JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-321A

November 17, 2021

Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities

This joint cybersecurity advisory is the result of an analytic effort among the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Australian Cyber Security Centre (ACSC), and the United Kingdom's National Cyber Security Centre (NCSC) to highlight ongoing malicious cyber activity by an advanced persistent threat (APT) group that FBI, CISA, ACSC, and NCSC assess is associated with the government of Iran. FBI and CISA have observed this Iranian government-sponsored APT group exploit Fortinet vulnerabilities since at least March 2021 and a Microsoft Exchange ProxyShell vulnerability since at least October 2021 to gain initial access to systems in advance of follow-on operations, which include deploying ransomware. ACSC is also aware this APT group has used the same Microsoft Exchange vulnerability in Australia.

Actions to take today to protect against Iranian state-sponsored malicious cyber activity:

- Immediately patch software affected by the following vulnerabilities: CVE-2021-34473, 2018-13379, 2020-12812, and 2019-5591.
- Implement multi-factor authentication.
- Use strong, unique passwords.

The Iranian government-sponsored APT actors are actively targeting a broad range of victims across multiple U.S. critical infrastructure sectors, including the Transportation Sector and the Healthcare and Public Health Sector, as well as Australian organizations. FBI, CISA, ACSC, and NCSC assess the actors are focused on exploiting known vulnerabilities rather than targeting specific sectors. These Iranian government-sponsored APT actors can leverage this access for follow-on operations, such as data exfiltration or encryption, ransomware, and extortion.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. 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. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov. Australian organizations can visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

This advisory provides observed tactics and techniques, as well as indicators of compromise (IOCs) that FBI, CISA, ACSC, NCSC assess are likely associated with this Iranian government-sponsored APT activity. The FBI, CISA, ACSC, and NCSC urge critical infrastructure organizations to apply the recommendations listed in the Mitigations section of this advisory to mitigate risk of compromise from Iranian government-sponsored cyber actors.

For more information on Iranian government-sponsored malicious cyber activity, see us-cert.cisa.gov/Iran.

TECHNICAL DETAILS

Threat Actor Activity

Since at least March 2021, the FBI and CISA have observed Iranian government-sponsored APT actors leverage Microsoft Exchange and Fortinet vulnerabilities to target a broad range of victims across multiple critical infrastructure sectors in furtherance of malicious activities. Observed activity includes the following.

- In March 2021, the FBI and CISA observed these Iranian government-sponsored APT actors scanning devices on ports 4443, 8443, and 10443 for Fortinet FortiOS vulnerability CVE-2018-13379, and enumerating devices for FortiOS vulnerabilities CVE-2020-12812 and CVE-2019-5591. The Iranian Government-sponsored APT actors likely exploited these vulnerabilities to gain access to vulnerable networks. **Note**: for previous FBI and CISA reporting on this activity, refer to joint Cybersecurity Advisory: APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attacks.
- In May 2021, these Iranian government-sponsored APT actors exploited a Fortigate appliance to access a webserver hosting the domain for a U.S. municipal government. The actors likely created an account with the username `elie` to further enable malicious activity. **Note**: for previous FBI reporting on this activity, refer to FBI FLASH: APT Actors Exploiting Fortinet Vulnerabilities to Gain Initial Access for Malicious Activity.
- In June 2021, these APT actors exploited a Fortigate appliance to access environmental control networks associated with a U.S.-based hospital specializing in healthcare for children. The Iranian government-sponsored APT actors likely leveraged a server assigned to IP addresses `91.214.124[.]143` and `162.55.137[.]20`—which FBI and CISA judge are associated with Iranian government cyber activity—to further enable malicious activity against the hospital's network. The APT actors accessed known user accounts at the hospital from IP address `154.16.192[.]70`, which FBI and CISA judge is associated with government of Iran offensive cyber activity.
- As of October 2021, these APT actors have leveraged a Microsoft Exchange ProxyShell vulnerability—CVE-2021-34473—to gain initial access to systems in advance of follow-on operations.

