



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations

Release Date: August 28, 2024

Alert Code: AA24-241A

RELATED TOPICS: [CYBER THREATS AND ADVISORIES](#), [MALWARE, PHISHING, AND RANSOMWARE](#), [NATION-STATE THREATS](#)

Summary

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Defense Cyber Crime Center (DC3) are releasing this joint Cybersecurity Advisory (CSA) to warn network defenders that, as of August 2024, a group of Iran-based cyber actors continues to exploit U.S. and foreign organizations. This includes organizations across several sectors in the U.S. (including in the education, finance, healthcare, and defense sectors as well as local government entities) and other countries (including in Israel, Azerbaijan, and the United Arab Emirates). The FBI assesses a significant percentage of these threat actors' operations against US organizations are intended to

obtain and develop network access to then collaborate with ransomware affiliate actors to deploy ransomware. The FBI further assesses these Iran-based cyber actors are associated with the Government of Iran (GOI) and—separate from the ransomware activity—conduct computer network exploitation activity in support of the GOI (such as intrusions enabling the theft of sensitive technical data against organizations in Israel and Azerbaijan).

This CSA provides the threat actor's tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs), as well as highlights similar activity from a previous advisory ([Iran-Based Threat Actor Exploits VPN Vulnerabilities <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-259a>](https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-259a)) that the FBI and CISA published on Sept. 15, 2020. The information and guidance in this advisory are derived from FBI investigative activity and technical analysis of this group's intrusion activity against U.S. organizations and engagements with numerous entities impacted by this malicious activity.

The FBI recommends all organizations follow guidance provided in the **Mitigations** section of this advisory to defend against the Iranian cyber actors' activity.

If organizations believe they have been targeted or compromised by the Iranian cyber actors, the FBI and CISA recommend immediately contacting your [local FBI field office <https://www.fbi.gov/contact-us/field-offices>](https://www.fbi.gov/contact-us/field-offices) for assistance and/or reporting the incident via CISA's [Incident Reporting Form <https://www.cisa.gov/report>](https://www.cisa.gov/report) (see the **Reporting** section of this advisory for more details and contact methods).

Give Feedback

For more information on Iran state-sponsored malicious cyber activity, see CISA's [Iran Cyber Threat <https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran>](https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran) webpage.

Download the PDF version of this report:




[AA24-241A Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations </sites/default/files/2024-08/aa24-241a-iran-based-cyber-actors-enabling-ransomware-attacks-on-us-organizations_0.pdf>](https://www.fbi.gov/sites/default/files/2024-08/aa24-241a-iran-based-cyber-actors-enabling-ransomware-attacks-on-us-organizations_0.pdf)

(PDF, 582.01 KB)

For a downloadable copy of IOCs, see:

 **AA24-241A STIX XML** /sites/default/files/2024-08/aa24-241a.stix_.xml

(XML, 29.02 KB)

 **AA24-241A STIX JSON** /sites/default/files/2024-08/aa24-241a-iran-based-cyber-actors-enabling-ransomware-attacks-on-us-organizations.stix_.json

(JSON, 29.19 KB)

Threat Actor Details

Background on Threat Group and Prior Activity

This advisory outlines activity by a specific group of Iranian cyber actors that has conducted a high volume of computer network intrusion attempts against U.S. organizations since 2017 and as recently as August 2024. Compromised organizations include U.S.-based schools, municipal governments, financial institutions, and healthcare facilities. This group is known in the private sector by the names Pioneer Kitten, Fox Kitten, UNC757, Parisite, RUBIDIUM, and Lemon Sandstorm.[1 <https://attack.mitre.org/versions/v15/groups/g0117/>][2 <https://www.crowdstrike.com/blog/who-is-pioneer-kitten/>] The actors also refer to themselves by the moniker Br0k3r, and as of 2024, they have been operating under the moniker “xplfinder” in their channels. FBI analysis and investigation indicate the group’s activity is consistent with a cyber actor with Iranian state-sponsorship.

