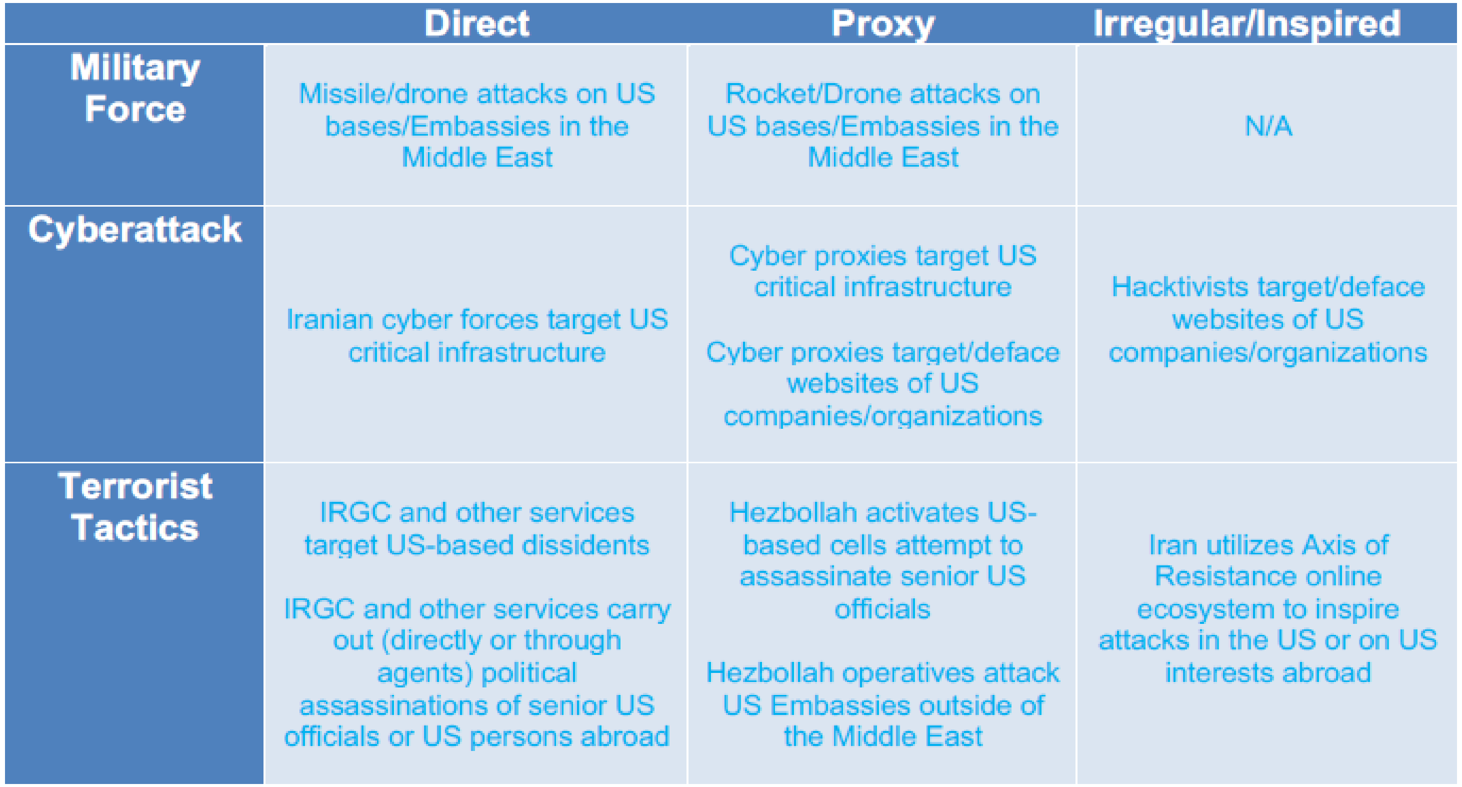
Iranian Advanced Persistent Threats

Select slides

IRAN LIKELY TO LEVERAGE FULL SPECTRUM OF CAPABILITIES TO ATTACK US

Following the June 22 US strikes on Iranian nuclear facilities, Iranian leaders have threatened to retaliate against the US, promising "everlasting consequences." Analysts assess that Tehran is likely to leverage a combination of direct, proxy, and irregular/inspired forces to conduct physical, cyber, or terrorist attacks against US interests both at home and abroad. In light of Israeli strikes and the degradation of the Iranian proxy network in the Middle East, Iran will likely seek to re-establish deterrence against its adversaries, potentially relying on crude or escalatory tactics and informal networks. US interests – particularly Embassies and military bases overseas – are likely to be targeted, and it is possible that Tehran will order or encourage attacks on US government institutions,



