



Executive Threat Insights

Q2 2026

Executive Threat Insights, Q2 2026

Contents

1. Significant ICS/OT Security Events & Reports
2. Q2 2026 Case Studies
3. Geographic Heat Map of ICS/OT Incidents
4. Impacted Sectors & ICS/OT Vendors
5. MITRE ATT&CK & ICS Cyber Kill Chain Observations
6. Ransomware Observations
7. Hacktivism Observations
8. Vulnerability Advisories
9. Call to Action

Q2 Executive Summary

BAUXITE

top Dragos TG
8 WV mentions

United States

top country
22 mentions

Energy

top sector
36 mentions

Edge Access

top vendor theme
31% advisory items

Stage 1

Kill-Chain
57 mentions

WHAT CHANGED FROM Q1

- 97 World View Products covered across 01 May 2026 to 31 July 2026.
- BAUXITE was the most frequently referenced Dragos threat group; TREMOLITE was introduced late in the reporting window.
- The United States, India, and Israel were the most frequently referenced countries.
- Energy/Utilities/Oil & Gas/Nuclear/Solar, Manufacturing, and Water/Wastewater led sector mentions.
- Majority of kill-chain mappings in WV Products Covered were Stage 1

Significant ICS/OT Security & Threat Events, Q2 2026

Significant ICS/OT Security Events & Reports from Q2, 2026

This timeline shows some of the most significant industrial control systems/operational technology (ICS/OT) security events and reports of the second quarter of 2026.

12 May: TAT26-32 (Ababil of Minab) Claims Attack on Tri-Rail/South Florida Regional Transportation Authority (SFRTA)

14 May: TAT23-44 Operational Relay Box (ORB) Network

15 May: OT Defense Fundamentals in an AI-Accelerated Threat Landscape

18 May: Taiwanese TETRA Spoofing Incident: A Transportation-Wide Warning

24 May: GitHub Breach Highlights Code Supply Chain Concerns

1 June: GRAPHITE Continues Targeted Credential Harvesting and Discovery Campaigns Using Defense Lures

1 June: When the World Is Watching, OT Threat Amplification During Global Sporting Events (FIFA World Cup and Olympics 2028)

5 June: Raspberry Robin Malware Detection Reported on Vendor-Supplied USB Media

11 June: The Pro-Houthi Persona (TAT26-48) Follows Hacktivist Precedent and Shifts to Internet-Exposed OT Systems

23 June: FortiBleed: 75,000+ Fortinet Firewalls Compromised via Credential-Harvesting Campaign

26 June: BAUXITE Reiterates Claims of Omron PLC Compromise in U.S. Telecommunications

6 July: Ransomware Targeting of the Australian and New Zealand Agriculture and Food Production Sector

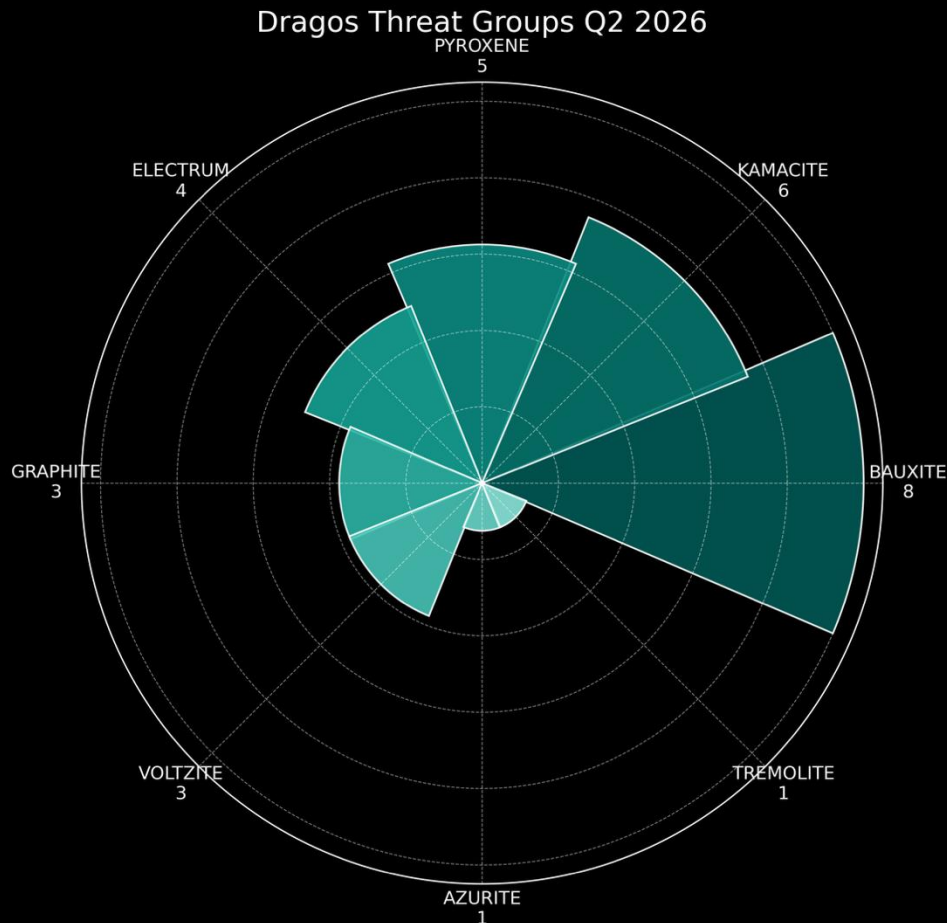
15 July: Escalating Campaign Targeting Automatic Tank Gauge Systems Across U.S. Critical Infrastructure

Note - This timeline is not all-encompassing and is intended to capture the most relevant and significant ICS/OT threats and risks discovered and analyzed by Dragos Intelligence.

Dragos Threat Groups

Q2, 2026 Observations

- **BAUXITE** remained the most frequently reported Dragos threat group in Q2 2026, with eight mentions. However, activity was less concentrated than in the previous quarter, as **KAMACITE** followed closely with six mentions and **PYROXENE** with five.
- **ELECTRUM** formed the next tier with four mentions, while **GRAPHITE** and **VOLTZITE** were each reported three times. **AZURITE** and **TREMOLITE** appeared once each, indicating a broader distribution of reported threat-group activity across the quarter.



Q2 2026 Case Studies

Based on Worldview Reporting

AI-Accelerated Threats to OT

A force multiplier, not a new threat Global • All sectors • 15 May 2026

WHAT IS ACTUALLY CHANGING

AI accelerates reconnaissance, automates routine tasks, and lowers the skill barrier to entry. It compresses the time between initial access and impact.

It does not change adversary intent or create new categories of risk, and human direction and oversight are still required. Today's models remain noisy and error-prone on complex, multi-step attacks.

The shift shows up across four areas: AI-assisted intrusions, AI-enhanced phishing and deepfakes, AI-generated malware, and AI-assisted vulnerability discovery.

80-90%

Share of a disclosed cyber-espionage operation automated with AI tooling (Nov 2025).

600+

FortiGate devices compromised using commercial AI, relying on weak credentials rather than zero-days (Feb 2026).