ACSC considers that this APT group has also used the same Microsoft Exchange vulnerability (CVE-2021-34473) in Australia.

MITRE ATT&CK® Tactics and Techniques

Note: this advisory uses the MITRE ATT&CK for Enterprise framework, version 10. See Appendix B for a table of the MITRE ATT&CK tactics and techniques observed.

FBI, CISA, ACSC, and NCSC assess the following tactics and techniques are associated with this activity.

Resource Development [TA0042]

The APT actors have used the following malicious and legitimate tools [T1588.001, T1588.002] for a variety of tactics across the enterprise spectrum.

- Mimikatz for credential theft [TA0006]
- WinPEAS for privilege escalation [TA0004]
- SharpWMI (Windows Management Instrumentation)
- WinRAR for archiving collected data [TA0009, T1560.001]
- FileZilla for transferring files [TA0010]

Initial Access [TA0001]

The Iranian government-sponsored APT actors gained initial access by exploiting vulnerabilities affecting Microsoft Exchange servers (CVE-2021-34473) and Fortinet devices (CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591) [T1190].

Execution [TA0002]

The Iranian government-sponsored APT actors may have made modifications to the Task Scheduler [T1053.005]. These modifications may display as unrecognized scheduled tasks or actions. Specifically, the below established tasks may be associated with this activity:

- `SynchronizeTimeZone`
- `GoogleChangeManagement`
- `MicrosoftOutLookUpdater`
- `MicrosoftOutLookUpdateSchedule`

Persistence [TA0003]

The Iranian government-sponsored APT actors may have established new user accounts on domain controllers, servers, workstations, and active directories [T1136.001, T1136.002]. Some of these accounts appear to have been created to look similar to other existing accounts on the network, so specific account names may vary per organization. In addition to unrecognized user accounts or accounts established to masquerade as existing accounts, the following account usernames may be associated with this activity:

- `Support`
- `Help`
- `elie`
- `WADGUtilityAccount`

Exfiltration [TA0010]

The FBI and CISA observed outbound File Transfer Protocol (FTP) transfers over port 443.

Impact [TA0040]

The APT actors forced BitLocker activation on host networks to encrypt data [T1486]. The corresponding threatening notes were either sent to the victim or left on the victim network as a `.txt` file. The ransom notes included ransom demands and the following contact information.

- sar_addr@protonmail[.]com
- WeAreHere@secmail[.]pro
- nosterrmann@mail[.]com
- nosterrmann@protonmail[.]com

DETECTION

The FBI, CISA, ACSC, and NCSC recommend that organizations using Microsoft Exchange servers and Fortinet investigate potential suspicious activity in their networks.

- Search for IOCs. Collect known-bad IOCs and search for them in network and host artifacts. **Note**: refer to Appendix A for IOCs.
- Investigate exposed Microsoft Exchange servers (both patched and unpatched) for compromise.
- Investigate changes to Remote Desktop Protocol (RDP), firewall, and Windows Remote Management (WinRM) configurations that may allow attackers to maintain persistent access.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating-system defined or recognized scheduled tasks for unrecognized “actions” (for example, review the steps each scheduled task is expected to perform).
- Review antivirus logs for indications they were unexpectedly turned off.
- Look for WinRAR and FileZilla in unexpected locations.

Note: for additional approaches on uncovering malicious cyber activity, see joint advisory Technical Approaches to Uncovering and Remediating Malicious Activity, authored by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.

MITIGATIONS

The FBI, CISA, ACSC, and NCSC urge network defenders to apply the following mitigations to reduce the risk of compromise by this threat.

Patch and Update Systems

- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Immediately patch software affected by vulnerabilities identified in this advisory: CVE-2021-34473, CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591.

Evaluate and Update Blocklists and Allowlists

- Regularly evaluate and update blocklists and allowlists.
- If FortiOS is not used by your organization, add the key artifact files used by FortiOS to your organization's execution blocklist. Any attempts to install or run this program and its associated files should be prevented.

