# 2025H1 Threat Review:

## Vulnerabilities, Threat Actors, and Ransomware

August 4, 2025

FORESCOUT RESEARCH | VEDERE LABS

# Contents

# KEY FINDINGS

## WHAT YOU NEED TO KNOW

## OPPORTUNISTIC ATTACKS

**Opportunistic attacks against OT are increasing.**

1. Modbus remains the most targeted OT protocol accounting for 57% of honeypot interactions *(up from 40%)*.
2. EtherNet/IP held second place at 20%, down from 28%.
3. BACnet moved up to third place at 8%, previously fifth at 7%.

## VULNS

**Published vulnerabilities rose 15%.**

**45%** of these had high or critical CVSS scores.

Zero-day exploitation increased by **46%.**

## RANSOMWARE

**Ransomware attacks rose by 36%.**

- At 3,649 attacks, they average 608 attacks per month, or **20 per day**.
- Active ransomware groups rose 8.5% from 82 to 89.
- **79% of attacks hit the top 10** targeted countries

## CISA KEV

**CISA KEV additions rose by 80%.**

Over **20%** of new exploited vulnerabilities targeted network infrastructure.

**47%** of newly exploited vulnerabilities were published before 2025.

## THREAT ACTORS

**137 threat actors had activity updates.**

China, Russia and Iran have the highest number of threat actors.

The most targeted industries are government, technology, financial services, energy and telecommunications.

The US, India, the UK, Germany, and Australia are the countries most targeted by threat actors.

## IRANIAN GROUPS

**Iranian groups - APT IRAN, CyberAv3ngers and other personas form a threat continuum focused on OT/ICS targets.**

- APT IRAN has started claiming OT/ICS attacks, often amplified by CyberAv3ngers, targeting the same kinds of devices the latter group used to claim.
- There is no evidence yet that these attacks are real, but similar early activity preceded real attacks by CyberAv3ngers in late 2023 and early 2024.
- Activity currently focuses on Israel and the US with potential to expand as it did in 2023.
- These personas are likely all controlled by the IRGC, known for shifting identities and hybrid threat operations.

## KEY TRENDS

### Lateral Movement

**IP cameras and BSD systems** are now common targets, increasingly used for lateral movement or operational impact in ransomware campaigns. These asset-types often fall outside the coverage of traditional endpoint protections.

### Hacktivism

**Hacktivist or state-sponsored?** In today's geo-political landscape, that line is increasingly blurred, often by design. Identity-shifting threat actors use this ambiguity to confuse attribution and complicate response.

*The report concludes with mitigation recommendations based on our findings from 2025H1*

FORESCOUT

# MITIGATION RECOMMENDATIONS

## WHAT YOU NEED TO DO

While we strongly recommend reviewing the full Mitigation Recommendations, here is a practical snapshot of the most urgent steps:

## PRIORITIZE VISIBILITY

**Prioritize visibility, risk assessment, and proactive controls across key areas of the attack surface, especially:**

- Network perimeter assets
- Operational technology (OT)
- Healthcare systems
- IoT device

## AGENTLESS SOLUTIONS

**Use agentless solutions to gain visibility into:**

- Device presence on the network
- Running software and firmware
- Communication behaviors and flows

## LATERAL MOVEMENT

**Prepare for lateral movement across device types by ensuring detection coverage from:**

1. Entry points (e.g. a vulnerable router)
2. Pivot points (e.g. a misconfigured workstation)
3. Final targets (e.g. an insecure device)

## THREAT DETECTION SOLUTION

**Ensure your threat detection solution covers all device types and ingests data from multiple sources, including:**

- Firewalls
- Intrusion detection systems (IDS/IPS)
- Endpoint detection and response (EDR)
- Identity and Access Systems
- Other existing security infrastructure.

# 1. Executive Summary

In the first half of 2025, Forescout Research – Vedere Labs published a broad range of blog posts and reports analyzing prominent vulnerabilities, threat actors, and ransomware operations. This mid-year review builds on our 2024 analysis, highlighting both persistent trends and emerging shifts in adversary behavior, attack surfaces, and defensive gaps.

Cybercriminals continue to rely on IT-centric techniques for malware delivery. ClickFix, in particular, has become a favored tool among infostealer and ransomware operators. Ransomware groups are expanding the types of assets leveraged in their attacks, frequently in attempts to bypass EDR solutions. Network infrastructure remains a major initial access vector, with over 20% of newly exploited vulnerabilities affecting such devices. Recent attacks highlight the growing role of IP cameras and BSD systems in lateral movement and impact – validating our 2022 R4IoT scenario that predicted this very convergence.

Beyond cybercrime, the line between hacktivist and state-sponsored activity is increasingly blurred, especially in attacks on critical infrastructure. Once the domain of shadowy state actor groups, these attacks are now frequently attributed to hacktivist front groups or hybrid personas. We analyzed this trend in detail in an April report, but since then, rising tensions in the Middle East have escalated the threat of Iranian-linked hacktivist attacks on Western targets. The tactics observed recall the lead-up to the late 2023 Unitronics campaign orchestrated by CyberAv3ngers.

This report reviews the threat landscape from January 1 to June 30, 2025 (2025H1) comparing it with the same period in 2024. It also includes a detailed case study on Iranian threat activity, showcasing how a continuum of personas, from ICTUS TEAM to APT IRAN, reflects a sophisticated OT/ICS targeting playbook that evolves in lockstep with regional conflicts and attribution pressures.

Crucially, many of the threats in 2025H1 exploited known vulnerabilities: 47% of newly exploited CVEs were published before 2025, and many targeted perimeter infrastructure. This underscores a core theme; *proactive defense gaps remain the greatest liabilities*.

# 2. Key Trends in the First Half of 2025

## 2.1. Cybercrime – Ransomware and Infostealers

Most cybercriminal activity we analyzed in 2025H1 relied on two dominant malware types: ransomware and infostealers. While the growth of ransomware is addressed in section 3, this section focuses on the evolving TTPs observed in campaigns delivering both malware types.

- **Initial Access**: Increased use of Initial Access Brokers (IABs) and exploitation of vulnerabilities in specific public-facing applications, including VPNs, remote access solutions, and file transfer applications.
- **Persistence, Execution, and C2**: Remote monitoring and management (RMM) tools become a preferred mechanism for persistence and execution. Attackers often abuse native functionality, such as remote shell access, to execute commands. Legacy techniques like user creation, scheduled tasks and web shells also remain prevalent.
- **Privilege Escalation**: Use of Cobalt Strike for post-exploitation has declined, though it remains in use for credential dumping and token manipulation.
- **Defense Evasion**: Obfuscation has taken a back seat to aggressive EDR bypass techniques. Tools such as KillAV, TrueSightKiller, and EDR Kill Shifter, and ‘bring your own vulnerable driver’ (BYOVD) methods are now standard. These tools are replacing traditional event-log purging and malware obfuscation.
- **Discovery**: To evade detection, threat actors increasingly use Active Directory Service Interfaces (ADSI) instead of prebuilt PowerShell tools for internal reconnaissance.

- **Exfiltration**: Data exfiltration is now routine across most groups. Many show preferences for specific tools, like Rclone or MEGA for this phase.

Two incidents in March 2025 illustrate how ransomware operators continue to expand the device types leveraged in their attacks, particularly to evade EDR:

- Akira ransomware was deployed to Windows endpoints via a compromised IP camera. echoing our 2022 R4IoT scenario, which demonstrated how attackers could leverage IoT, IT and OT assets in a chained attack.
- A new group dubbed VanHelsing introduced a multi-platform encryptor that includes support for BSD UNIX. BSD, while niche, is gaining attention from ransomware operators. The trend began in 2021, with a variant of Hive and continued into late 2024, with reports of Interlock running on the system. By 2025H1, new BSD-compatible variants emerged from RansomHub and Hunters International.

We expect both asset types – IP cameras and BSD systems – to be increasingly targeted in the near future.

Infostealers continue to grow in both volume and sophistication. As covered in our 2024 Threat Roundup, this malware category became the most common last year. In 2025H1, ClickFix campaigns became the leading innovation in delivery tactics. ClickFix campaigns use social engineering to trick victims into copying and executing attacker-supplied malicious commands (usually PowerShell). This technique, first observed in late 2024 has accelerated in popularity in 2025.

The table below summarizes recent infrastructure components and observed TTPs used by threat actors distributing infostealers.

| Infrastructure Component | Details | Purpose |
|---|---|---|
| Command and control domains | TLDs like `.shop, .top, .club, .run` | C2 Communication |
| GitHub repositories | Used for distribution and updates | Initial payload delivery |
| Telegram | Channels with bots sharing stolen data | Distribution, command and control and exfiltration |
| SEO | Distribution of ClickFix campaign links | Initial infection vector |
| Bulletproof hosting | Hosting malicious payloads | Payload storage |
| Cracked software sites | Distribution of Trojanized applications | Initial infection vector |

## 2.2. Healthcare – Malware and Data Breaches

Healthcare continues to be among the most targeted industries, as detailed in Section 3 of this report.

In February, we identified a cluster of 29 sophisticated malware samples masquerading as DICOM viewers. These samples delivered ValleyRAT, a backdoor remote access trojan used by the Chinese threat actor Silver Fox to take control of infected machines. A follow-up threat hunt, uncovered further compromise of healthcare-specific systems including central monitoring stations infected with commodity malware, and botnet samples targeting credentials for cardiology information systems. These findings underscore a key reality: IT malware is increasingly being delivered through, or against, medical systems, either directly or by exploiting weak configurations.

Ransomware and data breaches remain the most frequent and damaging types of cyber incidents in the healthcare sector. The Health-ISAC recently cited ransomware, VPN vulnerabilities and compromised credentials as the most persistent threats for healthcare organizations in 2025.