Hype ≠ threat

AI-built malware and autonomous zero-day claims remain largely unproven. Dragos rates them low-confidence near-term risks.

WHY IT MATTERS TO OT

Faster escalation, narrower response windows

As AI shortens the path from access to impact, the detection windows defenders rely on narrow.

Faster escalation raises the risk of conventional ICS impacts: loss of view or control, unsafe operating conditions, equipment damage, and unplanned outages.

Those consequences cascade into operational disruption, safety incidents, regulatory exposure, financial loss, and scrutiny from regulators, insurers, and investors.

AI targets weaknesses that already exist. Per the Dragos 2026 Year in Review, 81% of organizations have poor IT/OT segmentation and over 80% struggle to detect, contain, and activate incident response.

OT-RELEVANT CASE: APRIL 2026

Dragos analyzed an AI-assisted intrusion at a Mexican municipal water and drainage utility, following compromise of the enterprise IT network.

The adversary used a commercial AI assistant to speed up execution, flagged an IIoT gateway as a high-value access point, and ran password-spraying with default credentials.

Activity stayed at Stage 1 with no confirmed OT access. But weak authentication could have enabled escalation to a Stage 2 ICS attack.

WHAT TO DO

AI changes the speed, not the fundamentals

Resilience comes from consistent execution of the SANS Five ICS Cybersecurity Critical Controls, still the most effective layered defense.

- 1 OT/ICS Incident Response**
Define decision triggers and authority in advance. Treat loss of view or control as valid grounds to activate OT incident response.
- 2 Defensible Architecture**
Eliminate implicit trust across IT and OT. Minimize internet-reachable OT exposure and force movement through observable chokepoints.
- 3 ICS Network Visibility & Monitoring**
Deploy ICS-protocol-aware monitoring across IT/OT boundaries, remote access, and vendor connections, with retention for investigation.
- 4 Secure Remote Access**
Mandate MFA and conditional access. Limit session duration and privilege, and govern all vendor and cellular access paths.
- 5 Risk-based Vulnerability Management**
Prioritize with “Now, Next, Never.” In OT, reduce risk by restricting paths and improving detection, not by patching alone.

Dragos coverage: Platform visibility, WorldView intelligence, and Expert Services map directly to all five controls.

FortiBleed: FortiGate Firewalls Compromised

Credential-harvesting campaign · Threat group TAT26-50 · Reported June 2026
ICS Kill Chain Stage 1: Initial Intrusion

WHAT ACTUALLY HAPPENED

This is credential aggregation, not a new Fortinet software vulnerability. Operators harvested administrator credentials from exposed FortiGate configuration files through password reuse, brute force, and offline cracking of legacy SHA-256 hashes on devices not migrated to PBKDF2.

A rented, GPU-backed cracking pipeline validated credentials at scale, then packaged working access into a revenue-sorted catalog for sale.

On compromised devices, operators planted their own admin accounts disguised as Fortinet services, so rotating the original password does not evict them.

No CVE

No software exploit required. Access came from weak credential hygiene, missing MFA, and legacy password hashing.

Low hundreds

Confirmed domain compromises, against a 75,000+ device headline. Treat appearance in the data set as a trigger to investigate, not proof of breach.

Resold

Validated access is being monetized on criminal forums, placing the same footholds with multiple unknown buyers.

WHY IT MATTERS TO OT

The firewall is both boundary and key

In many OT environments, FortiGate is the enforcement point for IT/OT segmentation.

Validated admin credentials collapse that boundary with no exploit needed: an adversary can alter or disable firewall rules to open routes into SCADA and HMI networks, suppress logging to delay detection, and read the configuration to map VPN paths and access policies.

Where harvested Active Directory service accounts span the IT/OT divide (historians, jump hosts, engineering workstations, vendor remote access), the same access reaches the systems used to observe and command physical processes.

Dragos assesses with high confidence this access can collapse a primary security boundary and shorten the path to control systems without further exploitation.

THE DURABLE RISK: RESALE

The operators are financially motivated, but the access they validated is circulating on criminal markets, sold as bulk FortiGate access sorted by victim revenue.

A single exposed device can therefore draw repeated intrusion attempts from unrelated buyers, whose objectives are unknown and may include OT intent.

Planted admin accounts (forticloud-sync, support_fortinet, fgtssecure, and similar) survive a password reset. Their presence means compromise, not just exposure.

RECOMMENDED ACTIONS

Treat exposure as an incident, not hardening

If your FortiGate devices or domains appear in this data set, act on the assumption access may already exist or have changed hands.

1

Close exposure and reset access

Remove FortiGate management and SSL VPN interfaces from direct internet exposure. Reset all administrator and VPN credentials, terminate active sessions, and enforce MFA on every administrative and remote-access account.

2

Evict persistence, don't just rotate

Inventory admin accounts and remove any disguised as Fortinet services. Revoke and reissue admin SSH keys. Upgrade FortiOS to PBKDF2 hashing, rotate credentials stored in device configs, and patch the FortiCloud SSO chain (CVE-2025-59718/59719, CVE-2026-24858) and CVE-2024-55591.

3

Investigate Active Directory

Treat unfamiliar admin logins as compromise. Run AD forensics and hunt for anomalous LDAP enumeration, AS-REP roasting and Kerberoasting, and Kerberos or SMB password spraying against domain controllers.

Dragos coverage: Platform detections ship for FortiGate/SSL VPN exploitation, Kerberos brute force, AD enumeration, Impacket lateral movement, and external ICS traffic.

PAN-OS GlobalProtect Authentication Bypass

CVE-2026-0257 · Active exploitation since May 2026 · MITRE T1190 · ICS Kill Chain Stage 1: Initial Intrusion

HOW THE BYPASS WORKS

The same TLS certificate that protects the GlobalProtect HTTPS service is reused to encrypt authentication override cookies, and PAN-OS never verifies the cookie signature.

An attacker extracts the public key from the public certificate, forges a valid cookie for any user, and opens a fully authenticated VPN session with no credentials.

A public proof-of-concept lowered the barrier further. Dragos assesses with moderate confidence the activity is opportunistic, scanning for exposed portals rather than targeting any one sector.

KEV

Added to CISA's Known Exploited Vulnerabilities catalog on 29 May 2026; federal remediation mandated.

6 sectors

Finance, manufacturing, education, electric, engineering, healthcare — concentrated in the U.S.

3 conditions

GlobalProtect enabled, authentication override cookies on (non-default), and a reused or exposed certificate.

WHY IT MATTERS TO OT

A trusted foothold on the path to OT

VPN access places an adversary at a network location many environments still implicitly trust.

From there, unauthorized access lets adversaries harvest credentials, gather information to move laterally, and pivot deeper into corporate networks, including pathways into OT demilitarized zones (DMZs).

That makes it a highly sought-after initial access point for ransomware affiliates and state-sponsored adversaries alike.

Post-compromise activity so far is limited: only a subset of intrusions reached full VPN sessions, with Impacket and NTLM relay used for early SMB setup and light reconnaissance.

