - Detecting unsuccessful login attempts [CPG 2.G].
  - Having users deny MFA requests they have not generated.
  - Ensuring users with MFA-enabled accounts have MFA set up appropriately.
- Ensure password policies align with the latest NIST Digital Identity Guidelines.

- Meeting the minimum password strength [CPG 2.B] by creating a password using 8-64 nonstandard characters and long passphrases, when possible.

- Disable the use of RC4 for Kerberos authentication.

These mitigations apply to critical infrastructure entities across sectors.

The authoring agencies also recommend software manufacturers incorporate secure by design principles and tactics into their software development practices to protect their customers against actors using compromised credentials, thereby strengthening the security posture of their customers. For more information on secure by design, see CISA's Secure by Design webpage and joint guide.

Validate Security Controls

In addition to applying mitigations, the authoring agencies recommend exercising, testing, and validating organization security programs against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring agencies recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 1** to **Table 12**).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring agencies recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

Contact Information

Organizations are encouraged to report suspicious or criminal activity related to information in this advisory to:

- CISA via CISA's 24/7 Operations Center [report@cisa.gov or 1-844-Say-CISA (1-844-729-2472)] or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- For NSA cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

Intrusion events connected to this Iranian group may also include a different set of cyber actors–likely the third-party actors who purchased access from the Iranian group via cybercriminal forums or other channels. As a result, some TTPs and IOCs noted in this advisory may be tied to these third-party actors, not the Iranian actors. The TTPs and IOCs are in the advisory to provide recipients the most complete picture of malicious activity that may be observed on compromised networks. However, exercise caution if formulating attribution assessments based solely on matching TTPs and IOCs.

Version History

October 16, 2024: Initial version.

Appendix A: MITRE ATT&CK Tactics and Techniques

See **Tables 1–12** for all referenced actors' tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Table 1: Reconnaissance

Technique Title	ID	Use
Gather Victim Identity Information	T1589	The actors likely gathered victim information.

Table 2: Resource Development

Technique Title	ID	Use
Obtain Capabilities: Tool	T1588.002	The actors obtained a password spray tool through an open-source repository.

Table 3: Initial Access

Technique Title	ID	Use
Valid Accounts	T1078	The actors used password spraying to obtain valid user and group email account credentials, allowing them access to the network.
Valid Accounts: Cloud Accounts	T1078.004	The actors used accounts hosted on Microsoft 365, Azure, and Okta cloud environments as additional methods for initial access.
External Remote Services	T1133	The actors exploited Citrix systems' external-facing remote services as another method for gaining initial access to the system.

Table 4: Execution

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	The actors used PowerShell commands to maintain and expand access.

Table 5: Persistence

Technique Title	ID	Use
Account Manipulation: Device Registration	T1098.005	The actors used PowerShell commands to maintain and expand access.
Modify Authentication Process	T1556	The actors used a public facing Active Directory Federation Service (ADFS) domain to reset the passwords of expired accounts.
Modify Authentication Process: Multi-Factor Authentication	T1556.006	The actors used an MFA bypass method, such as Multi-Factor Authentication Request Generation, providing the ability to modify or completely disable MFA defenses.

Table 6: Privilege Escalation

Technique Title	ID	Use
Exploitation for Privilege Escalation	T1068	The actors attempted impersonation of the domain controller likely by exploiting CVE-2020-1472, Microsoft's Netlogon Privilege Escalation vulnerability.
Domain or Tenant Policy Modification: Trust Modification	T1484.002	The actors leveraged a public-facing ADFS password reset tool to reactivate inactive accounts, allowing the actor to authenticate and enroll their devices as any user in the AD managed by the victim tenant.

Table 7: Defense Evasion

Technique Title	ID	Use
Indirect Command Execution	T1202	The actors attempted impersonation of the Domain Controller likely by exploiting CVE-2020-1472, Microsoft's Netlogon Privilege Escalation vulnerability.

Table 8: Credential Access

Technique Title	ID	Use
Brute Force: Password Spraying	T1110.003	The actors targeted applications, including Single Sign-on (SSO) Microsoft Office 365, using brute force password sprays and imported the tool `DomainPasswordSpray.ps1`.
Credentials from Password Stores	T1555	The actors used the command `Cmdkey /list` likely to display usernames and credentials.

Technique Title	ID	Use
Steal or Forge Kerberos Tickets: Kerberoasting	T1558.003	The actors performed Kerberos Service Principal Name (SPN) enumeration of several service accounts and received Rivest Cipher 4 (RC4) tickets.
Multi-Factor Authentication Request Generation	T1621	The actors sent MFA requests to legitimate users.