One notable case involved the Interlock ransomware group (initially tracked as Chaya_002) which has increasingly targeted healthcare organizations. In February, we documented their use of ClickFix as a part of initial access and infection chains. Since that report, Interlock has claimed attacks against four additional large US healthcare institutions. In the most recent case, the group claimed to have stolen 941GB of data across 732,490 files. The affected organization required three weeks to restore normal operations.

The real-world consequences of these attacks continue to escalate. In June, multiple media outlets reported that a patient in the UK died in 2024, in part due to a delayed blood test result caused by a ransomware attack attributed to the Qilin group. Investigators linked the attack to 170 additional patient cases, most classified as low severity, but the cumulative effect has amplified concerns about the direct impact of ransomware on patient safety.

In our review of data breaches across sectors, we found that healthcare remains the most impacted across all industries. In addition, we analyzed 238 data breaches reported to the US Department of Health and Human Services (HHS) from Jan 1 to April 30, 2025. Below, we update those findings to include the whole 2025H1 period:

- 341 healthcare breaches affecting over 500 individuals each were reported. Of those, 306 are still under investigation. This is an average of almost two breaches per day.
- 29,799,648 individuals were impacted in total, averaging 87,388 individuals per breach.
- Five breaches affected more than one million individuals each.
- 74% of breaches occurred at healthcare providers; the remaining 26% at business associates, health plans, or clearing houses.
- 76% of breaches were attributed to hacking/IT incidents.
- In 62% of breaches, the compromised data was on network servers; 24% involved e-mail.

These findings highlight that healthcare remains highly vulnerable to both opportunistic and targeted attacks, with often outsized consequences due to its sensitive data and operational interdependencies.

## 2.3. OT – The Growth of Opportunistic Attacks

Opportunistic attacks on OT environments are increasing, not due to targeted campaigns, but because threat actors are broadening their scope to include any exposed or vulnerable system. These threat actors who are not pursuing specific victims but instead aim to cause disruption wherever feasible. We observe this trend through two complementary lenses:

1. **Hacktivist Activity Against OT.**
   Hacktivist groups are increasingly aligning with state interests and targeting cyber-physical systems. In some cases, state-sponsored actors operate under hacktivist fronts to conduct disruptive attacks while obscuring attribution.

   Key Examples from 2025H1 include:
   - GhostSec and Arabian Ghosts (pro-Iranian): Attacks on PLCs in Israel.
   - Sector16 and Z-Pentest (pro-Russian): Disruptive campaigns against oil and gas facilities in the US.

   As discussed in greater depth in Section 4, the emerging Iranian actor, APT IRAN, exemplifies the merging of traditional APT-grade capabilities with hacktivist-style messaging and operations.

2. **Internet-wide Scanning and Attacks on Honeypots.**
   Each year, we analyze traffic to our Adversary Engagement Environment (AEE), a global honeypot network designed to monitor malicious activity. This data provides insight into how attackers scan, identify, and test potential targets across OT networks.

   Key findings from 2025H1:
   - Modbus remains the most scanned OT protocol, involved in 57% of OT interactions, up from 40% in 2024.
   - Ethernet/IP holds second place at 20%, down from 28%.
   - BACnet has risen to third place with 8% up from 7%, overtaking KNX and Fox protocols.

   These shifts reflect sustained attacker interest in industrial automation and building management systems, particularly by threat actors scanning opportunistically for devices.

**PLC Honeypot Observations**
Between December 2024 and March 2025, we deployed real PLC honeypots simulating a water treatment environment. Over the 90-day period, the honeypot received 1,444,095 requests – about 16,000 per day or 11 per minute.

The PLCs honeypots had the following services enabled: S7comm, S7comm-plus, Modbus, HTTP and HTTPS.
- 98% of requests used standard web protocols (HTTP/HTTPS), not OT-specific protocols.
- Only 2% used OT-native protocols like Modbus or S7comm.

Most Modbus or S7comm requests were attempts to identify or read device data, suggesting either benign scanning or early reconnaissance. However, we observed occasional attempts to:
- Alter variables stored in the PLC.
- Stop the PLC via its web interface
- Connect using an engineering workstation – possibly to reprogram ladder logic.

These actions resemble real-world TTPs seen in hacktivist-posted videos and social media propaganda.

**Summary**
Opportunistic OT attacks now fall into two main categories:
1. Real-world disruption, often targeting critical services like manufacturing, or water treatment.
2. Wide-area scanning, laying the groundwork for exploitation or assessing exposure.

Together, these underscore the persistent interest in OT systems, even among threat actors not traditionally associated with ICS expertise. Attackers are increasingly willing to exploit any system they find exposed regardless of sector or impact sensitivity.

# 3. Statistics

## 3.1. Vulnerabilities

In the first half of 2025, 23,581 vulnerabilities were published, averaging 130 new CVEs per day or 3,930 per month. This represents a 15% increase compared to the same period in 2024, which saw 20,533 disclosures. Figure 1 provides a monthly breakdown of vulnerability publication rates across H1 2023, H1 2024 and H1 2025.

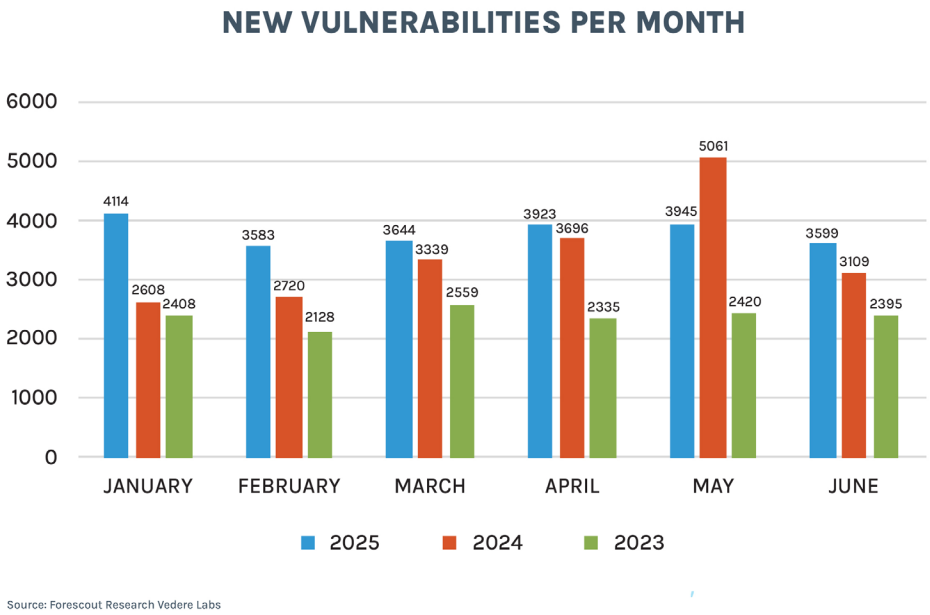



*Figure 1 – New vulnerabilities per month*

Many CVEs published in H1 2025 are still awaiting CVSS scoring, pending NVD analysis. Among those with assigned scores, 45% were rated low or medium, while 43% were rated high or critical. The proportions are similar to 2024, showing that volume continues to rise, but the distribution of severity remains largely unchanged, as illustrated in Figure 2.

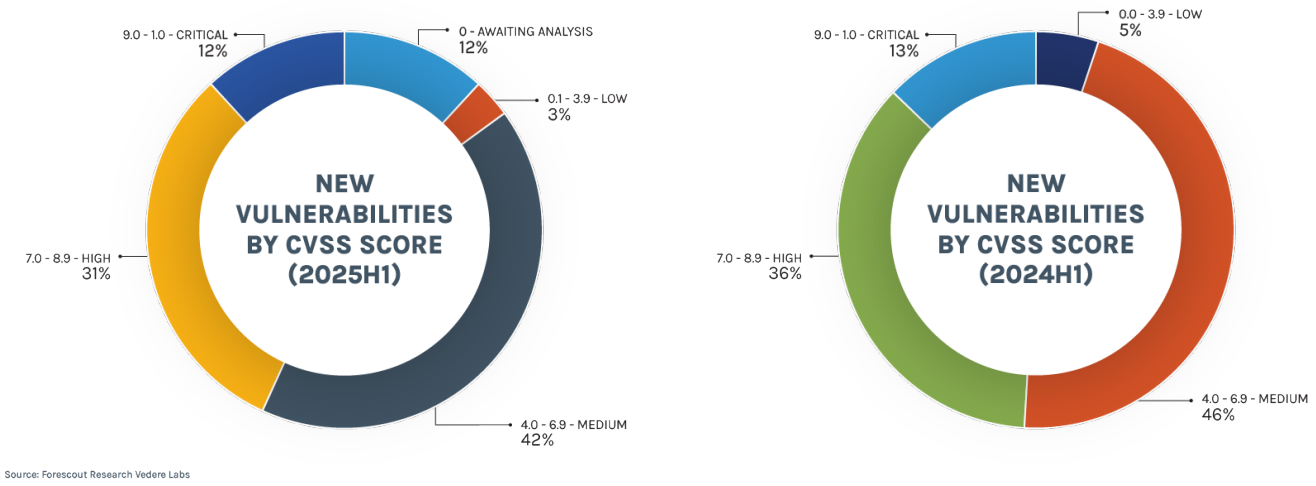



*Figure 2 – New vulnerabilities by CVSS score*

Raw CVE volume is one thing, but exploitation is what defines real-world risk. In 2025H1, 63 vulnerabilities were exploited as 0-days, up from the 43 in 2024H1, a 46% increase. These 0-days impacted products from 27 vendors, as shown in Figure 3. At this pace, 2025 is on track to exceed the record 100 exploited 0-days, set in 2024.

