JOINT
CYBERSECURITY
ADVISORY

*Authored by:*

INCD
Israel National
Cyber Directorate

TLP:CLEAR Product ID: JCSA-20241030-001
October 30, 2024

# New Tradecraft of Iranian Cyber Group Aria Sepehr Ayandehsazan aka Emennet Pasargad

## Summary

The Federal Bureau of Investigation (FBI), U.S. Department of Treasury, and Israel National Cyber Directorate are releasing this Cybersecurity Advisory (CSA) to warn network defenders of new cyber tradecraft of the Iranian cyber group Emennet Pasargad, which has been operating under the company name Aria Sepehr Ayandehsazan (ASA) and is known by the private sector terms Cotton Sandstorm, Marnanbridge, and Haywire Kitten. The group exhibited new tradecraft in its efforts to conduct cyber-enabled information operations into mid-2024 using a myriad of cover personas, including multiple cyber operations that occurred during and targeting the 2024 Summer Olympics – including the compromise of a French commercial dynamic display provider. ASA has also undertaken a project to harvest content from IP cameras and used online resources related to Artificial Intelligence. Since 2023, the group has exhibited new tradecraft including the use of fictitious hosting resellers to provision operational server infrastructure to its own actors as well as to an actor in Lebanon involved in website hosting. Recently released reporting from Microsoft indicates this group has demonstrated interest in election-related websites and media outlets, suggesting preparations for future influence operations.

This CSA provides the threat group's tactics, techniques, and procedures (TTPs), including its leveraging of online resources related to Artificial Intelligence, and indicators of compromise (IOCs). The CSA also highlights similar activity from a previous FBI advisory that was published on 20 October 2022. This new advisory's information and guidance are derived from FBI investigative activity and technical analysis of this group's intrusion activity against U.S. and foreign organizations and engagements with numerous entities impacted by this malicious activity.

The authoring agencies recommend all organizations follow guidance provided in the **Mitigations** section to defend against the Iranian cyber group's activities.

If you suspect your organization has been targeted or compromised by the Iranian cyber actors, the authoring agencies recommend immediately contacting your local FBI field office for assistance.

For more information on Iranian state-sponsored malicious cyber activity, see CISA's Iran Cyber Threat webpage.

# Threat Actor Details

## Details on Threat Group and Prior Activity

FBI previously reported in a Private Industry Notification[1] (PIN) that Emennet Pasargad[2, 3] has been conducting hack-and-leak operations against organizations primarily in Israel. FBI assesses these operations are intended to undermine public confidence in the security of the victim's network and data, as well as embarrass victim companies and targeted countries. These hack-and-leak campaigns involve a combination of hacking/theft of data and information operations that impact victims through financial losses and reputational damage. Similar to the Emennet campaign that targeted the 2020 U.S. Presidential election[4], FBI judges the group's recent campaigns include a mix of computer intrusion activity and exaggerated or fictitious claims of access to victim networks or stolen data to enhance the psychological effects of their operations.

Since the publication of this PIN, FBI has acquired new information on cyber tradecraft the group has employed in recent cyber operations impacting numerous countries, including Israel, France, Sweden, and the U.S. Further details regarding the "Anzu Team" cyber-enabled information operation against Sweden have been outlined in public statements made by Swedish government authorities.[5,6] Recently released information from Microsoft indicates this group has been actively scouting election-related websites and media outlets, suggesting preparations for more direct influence operations as Election Day nears.[7]

## New Attribution Details

FBI obtained reliable information in mid-2024 indicating Emennet Pasargad has more recently been using the Iranian company name Aria Sepehr Ayandehsazan (ASA, Iranian Registration Number 504415) as a nominal cover, including for human resources and financial-related purposes.