Table 9: Discovery

Technique Title	ID	Use
Remote System Discovery	T1018	The actors used LOTL to return information about domain controllers.
Permission Groups Discovery: Domain Groups	T1069.002	The actors used LOTL to return lists of domain administrators and enterprise administrators.
Permission Groups Discovery: Cloud Groups	T1069.003	The actors used LOTL to return lists of domain administrators and enterprise administrators.
System Information Discovery	T1082	The actors were able to query the AD to discover display names, operating systems, descriptions, and distinguished names from the computer.
Account Discovery: Domain Account	T1087.002	The actors used LOTL to return lists of domain administrators and enterprise administrators.
Domain Trust Discovery	T1482	The actors used LOTL to return information about trusted domains.

Table 10: Lateral Movement

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	The actors used Microsoft Word to open PowerShell to launch RDP binary `mstsc.exe`.

Table 11: Collection

Technique Title	ID	Use
Data from Local System	T1005	The actors downloaded files related to remote access methods and the organization's inventory.

Table 12: Command and Control

Technique Title	ID	Use
Application Layer Protocol: Web Protocols	T1071.001	The actors used `msedge.exe` to make outbound connections likely to Cobalt Strike Beacon C2 infrastructure.
Ingress Tool Transfer	T1105	The actors imported a tool from GitHub and used it to conduct password spraying.
Protocol Tunneling	T1572	The actors frequently conduct targeting using a virtual private network (VPN).

Appendix B: Indicators of Compromise

See **Tables 13 to 15** for IOCs obtained from FBI investigations.

Table 13: Malicious Files Associated with Iranian Cyber Actors

Hash	Description
1F96D15B26416B2C7043EE7172357AF3AFBB002A	Associated with malicious activity.
3D3CDF7CFC881678FEBCAFB26AE423FE5AA4EFEC	Associated with malicious activity.

Table 14: Network Indicators

Disclaimer: The authoring organizations recommend network defenders investigate or vet IP addresses prior to taking action, such as blocking, as many cyber actors are known to change IP addresses, sometimes daily, and some IP addresses may host valid domains. Many of the IP addresses provided below are assessed VPN nodes and as such are not exclusive to the Iranian actors' use. The authoring organizations do not recommend blocking these IP addresses based solely on their inclusion in this JCSA. The authoring organizations recommend using the below IP addresses to search for previous activity the actors may have conducted against networks. If positive hits for these IP addresses are identified, the authoring organizations recommend making an independent determination if the observed activity aligns with the TTPs outlined in the JCSA. The timeframes included in the table reflect the timeframe the actors likely used the IPs.

IP Address	Date Range
95.181.234.12	01/30/2024 to 02/07/2024
95.181.234.25	01/30/2024 to 02/07/2024
173.239.232.20	10/06/2023 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 01/12/2024
149.40.50.45	10/26/2023
181.214.166.59	10/26/2023
212.102.39.212	10/26/2023

IP Address	Date Range
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 11/08/2023
46.246.8.138	10/31/2023 to 01/26/2024
149.57.16.160	11/08/2023
149.57.16.37	11/08/2023
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 02/07/2024
45.88.97.225	11/27/2023 to 02/11/2024
84.239.45.17	12/04/2023 to 12/07/2023
46.246.8.104	12/07/2023 to 02/07/2024
37.46.113.206	12/07/2023
46.246.3.186	12/07/2023 to 12/09/2023
46.246.8.141	12/07/2023 to 02/10/2024
46.246.8.17	12/09/2023 to 01/09/2024
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 02/06/2024

IP Address	Date Range
46.246.3.226	12/31/2023 to 02/03/2024
46.246.3.240	12/31/2023 to 02/06/2024
191.101.217.10	01/05/2024
102.129.153.182	01/08/2024
46.246.3.196	01/08/2024
102.129.152.60	01/09/2024
156.146.60.74	01/10/2024
191.96.227.113	01/10/2024
191.96.227.122	01/10/2024
181.214.166.132	01/11/2024
188.126.94.57	01/11/2024 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

IP Address	Date Range
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	02/03/2024
46.246.3.223	02/03/2024
46.246.3.245	02/05/2024 to 02/06/2024
191.96.150.50	02/09/2024

Table 15: Devices

Device Type	Description
Samsung Galaxy A71 (SM-A715F)	Registered with MFA
Samsung SM-G998B	Registered with MFA
Samsung SM-M205F	Registered with MFA