	Direct	Proxy	Irregular/Inspired
Military Force	Missile/drone attacks on US bases/Embassies in the Middle East	Rocket/Drone attacks on US bases/Embassies in the Middle East	N/A
Cyberattack	Iranian cyber forces target US critical infrastructure	Cyber proxies target US critical infrastructure Cyber proxies target/deface websites of US companies/organizations	Hacktivists target/deface websites of US companies/organizations
Terrorist Tactics	IRGC and other services target US-based dissidents IRGC and other services carry out (directly or through agents) political assassinations of senior US officials or US persons abroad	Hezbollah activates US-based cells attempt to assassinate senior US officials Hezbollah operatives attack US Embassies outside of the Middle East	Iran utilizes Axis of Resistance online ecosystem to inspire attacks in the US or on US interests abroad

Figure 1: Table of Iranian capabilities to target US interests

Iranian Military/Intelligence Forces:

Iran's military is focused on Israel and Israeli targets in the region. As the country faces more pressure from an ongoing bombing campaign, there may be attempts to target direct military strikes with cyberattacks on US government critical infrastructure and businesses. Such attacks have compromised US water and wastewater systems in the past.

Proxy Groups:

These groups have infiltrated public infrastructure in the past and still retain that capacity. Groups like Hezbollah likely operate covert cells in the US that could carry out physical attacks. While Iranian cyber proxies are less sophisticated than their IRGC counterparts, these groups may maintain the capacity to disrupt public infrastructure and private sector services.

Source(s): Center For Internet Security

TLP: AMBER

IRAN LIKELY TO LEVERAGE FULL SPECTRUM OF CAPABILITIES TO ATTACK US

Direct Iranian Attacks:

Iran is likely to target US computer systems and critical infrastructure in retaliation for the June 22 strikes. **A physical attack on US soil is very unlikely. However, cyberattacks against US interests or US directly are expected.**

Cyber:

Iran maintains sophisticated cyberattack capabilities and has previously hacked into US administration emails and disrupted critical infrastructure. These capabilities could be used in tandem with direct and proxy attacks. Iran’s cyber capabilities include IRGC-led hacking units and hacktivist groups that have targeted US technology companies and infrastructure. These groups have both the capacity to

disrupt public infrastructure and private sector government partners such as Microsoft, OpenAI, and Amazon Web Services (AWS).

Terrorist Tactics:

The Iranian regime has previously targeted high-ranking members of US administration and Iranian dissidents in the US for assassination, and it is possible that they could attempt similar activity should the US bomb Iran. As recently as 2024, the US disrupted a plot by the Iranian regime to assassinate then Presidential Candidate Donald Trump. This came two years after the US disrupted another plot targeting former National Security Advisor John Bolton for assassination. There have been similar attempts to assassinate prominent Iranian dissidents such as Masih Alinejad.

Source(s): Center For Internet Security

IRAN LIKELY TO LEVERAGE FULL SPECTRUM OF CAPABILITIES TO ATTACK US

Iranian Proxy Forces:
There is a high likelihood that Iran-backed militias will target US bases and Embassies in the region and that Iranian cyber proxies will target US critical infrastructure or business interests

Cyber:
Beyond leveraging proxy groups for attacks on US interests in the region or abroad, it is highly likely the Iranian regime will leverage its proxy cyber actors to target US infrastructure in the wake of US involvement in the conflict between Israel and Iran. Reporting has indicated that the Iranian regime has built out its capacity to conduct cyberattacks and information operations globally. The regime demonstrated these capacities with high-profile hacks of water and wastewater treatment facilities in 2023. The IRGC-linked Cyber Av3ngers, responsible for the attacks on US water treatment plants, have a history of attacking water treatment plants and railroad infrastructure. Hacktivist groups such as the Cyber Av3ngers are aware that local and state systems in the US are incapable of dealing with large-scale cyber attacks.

Terrorist Tactics:
Hezbollah – and potentially other proxy groups – likely maintain networks in the US that could be activated to carry out terrorist attacks on US soil.

Source(s): Center For Internet Security

TLP: AMBER

IRAN LIKELY TO LEVERAGE FULL SPECTRUM OF CAPABILITIES TO ATTACK US

Irregular/Inspired Attacks:

The Iranian regime and its proxies have robust propaganda networks online that could influence individuals in the US or other locations globally to conduct physical or cyber attacks on US or Israeli. Since October 7, the Iranian digital ecosystem has both increased the volume of propaganda encouraging attacks but has also expanded the scope of individuals which it seeks to target, potentially raising the likelihood of inspired attacks.