STRONGEST DETECTION SIGNAL

kali device name +

login from an unexpected
hosting/VPS ASN +

authenticated as **admin**

- Hunt for cookie-based authentication originating outside your expected users.
- Do not rely on IP block lists alone. Source infrastructure spans many ASNs and VPS providers, so address lists miss activity.
- Other observed host names: WINDOWS-LAPTOP-001, DESKTOP-GP01, GP-CLIENT.

RECOMMENDED ACTIONS

What to direct your teams to do

*Aligns to Control 4, Secure Remote Access, of the Five ICS Cybersecurity Critical Controls.
Assess posture against all five.*

1

Patch, then close the door

Upgrade to Palo Alto's fixed PAN-OS version. As an interim measure, use a dedicated certificate for authentication override cookies (never the portal or gateway certificate), or disable Authentication Override entirely.

2

Harden remote access

Enforce MFA on all privileged GlobalProtect accounts, and disable or rename default "admin" accounts. Restrict gateway exposure and GlobalProtect access to trusted IP ranges.

3

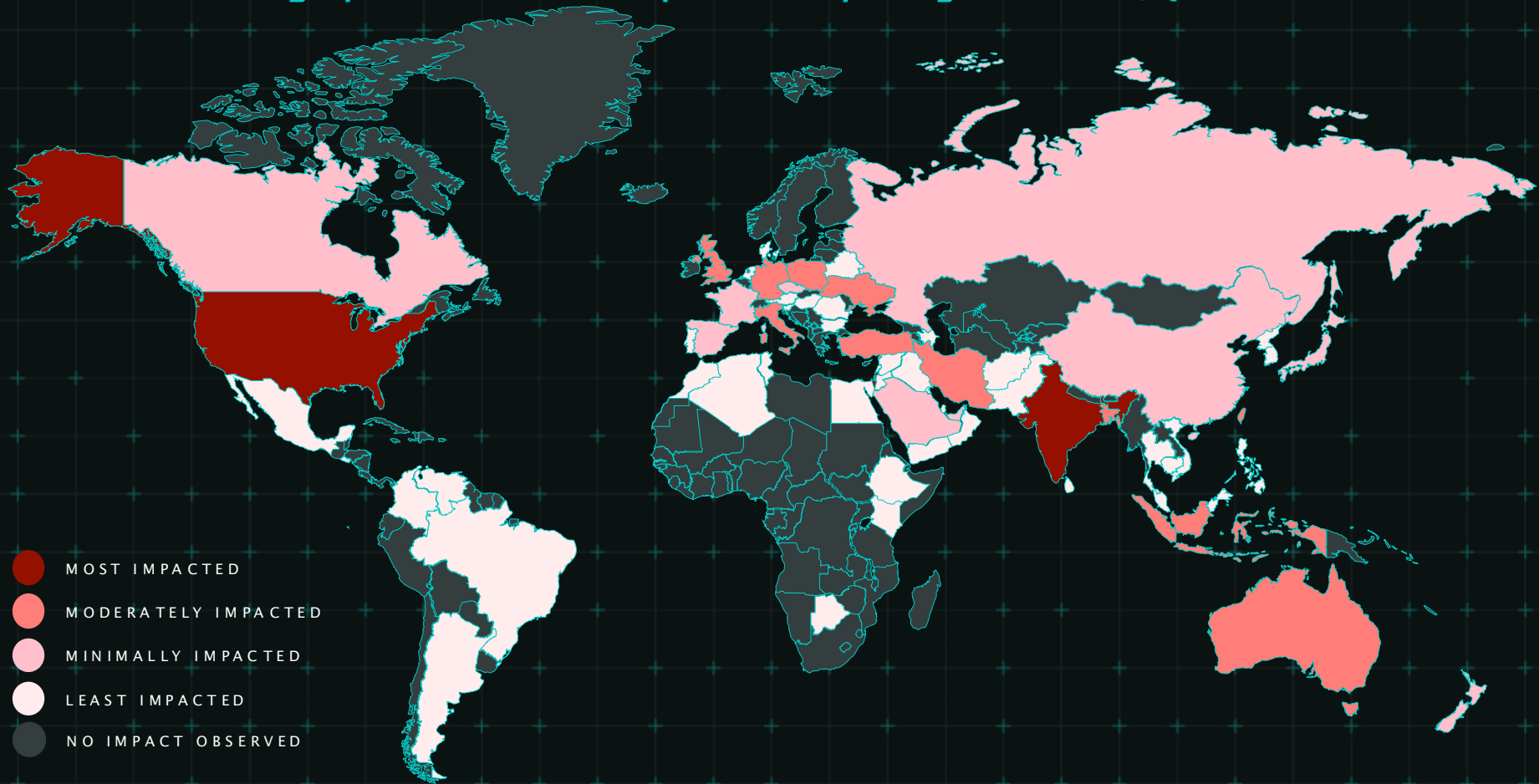
Hunt and treat as compromised

Hunt for the suspicious login signals in this report. Treat any device showing an unfamiliar successful administrative login as compromised, and audit for unauthorized accounts and altered security controls.

Dragos coverage: Platform detections ship for PAN-OS exploitation, NTLM relay, and Impacket lateral movement tied to this activity.