The FBI previously observed these actors attempt to monetize their access to victim organizations on cyber marketplaces. A significant percentage of the group’s US-focused cyber activity is in furtherance of obtaining and maintaining technical access to victim networks to enable future ransomware attacks. The actors offer full domain control privileges, as well as domain admin credentials, to numerous networks worldwide. More

Give Feedback

recently, the FBI identified these actors collaborating directly with ransomware affiliates to enable encryption operations in exchange for a percentage of the ransom payments. These actors have collaborated with the ransomware affiliates NoEscape[3

<https://www.sentinelone.com/anthology/noescape/>], Ransomhouse[4

<https://www.sentinelone.com/anthology/ransomhouse/>], and ALPHV (aka BlackCat)

(#StopRansomware: ALPHV Blackcat [https://www.cisa.gov/news-events/cybersecurity-](https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a)

[advisories/aa23-353a](https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a)). The Iranian cyber actors' involvement in these ransomware attacks goes beyond providing access; they work closely with ransomware affiliates to lock victim networks and strategize on approaches to extort victims. The FBI assesses these actors do not disclose their Iran-based location to their ransomware affiliate contacts and are intentionally vague as to their nationality and origin.

Furthermore, the FBI has historically observed this actor conduct hack-and-leak campaigns, such as the late 2020 campaign known as Pay2Key.[5

<https://attack.mitre.org/versions/v15/software/s0556/>],[6

<https://research.checkpoint.com/2020/ransomware-alert-pay2key/>] The actors operated a .onion

site (reachable through the Tor browser) hosted on cloud infrastructure registered to an organization previously compromised by the actors. (The actors created the server leveraging their prior access to this victim.) Following the compromise and the subsequent unauthorized acquisition of victim data, the actors publicized news of their compromise (including on social media), tagging accounts of victim and media organizations, and leaking victim data on their .onion site. While this technique has traditionally been used

to influence victims to pay ransoms, the FBI does not believe the objective of Pay2Key was to obtain ransom payments. Rather, the FBI assesses Pay2Key was an information operation aimed at undermining the security of Israel-based cyber infrastructure.

Attribution Details

FBI investigation identified that the Iranian cyber actors conduct malicious cyber activity, which FBI assessed to be in support of the GOI. The FBI judges this activity to be separate from the previously referenced ransomware-enabling activity. This group directs their

activity towards countries and organizations consistent with Iranian state interests, and typically not of interest to the group's ransomware affiliate contacts, such as U.S. defense sector networks, and those in Israel, Azerbaijan, United Arab Emirates. Instead, it is intended to steal sensitive information from these networks, suggesting the group maintains an association with the GOI. However, the group's ransomware activities are likely not sanctioned by the GOI, as the actors have expressed concern for government monitoring of cryptocurrency movement associated with their malicious activity.

The group uses the Iranian company name Danesh Novin Sahand (identification number 14007585836), likely as a cover IT entity for the group's malicious cyber activities.

Technical Details

Note: This advisory uses the [MITRE ATT&CK®](#)

<https://attack.mitre.org/versions/v15/matrices/enterprise/> **Matrix for Enterprise**

<https://attack.mitre.org/versions/v15/matrices/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](#) <https://www.cisa.gov/news-events/news/best-practices-mitre-attckr-mapping> and CISA's [Decider Tool](#) <https://github.com/cisagov/decider/>.

Give Feedback

Overview of Observed Tactics, Techniques, and Procedures

The Iranian cyber actors' initial intrusions rely upon exploits of remote external services on internet-facing assets to gain initial access to victim networks. As of July 2024, these actors have been observed scanning IP addresses hosting Check Point Security Gateways, probing for devices potentially vulnerable to CVE-2024-24919. As of April 2024, these actors have conducted mass scanning of IP addresses hosting Palo Alto Networks PAN-OS and GlobalProtect VPN devices. The actors were likely conducting reconnaissance and probing

for devices vulnerable to CVE-2024-3400. Historically, this group has exploited organizations by leveraging CVE-2019-19781 and CVE-2023-3519 related to Citrix Netscaler, and CVE-2022-1388 related to BIG-IP F5 devices.

Reconnaissance, Initial Access, Persistence, and Credential Access

The actors have been observed using the Shodan search engine to identify and enumerate IP addresses that host devices vulnerable to a particular CVE. The actors' initial access is usually obtained via exploiting a public-facing networking device, such as Citrix Netscaler (CVE-2019-19781 and CVE-2023-3519), F5 BIG-IP (CVE-2022-1388), Pulse Secure/Ivanti VPNs (CVE-2024-21887), and, more recently, PanOS firewalls (CVE-2024-3400) [T1596

<<https://attack.mitre.org/versions/v15/techniques/t1596/>>][T1190

<<https://attack.mitre.org/versions/v15/techniques/t1190/>>].