Cyber:

Just hours after the US strikes, the Iranian aligned hacktivist group 313 Team claimed a DDoS attack on the Truth Social platform. The group posted alleged proof of the attack in the form of outage reports. 313 Team is a component of the Cyber Islamic Resistance, whose leader claimed recruits from within the Badr Brigades in Iraq. The Cyber Islamic Resistance has primarily focused its attacks on Israel, targeting surveillance, red alert systems, public infrastructure and technology companies. The Cyber Islamic Resistance is one member of the largest

hacktivist alliance online known as the Holy League, which consists of 90+ pro-Iranian, pro-Russian, and pro-Palestinian cyber actors seeking to dismantle and disrupt public infrastructure, government websites, and technology companies in Israel and beyond. While most of these attacks were low-level Distributed Denial-of-Service (DDoS) attacks, established groups clearly supportive of Kremlin or Iran have had the

most success in penetrating digital infrastructure of public utilities. To this date, there appear to be 65 pro-Iranian hacktivist groups operating across Telegram, all of which are highly likely target US digital assets in the coming days and weeks.

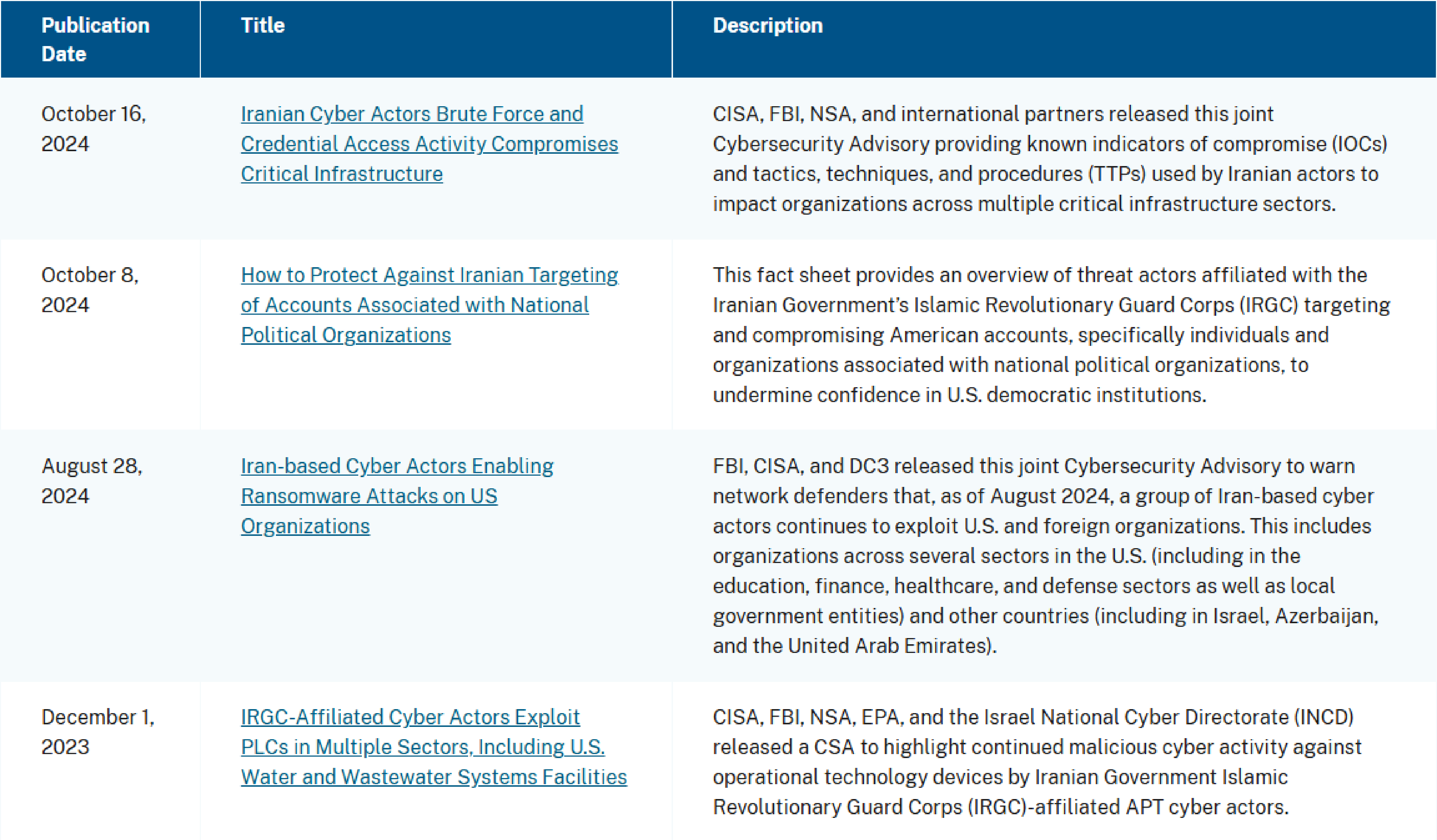
Terrorist Tactics:

Hezbollah – and potentially other proxy groups – likely maintain networks in the US that could be activated to carry out terrorist attacks on US soil.