Implement and Enforce Backup and Restoration Policies and Procedures

- Regularly back up data, air gap, and password protect backup copies offline.
- Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).

Implement Network Segmentation

- Implement network segmentation to restrict adversary's lateral movement.

Secure User Accounts

- Audit user accounts with administrative privileges and configure access controls under the principles of least privilege and separation of duties.
- Require administrator credentials to install software.

Implement Multi-Factor Authentication

- Use multifactor authentication where possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems.

Use Strong Passwords

- Require all accounts with password logins to have strong, unique passwords.

Secure and Monitor RDP and other Potentially Risky Services

- If you use RDP, restrict it to limit access to resources over internal networks.
- Disable unused remote access/RDP ports.
- Monitor remote access/RDP logs.

Use Antivirus Programs

- Install and regularly update antivirus and anti-malware software on all hosts.

Secure Remote Access

- Only use secure networks and avoid using public Wi-Fi networks.
- Consider installing and using a VPN for remote access.

Reduce Risk of Phishing

- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

RESOURCES

- For more information on Iranian government-sponsored malicious cyber activity, see us-cert.cisa.gov/Iran.
- For information and resources on protecting against and responding to ransomware, refer to StopRansomware.gov, a centralized, whole-of-government webpage providing ransomware resources and alerts.
- The joint advisory from the cybersecurity authorities of Australia, Canada, New Zealand, the United Kingdom, and the United States: Technical Approaches to Uncovering and Remediating Malicious Activity provides additional guidance when hunting or investigating a network and common mistakes to avoid in incident handling.
- CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.
- The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to $10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ website for more information and how to report information securely.
- ACSC can provide tailored cyber security advice and assistance, reporting, and incident response support at cyber.gov.au and via 1300 292 371 (1300 CYBER1).

APPENDIX A: INDICATORS OF COMPROMISE

IP addresses and executables files are listed below.

IP Addresses

- 91.214.124[.]143
- 162.55.137[.]20
- 154.16.192[.]70

Executable Files

Executable files observed in this activity are identified in table 1.

Table 1: Executable Files

Filename:	**MicrosoftOutLookUpdater[.]exe**
MD5:	1444884faed804667d8c2bfa0d63ab13
SHA-1	95E045446EFB8C9983EBFD85E39B4BE5D92C7A2A
SHA-256:	c51fe5073bd493c7e8d83365aace3f9911437a0f2ae80042ba01ea46b55d2624
SHA-512:	6451077B99C5F8ECC5C0CA88FE272156296BEB91218B39AE28A086DBA5E7E39813F044F9AF0FEDBB260941B1CD52FA237C098CBF4B2A822F08E3E98E934D0ECF
Filename:	**MicrosoftOutlookUpdater.bat**
MD5:	1A44368EB5BF68688BA4B4357BDC874F
SHA-1	FA36FEBFD5A5CA0B3A1B19005B952683A7188A13
SHA-256	3A08D0CB0FF4D95ED0896F22F4DA8755525C243C457BA6273E08453E0E3AC4C4
SHA-512	70AA89449EB5DA1D84B70D114EF9D24CB74751CE12D12C783251E51775C89FDCE61B4265B43B1D613114D6A85E9C75927B706F39C576DBB036079C7E8CAF28B2
Filename:	**MicrosoftOutlookUpdater.xml**
MD5:	47333937109F86BA292DC44CD3676F80
SHA-1	A8674983A45BD88A4D11BCFD686C2BF8182831A0
SHA-256	AC72790230817E6A72EF3A95B5F1F27144E56082606C425AD14C1F3D2FB2C5BD
SHA-512	A03F0D73136CBCACAEA5C8F7607F4A09F2DF9030D30735DB2E033DA668353636E0FCF7A2AA0B81691A6D7C30CFA67EC9707F7456615E007C025242DBFB6BCCF0