---

[1] FBI | PIN | Iranian Cyber Group Emennet Pasargad Conducting Hack-and-leak Operations Using False-Flag Personas | 20 October 2022 | ic3.gov/Media/News/2022/221020.pdf.
[2] Emennet Pasargad was previously known as Eeleyanet Gostar. (Reference: justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed)
[3] The U.S. Department of State's Rewards for Justice program is offering a reward of up to $10 million for information on Emennet Pasargad malign activities. Learn more at https://rewardsforjustice.net/rewards/emennet-pasargad/.
[4] For additional details, reference justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed.
[5] Statement from Swedish Security Service: https://www.sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2024-09-24-dataintrang-bakom-paverkanskampanj.html.
[6] Statement from Sweden Prosecutor's Office: https://www.aklagare.se/nyheter-press/pressmeddelanden/2024/september/grovt-dataintrang-utfort-av-iran.
[7] Microsoft report with Cotton Sandstorm information: https://blogs.microsoft.com/on-the-issues/2024/10/23/as-the-u-s-election-nears-russia-iran-and-china-step-up-influence-efforts/

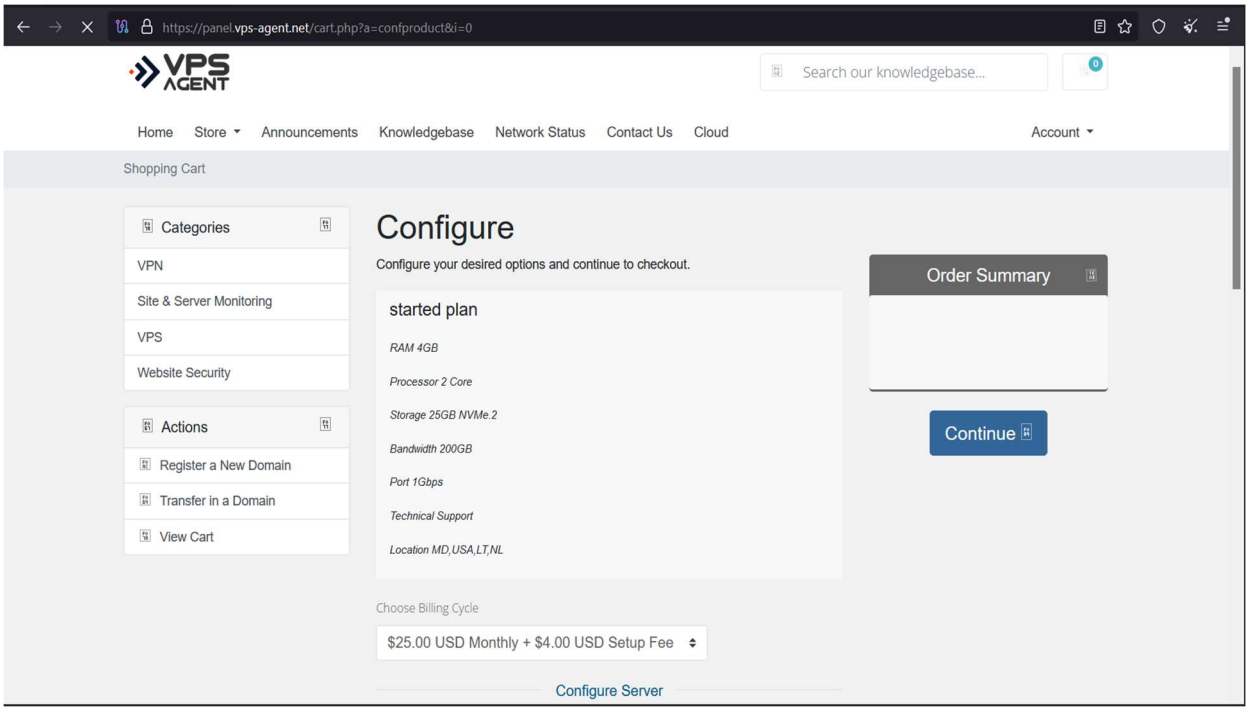

(ASA logo from company letterhead)

