SHIELDWORKZ

Authoritative Data Insights



OT Cybersecurity Threat Landscape Analysis Report

2026

www.shieldworkz.com

Table of contents

1. Introduction 7

2. RESEARCH METHODOLOGY 8

2.1 double-blind test 9

3. 10 REASONS TO READ AND UNDERSTAND THE DATA IN THIS REPORT 11

4. THE YEAR THAT WAS 12

4.1 Kinetic attacks (Destructive OT attacks) 13
4.2 Safety instrumentation system targeting (SIS-Specific) 13
4.3 Ransomware (Extortion-driven OT attacks) 14
4.4 "Insider or near-insider" attacks 14
4.5 Supply chain and update poisoning attacks 14
4.6 Tool hijack 16
4.7 Tactical and behavioral changes exhibited by hackers 17

5. MAJOR CYBERSECURITY TRENDS OBSERVED IN 2025 18

5.1 The era of coordinated attacks 18
5.2 Supply chain concerns multiply 18
5.3 Ever expanding threat surfaces 18
5.4 Rise in cyber-attacks and probes during the vacation season 18
5.5 Misuse of internet connectivity 18
5.6 Firewall and network configuration challenges 19
5.7 Threat actors tend to target 19
5.8 The payload deployment and execution models 19
5.9 Chinese and North Korean APT 19
5.10 The absence of a structured and rapid incident response 20
5.11 IT-OT convergence is enabling threats to move in both directions. 20
5.12 Lack of network segregation 20
5.13 Commoditization of attacks and the rise in the number of threat actors: 20

6. SECURITY CHALLENGES 21

6.1 Cyberattack trends 21

7. WHAT DO SECURITY LEADERS NEED TO WORRY ABOUT IN 2026? 22

8. GROWTH IN OT-LINKED CYBER EVENTS 25

9.MOST TARGETED CITIES 26

9.1 Types of attacks 26

10 WHICH COUNTRIES ARE BEING TARGETED? 28

11 WHAT ARE THE TARGETS DURING AN OT ATTACK? 28

11.1 Usage category, attacks and security challenges 29
11.2 Percentage of various attacks logged on key targets 31
11.3 Geographical distribution of attacks (percentage of global attacks detected at regional targets) 32
11.4 Why are cyber-attacks growing? 32
11.5 Days taken to place stolen data and credentials for sale across forums 33
11.6 Rising attacks 34
11.7 Which sectors getting attacked and why? 36
11.8 Mapping sectoral attacks to threat actors (types) 36
Legend 37
Key OT threat modelling insights on the data 39

12 DEEP DIVE ON USE OF AI IN CYBERATTACKS BY THREAT ACTORS 40
12.1 Percentage of overall attacks that had a AI signal 40
THE CURRENT STATE - AI AS AN ATTACK ACCELERATOR 41
12.2 Vulnerability discovery and reconnaissance 41
12.3 AI-based reconnaissance: 42
12.4 Social engineering and insider threat amplification 42
12.5 Insider threat modeling: 43
12.6 Malware development and customization 43
12.7 Documented Threat Actor AI Adoption 43
12.7.1 Nation-State Programs 43
12.7.7 Protocol Exploitation and Man-in-the-Middle 45
12.8 Adversarial machine learning against OT defenses 45
13. APT THREAT ACTOR PROFILES 47
13.1 Characteristics of Chinese APT groups 47
TTP DEEP-DIVE 49
INITIAL ACCESS TACTICS 49
13.1.1 Vulnerability Exploitation 49
13.5 Spear phishing Operations 50
13.5.1 Spear phishing Characteristics: 50
13.5.2 Recent TTP Evolution: 50
13.6 Supply Chain Compromises 50
13.6.1 Web Hosting Provider Targeting 51
13.6.2 Strategic Web Compromises (Watering Hole Attacks) 51
13.7. PERSISTENCE MECHANISMS 51
13.7.1 Web Shell Deployment 51
13.7.2 Legitimate Tool Abuse and DLL Sideloading 51
13.7.5 VPN Client Persistence 52
13.7.6 Bootkit and Rootkit Deployment 52
13.7.7 Network Device Modification 52
13.8 Credential Dumping Operations 52
13.8.3 Living Off the Land (LOTL) Techniques 52
13.9 Lateral movement 53
13.9.1 Network Reconnaissance 53
13.9.3 Lateral Movement Techniques 53
13.10 Command and control infrastructure 54
13.10.1 SOHO Router Botnet Infrastructure 54
13.10.3 Custom C2 Protocols 54
13.10.4 Shared Infrastructure Among Groups 54
13.11 MALWARE ARSENALS 54
13.12 Modular Backdoors and RATs 54
13.12.3 Web Shells 55
13.12.4 Rootkits and Kernel-Mode Malware 55
13.12.5 Custom Tool Suites 55
13.12.7 Shared Malware Families 55
13.13 DATA EXFILTRATION AND COLLECTION 56
13.13.1 Encryption and Staging 56
13.13.3 Custom SFTP Clients 56
13.14 DEFENSE EVASION TECHNIQUES 56
13.14.1 Living Off the Land 56

13.14.2 Log Modification and Anti-Forensics 56
13.14.3 Traffic Obfuscation 56
13.14.4 Fileless Execution 56
13.15.1. OPERATIONAL PATTERNS AND TRADECRAFT 56
13.15.1 Working Hours and Operational Tempo 56
13.15.2 Long-Term Persistence 57
13.15.3 Hands-On-Keyboard Activity 57
13.15.4 Adaptability and Resilience 57
13.16 Targeting priorities 57
13.16.1 Critical Infrastructure Focus 57
13.17 Strategic espionage objectives 57
13.17.3 Pre-Positioning for Disruption 58
13.18. Notable TTP variations 58
13.18.1 APT41 (Dual Mission Approach) 58
13.18.2 APT40/Leviathan (Maritime Specialist) 58
13.19 Volt Typhoon (Infrastructure Pre-Positioning) 58
13.19.2 Salt Typhoon (Telecommunications Specialist) 58
13.19.3 Stately Taurus/Mustang Panda (Government Focus) 59
13.20 Strategic assessment 59
13.20.1 Organizational Backing 59
13.20.2 Evolution of Tactics 59
13.20.2.3 Collaborative Ecosystem 59
13.21 Country: Russia 60
13.21.1 APT29 (COZY BEAR) - SVR FOREIGN INTELLIGENCE SERVICE 60
Organizational Affiliation 60
Aliases 60
Primary Objectives 60
Key Characteristics 60
Notable Operations 61
Tactics, Techniques, and Procedures (TTPs) 61
Current Threat Assessment 62
13.21.2 APT28 (FANCY BEAR) - GRU MILITARY INTELLIGENCE 62
Organizational Affiliation 62
Aliases 62
Primary Objectives 62
Key Characteristics 62
Notable Operations 62
Tactics, Techniques, and Procedures (TTPs) 63
Current Operations 63
13.21.3 APT44 / SANDWORM - GRU UNIT 74455 63
Organizational Affiliation 63
Aliases 63
Primary Objectives 63
Key Characteristics 64
Notable Operations 64
Tactics, Techniques, and Procedures (TTPs) 64
Evolution and Current Threat 65
13.21.4 GRU UNIT 29155 - EMERGING CYBER-KINETIC INTEGRATION UNIT 65
Organizational Affiliation 65
Aliases 65

Z-Pentest 68
Sector16 68
13.21.7 RUSSIAN FSB CENTER 16 - NETWORK INFRASTRUCTURE TARGETING 69
Recent Activity (2024-2025) 69
13.21.8 STRATEGIC ASSESSMENT AND FUTURE OUTLOOK 69
Operational Integration 69
Evolving Tactics 69
Threat Trajectory 69
14. MAJOR CYBERATTACKS REPORTED IN 2025 70
SOURCE: PUBLISHED DATA 72
15. STATE OF OT SECURITY 76
15.1 Common ICS/SCADA/PLC ports exposed to the internet 76
15.2 Research intent 77
15.3 Interesting considerations 77
15.4 Blindfold test and validation 78
15.5 Visualizing the methodology 79
15.6 OT Protocol Exposure Snapshot across stages 80
15.7 Country-wide exposure data across top nations with most exposed ports 80
15.9 Recommendations 82
Minimize/eliminate internet-facing OT exposure 82
Implement network segmentation and segregation 82
Harden devices and mitigate insecure protocols 82
Implement continuous network and security monitoring 83
Develop and practice a cyber Incident Response Plan 83
16 DISSECTING MAJOR CYBER INCIDENTS OF 2025 84
16.1 Jaguar Land Rover 84
WHAT WENT WRONG? 84
ROOT CAUSE ANALYSIS 85
ATTACK TIMELINE 85
PROOF OF ACCESS 86
THREAT ACTOR PROFILE 87
TARGETING LARGE BRANDS 88
MODUS OPERANDI 89
16.2 Oltenia Energy Complex 90
16.3 European Space Agency 92
What was stolen? 92
Forensic update: The "codebase" compromise 93
Missions at risk? 93
The "888" Strategy: A data broker's endgame 95
16.4 La Poste France 95
THE WEAPON OF CHOICE 95
THE CULPRIT: NONAME057(16) 96
WHY NOW? THE STRATEGIC TIMING 97
THE BROADER CONTEXT: A "WAVE" OF ATTACKS 97
16.5 Nissan Red Hat 97

THE TIMELINE OF THE ATTACK *98*
THE ANATOMY OF THE NISSAN ATTACK AND ITS AFTERSHOCK *98*
THE "CONSULTANT BLIND SPOT" *99*
THREE LESSONS FOR THE STRATEGIC CYBERSECURITY LEADER *100*

17. REGIONAL THREAT LANDSCAPE ANALYSIS 102

NORTH AMERICA 102
17.1 Threat landscape characterization 102
17.2 Data theft 105
17.3 Unique pressure tactics 106
17.4 Automated scripts and fragmented payloads 107

18. REGIONAL THREAT LANDSCAPE ANALYSIS 112

LATIN AMERICA 112
18.1 Ransomware as the Primary OT Threat Vector 113
18.2 Targeted sectors and attack surface 114
18.3 Attack origins and threat actors 115
18.4 Who is keeping an eye on the region? 115
18.5 Critical infrastructure vulnerabilities 116
18.6 Attack methodologies 117
18.7 The geopolitical dimension 117
18.8 Detection and response challenges 117
18.9 Key takeaways from an OT perspective 117

19. REGIONAL THREAT LANDSCAPE ANALYSIS 118

EUROPE 118
19.1 Unique challenges in Europe 120
19.2 Cluster level attacks logged in European honeypots 121
19.3 What motivates threat actors in Europe? 122
19.4 Detection vs recovery: Europe Vs RoW 123
19.5 Critical infrastructure: Regional sector risk profiles 123
19.6 Cross-sector risk interdependencies and cascading failure scenarios 123
19.7 Common regional attack vectors and exploitation pathways 123
19.8 Lateral movement: Crossing the IT/OT Boundary 124
19.9 Purdue Model violations in practice 125
19.10 DMZ traversal and historian exploitation 125
19.11 Living-off-the-Land (LotL) in OT Environments 125
19.12 Lack of Zones and network breaks 126
19.13 The firmware challenge 126
FIRMWARE IMPLANTS 126
BOOTKIT TECHNIQUES 126
PLC LOGIC MANIPULATION 126
ROGUE DEVICE IMPLANTATION 127
19.14 Continuing impact of the Ukraine-Russia war on cyberspace 127

20. REGIONAL THREAT LANDSCAPE ANALYSIS 129

INDO-PACIFIC 129
20.1 Specific TTPs observed in the region 130
20.2 Breaching perimeter defense 130
20.3 Network traffic manipulation and monitoring 130

20.4 Extended network access and stealthy data exfiltration 131
20.5 Large scale exploitation and persistence 131
20.6 What motivates threat actors in Indo-Pacific? 132
20.7 The Indo-Pakistan conflict spills over into cyberspace 134
20.8 Malicious phishing and payload URLs 137
20.9 Strategic context 134
20.10 A primer on Pakistani cyber threat actors 138
Assessing Pakistani Cyber Capabilities: A Scorecard 140
The Attribution Problem 141
Summary Assessment 141

21. REGIONAL THREAT LANDSCAPE ANALYSIS 141

MIDDLE EAST 141

21.1 Chief threat actors 142
KNOWN IRANIAN APT ACTORS AND THEIR MANDATE 143
21.2 Threat actor profiles: The active players 143
TACTICS, TECHNIQUES AND PROCEDURES 145
21.3 Targeting OT systems 146
21.4 Most targeted countries 147
21.5 Average number of incidents 147
21.6 What motivates these attacks 148
21.7 Geopolitical drivers (34% Combined) 149
21.8 Reconnaissance (21%) 149
21.9 Financial motivations: Ransom and access sale (26%) 149
21.10 Data Exfiltration (10%) 149
21.11 Disruption, Malware Testing, and Others (9%) 149
21.11 Sector-wise analysis 150
21.12 Oil and gas (26%) 150
TRANSPORT INFRASTRUCTURE (49%) 150
21.13 Water supply and management (9%) 151
21.14 Power utilities and manufacturing (9%) 151
21.15 Overall assessment 151
THE REGION IS A PRIMARY THEATRE, NOT A SECONDARY TARGET 151
THE RECONNAISSANCE SIGNAL DEMANDS ATTENTION 152
THE IT/OT CONVERGENCE DIVIDEND IS BECOMING AN IT/OT CONVERGENCE LIABILITY 152
ACCESS BROKERS ARE A FORCE MULTIPLIER RISK 152

22 OT SECURITY IN 2026 153
DOMAIN 1 – GOVERNANCE, RISK MANAGEMENT & COMPLIANCE 154
DOMAIN 2 – NETWORK ARCHITECTURE & SEGMENTATION 155
DOMAIN 3 – ASSET VISIBILITY & VULNERABILITY MANAGEMENT 157
DOMAIN 4 – IDENTITY, ACCESS MANAGEMENT & HUMAN FACTORS 159
DOMAIN 5 – THREAT DETECTION, INCIDENT RESPONSE & RESILIENCE 160
DOMAIN 6 – SUPPLY CHAIN & THIRD-PARTY RISK 162
IMPLEMENTATION ROADMAP 163
MATURITY BENCHMARKS: WHERE SHOULD YOU BE? 164
CLOSING ADVISORY 165

1. Introduction

Threat reports today are a dime a dozen. Most of these reports just skim the surface when it comes to detailing real threats and their implications. Further, the data in such reports cannot be used to support decision making.

Which is why Shieldworkz has always invested in making our reports more detailed, insightful, action oriented, informative and evidence based. Every report we bring out goes through multiple rounds of iterations in terms of content structure and analysis. This is to ensure that our report remains significantly relevant to the decision-making process at every level from the plant onwards to the board.

This year is no different. That is why you will see a new and refreshing change to our Table of Contents. We hope the 2026 edition comes even closer to your security goals than ever. The new sections will help you derive more insights into the specific implications of the evolving threat landscape to your operations.

Further, we have also added sections that dissect major cyber incidents to give you an idea of how these attacks were carried out with detailed analysis on the TTPs used and the extended measures that threat actors deployed to put more pressure on the victims while opening more parts of the infrastructure.

Rigorous analytical framework

Every captured attack is systematically fingerprinted, categorized, and analyzed. This rigorous, multi-layered approach ensures the integrity and reliability of our data, allowing us to deliver insights and forecasts with a high degree of confidence and share data that can stand true when measured through the highest levels of scrutiny.

- Threat ranking: We utilize a proprietary threat rank index, a priority assessment framework developed by Shieldworkz, to score and prioritize threats.
- Standardized classification: For tactical analysis, we use the MITRE ATT&CK framework to sub-classify attacks, ensuring our findings are aligned with industry-standard methodologies.
- Noise elimination: Background noise in the form of reconnaissance attacks and probing from white hat sources is removed after validation.

We hope you will find this edition useful in your security endeavors. We will also be available for any further information that you require on any part of this report.

Prayukth K V

Author and Primary Investigator



2. Research methodology

The core data for this report comes from the **70 plus honeypots** we run around the world and the **10 shadow honeypots** operating from confidential locations. Wherever possible, data is also gathered from our partner institutions, regional CERT teams, regulators and publicly available OSINT.

Every year, we collate cyber threat insights for analysis from January 1 of the subsequent year. The data collection happens throughout the year from January 1 12:00 AM of every year (**UTC+14 time zone**) until December 31, 11:59 PM (UTC+14 time zone). Christmas Island which receives the first rays of sunshine of the new year is the geographical location we consider for marking the time.

Every bit of data gathered is first sorted by our trained AI engine and classified for analysis by a team comprising security operations experts, forensic investigators, malware researchers, TTP identifiers, and threat researchers.

Deep surveillance capability

Each attack is studied, fingerprinted, analyzed, categorized, and marked according to a threat rank index, a priority assessment framework developed by Shieldworkz. We also use the MITRE framework for sub-classifying these attacks.

Shieldworkz's honeypot network includes over **10,500 physical and virtual devices** covering over **1,200 device architectures** supported by varied connectivity flavors. Devices are connected individually or in a constellation format to mimic real-world industrial and critical infrastructure deployments and configured at a granular level.

The networks supporting them are also configured to mimic device communications, network behaviors, remote site interactions and other network and device characteristics to ensure the prevalence of a near-real world ICS and IoT environment.

Our threat intelligence network spans hackers' forums, malware platforms, IM chats, the dark web, and other validated avenues where threat actors congregate/collaborate. Shieldworkz runs dark honeypots to monitor locations where untested vectors of concern emerge in the wild either for testing or for stealthy transfer. In addition, we also monitor known and emerging threat sinks which are known locations where tested semi-ready or fully ready versions of malware and malicious payloads are launched.

Our surveillance net gives our threat intelligence more depth and relevance giving more latitude to bring out insights that are exclusive to Shieldworkz. Post collection and unsupervised categorization, this data is analyzed thread-bare by our global threat research team. The analysis focuses on these areas



2.1 Double-blind test

In addition to this, random parts of the data are given to two different teams with more or less similar composition for a double-blind test without revealing the data source. The data pool is then contaminated with generic signals. Only if the analysis matches with an error margin of +/- 2.1 percent and the team is able to isolate injected data, do we consider the process accurate.
We also issue advisories to government agencies and enterprises. The feedback on the usefulness of such advisories becomes another validation point for us.

Here are a few more data points associated with this report:

- 200 million signals processed every day
- 80 collection nodes across the globe
- 10 stealthy nodes located in cyber threat hotspots
- 13 algorithms to lend authenticity
- 80 plus threat actors surveilled
- 9 Petabytes of data has flowed through the whole process
- 87 forums and collaboration platforms tracked

Criteria for selection of a city to host a honeypot

- National capitals
- Cities with extensive presence of OT infrastructure
- Cities having high density of OT operators
- Landing points for submarine cables
- Ground control stations for satellite communication
- Cities having critical infrastructure
- Geopolitical hotspots
- Cities having extensive research facilities
- Internet traffic hotspots

Cyber Threat Intel Gathering Locations



Resources & Disclaimer

More information on the data and the cyber incidents mentioned in this report is available in the blog section of our website.

To access our raw datasets, reach out to us at www.shieldworkz.com

Disclaimer: While every attempt is made to ensure the integrity and reliability of the data we have analyzed herein, we cannot offer any guarantee that this work and interpretations suggested therein are error-free. In case you come across any discrepancy, do let us know.



3. 10 Reasons to read and understand the data in this report

This report covers the most important parts of the threat landscape that are of relevance to businesses while filtering out the noise

- ✓ Widest range of industrial security-focused threat intelligence inputs from 80 cities around the world
- ✓ Detailed analysis of every data cluster is presented to offer a comprehensive view.
- ✓ Data to support all forms of decision-making around security priorities.
- ✓ Cybersecurity leaders can gain a much deeper understanding of how the threat landscape is evolving and its specific impact on their business
- ✓ Deep dive into threat actor TTPs, payloads, targets, and breach trends
- ✓ More actionable insights and less speculation
- ✓ Expert analysis by experienced threat and security analysts
- ✓ OT focused information
- ✓ Accurate cyber threat predictions based on a thorough investigation of existing TTP patterns
- ✓ Extensive investigative reports on major breaches



70+ cities







4. The year that was

The last major attack of 2025 was reported on December 30th by the European Space Agency. The incident closed the curtains on a tough year for cyber defenders everywhere. In addition to more breaches and overall confusion, 2025 was also marked by:

- Delayed incident response and a clear lack of measured and choreographed response to incidents
- Asset blind spots that enabled network entry and data exfiltration
- Arbitrary activation of services and lack of port hygiene
- Lack of adequate security being accorded during maintenance windows
- Extended gap between risk assessments; inadequate assessment of OT infrastructure
- Lack of privilege accountability in OT
- Lessons from previous incidents have not been learned

These represent only the most visible deficiencies observed. There were many other security challenges that went unaddressed or partially addressed leading to more cyber incidents and amplification of the fallout of such incidents.

On the other end, threat actors were able to configure and carry out more complex attacks thanks to the vast volume of data that they have access to now. By using more sensitive scanners and data scrapers, threat actors are now able to identify more assets of interest and get access to stolen credentials faster. AI is also helping them in this effort. Malware development and customization are now more accessible but malware developed using AI may contain kill switches unknown to the operators.

Just before the ESA breach, two Romanian critical infrastructure operators reported breaches across their complexes. This was a coordinated attack on Romanian critical infrastructure and while the attacks were carried out by different actors using different techniques, the overall strategy behind the attack was unmistakable. This was a coordinated attack designed to destabilize the CII of a nation and send a larger message to other CII operators. It is also possible that this attack was a practice run for a larger attack on a larger CII operator in another country.

This is how threat actors are now targeting major CII operators. Most of the state-backed threat actors have multiple threat actors at their beck and call to carry out smaller attacks. Such attacks are often carried out for these reasons:

- Exfiltrate data
- Train threat actors
- Deploy loiterware and/or latent malware
- The data exfiltrated is sold to generate revenue for the group
- Identify skilled hackers who are then recruited for critical missions

In the first half of the present decade, threat actors were actively hunting for rogue insiders who could help them carry out attacks from within. Now, however, with the easy availability of stolen credentials, threat actors are now able to target employees with appropriate credentials from outside the network. This is a major trend that emerged in 2025 and represents an evolutionary leap.

Let's now look at some more data from the year.

The average number of major cyber incidents per month involving OT continues to rise though it is still slightly higher than the Covid era peak attained in 2021. Incidents involving OT can be split further into the following categories based on the outcome or the asset or other parameters.

- **"Walked In the front door" attacks (Access abuse)**

Typical targets

- HMIs, engineering workstations
- Remote access gateways
- PLCs with weak authentication

- **"IT spillover" attacks (From corporate network to the plant floor)**
  - Phishing email infects corporate laptop
  - Malware spreads via shared AD, file servers, or backups
  - Eventually reaches OT network

- **Tool hijack attacks (Living off OT Tools)**

Abuse of legitimate software:

- Siemens TIA Portal
- Rockwell Studio 5000
- Schneider EcoStruxure

- **Silent process manipulation attacks (Integrity compromise attacks)**
  - Sensor data spoofed
  - Setpoints nudged within "acceptable" ranges
  - Control loops destabilized slowly

Targets

- PLC logic
- Instrumentation (pressure, temperature)
- OPC data flows

4.1 Kinetic attacks (Destructive OT attacks)

What it looks like

- Firmware wiped or corrupted
- PLCs put into STOP mode
- Safety systems disabled

Common techniques

- Unauthorized firmware updates
- Abuse of vendor protocols
- Logic bombs

Real impact

- Physical damage
- Long recovery times
- Equipment replacement

Example: PLCs rendered inoperable requiring weeks of reprogramming.
Safety instrumentation system targeting (SIS-Specific)

4.2 Safety instrumentation system targeting (SIS-Specific)

What it looks like

- **Attacks against:**
  - Triconex
  - HIMA
  - Safety PLCs

Why this is critical

- Safety ≠ control
- Often less monitored
- False sense of isolation

Real impact

- Safety layer neutralized
- Accidents become possible
- Regulatory nightmares

Example: SIS placed into program mode so it never trips during unsafe conditions.
Ransomware (Extortion-driven OT attacks)

4.3 Ransomware (Extortion-driven OT attacks)

What it looks like

- Encryption + threat of process disruption
- Attackers understand production pain points

New trend

- "Pay or we shut the plant down"
- Data theft + operational blackmail

Real impact

- Emergency shutdowns
- Supply chain disruptions
- Safety risk due to rushed restarts

Example: Attackers don't touch PLCs-but threaten to leak recipes and disrupt batch runs.
"Insider or near-insider" attacks

4.4 "Insider or near-insider" attacks

What it looks like

- Disgruntled employee
- Contractor with excess access
- Accidental but catastrophic mistakes

Why OT is exposed

- Broad privileges
- Limited peer review
- Minimal logging

Real impact

- Logic deletions
- Misconfigured safety
- Long troubleshooting cycles

Example: Engineer reuses old logic without realizing protections were removed.
Supply chain and update poisoning attacks

4.5 Supply chain and update poisoning attacks

What it looks like

- Compromised firmware
- Trojanized vendor updates
- Infected USB tools

Why OT suffers

- Trust in vendors
- Offline updates
- Rare patch cycles

Real impact

- Backdoors embedded for years
- Multi-site compromise

Example: Infected firmware installed during routine maintenance.
"Visibility and Control Denial" Attacks (Blindfolding Operators)

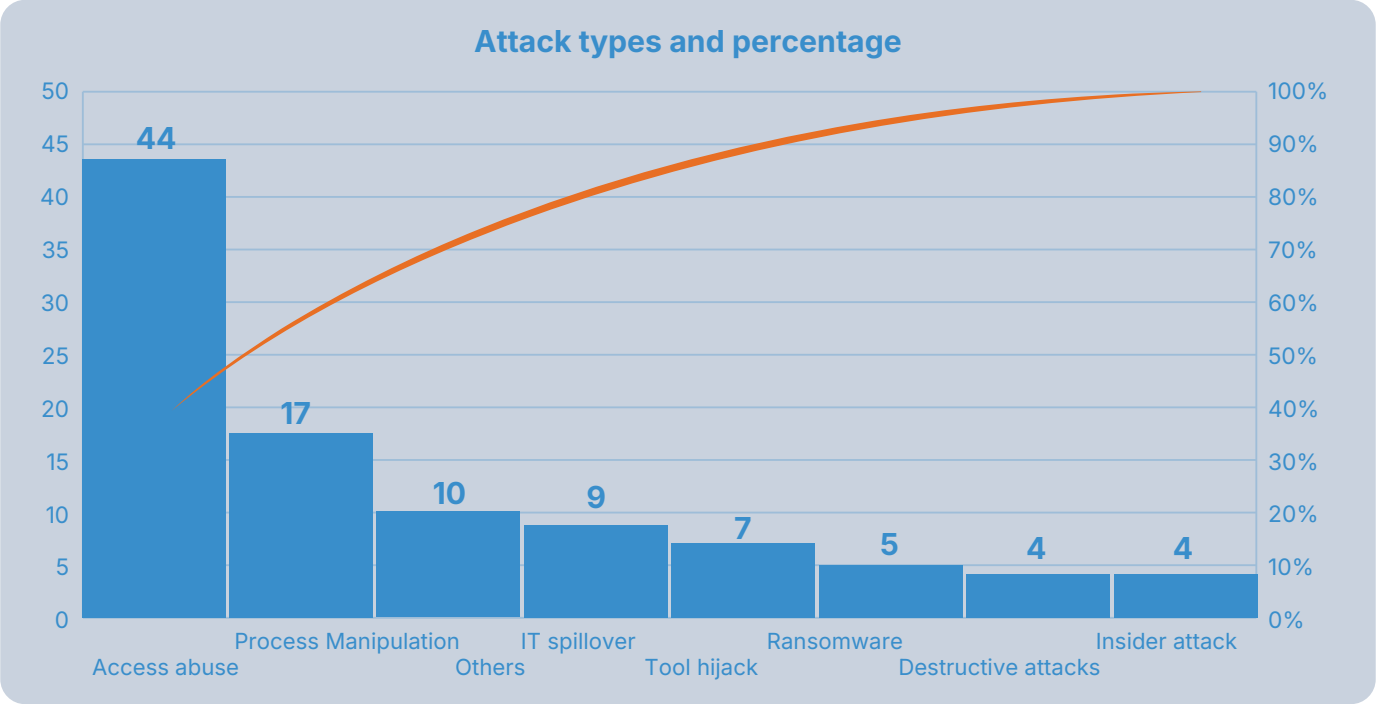
"Visibility and Control Denial" Attacks (Blindfolding Operators)

What it looks like

- HMI blackouts
- Historian corruption
- Alarm flooding or suppression

Real impact

- Unsafe manual operations
- Emergency shutdowns



Across all types of attacks, access abuse is the most prevalent one as per our research. This includes unauthorized abuse by insiders, vendors and others. Access abuse often goes unnoticed and unreported, but it could potentially open up doors for external threat actors to abuse. For instance, use of administrative privileges to install an unauthorized application or modify the operational parameters of a system on behalf of a senior employee fall under this category. While most of these attacks are harmless, it does represent a lack of cyber hygiene and compliance gaps. In case of threat actors, access abuse occurs when they use stolen credentials to illegally access parts of an infrastructure.