Following exploitation of vulnerable devices, the actors use the following techniques:

- Capture login credentials using webshells on compromised Netscaler devices and append to file named `netScaler.1` in the same directory as the webshell [T1505.003 <<https://attack.mitre.org/versions/v15/techniques/t1505/003/>>][T1056 <<https://attack.mitre.org/versions/v15/techniques/t1056/>>].
- Create the directory `/var/vpn/themes/imgs/` on Citrix Netscaler devices to deploy a webshell [T1505.003 <<https://attack.mitre.org/versions/v15/techniques/t1505/003/>>]. Malicious files deployed to this directory include:
 - > `netScaler.1`
 - > `netScaler.php`
 - > `ctxHeaderLogon.php`

- Specifically related to Netscaler, place additional webshells on compromised devices immediately after system owners patch the exploited vulnerability [T1505.003 <<https://attack.mitre.org/versions/v15/techniques/t1505/003/>>]. The following file locations and filenames have been observed on devices:
 - `/netscaler/logon/LogonPoint/uiareas/ui_style.php`
 - `/netscaler/logon/sanpdebug.php`
- Create the directory `/xui/common/images/` on targeted IP addresses [T1133 <<https://attack.mitre.org/versions/v15/techniques/t1133/>>].
- Create accounts on victim networks; observed names include “sqladmin\$,” “adfsservice,” “IIS_Admin,” “iis-admin,” and “John McCain” [T1136.001 <<https://attack.mitre.org/versions/v15/techniques/t1136/>>].
- Request exemptions to the zero-trust application and security policies for tools they intend to deploy on a victim network [T1098 <<https://attack.mitre.org/versions/v15/techniques/t1098/>>].
- Create malicious scheduled task SpaceAgentTaskMgrSHR in `Windows/Spaceport/` task folder. This task uses a DLL side-loading technique against the signed Microsoft SysInternals executable `contig.exe`, which may be renamed to `dllhost.ext`, to load a payload from `version.dll`. This file has been observed being executed from the Windows Downloads directory [T1053 <<https://attack.mitre.org/versions/v15/techniques/t1053/>>].
- Place a malicious backdoor `version.dll` in `C:\Windows\ADFS\` directory [T1505.003 <<https://attack.mitre.org/versions/v15/techniques/t1505/003/>>].
- Use a scheduled task to load malware through installed backdoors [T1053 <<https://attack.mitre.org/versions/v15/techniques/t1053/>>].
- Deployment of Meshcentral to connect with compromised servers for remote access [T1219 <<https://attack.mitre.org/versions/v15/techniques/t1219/>>].
- For persistence and as detection and mitigation occurs, the actors create a daily Windows service task with random eight characters and attempt execution of a similarly named DLL contained in the `C:\Windows\system32\drivers\` directory. For example, a service named “test” was observed attempting to load a file located at `C:\WINDOWS\system32\drivers\test.sys` [T1505 <<https://attack.mitre.org/versions/v15/techniques/t1505/>>].

Execution, Privilege Escalation, and Defense Evasion

- Repurpose compromised credentials from exploiting networking devices, such as Citrix Netscaler, to log into other applications (i.e., Citrix XenDesktop) [T1078.003 <<https://attack.mitre.org/versions/v15/techniques/t1078/003/>>].
- Repurpose administrative credentials of network administrators to log into domain controllers and other infrastructure on victim networks [T1078.002 <<https://attack.mitre.org/versions/v15/techniques/t1078/002/>>].
- Use administrator credentials to disable antivirus and security software, and lower PowerShell policies to a less secure level [T1562.001 <<https://attack.mitre.org/versions/v15/techniques/t1562/001/>>][T1562.010 <<https://attack.mitre.org/versions/v15/techniques/t1562/010/>>].
- Attempt to enter security exemption tickets to the network security device or contractor to get the actor's tools allowlisted [T1562.001 <<https://attack.mitre.org/versions/v15/techniques/t1562/001/>>].
- Use a compromised administrator account to initiate a remote desktop session to another server on the network. In one instance, the FBI observed this technique being used to attempt to start Microsoft Windows PowerShell Integrated Scripted Environment (ISE) to run the command "Invoke-WebRequest" with a URI including `files.catbox[.]moe`. Catbox is a free, online file hosting site the actors use as a repository/hosting mechanism [T1059.001 <<https://attack.mitre.org/versions/v15/techniques/t1059/001/>>].