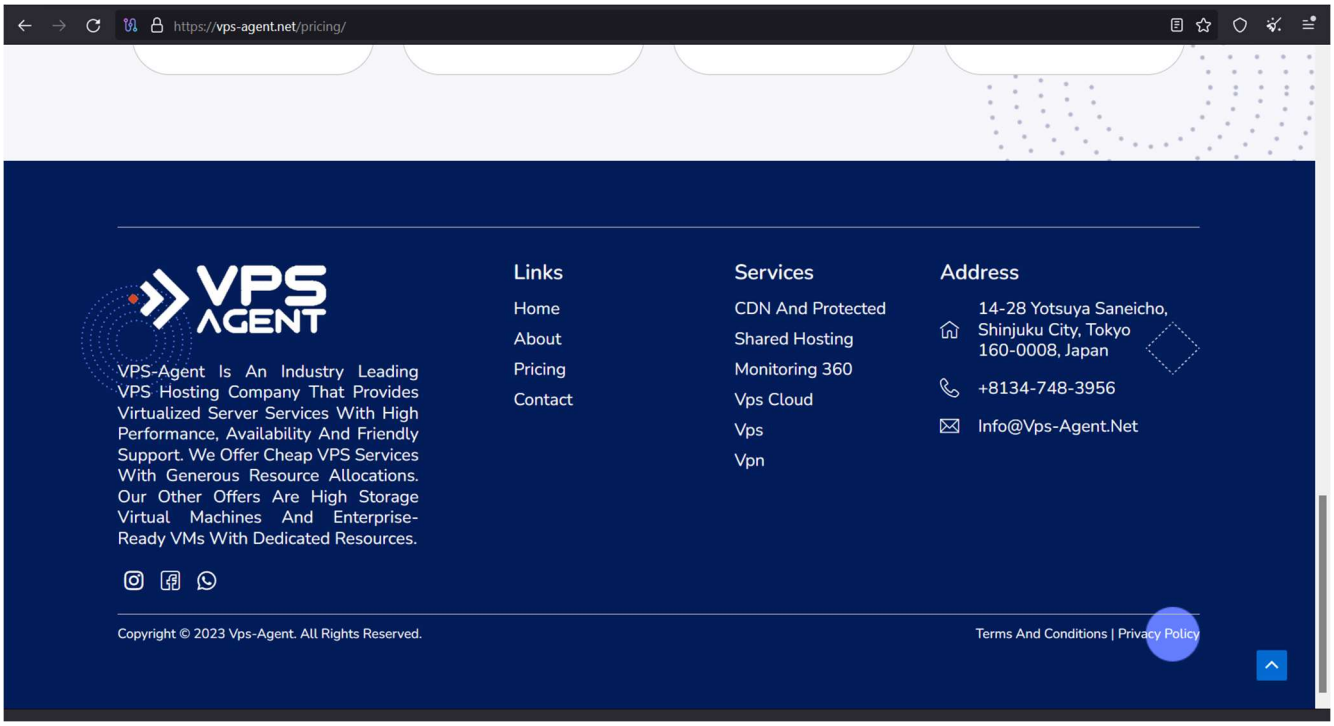
## New Infrastructure Tradecraft

FBI also acquired information indicating that since approximately mid-2023, ASA has used several cover hosting providers for infrastructure management and obfuscation. These two providers are "Server-Speed" (server-speed[.]com) and "VPS-Agent" (vps-agent[.]net[8]). Whereas actors typically procure virtual infrastructure from hosting resellers, ASA set up its own resellers and procured server space from Europe-based providers, including the Lithuania-based company BAcloud and Stark Industries Solutions/PQ Hosting (located in the United Kingdom and Moldova, respectively). ASA then leverages these cover re-sellers to provision operational servers to its own cyber actors for malicious cyber activities. FBI has also observed ASA using these cover re-sellers to provide technical support to identified Lebanon-based individuals, including with hosting for HAMAS-affiliated or themed websites. For example, FBI assesses the website alqassam[.]ps - a website associated with the military wing of HAMAS - was supported by both ASA and its contacts in Lebanon. ASA has also provided hosting support for Lebanon-based actors operating the website almaq.org.

FBI assesses these cover hosting providers were set up by ASA to centralize and manage provisioning of operational infrastructure, while providing plausible deniability that malicious infrastructure was being assigned by a legitimate hosting provider. FBI previously observed ASA use "Server-Speed" from approximately April 2023 until May 2024, when the actors pivoted to using the entity "VPS-Agent."