Unauthorized process manipulation is the second most prevalent form of cyber-attack. This could again involve people from within and without. This could also involve a threat actor that could use compromised credentials to manipulate an operational process to impact a function. This could include modifying the RPMs in case of a turbine or speed of a baggage conveyor belt in case of an airport. In the attacks we studied in our honeypot, threat actors were found to be keen on modifying processes to either to take control of the process itself or to create a distraction while they deployed a payload.

Another form of this attack involves spoofing data from a sensor or flooding a sensor with false data to overwhelm it.

IT spillover attacks include attacks wherein the IT infrastructure is used as a corridor to target the OT half of the infrastructure.

4.6 Tool hijack

Tool hijack involves the digital seizure of a tool to use it to target other parts of the infrastructure or to control a process or to retain access to the infrastructure for a long time. While the exchange of payloads and malware between networks is very old trend, what has changed is the use of networks to increase loiter time.

Device and tool hijackings occur with greater frequency than is generally recognized. There are two sub trends that contribute to the rising prevalence of tool hijack attacks. The first one has to do with high levels of supply chain poisoning that is occurring today. Supply chains linked to critical components are very opaque today and they often crisscross OFAC nations and suspicious entities. There are threat actors such as Qilin that even sell access to poisoned devices and components. When poisoned devices are deployed on a network, they open up the whole infrastructure to attacks in the future.

The second sub-trend is the use of cost effective devices that emerge from suspicious geographies. While these devices are often marketed as sensors and field devices with very low inherent compute capabilities, threat actors can easily hijack them and use them to launch DDoS attacks at scale or to target the enterprise from within. Unsegmented and/or misconfigured networks and devices can also be discovered and hijacked.

Ransomware attacks on OT are also growing. As we had mentioned in last year’s report, this is a challenge that should now draw attention from security teams everywhere. Prevalence of vulnerabilities, unsegmented networks, unsupervised use of pen drives, lack of adequate security for legacy systems and core systems are all contributing to this trend. Threat actors have understood the wide security gaps that exist in OT environments today and are working to develop and improve ransomware that can target OT systems specifically.

Kinetic\Destructive attacks are also rising though at the same rate as the other attacks. This is the one type of attack that can manifest in ways that can create a multitude of challenges for enterprises that host OT systems right from disruption all the way to health and safety risk for employees. An example of a kinetic attack is the Western Norway Dam Incident that occurred in April 2025 when Pro-Russian hackers gained unauthorized access to a small dam's control system via an internet-connected panel. They opened a valve for four hours, demonstrating a direct physical manipulation of critical infrastructure. As hybrid warfare intensifies, we will see the kinetic dimensions of cyber incidents playout in a much larger format with more implications.

Rogue insiders continue to create cyber incidents of concern everywhere. Shared credentials, lack of need-based access to systems and networks, lack of policy enforcement (and access audits) and in some cases a lack of strong disciplinary mechanisms are all contributing to this trend. While the motivations may be many for these criminals, the outcome is usually the same – revenue attrition, loss of systems and in one instance, an insider auctioned her credentials on a underground forum.

The modest growth in major OT cyber incidents could trigger complacency as it effectively hides an inconvenient truth. The volume of sub-kinetic events are growing at a staggering pace and this shows that the cyber defenses are not up to the mark and more needs to be done to secure systems. It is quite possible that hackers are not leveraging the access and control they have today to create a much larger fallout because they are playing the waiting game.

Clues to such an interpretation are available in the late December attacks on Romanian critical infrastructure firms. The attacks were carried out by different threat actors using different tools and tactics yet the outcomes were more or less the same. We have covered this attack in detail in a separate section. The takeaway is clear. Hackers are becoming more patient and controlled in their tactics. This means that they are now playing the waiting game more often and this is a worrying trend. They are willing to absorb the risk of being detected while waiting to create a larger incident at a time of their choosing.

4.7 Tactical and behavioral changes exhibited by hackers

Pre-2021	Now
Carry out the attack immediately or within the shortest period of time after gaining access	Wait and study the compromised infrastructure for a longer duration to set up a more devastating attack at a time of their choosing.
Exfiltrate data	Sell access, exfiltrate data and recruit potential insiders
Compromised environment is of not much interest once the attack is done	Hackers are carrying out secondary attacks and trying to deploy unerasable malware or trying to squirrel away malware in sections of the infrastructure that are not subjected to reimaging or wiping.
Employees were not immediate targets	Hackers are creating digital profiles of employees within target enterprises to guess credentials, send fake job offers, identify potential for recruitment or to target them for phishing and vishing.
Phishing cycles used to extend for months	Cycles are faster thanks to AI
Malware development was not customized	Malware development can be customized as per the device being targeted; Backdoors are embedded early in the SDLC
Attacks were not coordinated	The same actor can deploy multiple teams or even actors to target an entity. This is done to increase the chances of success
APTs were operating in relative isolation	APTs are working with independent and semi-state-backed actors

5. Major cybersecurity trends observed in 2025

5.1 The era of coordinated attacks

2025 was the year of coordinated attacks. In order to increase the chances of success, threat actors have now resorted to targeting victims across multiple fronts including using different affiliated groups and tactics to cause a breach. This indicates a new evolution frontier for threats. By using different affiliates, threat actors are now able to pit affiliates against each other thereby initiating an internal arms race while incentivizing innovation in tactics and ransomware. The group that manages to breach the target gets a higher share of the ransom payout while scoring earning credibility / gaining favor with the parent threat actor.

5.2 Supply chain concerns multiply

Till 2025, supply chain breaches were limited to vulnerabilities or Zero Days. In 2025, we also saw supply chains being misused using fake patches and source code modification. Such threats can bypass traditional security barriers such as Security Acceptance Testing and create an ongoing risk for enterprises that are not monitoring their devices and environments to the level required.

Jailbreaking commonly used or even rare devices are done by threat actors in their labs. They are able to procure industrial devices from secondary markets at reasonable prices and handed over to the lab. The team in the lab then works to reverse engineer the product and firmware. Such capabilities are used in situations where the target is a critical infrastructure operator. It is also common knowledge that Zero Days are also sold illegally across forums and command a heavy premium depending on the device concerned.

5.3 Ever expanding threat surfaces

As our 2025 survey has shown, many OT and IoT systems remain accessible from external networks with a bit of scanning. Lack of network monitoring, asset blind spots, use of unsecured remote connections, unmonitored use of pen drives are all leading to a substantial erosion of overall security posture. Even in case of enterprises with fairly mature OT security programs, one or more of these practices were found during our assessments. If we have to secure our infrastructure, then such practices have to be discontinued and replaced by more robust and validated security practices. The cumulative gains made by enterprises by implementing a series of incremental security measures staggered in time can wither away or be fully undone by a single security gap.

5.4 Rise in cyber attacks and probes during the vacation season

Vacation periods such as end of the year, Thanksgiving, July 4th and region-specific vacation seasons are now consistently logging a higher volume of attacks over the baseline volumes. Lack of adequate staffing (even in case of SOCs), employees in transition, lack of onsite guidance from senior employees are the main contributors to this trend. Threat actors are aware of this window and have begun working actively to run large scale campaigns to target enterprises during this vulnerable period.

5.5 Misuse of internet connectivity

Use of free yet compromised Wi-Fi on official devices, unauthorized use of Wi-Fi on the shop floor, use of free and compromised VPNs, are primarily responsible for this trend. Such behaviors open up security gaps that enable threats to propagate across networks. We have come across machines that were infected when they latched on to unsecured and compromised public Wi-Fi while in transit. IoT devices that have auto-connect on are at a risk from this trend. Most IoT devices lack the robust security features (by default) (such as antivirus, regular automatic updates, complex passwords) of traditional computers or smartphones.

A device that is set to auto-connect might latch on to an insecure or malicious public Wi-Fi network (often an "evil twin" attack), or an attacker who compromises an IoT device on your home network can use its default sharing permissions to gain access to more sensitive devices, such as work computers or mobile phones.

Data Interception: When an IoT device connects to an unsecure network (e.g., public Wi-Fi, a network with weak WPA2 encryption), the data that is transmitted between the device and its servers will be unencrypted and susceptible to interception through "man-in-the-middle" attacks. Such exposure includes personal identification, movement history, and confidential data, which threat actors can then leverage for various malicious activities.

Botnet Formation: IoT devices are often left on continuously and are rarely monitored, making them ideal for hackers to hijack and form massive botnets. These compromised devices can then be used to launch large-scale Distributed Denial of Service (DDoS) attacks, overwhelming online services and causing widespread outages. We have seen compromised IoT devices with some level of compute power being used to mine Bitcoins.

Credential Reuse: Widespread lack of unique passwords. MFA Gaps: Failure to implement phishing-resistant MFA (FIDO2) across all consumer and enterprise accounts.

Gaps between assessments: Even in case of business that are running OT security programs, the gap between risk assessments sometimes stretches beyond 1 year and there is no assessment that happens in a bespoke manner. This leads to a gradual degradation of security posture over the years

5.6 Firewall and network configuration challenges: Due to lack of proper configurations and traffic management, many OT operators are at risk of cyber incidents triggered from outside the network as well as rogue insider activity. Sometimes, third-parties are assigned the task for configuring firewalls and the result is rules that are not aligned with the actual security requirements of the enterprise. Suspicious traffic types or traffic originating from grey-listed IPs are allowed leading to staggered deployment of malware, loss of data, major rise in blast radius after an incident and risk of long term reconnaissance using stealthy malware.

5.7 Threat actors tend to target sectors with lower levels of protection while handling data critical to compliance, business operations, or privacy. Industries such as healthcare and education are prime targets due to their often weaker security measures. In healthcare, for example, Internet of Medical Things (IoMT) devices can be exploited to exfiltrate patient data or even locked remotely as part of a ransomware attack, disrupting operations and pressuring institutions into paying a ransom.

5.8 The payload deployment and execution models with growing competition among hacker groups, the evolution of hackers is proceeding at a faster pace than ever before. Threat actors are investing heavily in building malware that can be more easily deployed and launched. These include malware that can be device and firmware specific with stealth and communication obfuscation features that render it near invisible to NDR applications operating only on anomalies.

5.9 Chinese and North Korean APT groups remain among the most active threat actors worldwide, with their presence detected across diverse sectors such as healthcare and logistics. Chinese APT groups primarily seek valuable intelligence, while North Korean groups, particularly Lazarus, focus on financial gain. Lazarus is also known for selling exfiltrated data on underground forums. With its extensive digital footprint and an organized network of operatives supporting its activities, Lazarus stands as one of the most formidable threat actors today.

5.10 The absence of a structured and rapid incident response process is severely impacting enterprises. An analysis of 47 major ICS-related incidents conducted by our research team revealed that the lack of ICS event management specialists, documented response playbooks, and comprehensive operational and asset visibility significantly amplified the impact of these attacks.

5.11 IT-OT convergence is enabling threats to move in both directions. While the risk of threats
originating from OT is well understood, many enterprises have overlooked the danger of threats migrating from IT to OT. In 2023, malicious payloads embedded within seemingly harmless traffic evaded detection by antivirus systems due to low signatures, successfully compromising OT networks and workstations in multiple incidents.

5.12 Lack of network segregation
Another critical security gap is the lack of a well-architected network that properly segregates risk zones from functional zones. Without this segmentation, organizations struggle to implement granular security controls, maintain visibility, and enforce operational safeguards—leaving their OT environments vulnerable to attacks.

5.13 Commoditization of attacks and the rise in the number of threat actors: With the rise in ransom demand and easy access to potent malware, the number of threat actors is rising. In 2024, while we were able to track and profile 70 actors and 203 affiliated actors, these numbers rose to 81 and 302 respectively in 2025. The number of affiliates includes about 131 actors who have extremely feeble affiliations and/or are affiliated with multiple groups.

When the number of threat actors grows, the volume of attacks rise and this place additional detection and triaging stress on security teams (including those who are operating with a high level of automation).



6. Security challenges

Here are a few other security challenges that contributed to some of the above trends:

- **SaaS over-permissioning**: Excessive scopes granted to third-party integrations. OAuth Lifecycle Management: Lack of rotation or monitoring for long-lived refresh tokens.
- **Identity governance**: Weak verification processes for service desk password resets. Lateral Movement: Insufficient network segmentation allowed the infection to spread to production floor systems.
- **Patch latency**: Marked delays in applying critical emergency patches to business-critical legacy systems.
- **Shadow systems**: Unmapped and internet-facing devices and ERP instances.
- **Supply chain fragility**: Over-reliance on a single vendor for critical diagnostic services. Lack of Redundancy: Minimal clinical continuity plans for digital service outages.
- **API Insecurity**: Exposed, unmonitored internal APIs. Privileged Access Management (PAM): Lack of JIT (Just-In-Time) access for administrative queries.
- **Detection Blind Spots**: Failure to monitor for kernel-level anomalies. Network Hygiene: Lack of egress filtering on sensitive database segments.
- **Third-Party Risk Management (TPRM)**: Inadequate security vetting of vendors with deep system integrations. Data Minimization: Storing excessive customer metadata in shared environments.

6.1 Cyberattack trends

Cyberattacks on OT infrastructure registered a significant growth in 2025. Overall, there were over 6,000 mid to major sized events that were flagged globally of which:

- **5,327** events were connected with our honeypots. This is where the data came directly from the honeypots we run across multiple cities around the world
- **451** events relate to companies disclosing some form of incidents voluntarily as gleaned from publicly available documents
- **179** events were brought to our attention by our consultants and partners and involved some form of incident response from our end
- There were **21** cases of leaked (validated) compromise signals picked from the wild as well

7. What do security leaders need to worry about in 2026?

Trend	Concern	Scale
Lack of incident response maturity	There are two clear concerns: • Identifying an incident worthy of attention early to contain the blast radius • Responding accurately Without events being identified on time, the blast radius expands significantly. Couple this with a lack of segregated networks, well planned zones and conduits and lack of context to an incident, a slow response is often the result. Inaccurate response (where the response doesn't target the impacted systems or is not commensurate with the gravity of the threat) could lead to both security and operational impact. A poorly developed incident response (IR) capability exposes organizations to substantial operational, financial, and reputational risks.	Industry-wide problem
Prolonged malware loiter time	We have seen payloads waiting for lean staffing periods to arrive before execution or collation. With increasing malware sophistication, targeting, delayed detection and containment of malicious payloads can allow adversaries to exfiltrate sensitive data, disrupt operations, and deploy additional payloads such as ransomware .	Primarily critical infrastructure and large OT operators
Residual access points present a threat to victims	In the aftermath of a cyber incident, threat actors can re-enter previously compromised networks via residual access points. Residual attacks can cause multiple attacks as well if the access is sold by the threat actor or if the actor initiates a fresh round of exfiltration.	Cross-industry challenge
Lack of well-defined roles, responsibilities, tested responses and playbooks	The level of cyber discipline that prevails is not up to the mark across industries. Many key roles are left vacant, some roles are not well etched and lack of playbooks and defined response as mentioned earlier creates security gaps that can be easily exploited This could lead to a lack of cohesive approach to enforcing security mechanisms and use of tools in an organized manner leading to confusion and erosion of overall security posture.	Cross-industry challenge
Coordinated cyberattacks	Targeting different lines of business (Nissan) and/or targeting the same entity across different actors (Oltenia Energy Complex attack, Romania) and/or targeting the same enterprise using different malware or tactics	Cross-industry challenge

Trend	Concern	Scale
Operational downtime and disruptions due to cyber incidents	Multi-stage/long drawn attacks can lead to prolonged outages and halt production lines, disrupt supply chains, or even cause safety incidents. The revenue and operational impact of a major cyber incident can be severe.	Cross-industry challenge
Externally accessible systems and networks	More details are available in the state of OT security report that we have presented some pages down. Basic scanning itself reveals a wide range of OT devices that can be accessed from the web including linked services as well. The number of such systems continues to rise every year indicating a lack of security attention to this basic cybersecurity practice	Cross-industry challenge
Increasing number of threat actor affiliates	The expansion of affiliate networks within cybercriminal ecosystems will drive a surge in targeted attacks across multiple industries. Sectors such as healthcare and education, already high-priority targets, will continue to face sustained threats. Additionally, mid-sized and small-scale manufacturers, along with supply chain partners, will become increasingly vulnerable as threat actors seek to exploit weaker security postures. The scalability of affiliate-driven attacks, coupled with the commoditization of ransomware-as-a-service (RaaS) and exploit kits, will further amplify the attack surface, leading to a higher frequency of intrusions across interconnected business ecosystems.	Enterprises across industries are at risk
Use of complex attack modes	Threat actors are increasingly leveraging modern programming languages such as Rust to develop highly efficient and stealthy ransomware. By fine-tuning encryption speed and execution patterns, adversaries can evade detection for extended periods, allowing them to maintain persistent access within compromised environments. This strategic delay enables attackers to either stage a more extensive attack at a later time or trigger the breach at a moment of maximum disruption—such as during critical operations, high-stakes projects, or when highly sensitive data is present	Enterprises across industries are at risk
Risks due to voluntary or involuntary insider activity	Due to a lack of sensitization and training, cybersecurity priorities get relegated to the background leading to employees resorting to practices that may increase the risk knowingly or otherwise. Such risks may not just lead to a breach but long-term risks in terms of litigation and censure and/or fines from regulatory authorities.	Enterprises across industries are at risk
Lack of shop floor visibility, network architecture and related documentation, Purdue-level view, and asset information	Without real-time shop floor visibility, security teams cannot monitor unauthorized connections, lateral movement of threats, or anomalous activities in Operational Technology (OT) networks. Unmapped or undocumented assets introduce blind spots, allowing adversaries to exploit legacy or shadow devices. Lack of Purdue model-based segmentation makes it easier for threats to move from IT to OT (and vice versa), facilitating attacks such as ransomware propagation or command injection attacks.	Enterprises across industries are at risk

Trend	Concern	Scale
High levels of reliance on OEMs	In certain enterprises, Original Equipment Manufacturers (OEMs) have been responsible for both cybersecurity and the ongoing maintenance of critical devices. This dependency often results in delays in patch deployment, as updates are not applied within a standardized timeframe. Such delays prolong exposure to known vulnerabilities, increasing the risk of exploitation and compromising the security of the overall system and infrastructure.	Enterprises across industries are at risk
Lack of adequate supply chain visibility	This is an obvious one. Limited visibility into suppliers, subcontractors, and service providers makes it difficult to assess and mitigate security risks. Threat actors often exploit weak links in the supply chain to infiltrate enterprise networks, as seen in software supply chain attacks and hardware compromises. Without real-time tracking and risk assessment, organizations face delayed responses to supply chain disruptions, whether due to cyberattacks, geopolitical instability, or vendor failures.	Enterprises across industries are at risk
Lack of regular OT and IoT audits	Without systematic assessments, vulnerabilities remain undetected, attack surfaces expand, and risk mitigation efforts become reactive rather than proactive. Unassessed security risks can lead to system failures, process disruptions, and even physical damage in critical infrastructure. Attackers exploiting unmonitored IoT and ICS vulnerabilities can disrupt smart manufacturing, energy grids, water treatment facilities, and healthcare systems. Lack of audits results in reactive incident response, rather than proactive risk mitigation, leading to longer recovery times.	Enterprises across industries are at risk
Ransom demands are growing	As threat actors and affiliates are looking at increasing their revenue per breach, the average ransom demand is expected to grow significantly in 2026. The rise in ransom is also due to a significant rise in affiliate recruitment.	Enterprises across industries are at risk
New mandates to comply	As cyber breaches continue to rise, regulators everywhere are expected to introduce stricter compliance measures to enforce stronger cybersecurity practices across enterprises. Key focus areas for upcoming regulations will include workforce cybersecurity competency, the establishment of centralized Security Operations Centers (SOCs) for large organizations, enhanced incident response protocols, resilience measures, and mandatory breach reporting. These evolving regulatory demands will increase pressure on CISOs and business leaders, requiring them to allocate more resources toward compliance, security infrastructure, and risk management.	Enterprises across industries are at risk
Vacation and lean period attacks.	As seen in a major spurt in attacks in December and around known vacation windows, Shieldworkz recommends enterprises scale up their plans to provide additional security during vacation months/during lean staffing periods.	Enterprises across industries are at risk

Trend	Concern	Scale
The Rise of "Living off the Land 2.0" (LotL)	Attackers have moved beyond deploying custom malware. In 2026, the most sophisticated threats can and will use your own tools against you (Such as the attack on Romanian Waters). Attackers use legitimate industrial protocols (Modbus, Profinet, EtherNet/IP) and native engineering software to change setpoints or disable safety interlocks. Since the commands are "legal," traditional signature-based firewalls won't catch them.	Imminent threat for critical infrastructure operators.
Standardizing security posture across IT and OT	Security measures across IT and OT should be at a level where the controls are articulated to defend against the most complex and sophisticated threat or even a human error that could degrade the security posture and allow an attacker to sneak in.	Enterprises across industries are at risk

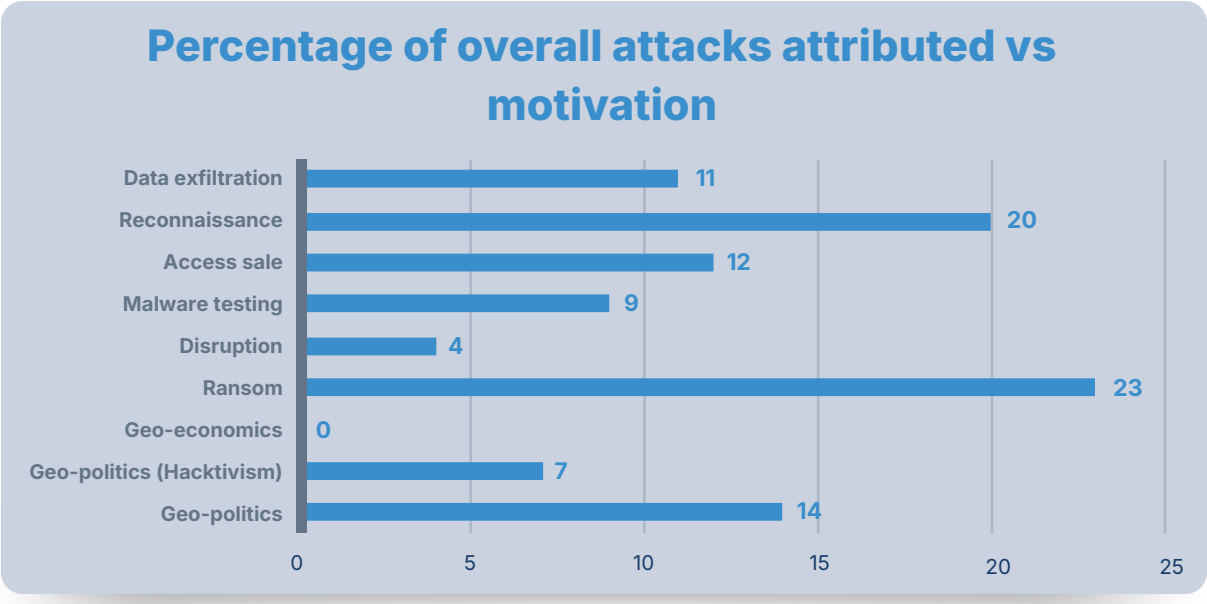
8. Growth in OT-linked cyber events

The difference between IT and OT security has been well articulated and understood by industry participants (remember the oft-heard CIA triad?). The difference between IT and OT security also plays out in the type of attacks they attract. IT attacks often involve a wider range of actors, tactics and malware while OT often attracts more complex attacks involving a lesser set of threat actors. OT cyberattacks also involve more state-backed actors than IT (this trend changes a bit when we consider a broader range of attacks involving government and government agencies and employees). It is essential to understand this context before proceeding to understanding the threat landscape that prevailed in the year 2025.

The most simplified way of defining the threat landscape would be by considering only complex attacks facilitated by or orchestrated by a state-backed actor. We have all heard about the role of geo-politics in shaping the threat landscape but it is also essential to know that the factors that lead to attacks on OT assets often involve a much more diverse set of motivations and factors. Let us look at some of them here:

Motivation	Actor	Outcome
Geo-politics	Nation-state	Kinetic attack
Geo-politics	Hacktivist	Production shutdown for a short window
Geo-economics	Nation-state and/or hacktivist	Extended shutdown of production, supply chain disruption
Ransom	Nation-state, hacktivists, threat actor affiliates, disgruntled employees and independent threat actors	Encryption of assets, temporary shutdown
Disruption	Independent threat actors	Disruption of production
Malware testing	Malware and malicious payload developers, intelligence agencies or masked law enforcement entities	Testing of new malware strains

Motivation	Actor	Outcome
Access sale	Nation-state, threat actor affiliates, disgruntled employees and independent threat actors	Sale of credentials
Reconnaissance	Nation state actors and/or independent actors	Exfiltration of data, staggered/ phased assembly of malware inside target networks
Data exfiltration	Nation state actors, hacktivists and/or independent actors	



Note: The value for geo-economics is less than 1 percent

9.Most targeted cities

The list of most-targeted cities corresponds directly to the list of cities that are heavily industrialized and are making significant contributions to the GDP of the host nation. Mexico City made its appearance in this list for the first time in 2025. The top cities of the world are also located on or close to geo-political faultlines giving threat actors more reasons to target them. For purposes of our study, we have considered both probing attacks and disruptive/malware -based attacks. This is because probing attacks are often the precursor for a full-fledged attack that follows.

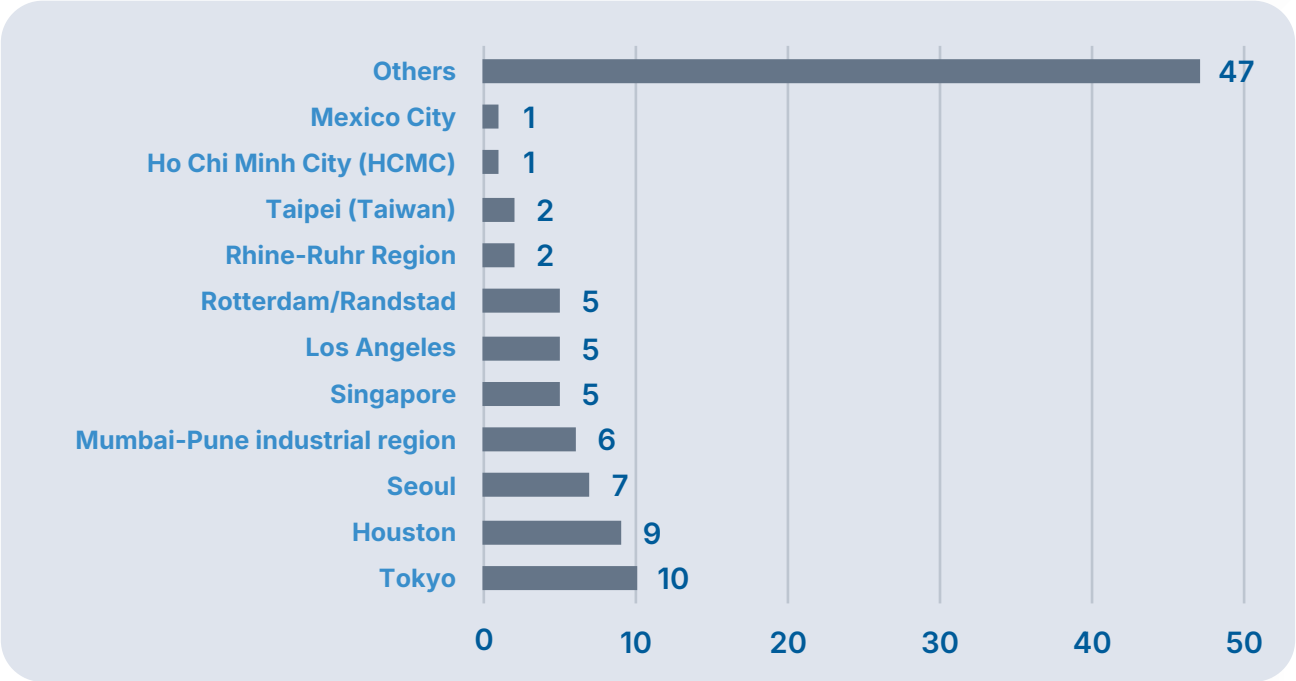
Most of these cities are attracting attention from state-backed actors affiliated to China and Russia.