Geographic Impacts

Geographic Areas with Reported ICS/OT Cyber Events, Q2 2026

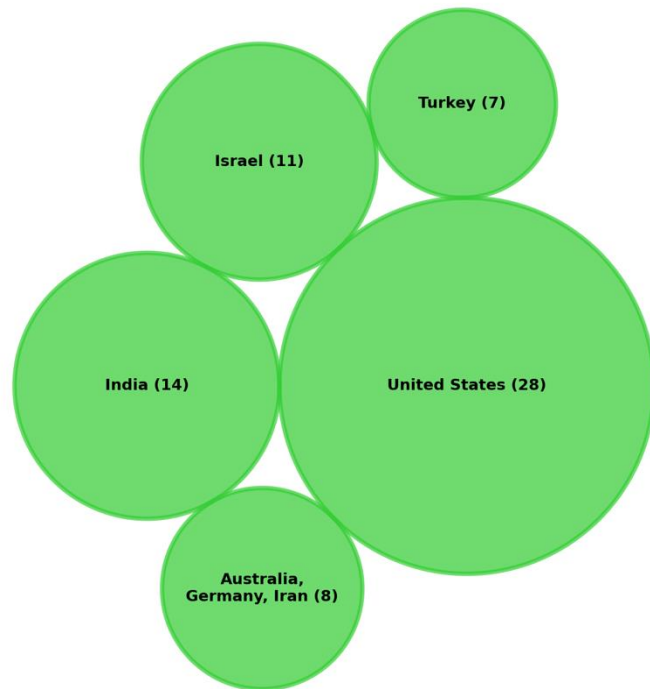


Top Geographic Regions & Countries Q2, 2026

Most Observed Regions in Dragos Reporting - Q2 2026

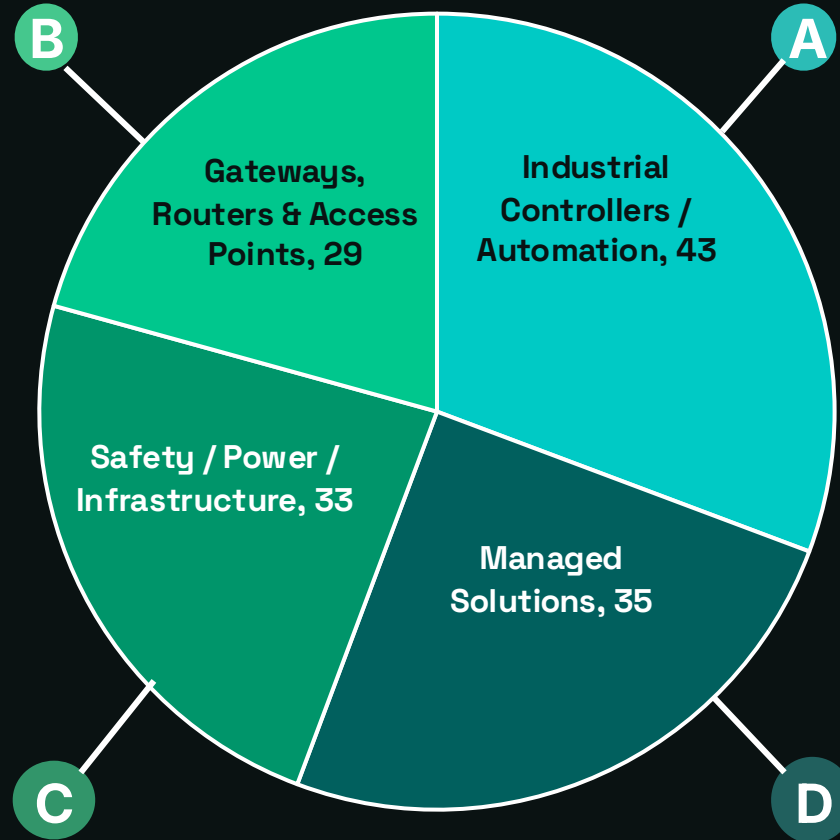


Most Observed Countries in Dragos Reporting - Q2 2026



Impacted Sectors & ICS/OT Vendors

Impacted ICS/OT Vendors: Q2 2026



**Categorical Breakdown
of Exploited or
Impacted Industrial
Vendor Solutions.**

Impacted ICS/OT Vendors: Q2, 2026

A Industrial controllers and automation platforms represented the largest advisory category this quarter, accounting for 43 advisories, or 30.7% of the total. Vulnerabilities affected PLCs, SCADA and HMI systems, automation runtimes, engineering workstations, industrial PCs, and robotic control platforms from vendors including Siemens, ABB and B&R, Rockwell Automation, Schneider Electric, JUMO, and Yokogawa. The breadth of affected technologies highlights persistent exposure in systems that directly support physical processes, production continuity, and operational safety.

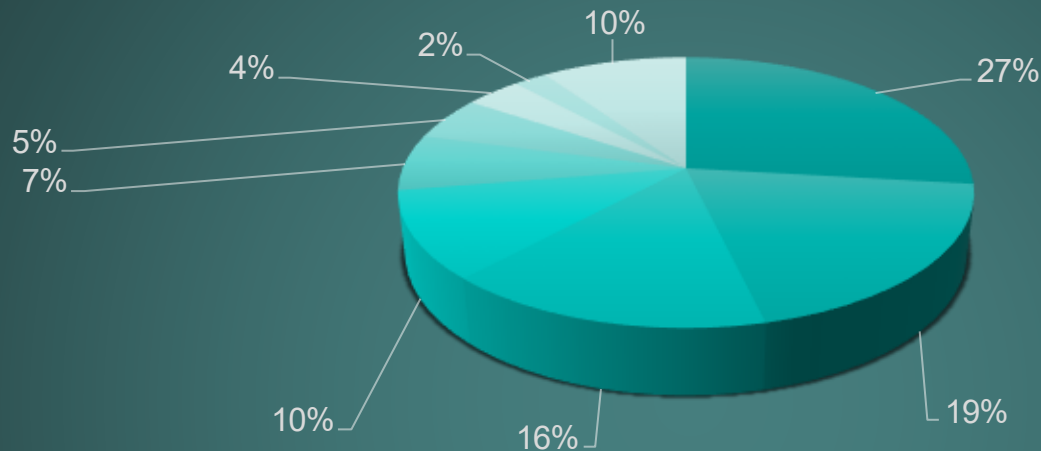
B Gateways, routers, access points, and other OT networking devices accounted for 29 advisories, or 20.7% of the quarter's total. Affected products included industrial routers, managed switches, serial device servers, wireless gateways, SD-WAN infrastructure, and remote-access platforms from vendors such as Siemens, Moxa, Cisco, Fortinet, Ubiquiti, Schneider Electric, and Digi International. Their position at the boundary between enterprise and operational networks makes weaknesses in these devices especially significant, as exploitation could enable unauthorized access, traffic interception, lateral movement, or persistent access to industrial environments.

Impacted ICS/OT Vendors: Q2, 2026

C **Safety, power, and infrastructure technologies** accounted for **33 advisories, or 23.6%** of the quarter's total. Affected products included protective relays, power-management systems, EV charging platforms, inverters, building controllers, camera systems, and other critical infrastructure technologies from vendors such as Siemens, Schneider Electric, ABB, Hitachi Energy, Phoenix Contact, and KACO. Vulnerabilities in these systems carry **outsized operational risk** because exploitation could disrupt electrical distribution, energy management, physical security, and site operations, potentially leading to prolonged outages, degraded safety controls, and broader business interruption.

D **Managed solutions** represented the second-largest advisory category this quarter, accounting for **35 advisories, or 25%** of the total. Affected technologies included centralized management portals, remote-access services, network and security management platforms, engineering and design applications, industrial monitoring tools, and data-management systems from vendors such as Cisco, Fortinet, Nozomi Networks, Siemens, Rockwell Automation, ABB, and Ubiquiti. Because these platforms often administer multiple devices, sites, or operational workflows, a single compromise can provide broad visibility, privileged access, and a pathway to downstream industrial environments.

Q2 2026 Impacted Sectors



■ Energy & Utilities

■ Water and Wastewater Systems

■ Critical Manufacturing

■ Transportation Systems

■ Communications

■ Food and Agriculture

■ Government Facilities

■ Defense Industrial Base

■ Other

Q2 Impacted Sectors

Top 3 Targeted Sectors in Q2 2026:

1. Energy & Utilities

2. Water and Wastewater

3. Critical Manufacturing

Q2 2026 threat activity remained heavily concentrated in operationally critical sectors. Energy and Utilities, Water and Wastewater Systems, Critical Manufacturing, and Transportation Systems accounted for 97 of 137 normalized sector assignments, or approximately 71% of the total.

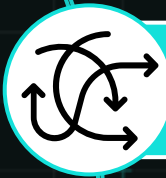
This distribution reinforces that reported activity continued to center on environments where cyber incidents could disrupt physical operations, essential services, and industrial processes.