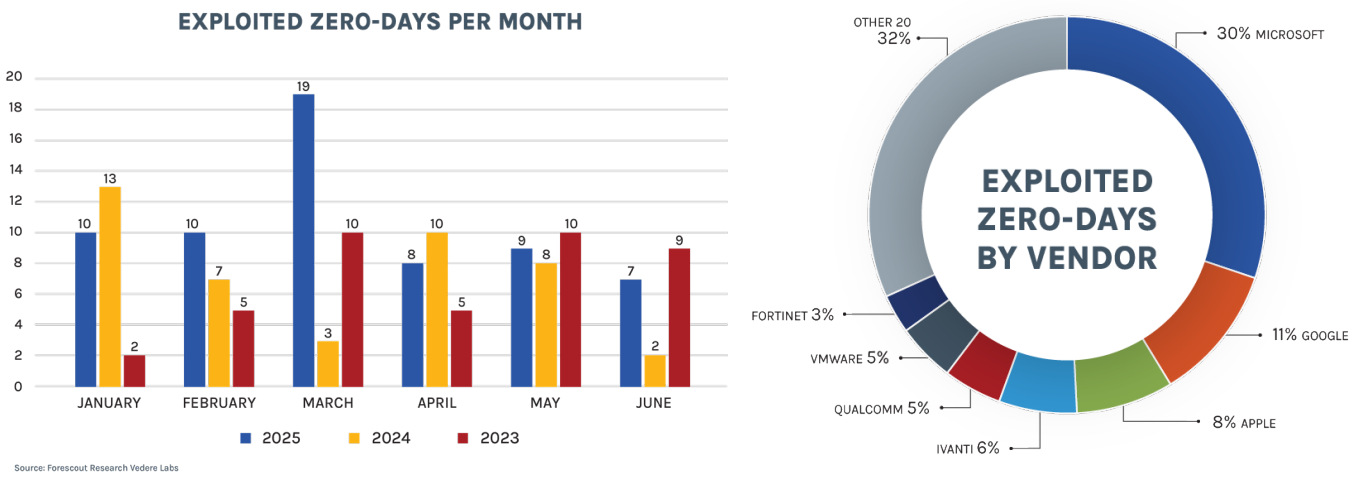



*Figure 3 – Distribution of new exploited 0-days per month and vendor*

Beyond 0-days, 132 CVEs were added to the CISA Known Exploited Vulnerabilities (KEV) catalog in 2025H1. That's an 80% increase from the 73 added in 2024H1, bringing the cumulative total to 1,371 CVEs. Figure 4 shows a breakdown of new vulnerabilities added to CISA KEV per month and vendor.

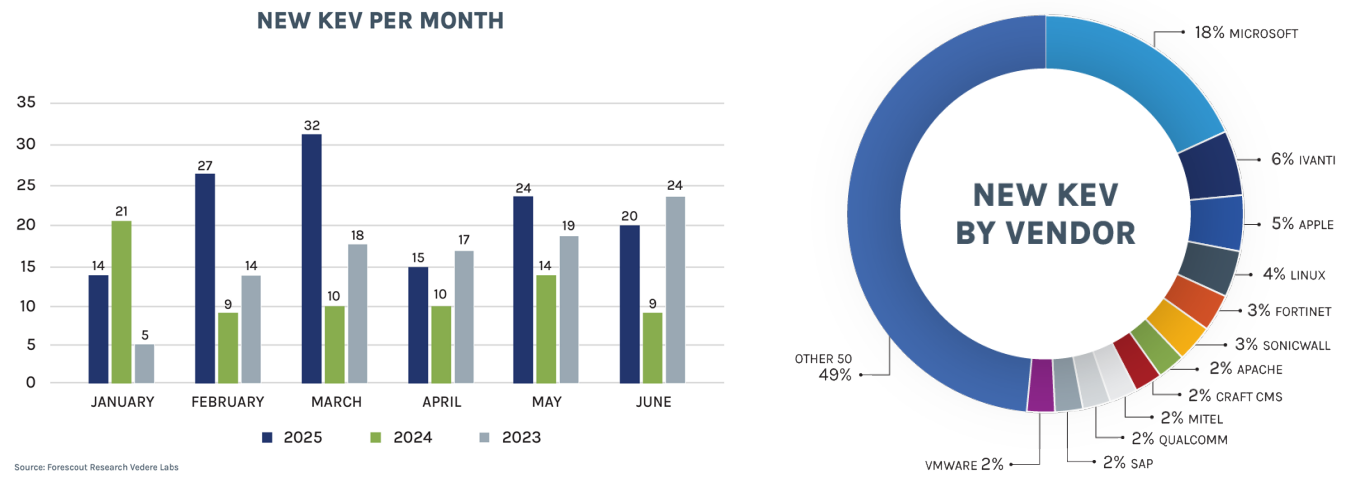



*Figure 4 – Distribution of new KEV per month and vendor*

On average, 22 new vulnerabilities were added to CISA KEV each month in 2025H1. The 132 new additions affected products from 62 vendors, an 88% increase from the 33 vendors affected in 2024H1. 26 of these vendors had more than one vulnerability added during the period.

Almost half of the new CISA KEV entries (47%) were for vulnerabilities published before 2025, a similar proportion as the previous year. Six of the vulnerabilities affected affect end-of-life products, which means no patches are available for this equipment: CVE-2024-0769, CVE-2023-33538, CVE-2021-32030, CVE-2024-11120, CVE-2024-6047, CVE-2025-1316. This underscores how legacy CVEs continue to represent active risk, as illustrated in Figure 5.

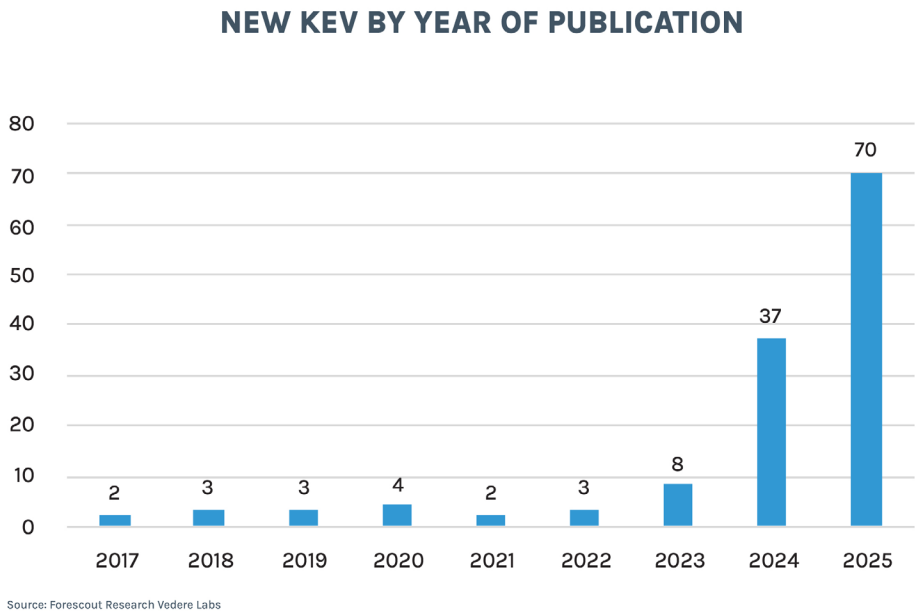



*Figure 5 – New known exploited vulnerabilities by year of publication*

The trend of exploits targeting perimeter and network infrastructure devices, first noted in 2023H1 and reported again in 2024H1, remains consistent in 2025. In 2025H1, 28 of the KEV entries (21%) targeted network infrastructure and security appliances. This is more than one in every five exploited vulnerabilities, aligning with last year. These figures reinforce our recent finding, that network infrastructure such as firewalls and routers are among the riskiest IT devices in 2025. These asset types are frequently internet-exposed, often undermanaged and highly attractive for lateral movement and persistent access.

## 3.2. Threat Actors

Forescout Research – Vedere Labs currently tracks 885 threat actors, of whom 137 had notable activity updates in 2025H1. Live tracking and actor profiles are available on our Threat Actor Dashboard. As shown in Figure 6, the majority of these 137 actors are:

- Cybercriminals (51%), including ransomware groups
- State-sponsored actors (40%)
- Hacktivists (9%)

This distribution has remained largely unchanged since 2023H1.

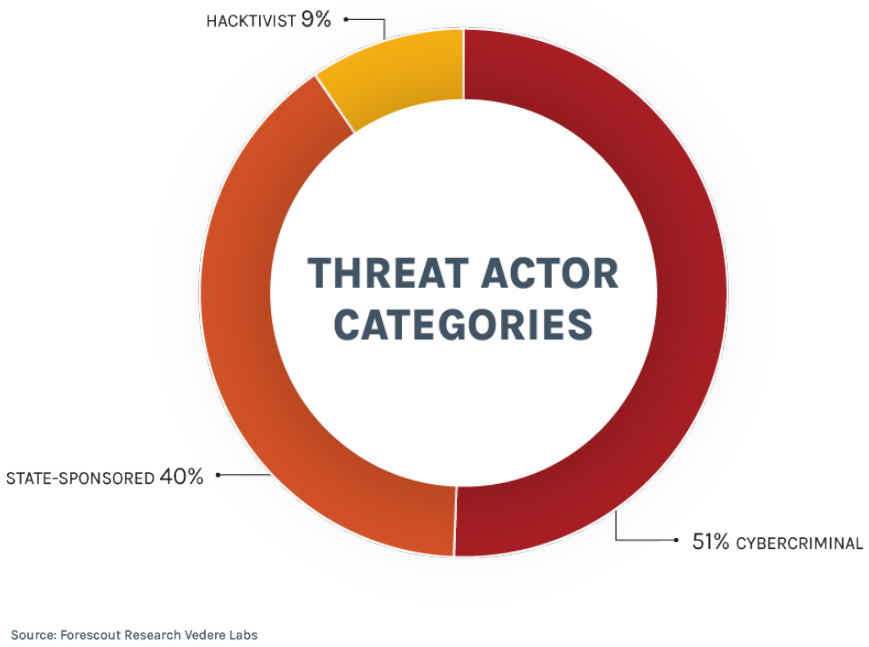



*Figure 6 – Distribution of solar power system vendors per country (top 5)*

Figure 7 shows that most active threat actors in 2025H1 continue to originate from China, Russia and Iran, accounting for 46% of tracked activity. This top three has remained unchanged year over year.