9.1 Types of attacks

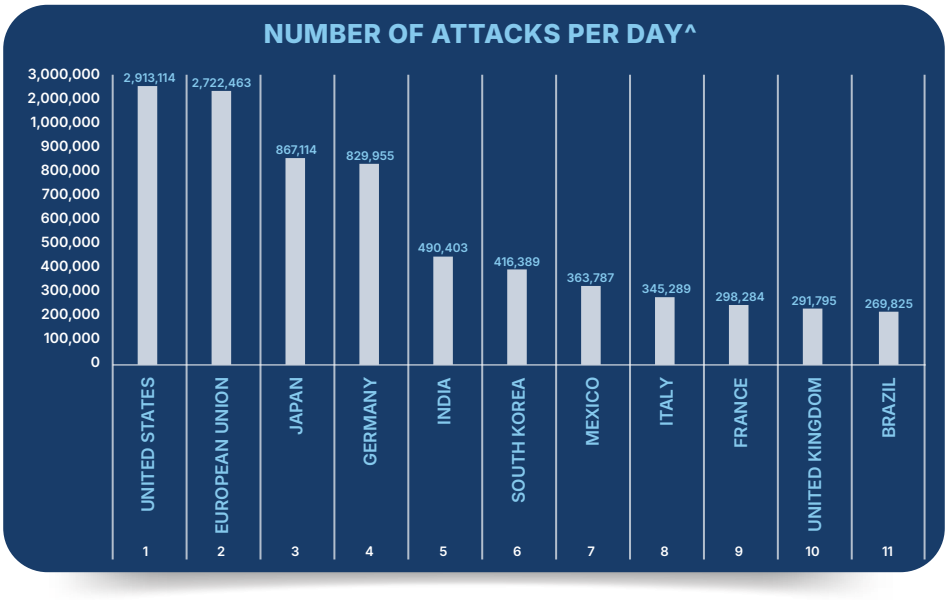
City	Type of attacks
Tokyo	Complex attacks targeted at information pilferage, long term surveillance and disruption. Sectors associated with robotics, automotive engineering, and precision manufacturing are the ones that get attacked more often.
Houston	Ransomware attacks and attacks designed to steal information; Houston also receives a huge volume of probing attacks as well

City	Type of attacks
Seoul	Ransomware attacks and attacks designed to steal information
Mumbai-Pune industrial region	This region receives a very high volume of probing attacks and some information stealing attacks as well.
Singapore	Singapore is among the cities receiving a high volume of attacks on IIoT and IoMT along with some probing attacks on the OT-based industrial infrastructure
Los Angeles	Ransomware attacks and attacks designed to steal information; Los Angeles also receives a huge volume of probing attacks as well. While the volume of attacks on IoT have dipped a little since 2023 and 2024, the quality of attacks have improved significantly in terms of both accuracy and potency.
Chicago	Ransomware attacks and attacks designed to steal information; Chicago also receives a huge volume of probing attacks as well. Some of these attacks are localized to target the financial eco-system in Chicago by masking the origin of the attack.
Rhine-Ruhr Region	Complex attacks possibly involving state-backed actors
Taipei (Taiwan)	Highly complex attacks designed to steal information and disrupt.
Ho Chi Minh City (HCMC)	Highly complex attacks designed to steal information and disrupt.
Mexico City	Highly complex attacks designed to steal information and disrupt.

Percentage of attacks logged



10. Which countries are being targeted?



US continues to be the most targeted country in the world followed by EU, Japan and Germany. The presence of diverse manufacturing clusters in key nations is attracting attacks from both state-backed groups as well as independent and loosely affiliated actors. Countries like India, South Korea and France have seen a massive jump in the number of attacks. Such a rise is due to factors specific to these countries. We will do a deep dive on them in subsequent sections.

But what is essential to note for all cyber defenders is the rising persistence of threat actors. Exposed ports are now (2025) getting scanned (and rescanned) almost once every 17 hours as opposed to once every 72 hours in 2022. Higher scans indicate a higher level of interest as well as motivation. Follow-up scans could also indicate a higher level of vigil being maintained on such infrastructure.

Attacks on critical infrastructure have now become more targeted. This means that a specific process or an asset category or even an individual could be targeted specifically to improve the chances of success. The high level of social media monitoring and use of LLMs trained to identify weak links in security chains are helping threat actors build a heat map of the target so to speak in order to strike at points that may break faster. This is what attack sophistication is all about. It is not just about the attacks getting sophisticated, but the methods and actors are also moving upwards on the scale of complexity.

11 .What are the targets during an OT attack?

Attacks on OT are not just unique but can lead to complex outcomes as well. When we do a deep dive into the data collected this year, a few trends become apparent including:

- There are many misconceptions when it comes to understanding the level of field device connectivity. While many OT operators believe that such systems are isolated, that is not entirely true. These devices are often connected via control networks (EtherNet/IP, PROFINET, Modbus TCP, DNP3, IEC 61850) and remote access for vendors and maintenance, Historians, MES, ERP, cloud analytics. This why our honeypots are registering a good volume of attacks targeted at field devices. The threat actors are aware of such systems being connected at some level and are therefore targeting these devices. Field devices are certainly a part of the attack surface of an enterprise.

- Rising attacks show that attackers are becoming more familiar with OT. HMIs based on traditional operating systems that are aging with a huge list of known exploits are one of the factors contributing to this trend
- Engineering workstations represent another conduit for attacks. This is another OT familiarity builder for threat actors.
- Lack of separation of SIS and BPCS engineering and time-bound supervised connections is leading to the compromise of the last independent layer of protection, enabling uncontrolled physical events. It is possible that some of the SIS systems may be compromised without the operator's knowledge.
- Poor network level security including lack of asset visibility and network level insights and security for remote sites and connections are other challenges that are harming the overall security posture of enterprises from an OT perspective.

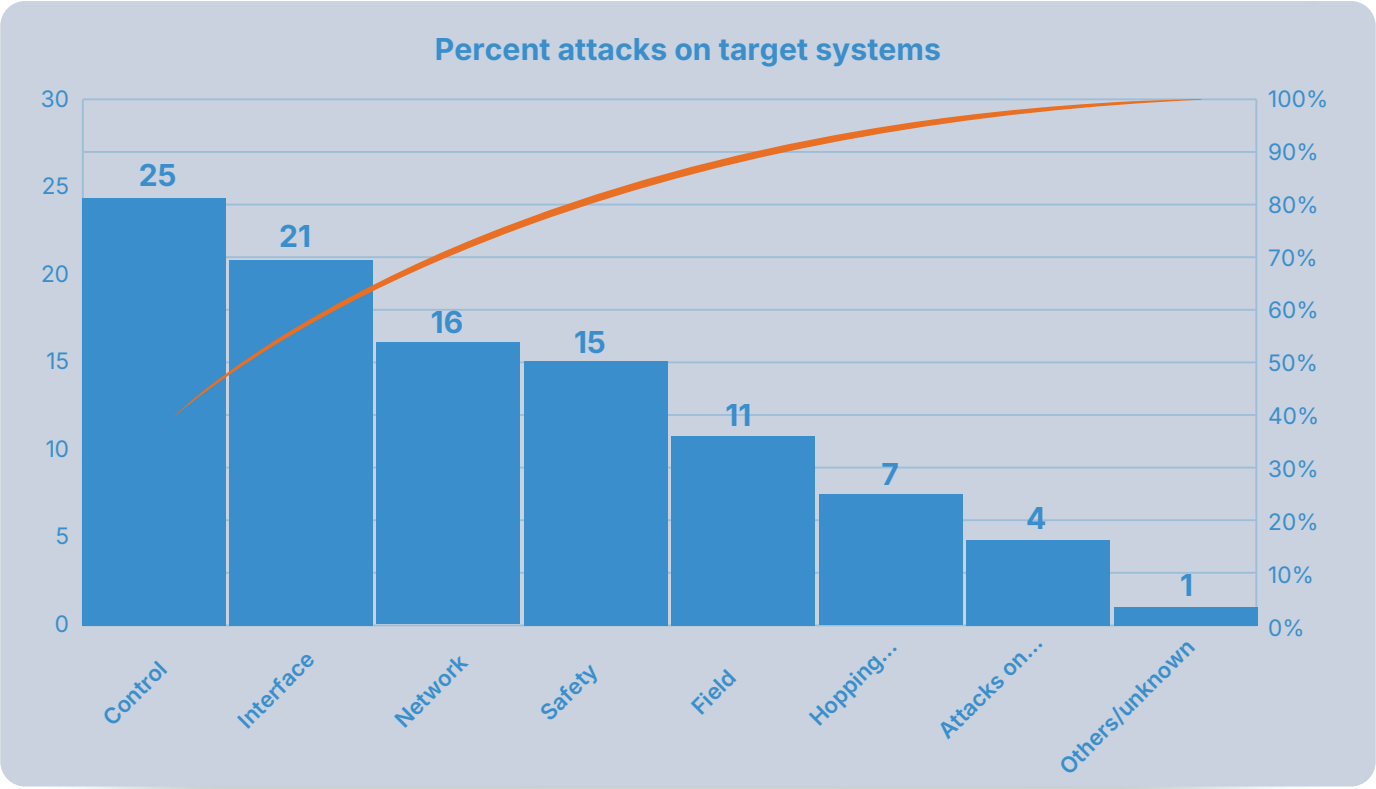
11.1 Usage category, attacks and security challenges

Usage category	Specific targets	Impact of the attack	Security challenges that contribute to or facilitate such attacks
Field	PLCs, RTUs, sensors, VFDs, actuators	Physical damage, shutdown, process disruption, field device reset/bricking, wrong data on various parameters collected, Protection relay misconfiguration, firmware tampering	• Minimal or no logs • Change detection (logic, firmware, config) is absent in many plants • Operations teams normalize anomalous behavior as "process issues" Attackers target field devices because: • They directly control physical processes • They often lack authentication, encryption, and logging • Changes are hard to detect and easy to persist
Interface	HMIs, SCADA terminals	These are the primary entry point for attacks on the OT network. Operator "blinding," unauthorized commands, data poisoning/false data injection, modification of HMI scripts, SCADA screen replacement, abuse of scheduled tasks or startup services, alarm suppression,	**Aging HMI software** • With known exploits **Excessive trust** • HMIs implicitly trusted by operators • SCADA servers trusted by PLCs • Little validation of command origin or intent **Weak monitoring** • Traditional SOC tools ignore OT protocols • No baselining of normal HMI behavior • Changes seen as "operator activity"

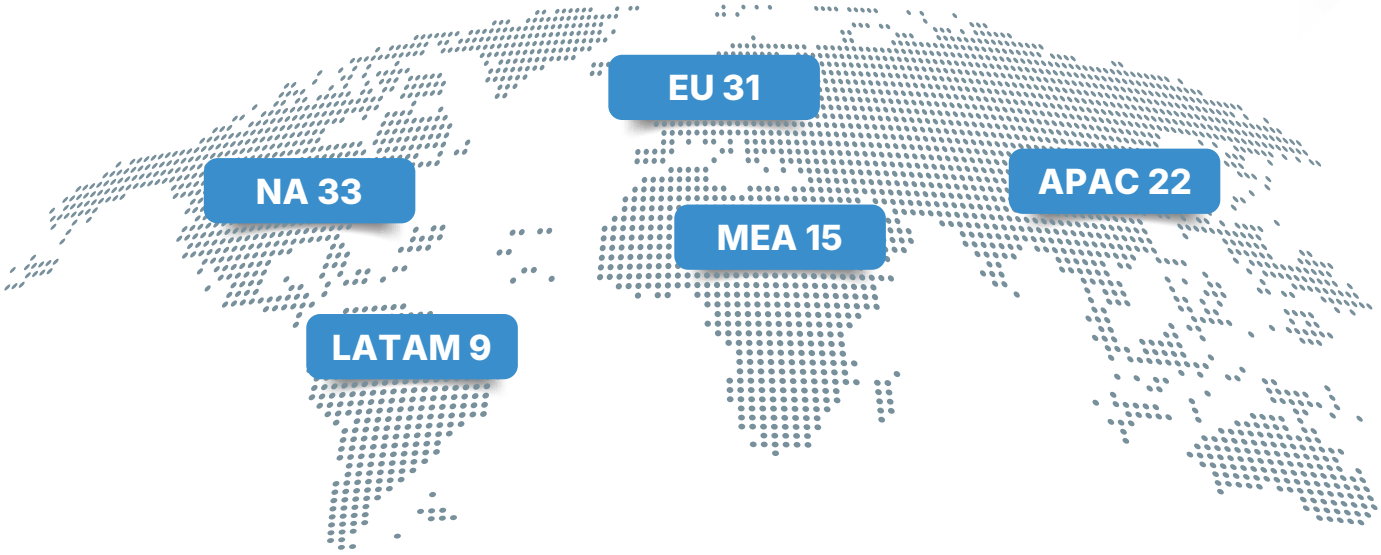
Usage category	Specific targets	Impact of the attack	Security challenges that contribute to or facilitate such attacks
Interface	HMIs, SCADA terminals		**Availability-first mindset** • Security controls avoided due to fear of downtime. • BAU is considered more important
Control	Engineering workstations	Engineering workstations are usually the single most dangerous asset in most OT environments. If an attacker gets an EWS, they effectively get the plant's source code, admin keys, and safety limits. System-wide malicious reprogramming, degradation of system management; allowing threat actors to take control of systems remotely, Modify PLC logic subtly (timing, thresholds, interlocks), upload "valid-looking" projects with malicious intent, disable or desensitize alarms, change SIS parameters just within tolerances, install backdoored firmware, poison backups and golden images	• Engineering software generates no security logs • Change approvals are informal or undocumented • No cryptographic verification of logic changes • Operators trust engineers implicitly
Safety	SIS (Safety Instrumented Systems)	Attacks on Safety Instrumented Systems are rare in volume but extreme in consequence. Manipulation of safety thresholds, slowing down or even prevention of intervention of such systems during an emergency Prevention of emergency shutdowns, escalating situation leading to health and safety hazard	**Ideally, SIS should be:** •Physically and logically segregated •Independently engineered •Rarely changed **In reality, SIS on the shop floor often has:** • Engineering workstations shared with BPCS • Temporary connections for maintenance • Vendor remote access paths • Poorly enforced separation due to operational pressure **Even a brief connection is enough for compromise.**

Usage category	Specific targets	Impact of the attack	Security challenges that contribute to or facilitate such attacks
Network	Industrial firewalls, protocols	Unauthorized access, data manipulation, credential theft, insertion of fake devices, manipulation of traffic characteristics by insertion of fake data to confuse network detection solutions	**Many plants still have:** • Minimal segmentation • Shared VLANs • "Temporary" firewall rules that became permanent • Once inside, attackers can see everything.
Hopping attacks/ lateral movement/ attacks that transit through OT network	IT	Attacks on IT systems and infrastructure	Poor network hygiene and extended unprotected threat surface.
Attacks on remote sites	OT systems operating at remote locations	Shutdown of remote sites or extended lag in communication with such sites or disruption of site operations	Lack of security for remote site communications and maintenance

11.2 Percentage of various attacks logged on key targets



11.3 Geographical distribution of attacks (percentage of global attacks detected at regional targets)



Attacks on NA and EU rose on a year-on-year basis leading to a proportional decline in the (as a percentage of overall attacks) attacks logged by other geos. As mentioned earlier, growth in the volume of threat actors has also contributed to a rise in attacks.

"Threat actors such as Everest Ransomware Group are willing to pay insiders for selling access credentials"

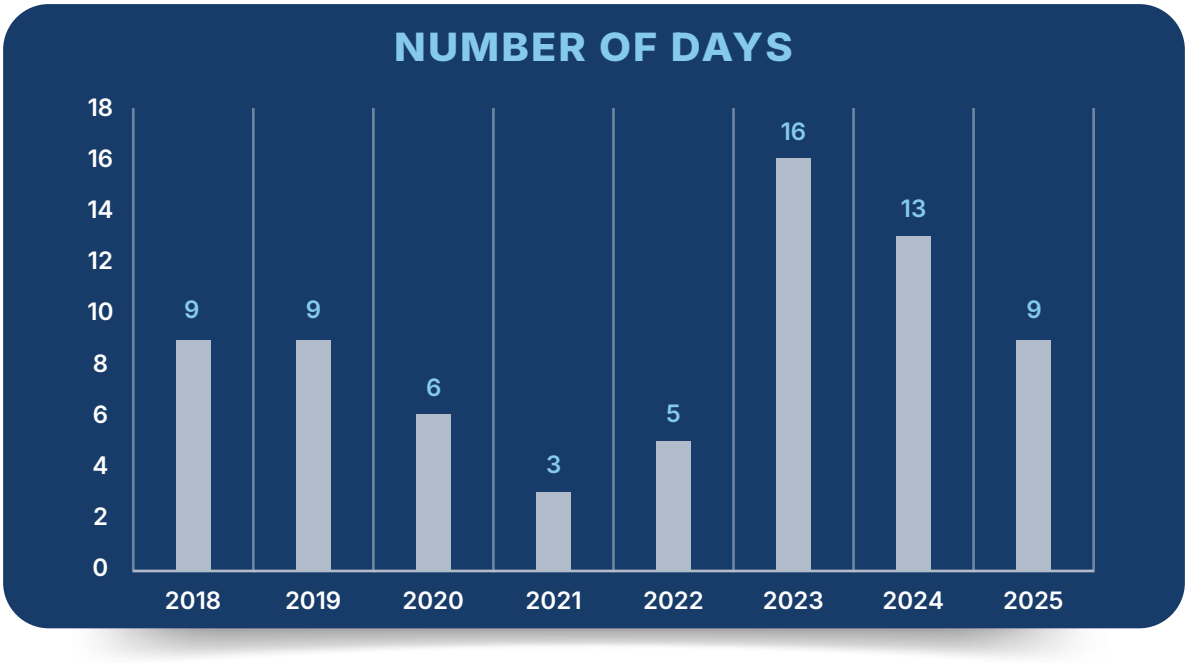
11.4 Why are cyberattacks growing?

- Growth in the number of threat actors
- State-backed actors are using multiple affiliates to breach their targets
- Probe volume goes up every year as more affiliates deploy scanner to identify accessible targets
- Easy availability of stolen credentials and target information
- Easier access to complex tools floated by threat actors from Russia, China and North Korea
- Increase in repeat attacks on existing victims (carried out via residual malware)
- Rise in attacks during vacations
- Threat actors are willing to pay insiders to part with access information
- They are also running recruitment campaigns to target insiders
- Expanding numbers of Identity Access Brokers

The lines between state-backed actors, freelance groups and affiliates are blurring now. Malware, stolen data, funding and tactics move both ways. This means higher levels of collaboration between the actors which is a clear cause for worry. Even groups like the North Korean Lazarus which is a highly isolated group is now working with affiliates directly and through their collaboration with China's APT 41 (more on this in our APT section).

While these are the core trends that we are observing globally, there are regional factors at play in some geographies. Conflict zones often see a steep rise in attacks during periods of geopolitical tensions and the increased volumes are sustained well after the conflict cools down and tensions subside. Threat actors are highly opportunistic, and they see such windows (of conflicts) as moments where they can push through attacks without getting blamed.

11.5 Days taken to place stolen data and credentials for sale across forums



Source: Published data plus Shieldworkz research

Stolen data is now making its way into forums much faster. But at the same time, bad actors are retaining a major portion of the stolen data with them as is evident from the declining volume of data released by threat actors (during sale or as a dump). This could mean a few things:

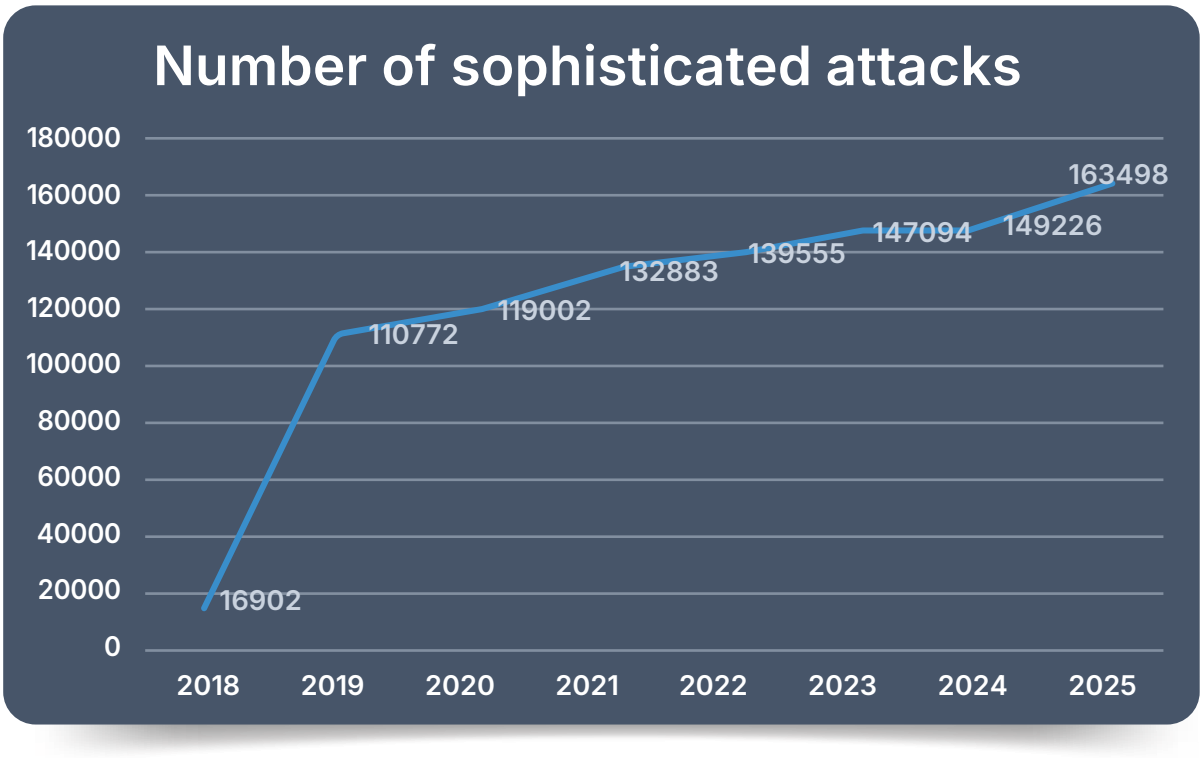
- They are using this data to train LLMs
- The data is being used internally for either training or for identifying patterns to exploit in target networks
- This data could be sold across multiple identity access brokers

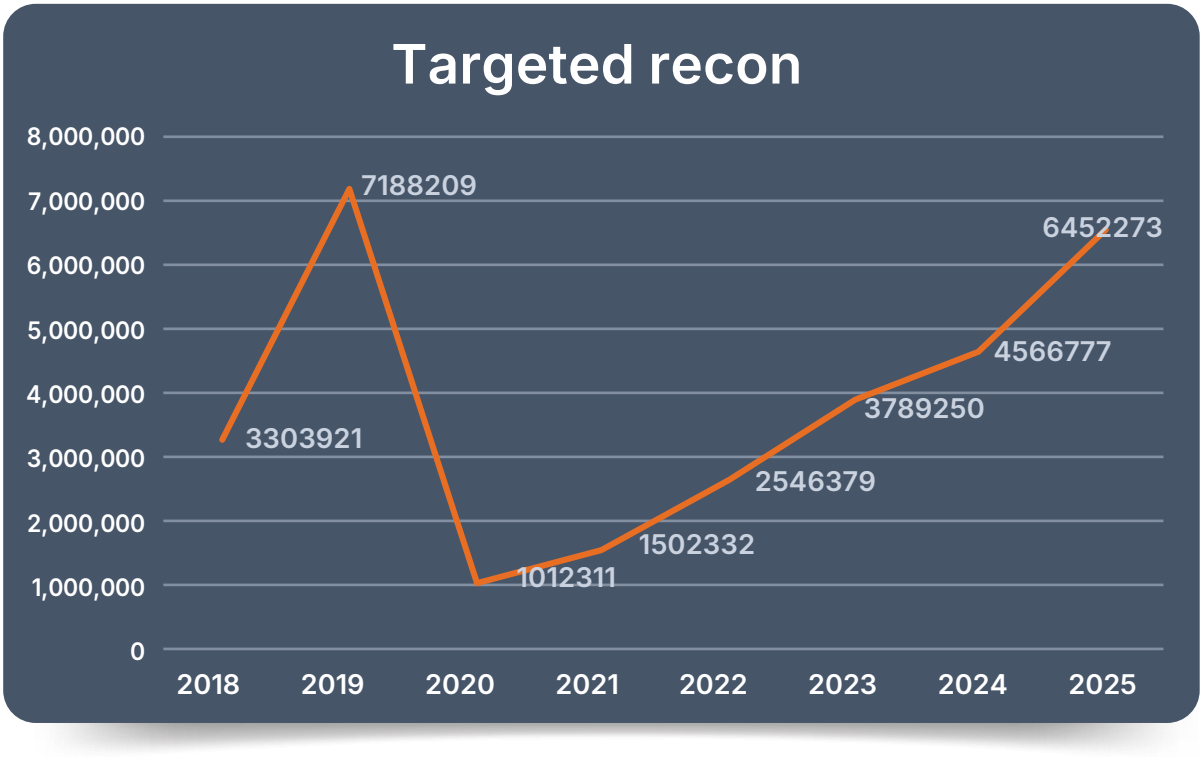


Source: Published data plus Shieldworkz research

11.6 Rising attacks

All honeypots around the world logged a rise in cyberattacks over the year.





Methods used to detect external scans:

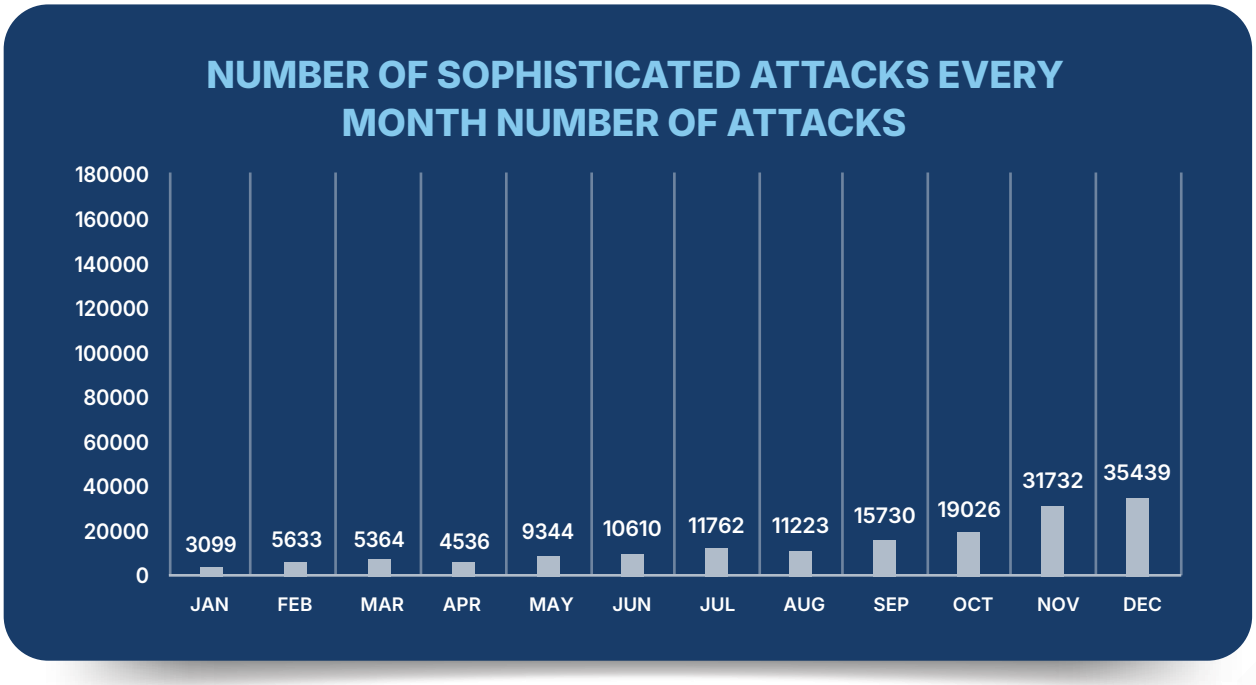
- Unexpected "Asset Discovery"/enumeration: Detection of unauthorized tools attempting to inventory assets.
- An unusual volume of TCP/UDP packets targeting varied ports on controllers or HMIs.
- Unauthorized "Read" commands. Unexpected PLC queries for instance trying to read memory registers. This indicates an attacker trying to understand the control logic.
- Vulnerability scans. Crude attempts to identify outdated, unpatched software CVEs

This brings us to an important point. If the attacks are rising, aren't we seeing more breaches and more reports on successful attacks? Every threat report worth its IOCs talks about rising attacks but no one talks about the real-world implications. So, are these attacks directed only at honeypots? The answer to this is very simple. We just have to consider these trends:

- Cyberattacks reported by enterprises on both OT and IT have increased in 2025
- A significant volume of the attacks are probes designed to build a digital profile of the potential victim in the future
- Access to a network doesn't automatically translate into a kinetic attack (by threat actor). Threat actors are known to wait for months or even years to launch a disruptive attack
- We have seen payloads bound for (or targeting) IT cross through OT networks

Can honeypot networks attract attacks that are not bound for actual OT networks? While it cannot be completely ruled out, there are a couple of sources that could possibly serve as the origin for unique attacks that are not seen in the wild. These are researchers and academicians who are probing networks using modified scanners. Our honeypots are configured to eliminate such attacks (more on it on the section on the State of OT security).