[8] This domain has been seized in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 1030(i) and 21 U.S.C. § 853 issued by the United States District Court for the Southern District of New York as part of a joint law enforcement operation and action by The United States Attorney's Office for the Southern District of New York and the Federal Bureau of Investigation.




(Images of vps-agent[.]net website)

## Continuing Cyber-Enabled Information Operations

The authoring agencies have continued to observe ASA conducting cyber-enabled information operations over the past year. In particular, following the October 7, 2023, HAMAS attack against Israel, ASA used various cover personas such as "Cyber Flood" and "Contact-HSTG." In its “Contact-HSTG” operation, ASA attempted to contact family members of Israeli hostages, likely in an effort to cause additional psychological effects and inflict further trauma on family members. An example of this messaging is shown below:


SMS translation:

*“Family*

*This the message from Al-Qasam*

*We offered your government hostage exchange deal, but*

*It did not accept it.*

*This is our message:*

*Releasing all the Zionists hostages in exchange*

*To all Palestinians prisoners*

*In order to know what is the condition of all your hostages*

*Keep in touch with us”*

ASA was also responsible for a cyber-enabled influence operation in December 2023 that impacted a US-based Internet Protocol Television (IPTV) streaming company. The operation, which used the persona name "For-Humanity," leveraged unauthorized access to IPTV streaming services to disseminate crafted

messaging pertaining to the Israel-HAMAS military conflict. The authoring agencies warn that future ASA cyber operations may either directly target, or collaterally impact, US organizations.

The authoring agencies assess that, since April 2024, ASA has used the online persona “Cyber Court” to promote the activities of several purported hacktivist groups conducting malicious activity against various countries as a means of protesting the Israel-HAMAS conflict in Gaza. Using “Cyber Court,” ASA promotes the hacking activities of cover-hacktivist groups - run by ASA itself - including “Makhlab al-Nasr,” “NET Hunter,” “Emirate Students Movement,” and “Zeus is Talking.” “Cyber Court” posted updates regarding these groups' purported activities on its Telegram channel (@cybercourt_io) as well as its website cybercourt[.]io[9]. ASA has also been developing an information operation campaign named ”Sample,” intended to intimidate Israelis via crowdsourcing reporting to positively identify specified individuals, such as members of Israeli law enforcement.

(Content related to ”Sample” information operations campaign)

In July 2024, the actors used "VPS-agent" infrastructure to compromise a French commercial dynamic display provider, attempting to display photo montages denouncing the participation of Israeli athletes in the 2024 Olympic and Paralympic Games. This cyberattack was coupled with disinformation maneuvers including publication of a fake news article onto a French collaborative media website and the spread of threat messages to several Israeli athletes and their entourage under the banner of a fake French far-right group 'Regiment GUD', impersonating the real French far-right group 'GUD'.

## IP Camera Targeting Activity

ASA also undertook a significant effort to enumerate and obtain content from IP cameras in Israel, including hours after the October 7, 2023, HAMAS attack. ASA enumerated IP addresses running the Real Time Streaming Protocol (TCP Port 554), primarily in Israel but also in Gaza and Iran. ASA made images and content from Israeli cameras available for clients to access via several servers beginning in October 2023, including 5.230.56[.]148 and 77.91.74[.]158 – the latter IP being used between January and

[9] This domain has been seized in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 1030(i) and 21 U.S.C. § 853 issued by the United States District Court for the Southern District of New York as part of a joint law enforcement operation and action by The United States Attorney’s Office for the Southern District of New York and the Federal Bureau of Investigation.

October 2024. FBI has reliable information indicating this platform currently resides at the following three IP addresses:

- 195.26.87[.]80
- 213.109.147[.]97
- 185.110.188[.]112

Below is an example of Iranian camera content obtained by ASA:


### Harvesting of Open Source Information

Also following October 7, 2023, ASA attempted to identify information concerning Israeli fighter pilots and UAV operators by searching for information across numerous platforms including Pastebin and LinkedIn. ASA also used a Python script to identify location data from Instagram and correlate the data with the service openstreetmap.org. ASA uses numerous online services for identifying people, reverse-image searching, and username checks through open source software including knowem.com, facecheck.id, socialcatfish.com. The actors also use online resources such as ancestry.com and familysearch.org in their operations. ASA will also search for information concerning previously leaked data sets, including using the resource ghostproject.fr.