What “Impact” Looks Like for These Sectors



Loss of Availability

- Service disruption, shutdowns, and denial-of-service conditions affecting OT-dependent operations
- Most frequently observed across energy, water, and transportation infrastructure



Loss of Control

- Unauthorized manipulation of industrial processes, PLCs, and control logic
- Includes parameter changes, controller task modification, and program downloads



Loss of Visibility

- Degraded or deceptive operator insight through HMI suppression, spoofed data, or telemetry loss
- Increases risk of unsafe or delayed operational decisions



Safety & Operational Risk

- Potential downstream impact to people, equipment, environment, and essential public services
- Especially acute in energy generation, water treatment, and transportation sectors

Impacts are directly tied to physical process outcomes, not just IT system downtime

Adversary activity reflects intent to influence or degrade operations, not opportunistic access alone

Ransomware, destructive activity, and OT intrusion increasingly overlap, reinforcing consequence-driven campaigns

Notable Trends Targeting Sub-Sectors & Systems



Agricultural systems such as **Microclimate Controllers** in the **Turkey** and **Fertigation Systems** in **Portugal** were targeted by hacktivist personas. Additionally, adversaries used **ransomware** to halt production of agricultural processing facilities such as a **sugar producer** in **Australia** and suspended production at a **U.S. dairy producer** (See [AA-2026-44](#), [AA-2026-46](#), [AA-2026-51](#) and [AA-2026-59](#))



Industrial refrigeration systems such as a Spanish/Catalan-language refrigeration HMI were targeted by hacktivists in **Spain**, and a refrigeration screw-compressor control system and industrial refrigeration/freezing plant were targeted in **Argentina** (See [AA-2026-43](#) and [TR-2026-45](#))



Rail transportation systems and networks such the Los Angeles Metro and the South Florida Regional Transportation Authority were targeted by hacktivists in the **United States** (See [AA-2026-40](#) and [TR-2026-24](#))



Adversaries targeted **flood reduction systems** in Italy used to **protect Venice from flood waters**, claiming unauthorized access to a flood risk reduction control system associated with Italy's Ministry of Infrastructure and Transport. (See [AA-2026-36](#))



A multi-adversary campaign targeted **Automatic Tank Gauge Systems (ATG)** in internet-exposed ATG systems across the United States fuel retail sector and other critical infrastructure (See [AA-2026-58](#))



Hacktivists targeted **nuclear-related water and power systems** in **Bangladesh** and **Indonesia**. TAT25-47 claimed unauthorized access to ICS linked to the Bangladesh Atomic Energy Commission, while TAT26-39 claimed a sabotage attack against Indonesia's National Research and Innovation Agency. (See [AA-2026-49](#) and [AA-2026-57](#))

Bigger Trends

Smaller Outliers

Impacted ICS/OT Sectors & Vendors

Why Track Impacted Sectors & Vendors?

- Adversaries seek methods to exploit or **undermine legitimate products** and services.
- Underscores that industrial organizations must **collaborate with vendors** to assess and address threat and risk challenges.
- Understanding which ICS/OT sectors are being attacked can improve relative security posture through **more informed and efficient prioritization**.
- Organizations are encouraged to **leverage these observations to influence** respective security strategies, policies, and priority intelligence requirements.



MITRE ATT&CK and ICS Cyber Kill Chain Metrics

MITRE ATT&CK for ICS Observed in Q2 2026

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	RECONNAISSANCE	EXFILTRATION	ICS IMPACT
External Remote Services	Execution through API	Valid Accounts	Exploitation for Privilege Escalation	Masquerading	Remote System Information Discovery	Valid Accounts	Monitor Process State	Standard Application Layer Protocol			Manipulation of Control
Exploit Public-Facing Application	Graphical User Interface	Modify Program			Network Connection Enumeration	Program Download	Data from Information Repositories	Connection Proxy			Loss of Availability
Internet Accessible Device	Modify Controller Tasking				Network Sniffing	Lateral Tool Transfer	Screen Capture				Damage to Property
Replication Through Removable Media	Native API				Wireless Sniffing		Point & Tag Identification				Denial of Control
Rogue Master	User Execution						Adversary-in-the-Middle				Loss of Control
Supply Chain Compromise							Automated Collection				Theft of Operational Information
Wireless Compromise							I/O Image				Loss of View
							Program Upload				Manipulation of View
											Loss of Safety

Least Observed → Most Observed

Ransomware Observations & Trends

Key Findings

1,140 Industrial organizations were found on ransomware Data Leak Sites (DLS).

65% Of the Q2 ransomware claims were against the Manufacturing sector.

45% Of all claims/incidents impacted organizations in North America.

Active Groups

Qilin, Akira, and The Gentlemen were responsible for the largest victim volumes in Q2.



Most impacted industries worldwide:

- Manufacturing
- ICS Firms/Integrators/Manufacturers
- Transportation



Trends and Observations

Q2 2026

- **Concentrated Activity:**

- Similar to previous quarters, a small number of ransomware groups accounted for a disproportionate share of activity, with Qilin, Akira, and The Gentlemen responsible for the largest victim volumes in Q2

- **Top Initial Access Methods:**

- Exploitation of vulnerabilities in VPN appliances/edge devices
- Compromised credentials
- Social engineering via helpdesk impersonation and vishing using Microsoft Teams

- **Data Theft:**

- Ransomware has shifted from encryption-only attacks to data theft-led extortion in which some affiliates prioritize data theft during intrusions over using file-encrypting ransomware

Ransomware by ICS Sector

Q1 vs Q2 2026



Manufacturing consistently ranks as the top industrial sector worldwide impacted by ransomware, accounting for 65% of all observed industrial victims in Q2.

While ransomware numbers in the **energy and utilities** sectors are much lower, they continue to rise in recent years, driven by geopolitical tensions and the increased profit-sharing offered by the numerous active **Ransomware-as-a-Service** operations.