Source(s): Center For Internet Security

TLP: AMBER

Iran State-Sponsored Cyber Threat: Advisories

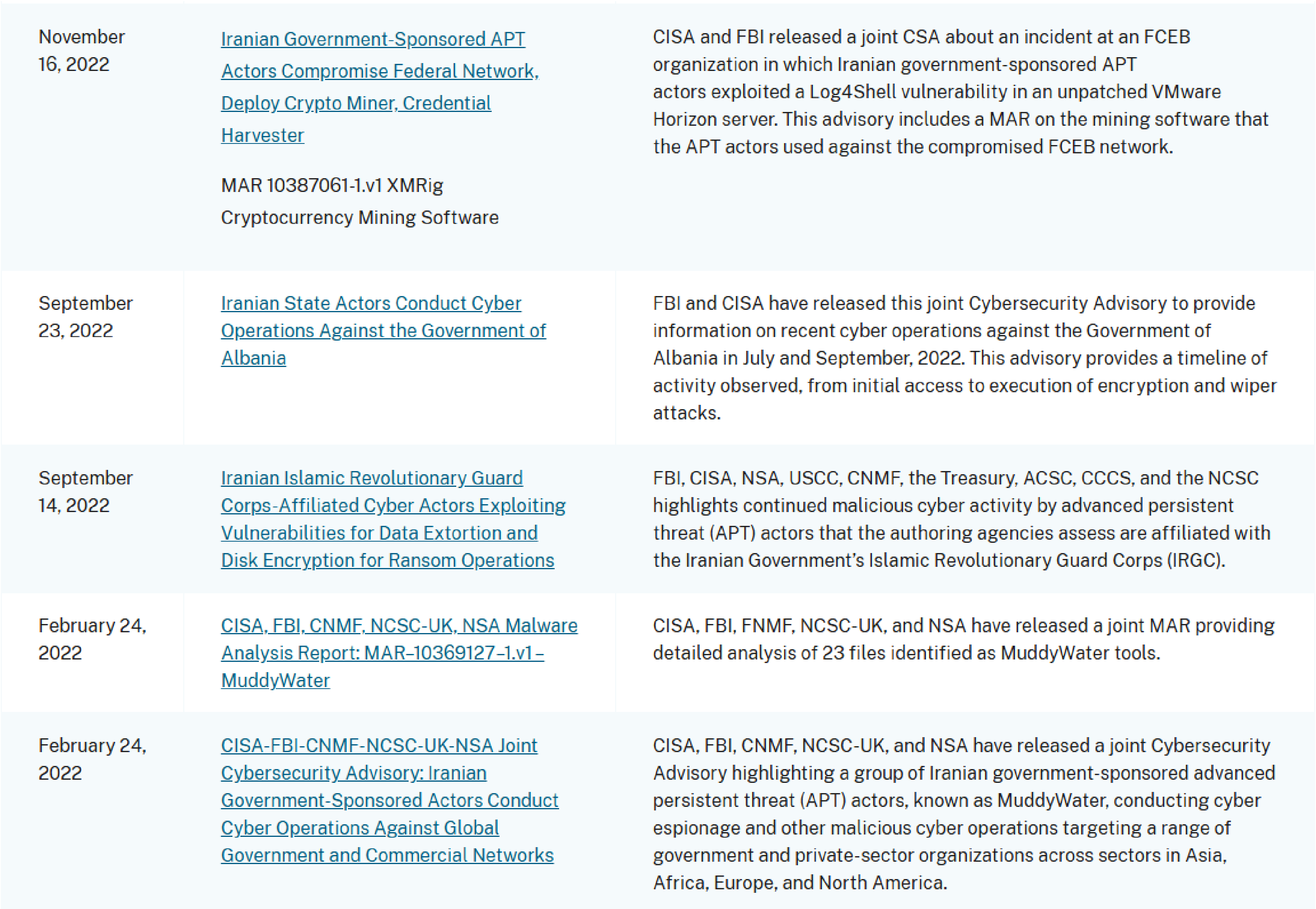


Publication Date	Title	Description
October 16, 2024	Iranian Cyber Actors Brute Force and Credential Access Activity Compromises Critical Infrastructure	CISA, FBI, NSA, and international partners released this joint Cybersecurity Advisory providing known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) used by Iranian actors to impact organizations across multiple critical infrastructure sectors.
October 8, 2024	How to Protect Against Iranian Targeting of Accounts Associated with National Political Organizations	This fact sheet provides an overview of threat actors affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC) targeting and compromising American accounts, specifically individuals and organizations associated with national political organizations, to undermine confidence in U.S. democratic institutions.
August 28, 2024	Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations	FBI, CISA, and DC3 released this joint Cybersecurity Advisory 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).
December 1, 2023	IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities	CISA, FBI, NSA, EPA, and the Israel National Cyber Directorate (INCD) released a CSA to highlight continued malicious cyber activity against operational technology devices by Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated APT cyber actors.

Source(s): https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/iran/publications

TLP: AMBER

Iran State-Sponsored Cyber Threat: Advisories



November 16, 2022	Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester MAR 10387061-1.v1 XMRig Cryptocurrency Mining Software	CISA and FBI released a joint CSA about an incident at an FCEB organization in which Iranian government-sponsored APT actors exploited a Log4Shell vulnerability in an unpatched VMware Horizon server. This advisory includes a MAR on the mining software that the APT actors used against the compromised FCEB network.
September 23, 2022	Iranian State Actors Conduct Cyber Operations Against the Government of Albania	FBI and CISA have released this joint Cybersecurity Advisory to provide information on recent cyber operations against the Government of Albania in July and September, 2022. This advisory provides a timeline of activity observed, from initial access to execution of encryption and wiper attacks.
September 14, 2022	Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations	FBI, CISA, NSA, USCC, CNMF, the Treasury, ACSC, CCCS, and the NCSC highlights continued malicious cyber activity by advanced persistent threat (APT) actors that the authoring agencies assess are affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC).
February 24, 2022	CISA, FBI, CNMF, NCSC-UK, NSA Malware Analysis Report: MAR–10369127–1.v1 – MuddyWater	CISA, FBI, FNMF, NCSC-UK, and NSA have released a joint MAR providing detailed analysis of 23 files identified as MuddyWater tools.