In 2025H1, we analyzed campaigns from Chinese threat actors targeting medical systems and enterprise software, and other researchers also reported their continued preference for targeting small office and home (SOHO) routers to create proxy botnets and continued activity against telecom and critical infrastructure providers. These campaigns reinforce China's continued interest in both espionage and infrastructure exploitation.

Russian and Iranian actors included hacktivist-style personas, such as NoName057(16) and Handala Group, whose attacks we analyzed in a recent report. These groups have focused on disruptive messaging and infrastructure impact, often aligning their activities with geopolitical flashpoints. On June 30, 2025, the CISA, FBI and NSA jointly issued an alert warning of the potential for increased targeting of US critical infrastructure by Iranian-linked actors.

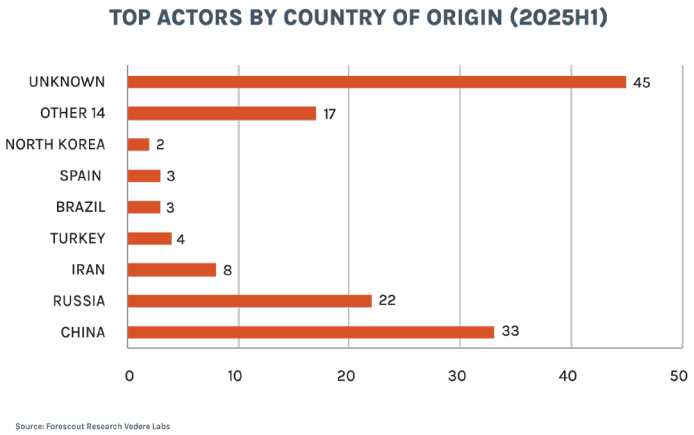



*Figure 7 – Threat actors by country of origin*

In total, threat actors in our dataset have targeted 159 countries. As seen in Figure 8, the US, India and the UK represent the primary targets. One notable shift: China dropped out of the top 10 list and was replaced by the Philippines. A similar pattern of minor reshuffling occurred in targeted industry verticals, as shown in Figure 9. The top 10 sectors remained consistent with 2024, with only minor changes in rank. Financial services dropped from second to third place, for example, and energy rose from eighth to fifth, reflecting increased threat activity against this sector.

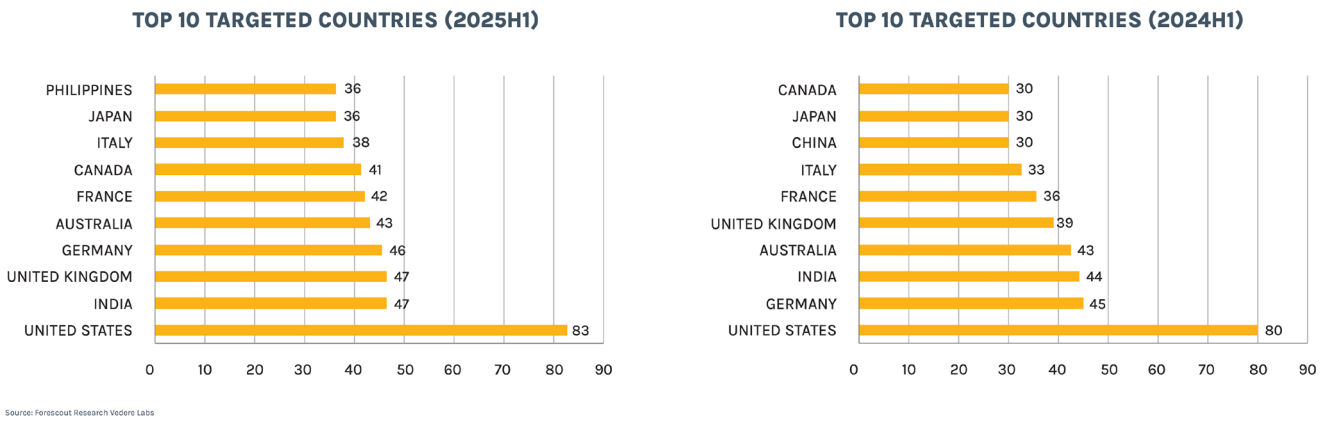



*Figure 8 – Top 10 targeted countries (by number of threat actors)*

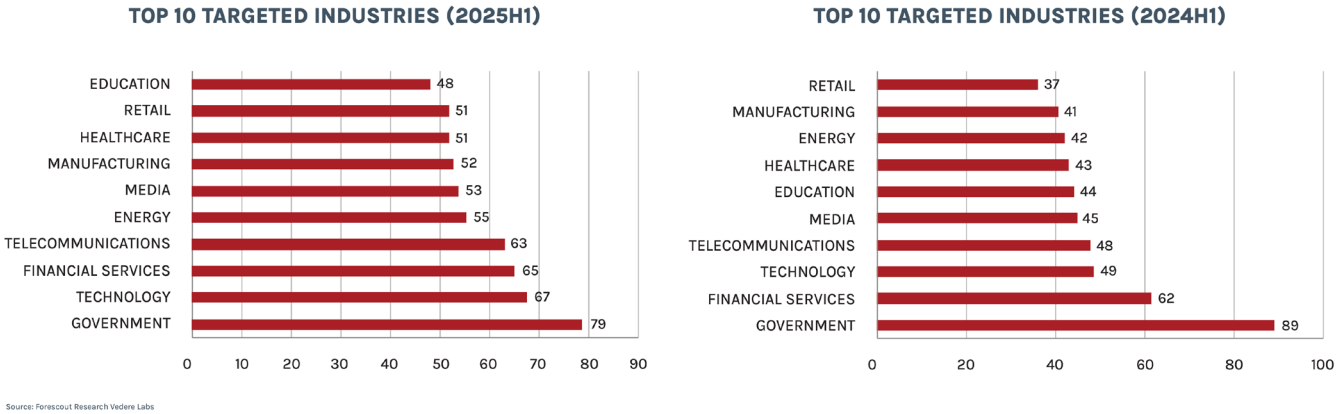



*Figure 9 – Top 10 targeted industries (by number of threat actors)*

## 3.3. Ransomware

Based on open-source tracking of ransomware leak sites, we observed 3,649 attacks in 2025H1, a 36% increase over the 2,676 attacks recorded in the same of 2024. This averages to 608 attacks per month or 20 per day.

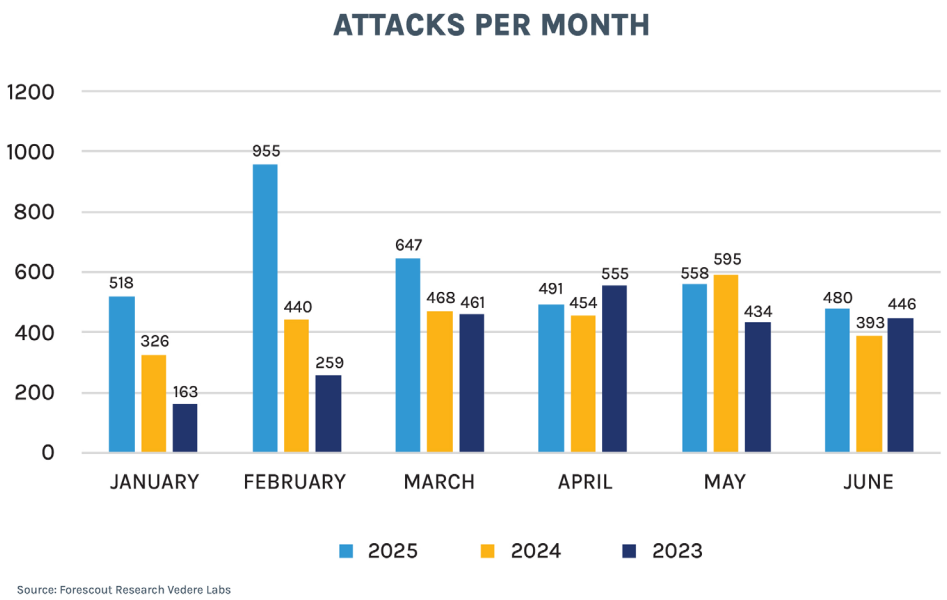



*Figure 10 – Ransomware incidents per month*

Figure 11 shows a breakdown of attacks by ransomware group in 2025H1 and 2024H1. Key developments: Cl0p became the most active group, overtaking LockBit, which dropped to 19th position following a major law enforcement operation in February 2024 and a leak of their affiliate panel data in 2025. Only four groups from last year's top 10 remained in the top tier: Akira, RansomHub, Play and Medusa. Overall, the ransomware landscape continues to fragment and expand although growth is slowing. The top 10 groups accounted for 59% of attacks in 2024H1 and 60% in 2025H1, while the number of active groups increased from 82 to 89, an 8.5% increase.