Ransomware by Region

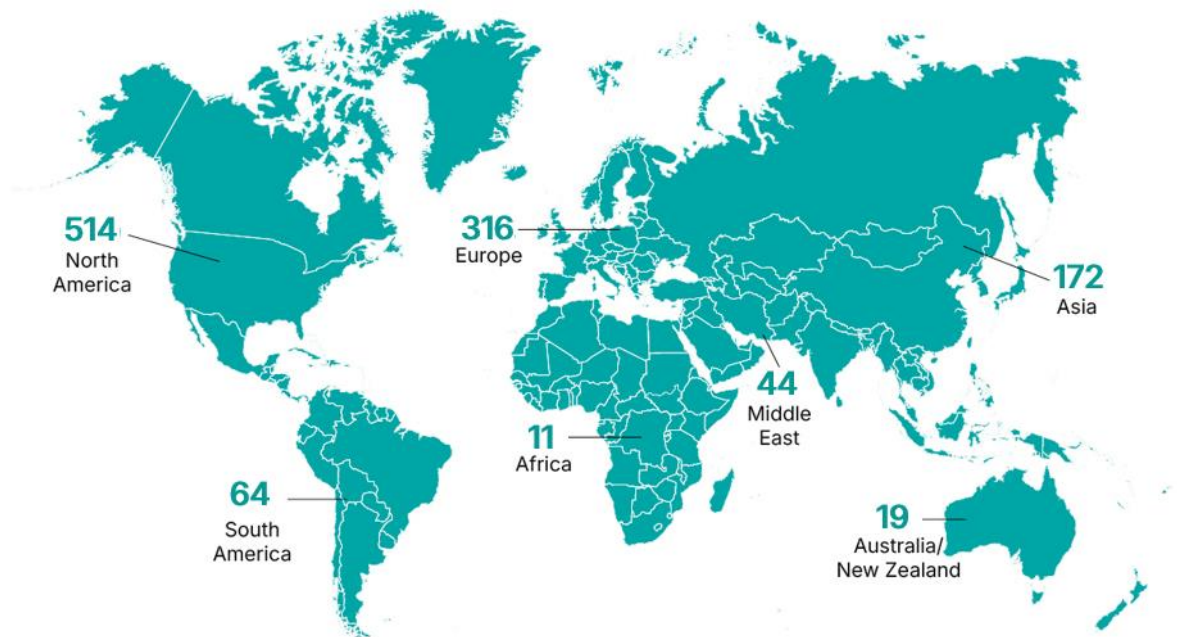
Q2 2026

Dragos observed **1,140** industrial organizations on ransomware leak sites worldwide (an 11% increase from Q1).

The **United States** consistently ranks as the country most affected by ransomware, with U.S.-based industrial organizations accounting for **38%** (431) of all observed industrial victims in Q2.

As in previous quarters, **Europe** ranks second among the most impacted regions. The country with the greatest overall increase from Q1 (37 incidents) to Q2 (68 incidents) was Germany. Primarily impacting the **manufacturing** sector.

Ransomware Incidents by Region Q2 2026



Hacktivism Observations Q2 2026



Geographic Scope

46 unique countries were targeted in Q2 2026. The most targeted countries were **Ukraine** (35), **United States** (26), **Spain** (18), **Austria** (17), **France** (17), **Italy** (16), and **Russia** (15)



Hacktivist Groups

Dragos observed the claims of **41 unique hacktivist personas** in Q2 2026. The top five most active threat actors by volume of claims were: 1. TAT25-47 (Infrastructure Destruction Squad) (70), 2. TAT24-96 (NoName05716) (60), 3. TAT25-106 (NullSecHackers) (25), 4. TAT24-56 (Z_PENTEST) (24), 5. itarmyofukraine2022 (17)



Impacted Scores

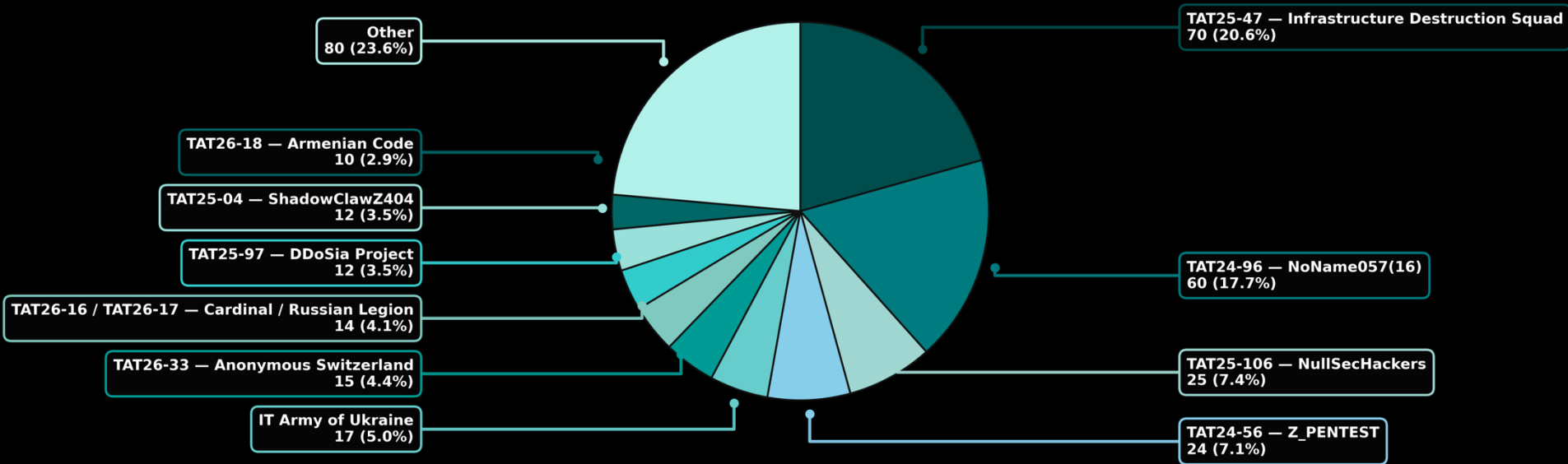
Government, Energy , and Manufacturing were the most targeted sectors in claims made by hacktivists in Q2 2026. Targeting patterns continued to emphasize operational disruption, public impact, and symbolic value.