### Incorporation of Artificial Intelligence into Operations

The aforementioned "For-Humanity" operation is well-known for its incorporation of generative Artificial Intelligence (an AI-generated news anchor) as part of its messaging efforts. This is consistent with a greater ASA effort to incorporate AI-related services into its operations including using the Remini AI Photo Enhancer, Voicemod (voicemod.net) and Murf AI (murf.ai) for voice modulation, and Appy Pie for image generation.

## Technical Details

**Note:** This advisory uses the MITRE ATT&CK® for Enterprise framework, version 15.1. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques. 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.

## Overview of Observed Tactics, Techniques, and Procedures

The following sections outline cyber TTPs used by the ASA group during its current and historical cyber operations.

ASA will likely seek opportunities where they can achieve a high number of compromises with minimal effort by targeting hosting providers that would offer access to other entities, or targeting a specific content management system used by entities in a specific sector.

## Reconnaissance, Initial Access, Persistence, and Credential Access

ASA leverages numerous types of online datasets to conduct research against its targets, including both individual users and organizations. When targeting individuals , ASA uses websites to identify email addresses associated with particular domains, conduct username checks against social media, and reverse image and email searching. When conducting target reconnaissance and enumeration against organizations, ASA uses open source resources such as Shodan, IP2location, and subdomainfinder.c99[.]nl.

For initial access and exploitation, ASA uses commercially available tools such as Masscan, Acunetix, Burp Suite, and SQLMap.

## Resource Development

ASA has used the aforementioned cover hosting resellers "Server-Speed" and "VPS-Agent" to procure operational infrastructure. The actors also heavily leverage commercial VPN service providers such as Private Internet Access, Windscribe, ExpressVPN, Urban VPN, and NordVPN.

## Credential Access

ASA has accessed victim infrastructure via automated password-guessing attempts as well as online resources for cracking password hashes.

## Command and Control

ASA has used an exploitation tool for gathering information about an end point and running remote commands.

ASA has also used the file 'Google Chrome Installer.msi', which is a Microsoft Software Installer package file. This file originally contained the instructions and information needed to install a security patch for the Google Chrome Web browser (version 126.0.6478.255). The msi file has been altered to run an executable after the Google Chrome install/update. This executable was compiled with the name bd.exe and was compiled by the threat actor under a project name of 'bd'.

The 'bd' executable is a remote access trojan (RAT) program that is heavily obfuscated. This program will collect basic system information about the infected computer and connect to a web-server that is specified when the program is run on the command line, when an appropriate de-obfuscation key is also passed on

the command line. As encoded in this specific MSI package, the de-obfuscation key is '8765' and the web-server address is 'connect.il-cert.net'. Once the malicious MSI package is run, Google Chrome will be installed on the victim computer and then the RAT is executed. This malicious program will check in to the web-server and await instructions to be passed to it via responses to the requests 'bd' issues.

## MITRE ATT&CK Tactics and Techniques

See **Table 1** to **Table** for all referenced threat actor tactics and techniques in this advisory and previous FBI reports on this particular actor.

*Table 1. Reconnaissance*

| Technique Title | ID | Use or Assessed Use |
|---|---|---|
| Search Open Technical Databases | T1596 | Shodan (Shodan[.]io) to identify internet infrastructure hosting devices hosting IP cameras |
| Gather Victim Identity Information | T1589 | Online resources such as knowem[.]com, facecheck[.]id, ancestry[.]com, socialcatfish[.]com, and peekyou[.]com |
| Email Addresses | T1589.002 | Online resources such as snov[.]io, email-format[.]com, and hunter[.]io |
| Employee Names | T1589.003 | Researching potential victims on social media, including Instagram and LinkedIn, |
| Determine Physical Location | T1591.001 | Online searching for information concerning military bases and the Israeli Air Force flight academy \| Use of mapping resources such as Wikimapia[.]org |
| Active Scanning | T1595.002 | Actors use Acunetix to conduct vulnerability scans against target infrastructure \| Use of Burp Suite |
| Gather Victim Network Information: Domain Properties | T1590.001 | Actors use subdomainfinder.c99[.]nl for reconnaissance on target |
| Active Scanning: Scanning IP Blocks | T1595.001 | Actors use the Masscan application |
| Search Open Technical Databases | T1596 | Actors use the resource ip2location[.]com |