Give Feedback

Discovery

- Export system registry hives and network firewall configurations on compromised servers [T1012 <<https://attack.mitre.org/versions/v15/techniques/t1012/>>].
- Exfiltrate account usernames from the victim domain controller, as well as access configuration files and logs—presumably to gather network and user account information for use in further exploitation efforts [T1482 <<https://attack.mitre.org/versions/v15/techniques/t1482/>>].

Command and Control

- Install “AnyDesk” remote access program as a backup access method [T1219 <<https://attack.mitre.org/versions/v15/techniques/t1219/>>].
- Enable servers to use Windows PowerShell Web Access [T1059.001 <<https://attack.mitre.org/versions/v15/techniques/t1059/001/>>].
- Use the open source tunneling tool Ligolo (ligolo/ligolo-ng) [T1572 <<https://attack.mitre.org/versions/v15/techniques/t1572/>>].
- Use NGROK (ngrok[.]io) deployment to create outbound connections to a random subdomain [T1572 <<https://attack.mitre.org/versions/v15/techniques/t1572/>>].

Exfiltration and Impact

After infiltrating victim networks, the actors collaborate with ransomware affiliates (including NoEscape, Ransomhouse, and ALPHV [aka BlackCat]) in exchange for a percentage of the ransom payments by providing affiliates with access to victim networks, locking victim networks, and strategizing to extort victims [T1657 <<https://attack.mitre.org/versions/v15/techniques/t1657/>>]. The actors also conduct what is assessed to be separate set of malicious activity—stealing sensitive data from victims [TA0010 <<https://attack.mitre.org/versions/v15/tactics/ta0010/>>], likely in support of the GOI.

Give Feedback

MITRE ATT&CK Tactics and Techniques

See **Table 1** to **Table 9** for all referenced threat actor tactics and techniques in this advisory.

Table 1. Reconnaissance

Technique Title	ID	Use or Assessed Use
-----------------	----	---------------------

Technique Title	ID	Use or Assessed Use
Search Open Technical Databases	T1596 < https://attack.mitre.org/versions/v15/techniques/t1596/ >	Iranian cyber actors use Shodan (Shodan[.]io) to identify internet infrastructure hosting devices vulnerable to particular CVEs.

Table 2. Initial Access

Technique Title	ID	Use or Assessed Use
-----------------	----	---------------------

Technique Title	ID	Use or Assessed Use
Exploit Public-Facing Application	T1190 < https://attack.mitre.org/versions/v15/techniques/t1190/ >	<p>Iranian cyber actors scan and exploit public-facing networking devices, including the following devices and associated CVEs:</p> <ul style="list-style-type: none">■ Citrix Netscaler (CVEs-2019-19781 and CVE-2023-3519)■ F5 BIG-IP (CVE-2022-1388)■ Pulse Secure/Ivanti VPNs (CVE-2024-21887)■ PanOS firewalls (CVE-2024-3400)■ Check Point Security Gateways (CVE-2024-24919)
External Remote Services	T1133 < https://attack.mitre.org/versions/v15/techniques/t1133/ >	<p>Iranian cyber actors create <code>/xui/common/images/</code> directory on targeted IP addresses.</p>

Give Feedback

Table 3. Persistence

Technique Title	ID	Use or Assessed Use
Server Software Component: Web Shell	T1505.003 < https://attack.mitre.org/versions/v15/techniques/t1505/003/ >	Iranian cyber actors capture login credentials on compromised Netscaler devices via deployed webshell; create a directory on Netscaler devices for webshell deployment; deploy webshells on compromised Netscaler devices in two directories (observed closely after system owning patching); and place the malicious backdoor <code>version.dll</code> .
Create Account (Local Account)	T1136.001 < https://attack.mitre.org/versions/v15/techniques/t1136/ >	Iranian cyber actors create local accounts on victim networks.
Account Manipulation	T1098 < https://attack.mitre.org/versions/v15/techniques/t1098/ >	Iranian cyber actors request exemptions to zero-trust application for tools they intend to deploy.