Hacktivism Trends Q2 2026

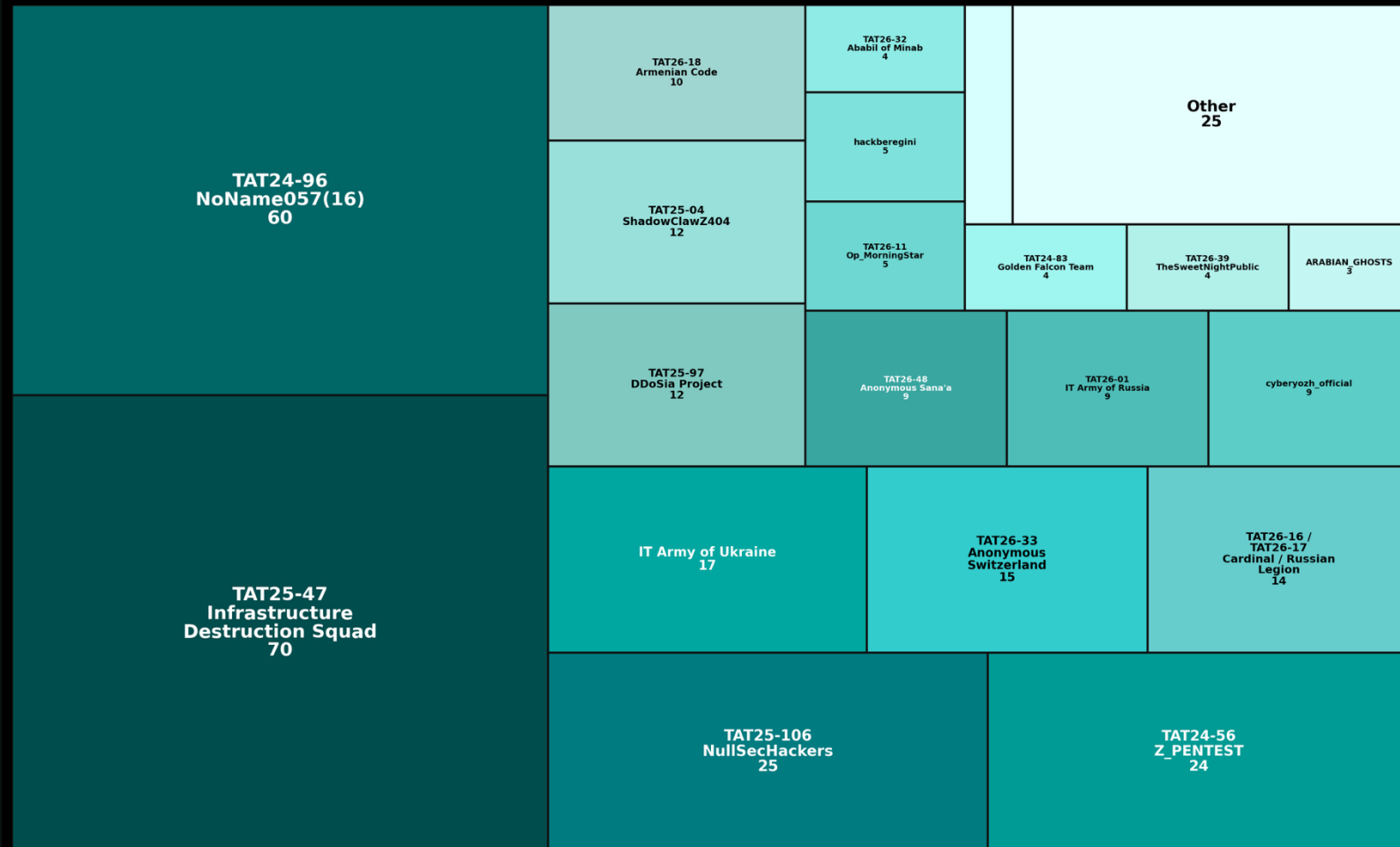
Consistent Targeting of OT & ICS

- In Q2 2026, out of the total 339 hacktivist claims examined by Dragos, 111 claims directly targeted ICS or OT systems.
- Meaning Dragos saw approximately **32.74%** of **hacktivist claims targeting OT & ICS** in Q2 2026.
- In **May**, 35 claims targeted ICS/OT, representing **19.6%** of total claims observed in May 2026.
- In **June**, 45 claims targeted ICS/OT, representing **41.3%** of total claims observed in June 2026.
- In **July**, 31 claims targeted ICS/OT, representing **60.78%** of total claims observed in July 2026.