February 24, 2022	CISA-FBI-CNMF-NCSC-UK-NSA Joint Cybersecurity Advisory: Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks	CISA, FBI, CNMF, NCSC-UK, and NSA have released a joint Cybersecurity Advisory highlighting a group of Iranian government-sponsored advanced persistent threat (APT) actors, known as MuddyWater, conducting cyber espionage and other malicious cyber operations targeting a range of government and private-sector organizations across sectors in Asia, Africa, Europe, and North America.

Source(s): https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/iran/publications

TLP: AMBER

Iran State-Sponsored Cyber Threat: Resources

Iranian Cyber Threat Information:

- IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities | CISA
- Iran State-Sponsored Cyber Threat: Advisories | CISA
- Iranian-Linked Cyber Army Had Partial Control Of Aliquippa Water System - BeaverCountian.com
- Cyber Intelligence: Iran’s cyber capabilities are improving – CSCIS
- Rinse and repeat: Iran accelerates its cyber influence operations worldwide - Microsoft On the Issues
- Global Revival of Hacktivism Requires Increased Vigilance from Defenders | Google Cloud Blog
- Iran-linked cyberattacks threaten U.S. water, heath care and energy sectors : NPR
- Iranian APTs Dress Up as Hacktivists for Disruption, Influence Ops
- APT 34 Is an Iran-Linked Hacking Group That Probes Critical Infrastructure | WIRED
- Iran-Backed Militias Resume Attacks on US Positions
- NTAS bulletin highlights rising cyber, terror threats to US critical infrastructure from Iran-linked hackers - Industrial Cyber
- ODNI 2025 Threat Assessment notes threats from Russia, China, Iran, North Korea targeting critical infrastructure, telecom - Industrial Cyber
- DHS expects Iran’s cyber forces will target US networks after strikes on nuclear sites - Nextgov/FCW
- National Terrorism Advisory System Bulletin - June 22, 2025 | Homeland Security
- IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities

Source(s): https://www.bleepingcomputer.com/news/security/no-the-16-billion-credentials-leak-is-not-a-new-data-breach/

Demystifying Iranian Cyber Threat Groups

Executive Summary:
The IRGC directly and indirectly support many Advanced Persistent Threat (APT) groups that target Critical infrastructure (CI) and Government Infrastructure (GI) in the United States. With the increased tensions between the U.S. and Iran, this activity is likely to rapidly increase. While each Cyber Threat Intelligence (CTI) tracker uses different monikers, the capabilities of many of these IRGC sponsored APT groups are well documented and understood. From high profile CI attacks targeting water and wastewater systems, to sponsored Denial of Service (DoS) attacks against U.S. based social media platforms, IRGC sponsored threats vary widely in scope. This brief focuses on APT groups that may pose a threat to critical systems or infrastructure, based on past exploitation or influence operations.

