RiverForgeCyber.com

RiverForge Cyber Global Threat Report

Including Energy Sector Focus, Threat Actor Profiles, MITRE ATT&CK & ICS-CERT Mapping

Prepared by Kumar Rachuri, Founder of RiverForge Cyber
Kumar.Rachuri@RiverForgeCyber.com

Date: June 8, 2025

Table of Contents

RiverForge Cyber Global Threat Report

RiverForge Cyber is Proud to present this **Global Threat Report** tailored for **Operational Technology and Networked Information Technology (OTNIT)** threats, with an intel-rich layout that mimics a cybersecurity "league table."We Also focus in on critical vulnerabilities, threat actor activity, and mapped TTPs from MITRE and ICS-CERT specific to the **energy sector**, one of the top targets for nation-state and ransomware operators.

---

1. Threat Overview & Scorecard (OTN/IT)

Threat Actor / Group	Origin Country	Threat Score (1–10)
Lazarus Group (North Korea)	North Korea	9.2
Evil Corp / Treasury-aligned gangs	Russia	8.7
DarkSide / BlackCat ransomware	Russia/Eastern Europe	8.1
Syrian Electronic Army (SEA)	Syria (+ possible Iran)	6.8
Islamic State Hacking Division (ISHD)	Middle East (mainly Syria, Iraq)	6.3
Anonymous Sudan	Sudan / unclear	5.7

Threat Score is based on: **capability**, **frequency**, **target criticality**, and **state ties**.

---

2. Major Cyber Gangs & Terrorist Actors

• Lazarus Group

- **Country**: North Korea
- **Capabilities**: APT with zero-days, spear-phishing, crypto-heists (e.g., Bangladesh Bank), espionage (Sony, WannaCry). (en.wikipedia.org, thesun.co.uk, en.wikipedia.org, en.wikipedia.org, en.wikipedia.org)
- **ICS-CERT / MITRE (Enterprise & ICS)**:

    - T1193 Spearphishing Attachment
    - T1486 Data Encrypted for Impact (ransomware worm)
    - ICS-WIN-EBS PLC WinCC attacks (mapped to ATT&CK for ICS) (nozominetworks.com, dragos.com)

• Evil Corp

- **Country**: Russia
- **Capabilities**: Dridex/Zeus malware, financial extortion via RaaS and direct escort; ties to FSB shielding their ops. (thesun.co.uk)
- **MITRE ATT&CK**:
    - T1059 – Command and Scripting
    - T1566 – Spearphishing
    - T1486 – Data Encrypted for Impact

• DarkSide / BlackCat

- **Region**: Russia/Eastern Europe
- **Capabilities**: Colonial Pipeline-style large-scale, RaaS attacks on critical infra. (dragos.com, en.wikipedia.org, en.wikipedia.org)
- **MITRE / ICS-CERT**:
    - T1486 (ransomware), T1490 (Impact), T1059
    - Platform-level ICS alert AA21-131A from CISA/FBI (industrialcyber.co, en.wikipedia.org)

• Syrian Electronic Army (SEA)

- **Country**: Syria (with possible Iran support)
- **Capabilities**: Propaganda-driven defacements, spear-phishing; attacks on media, Western governments. (en.wikipedia.org)
- **MITRE**:
    - T1499 – Endpoint Denial of Service
    - T1192 – Spearphishing via Service

• Islamic State Hacking Division (ISHD)

- **Region**: ISIS strongholds (Syria, Iraq)
- **Capabilities**: Low-sophistication defacements, DDoS, doxing, some ransomware; possibly cover for APT28 operations.
- **MITRE**:
    - T1498 – Network Denial of Service
    - T1565 – Data Manipulation

• Anonymous Sudan

- **Country**: Sudan (accusations of Russian links)

- **Capabilities**: 35,000+ DDoS attacks targeting hospitals, government, LGBT sites. (en.wikipedia.org)
- **MITRE**:
  - T1499 – Endpoint Denial of Service
  - T1566 – Phishing or extortion-based coercion

---

3. 🛡 ICS-CERT Bulletins & MITRE ICS Alignments

- **DarkSide/BlackCat**:
  - *Alert AA21-131A*: Guidance on post-ransomware recovery for ICS. (en.wikipedia.org, icct.nl)
- **MITRE ATT&CK for ICS**:
  - Bulk use for mapping all above actors to industrial tactics (e.g., PLC manipulation, firmware tampering). (dragos.com)

---

4. 🔍 Intel Briefing

- **Trend 1**: Increasing **state/CRIMINAL hybridization**, especially with Russia, Iran, North Korea using criminal groups as proxy forces. (wsj.com)
- **Trend 2**: **Hacktivism rebounds**, driven by geopolitical conflicts (Russia-Ukraine, Israel-Hamas), with groups like Holy League and Moroccan Black Cyber Army emerging. (lemonde.fr)
- **Trend 3**: Heightened threats on **critical infrastructure** (energy, pipelines, healthcare). Ransomware groups specifically target ICS environments.

---

5. 🧠 Threat Actor Profiles

1. **Lazarus Group** – Highly advanced North Korean APT; financial heists + global espionage; dubbed TTP-rich suite (EternalBlue, SWIFT thefts).
2. **Evil Corp** – FSB-protected RaaS operators; large-scale financial extortion via malware distributions and connections with state.
3. **DarkSide / BlackCat** – Profit-driven ransomware-as-a-service; focus on U.S. pipelines; moderate sophistication in ICS targeting.
4. **Syrian Electronic Army** – Government-affiliated hacktivists engaging in propaganda and defacements.
5. **ISHD (UCC)** – Ideologically driven doxing and defacement; possibly a front for state APT's influence.