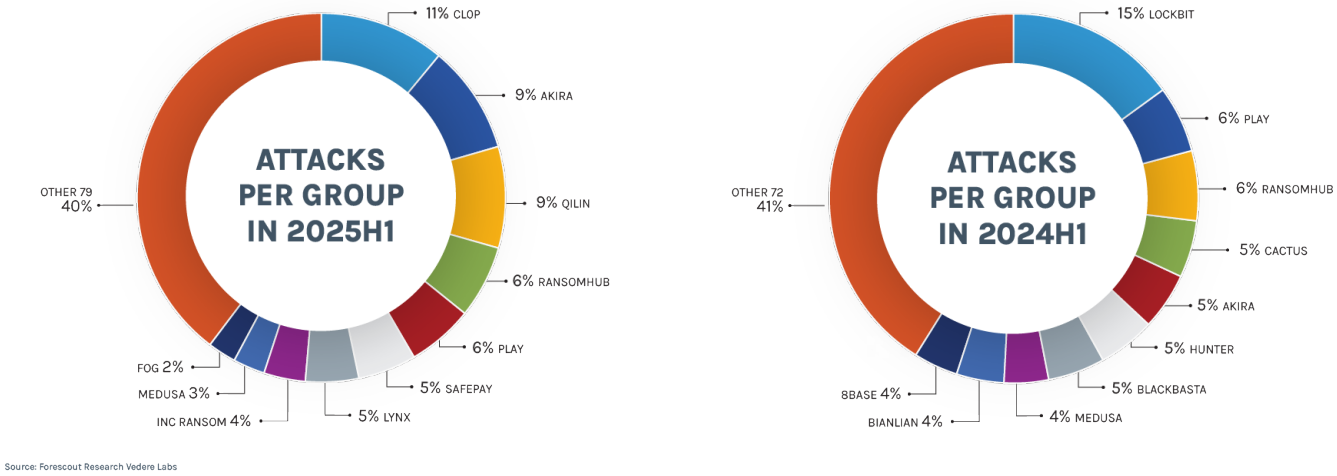



*Figure 11 – Ransomware incidents per group*

As in 2024, the top 10 targeted countries suffered 79% of all ransomware attacks. The U.S. alone accounted for 53% of global ransomware attacks, an increase from 48% in 2023 and 20% in 2024. Ransomware victims were recorded in 112 countries, a 9% increase from the 103 countries impacted in 2024H1. The top 10 country list remained consistent, with minor ranking changes. Canada overtook the UK to become the second most targeted country, and France surpassed Spain to move into sixth place.

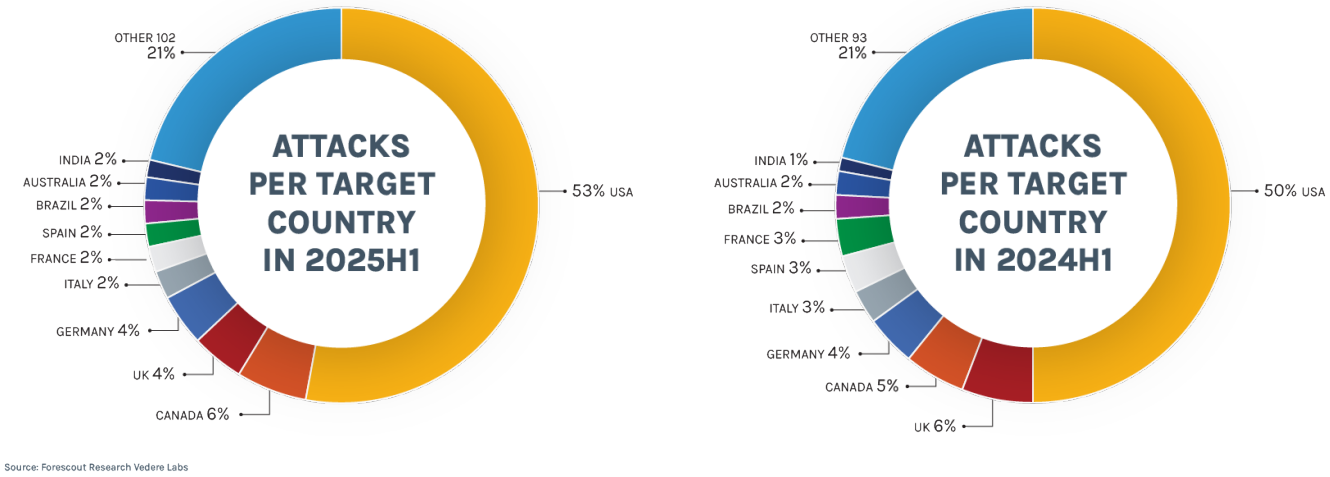



*Figure 12 – Ransomware incidents per target country*

Figure 13 illustrates the industry verticals most targeted by ransomware in 2025H1, showing little change from the previous period. The top five industries had only one minor change: services, manufacturing, technology, retail and healthcare – while in 2024H1 healthcare had more attacks than retail.

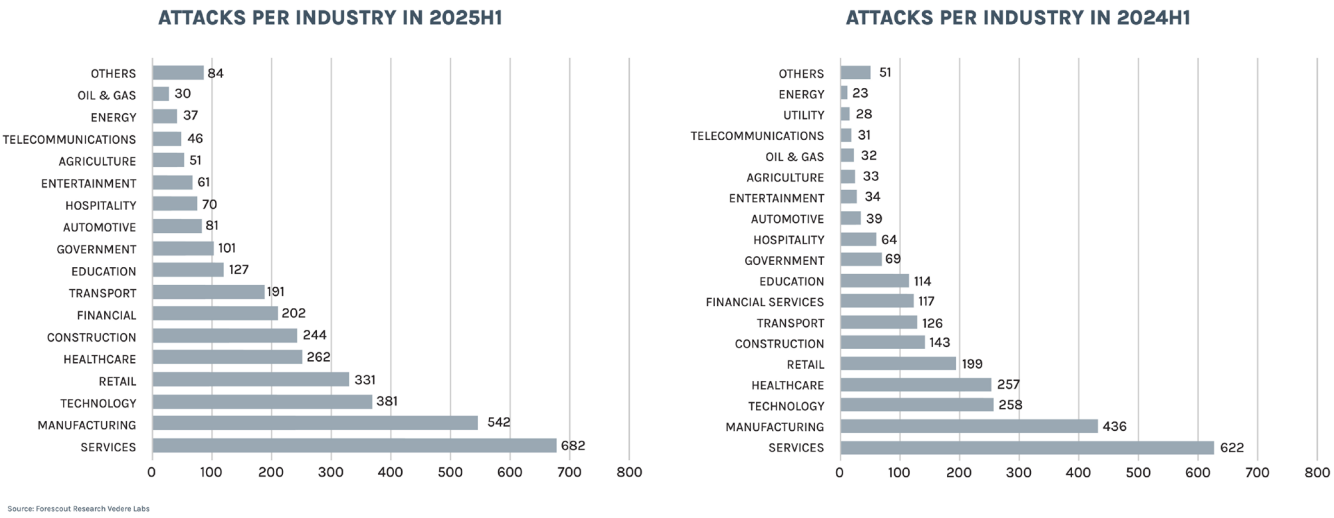



*Figure 13 – Ransomware incidents per target industry*

# 4. Deep Dive: APT IRAN and Shifting Identities – A Continuum of Iranian Hacktivist Threats to OT/ICS

Iranian hacktivist groups, often best described as state-sponsored faketivists, have consistently targeted operational technology and industrial control systems (OT/ICS) in the US and Israel since at least 2020. These attacks are frequently tied to geopolitical flashpoints and often accompanied by exaggerated or fabricated claims designed to maximize psychological impact.

With heightened tensions and conflict escalation in the Middle East in June 2025, CISA issued a warning that "*Iranian cyber actors may target vulnerable US networks and entities of interest.*" Soon after, the UK Parliament's Intelligence and Security Committee published a comprehensive threat report on Iran, highlighting "*rising and unpredictable threats*" including the country's cyber capabilities. The report noted Iran's motivation to build OT/ICS capabilities likely as a retaliatory evolution, specifically following attacks suffered in 2010 (Stuxnet) and 2012 (Wiper).

One critical omission in both reports is attribution to specific groups that may launch these attacks. We argue this is intentional, or at least understandable. Iran's threat landscape is now characterized by frequent identity shifting, which undermines the utility of tracking discrete group names.

Over the past five years, Iranian hacktivists have operated under multiple evolving personas. The most notorious, CyberAv3ngers, was attributed by the US in early 2024 to the Islamic Revolutionary Guard Corps – Cyber-Electronic Command (IRGC-CEC) and specifically to six senior officials within that organization.

The tactic of rotating identities, whether using hacktivist fronts or more covert rebranding, has precedent. IRGC-linked groups use this tactic to stay ahead of sanctions and attribution. Groups like APT33 (aka Elfin) and APT35 (aka Charming Kitten) have repeatedly cycled through public-facing identities, domains, and Telegram personas to evade attribution, minimize reputational cost, and complicate response efforts.

In this section, we demonstrate clear overlaps in targeting, capabilities and social media behavior across multiple Iranian personas. Our analysis indicates that CyberAv3ngers the Iranian Cyber Army and APT IRAN, likely form part of a deliberate continuum of state-directed or state-aligned activity, all converging on a core target set: Western OT and ICS infrastructure.

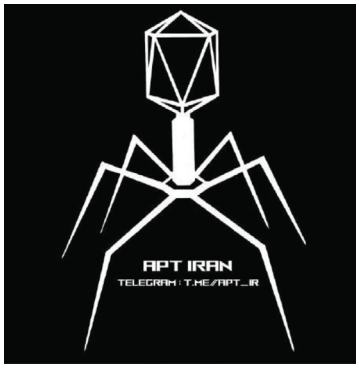
## 4.1. A Tale of Three Identities

Over the past five years, Iranian hacktivist operations targeting OT/ICS have appeared under multiple group names. Even a brief examination of three of these personas - ICTUS TEAM, CyberAv3ngers, and APT IRAN - reveals a pattern of calculated identity confusion, likely designed to hinder attribution and enable sustained disruptive activity with plausible deniability.