Focus:
The APT groups discussed in the following slides have been chosen based on their level of recent activity, commonly targeted organizations and domains, and narrowed down to groups that have historically, or are currently, targeting the U.S. Each slide will briefly summarize the activity and known intelligence of each group, with select links provided for further detail or information.

Remediation and Prevention:
The focus of this briefing is to both provide awareness to IRGC sponsored threats and potential attack vectors, as well as to provide clear and concise remediation and prevention steps. Operational Technology (OT) and Industrial Control Systems (ICS) are commonly targeted systems that control essential services. These systems often face security related challenges that make them prime targets for low level APT groups looking to cause maximum damage with minimal resources. Industry standard recommendations will be shared at the end of the brief for safeguarding these systems from potential abuse or exploitation.

Source(s): The Iranian Cyber Capability, Threat Group Cards: A Threat Actor Encyclopedia, Iranian APTs: An overview | Middle East Instit

TLP: AMBER

Demystifying Iranian Cyber Threat Groups – CyberAv3ngers

TLP: AMBER

Executive Summary:
CyberAv3ngers is a state sponsored (IRGC) cyber threat group behind some of the most prolific IRGC cyberattacks against US CI/GI. These attacks are primarily motivated by sabotage and destruction operations. The goal of this APT group is to cause as much disruption to CI as possible. CyberAv3ngers is the APT group behind the 2023 cyberattack that shut down a Pennsylvania water authority. They targeted Israeli-made Unitronics Vision Series Programmable Logic Controllers (PLCs) commonly used in water and wastewater systems.

Focus:
This APT group focuses on targeting industrial and government sectors. Their primary targets have been Ireland, Israel, and the United States. Most prominent associated incidents have occurred with Israeli-made Unitronics PLCs. These incidents have led to service disruptions in both the United States and Ireland. The IRGC-affiliated cyber actors left a defacement image stating, “You have been hacked, down with Israel. Every equipment ‘made in Israel’ is CyberAv3ngers legal target.”

Remediation and Prevention:
Common PLC security measures such as network segmentation and isolation protect against these attacks. The historic CyberAv3ngers TTPs relate to Brute Force activity, Stolen Account Credentials, and Denial of Service. Implementing standard controls protects against these.

Specific remediation steps for Unitronics PLCs are:

- Upgrading engineering workstations to 9.9.00 VisiLogic software and upgrading all firmware of the Vision series PLCs and HMI devices.
- Replacing all default passwords on PLCs and HMIs.
- Disconnecting PLCs from public-facing internet.

Note: Unitronics PLCs may be rebranded or appear to come from other manufacturers. More information in the attached links.

Source(s): Pennsylvania water authority hit with cyberattack allegedly tied to pro-Iran group | The Record from Recorded Future News, CyberAv3ngers - Threat Group Cards: A Threat Actor Encyclopedia, IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater

Demystifying Iranian Cyber Threat Groups – APT 42

TLP: AMBER

Executive Summary:
APT 42 is an IRGC sponsored Intelligence Organization primarily focused on espionage. This APT group is tasked with conducting information collection and surveillance operations against individuals and organizations of strategic interest to the Iranian government. Specifically, APT 42 is theorized to be a subsection of the IRGC-IO. Per Mandiant, this group has been active since 2015 and has conducted spear phishing and surveillance operations against government officials, political figures, opposition groups, journalists, and many more targets of strategic interest to the IRGC. These operations typically include the APT group building a rapport with the victim before deploying malware giving the group access to victim location, phone calls, emails, SMS, and other sensitive information. It is expected that APT 42 will continue to target individuals and organizations in the US.

Focus:
APT 42 largely focuses on targeting individuals and organizations in Israel and the United States. Between February and July 2024, the U.S. and Israel accounted for roughly 60% of APT42's known geographic targeting, including the likes of former senior Israeli military officials and individuals affiliated with both U.S. presidential campaigns. APT 42 activity has continually increased throughout 2024 and 2025. Due to the varied tactics deployed by APT 42, such as malware hosts, phishing, malicious redirects, and cloud infrastructure abuse, tracking the group's activity can be challenging. Mandiant, as part of Google, has put forth significant effort in disrupting APT 42 activity by dismantling GCP and Google service infrastructure that has been historically abused by this group. Most APT 42 operations target military, defense, diplomat, academic, and civil society targets.