The rise in attacks during vacation months is a trend that has picked up in the last few years. Vacation months are usually periods of lean staffing and as we have seen with attacks on Poland and Romania's energy infrastructure, these are attractive windows for hackers to strike.



11.7 Which sectors getting attacked and why?

Sector	Percentage
Utilities (Power)	11
Utilities (Renewables)	2
Water supply and management	5
Job shop manufacturing (Specialized aviation and marine components, high-tech industrial machinery, luxury consumer goods)	9
Repetitive manufacturing (Electronics, toys, confectionery)	7
Discrete manufacturing (Clothing, automotive, firearms, medical devices)	5
Batch manufacturing (Food and beverage, pharmaceuticals, plastics)	10
Continuous manufacturing (Oil refining, Fertilizer production, chemical processing, pharmaceuticals)	9
3-D printing/additive manufacturing	3
Oil and gas (Refineries)	19
Oil and gas (Field activity)	1
Transport (Railway systems of all types)	3
Transport (Ports – inland and sea facing)	4
Transport (Airports)	3
Transport (Pipelines)	6
Others\undefined	3

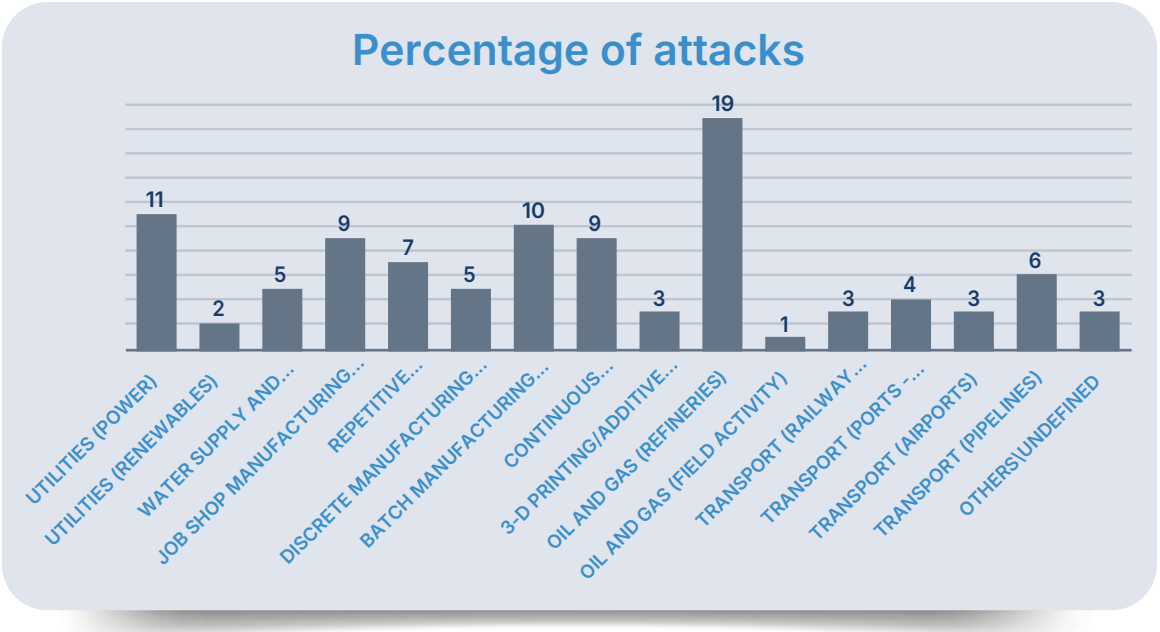
11.8 Mapping sectoral attacks to threat actors (types)

Sector / Sub-sector	Ransomware and Criminal Groups	Nation-State / State-Aligned Actors	Why this actor dominates
Utilities (Power)	◐ Medium	● High	Power disruption has strategic, geopolitical value. Nation-states target grid visibility, switching, and stability for coercion or pre-positioning. Criminals focus mainly on IT-side extortion.
Water supply and management	◐ Medium	● High	Water affects public health and civil stability. Often targeted by state actors for intimidation and influence; criminals exploit weak security for extortion.
Manufacturing (general)	● High	◐ Low	Downtime sensitivity and low tolerance for outages make manufacturing ideal for ransomware monetization rather than strategic sabotage.
Job shop manufacturing (Aviation, marine, high-tech machinery, luxury goods)	◐ Medium	● High	High-value IP and defense-adjacent supply chains attract espionage-driven nation-state actors alongside selective extortion.

Sector / Sub-sector	Ransomware and Criminal Groups	Nation-State / State-Aligned Actors	Why this actor dominates
Repetitive manufacturing (Electronics, toys, confectionery)	● High	○ Very Low	High-volume operations maximize ransom leverage; limited strategic value for nation-states.
Discrete manufacturing (Clothing, automotive, firearms, medical devices)	● High	◐ Medium	Criminals exploit JIT disruption; state actors target defense-related or dual-use manufacturing (automotive, firearms, medical devices).
Batch manufacturing (Food, pharma, plastics)	● High	◐ Medium	Ransomware thrives due to recall risk; state actors selectively target pharma and chemicals for IP theft or supply disruption.
Continuous manufacturing (Oil refining, fertilizers, chemicals, pharma)	◐ Medium	● High	High safety and environmental impact makes this sector attractive for strategic disruption, pre-conflict positioning, and deterrence signaling.
3-D printing / Additive manufacturing	◐ Medium	● High	High safety and environmental impact makes this sector attractive for strategic disruption, pre-conflict positioning, and deterrence signaling.
Oil and gas (Refineries)	◐ Medium	● High	Energy security and geopolitical leverage dominate; criminals usually target corporate IT, states focus on OT reconnaissance and control.
Transport (Railways)	◐ Medium	● High	National mobility, safety, and public confidence make rail OT a strategic target for state actors; criminals exploit passenger disruption.
Transport (Ports – inland & sea)	● High	◐ Medium	Dual-use target: criminals monetize logistics downtime; state actors target trade flows, sanctions enforcement, and military logistics.
Transport (Airports)	● High	◐ Medium	High public disruption favors ransomware; state actors focus more on intelligence collection and contingency planning than overt disruption.
Transport (Pipelines)	● High	● High	Proven ransomware monetization (fuel disruption) combined with strategic energy leverage attracts both actor classes.
Others / Undefined	◐ Medium	◐ Medium	Typically exploited as weakly defended entry points, staging infrastructure, or supply-chain pivots rather than primary targets.

Legend

- ● High: Primary threat actor
- ◐ Medium: Regular but secondary presence
- ○ Very Low: Rare or opportunistic only



Notes: Smart cities were attacked but the volumes were less than 1 percent, so we have not considered for this analysis.

Sector / Sub-sector	Why are they being targeted by OT cyberattacks
Utilities (Power)	High national criticality; disruption causes immediate societal and economic impact making it an attractive target for state-backed threat actors. Legacy OT, long asset lifecycles, and tight IT–OT coupling make power grids attractive for state-sponsored sabotage, coercion, and ransomware extortion.
Water supply and management	Often under-secured with aging control systems. Attacks can directly impact public health, safety, and trust, making water utilities ideal targets for disruption, intimidation, or politically motivated operations.
Manufacturing (general)	High availability requirements, fragile production schedules, and low tolerance for downtime make manufacturers prime ransomware and extortion targets. OT environments are often flat, legacy-heavy, and weakly monitored.
Job shop manufacturing (Specialized aviation and marine components, high-tech industrial machinery, luxury consumer goods)	High-value IP, proprietary designs, and limited redundancy. Even small disruptions cause disproportionate financial and contractual impact, making these firms vulnerable to IP theft and targeted extortion.
Repetitive manufacturing (Electronics, toys, confectionery)	Large volumes and thin margins mean attackers can maximize impact by halting production. Often highly automated, with standardized PLCs and HMIs that are widely understood and easier to exploit at scale.
Discrete manufacturing (Clothing, automotive, firearms, medical devices)	Complex supply chains and just-in-time production amplify the downstream impact of disruptions. Safety -critical products and regulatory exposure increase pressure to pay ransoms quickly.
Batch manufacturing (Food and beverage, pharmaceuticals, plastics)	Process integrity and quality are critical; small manipulations can cause large product recalls or safety incidents. Attackers exploit quality control, recipe management, and changeover phases.

Sector / Sub-sector	Why are they being targeted by OT cyberattacks
Continuous manufacturing (Oil refining, fertilizer production, chemical processing, pharmaceuticals)	Continuous processes are difficult and expensive to stop or restart. Attacks can cause physical damage, environmental incidents, or safety hazards, making these sectors prime targets for sabotage and geopolitical signaling.
3-D printing / Additive manufacturing	Digital-to-physical workflows allow attackers to manipulate designs, weaken components, or steal sensitive IP. Detection is difficult, and compromised parts may fail later, increasing long-term risk.
Oil and gas (Refineries)	High economic value, geopolitical sensitivity, and safety impact. Refineries rely on tightly coupled OT systems where disruptions can cause fires, explosions, or prolonged outages, making them attractive to both criminals and nation-states.
Transport (Railway systems of all types)	Strong safety implications and public visibility. Legacy signaling systems, remote access for maintenance, and large attack surfaces make railways attractive for disruption and coercion.
Transport (Ports – inland and sea facing)	Strategic chokepoints in global trade. Highly heterogeneous OT environments, heavy third-party access, and poor segmentation enable attackers to cause cascading supply-chain disruptions.
Transport (Airports)	High public impact, complex IT-OT interdependencies, and reliance on time-critical systems. Even limited outages cause widespread disruption, reputational damage, and regulatory scrutiny.
Transport (Pipelines)	Linear, distributed assets with remote monitoring and control. Attacks can halt energy supply, cause environmental damage, or trigger national-level responses, as demonstrated by past ransomware incidents.
Others / Undefined	Typically targeted due to weak governance, unmanaged legacy OT, lack of visibility, or because they serve as indirect entry points into larger critical-infrastructure ecosystems or supply chains.

Key OT threat modelling insights on the data

- Ransomware groups optimize for downtime, not destruction Manufacturing, ports, pipelines, and airports dominate because availability = revenue.
- Nation-states optimize for leverage, pre-positioning, and signaling Power, water, energy, chemicals, and transport control systems are targeted even without immediate disruption.
- Overlapping sectors are the highest risk Ports, pipelines, continuous manufacturing, and discrete defense-adjacent manufacturing face both monetization and strategic threats.
- OT intrusion ≠ immediate disruption for state actors Many nation-state campaigns focus on persistent access, engineering workstation compromise, and logic understanding, not instant outages.

12. Deep dive on use of AI in cyberattacks by threat actors

We have been tracking the growth in AI-based or AI-enabled attacks since the year 2020. Before we move forward, let us first define the two broad categories of AI-connected attacks.

AI-based attacks: Involve AI-based vectors or payloads generated or modified by AI

AI-enabled attacks: Attacks that are supported by threat actors using AI such as for instance for writing phishing scripts generated or modified by AI or use of AI agents to gather data on targets or

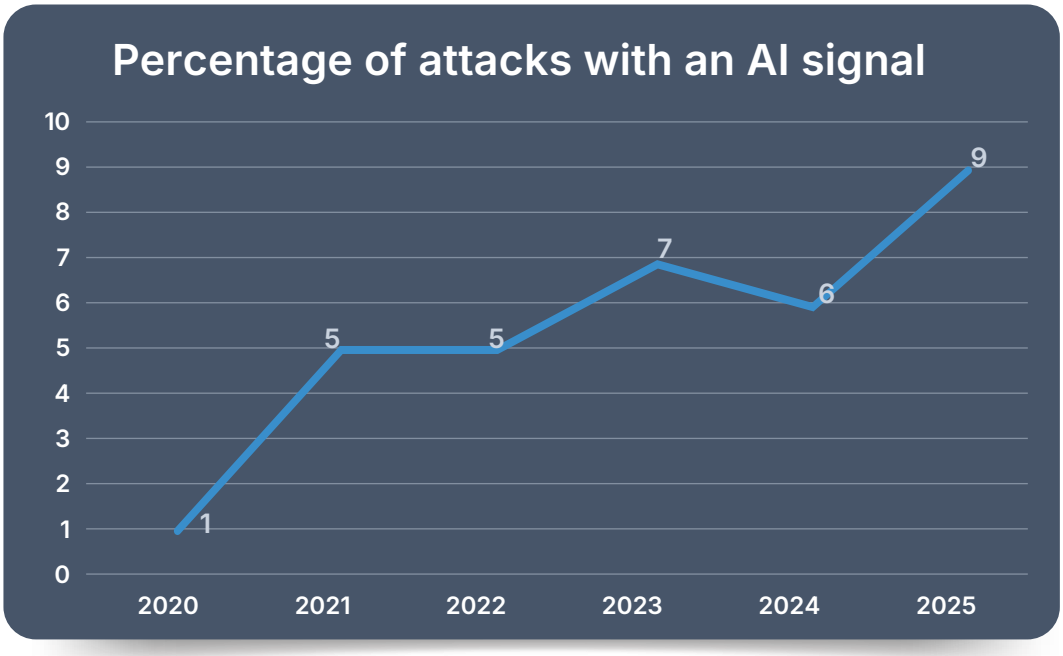
Key trends:

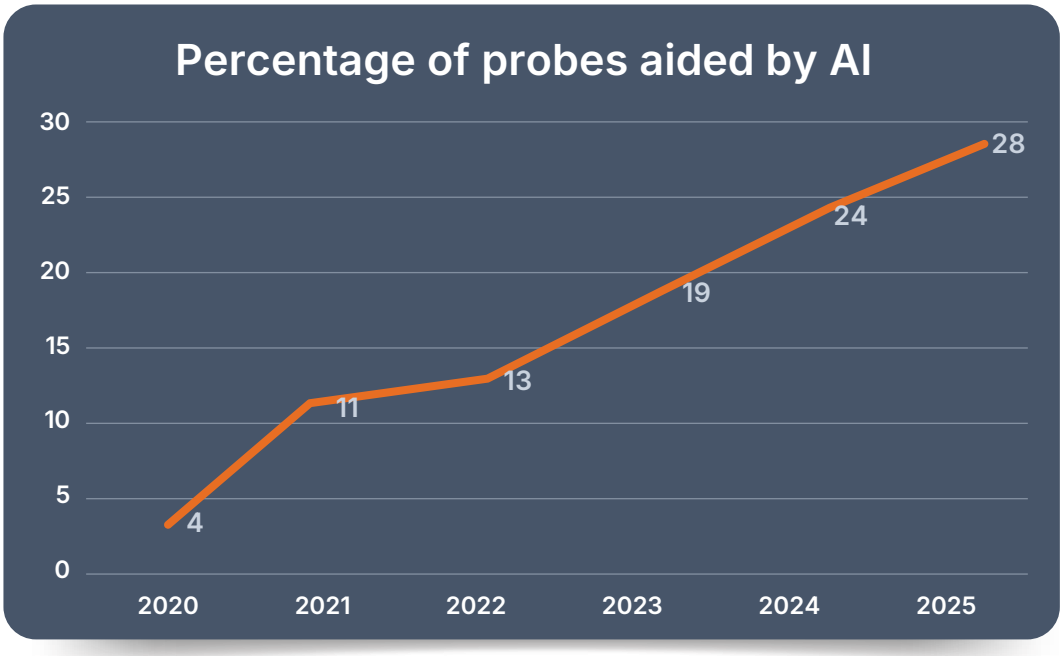
All inferences here are based on what we are observing in the wild and elsewhere.

- AI has brought down malware and recon cycles: From weeks to days and days to hours. Building and deploying custom malware is now easier than ever.
- Managing attacks, attack vectors and groups: The rise in coordinated attacks clearly shows that all types of challenges associated with running affiliate programs and managing large groups of threat actors is now history. The coordination efficiency shows that threat actors have mastered coordination and it is no coincidence that the evolution of AI has also intensified in the duration that such coordination improved. It is possible that major threat actors are using AI to manage attacks and groups.
- Attack modelling: The late 2025 attacks show a level of sophistication that we have not encountered before. Almost all attacks involved a near flawless execution. This indicates that threat actors could be gaming attacks and attack scenarios before launching the actual attacks.
- Attack surface expansion: AI is enabling threat actors to discover and exploit OT vulnerabilities 10-100x faster than manual methods, particularly in legacy systems never designed for adversarial environments. AI agents can also run scans from external networks to determine points of entry, networks and services that are accessible from outside as well as information on credentials and roles and responsibilities of key employees. All this information can be crunched to fashion an attack path on a target.
- Wider commoditization: AI-powered tools are transforming OT attacks from nation-state capabilities requiring specialized ICS knowledge into commoditized attacks accessible to mid-tier criminal groups. The concern is about sophisticated commoditization wherein a large number of complex attacks can be launched at a very small range of targets.
- Speed differential: While AI assists defenders, the asymmetry favors attackers who can operate without safety constraints, testing attacks at scale against digital twins and simulations before deployment.
- Strategic implications: Organizations relying on "security through obscurity" of proprietary protocols or air-gap assumptions face existential risk as AI eliminates these traditional defenses.

12.1 Percentage of overall attacks that had a AI signal

Year	Percentage
2020	1
2021	5
2022	5
2023	7
2024	6
2025	9





The current state - AI as an attack accelerator

12.2 Vulnerability discovery and reconnaissance

Traditional OT attack reconnaissance: Historically, targeting industrial control systems required threat actors to:

- Manually map network architectures through patient observation
- Reverse-engineer proprietary industrial protocols (Modbus, DNP3, IEC 61850)
- Avoid honeypots (they are a waste of time and attention for hackers)
- Gain a level of understanding of OT network traffic dynamics
- Understand process engineering to craft attacks with physical effects
- Develop custom tools for each manufacturer's systems

This expertise barrier limited serious OT attacks to nation-state actors (Russia, China, Iran, North Korea) and their proxies.

12.3 AI-based reconnaissance:

Large Language Models (LLMs) and machine learning now enable:

- **Automated protocol analysis**: AI can analyze network traffic captures and reverse-engineer proprietary industrial protocols in hours versus months. LLMs can successfully reverse-engineer and dissect protocols to identify and tag previously unknown command structures and network dynamics by analyzing packet captures.
- **Vulnerability pattern recognition**: Machine learning models that are trained on global CVE databases (and even Zero day data procured from underground sources) can identify vulnerability patterns in ICS firmware binaries, scanning thousands of devices for exploitable conditions. The MITRE ATT&CK for ICS framework now documents 81 distinct techniques across 12 tactics and that's only the known part. AI can systematically test all permutations and come up with a combination that can be exploited along with the best window for launching an attack after the initial compromise.
- **OSINT aggregation at scale**: AI scrapers can easily correlate:
  - Shodan/Censys industrial device exposures. Approximately ~230,000 ICS devices directly internet-accessible (More on this in our report on exposed ICS devices
  - LinkedIn employee profiles revealing technology stacks and responsibilities
  - Vendor documentation and manuals
  - Regulatory filings disclosing facility operations
  - Satellite imagery showing physical layouts

Such data can be used to create comprehensive target packages that can be used in building attack kits in hours versus weeks or even months of manual intelligence collection.

12.4 Social engineering and insider threat amplification

AI-enhanced spear phishing:
Generative AI has led to the industrialization of social engineering against OT environments:

1- Deepfake voice attacks: In 2023, a European energy company reported an attempted wire fraud using AI-cloned voice of their CEO. The caller asked for emergency payment for "control system upgrades." While the finance team was able to detect the fraud, the same technique could authorize emergency maintenance access or system changes.

2- Contextual phishing at scale: AI can generate thousands of highly customized phishing emails in minutes by:

- Scraping company announcements about equipment upgrades
  Mimicking vendor communication styles from training data
- Creating believable pretext scenarios (safety recalls, compliance updates, firmware patches)
- Localizing content to specific facilities based on public records

If enough data is fed, it can even determine the percent chances of success.

3- Credential harvesting optimization: AI analyzes which social engineering approaches succeed across industries, continuously refining techniques. CISA's 2024 threat assessment notes a 300% increase in credential phishing specifically targeting OT personnel Within this, AI-generated content showed higher success rates than traditional templates.

12.5 Insider threat modeling:

AI enables sophisticated profiling of potential insider threats:

- Behavioral analytics that identify employees facing financial stress, disgruntlement, or access pattern anomalies
- Automated identification of employees that have both access and opportunity
- Targeting individuals most likely to be recruited or coerced
- Identify employees to be recruited for long term missions

12.6 Malware development and customization

Evolution from Stuxnet to AI-Generated ICS Malware:

Current AI Capabilities:

1 - **Code Generation**: Recent research from research institutions demonstrated LLMs generating functional Modbus TCP attack code when prompted with ICS attack scenarios, including:

- Register manipulation to alter setpoints
- Command injection sequences
- Covert channel establishment
- Logic bomb insertion

2 - **Polymorphic Malware**: AI can generate infinite variants of the same malware, each with different signatures, defeating signature-based detection. This is particularly effective against OT environments running legacy antivirus with infrequent updates.

3 - **Logic Bomb Optimization**: AI can analyze process control logic (ladder logic, function blocks) and identify optimal injection points for:

- Maximum physical damage
- Delayed activation to avoid detection
- Plausible deniability (making attacks look like equipment failures)

12.7 Documented Threat Actor AI Adoption

12.7.1 Nation-State Programs

12.7.2 Russia:

Documented Capabilities:

- MITRE ATT&CK attributes multiple Russian APT groups (ELECTRUM, VOODOO BEAR) with ICS-targeting capabilities
- 2015 and 2016 Ukraine power grid attacks demonstrated sophisticated understanding of SCADA systems
- 2017 Triton/TRISIS attack on Saudi petrochemical facility targeted safety instrumented systems (SIS)

AI Integration Assessment: While specific AI tool usage remains classified, open-source Russian cybersecurity research shows extensive work on:

- Automated vulnerability discovery in ICS protocols
- Machine learning for network traffic analysis
- Natural language processing for social engineering

Russian doctrine emphasizes pre-positioning in critical infrastructure for future conflict. AI accelerates both initial access and maintaining persistent, low-and-slow reconnaissance. The 2024 Volt Typhoon campaign (attributed to China but using Russian TTPs) demonstrated pre-positioning in U.S. critical infrastructure - AI likely accelerated the scale of infiltration.

12.7.3 China:

Documented Capabilities:

- Volt Typhoon campaign (2023-2024): Confirmed infiltration of U.S. critical infrastructure including energy, water, telecommunications
- MSS (Ministry of State Security) directives explicitly call for AI integration in cyber operations
- PLA Strategic Support Force invests heavily in AI-enabled cyber warfare

AI Integration:

- Chinese academic publications openly discuss AI for industrial control system security research (offensive applications obvious dual-use)
- State-sponsored groups demonstrate rapidly adapting tradecraft, suggesting automated tool development
- Scale of Volt Typhoon (compromise across multiple sectors simultaneously) suggests automated reconnaissance and exploitation

U.S. Cybersecurity Review Board's 2024 report on Volt Typhoon noted the campaign's "unprecedented scope and sophistication in mapping critical infrastructure dependencies" - strongly suggesting AI-assisted analysis of infrastructure interdependencies.

12.7.4 Iran:

Documented Capabilities:

- 2012 Shamoon attacks on Saudi Aramco (though IT-focused)
- 2013 dam control system compromise in New York
- Increasing sophistication in targeting water and energy infrastructure

AI Adoption:

- Iran's 2019 National AI Strategy explicitly mentions cybersecurity applications
- Sanctions limitations on commercial AI access push toward indigenous development
- Likely integrating open-source AI tools (LLMs, automated exploit frameworks)

Assessment: Iran represents the "mid-tier" threat actor rapidly gaining capabilities through AI adoption. What required elite teams in 2015 is increasingly accessible through AI tools.

12.7.5 North Korea:

Documented Capabilities:

- Lazarus Group's evolution from destructive attacks (Sony 2014) to revenue-generation (WannaCry ransomware aspects, cryptocurrency theft)
- 2014 Korea Hydro & Nuclear Power compromise

AI Adoption:

- Resource constraints drive maximum automation
- Cryptocurrency theft operations fund acquisition of commercial AI tools
- Focus on monetization over physical disruption (for now)

12.7.6 AI integration in ransomware:

Current ransomware groups are incorporating AI for:

- **Target selection**: AI analyzes financial records, insurance policies, operational criticality to optimize ransom demands
- **Lateral movement**: Automated discovery and exploitation of OT networks after initial IT compromise
- **Data exfiltration**: AI identifies high-value operational data (process recipes, SCADA configurations) for additional extortion leverage
- **Negotiation**: AI-powered chatbots handle ransom negotiations, optimizing payment extraction

12.7.7 Protocol Exploitation and Man-in-the-Middle

OT Protocol Vulnerabilities:

Industrial protocols were designed for closed, trusted networks:

- **Modbus TCP:** No authentication, no encryption
- **DNP3**: Optional security, rarely implemented
- **Profinet**: Vulnerable to replay attacks
- **OPC UA**: Security features often disabled for "compatibility"
- **IEC 61850**: Complex implementation leads to security gaps

AI-Enhanced Protocol Attacks:

- **Automated Protocol Fuzzing**: AI can:
  - Generate millions of malformed packets to discover crash conditions
  - Identify exploitable state machine vulnerabilities
  - Map undocumented command structures
- **Intelligent Man-in-the-Middle**: AI can:
  - Understand process context to craft believable false sensor readings
  - Inject commands that appear legitimate within operational parameters
  - Gradually manipulate setpoints to avoid threshold alarms
  - Coordinate multi-stage attacks across protocol boundaries

12.8 Adversarial machine learning against OT defenses

12.8.1 The defensive AI paradox:

As organizations deploy AI-based OT security tools (anomaly detection, behavioral analytics), adversaries develop adversarial AI to evade them:

- **Evasion Attacks**: AI generates attack traffic that mimics normal operational patterns:
  - Learns baseline behaviors from reconnaissance
  - Crafts attacks that stay within learned parameters
  - Adapts in real-time to detection responses
- **Poisoning Attacks**: If attackers gain access during model training periods:
  - Inject malicious traffic labeled as "normal"
  - Corrupt baseline models to accept attack traffic
  - Create persistent blindspots in detection systems

- **Model Inversion**: AI can probe defensive systems to reverse-engineer detection logic:
  - Discover what triggers alerts
  - Map detection coverage gaps
  - Optimize attacks for maximum impact with minimum detection probability

Strategic concern: The offensive/defensive AI arms race inherently favors attackers because:

- Attackers can test freely without safety constraints
- Defenders must minimize false positives (attackers don't care about false negatives)
- Single attacker success vs. defender must stop all attacks

12.9 AI-Enabled Orchestration:

AI can coordinate complex, multi-stage attacks across IT/OT boundaries:

1. **Simultaneous Multi-Target Attacks:**
   - AI maps dependencies across interconnected systems
   - Identifies attack sequences with cascading effects
   - Orchestrates timing for maximum disruption (e.g., attacking backup systems before primary systems)
2. **IT/OT Convergence Exploitation:**
   - Modern OT increasingly connected to IT (ERP, MES, cloud analytics)
   - AI can automate lateral movement from IT to OT
   - Combines IT attack techniques (credential theft, privilege escalation) with OT -specific attacks (process manipulation)
3. **Critical Infrastructure Interdependency Attacks:**
   - Power grid → water treatment → communications
   - AI models cascading failures across sectors
   - Optimizes attacks for maximum societal disruption

12.10 Scenario modeling: The U.S. Department of Energy's 2023 exercise "GridEx VI" simulated coordinated attacks on power, water, and communications. After-action reports noted AI would dramatically reduce attack planning time from months to days, enabling adversaries to rapidly adapt to defensive responses.