The first group which operated under the names ICTUS TEAM and Tapesh Digital Security Team Iran, used multiple logos throughout its activity, and deleted its posts on at least two occasions. Its logos included Iranian flag motifs biohazard symbols often used to represent computer viruses, and stylized references to their Persian name "Tapesh", meaning heartbeat.

The second group has maintained a consistent name, but has used multiple spellings interchangeably, CyberAv3ngers, CyberAveng3rs, CyberAvengers and Cyber Avengers. It also changed Telegram channels following a supposed account takeover by a rival Israeli group. Its logo prominently features the colors of the Palestinian flag and an image of a bird.


The third group, APT IRAN, has thus far only altered its logos and Telegram channels. The images below show its original logo, a bacteriophage, a virus that infects bacteria, (again possibly alluding to computer viruses) and its recent version, where the virus is depicted piercing a bird, possibly a sparrow in allusion to Israel's "Predatory Sparrow" group, which was responsible for high profile intrusions into Iran's Sepah Bank and Nobitex crypto exchange, both of which were extensively discussed by APT IRAN on Telegram.




While recurring imagery such as birds, national flag colors and virus iconography may not, on their own, confirm a connection between these identities, since these visual clues are used by others as well, the operational, thematic and behavioral links among them will become evident in the sections that follow.

**Early activity – ICTUS TEAM and the Iranian Cyber Army**

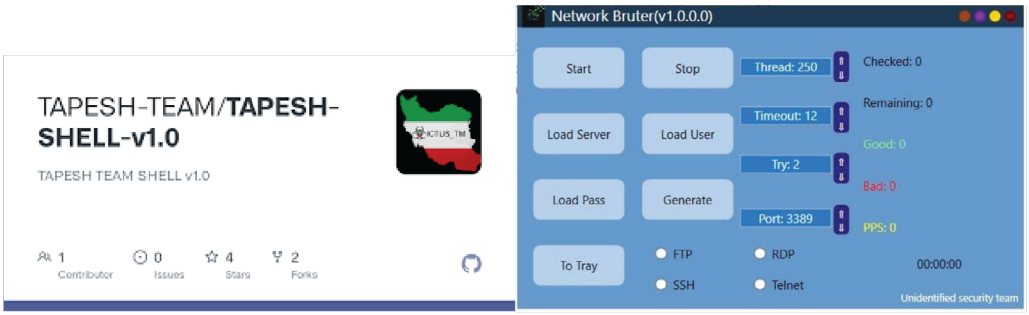
In December 2020, the persona known as 'ICTUS TEAM' (created earlier that year on April 25 and also known as Tapesh Digital Security Team Iran) published claims on Telegram that it had compromised the human machine interfaces (HMIs) of an American water facility and a Israeli energy provider. These claims, however, were never independently confirmed, and the actual impact remains unknown.

Throughout 2020 other Iranian groups including Bax026 and Unidentified Security Team reported similar attacks, asserting they had gained control over the HMIs of multiple Israeli facilities. Many of these actors aligned themselves with the "Iranian Cyber Army," a loosely defined coalition of Iranian hacktivists that primarily targeted Israeli organizations and their allies.

This wave of OT/ICS targeting coincided with, and was accompanied by, defacement campaigns against American and Israeli websites, some of which were later compiled into propaganda videos by ICTUS TEAM. All this activity happened during the early stages of the US government's 'maximum pressure' campaign against Iran and particularly in the aftermath of the assassination of Iranian general Qassem Soleimani. His image was

frequently featured in website defacements carried out by these groups, reinforcing the political motivations behind their operations.

Many of these actors also distributed hacking tutorials and custom tooling. ICTUS TEAM, for example, shared exploit and malware code via a now-deleted repository (`github.com/TAPESH-TEAM`), and posted instructional videos to YouTube until 2022. The Unidentified Security Team published tools such as a "Network Bruter" through its own GitHub page (`github.com/Unidentified-security-team`).




These materials, often technical in nature, were accompanied by propaganda and commentary on Telegram, where most posts were written in Farsi. In contrast, their defacement messages were typically presented in English, likely intended for international audiences.

There were several periods of activity and hiatus among these groups, often reflecting geopolitical developments or internal disruptions:

- **The Unidentified Security Team** remained active until June 2022, then resurfaced in February 2023 and has continued operations through to the present.
- **Bax026** maintained consistent activity until September 2022, followed by sporadic appearances in 2023 and 2024. The group returned on June 13, 2025 – coinciding with Israel's strikes on Iran.
- **ICTUS TEAM** deleted its original Telegram posts on 3 February 2022, and redirected members to the BiskooitPedar channel, which had been created in March 2021 to share hacking tutorials. On February 12, ICTUS TEAM resumed activity by reposting content from BiskooitPedar. Then, on 12 September 2022, the group again wiped its post history, formally announced its dissolution and encouraged followers to migrate to other groups, including APT IRAN, which we examine in detail below. ICTUS TEAM also submitted their defacements to Zone-H, though activity on that platform ceased in 2022, with only two entries recorded in June 2024 before a brief return in April 2025.

The hiatuses or declared dissolutions of several of these groups occurred around the same time as the wave of civil unrest in Iran following the death of Mahsa Amini in police custody. That period of internal upheaval, which lasted roughly a year, likely disrupted coordination among Iranian hacktivist actors. Notably, the end of that unrest coincided with the emergence of a new and more globally visible hacktivist persona: CyberAv3ngers.

**CyberAv3ngers**

CyberAv3ngers started posting on Telegram on September 13, 2023, with three introductory messages: "Hello world!", "We Are Back Again!", and "Do You Remember Us?" These posts strongly suggest that the persona was a rebranding or revival of a previously active group.

The earliest reference to "Cyber Avengers" dates back to 2020 when the name was associated with claimed attacks including a gas tank explosion and disruption to Israel's railway system, claims later denied by the Israeli government. These messages circulated on various Telegram channels, accompanied by propaganda videos in English, as seen in the screenshots below.



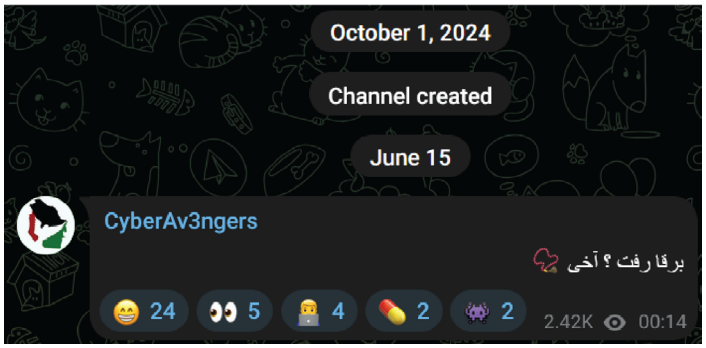
Throughout 2023, CyberAv3ngers continued to publish claims of cyberattacks, many of which appeared to be fabricated or exaggerated. A notable example was the group's claim to have hacked Israel's Dorad power station. However, the materials they shared were reused images from a prior leak attributed to the Iranian group Moses Staff.

From the outset, CyberAv3ngers posted exclusively in English – a marked shift from the Iranian Cyber Army's Farsi-language communications. This linguistic choice suggests the group aimed to gain international visibility, a goal they achieved in late 2023 and early 2024 through a campaign of confirmed attacks on Israeli-made Unitronics programmable logic controllers (PLCs). These attacks defaced PLCs across multiple countries and, unlike prior claims from ICTUS and CyberAv3ngers, the attacks were verified by numerous victims, including at least 29 incidents in the US, the majority of which were water utilities.

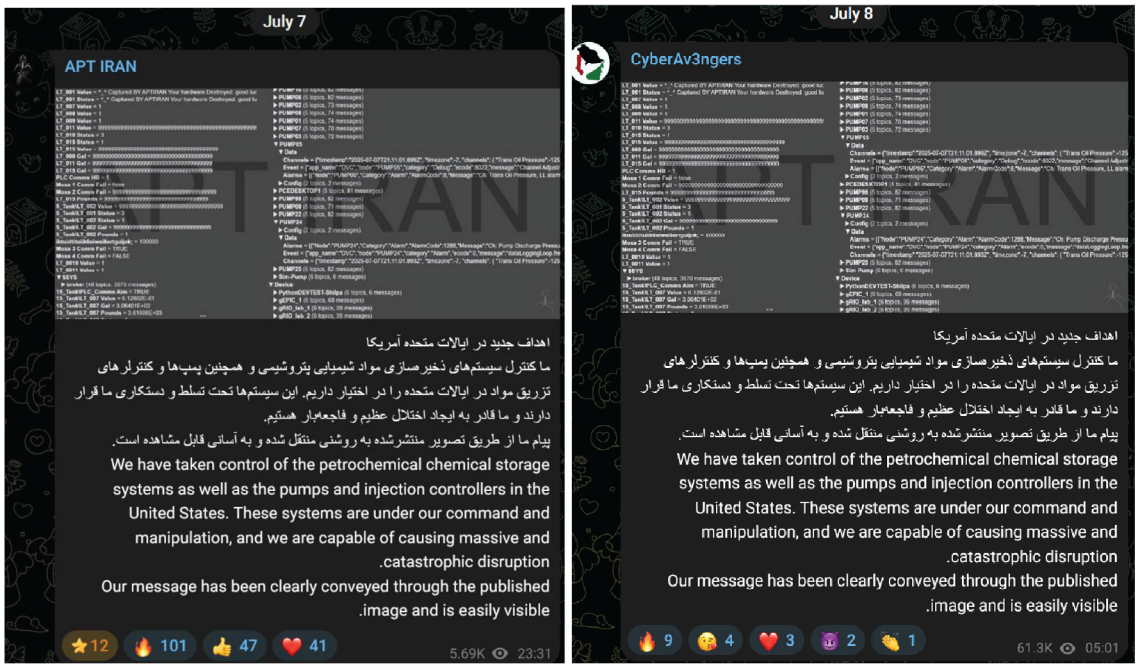
In February 2024, the US Department of the Treasury sanctioned six IRGC officials allegedly affiliated with the group. CyberAv3ngers remained active publicly until April 2024, when their original Telegram channel was supposedly taken over by an Israeli actor known as “WeRedEvilsOG”. Around the same time, the identity of one of the sanctioned IRGC officers was further exposed. In response, the group shifted its activity to its X (formerly Twitter) account, where it posted a defiant message, “wait for next steps”, and published a letter condemning the “oppression of Telegram platform.”