*Table 2. Resource Development*

| Technique Title | ID | Use or Assessed Use |
|---|---|---|
| Acquire Access | T1650 | ASA seeks out leaked datasets, including ones containing account credentials, from online resources such as ghostproject[.]fr |

| Technique Title | ID | Use or Assessed Use |
|---|---|---|
| Acquire Infrastructure | T1583 | Use of commercial VPN service providers such as Private Internet Access, Windscribe, Express VPN, NordVPN, and Urban VPN |
| Acquire Infrastructure | T1583 | ASA has obtained operational servers from its cover-hosting resellers (server-speed[.]com and more recently vps-agent[.]net) |
| Develop Capabilities | T1587 | Weaponization of CVE 2023-38831 exploit |

*Table 3. Initial Access*

| Technique Title | ID | Use or Assessed Use |
|---|---|---|
| Initial Access | T1190 | The actors use SQLMap to exploit target infrastructure via SQL injection |

*Table 4. Credential Access*

| Technique Title | ID | Use or Assessed Use |
|---|---|---|
| Bruce Force: Password Guessing | T1110.001 | Accessing victim infrastructure via automated password-guessing attempts |
| Bruce Force: Password Cracking | T1110.002 | Online resources for cracking password hashes such as crackstation[.]net, hashes[.]com, and md5hashing[.]net |

*Table 5. Command and Control*

| Technique Title | ID | Use or Assessed Use |
|---|---|---|
| Application Layer Protocol: Web Protocols | T1071.001 | Use of exploitation tool on victims to gather information about an end point and running remote commands. Has the ability to maintain persistence when added to the Windows Startup directory. |
| Remote Access Trojan | T1219 | Collects basis system information about an infected computer and connect to a specified web-server when the program is run on the command line. Will check in to the web-server and await instructions. Packaged with Google Chrome installer. |

# Indicators of Compromise

## IP Address and Domain Identifiers

**Disclaimer:** The IP addresses listed in **Table 6** were observed in use by the cyber actors in the specified timeframes. The authoring agencies recommend organizations investigate or vet these IP addresses prior to taking action, such as blocking the IPs. The authoring agencies do not recommend blocking the indicators based solely on their inclusion in this CSA. This data is being provided for informational purposes and to enable better tracking and attribution of these cyber actors.

*Table 6. Indicators of Compromise – Historical*

| Indicator | Beginning of Actor Association | End of Actor Association |
|---|---|---|
| 45.140.146[.]139 | June 2024 | September 2024 |
| 45.84.0[.]237 | May 2024 | September 2024 |
| 45.140.146[.]197 | June 2024 | September 2024 |
| 45.140.146[.]137 | May 2024 | September 2024 |
| 45.84.0[.]254 | June 2024 | September 2024 |
| 45.142.212[.]21 | July 2024 | September 2024 |
| 45.140.146[.]108 | June 2024 | September 2024 |
| 45.140.146[.]208 | June 2024 | September 2024 |
| 85.206.170[.]160 – 85.206.170[.]191 | September 2024 | October 2024 |
| 85.206.167[.]224 – 85.206.167[.]255 | August 2023 | June 2024 |
| 85.206.169[.]64 – 85.206.169[.]79 | May 2023 | May 2024 |
| 85.206.169[.]80 – 85.206.169[.]95 | May 2023 | March 2024 |
| onlinelive[.]info | August 2023 | August 2024 |
| zeusistalking[.]io | August 2024 | October 2024 |
| zeusistalking[.]net | July 2024 | August 2024 |
| zeusistalking[.]com | July 2024 | July 2024 |

| Indicator | Beginning of Actor Association | End of Actor Association |
|---|---|---|
| rgud-group[.]net | July 2024 | August 2024 |
| rgud-group[.]com | July 2024 | July 2024 |
| cyberflood[.]io | October 2023 | October 2023 |
| cybercourt[.]io | April 2024 | September 2024 |
| 213.109.147[.]63 | August 2024 | October 2024 |
| 146.19.254[.]61 | September 2024 | October 2024 |
| 31.42.177[.]114 | August 2024 | October 2024 |
| pro-today[.]org | March 2024 | October 2024 |
| il-cert[.]net | October 2024 | October 2024 |
| 45.143.167[.]87 | October 2024 | October 2024 |
| 45.143.166[.]233 | October 2024 | October 2024 |