Give Feedback

Technique Title	ID	Use or Assessed Use
Scheduled Task/Job	T1053 <https://attack.mitre.org/versions/v15/techniques/t1053/>	Iranian cyber actors implement a scheduled task that uses a DLL side-loading technique and a scheduled task that loads malware through back doors.
Server Software Component	T1505 <https://attack.mitre.org/versions/v15/techniques/t1505/>	Iranian cyber actors implement the daily creation of a Windows service task for persistence as detection and mitigation occur.

Table 4. Privilege Escalation

Technique Title	ID	Use or Assessed Use
Valid Accounts: Local Accounts	T1078.003 <https://attack.mitre.org/versions/v15/techniques/t1078/003/>	Iranian cyber actors repurpose compromised credentials (e.g., from a Netscaler device) to log into other applications.

Give Feedback

Technique Title	ID	Use or Assessed Use
Valid Accounts: Domain Accounts	T1078.002 < https://attack.mitre.org/versions/v15/techniques/t1078/002/ >	Iranian cyber actors repurpose administrative credentials of network admins to log into domain controllers and other infrastructure.

Table 5. Defense Evasion

Technique Title	ID	Use or Assessed Use
Impair Defenses: Disable or Modify Tools	T1562.001 < https://attack.mitre.org/versions/v15/techniques/t1562/001/ >	Iranian cyber actors use administrator credentials to disable antivirus and security software.
Impair Defenses: Disable or Modify Tools	T1562.001 < https://attack.mitre.org/versions/v15/techniques/t1562/001/ >	Iranian cyber actors attempt to enter security exemption tickets to the network security device or contractor to get their tools allowlisted.
Impair Defenses: Downgrade Attack	T1562.010 < https://attack.mitre.org/versions/v15/techniques/t1562/010/ >	Iranian cyber actors lower PowerShell policies to a less secure level.

Give Feedback

Table 6. Credential Access

Technique Title	ID	Use or Assessed Use
Input Capture	T1056 < https://attack.mitre.org/versions/v15/techniques/t1056/ >	Iranian cyber actors capture login credentials on compromised Netscaler devices via a deployed webshell.

Table 7. Execution

Technique Title	ID	Use or Assessed Use
Command and Scripting	T1059.001 < https://attack.mitre.org/versions/v15/techniques/t1059/001/ >	Iranian cyber actors use an admin account to initiate a remote desktop session to start Microsoft Windows PowerShell ISE.
Command and Scripting Interpreter	T1059.001 < https://attack.mitre.org/versions/v15/techniques/t1059/001/ >	Iranian cyber actors enable servers to use Windows PowerShell Web Access.

Give Feedback

Table 8. Discovery

Technique Title	ID	Use or Assessed Use
Query Registry	T1012 < https://attack.mitre.org/versions/v15/techniques/t1012/ >	Iranian cyber actors export registry hives and network firewall configurations.

Technique Title	ID	Use or Assessed Use
Domain Trust Discovery	T1482 < https://attack.mitre.org/versions/v15/techniques/t1482/ >	Iranian cyber actors exfiltrate account usernames from the domain controller and access configuration files and logs.

Table 9. Command and Control

Technique Title	ID	Use or Assessed Use
Remote Access Software	T1219 < https://attack.mitre.org/versions/v15/techniques/t1219/ >	<p>Iranian cyber actors install “AnyDesk” remote access program.</p> <p>Iranian cyber actors deploy Meshcentral to connect with compromised servers for remote access.</p>
Protocol Tunneling	T1572 < https://attack.mitre.org/versions/v15/techniques/t1572/ >	Iranian cyber actors use <code>ligolo / ligolo-ng</code> for open source tunneling and <code>ngrok[.]io</code> NGROK to create outbound connections to a random subdomain.

Indicators of Compromise

IP Address and Domain Identifiers

Disclaimer: The IP addresses and domains listed in **Table 10** were observed in use by the actors in the specified timeframes in 2024. The authoring agencies recommend organizations investigate or vet these IP addresses prior to taking action, such as blocking.