Reports published later in 2024 confirmed that the group’s custom malware, IOCONTROL developed to target fuel station infrastructure and IoT devices, remained active in the wild as late as August 2024.

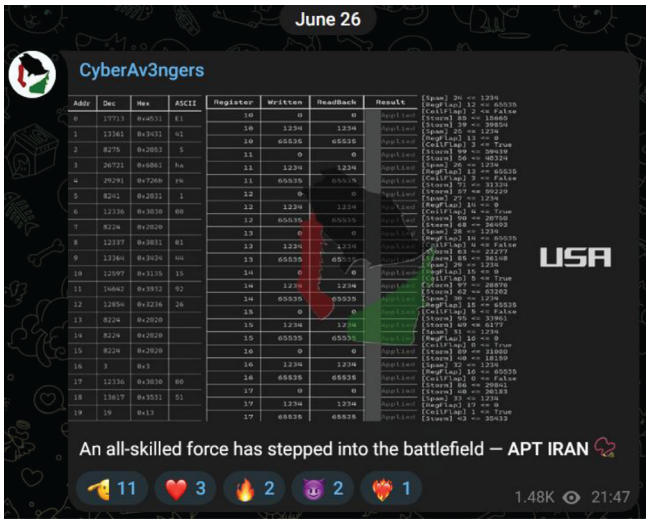
After several months of silence, CyberAv3ngers reappeared on June 15, 2025, posting in Farsi. The message read: “Did the electricity go out? Oh my”. It was posted on a new Telegram channel that had been quietly created in October 2024.




Following this reappearance, the group began sharing a series of attack claims against OT/ICS targets. Many of these posts either featured APT IRAN’s branding or were directly reposts from APT IRAN’s Telegram channel. In some cases, there was no clear distinction between original content and forwarded messages. In one particularly striking instance, CyberAv3ngers posted the exact same message and image as APT IRAN had shared, only five hours later, without using Telegram’s native forwarding feature.



CyberAv3ngers's second post after their hiatus, on June 26, carried a telling message:




**APT IRAN**

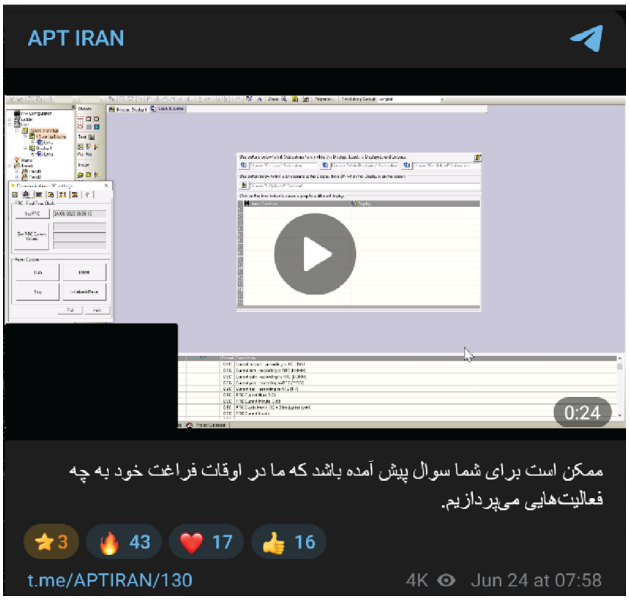
The "APT IRAN Research Center" Telegram channel was created on March 27, 2024, though its first post did not appear until November 29. However, the APT IRAN group predates this channel and had previously operated through other handles, including now deleted GitHub repositories. Content shared under the APT IRAN banner has largely focused on exploit and malware PoCs, including Linux rootkits and alleged 0-days targeting wireless access points.

Their messages are predominantly in Farsi, consistent with earlier groups such as ICTUS and the Iranian Cyber Army, but some examples also appear in Russian and Chinese, as shown in the image below where they promote the Black Market Telegram channel hosting several C2, infostealer and ransomware samples.

On June 13, 2025, coinciding with Israeli strikes on military and nuclear facilities in Iran, the group posted a long message on their channel that boiled down to “Enough talk... it’s time for action”. They promised to release sensitive material and, later that day, claimed to have leaked credentials for Israeli government systems and universities.

On June 14, the group escalated its approach from tool-sharing to destructive action. They announced the use of LockBit and ALPHV ransomware against government servers, explicitly stating that decryption would not be offered to victims. The message warned that these actions represented only “part of the initial capabilities” at their disposal. This was a clear step-up from their usual focus on sharing known exploit proofs-of-concept for web applications and IoT devices.

On June 24, the same day a ceasefire was announced between Israel and Iran, APT IRAN began posting about PLC targeting. One post read “You may have wondered what activities we do in our free time.” and was accompanied by a video showing an actor connecting to a Unitronics PLC via engineering software and performing a reset. The choice of target echoed the earlier, widely publicized Unitronics attacks conducted by CyberAv3ngers.

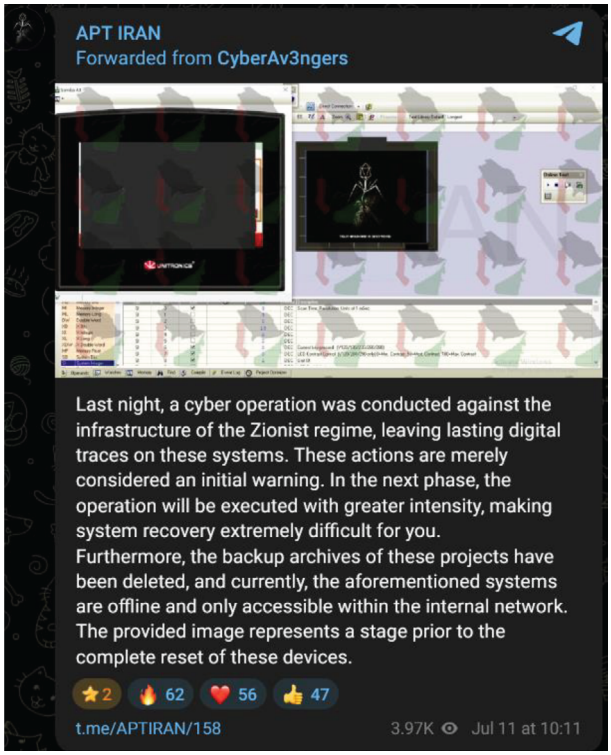



On June 25, the group revealed a new visual branding image they stated would be used in future defacement operations.

On June 26, they claimed to have launched a “false data injection” attack on “control devices in the United States that use AT&T services.” A screenshot posted alongside the message showed a command-line interface issuing commands to rewrite coil and register values, using names such as RegFlap, CoilFlap, Storm and Spam. The precise controller type and sector were not disclosed, but the message asserted that “*The main goal of these tools is to push the devices into a critical state such as exploding or going out of service. We can confidently announce that in the most pessimistic scenario, these devices are currently stopped and unable to provide services.*” This attack was the first APT IRAN attack claim to be to be reposted by the CyberAv3ngers channel.

On June 27, APT IRAN claimed responsibility for an attack on fuel stations in both Israel and the US, sharing screenshots of the HMI of a specific station and stating that they had the ability to “completely erase the data of these systems.” This was the first message from the group written entirely in English. On July 7, they claimed to have taken control of petrochemical storage infrastructure in the US, including pumps and injection controllers. That message was delivered both in Farsi and English, reflecting a growing emphasis on international visibility.

Finally, on July 11, APT IRAN forwarded a message originally posted by CyberAv3ngers, which showed a defaced Unitronics PLC, bearing the logos of both groups. The shared imagery suggested close coordination or even operational merging between the two personas.




At the time of writing, none of the recent attacks claimed by APT IRAN have been independently verified. The group’s behavior closely mirrors that of CyberAv3ngers, which in its early stages exaggerated or fabricated claims, but later proved capable of successfully compromising several Unitronics PLCs and other devices. Although the number of Internet-exposed Unitronics devices has declined since the wave of attacks in 2023, a measurable number remain publicly accessible.

## 4.2. Comparative Analysis

**Targeting**
All three identities, ICTUS TEAM, CyberAv3ngers, and APT IRAN, appear to mix political motivation with opportunistic targeting. Their typical criteria involve targets being located in Israel or allied nations or

organizations using Israeli-made technology. The latter focus was introduced by CyberAv3ngers as a distinctive targeting tactic, and has since been adopted by APT IRAN, though the newer group has not emphasized it as strongly in its defacement imagery.

As with other hacktivist personas, whether independently operated or state-sponsored, these groups likely compiled target lists based on those criteria, then opportunistically attacked critical infrastructure within that scope. Rather than selecting the most high-value or hardened targets, they appear to prioritize systems that are exposed, vulnerable, and likely to generate maximum visibility with minimal effort.

The prevalence of victims in the water sector says more about systemic weakness in that sector, such as internet-exposed devices and limited security budgets, than it does about the attackers' strategic priorities. It is also important to consider the role of visibility bias. Water utilities, particularly in the US, are more likely to report cyber incidents due to regulatory obligations or media scrutiny. That may skew the perceived targeting patterns of Iranian hacktivist groups. Their intent may in fact be broader, but their confirmed successes tend to occur in sectors with both weak defenses and mandatory disclosure requirements.