12.11 Real-world near-miss: The 2021 Texas power crisis, while weather-induced, demonstrated cascading failures across water, power, and communications. AI-armed adversaries could deliberately engineer similar cascades.

12.12 Activation scenarios:

- Mass activation for DDoS against critical infrastructure
- Simultaneous false sensor readings across industrial facilities (spoofing equipment failures)
- Data corruption in safety systems
- Platform for delivering secondary payloads (ransomware, destructive malware)

12.13 Precedent:

- Mirai botnet (2016): Exploited IoT devices for DDoS - primarily consumer devices but demonstrated potential
- Industroyer2 (2022): Targeted Ukrainian energy infrastructure with multi-stage malware

12.14 Why this scenario is concerning:

- IIoT adoption outpacing security maturity
- Many devices deployed in late 2010s/early 2020s now out of vendor support
- Flat network architectures common in rushed IIoT deployments
- AI dramatically reduces time from vulnerability discovery to weaponization

Likelihood: MEDIUM-HIGH within 2-3 years. Technical feasibility exists; primary question is attacker motivation and acceptable risk of global impact.

13. APT Threat Actor Profiles

Country: China

Groups: APT1, APT41, APT10, APT40, APT31

Tactics and goals: industrial espionage, data theft, state espionage, disruption

Chinese APT groups operate with a very high degree of financial autonomy. This means that unlike their North Korean, Russian or even Iranian counterparts, Chinese APT groups do not always have to raise budgetary allocation requests to their parent ministries or departments. This should give you an idea of how unique a threat these groups have become in the last decade.

They are everywhere and their operational depth may even shock a seasoned threat researcher. However, it is the level to which these APTs are integrated with technology and the strategic goals of the Chinese state that place these groups in a separate league altogether. Involuntarily, Chinese APT groups are already playing a key role in influencing cyber defense approaches being fashioned by governments and enterprises alike. Their playbooks and tactics are being studied to develop network architectures and SOPs that can be defended.

In this section, we will take a high-level look at Chinese state backed threat actors APT1, APT41, APT10 APT40 , APT 31 and understand their operational strategies and priorities along with how these groups are leveraging AI to breach their targets and to make sense of a huge volume of stolen data.

13.1 Characteristics of Chinese APT groups

Parameter	Characteristic(s)
Functional autonomy	Low: All groups are strictly controlled by the Ministry of State Security. The 14th Bureau responsible for technical reconnaissance is the primary designated body of control. While the operations are broadly assigned by (or through) the 14th bureau, some reporting teams are allowed a little wriggle room to try out new tactics to breach designated targets. The functional autonomy is purely dependent on the success logged by the APT group in the past.

Parameter	Characteristic(s)
Use of AI	China has been using AI for domestic surveillance since a while and a natural fallout of this was the need for automated data crunching to identify patterns of interest. China linked its domestic surveillance data to "naturalized" LLMs in the last decade and in the process, it was able to evolve by leaps and bounds in the area of AI-driven data processing. Since the pandemic, China shifted its attention to the use of AI to run initial probes on target networks. This included automated pinging, collecting stolen credentials belonging to key employees of target enterprises, developing and manipulating malware and phishing. Since 2023, attacks, data exfiltration and data crunching have all been automated through AI. Teams within the MSS are now experimenting with use of AI for injecting fake data packets in order to poison data sets within breached environments.
Hierarchy	APT 1, 41 and 10 are considered relatively senior and used for high-end projects while other APT groups and sub-groups are used to open or create an opening in case of strategic targets. APT 41 is used by the MSS to also create breach chains that go upstream and downstream. Sub-groups that can manage projects on their own may be upgraded for certain projects. Senior groups like APT 41, 1 and 10 are also tasked with mentoring sub groups as well.
Travel	Employees of these groups are not allowed to travel to other countries except under Chinese diplomatic cover (that is a rare occurrence too). APT 1 and 10 are known to have active knowledge and information exchange programs running with their counterparts in North Korea. We have reasons to believe that North Korean threat actor Lazarus (APT 38) maintains a small presence within China. The presence may indicate a high level of collaboration and joint targeting including payment of royalty or equivalent by Lazarus to an unknown Chinese entity.
Targets	Broadly divided into two categories viz., commercial and strategic. The former has to do with mopping revenue and the second has to do with mopping intelligence and IP. Both are important and groups like APT 41 in fact straddle both worlds. There have been at least two instances of APT 41 monetizing stolen data internally and externally.
Integration with Chinese foreign policy objectives	Complete. This is one area where there is zero ambiguity. From a classification perspective, nations and targets are classified as per advisories issued by the Chinese government. There is a feedback loop that is active as well, with the information stolen from targets being used to shape foreign policy interventions and methods.
Handlers	Each group while reporting into Bureau 14 also has a MSS designated handler or manager who is primarily responsible for supervising operations, holding briefings and reporting on projects to the Central Political and Legal Affairs Commission (CPLC) of the Chinese Communist Party. There is also a reporting line that includes local MSS entities but this relationship is not very clear as of now. The handlers are accountable for the operational aspects and are personally held responsible for the threat actors attaining their targets. Interestingly, the CPLC also has a proxy or a shadow supervisor embedded in the chain to keep an eye on the activities of the group and to validate the information shared by the handler.

Parameter	Characteristic(s)
What do these groups do with stolen data?	Part of this question has already been answered. Here is the other part: · All data is first crunched and analyzed using AI algorithms, primarily with machine learning and Deep Learning. These are used to process large data sets by learning from the data. These algorithms built or developed or otherwise is able to handle unstructured data, like text and images, and structured data, like numbers and statistics. The refined data with underlines are marked for the attention of a human analyst. · Data of financial importance or containing industrial IP is marked for attention for commercial action or for negotiation with the victim · Any data of strategic importance is classified, filed and tagged for the attention of a senior analyst · Data that can be weaponized to create further breaches or maintain access to a target environment is handed over to the specific team within the specific threat actor handling that account · The residual data is sent to a common pool accessible to all groups for training · The average data cycle lasts about 28 days



Logos: Ministry of Public Security and Ministry of State Security (source: prcleader.org)

TTP deep-dive

Initial access tactics

13.1.1. Vulnerability Exploitation

Chinese APT groups demonstrate exceptional capability in identifying and exploiting both known and zero-day vulnerabilities in internet-facing infrastructure.

13.2 Network Edge Device Exploitation

Chinese state-sponsored actors have repeatedly exploited publicly known vulnerabilities in network edge devices since at least 2021, focusing particularly on large backbone routers of telecommunications providers, as well as provider edge and customer edge routers. Priority targets include VPN appliances, firewalls, and network management interfaces.

13.3 Most Frequently Exploited CVEs (2023-2025):

- **CVE-2024-21887** - Ivanti Connect Secure and Ivanti Policy Secure web-component command injection vulnerability, commonly chained after CVE-2023-46805 for authentication bypass
- **CVE-2024-3400** - Palo Alto Networks PAN-OS GlobalProtect arbitrary file creation leading to OS command injection, enabling unauthenticated remote code execution
- **CVE-2023-20273 & CVE-2023-20198** - Cisco IOS XE software web management user interface vulnerabilities, commonly chained for authentication bypass and privilege escalation to achieve root access
- **CVE-2018-0171** - Cisco IOS and IOS XE Smart Install remote code execution vulnerability

A typical entry point is via vulnerable external-facing servers, including exploits in Microsoft Exchange and VPN appliances. Groups frequently chain multiple exploits to achieve full system compromise.

13.4 Zero-Day Capabilities

Chinese APT groups are believed to have the capability to identify and develop their own zero-day exploits while also taking advantage of publicly disclosed vulnerabilities and exploits. While public zero-days are less common, these actors demonstrate rapid weaponization of newly disclosed vulnerabilities.

13.5 Spear phishing Operations

Spear phishing remains a primary initial access vector for Chinese APT groups, characterized by extensive reconnaissance and highly targeted social engineering.

13.5.1 Spear phishing Characteristics:

APT40 typically poses as a prominent individual who is probably of interest to a target to send spear phishing emails, including pretending to be a journalist, an individual from a trade publication, or someone from a relevant military organization or non-governmental organization. In some instances, groups leverage previously compromised email addresses to send spearphishing emails, increasing perceived legitimacy.

APT41 often relies on spear phishing emails with attachments, such as compiled HTML (.chm) files, to initially compromise their victims. Other common attachment types include:

- Microsoft Office documents with malicious macros
- ZIP, RAR, and ISO archive formats containing malware
- Screensaver executable (SCR) files
- PDF documents with embedded exploits

13.5.2 Recent TTP Evolution:

In March 2024, Stately Taurus (Mustang Panda) switched tactics by employing an executable with a screensaver file extension for initial infection, departing from their typical reliance on file archive formats.

13.6 Supply Chain Compromises

Chinese APT groups increasingly target supply chains, software development pipelines, and managed service providers to gain access to downstream victims.

13.6.1 Web Hosting Provider Targeting:

Recent campaigns have specifically targeted web hosting services to gain access to multiple customer networks simultaneously. Chinese APT groups exploit known vulnerabilities on unpatched servers exposed to the internet for initial access to web hosting providers.

13.6.2 Strategic Web Compromises (Watering Hole Attacks)

Chinese APT groups are known to use strategic web compromises in order to passively exploit targets of interest, identifying vulnerable public-facing web servers on victim networks and uploading web shells to gain access.

13.7. PERSISTENCE MECHANISMS

13.7.1 Web Shell Deployment

Web shells represent one of the most prevalent persistence mechanisms across Chinese APT operations.

Common Web Shell Families:

- **China Chopper** - Lightweight web shell widely shared among Chinese APT groups, providing remote access and command execution capabilities
- **Custom web shells** - Deployed under different applications and folders to evade detection
- **Godzilla web shell** - Advanced web shell with encrypted communications

The threat actors commonly deploy web shells for persistent access to compromised networks. These web shells are particularly dangerous for organizations as they remain in the compromised systems even if the vulnerable assets are patched. Adversaries often deploy multiple web shells under different applications and folders, requiring thorough threat-hunting to remove all artifacts.

13.7.2 Legitimate Tool Abuse and DLL Sideloading

Chinese APT groups extensively employ DLL sideloading as a persistence and defense evasion technique.

13.7.3 DLL Sideloading Process:

A legitimate VipreAV component was used by attackers for DLL-sideloading to install a loader, a technique previously used by China-linked threat actors including Space Pirates and Earth Longzhi (an APT41 sub-group).

The script's primary function was to deploy two files to the Windows directory: a legitimate Windows binary and a malicious dynamic-link library (DLL), a classic example of DLL sideloading where an attacker places a malicious DLL in a location where a legitimate program will search for it.

13.7.4 Commonly Abused Legitimate Applications:

- KeyScrambler.exe (anti-keylogging software)
- VipreAV components
- Microsoft IME binaries
- Various signed system utilities

13.7.5 VPN Client Persistence

Chinese APT groups use the SoftEther VPN client to achieve persistence and later access systems via remote desktop protocol, with indications of using SoftEther over a two-year period in some compromised environments.

13.7.6 Bootkit and Rootkit Deployment

For high-value targets, Chinese APT groups deploy advanced persistence mechanisms:

APT41 has deployed rootkits and Master Boot Record (MBR) bootkits on a limited basis to hide their malware and maintain persistence on select victim systems.

The Demodex rootkit operates at the kernel level deep within Windows to hide the malware's presence from detection tools, using novel techniques to load unsigned drivers by abusing features from a signed driver from Cheat Engine software.

13.7.7 Network Device Modification

Once inside, Chinese state-sponsored actors modify router configurations to secure persistent access, including altering Access Control Lists to allow traffic from attacker-controlled IP addresses and exposing services on both standard and non-standard ports.

13.8 Credential Dumping Operations

Chinese APT groups employ multiple techniques for extracting credentials from compromised systems:

13.8.1 NTDS.dit Extraction:

If an actor can exfiltrate the ntds.dit and SYSTEM registry hive, the entire domain should be considered compromised, as the actor will generally be able to crack the password hashes for domain user accounts, create their own accounts, and join unauthorized systems to the domain.

13.8.2 Credential Harvesting Techniques:

- Kerberoasting attacks to obtain valid domain credentials
- Dumping credentials, JSON Web Tokens (JWTs), and MFA tokens from compromised appliances
- TACACS+ protocol targeting for network device authentication
- Living-off-the-land tools like ntdsutil and PowerShell

13.8.3 Living Off the Land (LOTL) Techniques

A defining characteristic of recent Chinese APT operations, particularly Volt Typhoon, is the extensive use of legitimate system tools.

Volt Typhoon rarely uses malware in their post-compromise activity. Instead, they rely on living-off-the-land commands to find information on the system, discover additional devices on the network, and exfiltrate data.

13.8.4 Common LOTL Binaries Used:

- **wmic** - Windows Management Instrumentation Command-line
- **ntdsutil** - Active Directory database utility
- **netsh** - Network shell utility
- **PowerShell** - Windows automation framework
- **cmd.exe** - Command prompt
- Native SSH/SFTP clients

This tactic avoids endpoint detection and response programs which would alert on the introduction of third-party applications to the host, and limits the amount of activity captured in default logging configurations.

13.9 LATERAL MOVEMENT

13.9.1 Network Reconnaissance

Chinese APT groups conduct extensive reconnaissance using both custom tools and legitimate utilities:

They conducted network reconnaissance using basic system commands and exfiltrated sensitive data by compressing it into encrypted archives before transmitting it to remote servers.

13.9.2 Reconnaissance Tools and Techniques:

- SNMP enumeration for network device discovery
- Web application security scanners
- Open-source tools like Impacket for Active Directory enumeration
- Custom network mapping utilities

13.9.3 Lateral Movement Techniques

13.9.3.1 Protocol-Based Movement:

Following initial access, the APT actors target protocols and infrastructure involved in authentication-such as Terminal Access Controller Access Control System Plus (TACACS+) -to facilitate lateral movement across network devices, often through SNMP enumeration and SSH.

13.9.3.2 Pivoting Infrastructure:

Chinese APT actors leverage open source multi-hop pivoting tools, such as STOWAWAY, to build chained relays for command and control and operator access, including interactive remote shells, file upload and download, SOCKS5/HTTP proxying, and local/remote port mapping with support for forward and reverse connections over encrypted node-to-node links.

13.9.4.2 Custom Tools:

- Fast Reverse Proxy (FRP) - Custom variants with hardcoded C2 callbacks
- Earthworm - Tunneling tool for pivoting through compromised systems
- SoftEther VPN - For establishing persistent network bridges

13.10 COMMAND AND CONTROL INFRASTRUCTURE

13.10.1 SOHO Router Botnet Infrastructure

One of the most sophisticated TTP innovations from Chinese APT groups involves using compromised small office/home office routers as intermediate infrastructure.

The actor has leveraged compromised small office/home office network devices as intermediate infrastructure to obscure their activity by having much of the command and control traffic emanate from local ISPs in the geographic area of the victim.

13.10.2 KV-Botnet Operation:

Volt Typhoon used privately-owned SOHO routers infected with the "KV Botnet" malware to conceal the PRC origin of further hacking activities directed against U.S. critical infrastructure. This technique provides plausible deniability and makes attribution more difficult.

13.10.3 Custom C2 Protocols

Chinese APT groups employ diverse C2 mechanisms:

Backdoor C2 Characteristics:

GhostSpider is a multi-modular backdoor communicating over encrypted TLS channels with C2 servers, using fake media file headers to hide traffic.

Common C2 Ports:

- Standard ports: 8080, 8443, 8000
- Custom ports: 8043, 10443
- Protocols: SSH, SFTP, RDP, FTP, HTTP, HTTPS

13.10.4 Shared Infrastructure Among Groups

Phantom Taurus uses a shared Chinese APT operational infrastructure that has been exclusively used by Chinese threat actors, including Iron Taurus (APT27), Starchy Taurus (Winnti) and Stately Taurus (Mustang Panda).

The sharing of tools among groups has been a long-standing trend among Chinese threat actors, making it difficult to say which specific group is behind a set of activities.

13.11 MALWARE ARSENALS

13.12 Modular Backdoors and RATs

13.12.1 ShadowPad:

ShadowPad is a highly modular remote access trojan commonly linked to Chinese threat actors, deployed alongside Cobalt Strike in sophisticated campaigns. ShadowPad is shared among multiple Chinese APT groups and represents one of their most capable platforms.

13.12.2 Custom Backdoor Families:

- **Crowdoor** - Custom malware written in C++ targeting Windows environments, including Cisco network devices, used for persistent access and network sniffing
- **GhostSpider** - Multi-modular backdoor with encrypted TLS C2 communications
- **SNAPPYBEE & MASOL RAT** - Additional modular backdoors used for broader espionage tasks and targeting Linux platforms
- **Kazuar** - Sophisticated backdoor used by multiple Chinese groups
- **Cobalt Strike** - Widely adopted legitimate penetration testing framework used as a staple backdoor implant

13.12.3 Web Shells

- China Chopper - Ubiquitous lightweight web shell
- Godzilla - Advanced web shell with encryption capabilities
- Custom variants - Tailored to specific victim environments

13.12.4 Rootkits and Kernel-Mode Malware

Demodex Rootkit is a Windows kernel-mode rootkit that hides malware artifacts such as files, registry keys, and network traffic, using novel techniques to load unsigned drivers.

13.12.5 Custom Tool Suites

13.12.6 NET-STAR Malware Suite:

Phantom Taurus uses the NET-STAR malware suite, which includes components like AssemblyExecuter, a .NET assembly designed for executing other .NET assemblies directly in memory without writing them to disk.

13.12.6 EggStreme Framework:

The EggStreme framework is a sophisticated new malware toolset used by China-linked APT groups for long-term espionage and surveillance, with the primary focus on achieving persistent access.

13.12.7 Shared Malware Families

Chinese APT groups demonstrate extensive tool sharing:

At least seven non-public tools (BADSIGN, FIELDGOAL, FINDLOCK, PHOTO, SCANBOX, SOGU, and WIDETONE) are shared with other suspected China-nexus operators.

13.12.8 Common Shared Tools:

- PlugX/SOGU
- Cobalt Strike
- Impacket framework
- Mimikatz
- China Chopper
- Potato suite (privilege escalation)

13.13 DATA EXFILTRATION AND COLLECTION

13.13.1 Encryption and Staging

Volt Typhoon issues commands via the command line to collect data, including credentials from local and network systems, put the data into an archive file to stage it for exfiltration, and then use the stolen valid credentials to maintain persistence.

13.13.2 Exfiltration Methods:

In at least one instance, Chinese APT actors utilized GRE and MPLS tunnels to move data back to China. This demonstrates advanced understanding of network protocols to blend exfiltration with legitimate traffic.

13.13.3 Custom SFTP Clients

The APT actors use a custom SFTP client, which is a Linux binary written in Golang, to transfer encrypted archives from one location to another, with some variants having the additional capability of collecting network packet captures on the compromised network.

13.14 DEFENSE EVASION TECHNIQUES

13.14.1 Living Off the Land

A hacking technique known as "Living Off the Land" is being used to compromise critical networks by permitting undetected intrusions into critical systems, where hackers use privileged access credentials and pre-position themselves in networks until they are ready to attack.

13.14.2 Log Modification and Anti-Forensics

Adversaries modify log files to cover their tracks and hinder the incident response process.

Chinese APT actors use guestshell disable and guestshell destroy commands to deactivate and uninstall Guest Shell container and return all resources to the system, effectively removing evidence of their activities.

13.14.3 Traffic Obfuscation

Volt Typhoon tries to blend into normal network activity by routing traffic through compromised SOHO devices, making detection challenging as the traffic appears to originate from legitimate local ISPs.

13.14.4 Fileless Execution

AssemblyExecuter accepts assembly bytecode as input parameters, loads it using the .NET Assembly.Load() method and invokes the assembly's entry point, enabling threat actors to dynamically load and execute additional functionality after a compromise without writing files to disk.

13.15.1. OPERATIONAL PATTERNS AND TRADECRAFT

13.15.1 Working Hours and Operational Tempo

Chinese APT groups demonstrate consistent operational patterns aligned with Chinese business hours and holidays:

Researchers observed a distinct lull coinciding with the Lunar New Year and the Chinese mandated "Special Working Day", with working hours consistent with business hours on weekdays adjusted to UTC +08:00 (China Standard Time).

13.15.2 Long-Term Persistence

Microsoft assesses with moderate confidence that the Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises.

Volt Typhoon's operations indicate a long-term strategy to maintain covert access across lifeline sectors to disrupt these key services during a crisis.

13.15.3 Hands-On-Keyboard Activity

Once Volt Typhoon gains access to a target environment, they begin conducting hands-on-keyboard activity via the command line. Some of these commands appear to be exploratory or experimental, as the operators adjust and repeat them multiple times.

13.15.4 Adaptability and Resilience

Following an FBI disruption of their malware botnet, Volt Typhoon swiftly rebuilt its infrastructure, highlighting the group's commitment to its objectives and its capacity to sustain prolonged campaigns.

13.16 TARGETING PRIORITIES

13.16.1 Critical Infrastructure Focus

Primary sectors targeted:

People's Republic of China state-sponsored cyber threat actors are targeting networks globally including telecommunications, government, transportation, lodging, and military infrastructure networks.

APT40 has targeted governmental organizations, companies, and universities in a wide range of industries—including biomedical, robotics, and maritime research—across the United States, Canada, Europe, the Middle East, and the South China Sea area, as well as industries included in China's Belt and Road Initiative.

13.17 Strategic espionage objectives

13.17.1 Economic and Technology Theft:

Wu's CNE activities resulted in the theft of trade secrets, intellectual property, and other high-value information from companies and organizations in the United States and abroad, as well as from multiple foreign governments.

13.17.2 Maritime domain focus:

APT40 was targeting the maritime industry, reflecting China's strategic interest in naval dominance and maritime trade routes, targeting research institutions, universities, and private companies involved in naval technology and maritime research.

13.17.3 Pre-Positioning for Disruption

The Intelligence Community assesses that Volt Typhoon's targeting of these companies carries limited espionage potential, and is instead part of an effort to prepare to disrupt U.S. infrastructure.

The PRC may attempt to launch large-scale cyberattacks against lifeline sectors to slow US military mobilization in response to a conflict involving the US and China, particularly over Taiwan.

13.18. NOTABLE TTP VARIATIONS

13.18.1 APT41 (Dual Mission Approach)

APT41 has been observed using at least 46 different code families and tools. In a campaign running almost a year, APT41 compromised hundreds of systems and used close to 150 unique pieces of malware, including backdoors, credential stealers, keyloggers, and rootkits.

APT41 uniquely combines state-sponsored espionage with financially motivated cybercrime, representing a hybrid threat model.

13.18.2 APT40/Leviathan (Maritime Specialist)

APT40 is an Advanced Persistent Threat linked to the Chinese Ministry of State Security, specifically to the Chinese Ministry of State Security Hainan State Security Department, active since 2013 and recognized for state-sponsored espionage campaigns.

Distinctive APT40 TTPs:

- Use of Secure Socket Funnelling (SSF) for remote command execution
- Multiple web shell deployment strategy
- Focus on maritime, defense, and aerospace sectors

13.19 Volt Typhoon (Infrastructure Pre-Positioning)

Volt Typhoon has been active since mid-2021 and has targeted critical infrastructure organizations in Guam and elsewhere in the United States, with affected organizations spanning the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors.

13.19.1 Distinctive Volt Typhoon Characteristics:

- Almost exclusive reliance on LOTL techniques
- SOHO router botnet infrastructure
- Minimal malware usage post-compromise
- Focus on pre-positioning rather than immediate data theft

13.19.2 Salt Typhoon (Telecommunications Specialist)

Salt Typhoon, a Chinese state-sponsored APT active since 2020 and linked to China's Ministry of State Security, has intensified activities in 2024 with a primary focus on the telecommunications sector, exploiting zero-day vulnerabilities to maintain long-term persistence in compromised systems.

The fact that Salt Typhoon successfully targeted over 600 organizations across 80 countries in 2024 alone required an extreme amount of inside knowledge and resources.

13.19.3 Stately Taurus/Mustang Panda (Government Focus)

Stately Taurus (Mustang Panda) has been operating since at least 2012 and routinely conducts cyberespionage campaigns, historically targeting government entities and nonprofits, as well as religious and other nongovernmental organizations across North America, Europe and Asia.

Distinctive Characteristics:

- DLL sideloading using legitimate software
- Archive-based delivery mechanisms (ZIP, RAR, ISO)
- Government and NGO targeting
- Alignment with Chinese geopolitical events

13.20 STRATEGIC ASSESSMENT

13.20.1 Organizational Backing

The APT actors' malicious operations have been linked to multiple China-based entities, including at least Sichuan Juxinhe Network Technology Co. Ltd., Beijing Huanyu Tianqiong Information Technology Co., Ltd., and Sichuan Zhixin Ruijie Network Technology Co., Ltd.

These front companies provide operational support and technical capabilities to Chinese intelligence services.

13.20.2 Evolution of Tactics

13.20.2.1 From Malware to LOTL:

The shift from traditional malware-heavy operations to living-off-the-land techniques represents a significant tactical evolution driven by improved defensive capabilities in target environments.

13.20.2.2 From Espionage to Pre-Positioning:

In contrast to the espionage activity typically associated with similar groups, Volt Typhoon demonstrates an operational emphasis on stealth, persistence, and disruption preparedness.

13.20.2.3 Collaborative Ecosystem

While many Chinese APTs employ common tools such as China Chopper and the Potato suite, some groups like Phantom Taurus distinguish themselves through unique, custom-developed TTPs that enable highly covert, persistent operations.

The Chinese APT ecosystem demonstrates:

- Extensive tool and infrastructure sharing
- Coordinated targeting aligned with national interests
- Specialization by sector and objective
- Shared development of common capabilities

The link between Chinese state and these actors gets reinforced each time there is a major political upheaval in China. In 2021 and 2022, during major political events in China, the footprint of these threat actors shrunk dramatically. APT 41 was in fact notably absent for almost a month during both occasions. So how do we explain such a gap in operations during times of political turbulence?

- The Ministry of State Security may be redeploying some of the resources on internal projects
- The MSS may have been ordered to standdown while the turbulence settles
- The MSS, being a government agency, is just waiting for guidance from above

Because of a very high level of convergence of state objectives with the functional priorities of Chinese threat actors, these groups are among the most dangerous state-backed threat actors across countries.

13.21 Country: Russia

Russia operates one of the most sophisticated and aggressive state-sponsored cyber espionage and sabotage programs in the world. Unlike many nation-state actors who specialize in specific missions, Russian cyber operations span the full spectrum of activities: intelligence collection, destructive attacks, influence operations, and electoral interference. These operations are orchestrated by multiple intelligence agencies, each with distinct mandates, tradecraft, and operational priorities.

As of January 2026, Russian cyber operations have evolved to support the Kremlin's geopolitical objectives, particularly in relation to the ongoing conflict in Ukraine and broader strategic competition with Western nations. This analysis examines the primary Russian state-backed threat actors, their organizational affiliations, capabilities, and recent operations.

13.21.1 APT29 (Cozy Bear) - SVR Foreign Intelligence Service

Organizational Affiliation

APT29 operates under Russia's Foreign Intelligence Service (SVR), confirmed through surveillance operations by Dutch and American intelligence services. The group has been active since at least 2008 and represents one of Russia's premier cyber espionage units.

Aliases

Cozy Bear, The Dukes, Midnight Blizzard, NOBELIUM, Dark Halo, Cloaked Ursa, UNC2452, StellarParticle, Office Monkeys, YTTRIUM

Primary Objectives

APT29 conducts strategic intelligence collection aligned with Russian foreign policy interests. The group conducts cyber espionage campaigns to gather intelligence that aligns with Russian geopolitical objectives, targeting governments, defense contractors, and international organizations.

Key Characteristics

Stealth and Persistence: APT29 does not rush in through the front door, nor make its mark by leaving a calling card—they sneak in, stay until needed, and leave with precisely what they came for. The group is known for maintaining long-term access to target networks, sometimes for years, while avoiding detection.