Comment: In addition to the infrastructure provided in the table below, the FBI and CISA warn that these actors are known to leverage information obtained through intrusions into cloud-computing resources associated with victim organizations. The actors have used this cloud infrastructure to conduct further cyber operations targeting other organizations. The FBI observed use of this tradecraft against U.S. academic and defense sectors, but it could theoretically be used against any organization. The FBI and CISA warn that if these actors compromised your organization, they may be leveraging your cloud services accounts to conduct malicious cyber activity and target other victims. The FBI has observed instances of the actors using compromised cloud service accounts to transmit data stolen from other compromised organizations.

Table 10. Indicators of Compromise – Recent

Indicator	First Seen	Most Recently Observed Date
138.68.90[.]19	January 2024	August 2024
167.99.202[.]130	January 2024	August 2024
78.141.238[.]182	July 2024	August 2024
51.16.51[.]81	January 2024	August 2024
51.20.138[.]134	February 2024	August 2024

Give Feedback

Indicator	First Seen	Most Recently Observed Date
134.209.30[.]220	March 2024	August 2024
13.53.124[.]246	February 2024	August 2024
api.gupdate[.]net	September 2022	August 2024
githubapp[.]net	February 2024	August 2024

Disclaimer: The infrastructure in **Table 11** reflects historical IP addresses and domains associated with these actors. This data is being provided for informational purposes and to enable better tracking and attribution of these actors. The FBI and CISA do not recommend blocking of the indicators in **Table 11** based solely on their inclusion in this CSA.

Table 11. Indicators of Compromise – Historical

Indicator	First Seen	Most Recently Observed Date
18.134.0[.]66	September 2023	November 2023
193.149.190[.]248	September 2023	January 2024
45.76.65[.]42	September 2023	December 2023
206.71.148[.]78	October 2023	January 2024
193.149.187[.]41	October 2023	November 2023
login.forticloud[.]online	October 2023	November 2023

Indicator	First Seen	Most Recently Observed Date
fortigate.forticloud. []online	October 2023	November 2023
cloud.sophos[.]one	October 2023	November 2023

Actor Identifiers

Disclaimer: The FBI observed the following identifiers associated with the Iranian cyber group and their ransomware affiliates. The FBI is providing this information to enable improved threat actor identification and tracking of malicious cyber activity. Please see **Appendix A** for list of TOX identifiers.

The FBI observed the threat actors to be associated with the following bitcoin address values:

- bc1q8n7jjgdepuym825zwwftr3qpem3tnjx3m50ku0
- bc1qlwd94gf5uhdpu4gynk6znc5j3rwk9s53c0dhjs
- bc1q2egjjzmchtm3q3h3een37zsvpph86hwgq4xskh
- bc1qjzw7sh3pd5msgehdaurzv04pm40hm9ajpwjqky
- bc1qn5tla384qxpl6zt7kd068hvl7y4a6rt684ufqp
- bc1ql837eewad47zn0uzzjfgqjhsnf2yhkyxvxyjjc
- bc1qy8pnttrfmyu4l3qcy59gml1zqq66gmr446ppcr
- bc1q6620fmev7cvkfu82z43vwjte6mzgcp5hjrdne
- bc1qr6h2zcxlntpcjystxdf7qy2755p25yrwucm4lq
- bc1qx9tteqhama2x2w9vwqsy6hldh8my8udx5jlm
- bc1qz75atxj4dvgezyuspw8yz9khtkuk5jpdgfauq8
- bc1q6w2an66vrje747scecrgezucw9ksha66x9zt980
- bc1qsn4l6h3mhyhmr72vw4ajxf2gr74hwpalks2tp9

■ bc1qtj hvqkun4uxtr4qmq6s3f7j49nr4sp0wywp489

Mitigations

The FBI and CISA recommend all organizations implement the mitigations listed below to improve their cybersecurity posture based on the Iranian cyber group's activity. The FBI judges the group's targeting is primarily based on the identification of devices vulnerable to CVEs named in this notification (see **Technical Details** section for a list of CVEs). As such, any U.S. organization deploying software with these vulnerabilities may be targeted for further exploitation and should follow this guidance to defend against exploitation by this group.

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 to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's [Cross-Sector Cybersecurity Performance Goals](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>> for more information on the CPGs, including additional recommended baseline protections.