6. **Anonymous Sudan** – Hacktivist-for-hire DDoS network; focused on socio-political targets globally.

---

6. US Top 5 Nation-State Threat Actors Against the U.S.

1. **North Korea** – Lazarus Group, Bureau 121 (9.2)
2. **Russia** – Evil Corp, DarkSide, numerous APTs (8.8 combined)
3. **China** – Though not detailed above, continues to run espionage operations (estimated 8.5)
4. **Iran** – ASPs, state-linked hacktivists operating via SEA-like proxies (7.6)
5. **North Korea**, Russia, China, and Iran are repeatedly noted in U.S. Intel as the most active cyber threats. (en.wikipedia.org, thesun.co.uk, en.wikipedia.org, en.wikipedia.org, en.wikipedia.org, en.wikipedia.org)

---

7. 📊 MITRE ATT&CK & ICS Mapping Highlights

- **Enterprise**: Spear-phishing, ransomware deployment, credential theft (T1078), lateral movement (T1570), encryption (T1486).
- **ICS**:
  - **Network Denial** (T1499) – used by SEA, Anonymous Sudan
  - **Unsafe input injection** to PLCs – documented in ICS-CERT alerts
  - Firmware tampering & remote access (Mimikatz, backdoors) – utilized by Lazarus & Evil Corp (en.wikipedia.org)

---

8. ⚡ Sector Focus: ENERGY INFRASTRUCTURE

🔍 Why Energy?

The energy sector is an apex target because:

- It is **mission-critical** (fuel, grid, nuclear).
- It uses **OT/ICS environments** often running legacy systems with poor segmentation.
- Attacks have **geopolitical leverage** (e.g., pipeline shutdowns, oil supply disruption).
- Many providers are **private entities** lacking comprehensive cyber resilience programs.

🧨 Notable Attacks on Energy Sector

Attack	Threat Actor	Country	Method	Impact
Colonial Pipeline (2021)	DarkSide	Russia	Ransomware via VPN creds	Pipeline shutdown; $4.4M ransom
Ukraine Grid Attack (2015 & 2016)	Sandworm	Russia	Custom malware on ICS	Power outage to 230,000+
Saudi Aramco Shamoon (2012, 2017)	APT33 (linked)	Iran	Disk wiper	35,000 machines destroyed
Dragonfly / Energetic Bear Campaign	Dragonfly	Russia	Spearphishing, watering hole	ICS visibility, staging attacks
Triton/Trisis (2017)	Xenotime	Possibly Russia/Iran	Safety controller exploit	Targeted fail-safe systems at petrochemical plant

---

🛠️ MITRE ATT&CK for ICS Mapping – Energy-Specific TTPs

Tactic	Technique	Description	Actor Examples
Initial Access	T0861 – Exploit Public-Facing Application	Gained access via exposed HMI/VPN	DarkSide, Xenotime
Execution	T0803 – Command-Line Interface	Used for script-based lateral movement	Sandworm
Persistence	T0847 – Valid Accounts	Use of stolen domain creds or hardcoded ICS creds	Dragonfly, Lazarus
Impair Process Control	T0810 – Manipulation of Control	Altering PID loops, pressure, temp	Triton, Energetic Bear

Tactic	Technique	Description	Actor Examples
Impact	T0806 – Denial of Control	Disabled user HMI control interfaces	Ukraine Grid attack

📌 **Source**: MITRE ATT&CK for ICS Framework (attack.mitre.org)

Relevant ICS-CERT & CISA Bulletins

- **ICS-ALERT-21-131-01**: DarkSide ransomware incident affecting Colonial Pipeline
- **ICS-ALERT-17-352-01**: Triton malware targeting Triconex SIS (Schneider Electric)
- **ICS-TIP-13-164-01B**: Dragonfly threat group compromises industrial control systems
- **AA20-049A**: Recommended practices for ransomware response in ICS/SCADA systems

These alerts offer Indicators of Compromise (IOCs), recovery playbooks, and system hardening guidance.

Energy Sector Risk Scorecard

Risk Factor	Score (1–10)	Notes
Nation-State Threat Activity	9.5	Russia, Iran, China heavily involved
Ransomware Risk	9.2	Financial + geopolitical motivators
Supply Chain Vulnerability	8.4	Vendors often poorly secured
OT/ICS Security Maturity	6.5	Many orgs lack network segmentation & asset inventory
Regulatory Pressure	7.0	NERC CIP, TSA pipeline directive enforcement varies

Key Takeaways & Recommendations

- **Fortify ICS defense** by mapping risks to MITRE techniques; ensure recovery plans address ransomware.
- **Monitor cybercrime-state nexus** – especially Russian and North Korean affiliates.
- **Cross-border intelligence share** on hacktivist networks behind geopolitical hacking waves.
- **Enhance U.S. inter-agency posture** focusing on nation-state-backed criminal ecosystems.

Recommendations for Energy Operators

1. **Segment OT and IT networks** with strict firewall rules and one-way communication zones.
2. **Deploy anomaly detection platforms** that support industrial protocols (e.g., Modbus, DNP3).
3. **Implement secure remote access** with MFA, logging, and time-bound sessions.
4. **Practice incident response simulations** using realistic OT/ICS threat scenarios.
5. **Patch PLCs and RTUs**, or implement virtual patching if legacy constraints prevent updates.