Cloud-First Tradecraft: APT29 has moved beyond its usual methods of gaining initial access and is directly targeting victims' via cloud services. The group has adapted to the migration of enterprise systems to cloud environments, developing sophisticated techniques to compromise Microsoft 365, Azure, and other cloud platforms.

Identity-Based Attacks: The group increasingly exploits trust relationships in the cloud -consent phishing, malicious app registrations, and token lifecycles-because those vectors are harder for defenders to trace end-to-end.

Notable Operations

SolarWinds Supply Chain Attack (2020): The group compromised the software development pipeline of SolarWinds and embedded the SUNBURST malware into routine updates of the Orion network administration tool, infiltrating thousands of organizations on a massive scale. This operation demonstrated unprecedented sophistication in supply chain compromise.

Microsoft Corporate Email Breach (2024): In December 2024, password spraying allowed access to Microsoft's corporate environment and senior leadership mailboxes. This intrusion targeted what Microsoft knew about APT29's operations, turning the compromise into potential downstream access across Microsoft's customer base.

TeamViewer Compromise (2024): German technology company TeamViewer SE reported on June 28, 2024, its corporate IT network had been compromised by Cozy Bear.

Recent Cloud-Focused Campaigns (2024-2025): APT29 compromised legitimate websites and injected malicious JavaScript code that redirected visitors to actor-controlled domains designed to trick people into entering device codes into Microsoft account sign-in pages.

Tactics, Techniques, and Procedures (TTPs)

Initial Access:

- Spearphishing with sophisticated lures impersonating legitimate organizations
- Exploitation of cloud service vulnerabilities
- Password spraying campaigns against enterprise accounts
- Residential proxies to obscure malicious connections, making traffic appear to originate from IP addresses within ISP ranges used for residential broadband customers

Malware Arsenal:

- Custom tools including SUNBURST/Solorigate, EnvyScout, BoomBox, GoldMax, TrailBlazer, MiniDuke, SeaDuke, CozyDuke, and CosmicDuke
- Starting in February 2024, they added WINELOADER to their array of downloaders, which is injected into legitimate executables via DLL-sideloading
- MagicWeb for maintaining access to compromised Windows networks

Persistence:

- OAuth application abuse and refresh tokens to entrench themselves inside cloud tenant environments

  Golden SAML attacks to impersonate users
- DLL sideloading to hide inside legitimate processes

Command and Control:

- Encrypted HTTPS traffic disguised as normal web services, often using trusted cloud platforms like Microsoft 365, Azure, and Google Drive

Current Threat Assessment

APT29 will continue to carry out supply chain-style intrusions, target governments, NGOs and critical sectors while refining identity-based tradecraft. The group shows no signs of slowing down and continues to adapt to defensive measures by exploiting emerging technologies and trust relationships in cloud environments.

13.21.2 APT28 (Fancy Bear) - GRU Military Intelligence

Organizational Affiliation

APT28 is formally attributed to the 85th Main Special Service Center (85th GTsSS), military unit 26165 of Russia's military intelligence agency, the GRU. The group represents the GRU's primary cyber espionage capability.

Aliases

Fancy Bear, Sofacy, Pawn Storm, Sednit, STRONTIUM, Forest Blizzard, BlueDelta, FROZENLAKE, TG-4127, Swallowtail, Fighting Ursa, TA422

Primary Objectives

The group targets aerospace, defense, energy, government, media, and dissidents, using sophisticated and cross-platform implants. APT28's profile closely mirrors Russian military intelligence strategic interests.

Key Characteristics

Operational Tempo: APT28 has demonstrated the ability to run multiple and extensive intrusion operations concurrently, enabling the group to maintain pressure across numerous targets simultaneously.

Adaptability: The group is characterized by its ever-evolving toolset, showing the ability to compromise networks of high-profile agencies and institutions through simple but convincing phishing emails and self-developed malware.

Ukraine-Focused Operations: Since late February 2022, as Russian military forces failed to meet objectives and Western countries provided aid to Ukraine, unit 26165 expanded targeting of logistics entities and technology companies involved in aid delivery.

Notable Operations

Democratic National Committee Breach (2016): APT28 compromised the Democratic National Committee and other related organizations, stealing and leaking sensitive information in one of their most notorious attacks.

World Anti-Doping Agency (2016): The group infiltrated WADA's database, releasing medical data of numerous Olympic athletes.

Logistics and Technology Campaign (2022-Present): For over two years, the group has conducted campaigns using reconstituted password spraying capabilities, spearphishing, and modification of Microsoft Exchange mailbox permissions. The hackers accessed legitimate municipal traffic cameras as well as private cameras at key locations near border crossings, military installations, and rail stations to track the movement of materials into Ukraine.

Ukrainian Defense Supply Chain Targeting (2023-2024): The campaign, ongoing since at least 2023, has taken advantage of spearphishing and cross-site scripting vulnerabilities in webmail software products, targeting email accounts of high-ranking Ukrainian officials and executives at defense contractors who sell weapons to Kyiv.

"Nearest Neighbor" Wi-Fi Attack (2024): This campaign involved the use of nearby Wi-Fi networks for covert system access, using password spraying and credential harvesting.

Tactics, Techniques, and Procedures (TTPs)

Initial Access:

- Spearphishing campaigns involving emails containing malicious attachments (Microsoft Office documents, RAR archives) or links to malicious websites
- Password spraying capabilities, targeting enterprise credentials
- Cross-site scripting vulnerabilities in webmail software including Roundcube, Horde, MDaemon and Zimbra
- Zero-day exploitation

Extensive Malware Arsenal: APT28 employs diverse malware including ADVSTORESHELL, Cannon, CHOPSTICK, CORESHELL, DealersChoice, Downdelph, Drovorub, Fysbis (Linux backdoor), JHUHUGIT, Koadic, Komplex (macOS Trojan), LoJax (UEFI rootkit), Mimikatz, Responder, and USBStealer.

Credential Harvesting:

- Exploitation of legitimate system tools for credential dumping
- Use of tools like Certipy, Get-GPPPassword.py, and ldap-dump.py for Active Directory enumeration

Current Operations

Victims in 2024 alone included officials from regional national governments in Ukraine, Greece, Cameroon and Serbia, military officials in Ukraine and Ecuador, and employees of defense contracting firms in Ukraine, Romania and Bulgaria.

13.21.3 APT44 / Sandworm - GRU Unit 74455

Organizational Affiliation

Sandworm is operated by Military Unit 74455, a cyberwarfare unit of the GRU's Main Center for Special Technologies (GTsST). In 2024, given the active and persistent threats Sandworm posed to governments and critical infrastructure operators globally, Mandiant "graduated" Sandworm into a named Advanced Persistent Threat: APT44.

Aliases

Sandworm, Voodoo Bear, Telebots, IRIDIUM, Seashell Blizzard, Iron Viking, ELECTRUM, TEMP.Noble, Blue Echidna, FROZENBARENTS

Primary Objectives

APT44 stands apart in how it has honed capabilities in espionage, attack, and influence operations and sought to integrate them into a unified playbook over time. Unlike most state-backed groups that specialize in one mission, APT44 conducts the full spectrum of cyber operations.

Key Characteristics

Destructive Capability: Then-United States Attorney Scott Brady described the group's cyber campaign as "representing the most destructive and costly cyber-attacks in history".

Critical Infrastructure Focus: Unlike a typical APT focused on espionage, the distinguishing feature of Sandworm is its ability to sabotage at scale. The group specializes in targeting industrial control systems and operational technology.

Coordination with Military Operations: Through disruptive cyber tools such as wiper malware, APT44 has sought to impact critical infrastructure sectors, with operations at times coordinated with conventional military activity, such as kinetic strikes or other forms of sabotage.

Notable Operations

Ukraine Power Grid Attacks (2015-2016): The team is believed to be behind the December 2015 Ukraine power grid cyberattack, marking the first publicly acknowledged cyberattack to cause a power outage. The group repeated this in 2016 with increased sophistication.

NotPetya Global Cyberattack (2017): The group conducted the 2017 cyberattacks on Ukraine using the NotPetya malware, which became one of the most costly cyber incidents in history, causing over $10 billion in global damages.

2018 Winter Olympics Disruption: During the opening ceremony of the Winter Olympics in Pyeongchang, South Korea, hackers launched a cyberattack and successfully disrupted IT infrastructure including Wi-Fi, televisions, RFID-based security gates, and the official Olympics app.

Ukraine War Operations (2022-Present): Throughout Russia's war, APT44 has waged a high intensity campaign of cyber sabotage inside Ukraine, deploying disruptive cyber tools such as wiper malware to impact critical infrastructure sectors. In April 2022, the group attempted a power blackout in Ukraine using an updated Industroyer2 malware variant.

Western Critical Infrastructure Campaign (2021-Present): Amazon Threat Intelligence attributed a persistent multi-year cyber espionage campaign targeting Western critical infrastructure, particularly the energy sector, to the group, with operations spanning from 2021 through the present day. The threat group simplified operations earlier this year by shifting away from vulnerability exploitation to focus on misconfigured network edge devices hosted on Amazon Web Services.

Tactics, Techniques, and Procedures (TTPs)

Initial Access:

- Spearphishing campaigns, exploitation of edge vulnerabilities, and supply chain compromises
- Exploiting customer misconfigured devices, particularly exposed network appliances

Destructive Malware: Custom malware families such as NotPetya, BlackEnergy, Industroyer, and Industroyer2, designed to wipe data, disrupt systems, or directly manipulate industrial control systems. Sandworm developed newer wiper families, including AcidPour, to not only wipe but exfiltrate sensitive military and telecommunication information.

Living Off The Land: The group employs LOTL techniques to blend into normal network activity and establish persistence.

Infrastructure Hijacking: Sandworm has close ties with CyberArmyofRussia_Reborn, a 'hacktivist' persona that recently claimed to have targeted US and Polish water utilities as well as a French dam.

Evolution and Current Threat

Operational Shift: As the war has endured, APT44's relative focus has transitioned away from disruption to intelligence collection, with increasing emphasis on espionage activity intended to provide battlefield advantage to Russia's conventional forces.

Battlefield Support: One long-running APT44 campaign has assisted forward-deployed Russian ground forces to exfiltrate communications from captured mobile devices in order to collect and process relevant targeting data.

Global Reach: Due to its history of aggressive use of network attack capabilities, APT44 presents a persistent, high severity threat to governments and critical infrastructure operators globally where Russian national interests intersect.

13.21.4 GRU Unit 29155 - Emerging Cyber-Kinetic Integration Unit

Organizational Affiliation

Cyber actors affiliated with the Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) are responsible for computer network operations against global targets for espionage, sabotage, and reputational harm since at least 2020. FBI, NSA, and CISA assess Unit 29155 is responsible for attempted coups, sabotage and influence operations, and assassination attempts throughout Europe.

Aliases

Unit 29155, GRU 161st Specialist Training Center

Key Characteristics

Cyber-Kinetic Integration: Unit 29155 represents a unique fusion of traditional GRU sabotage operations with cyber capabilities. These cyber actors are separate from other known and more established GRU-affiliated cyber groups, such as Unit 26165 and Unit 74455.

Junior Personnel: FBI assesses the Unit 29155 cyber actors to be junior active-duty GRU officers under direction, suggesting this may be a training or developmental unit for future cyber operations.

Notable Operations

WhisperGate Campaign Against Ukraine (2022): GRU Unit 29155 cyber actors began deploying the destructive WhisperGate malware against multiple Ukrainian victim organizations as early as January 13, 2022. WhisperGate has two stages that corrupts a system's master boot record, displays a fake ransomware note, and encrypts files based on certain file extensions.

Global Espionage Campaign: The analysis provides insight into Unit 29155 cyber actor infrastructure used for network scanning, password compromising, and data exfiltration against Ukraine, NATO members in Europe and North America, and countries in Latin America and Central Asia.

Tactics, Techniques, and Procedures (TTPs)

Infrastructure: Since at least 2020, Unit 29155 cyber actors have used virtual private servers to host operational tools, perform reconnaissance, exploit victim infrastructure, and exfiltrate victim data.

Tools:

- The actors used multiple Discord accounts to store malware files, including development versions or iterations of the binaries
- Use of Meterpreter and Netcat for reverse shells
- Use of Impacket tools
- Pass-the-Hash attacks via ProxyChains

Data Exfiltration: In one instance following WhisperGate deployment, Unit 29155 cyber actors exfiltrated data to mega[.]nz using Rclone.

13.21.5 Turla (Snake) - FSB Center 16

Organizational Affiliation

Turla is a cyber espionage threat group attributed to Russia's Federal Security Service (FSB), specifically to Center 16 of the FSB, Russia's main signals intelligence (SIGINT) agency. The FBI and DOJ officially confirmed that Turla works for the FSB's Center 16 group in Ryazan, outside Moscow.

Aliases

Snake, Uroburos, Venomous Bear, Waterbug, WhiteBear, Krypton, Secret Blizzard, IRON HUNTER, Pensive Ursa, BELUGASTURGEON, Blue Python, SUMMIT

Primary Objectives

The group has compromised victims in over 50 countries since at least 2004, spanning government, embassies, military, education, research and pharmaceutical industries. Turla conducts long-term strategic intelligence collection for Russian state interests.

Key Characteristics

Longevity and Sophistication: Turla is a Russian-based threat group operating since at least 2004, which is linked to the Russian Federal Security Service. First emerging in 2003, the malicious tool has been used by the Turla group for attacks against various targets of interest, including NATO member governments.

Infrastructure Hijacking: The group has a history of hijacking other threat actors' infrastructure for its own purposes. In October 2019, the U.K. and U.S. governments revealed Turla's exploitation of an Iranian threat actor's backdoors to advance their own intelligence requirements.

Recent Third-Party Infrastructure Exploitation: Starting in December 2022, Secret Blizzard gained access to Storm-0156 (Pakistani APT) command-and-control servers and by mid-2023 had expanded control to multiple C2s, leveraging Storm-0156 intrusions to deploy custom malware.

Notable Operations

Snake Malware Campaign (2004-2023): For nearly 20 years, Turla used versions of the Snake malware to steal sensitive documents from hundreds of computer systems in at least 50 countries, belonging to NATO member governments, journalists, and other targets of interest. The FBI called Snake the FSB's "most sophisticated cyber espionage tool".

Operation MEDUSA Disruption (2023): The Justice Department announced the completion of Operation MEDUSA to disrupt the global peer-to-peer network of computers compromised by Snake malware, with the FBI deploying a tool named PERSEUS that overwrote vital components of the malware.

Gamaredon Collaboration (2024-2025): In February 2025, ESET detected four different Gamaredon-Turla co-compromises in Ukraine, where Gamaredon deployed a wide range of tools while Turla only deployed Kazuar v3. Both groups are affiliated with the FSB-Gamaredon is operated by officers of Center 18 in Crimea, while Turla is attributed to Center 16.

Diplomatic Mission Targeting (2020-Present): ESET attributed activity with medium confidence to Turla involving deployment of LunarWeb on servers and LunarMail on workstations, persisted as an Outlook add-in, in diplomatic missions.



Tactics, Techniques, and Procedures (TTPs)

Advanced Malware Suite: Top malware in Turla's arsenal includes Capibar, Kazuar, Snake, Kopiluwak, QUIETCANARY/Tunnus, Crutch, ComRAT, Carbon, HyperStack and TinyTurla.

Snake Implant Characteristics: Snake would pull modules needed to perform an FSB operator's bidding, collect sensitive data, and exfiltrate information via a custom, encrypted, and fragmented communication protocol. All systems infected with Snake acted as proxies as part of a larger Snake P2P botnet that helped mask and hide traffic from other Snake attacks.

Email-Based C2: LunarMail uses email messages for command-and-control communications, sharing operational ideas with LightNeuron, another Turla backdoor.

Living Off Compromised Infrastructure: Turla leveraged access to Storm-0156 servers to deploy custom malware families TwoDash and Statuez, and laterally moved to the Pakistani operator's workstation to obtain intelligence on their tooling, C2 credentials, and exfiltrated data.

Current Assessment

Turla remains an active and formidable threat in cyber-espionage, with a long history of successful campaigns against high-value targets, with adaptability, stealth, and persistence making it a dangerous adversary likely to continue targeting organizations worldwide.

13.21.6 Pro-Russia Hacktivist Groups (GRU-Affiliated)

CyberArmyofRussia_Reborn (CARR)

The Russian GRU Main Center for Special Technologies military unit 74455 is likely responsible for supporting the creation of CARR in late February or early March 2022. Actors suspected to be from GRU unit 74455 likely funded the tools CARR threat actors used to conduct distributed denial-of-service attacks through at least September 2024.

Evolution: In late 2023, CARR expanded operations to include attacks on industrial control systems, claiming an intrusion against a European wastewater treatment facility in October 2023 and targeting human-machine interface devices at two U.S. dairy farms in November 2023.

Dissatisfaction and Breakaway: By late September 2024, CARR channel administrators became dissatisfied with the level of support and funding provided by the GRU, leading CARR administrators and a NoName057(16) administrator to create the Z-Pentest group.

Z-Pentest

Established in September 2024, Z-Pentest is composed of members from CARR and NoName057(16), specializing in OT intrusion operations targeting globally dispersed critical infrastructure entities. Unlike other pro-Russia hacktivist groups, Z-Pentest largely avoids DDoS activities, claiming OT intrusions as attempts to garner more attention from the media.

Sector16

Formed in January 2025, Sector16 is a novice pro-Russia hacktivist group that emerged through collaboration with Z-Pentest. Sector16 actively maintains an online presence including a public Telegram channel where they share videos, statements, and claims of compromising U.S. energy infrastructure. Members of Sector16 may have received indirect support from the Russian government in exchange for conducting specific cyber operations that further Russian strategic goals.

13.21.7 Russian FSB Center 16 - Network Infrastructure Targeting

Recent Activity (2024-2025)

The FBI detected Russian FSB cyber actors exploiting Simple Network Management Protocol and end-of-life networking devices running an unpatched vulnerability (CVE-2018-0171) in Cisco Smart Install to broadly target entities in the United States and globally. In the past year, the FBI detected actors collecting configuration files for thousands of networking devices associated with US entities across critical infrastructure sectors, with some vulnerable devices having configuration files modified to enable unauthorized access.

13.21.8 Strategic Assessment and Future Outlook

Operational Integration

Russian cyber operations demonstrate increasing integration across different agencies and operational domains:

- **Cyber-Kinetic Coordination**: APT44 operations have at times been coordinated with conventional military activity, such as kinetic strikes or other forms of sabotage, in attempts to achieve joint military objectives.
- **Multi-Agency Collaboration**: The Gamaredon-Turla collaboration demonstrates coordination between different FSB centers (Center 18 and Center 16) for operational purposes.
- **Hacktivist Cover**: Multiple Russian intelligence units use "hacktivist" personas to provide plausible deniability while conducting state-directed operations.

Evolving Tactics

Cloud Migration: APT29 focuses on testing edge and identity infrastructure for new vulnerabilities, searching for zero-day vulnerabilities in VPNs and authentication systems.

Infrastructure Targeting: Sandworm's shift from vulnerability exploitation to targeting misconfigured network edge devices represents a tactical adaptation enabling the same destructive objectives with reduced operational complexity.

Supply Chain Attacks: In one recent case, APT44's access to a software developer resulted in downstream compromise of critical infrastructure networks in Eastern Europe and Central Asia, followed by wiper malware deployment.

Threat Trajectory

Persistent and Escalating: Nothing in analysis suggests a slow down in APT29 operations. All major Russian cyber threat actors continue active operations with no indication of reduced tempo.

Critical Infrastructure Focus: The expansion of targeting against operational technology and industrial control systems, particularly by APT44 and pro-Russia hacktivist groups, represents an escalating threat to critical infrastructure globally.

Electoral and Democratic Targeting: APT44 has repeatedly targeted Western electoral systems and institutions, including those in current and prospective NATO member countries, attempting to interfere with democratic processes by leaking politically sensitive information and deploying malware to access election systems.

14. Major cyberattacks reported in 2025

Date	Attack	Victim	Threat Actor	Impact	What Went Wrong	Remedial Steps Taken
Dec 19-28, 2024 (disclosed Jan 2025)	Data breach via compromised credential	Power School (K-12 education software)	Matthew D. Lane (19-year-old student)	Millions of students and teachers' personal data stolen including names, addresses, SSNs, medical info. Ransom paid but data still used for extortion in May 2025.	Compromised credentials for PowerSource customer support portal. Lack of multi -factor authentication MFA). Maintenance tool allowed broad data access.	Paid ransom (amount undisclosed). Offered credit monitoring via Experian. Improved security protocols. However, threat actors continued extortion attempts despite payment.
Jan 2025 (disclosed Oct)	Ransomware attack	SimonMed Imaging	Medusa ransomware group	Patient data exposed including names, addresses, DOB, medical records, diagnoses, treatment info, health insurance, driver's licenses.	Third-party application vulnerabilities.	Vendor risk mapping recommended. Penetration testing advised. Data-centric encryption implementation.
Jan-Feb 2025	Data breach	Episource	Unknown cybercriminal	Unauthorized party gained access and copied data between Jan 27 - Feb 6, 2025.	Cybercriminal gained unauthorized access to systems.	Incident response engaged. Credit monitoring offered to affected individuals.
Feb 21, 2025	Cryptocurrency theft (largest in history)	Bybit (cryptocurrency exchange)	Lazarus Group / TraderTraitor (North Korea)	$1.5 billion in Ethereum stolen. Largest crypto heist ever. Market impact: ETH dropped 24%, Bitcoin below $90k.	Malicious JavaScript injected into Safe{Wallet} UI via compromised developer machine. Third-party service provider compromised. Lack of security standards for third -party integrations.	FBI issued alerts. Industry-wide tracking of stolen assets. Bybit covered losses, remained solvent. Enhanced security measures implemented. Recovery bounty program (up to 10% of recovered amount).
Easter Weekend, Apr 19-21, 2025	Ransomware attack	Marks & Spencer (UK retail)	DragonForce ransomware / Scattered Spider group	£300 million estimated profit loss. £700+ million wiped from market value. Online shopping suspended for 46 days. Stock systems disrupted.	Third-party supplier compromise (Tata Consultancy Services IT helpdesk). Social engineering attacks tricking helpdesk staff into providing credentials.	Systems isolated. External cybersecurity experts hired. Online ordering gradually restored by June 10. Password resets required. Four individuals arrested in July (ages 17-20).
Late Apr - Early May 2025	Ransomware /data theft	Co-op (UK retail)	Scattered Spider / DragonForce (believed)	Data of all 6.5 million members compromised (names, DOB, contact details). Estimated £206 million in lost sales.	Social engineering of employee. Password reset attack. Active Directory compromise.	Quickly disconnected IT systems, preventing full ransomware deployment. Notified members. Confirmed financial information not accessed.

Date	Attack	Victim	Threat Actor	Impact	What Went Wrong	Remedial Steps Taken
May 1, 2025	Cyberattack attempt / Data breach (Sep 2025)	Harrods (luxury retailer)	DragonForce (April), Unknown (September)	April: Minimal operational impact. September: 430,000 customer records stolen (names, emails, phone numbers, marketing preferences).	April: Targeted as part of UK retail campaign. September: Third-party provider system compromised.	April: Restricted internet access at all sites. September: Customer notifications sent. Assured payment details and passwords not compromised.
May 25-26 2025	Cybersecurity incident	Victoria's Secret	Unknown (no group claimed responsibility)	Corporate systems and e-commerce site taken offline. Q1 earnings report delayed. Some in-store services disabled.	Attack timed during Memorial Day weekend (staff shortages).	Systems taken offline proactively. Physical stores remained open. No material impact to fiscal 2025 expected.
May 2025	Ransomware attack	Southeast Asian energy provider	NightSpire group	Control systems disabled for 18 days. $8 million ransom demanded.	Targeted attack on industrial control systems.	Incident contained.
Jun 5, 2025	Ransomware attack	United Natural Foods Inc. (UNFI)	Unknown	Supply chain disruption across North America. Bread shortages at Whole Foods. Stock plunged 17.3% ($292 million market value loss).	Critical systems vulnerability.	Affected systems taken offline. Q1 earnings delayed. Not expected to materially impact fiscal 2025.
Jun 2025	Ransomware attack	McLaren Health Care (Michigan)	Unknown	743,000+ patient records compromised. Second major attack in two years.	Healthcare system vulnerabilities.	Credit monitoring offered. Enhanced security protocols.
Jul 2025	DDoS attacks disrupted	Pro-Russian hacktivist group	Various European law enforcement	DDoS attacks on Ukraine and NATO countries.	Ongoing cyber warfare operations.	Europol operation led to arrests in France and Spain. Warrants issued for six Russian nationals.
Aug 2025	Cyberattack	Norway dam (Bremanger)	Russia (formally attributed)	Brief seizure of dam control. No physical damage but aimed to create fear/chaos.	Exploitation of dam control systems.	Incident formally attributed to Russia.
Aug 2025	Data breach	Canada's House of Commons	Unknown (exploited Microsoft vulnerability)	Employee data and government device details exposed.	Microsoft vulnerability exploited.	Warning issued about potential use in scams /impersonation.

Date	Attack	Victim	Threat Actor	Impact	What Went Wrong	Remedial Steps Taken
Aug-Sep 2025	Ransomware attack	Jaguar Land Rover (JLR)	Scattered Lapsus$ Hunters (Scattered Spider, ShinyHunters, Lapsus$)	£1.9 billion estimated cost (most economically damaging UK cyber incident). Productio halted for 5 weeks. 5,000+ businesses in supply chain affected. Full recovery expected Jan 2026.	Third-party supplier software vulnerabilities. Lateral movement into core systems.	Manufacturing sites in UK, Slovakia, Brazil temporarily shut down. Full manufacturing operations restarted in October but recovery ongoing.
Sep 2025	Ransomware attack	Asahi (Japanese brewing giant)	Qilin ransomware group	Operations in Japan suspended. 27 GB of files stolen (claimed).	System failure due to cyberattack.	Operations gradually restored.
Sep 2025	Supply chain attack via Salesforce/ Salesloft Drift	Multiple global organizations (700+)	ShinyHunters	Potentially 1.5 billion records exposed (claimed). Stolen tokens leveraged. Called "SolarWinds moment for SaaS."	Compromise of Salesloft Drift integrations with Salesforce. Insufficient validation of third-party SaaS integrations.	Ongoing investigation across global enterprises. Enhanced SaaS security policy discussions.
Sep 2025	Third-party data breach	Volvo Group (North America)	Ransomware group	870,000 records leaked across vendor's client base via HR software provider Miljödata.	Third-party HR software provider (Miljödata) compromised.	Vendor risk assessments recommended. Enhanced third-party monitoring.
Oct 2025	Zero-day exploitation	Oracle E-Business Suite users (GlobalLogic, Barts Health NHS, others)	Clop hackers	Large number of organizations targeted. Patient data and corporate systems compromised.	CVE-2025-61882 zero-day vulnerability. Exploited alongside other flaws.	Oracle released emergency patch on Oct 5. Enhanced monitoring for Oracle systems.
Oct 2025	Data breach	Red Hat (GitLab instance)	Crimson Collective	570 GB compressed data exfiltrated. 28,000+ internal repositories accessed. 800+ Customer Engagement Reports stolen including VPN settings, API keys, credentials.	Self-managed GitLab instance compromised.	Incident investigation ongoing. AWS environment security review. Cloud credential management improvements.
Throughout 2025	Ongoing espionage	Salt Typhoon telecommunications campaign	China (state-aligned)	Multiple major telecom providers in US, Canada compromised. Military networks including US National Guard breached.	Unpatched Cisco network devices. Privileged access abuse. Custom telecom malware.	Continued investigation. Enhanced telecom security measures. International coordination.