Give Feedback

The FBI and CISA recommend all organizations implement the following mitigations:

- Review available logs for IP addresses in **Table 10** for indications of traffic with your organization's network in the provided timeframes [[CPG 3.A](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#detectingrelevantthreatsandhttps3a) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#detectingrelevantthreatsandhttps3a>>]. The indicators in Table 11 should also be reviewed to identify historical activity or incidents which may have previously been identified by your organization.

- Apply patches and/or mitigations for CVE-2024-3400, CVE-2022-1388, CVE-2019-19781, and CVE-2023-3519 [CPG 1.E <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#mitigatingknownvulnerabilities1e>>].
 - Be advised, patching for the above referenced CVEs may be insufficient to mitigate malicious activity if your network has already been compromised by these actors while the network device was vulnerable. Additional investigation into the use of stolen credentials (e.g., via the webshell on Netscaler devices) is strongly encouraged to identify threat actor attempts to establish footholds on other parts of the network [CPG 3.A <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#detectingrelevantthreatsandttps3a>>].
- Check your systems for the unique identifiers and TTPs used by the actors when operating on compromised networks, including creation of specific usernames, use of NGROK and Ligolo, and deployment of webshells in specific directories [CPG 3.A <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#detectingrelevantthreatsandttps3a>>].
- Check your systems for outbound web requests to `files.catbox[.]moe` and `***.ngrok[.]io` [CPG 3.A <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#detectingrelevantthreatsandttps3a>>].

Validate Security Controls

In addition to applying mitigations, the FBI and CISA 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 2** to **Table 10**).
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.

References

1. Fox Kitten, UNC757, Parisite, Pioneer Kitten, RUBIDIUM, Lemon Sandstorm, Group G0117 | MITRE ATT&CK® <<https://attack.mitre.org/versions/v15/groups/g0117/>>
2. PIONEER KITTEN: Targets & Methods [Adversary Profile] (crowdstrike.com) <<https://www.crowdstrike.com/blog/who-is-pioneer-kitten/>>
3. NoEscape - SentinelOne <<https://www.sentinelone.com/anthology/noescape/>>
4. RansomHouse - SentinelOne <<https://www.sentinelone.com/anthology/ransomhouse/>>
5. Pay2Key, Software S0556 | MITRE ATT&CK® <<https://attack.mitre.org/versions/v15/software/s0556/>>
6. Pay2Key Ransomware Alert - Check Point Research <<https://research.checkpoint.com/2020/ransomware-alert-pay2key/>>

Reporting

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

Ransomware Incidents

The FBI and CISA are interested in any information that can be shared in the case of a ransomware incident, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with threat actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

Additional details of interest include a targeted company point of contact, status and scope of infection, estimated loss, operational impact, transaction IDs, date of infection, date detected, initial attack vector, and host- and network-based indicators.

The FBI and CISA do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to the FBI's [Internet Crime Complain Center \(IC3\)](https://www.ic3.gov/home/complaintchoice)

[<https://www.ic3.gov/home/complaintchoice>](https://www.ic3.gov/home/complaintchoice), your [local FBI Field Office <https://www.fbi.gov/contact-us/field-offices>](https://www.fbi.gov/contact-us/field-offices), or CISA via the agency's [Incident Reporting Form <https://www.cisa.gov/report>](https://www.cisa.gov/report) or its 24/7 Operations Center (report@cisa.gov), or by calling 1-844-Say-CISA (1-844-729-2472).

Other Incidents

U.S. organizations are encouraged to report suspicious or criminal activity related to information in this advisory to the FBI's [Internet IC3 <https://www.ic3.gov/home/complaintchoice>](https://www.ic3.gov/home/complaintchoice) or your [local FBI Field Office <https://www.fbi.gov/contact-us/field-offices>](https://www.fbi.gov/contact-us/field-offices). Report suspicious or malicious cyber activity to CISA via the agency's [Incident Reporting Form <https://www.cisa.gov/report>](https://www.cisa.gov/report) or its 24/7 Operations Center (report@cisa.gov) or by calling 1-844-Say-CISA (1-844-729-2472). 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.

Give Feedback

Disclaimer

The information in this report is being provided “as is” for informational purposes only. The FBI and CISA 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 FBI and CISA.