Filename:	MicrosoftOutlookUpdateSchedule.xml
MD5:	AA40C49E309959FA04B7E5AC111BB770
SHA-1	F1D90E10E6E3654654E0A677763C9767C913F8F0
SHA-256	5C818FE43F05F4773AD20E0862280B0D5C66611BB12459A08442F55F148400A6
SHA-512	E55A86159F2E869DCDB64FDC730DA893718E20D65A04071770BD32CAE75FF8C34704BDF9F72EF055A3B362759EDE3682B3883C4D9BCF87013076638664E8078E
Filename:	**GoogleChangeManagement.xml**
MD5:	AF2D86042602CBBDCC7F1E8EFA6423F9
SHA-1	CDCD97F946B78831A9B88B0A5CD785288DC603C1
SHA-256	4C691CCD811B868D1934B4B8E9ED6D5DB85EF35504F85D860E8FD84C547EBF1D
SHA-512	6473DAC67B75194DEEAEF37103BBA17936F6C16FFCD2A7345A5A46756996FAD748A97F36F8FD4BE4E1F264ECE313773CC5596099D68E71344D8135F50E5D8971
Filename:	**Connector3.exe**
MD5:	e64064f76e59dea46a0768993697ef2f
Filename:	**Audio.exe or frpc.exe**
MD5:	b90f05b5e705e0b0cb47f51b985f84db
SHA-1	5bd0690247dc1e446916800af169270f100d089b
SHA-256:	28332bdbfaeb8333dad5ada3c10819a1a015db9106d5e8a74beaaf03797511aa
Vhash:	017067555d5d15541az28!z
Authentihash:	ed463da90504f3adb43ab82044cddab8922ba029511da9ad5a52b8c20bda65ee
Imphash:	93a138801d9601e4c36e6274c8b9d111
SSDEEP:	98304:MeOuFco2Aate8mjOaFEKC8KZ1F4ANWyJXf/X+g4:MeHFV2AatevjOaDC8KZ1xNWy93U
Note:	Identical to “frpc.exe” available at: https://github[.]com/fatedier/frp/releases/download/v0.34.3/frp_0.34.3_windows_amd64.zip
Filename:	**Frps.exe**
MD5:	26f330dadcdd717ef575aa5bfcdbe76a

SHA-1	c4160aa55d092cf916a98f3b3ee8b940f2755053
SHA-256:	d7982ffe09f947e5b4237c9477af73a034114af03968e3c4ce462a029f072a5a
Vhash:	017057555d6d141az25!z
Authentihash:	40ed1568fef4c5f9d03c370b2b9b06a3d0bd32caca1850f509223b3cee2225ea
Imphash:	91802a615b3a5c4bcc05bc5f66a5b219
SSDEEP:	196608:/qTLyGAlLrOt8enYfrhkhBnfY0NIPvoOQiE:GLHiLrSfY5voO
Note:	Identical to “frps.exe” available at: https://github[.]com/fatedier/frp/releases/download/v0.33.0/frp_0.33.0_windows_amd64.zip

APPENDIX B: MITRE ATT&CK TACTICS AND TECHNIQUES

Table 2 identifies MITRE ATT&CK Tactics and techniques observed in this activity.

Table 2: Observed Tactics and Techniques

Tactic	Technique
Resource Development [TA0042]	Obtain Capabilities: Malware [T1588.001]
	Obtain Capabilities: Tool [T1588.002]
Initial Access [TA0001]	Exploit Public-Facing Application [T1190]
Execution [TA0002]	Scheduled Task/Job: Scheduled Task [T1053.005]
Persistence [TA0003]	Create Account: Local Account [T1136.001]
	Create Account: Domain Account [T1136.002]
Privilege Escalation [TA0004]	
Credential Access [TA0006]	
Collection [TA0009]	Archive Collected Data: Archive via Utility [T1560.001]
Exfiltration [TA0010]	
Impact [TA0040]	Data Encrypted for Impact [T1486]