## Malicious file Identifiers

*Table 1. Indicators of Compromise*

| Indicator | SHA256 | Context |
|---|---|---|
| First.exe | **4431b2a4d7758907f81fb1a0c1e36b2ce03e08d43123b1c398487770afd20727** | **45.120.177[.]8 communicates with malicious file. Communicates to following paths:**<br>**http[:]//onlinelive.info/wez/insert.php**<br>**http[:]//onlinelive.info/wez/api.php** |

| Indicator | SHA256 | Context |
|---|---|---|
| Google Chrome Installer.msi | 6f765dda126e830c6cd2c7938dbb970d03be728e82c00388903a4ef3f9ecc853 | Collects basis system information about an infected computer and connect to a specified web-server when the program is run on the command line. Will check in to the web-server and await instructions. Packaged with Google Chrome installer. |

## Mitigations

The authoring agencies recommend all organizations implement the mitigations listed below to improve their cybersecurity posture based on the Iranian cyber group's activities.

These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance designed to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

The authoring agencies recommend all organizations implement the following mitigations:

- Closely review any successful authentications to your network or company accounts from Virtual Private Network services such as Private Internet Access, Windscribe, ExpressVPN, Urban VPN, and NordVPN.
- If your organization's information was previously compromised, take appropriate measures to ensure security measures are in place to protect against the leveraging of any exfiltrated data to conduct further malicious activity against your network.
- Employ regular updates to applications and the host operating system to ensure protection against known vulnerabilities.
- Establish, and backup offline, a "known good" version of the relevant server and a regular change management policy to enable monitoring for alterations to servable content with a file integrity system.
- Employ user input validation to restrict local and remote file inclusion vulnerabilities.
- Implement a least-privileges policy on the Webserver to:
    - Reduce adversaries' ability to escalate privileges or pivot laterally to other hosts.
    - Control creation and execution of files in particular directories.

- If not already present, consider deploying a demilitarized zone (DMZ) between your organization's Web-facing systems and corporate network. Limiting the interaction and logging traffic between the two provide a method to identify possible malicious activity.
- Consider reputable hosting services for websites and content management systems (CMS), if you need assistance in configuring and maintaining your external facing applications.
- Consider employing a Web Application Firewall (WAF) to block inbound malicious traffic.
- Review the logs generated by security devices for signs that your organization's external networks are being scanned for vulnerabilities.
- Ensure a secure configuration of Webservers. All unnecessary services and ports should be disabled or blocked. All necessary services and ports should be restricted where feasible. This can include whitelisting or blocking external access to administration panels and not using default login credentials.
- Use a reverse proxy or alternative service to restrict accessible URL paths to known legitimate ones.
- Conduct regular system and application vulnerability scans to establish areas of risk. While this method does not protect against zero-day attacks, it will highlight possible areas of concern.
- Disable CMS features if they are not needed, and configure them to:
  - Disable remote file editing
  - Restrict file execution to specific directories
  - Limit login attempts applications.

## Validate Security Controls

In addition to applying mitigations, the authoring agencies recommend exercising, testing, and validating your organization's security program 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** ).
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.

## Reporting

Your organization has no obligation to respond or provide information back to FBI in response to this joint advisory. If, after reviewing the information provided, your organization decides to provide information to FBI, reporting must be consistent with applicable state and federal laws.

### Other Incidents

US organizations are encouraged to report suspicious or criminal activity related to information in this advisory to FBI's Internet IC3 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.

## 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.

## Version History

October 30, 2024: Initial version.