**Capabilities**

All three personas share a common baseline of technical capabilities, with some important distinctions:

- **Little to no use of DDoS.** While Distributed Denial of Service (DDoS) attacks are a signature tactic for many hacktivist groups – including prominent Russian actors like NoName057(16) and Killnet – none of the Iranian personas discussed here have used this method frequently, suggesting a more strategic or technically-focused approach.
- **Preference for defacements.** All three groups have consistently employed defacement as a method of disruption and propaganda. In the early phases, this took the form of website defacements, particularly by ICTUS TEAM and the Iranian Cyber Army. More recently the technique has extended to OT environments, with CyberAv3ngers and APT IRAN defacing PLCs.
- **Development of custom tools and exploits.** While many hacktivist actors rely on repackaged tools, these Iranian personas have demonstrated more advanced capabilities. ICTUS TEAM developed a custom web shell and several exploit proof-of-concepts, many attributed to the alias Aryan Chehreghani on Exploit-DB. APT IRAN also shared at least one 0-day targeting wireless routers and seemed to develop its own tool to interact with controller variables. CyberAv3ngers went a step further with the creation of IOCONTROL, a sophisticated malware strain designed to disrupt fuel station systems and other IoT devices.
- **Progressive familiarity with OT/ICS.** Earlier groups like ICTUS team and the Iranian Cyber Army often shared screenshots of HMIs and web GUIs of control systems, but their posts reflected limited operational understanding, more propaganda than proof of access. In contrast, CyberAv3ngers demonstrated a clear ability to interact with and manipulate OT devices, particularly Unitronics PLCs. Their attacks included reprogramming logic, altering network settings, and locking out legitimate operators. APT IRAN's more recent activity shows similar interaction with OT protocols (likely Modbus) and suggests a comparable level of sophistication.

Among the three, CyberAv3ngers remain the most capable in OT/ICS-specific operations. As detailed in CISA's report the group successfully "*supplanted existing ladder logic files with their own, renamed devices likely to forestall owner access, reset software versions to older versions, disabled upload and download functions, and changed the default port numbers.*" These TTPs are significantly more advanced than what is typically observed in hacktivist circles, including those that target IoT or OT assets. It is likely that APT IRAN is now employing these same techniques, given their mirrored targeting of Unitronics devices and shared operational infrastructure.

An additional relevant capability is the use of ransomware as a tool of disruption. As detailed earlier in this report, APT IRAN claimed to have deployed ransomware with the specific goal of wiping data, not extorting payment. A similar claim was made in 2023 by a group called Soldiers of Solomon, known to be IRGC-affiliated and is tracked by Microsoft as the same threat actor as CyberAv3ngers.

Iran has a long history of politically motivated destructive malware campaigns. The 2012 Shamoon attack, on Saudi Aramco, remains one of the most devastating examples, and since then, Iran-linked actors have deployed successive iterations such as ZeroCleare and AzureWiper. The pattern of blending ransomware and wiper malware tactics is now well-established across these personas.

**Social media activity**
There are notable similarities in how these three personas have used online platforms to shape their narratives, attract followers, and disseminate propaganda:

- **Delayed channel activation.** In every case, the groups created communication channels, especially on Telegram, months before they began posting. This is behavior echoes "domain parking" strategies used in malware campaigns. Such premeditation is more consistent with state-backed organizations than grassroots hacktivism.
- **Shared platforms and formats:** With the exception of CyberAv3ngers, all the personas used the same platforms (Telegram, X, YouTube and GitHub) and shared similar content types: hacking tutorials, exploit proof-of-concepts, training materials, attack claims (mostly defacement) and ideological propaganda primarily in Farsi. CyberAv3ngers stood out by publishing almost exclusively in English from the outset and focusing almost entirely on attack claims and visual messaging designed for an international audience.
- **Orchestrated inactivity and rebranding:** All three groups experienced extended periods of silence, often coupled with announcements that the group was dissolving. These pauses mostly appear to have been strategic. In each case, followers were redirected to new channels and personas suggesting an intentional mechanism for rotating identities while maintaining momentum and narrative continuity.

## 4.3. What Does It All Mean?

The recurring similarities in targeting, capabilities and social media behavior across ICTUS TEAM, CyberAv3ngers, and APT IRAN strongly suggest that most, if not all, of these identities are controlled or coordinated by the IRGC. Taken together, they form a continuum of Iranian threats to OT/ICS assets in the West which can be broadly divided into three distinct operational phases:

- A 'test' phase with ICTUS and the Iranian Cyber Army (2020-2022). During this period, Iranian actors experimented with accessing OT/ICS systems, primarily through HMIs and publicized their claims on Telegram. Many of these attacks, like those attributed to the original Cyber Avengers, were either exaggerated or fabricated. However, they demonstrated that psychological impact, particularly when tied to infrastructure, could be more effective than traditional defacements or DDoS.
- An 'operational' phase with CyberAv3ngers (2023-2024). This was the turning point, during which the threat actor developed credible OT/ICS disruption capabilities. Attacks on Unitronics PLCs resulted in verifiable global impact, especially in the US water sector. The group's success ultimately led to public attribution and sanctions by the US government.
- A 'post-sanctions' phase with APT IRAN (2025). Following the US sanctions and an extended period of apparent inactivity, multiple Iranian hacktivist personas have reactivated, most notably APT IRAN. This group appears to have inherited both the infrastructure and tactics of CyberAv3ngers: targeting Unitronics devices, switching to English-language messaging, and claiming impactful OT/ICS disruptions. Their reemergence has coincided with increased geopolitical tension in the region, particularly following Israeli military actions on June 2025.

Whether all these personas are controlled by a single entity or are operated by different subgroups within the IRGC is unclear. However, the use of multiple overlapping identities is not without precedent. For instance, Microsoft has linked CyberAv3ngers and Soldiers of Solomon to the same underlying IGRC group. Similarly, Mandiant has attributed three Russian hacktivist personas – Xaknet, Cyber Army of Russia Reborn (CARR), and SoIntsepek – to the APT44/Sandworm threat actor, which blends espionage, disruption and influence operations under a rotating set of names.

An alternative theory suggests that the IRGC may have taken over originally grassroots hacktivist accounts. Supporting this possibility, UK-based Iranian opposition activist Nariman Gharib has claimed that the IRGC arrested the original APT IRAN channel admins, potentially co-opting the platform for state-directed operations. Notably, APT Iran was involved in a 2024 campaign against Iran's own railway infrastructure, an unusual action for a state-aligned actor unless aimed at discrediting internal dissent or seizing control of the group.

Regardless of their origin, these personas offer operational advantages to the IRGC. They can be activated or de-activated at will, allowing for staged exits, rebranding and resurrection during periods of heightened tension. This fluidity helps create the illusion of popular, grassroots support while complicating attribution and response for defenders and analysts.

It's also essential to understand that periods of silence do not necessarily indicate inactivity. Personas may be shelved, rebranded, or shifted toward more covert activities, such as espionage or lateral access operations that are intentionally less visible. A move away from noisy publicly claimed ICS attacks may simply indicate a strategic pivot to more destructive operations, timed to coincide with kinetic escalation or regional events.

It is highly likely that the IRGC maintains a stable of additional hacktivist personas beyond those detailed in this report, accounts that can be rapidly activated as geopolitical conditions demand.

# 5. Mitigation Recommendations

Organizations should **prioritize extending** visibility, risk assessment **and** proactive controls **across the increasingly exploited attack surface including network perimeter assets, operational technology, healthcare systems and IoT assets.**

At a minimum, organizations should:

- Ensure full visibility into these assets, including their presence on the network, the software they run, and their communication patterns. This can be achieved at scale with agentless solutions.
- Understand their risk profile concerning vulnerabilities, weak configurations, exposure and other factors.
- Disable unused services and patch vulnerabilities to reduce the window of exploitation.
- Change default or easily guessable credentials and use strong, unique passwords for each device.
- Enforce Multi-factor Authentication (MFA) whenever possible to add an additional layer of security, especially for VPN authentication processes.
- Encrypt all sensitive data in transit and at rest, especially personally identifiable information (PII), protected health information (PHI) and financial data.
- Avoid exposing unmanaged or legacy devices directly to the internet, unless absolutely necessary. Where exposure is required, ensure administrative interfaces (such as web UIs and engineering ports) require authentication and are secured behind IP-based access control lists or a VPN-protected management VLAN.
- Enable IP-based access control lists for specific protocols, such as Modbus and BACnet for OT networks.
- Segment the network to isolate IT, IoT and OT devices, limiting network connections to only authorized management and engineering workstations or among unmanaged devices that need to communicate. Segmentation also helps to prevent lateral movement with compromised credentials.

Informed by our research in 2025H1, we also recommend the following enhanced measures:

- Enable endpoint logging beyond alerts to include process, file, user, network, registry, driver and PowerShell activities.
- Gather logs from systems handling user authentication, especially SSO and cloud service access.
- Deploy continuous monitoring for suspicious authentication attempts and frequently review logs for potential unauthorized access.
- Rotate credentials and cryptographic keys suspected of being compromised.
- Block suspicious TLDs associated with infostealer infrastructure.

- Implement browser security controls to protect against credential theft.
- Conduct targeted training on social engineering techniques.

Once these controls are in place, ensure that threat detection and response systems encompass every device within the entire organization. Today's threats now move from one type of device to another, and it is crucial to detect them across the entire organization – from an entry point such as a vulnerable router, to a pivot point, like a misconfigured workstation, and to a final target such as an insecure OT device. Ensure your threat detection solution covers all device types and ingests data from multiple sources, including firewalls, intrusion detection systems, endpoint detection and response (EDR), and other existing security infrastructure.