Version History

August 20, 2024: Initial version.

Appendix A: TOX Identifiers

TOX Identifier	TOX Public Key	Comment
xplfinder	ea2ec0c3859d8d8c3 6d95a298beef6d7ad d17856655bfbea255 4b8714f7c7c69	Iranian cyber group
Br0k3r	B761680E23F2EBB5 F6887D315EBD05B2 D7C365731E093B49 ADB059C3DCCAA30 C	Iranian cyber group
Access	185ADA4556737A4F 26AE16F1A99CA82A B5684C32719EE426 C420C0BC14384A0A	Ransomware affiliate
Admin ALPHV aka BlackCat	3488458145EB62D7 D3947E3811234F466 3D9B5AEEF6584AB 08A2099A7F946664	Ransomware affiliate

Give Feedback

TOX Identifier	TOX Public Key	Comment
Admin_NoEscape	0A6F992E1372DB4F 245595424A7436EB B610775D6ADDC4D5 68ACC2AF5D315221	Ransomware affiliate
Americano_Sneeckers	14F8AD7D1553D1A4 7CF4C9E7BEDABCC 5B759C86E54C6361 75A472C11D7DEC70 F	Ransomware affiliate
Bettersock	2C76104C9AAAF324 53A814C227E7D9D7 55451B551A3FD30D 2EA332DF396B3A31	Ransomware affiliate

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

Give Feedback

Tags

Co-Sealers and Partners: Federal Bureau of Investigation

MITRE ATT&CK TTP: Command and Control (TA0011), Credential Access (TA0006), Defense Evasion (TA0005), Discovery (TA0007), Execution (TA0002), Initial Access (TA0001), Persistence (TA0003), Privilege Escalation (TA0004), Reconnaissance (TA0043)

Nation-State Actor: Iran

Topics: [Cyber Threats and Advisories](/topics/cyber-threats-and-advisories), [Cybersecurity Best Practices](/topics/cybersecurity-best-practices), [Malware, Phishing, and Ransomware](/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware), [Nation-State Threats](/topics/cyber-threats-and-advisories/nation-state-cyber-actors), [Organizations and Cyber Safety](/topics/cybersecurity-best-practices/organizations-and-cyber-safety)



Please share your thoughts

We recently updated our anonymous [product survey](#); we welcome your feedback.

Give Feedback

Related Advisories

SEP 23, 2025 ■ CYBERSECURITY ADVISORY |
AA25-266A

[CISA Shares Lessons Learned from an Incident Response Engagement](#) [</news-events/cybersecurity-advisories/aa25-266a>](#)

AUG 27, 2025 ■ CYBERSECURITY ADVISORY |
AA25-239A

[Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System](#) [</news-events/cybersecurity-advisories/aa25-239a>](#)

JUL 31, 2025 ■ CYBERSECURITY ADVISORY |
AA25-212A

[CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization](#) [</news-events/cybersecurity-advisories/aa25-212a>](#)

JUL 22, 2025 ■ CYBERSECURITY ADVISORY |
AA25-203A

[#StopRansomware: Interlock](#) [</news-events/cybersecurity-advisories/aa25-203a>](#)

Give Feedback

[Return to top](#)

Topics [</topics>](#)

Spotlight [</spotlight>](#)

Resources & Tools [</resources-tools>](#)

News & Events [</news-events>](#)

Careers [</careers>](#)

About [</about>](#)



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY



CISA Central

1-844-Say-CISA

contact@cisa.dhs.gov



CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA </about>](#)

[Budget and Performance](#)

[DHS.gov <https://www.dhs.gov>](#)

[<https://www.dhs.gov/performance-financial-reports>](https://www.dhs.gov/performance-financial-reports)

[FOIA Requests](#)

[<https://www.dhs.gov/foia>](https://www.dhs.gov/foia)

[No FEAR Act </no-fear-act>](#)

[Office of Inspector General](#)

[<https://www.oig.dhs.gov/>](https://www.oig.dhs.gov/)

[Privacy Policy </privacy-policy>](#)

[Subscribe](#)

[The White House](#)

[<https://www.whitehouse.gov/>](https://www.whitehouse.gov/)

[<https://www.usa.gov/>](https://www.usa.gov/)

[Website Feedback </forms/feedback>](#)

Give Feedback