Source: Published data

Major vulnerabilities disclosed in 2025

ID	Alternative ID	Exploitation	CVSS	Product	Vendor	Description
EUVD-2025-34162	CVE-2025-40755	0.04%	v4.0: 8.7	SINEC NMS	Siemens	A vulnerability in SINEC NMS (All versions < V4.0 SP1) allows SQL injection via the endpoint. An authenticated low-privileged attacker could insert data and escalate privileges. (ZDI-CAN-26570)
EUVD-2025-197785	CVE-2025-40834	0.03%	v4.0: 6.8	Mendix RichText	Siemens	A vulnerability in Mendix RichText (All versions ≥ V4.0.0 < V4.6.1) where input is not properly neutralized, enabling potential cross-site scripting attacks.
EUVD-2025-197784	CVE-2025-40936	0.02%	v4.0: 7.3	PS/IGES Parasolid Translator Component	Siemens	An out-of-bounds read in PS/IGES Parasolid Translator Component (All versions < V29.0.258) when parsing crafted IGS files could cause a crash or allow code execution. (ZDI-CAN-26755)
EUVD-2025-197610	CVE-2025-11918	Not available	v4.0: 7.1	Arena® Simulation	Rockwell Automation	Rockwell Automation Arena® contains a stack-based buffer overflow in DOE file parsing. Local attackers can exploit this to potentially execute arbitrary code by tricking a user into opening a malicious DOE file.
EUVD-2025-84346	CVE-2025-11084	0.02%	v4.0: 7.6	FactoryTalk® DataMosaix™ Private Cloud	Rockwell Automation	A vulnerability in DataMosaix™ Private Cloud allows bypassing MFA during setup, granting a valid login-token cookie without the user's password if MFA is enabled but not completed within 7 days.
EUVD-2025-84347	CVE-2025-11085	0.07%	v4.0: 8.6	FactoryTalk® DataMosaix™ Private Cloud	Rockwell Automation	Persistent XSS vulnerability in DataMosaix™ Private Cloud allows injection and execution of malicious JavaScript, potentially leading to account takeover, credential theft, or redirection attacks.
EUVD-2025-84345	CVE-2025-11862	0.04%	v4.0: 8.4	Verve Asset Manager	Rockwell Automation	A vulnerability in Verve Asset Manager allows unauthorized read-only users to read, update, and delete users via the API.
EUVD-2025-84343	CVE-2025-11696	0.02%	v4.0: 8.9	Studio 5000® Simulation Interface™	Rockwell Automation	Local SSRF vulnerability via the API allows any Windows user to trigger outbound SMB requests, enabling capture of NTLM hashes.
EUVD-2025-84342	CVE-2025-11697	0.02%	v4.0: 8.9	Studio 5000® Simulation Interface™	Rockwell Automation	Local code execution vulnerability via API path traversal allows any Windows user to extract files, leading to script execution with Administrator privileges on system reboot.
EUVD-2025-131908	CVE-2025-11567	0.01%	v4.0: 7.3	PowerChute Serial Shutdown	Schneider Electric	CWE-276: Incorrect Default Permissions could result in elevated system access if the installation folder is not properly secured.
EUVD-2025-131907	CVE-2025-11566	0.08%	v4.0: 6.9	PowerChute Serial Shutdown	Schneider Electric	CWE-307: Improper Restriction of Excessive Authentication Attempts allows an attacker on the local network to brute-force credentials via unlimited attempts on /REST/shutdownnow.

ID	Alternative ID	Exploitation	CVSS	Product	Vendor	Description
EUVD-2025-131906	CVE-2025-11565	0.02%	v4.0: 7.3	PowerChute Serial Shutdown	Schneider Electric	CWE-22: Path Traversal in POST /REST /UpdateJRE allows a Web Admin on the local network to escalate system access.
EUVD-2025-21130	CVE-2025-50123	0.05%	v4.0: 7.2	EcoStruxure T Data Center Expert	Schneider Electric	CWE-94: Code Injection vulnerability allows remote command execution by a privileged user exploiting hostname input when accessed via console.
EUVD-2025-38356	CVE-2025-11972	0.03%	v3.1: 4.9	Tag, Category, and Taxonomy Manager – AI Autotagger with OpenAI	stevejburge	WordPress plugin vulnerable to SQL Injection via post_types parameter up to version 3.40.0; requires Editor+; can extract sensitive DB info.
EUVD-2025-199815	CVE-2025-30186	0.03%	v3.1: 5.4	OX App Suite	Open-Xchange GmbH	Malicious uploaded files may trigger script execution via attacker-controlled links; enables sensitive data exfiltration.
EUVD-2025-199814	CVE-2025-30190	0.03%	v3.1: 5.4	OX App Suite	Open-Xchange GmbH	Malicious office document content may inject script during editing, enabling account-context actions and data exfiltration.
EUVD-2025-199813	CVE-2025-59025	0.03%	v3.1: 6.1	OX App Suite	Open-Xchange GmbH	Malicious email content may execute script; sanitization bypass previously possible; updated to prevent exploitation.
EUVD-2025-199812	CVE-2025-59026	0.03%	v3.1: 5.4	OX App Suite	Open-Xchange GmbH	Malicious uploaded files can trigger script execution when following attacker links; enables account-context actions.
EUVD-2025-37318	CVE-2025-30189, GHSA-396v-898v-98hg	0.04%	v3.1: 7.4	OX Dovecot Pro	Open-Xchange GmbH	Cache misconfiguration causes wrong user auth mapping; logins after cache hit authenticate as same user.
EUVD-2025-199018	CVE-2025-65956, GHSA-7j46-f57w-76pj	0.03%	v3.1: 6.5	formwork	get formwork	CMS vulnerability: stored XSS in blog tags.
EUVD-2025-199607	CVE-2025-21621, GHSA-w66h-j855-qr72	0.04%	v3.1: 6.1	geoserver	geoserver	Reflected XSS in WMS GetFeatureInfo HTML format.
EUVD-2025-199606	CVE-2025-58360, GHSA-fjf5-xgmq-5525	0.05%	v3.1: 8.2	geoserver	geoserver	Unauthenticated XXE via WMS GetMap feature.
EUVD-2025-198990	CVE-2025-65944, GHSA-6465-jgvq-jhgp	0.04%	v4.0: 5.1	sentry-javascript	getsentry	Sensitive headers leaked when sendDefaultPii=true.
EUVD-2025-199799 (entry 2)	CVE-2025-12151	0.03%	v3.1: 6.4	Simple Folio	Press Tigers	Stored XSS via portfolio_name, versions ≤ 1.1.0; Subscriber+ can inject scripts.
EUVD-2025-199632	CVE-2025-34350	0.24%	v4.0: 8.7	UnForm Server	Synergetic Data Systems	Unauthenticated arbitrary file read + SMB coercion in arcendpoint; can leak files or NTLM hashes.
EUVD-2012-6570	CVE-2012-10026	61.73%	v4.0: 10	WordPress Plugin Asset-Manager	Asset-Manager	Unauthenticated arbitrary file upload → remote code execution.

ID	Alternative ID	Exploitation	CVSS	Product	Vendor	Description
EUVD-2024-51148	CVE-2024-12847	75.23%	v3.1: 9.8	DGN1000	Netgear	Auth bypass → root OS command execution via setup.cgi; exploited in the wild.
EUVD-2024-21151	CVE-2024-23690	0.58%	v3.1: 7.2	FVS336Gv3	Netgear	Telnet command injection via util backup _configurationcommand.
EUVD-2025-198465	CVE-2025-66082	0.03%	v3.1: 4.3	WpEvently	mage people team	Missing authorization allows privilege abuse ≤ 5.0.4.
EUVD-2025-198464	CVE-2025-66083	0.03%	v3.1: 4.3	WpEvently	mage people team	Same missing authorization flaw as above.
EUVD-2025-20764	CVE-2025-34077	84.71%	v4.0: 10	Pie Register (WordPress)	Genetech Solutions	Auth bypass → impersonate any user → plugin upload → RCE.
EUVD-2025-198469	CVE-2025-66075	0.03%	v3.1: 4.2	WP Cookie Notice (GDPR/CCPA)	WP Legal Pages	Missing authorization allows privilege abuse ≤ 4.0.3.
EUVD-2025-36196	CVE-2025-12351, GHSA-8crg-fp2w-xqgv	Not available	v3.1: 6.8	S35 AI Cameras	Honeywell	Auth bypass via user controller key → privilege escalation.
EUVD-2023-44347	CVE-2023-3712	0.07%	v3.1: 6.6	PM45	Honeywell	Files accessible → privilege escalation; update to MR19.5.
EUVD-2023-44346	CVE-2023-3711	0.26%	v3.1: 6.4	PX45/65	Honeywell	Session fixation vulnerability → credential falsification.
EUVD-2023-44345	CVE-2023-3710	90.77%	v3.1: 9.9	PM42	Honeywell	Improper input validation → command injection.
EUVD-2025-21065	CVE-2025-3947	0.14%	v3.1: 8.2	C200E	Honeywell	Integer underflow → DoS; affects multiple Experion PKS modules.
EUVD-2025-21064	CVE-2025-3946	0.28%	v3.1: 8.2	FIM4	Honeywell	Wrong handler deployment → packet mishandling → RCE.
EUVD-2025-21063	CVE-2025-2523	0.27%	v3.1: 9.4	C300 PCNT05	Honeywell	Integer underflow → communication channel manipulation → RCE.
EUVD-2025-21066	CVE-2025-2522	0.05%	v3.1: 6.5	FIM4	Honeywell	Sensitive information in resource → data leakage → misbehavior.
EUVD-2025-21068	CVE-2025-2520	0.14%	v3.1: 7.5	FIM8	Honeywell	Uninitialized variable → DoS via pointer dereference.
EUVD-2025-21067	CVE-2025-2521	0.27%	v3.1: 8.6	FIM8	Honeywell	Memory buffer over-read → remote code execution.
EUVD-2025-13247	CVE-2025-2605, GHSA-4p7f-6rw5-m5v7	0.14%	v3.1: 9.9	MB-Secure	Honeywell	OS command injection → privilege abuse; update required.
EUVD-2025-199803	CVE-2025-3784	0.01%	v3.1: 5.5	GX Works2	Mitsubishi Electric	Credentials stored in plaintext → sensitive info disclosure.
EUVD-2025-197931	CVE-2025-10089	0.01%	v3.1: 7.7	MILCO.S Setting Application	Mitsubishi Electric	DLL hijacking via uncontrolled search path during installation.
EUVD-2025-37980	CVE-2025-10259	0.02%	v3.1: 5.3	MELSEC iQ-F FX5UJ-60MT/ESS	Mitsubishi Electric	TCP packet handling flaw → DoS of attacked connection.

ID	Alternative ID	Exploitation	CVSS	Product	Vendor	Description
EUVD-2025-29683	CVE-2025-9818	0.02%	v3.1: 6.7	PowerAct Pro (Slave Agent)	OMRON Social Solutions	Unsafe service paths (CWE-428) → malicious file execution.
EUVD-2025-21287	CVE-2025-1384	0.08%	v3.1: 7.0	NX-series Controller	OMRON	Least privilege violation → remote unauthorized code execution.

Source: European Union Vulnerability Database https://euvd.enisa.europa.eu/

15. State of OT Security

15.1 Common ICS/SCADA/PLC ports exposed to the internet

Accessibility of OT devices from the internet is becoming a major source of concern for asset owners from an infrastructure security standpoint. In most of these instances, the asset owners are not even aware of the accessibility of these ports from outside their network. This creates a cyber risk for the organizations that are hosting the devices that are accessible from external networks. Some of these risks include:

- Data breach
- Operational shutdowns
- DDoS attacks
- Device manipulation
- Extension of maintenance windows
- Misuse of networks
- Third party litigation
- Production and output risks
- Manipulation of privileges

Industrial Control Systems (ICS) that include SCADA systems, PLCs, RTUs, HMIs, and data historians rely on a variety of specialized communication protocols. Many of these protocols were designed some time ago, with little or no security considerations, and were intended for isolated networks.

However, with the increasing convergence of IT and OT networks and misconfigurations in perimeter defenses, numerous ICS ports are now directly exposed to the public internet, introducing serious security risks.

Common ICS protocols such as Modbus (TCP/502), DNP3 (TCP/20000), Siemens S7 (TCP/102), BACnet (UDP/47808), EtherNet/IP (TCP/44818), and OPC UA (TCP/4840) are frequently observed in internet-wide scans. Many of these services:

- Lack authentication or encryption by design
- Provide sensitive process information or allow control commands
- Are exposed unintentionally due to poor segmentation or misconfigured firewalls

Real-world data gathered from an discovery, ping and analyze project run by Shieldworkz researchers confirms that thousands of ICS devices are reachable online. Many of these are running with default configurations or known vulnerabilities and without any restrictions and are therefore visible during scans.

Further, the exposure of these ports:

- Violates ICS security best practices (e.g., ISA/IEC 62443, NIST SP 800-82)
- Increases the risk of unauthorized access, espionage, ransomware, and sabotage
- Provides an attack surface for both opportunistic and targeted threats (e.g., APTs)

15.2 Research intent

We undertook this research in order to improve awareness about exposed ICS systems. While many asset owners are taking strong steps to prevent inadvertent or unmonitored device and network access, a lot needs to be done. Lack of asset visibility and cyber hygiene are creating opportunities to access critical systems from outside.

To give you an idea of the magnitude of the problem, our research team was able to engage over 9000 ICS devices within 12 minutes of project initiation.

15.3 Interesting considerations

- There could be multiple ports open across protocols in the same organization
- The more pervasive a protocol, more are the devices accessible
- Maximum number of honeypots are today run with very minimal attempt being made to mask their intent

Research methodology

Our research team worked to scan the application layers spread across ports to identify the devices connected with them. This enables us to bypass restrictions imposed by active port scanning methods. This also helps the scanning process establish handshakes and establish connections. The application layer also adds another level of validation to detect and avoid honeypots that have willingly left ports open for engaging various types of traffic of interest. Generic studies often do not account for the application layer activity which impairs the quality of findings and confidence in the results. Lack of application layer analysis also leads to honeypots being treated as genuine ICS environments.

In addition to the application layer scans, we are also using various attributes to isolate ports of interest with a very high degree of confidence. We have not considered exposed devices and ports from environments of low confidence to increase the accuracy of our research. Data gathered was also validated with data from public search engines to further improve the accuracy of our research effort.

The focus of this research paper is not on honeypots. Instead wherever possible we have by process of validated elimination removed suspected honeypots that are emulating protocols from this study. Having honeypots dilutes the research and may take us to the wrong assumptions and conclusions. Further, honeypots also increase the number of exposed devices leading to a wrong impression about the number of exposed devices.

There is also a possibility of threat actors running some of these honeypots to engage threat researchers. The volumes of honeypots identified by us with a high level of confidence is in the range of 32-35 percent of all ports discovered.

In all, devices hosting applications on ports that responded to pings within networks that were verifiable were identified and shortlisted for this study. The pings and online discovery mechanism were triggered two more times:

a) To validate the primary findings
b) To see if any of the ports are closed or the gaps addressed (or how long does it take to close an open port or block an accessible device)
c) To see how these ports behave on days when the operations are not running such as Sundays
d) To note any change in the application behaviour during the period of the study

15.4 Blindfold test and validation

A) Lastly, we also used the triggering mechanism to detect and identify our own honeypots that are presently operational in over 80 cities. In the blindfold test, we were able to identify a majority of our honeypots with near high level of confidence across all attempts. Many of the honeypots however evaded detection indicating the effectiveness of our honeypots. During the actual project, we excluded our honeypots from this study by turning them off regionally for the duration of the scans

B) In another study, we reached out to the operators of a suspected honeypot. This was a honeypot run by an ISP to validate our findings.

Positive validation on both counts boosted our confidence in our approach. However, we do not make any claims on the data being entirely error free. The findings should be treated as a snapshot of the overall levels of accessibility that OT infrastructures afford to researchers and threat actors alike.

Various types of honeypots, characteristics and reason for disqualification

Honeypot type and/or detection mechanism	Characteristic	Decision
Open ports with very less traffic or activity	Potential generic honeypot (high level of confidence)	Dropped from study
Unusually large number of open ports (100s or even thousands)	Potential honeypot	Dropped from study
ICS environments simulated by honeypot software part of large honeypot installations running other simulations	Potential honeypot run by an ISP or other authorized entity	Dropped from study
Honeypots detected that are running on open source honeypot frameworks (excluding Conpots and T-Pots)	A definitive honeypot	Dropped from study
Conpot based honeypots	A definitive honeypot	Dropped from study
T-Pots	A definitive honeypot	Dropped from study
Honeypots with zero application layer activity (no handshakes) and zero returns. The host disconnects without offering a return response.	Possible passive listening honeypots	Dropped
Honeypots detected via fingerprinting including errors in emulation		Dropped
Honeypots with default configuration		Dropped
Unidentifiable protocol emulation		Dropped after verification
Multiple unrelated protocols on the same device		Dropped after verification

All the hosts that do not meet the above criteria are finally tagged as systems of interest for further studies.

15.5 Visualizing the methodology

- Primary data capture
- First level validation with open source scanning platforms
- Second level validation
- Final list

Common protocols and the associated ports

ANSI C12.22	1153
BACNet	47808
Beckhoff-ADS communication	48898
Crimson 3	789
DNP3	20000
Danfoss ECL apex	5050
EtherCAT	34980
EtherNet/IP	2222
FATEK FB Series	500
GE-SRTP	18245
HART-IP	5094
HITACHI EHV Series	3004
ICCP	102
IEC 60870-5-104	2404
IEC 61850 / MMS	102
KEYENCE KV-5000	8501
KOYO Ethernet	28784
LS Fenet	2004/5
MELSEC Q	5006/5007
Modbus/TCP	502
Moxa	4800
Niagara Tridium Fox	1911,4911
OMRON FINS	9600
PCWorx	1962
Panasonic FP (Ethernet)	9094
Panasonic FP2 (Ethernet)	8500
Quick Panel GE	57176
SAIA S-BUS (Ethernet)	5050
Siemens S7	102
Simatic	161
Unitronics Socket1	20256/7
Yokogawa FA-M3 (Ethernet)	12289

15.6 OT Protocol Exposure Snapshot across stages

Triggered protocol	Primary scan Hosts	Countries	Validation from open source search engines	Countries	Final validation scan	Countries
MODBUS	76,390	126	65033	126	77,901	129
FOX	33,632	97	23551	97	21007	98
EIP	22098	86	17353	86	21034	86
IEC 60870-5-104	11010	61	7678	61	11777	61
S7	9455	59	8136	59	8222	59
ATG	13119	42	6109	44	12165	44
WDBRPC	5000	44	3855	48	7287	48
CODESYS	4722	53	4187	53	5195	53
FINS	2018	56	2091	59	2521	59
OPC UA	1934	65	1077	65	1945	65
DNP3	606	31	401	31	606	31
PCWORX	568	22	506	22	561	22
PRO CON OS	566	13	209	13	566	13
MMS	43	10	51	10	43	10
GE SRTP	15	6	22	6	15	6
HART	7	3	19	3	6	3
Others	17008	76	22534	49	22176	41
Total	2,03,182		154940		1,99,960	

15.7 Country-wide exposure data across top nations with most exposed ports

Country	Majorly accessible protocol	Number of ports accessible from external network (across protocols) during first scan	Number of ports accessible during final validation
USA	Modbus, Fox	76343	61092
China	Fox, Modbus	36544	39882
Canada	BACnet, Modbus	31398	30022
UK	Fox, Modbus	19,151	13855
Germany	Modbus, BACnet,Fox	19,090	18043
Vietnam	Modbus, Bacnet	14,409	14630
Russia	IEC 60870-5-104	13,676	13734
Japan	Modbus, Bacnet	11099	11001
India	WDBRPC, Modbus, S7	7901	8109
Singapore	EIP, Fox, Modbus	5666	6028

The data reveals a significant issue: critical infrastructure systems, which should be isolated, are widely exposed to the external network. This exposure represents a major security risk, making these systems potential targets for cyberattacks. The "first scan" and "final validation" shows that this is a dynamic situation, with some countries improving their security posture while others are becoming more vulnerable over time.

15.8 Observations

- US, China, Canada and UK host the maximum number of ports accessible from the internet across protocols
- The high number of exposures across common protocols indicates that many of these devices have ports that have been left open inadvertently
- MODBUS, FOX and BACNET are among the most accessible protocols. One of the reasons could be their widespread use
- In some countries, the number of accessible protocols reduces by the time we run the final scan. This indicates that the port has been blocked or rendered inaccessible. Though it is possible that the final scans hit the port during a maintenance window when the internet connectivity was barred or limited.
- The USA Has the Highest Exposure: The United States has, by far, the highest number of accessible ports. However, the number decreased significantly (by over 15,000) between the two scans, suggesting that there may have been a concerted effort to secure these systems.
- Exposure is Growing in Some Nations: China, Vietnam, Russia, India, and Singapore all saw an increase in the number of accessible ports. This is a worrying trend, indicating a growing attack surface in these countries. China's increase is particularly notable, making it the second most exposed country in this list.
- Some Countries Are Reducing Exposure: The USA, Canada, UK, Germany, and Japan all managed to reduce the number of exposed ports. The UK, in particular, had a substantial percentage decrease, closing over 5,000 ports.
- Modbus is a Universal Problem: The Modbus protocol is listed for nearly every country. This is a major concern because Modbus is a very old protocol with virtually no built-in security features. Its widespread accessibility is a significant vulnerability.
- Specific Critical Protocols Are Exposed: The presence of protocols like IEC 60870-5-104 (primarily in Russia) and S7 (in India) is alarming. These are used in critical sectors like electrical utilities (IEC-104) and industrial automation (Siemens S7), and their exposure could have serious real-world consequences.



Geographic locations of OT network ports accessible from the internet

15.9 Recommendations

Minimize/eliminate internet-facing OT exposure

The most critical first step is to remove direct internet connections to any OT device. The port counts in your data indicate a widespread failure of this fundamental principle.

Action: Conduct a thorough asset inventory and external network scan to identify all internet -facing devices. Immediately place these devices behind firewalls and remove public IP addresses.

Guidance:

- NERC CIP-005 (Electronic Security Perimeters): Requires defining and protecting the Electronic Security Perimeter (ESP) to prevent unauthorized inbound and outbound traffic. No device using protocols like Modbus, DNP3, or S7 should ever be directly on the internet.
- NIST SP 800-82: Explicitly advises against direct internet connectivity for ICS and recommends using demilitarized zones (DMZs) for any required data exchange.

Implement network segmentation and segregation

Once external exposure is removed, you must prevent lateral movement within your network. An attacker who gains a foothold in the IT network should not be able to easily pivot to the OT environment.

Action: Segment your network into distinct security zones based on criticality and function. Use firewalls and access control lists (ACLs) to strictly control all traffic flowing between these zones.

Guidance:

- IEC 62443 (Zones and Conduits): This is the foundational standard for this practice. Group assets with similar security requirements into "Zones" and define controlled communication pathways called "Conduits." All traffic passing through a conduit must be inspected and filtered.
- NIS2 Directive: Emphasizes supply chain security and risk management. Proper segmentation ensures that a compromise at a less critical vendor or partner network doesn't cascade into your most critical control systems.

Harden devices and mitigate insecure protocols

Your data shows a high prevalence of insecure-by-design protocols like Modbus, Fox, and S7. Since you often can't replace the underlying devices, you must add compensating controls.

Action:

- Protocol-Aware Firewalls: Use deep packet inspection (DPI) firewalls that understand OT protocols to block unauthorized commands or function codes (e.g., block all write commands from unauthorized sources).
- Secure Gateways/Proxies: For legacy protocols, use a secure gateway that can convert the insecure protocol to a modern, encrypted one for any necessary remote communication.
- Disable Unused Ports: Physically or logically disable all unused ports on controllers, switches, and servers within the OT environment.

Guidance:

- IEC 62443-4-2: Provides technical security requirements for IACS components, including hardening measures and session controls.
- NIST Cybersecurity Framework (CSF): The "Protect" function (PR.AC-3, PR.PT-3) calls for implementing access control and ensuring system components are protected from tampering.

Implement continuous network and security monitoring

You cannot protect what you cannot see. The data suggests a lack of visibility into what is happening on these networks.

Action: Deploy an OT-native network monitoring solution. This is not just about security but also about operational reliability. The tool should be able to baseline "normal" traffic and alert on anomalies.

Guidance:

- NERC CIP-015 (Internal Network Security Monitoring): As discussed previously, this standard mandates a program to detect, evaluate, and respond to anomalous network activity inside your trusted perimeter.
- NIST CSF (Detect function): Focuses on implementing capabilities to identify cybersecurity events in a timely manner. This requires continuous monitoring and anomaly detection.

Develop and practice a cyber Incident Response Plan

Given the high level of exposure, you must assume a breach is possible and be prepared to respond.

Action: Develop an OT-specific incident response (IR) plan. This plan must be different from an IT IR plan; you cannot simply shut down a power plant or manufacturing line. The plan should be tested through tabletop exercises and simulations involving both engineering and security staff.

Guidance:

- NERC CIP-008 (Incident Reporting and Response Planning): Requires a formal plan to identify, classify, and respond to cybersecurity incidents.
- NIS2 Directive: Mandates strict incident reporting timelines (an initial warning within 24 hours). A well-practiced IR plan is essential to meet this requirement.

Disclaimer

- While every attempt has been made to eliminate honeypots, it is impossible to eliminate every single honeypot out there. It is possible that highly advanced honeypots designed to engage sophisticated threat actors and advanced honeypots run by threat actors to engage low signal traffic may have made its way into this study.
- Some of the attributes such as geolocation may not be entirely accurate.
- At no point was any data belonging to an individual collected or processed by us. PIIs and credentials or any data that was accidently retrieved (if any) was eliminated conclusively within 8 hours as part of our standard data retention protocol.

16. Dissecting major cyber incidents of 2025

16.1 Jaguar Land Rover

A major cyberattack threw Jaguar Land Rover (JLR) into turmoil, forcing a complete halt to its global vehicle production since the end of August 2025. The incident, which has been described as a "digital siege," has had a significant financial impact on the British luxury carmaker and its extensive supply chain, with production now paused until at least the beginning of October 2025.

The attack, which targeted the company's IT systems, has effectively paralyzed JLR's manufacturing capabilities worldwide. The company has been forced to repeatedly extend the production shutdown as it works with cybersecurity experts and law enforcement to investigate the breach and ensure a secure restart of its operations.

The financial fallout from the incident is substantial, with estimates suggesting the production stoppage cost JLR millions of pounds daily with the final estimate ranging from over a billion pounds to 2.5 Billion Pounds. The ripple effect is still being felt acutely throughout the automotive supply chain, with many smaller suppliers who are heavily reliant on JLR facing significant financial distress and potential job losses. The UK government has been urged to intervene and provide support to affected workers and businesses.

While JLR has not officially disclosed the specifics of the attack, reports have linked it to a ransomware group. The hackers are believed to have gained access to the company's internal systems, disrupting everything from manufacturing to vehicle diagnostics and parts ordering.

What went wrong?

As per sources and Jaguar Land Rover, the incident began with the company discovering an “unauthorized intrusion” in its network. The intrusion was discovered when some anomalous activity was noticed on a peripheral network and reported by an employee. Jaguar Land Rover then initiated a series of measures as part of its incident response policy to contain the intrusion including:

- Shutting down systems
- Blocking access and privileges to impacted systems
- Shutting down production lines with connected systems
- Launching an internal investigation
- Engaging external agencies for a more detailed forensic investigation

Root cause analysis

The origins of the attack can be traced back to a social engineering/Vishing campaign that threat actor ShinyHunters ran a few months ago. ShinyHunters is known to target well known brands globally across campaigns. The group began its activities by targeting known vulnerabilities across cloud applications and restricted use databases and then decided to change tracks when it realized its activities were not yielding the level of results it sought for.

ShinyHunters, in association with another threat actor Scattered Spider, then began going after large scale corporate database managers in order to get more relevant data and credentials. Scattered Lapsus$ Hunters (AKA SCATTERED SP1D3R HUNTERS AKA THE COMHQ) a group within ShinyHunters decided to use the database stolen by ShinyHunters to run large scale ransomware campaigns targeting major global brands. It is one of these very campaigns that contributed to this attack on Jaguar Land Rover.

Scattered Lapsus$ Hunters is nothing but another brand identity of ShinyHunters and possibly a rebranded variant of AlphV. The constant rebranding is designed to keep law enforcement agencies busy chasing empty trails. In fact, when one analysis the communications of these three threat groups, there is very little effort being placed in disguising their common origin.

It could very well be that these 3 groups are not just sharing members but are also operating under a single banner under a single set of masterminds. Since Scattered Lapsus$ Hunters also operates a Ransomware-as-a-service, it is possible that stolen credentials are being actively traded by this group.

Scattered Lapsus$ Hunters has also placed a ransom threat to Google asking them to fire two key security researchers and abandon an ongoing investigation against them or risk a potential dataleak. They are also known to run campaigns on social media to determine their next targets. A recent campaign had them asking followers to indicate if they wanted to target the world's largest beverage company and a food delivery service in India. Both these companies have been subsequently targeted by the group.