Remediation and Prevention:
The best defense against APT 42 operations are phishing awareness and user training. APT 42 creates extensive infrastructure that appears legitimate and may not be detected by automated tools. Robust user training to identify suspicious emails provides a first line of defense against these types of intelligence operations.

Source(s): APT 42 - Threat Group Cards: A Threat Actor Encyclopedia, Iranian backed group steps up phishing campaigns against Israel, U.S.

Demystifying Iranian Cyber Threat Groups – APT 33 “Elfin”

TLP: AMBER

Executive Summary:

APT 33, AKA “Elfin”, “Magnallium”, “Refined Kitty”, is an IRGC sponsored APT group that conducts both espionage and sabotage operations. This APT group has been in operation since at least 2013 and has targeted many different sectors and organizations. One of the oldest and most prolific IRGC APT groups, APT 33 has recently been seen deploying custom malware targeting satellite comms, oil and gas, as well as federal and state government sectors in the US and UAE. The APT group leverages common techniques such as password spraying to gain access to user accounts, compromising high value targets with a high level of success.

Focus:

APT 33 focuses on performing intelligence operations against strategic interests for the IRGC. APT 33 utilizes a variety of tooling, including custom backdoors, C2 infrastructure, and malware loaders, to engage in intelligence theft and other operations. Primarily targeting CI/GI and targets of military interest, APT 33 has seen significant success in abusing and exploiting social engineering tactics and Open-Source Intelligence (OSINT) tactics to compromise high-value targets. Once compromised, these accounts are used to deploy custom malware backdoors and create or abuse malicious Azure resources. APT 33 often utilizes fake LinkedIn profiles, masquerading as students, developers, and talent acquisition based in the United States and Western Europe. These accounts are used in targeted social engineering attacks against strategic interests in higher education, satellite sectors, and related industries.

Remediation and Prevention:

APT 33 deploys advanced, custom, malware and infrastructure for intelligence operations against multiple industries in the United States. Initial access is gained through social engineering tactics and common attacks like Password Spraying. Endpoint security solutions actively monitor for suspicious behavior on devices, and robust user training programs help deter common social engineering tactics from succeeding.

Source(s): APT33 Targets Aerospace & Energy Sectors | Spear Phishing | Google Cloud Blog, Peach Sandstorm deploys new custom Tickler malware in long-running intelligence gathering operations | Microsoft Security Blog

Demystifying Iranian Cyber Threat Groups – APT 35 “Magic Hound”

TLP: AMBER

Executive Summary:

APT 35, AKA “Magic Hound”, ”Cobalt Illusion”, and “Charming Kitten”, is an IRGC sponsored threat group that performs intelligence operations for the IRGC, primarily targeting strategic interest groups within energy, government, and technology sectors in multiple countries. APT 35 has several sub-groups, including “Nemesis Kitten” and “Smoke Sandstorm”. Magic Hound has been observed since 2012 and may be an evolution of the “Cutting Kitten” APT group. APT 35 has been the target of significant counter-operations from the United States and US-based organizations. These operations largely attempt to disrupt social engineering campaigns led by APT 35.

Focus:

APT 35 commonly targets multiple sectors, including government, education, dissidents, and other strategic interests. APT 35 is considered a highly skilled social engineering group and utilizes a tradecraft that lacks many of the hallmarks of traditional phishing and social engineering attacks that are commonly seen. The APT group uses legitimate compromised accounts to send phishing lures, and to deploy custom malware backdoors that communicate with actor-controlled C2 infrastructure. In some cases, APT 35 also creates false identities using LinkedIn and masquerades as journalists or other high-profile individuals. In these incidents, APT 35 often spoofs email addresses to appear more legitimate. APT 35 will typically build a rapport with a victim by sending legitimate and benign emails before delivering malicious content.

Remediation and Prevention:

APT 35 engages in extremely successful social engineering campaigns that are typically customized per victim. This makes training or detection efforts more difficult. However, APT 35 does not have particularly advanced malware delivery or evasion methods in most payloads. Sufficient EDR protections and user training to avoid sending confidential data to untrusted sources counters many of the TTPs utilized by this group.