Top 10 Hacktivist Personas– Q2 2026

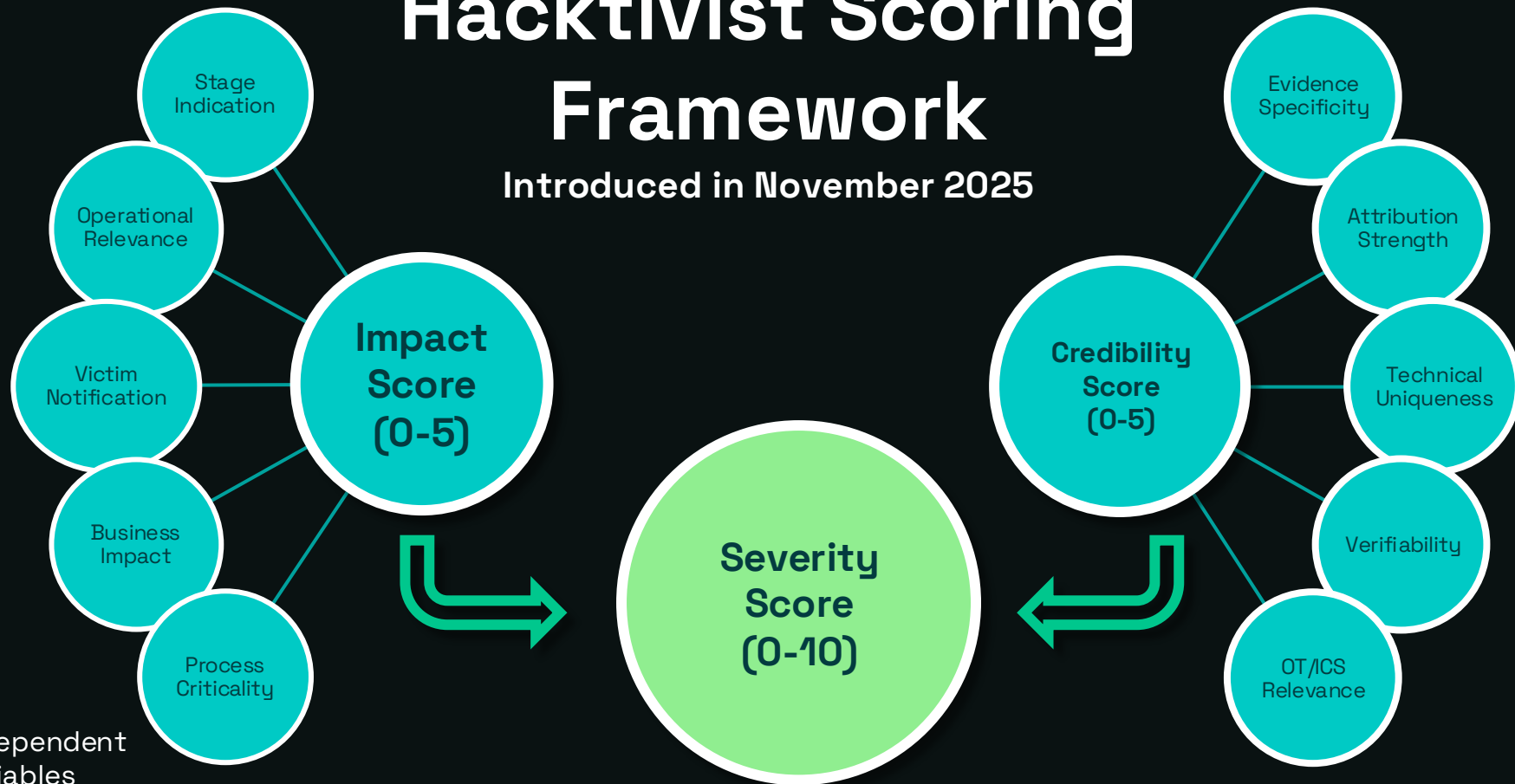


Hacktivist Personas, Observed Claims — Q2 2026



Hacktivist Scoring Framework

Introduced in November 2025

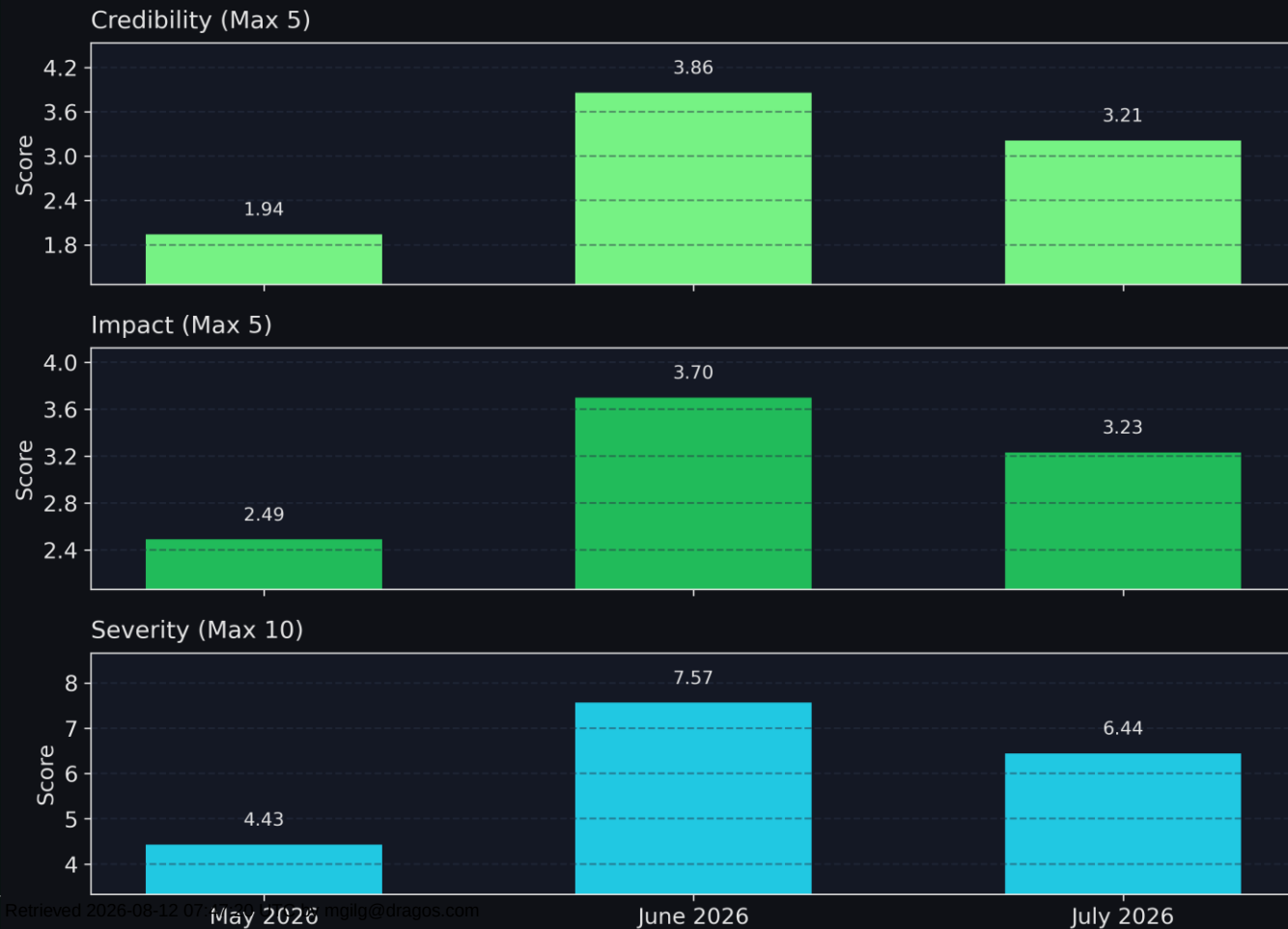


Independent
Variables

**Credibility, Impact,
and Severity Score
of Hactivist
Claims: Change
Month Over Month**

Q2 2026

Hactivist Scoring by Month - Q2 2026



Delta of Hacktivist Scoring by Month - Q2 2026



**Credibility, Impact,
and Severity Score
of Hacktivist
Claims: Delta
Month Over Month**

Q2 2026

Vulnerability Advisories

Vulnerability Advisories

Dragos identified 3 high severity/high impact vulnerabilities that could be used to gain initial access to industrial networks:

Siemens SINEC INS Weak Password Hashing

CVSS Score: 9.8 (Critical)
CVE-2026-46749

- CVE-2025-43873 is a high-severity OS command injection vulnerability (CWE-78) affecting Siemens SINEC INS versions earlier than V1.0 SP2 Update 6. SINEC INS uses a static, hardcoded password salt shared among users and installations, together with an insufficient number of hashing iterations. An adversary who obtains password hashes could perform more efficient brute-force or precomputed attacks, potentially recovering credentials and gaining unauthorized access.
- See Dragos Worldview Week 26 [WWV-2026-26](#).

Fortinet FortiCloud SSO Authentication Bypass

CVSS Score: 9.8 (Critical)
CVE-2026-24858

- CVE-2026-24858 is an actively exploited authentication-bypass vulnerability affecting several Fortinet products. When FortiCloud single sign-on is enabled, an adversary who controls a FortiCloud account and has a device registered to that account may authenticate to vulnerable Fortinet devices belonging to other customers, without possessing credentials for the targeted device.
- See [AA-2026-52](#): FortiBleed: 75,000+ Fortinet Firewalls Compromised via Credential-Harvesting Campaign

BlueKeep - Microsoft Remote Desktop Service

CVSS Score: 9.8 (Critical)
CVE-2019-0708

- CVE-2019-0708, known as BlueKeep, is a critical remote code execution vulnerability in Microsoft Remote Desktop Services on older Windows systems. It can be exploited without authentication or user interaction and is considered wormable, meaning it could spread automatically between vulnerable devices. Organizations should patch affected systems, restrict RDP exposure, and retire unsupported Windows versions.
- See [TR-2026-33](#): Introducing TREMOLITE, a Threat Group Compromising Indian Critical Infrastructure

Call to Action

Call to Action

ICS/OT Asset Owners & Operators are encouraged to consider the following:

- Asset owners should join industry or regional threat-sharing groups and monitor sector- and country-specific threats. This helps improve response plans, enhance threat hunting, and proactively address vendor or technology-specific vulnerabilities before adversaries exploit them.
- Asset owners should use MITRE ATT&CK and the ICS Cyber Kill Chain to strengthen threat hunting, detection, and training by focusing on realistic attack paths and refining threat models.
- Ransomware remains a major global threat to industrial orgs, often entering via IT networks—making network segmentation and hardening essential defenses.
- Since legacy systems can not always be removed, asset owners should apply compensating controls like segmentation and firewalls, while improving third-party software policies and security awareness training.
- As always, Dragos encourages all ICS/OT asset owners and operators to implement the 5CCs:
<https://www.dragos.com/resources/infographic/5-critical-controls-for-world-class-ot-cybersecurity-infographic/>

Thank you

Dragos is an industrial (OT/ICS/xOT) cybersecurity company on a mission to safeguard civilization.

Dragos is private and headquartered in the Washington, D.C. area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Proprietary Statement

This material constitutes proprietary and trade secret information and shall not be disclosed to any third party, nor used by the recipient except under the terms and conditions prescribed by Dragos, Inc.

Copyright Statement

Copyright © 2026 Dragos, Inc. All Rights Reserved

Dragos Global Headquarters

1745 Dorsey Rd

Suite R

Hanover, Maryland 21076

(855)-372-4670

www.dragos.com

Customer Support Requests

<https://portal.dragos.com/#/>