Source(s): New TTPs observed in Mint Sandstorm campaign targeting high-profile individuals at universities and research orgs | Microsoft Security Blog, How a Fake Podcast Invite Delivers BlackSmith Malware | Proofpoint US, Subgroup: DEV-0270, Nemesis Kitten - Threat Group Cards: A Threat Actor Encyclopedia, Subgroup: TA455, Smoke Sandstorm - Threat Group Cards: A Threat Actor Encyclopedia

Mitigating IRGC APT Group Activity

TLP: AMBER

- Reset account passwords for any accounts targeted during a password spray attack. If a targeted account had system-level permissions, further investigation may be warranted.
- Revoke session cookies in addition to resetting passwords.
  - Revoke any MFA setting changes made by the attacker on any compromised users' accounts.
  - Require re-challenging MFA for MFA updates as the default.
- Implement the Azure Security Benchmark and general best practices for securing identity infrastructure, including:
  - Create conditional access policies to allow or disallow access to the environment based on defined criteria.
  - Block legacy authentication with Microsoft Entra by using Conditional Access. Legacy authentication protocols don't have the ability to enforce multifactor authentication (MFA), so blocking such authentication methods will help prevent password spray attackers from taking advantage of the lack of MFA on those protocols.
  - Enable AD FS web application proxy extranet lockout to protect users from potential password brute force compromise.
- Secure accounts with credential hygiene:
  - Practice the principle of least privilege and audit privileged account activity in your Microsoft Entra environments to help slow and stop attackers.
  - Deploy Microsoft Entra Connect Health for Active Directory Federation Services (AD FS). This captures failed attempts as well as IP addresses recorded in AD FS logs for bad requests in the *Risky IP report*.
  - Use Microsoft Entra password protection to help detect and block known weak passwords and their variants.
  - Turn on identity protection in Microsoft Entra to monitor for identity-based risks and create policies for risky sign ins.
- Comply with the recent MFA enforcement policy requiring all Azure accounts to utilize MFA. Keep MFA always-on for privileged accounts and apply risk-based MFA for normal accounts.
- Secure remote desktop protocol (RDP) or Windows Virtual Desktop endpoints with MFA to harden against password spray or brute force attacks.

Source(s): Peach Sandstorm deploys new custom Tickler malware in long-running intelligence gathering operations | Microsoft Security Blog

Mitigating IRGC APT Group Activity

TLP: AMBER

To protect against password spray attacks, implement the following mitigations:

- Eliminate insecure passwords.
- Educate users to review sign-in activity and mark suspicious sign-in attempts as “This wasn’t me”.
- Reset account passwords for any accounts targeted during a password spray attack. If a targeted account had system-level permissions, further investigation may be warranted.
- Detect, investigate, and remediate identity-based attacks using solutions like Microsoft Entra ID Protection.
- Investigate compromised accounts using Microsoft Purview Audit (Premium).
- Enforce on-premises Microsoft Entra Password Protection for Microsoft Active Directory Domain Services.
- Use risk detections for user sign-ins to trigger multifactor authentication or password changes.
- Investigate any possible password spray activity using the password spray investigation playbook.

Source(s): Peach Sandstorm deploys new custom Tickler malware in long-running intelligence gathering operations | Microsoft Security Blog

Common OT/ICS Security Controls and Recommendations

TLP: AMBER

- **Implement network segmentation** [CPG 2.F]
- **Adopt mature asset management processes**
- **Periodically inventory internet accessible devices** [CPG 1.A]
- **Configure external and internal firewalls to block traffic using common ports associated with network protocols that are unnecessary for the particular network segment.**
- **Authenticate all access to field controllers before authorizing access to, or modification of, a device's state, logic, or programs**.
- **Disable any unused authentication methods, logic, or features,** such as default authentication keys.
- **Use a role-based mechanism to limit operating mode changes to required authenticated users only.**
- **Implement device management systems** that can authenticate all network messages to prevent unauthorized system changes.
- **Ensure all field controllers require users to authenticate for all management sessions.**
- **Use host-based allowlists to prevent devices from accepting connections from unauthorized systems and ensure they can only connect with known workstations.**
- **Implement network intrusion detection and prevention systems** whenever possible to identify malicious activity.
- **Retain cold-standby or replacement hardware of similar models** to ensure continued operations of critical functions if the primary system is compromised or unavailable [CPG 2.R].[12]
- **Utilize watchdog timers,** when possible, to enable quick detection of unresponsive systems.
- **Monitor asset management systems for device configuration changes,** which can be used to understand expected parameter settings.
- **Monitor the content of network traffic for the following**:
  - Unusual logins to internet-connected devices or unexpected protocols to/from the internet.
  - Functions of ICS management protocols that change an asset's operating mode or modify programs.
  - Unexpected protocols connected to ports that are mismatched with the protocols that would normally connect to these ports.[11] Block all non-used high ephemeral ports and monitor for attempted connections using standard protocols on non-standard ports

Source(s): IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities | CISA, Cross-Sector Cybersecurity Performance Goals | CISA