TTP

- First level or initial access: Deployment of OAuth apps using trial accounts followed by compromised accounts from unrelated orgs.
- Vishing and targeted social engineering: Calling key employees using AI generated voice samples and by mimicking helpdesk/support
- Data theft: Exfiltration is done via engineered Python scripts that mimic DataLoader ops.
- Infrastructure used: Vishing calls are routed through VPN IPs while data is transferred through TOR exit nodes.
- Threats: First level of threats could be simple and direct followed by a demand for immediate payment made to the CEO of the victim enterprise

Attack timeline

Data from previous attacks carried out by Scattered Lapsus$ Hunters and other threat actors was used to conduct an attack on certain segments of Jaguar Land Rover infrastructure. In addition, a vishing attack was used to compromise The CRM attack exposed common credentials that were then used to access and manipulate applications using VPN-based access.

Once the attack succeeded, the threat actor went about following its TTP playbook to move across the JLR's network and escalate privileges across one or more key applications. Several queries for data theft were then deleted using TOR IP addresses. TOR traffic may have been blended with regular traffic to avoid detection. Data was also possibly exfiltrated via TOR exit nodes.

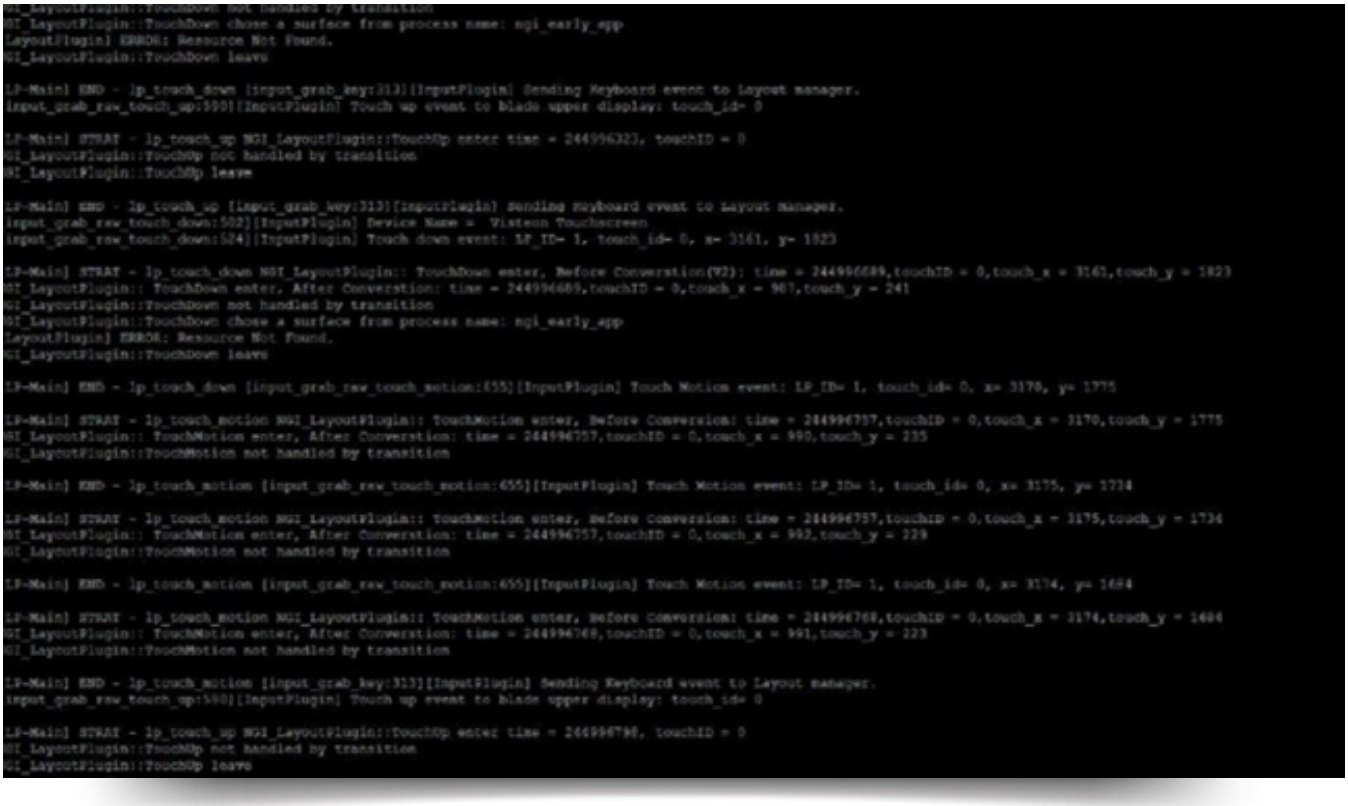
Once the core applications were accessible and data was exfiltrated, the actor then deployed a modular ransomware and triggered it complete the first two phases of the attack. Encryption of the data alerted the security teams in the organization to the breach and then swift action was taken to control the breach and isolate systems.
Because of the delayed detection, the attack spread across the organization riding on ERP and other connected applications.

Proof of access

The threat actor published the following screenshots to confirm their access to the target infrastructure in Jaguar.
The first one belongs to an internal portal connected to a shopfloor



A possible debug log.



Backend code for identification of a user connected with a vehicle



Threat actor profile

Scattered Spider, also known as Sp1d3rhunters or Shiny Hunters, the group claiming responsibility for the Jaguar Land Rover cyber incident, signals a new evolutionary leap in the global threat actor TTP landscape. What sets them apart is their carefully crafted modus operandi, one that fuses three potent ingredients for instant notoriety in cyberspace viz., customer data, large brands and a unique revenue and op. model to target victims.

To the untrained eye, Scattered Spider, may appear as just another threat actor chasing ransom. However, when you scratch the surface, you will start seeing operational layers that unambiguously point to a higher level of evolution both in terms of TTPs and in terms of post-incident pressure tactics. Let us now understand the group in detail to understand why the Jaguar Land Rover incident is proving to be such a long-drawn affair.

This group surfaced in the year 2020 through a series of global breaches. We have reasons to believe that the group was started by former members of ALPHV and RansomHub. The group was possibly incubated by either of these groups and provided stolen data and credentials to breach target networks in its initial stages. Using a best-of-breed approach, Scattered Spider, quickly gained a life of its own and as the revenue counters started humming, the group started paying more attention to its business model.

Between 2021 and 2023, the group underwent a series of leadership changes with the average age of leadership shrinking by nearly a decade. During this period, several new individuals entered the group while the elders moved out. The newbies settled down fairly quickly and continued to scale operations as is evident from the list of successful crimes committed by Scattered Spider, even during the transition period.

Even for the most sophisticated threat actors, the business and operational models are mostly about raking in ransom while they can and then disappearing in the shadows. ShinyHunters is an exception to this trend. Not only has Scattered Spider, developed many models to sustain revenue for its operations, it also runs one of the most mature ransomware -as-a-service operations with multiple affiliate friendly revenue sharing models. Small wonder that its affiliate base grew by a whopping 700 percent in the last two years.

They are easily among the most collaborative and cyber crime groups out there. Thanks to a fluid leadership structure with deep links to multiple established threat actors, ShinyHunters has many active cyber crime projects running with groups around the world. Today, a large number of the over 400 cyber incidents attributed to the group are carried out by affiliates through the revenue sharing model.

Targeting large brands

In addition to seeking publicity for its actions, Scattered Spider, had large brands in its crosshairs since it commenced operations. In its initial phases, the targets were a blend of large and small brands chosen ostensibly for revenue. Zoosk, Home Chef, Minted, Chatbooks, and the Chronicle of Higher Education, Tokopedia and Wattpad were among its early victims.

In the subsequent years, as the new leadership began settling in, the group scaled up its operations to target many small and medium businesses that paid off ransoms quietly fearing regulatory attention or investor scrutiny

In 2024, the group went after AT&T, Twilio and Ticketmaster among other large brands gathering confidence and an unquenchable hunger for publicity in the process. As the year 2025 arrived, the group had grown and its affiliates spread tentacles across the web netting several large brands including:

- Google: Breached through a third-party CRM environment, exposing contact information of business customers.
- Kering (Gucci, Balenciaga, Alexander McQueen): Customer data from the luxury fashion group was compromised.

- **LVMH (Louis Vuitton, Dior, Tiffany & Co.)**: Gained access to a customer information database
- **Air France-KLM**: Customer service data, including names and loyalty program information, was accessed.
- **Adidas**: Customer service tickets were allegedly stolen.
- **Chanel**: A client care database was compromised.
- **Pandora**: Customer profiles were accessed.
- **Qantas**: Customer data stored in a CRM platform was breached.
- **Allianz Life**: The North American branch of the insurance giant was targeted.
- **Cisco**: User profile information from a CRM system was stolen.
- **Cartier**: Limited client information was accessed.
- **Workday**: A customer support database was breached.
- **Vietnam's National Credit Information Center (CIC)**: Scattered Spider, claimed to have exfiltrated nearly 160 million records.

Modus operandi

Unlike other groups, that rely purely on domain impersonation, phishing and vishing, Scattered Spider, went a step further by blending these methods with manipulation of MFA applications. The attack begins with a call placed by a gang member pretending to be from the support team to a pre-identified employee. The employee is guided to deploy a modified data loader to enable the gang member to gain access to the CRM data.

The attack is then escalated to target multiple systems. From the preliminary information available, it seems that the group was able to penetrate deep within the networks of Jaguar Land Rover with access to multiple applications and data. It appears that Jaguar is trying to control the spread of the breach by disabling the impacted systems. However, in the initial days when the exact blast radius was unknown, it is possible that some impacted systems in Jaguar Land Rover were kept ‘alive’ leading to loss of data, extension of system impact and delayed recovery.

Leaking data, double extortion and open threats from across social platforms is a common tactic used by this group. Scattered Spider, is also known to use stolen credentials and hijacked victim applications to send phishing mails to entirely new potential victims.

The US and UK recently charged two members of the group who were arrested earlier. Such arrests as well as a message sent by the group on its Telegram channel which said “We LAPSUS$, Trihash, Yurosh, yaxsh, WyTroZz, N3z0x, Nitroz, TOXIQUEROOT, Prosox, Pertinax, Kurosh, Clown, IntelBroker, Scattered Spider, Yukari, and among many others, have decided to go dark,” indicate that the group is just covering tracks and fading for the time being to bounce back later. The leadership of the group is still at large and we believe they will reappear as a rebranded org very soon.

16.2 Oltenia Energy Complex

The Oltenia Energy Complex is a network of coal mines and power plants, operated by Complexul Energetic Oltenia S.A. (CEO), across Gorj, Vâlcea, and Mehedinţi counties in Romania. These counties are part of the historical region of Oltenia that blends heritage and scenic beauty to offer a unique treat for visitors.

The Oltenia Energy Complex was established in 2012 by integrating Societatea Naţionala a Lignitului Oltenia with Energy Complexes Turceni, Rovinari and Craiova. As per a Euracoal report published in early 2024, reserves of lignite are concentrated in a relatively small area of 250 square kilometres. This is where lignite is mined at ten surface mines and is a critical part of the complex.

The assault on CEO: The "Gentlemen" Move In

On December 26, 2025, at approximately 01:40 AM (regional time), a ransomware group calling itself "Gentlemen" launched a coordinated strike against CEO's business IT infrastructure. The timing was no coincidence. It was instead a coordinated tactical strike that came during the Christmas break when staffing is lean and reaction times are often not up to the mark.

The impact was near immediate:

- Systems went offline: ERP (Enterprise Resource Planning), document management, email services, and the official website were encrypted and taken offline.
- Operations impacted: While the National Energy System (SEN) remained stable, the administrative and logistical backbone of a company that provides 30 percent of Romania's electricity was essentially paralyzed.
- The threat actor: The "Gentlemen" group, that first emerged in August 2025, is known for exploiting internet-exposed services and compromised credentials. Unlike "smash -and-grab" actors, they often conduct multi-stage reconnaissance to ensure they hit the ERP layer which is essentially the "brain" of corporate operations.
- Such scans are conducted opportunistically by the threat actor to leverage windows provided by post-maintenance activities, activation of new services or operational drills.

Connecting the dots: The "Romanian Waters" precursor

To understand the gravity (and context) of the CEO attack, we must look back just six days to December 20, 2025. The national water management authority, Administrația Națională "Apele Române", suffered a massive ransomware event that compromised nearly 1,000 IT systems across 10 of its 11 regional offices. We have covered that attack in detail here.

The investigation

While the CEO attack used a dedicated and possibly a new strain of the "Gentlemen" ransomware, the water authority attack was more "living off the land," weaponising Windows BitLocker to lock out employees. The two attacks are as different as chalk and cheese but despite the different tools and methods, the strategic link is pretty much undeniable:

- Systemic targeting: Both attacks targeted the administrative IT layers of entities that underpin the National Energy and Water systems.
- The "Holiday Gap": Both occurred in late December, exploiting the decreased level of vigilance that comes with any vacation season.

- Hydro-energy Interdependency: "Apele Române" manages the dams and water flows that CEO and other energy providers rely on for cooling and hydro-power. By hitting the water management first, the threat actor effectively mapped the dependencies of the Romanian grid before moving on to the energy giant itself. This is something that all CI operators need to pay attention to.
- Both attacks targeted Romania

The threat actor

The group behind the attack “The Gentlemen” is a relatively new entrant that has significantly matured over the last few years. Unlike traditional threat actors that often indulge in hit and run tactics, this group is known to conduct reconnaissance operations spread across months. The three common tactics employed by The Gentlemen during the early stages include:

- Documenting all accessible infrastructure parts from the web (such as open ports)
- Gathering breached data records to create a vulnerability profile (including potential services that could be compromised) of the potential victim
- Identifying a window for launching the attack and/or deploying the ransomware
- Data exfiltration and delivery of ransom note

Given below is the timeline of the attack as determined by our researchers.

In the month of November 2025, the group could have started probing exposed services (using advanced IP scanner) connected to CEO’s operations. Once the services were detected the group sourced and used previously leaked credentials from other breaches to target them. For instance, our team was able to locate two such credentials during the first phase of our investigation. One set belonged to an employee from the operations team (the credentials were breached in 2021 during the Nitro PDF breach incident). Another set of credentials linked to a generic corporate email ID was found in a leak connected with Bureau van Dijk's (BvD) "Orbis" product breach.

Once the bad actor was able to gain access and control the services, they mapped various segments of the infrastructure and connected networks along with system usage patterns. In parallel, the actor also shut down several anti virus software by abusing multiple Windows drivers to terminate protected processes. We feel this exercise initiated around the St. Andrew's Day holiday must have been completed towards the end of second week of December 2025. From then onwards it was just a waiting game as The Gentlemen waited for the lean season to arrive to finally activate the ransomware.

The "Gentlemen" may claim to be sophisticated, but they are also opportunistic, tactic aware and patient. They prey on multiple security gaps that exist among critical infrastructure operators everywhere. Romania’s 2025 winter crisis is a loud wake-up call for the rest of Europe: compliance with NIS2 is the floor (or baseline), not the ceiling.

16.3 European Space Agency

The ESA's initial statement emphasizes that the compromised systems were limited external servers supporting collaborative engineering. However, when it comes to data, for a space agency, the line between "external collaboration" and "mission-critical" could be increasingly blurred.

What was stolen?

As per the threat actor, the stolen data includes source code files, CI/CD pipelines, API and access tokens, confidential documents, configuration files, Terraform files, SQL files, hardcoded credentials, and private Bitbucket repositories.

Our analysis of the leaked samples and an analysis of the actor's claims reveals a possible failure at the intersection of identity management and third-party collaboration tools.

- The entry point: The attacker is said to have gained access on December 18, 2025, and was able to maintain a foothold for a duration of an entire week.
- Targeted platforms: The breach was focused on Atlassian's suite elements specifically Jira and Bitbucket. These are the "nervous systems" of modern engineering, used to track bugs, manage tasks, and store source code.
- The "Shadow" Infrastructure: Available clues point to a potential compromise of CI/CD pipelines (Continuous Integration/Continuous Deployment) and Terraform files.

If the hacker gained access to Terraform code, it is possible that they didn't just get some basic data. Instead, they could very well have got the architectural blueprint of ESA's cloud infrastructure. This could allow an adversary to see how servers are provisioned, where the firewall rules are weak, and how to potentially pivot into deeper networks.

Threat actor profile: Who is hiding behind "888"?

The threat actor hiding behind the pseudonym "888" isn't new to the cybercrime underground. This threat actor has rapidly ascended the ranks of BreachForums since early 2024. Here are a few details on some of the cyber incidents claimed by the group.

Attribute	Details
Known History	Linked to breaches of Shopify, Decathlon, and HPE (boasted in early 2025).
Tactics (TTPs)	Heavily relies on stolen credentials (likely sourced from infostealer logs) and exploiting misconfigured API tokens.
Motive	Primarily financial. The ESA data is being sold for Monero (XMR) to ensure anonymity.
Sophistication	Moderate to High. They aren't just "smash and grab" artists; they know how to navigate development environments like Bitbucket to find the highest-value assets (keys and tokens).

During the Shopify related breach, 888 claimed to have stolen a huge cache of data from a compromised third-party app. Subsequently, on July 3, 2024, "888" offered a database for a one-time sale using the anonymous cryptocurrency Monero (XMR). The data contained around 180,000 rows of user information, including:

- Shopify ID
- First and last names
- Email addresses
- Mobile phone numbers
- Order counts and total amount spent
- Email and SMS subscription details

Shopify denied any breach in its core systems.

Earlier in May 2024, 888 had claimed to have breached Decathlon. The target was Decathlon Spain and the breach impacted nearly 6600 employees.

Forensic update: The "codebase" compromise

The targeted repositories

An initial analysis of the screenshots and directory structures shared by the threat actor points to the compromise of private Bitbucket instances specifically linked to Open Science and Collaborative Engineering. While these are mostly "unclassified," they do house the logic and plumbing for several high-profile initiatives that include (but are not limited to):

- Earth observation (EO) processing pipelines: The leak seems to include Python and C++ source code for data ingestion and calibration. This could likely impact components of the Copernicus programme (specifically Sentinel-related data processing) where external university partners contribute to the code.
- Infrastructure-as-Code (IaC) Assets: Most alarming are the Terraform and Ansible files. These are not just "documents". Instead, they are the instructions used to assemble ESA's cloud environments. If an attacker gets their hands on these, they can potentially understand the exact network topology (including additional security measures), the IP addresses of internal gateways and the types of encryption used for data-at-rest.
- CI/CD Pipeline Configurations: The exfiltration of Jenkins and GitHub Action/Bitbucket Pipe configurations suggests that "888" had some degree of visibility into how ESA validates its software. This creates a "long-tail" risk of logic-bomb injections in future software updates.

Missions at risk?

Though ESA has not released a specific "list" of missions, the platforms compromised (Jira and Bitbucket) are the primary coordination hubs for:

- Hera and planetary defense: Collaborative missions involving international partners frequently use these "science-DMZ" servers for task tracking and code sharing.
- Space safety and debris removal: Projects like ClearSpace-1 involve heavy external engineering coordination, making them prime candidates for the "collaborative science" servers ESA mentioned.
- Horizon Europe Space Research: Any unclassified research funded by the EU and managed by ESA often resides on these specific external-facing development servers.

The "888" Strategy: A data broker's endgame

Unlike "smash-and-grab" ransomware groups, 888 also functions as a high-end data and compromise broker. Their reputation on the dark web that was built on previous breaches of Shopify, Decathlon, and HPE is based on the authenticity of their samples.

- Monero (XMR) Exclusive: The demand for Monero suggests the actor is looking for a clean, untraceable exit. No surprises here.
- The "Silent Buyer" Risk: There is a high probability that the 200 GB won't be leaked publicly but will instead be sold to a state-sponsored entity (APT). For a nation-state, "unclassified" telemetry formats and satellite command structures are "zero-day" intelligence.
- Rogue nations could potentially use this data to augment their capabilities around payload delivery in space, earth observation systems, internal collaboration on projects and for smaller projects linked to dual use technologies.

Future risks and threats

The ESA has maintained that no classified systems were affected in the incident. However, in the world of orbital mechanics and satellite defense, even unclassified data offers a goldmine for secondary exploitation.

The Telemetry treasure trove

The breach reportedly includes telemetry datasets and simulation models. While not "Top Secret," this data provides adversaries with the exact operational parameters of ESA satellites. Knowing the precise fuel consumption or thermal tolerances of a satellite allows a hostile actor to plan "non-kinetic" interference (e.g., signal jamming or laser dazzling) with pinpoint accuracy.

The hardcoded credential-related challenges

The attacker has claimed to have seized hardcoded credentials and API access tokens.

- The risk: These tokens act like "skeleton keys." Even if the ESA secures the initial server, a single forgotten token in a private repository could allow "888" (or whoever buys the data) to re-enter the network months later.

Supply chain vulnerability

By leaking CI/CD pipeline configurations, the actor has exposed how the ESA builds and deploys its software. This opens the door for a SolarWinds-style supply chain attack, where a malicious update could be injected into future mission software before it ever leaves the ground.

ESA has taken many steps to augment its security posture in the past and remains committed to securing its infrastructure from bad actors. The agency's newly inaugurated state-of-the-art Cyber Security Operations Centre (C-SOC) in Germany that is supposedly leading the forensic cleanup is one such measure. There is always room for improvement and a unified Zero Trust approach covering all parts of the infrastructure could be a strong measure in this direction.

16.4 La Poste France

As families across France prepared for the 2025 holiday season, a different kind of "package" was delivered at the headquarters of **La Poste**. Just days before Christmas, on December 22, the nation's postal and banking giant was hit by a massive cyberattack. This one did way more than just crash a website. It actually weaponized the year's busiest logistics window for some form of geopolitical gain.

On December 22, the organization's website uploaded a brief message that opens "Notre site est indisponible" or our site is unavailable. It added that La Poste teams are doing everything they can to resolve the situation quickly.

Further, on its Facebook page, La Poste published another notice that stated "A major network incident is currently disrupting all of our information systems."

The notice stated that the laposte.fr site is down right now, as is the Digiposte secure document storage service, La Poste's digital identity service, and the La Poste app.

The notice also warned that some post offices could experience some level of degraded service. It however stated that over-the-counter transactions remain possible.

La Poste also operates a bank, Banque Postale.

Pro-Russian Hacktivist Group NoName057(16) that claimed the attack is a known threat actor that has been targeting NATO and Ukrainian cyber assets. The timing of the attack and choice of La Poste offer many clues on the motivations behind the attack and the timing is not coincidental. Instead it seeks to serve a year-end reminder of the nuisance value that such groups backed by nation states hold.

The weapon of choice

The attack has been identified by Shieldworkz researchers as a Distributed Denial of Service (DDoS). Unlike a ransomware attack that steals data for a fee, a DDoS attack is designed to overwhelm a system with sheer volume. This is often a preferred mode for hacktivist groups that wish to leave a message behind without asking for ransom or get into any form of negotiation with the crooks behind a cyberattack. Sometimes such attacks are also used to:

- Test the defenses of an organization
- Identifies possible windows for data exfiltration
- Checks employee competencies
- Grades incident response capabilities of an organization

All this is done to create grounds for more accurate and targeted attacks in the future.

Coming to what happened on December 22, by flooding La Poste's DNS (Domain Name System) servers with illegitimate traffic, the hackers effectively "locked the front door" to the company's digital services.

- **The Impact**: While physical letters were not impacted from a delivery standpoint, the digital brain managing operations was effectively paralyzed.
- **The casualties**: Package tracking went offline, the La Banque Postale app (that at the time of writing was serving nearly 11 million people) went silent, and the Digiposte document vault became inaccessible

The culprit: NoName057(16)

The pro-Russian hacktivist group **NoName057(16)** has already claimed responsibility for the incident. This group has become a persistent thorn in the side of NATO nations and allies. Emerging shortly after the 2022 invasion of Ukraine, they specialize in "propaganda through disruption."

By targeting La Poste, the group isn't just seeking data; they are also seeking visibility and attention within Russia and outside. Their goal is to create a sense of digital insecurity in Western societies, punishing France for its continued military and political support of Ukraine.

It may be remembered that between 14 and 17 July, a joint international operation, known as Operation Eastwood and coordinated by Europol and Eurojust to target the cybercrime network associated with NoName057(16) was launched. Law enforcement and judicial authorities from Czechia, France, Finland, Germany, Italy, Lithuania, Poland, Spain, Sweden, Switzerland, the Netherlands and the United States took simultaneous actions across jurisdictions against cyber criminals and infrastructure belonging to the pro-Russian cybercrime network. The investigation was also supported by ENISA, as well as nations such as Belgium, Canada, Estonia, Denmark, Latvia, Romania and Ukraine. The private parties ShadowServer and abuse.ch also assisted by chipping into support the technical part of the operation.

This campaign led to the disruption of an attack-infrastructure put together by the group. This included over one hundred computer systems and networks worldwide. A major part of the group's central server infrastructure was taken offline. Beyond the effort, Germany issued six warrants for the arrest of offenders living on Russian soil. Two of these persons were accused of being the main instigators responsible for the activities of "NoName057(16)". These people could have been the handlers of the actual hacktivists or coordinators. Either way these were the proverbial big fish.

In total, national authorities issued seven arrest warrants in July, which were directed, inter alia, against six Russian nationals for their involvement in the operations of NoName057(16). All of the suspects have since been listed as internationally wanted, and in some cases, the identities were released to the media in order to engage citizens in reporting the activities of these criminals. Profiles of five NoName057(16) cybercrooks were also published on the EU Most Wanted website.

National authorities since then reached out to many individuals believed to be underground supporters of this cybercrime network. The messages were sent via a popular messaging application, to inform the recipient of the official measures highlighting the criminal liability they bear for their actions pursuant to national legislations.

It was then reported by Europol that individuals acting for NoName057(16) are mainly Russian -speaking sympathisers who use automated tools to carry out distributed denial-of-service (DDoS) attacks. Operating without formal leadership or sophisticated technical skills, they are motivated by ideology and rewards.

Despite this operation, it seems that NoName057(16) has been resurrected and is now in a state wherein it can conduct operations. How did that happen? We have a theory for that as well. I will reveal that bit towards the end.

Why now? The strategic timing

In the world of cyber-warfare, timing (more often than not) is everything.

- **Logistical stress**: La Poste sorts and delivers over 2 million items daily in the run-up to Christmas. By disabling tracking and online payments, the hackers forced a return to manual processing, creating a massive bottleneck. Besides, it also led to La Poste requestioning the services of additional employees to manage the stress.
- **Psychological impact**: By targeting a service as "homely" and essential as the post office during the holidays maximizes public frustration. It turns a technical glitch into a national conversation at the dinner table.
- **Year-end reminder**: While the operation to wipe out the group was carried out in July, NoName057(16) wanted to convey a message to the law enforcement machinery of the EU that it is very much around and willing to engage in more disruption.

The broader context: A "wave" of attacks

This incident certainly wasn't an isolated event. It capped a month of escalating geo-political and digital tension in France:

- **The Interior Ministry**: A separate breach recently compromised sensitive files.
- **Maritime Security**: Remote access malware was recently discovered on a passenger ferry.
- **Public Services**: France Travail (the employment agency) has faced repeated attempts to compromise citizen data.

Geopolitically, the strong stand taken by the French government on Ukraine has brought France into the crosshairs of Russian cyber criminals and their state-backed handlers. France is also actively working to bring more security guarantees for Ukraine.

French intelligence (the **DGSI**) has officially taken over the probe, signaling that the state views this as a matter of national security rather than a simple corporate IT failure.

Lastly you may we wondering how NoName057(16) has been able to resurrect itself so quickly. The answer is simpler than you can imagine. State-backed actors maintain a steady pipeline of resources and people to continue operations in case of a disruption. These resources are scattered at locations such as North Korea and Iran where they are immune from any form of legal action. Once the threat actor playbooks are mature and the TTPs are framed, then it doesn't matter where the group operates from or what kind of an action it is subject to. The hacktivist or threat actor is able to bounce back within a very short period of time under a new identity or using new members.

Such an approach ensures continuity of operations and learning for the threat actor and it's handler.

16.5 Nissan Red Hat

Modern threat actors and data thieves no longer view the enterprise as a monolith. Instead, they apply a clinical taxonomy to their targets, systematically triaging an organization's assets into four (initial) strategic domains of interest. This includes Customer Trust (PII), Internal Stability (Employee Data), Intellectual Capital (Enterprise Data), and most critically, Functional Sovereignty (Operational Control)." This makes it easier to figure out attack paths and harvest the relevant data bits with more focus, attention and tactics.

In the automotive world populated by high-stakes technology, we often talk about cybersecurity within the "perimeters" of our business and treat them as if they were solid walls. Enterprises also invest millions in firewalls, EDR, and SOCs to secure their internal gates. However, as the recent breach involving Nissan and Red Hat demonstrates, the modern enterprise certainly has no walls. Instead it has a well networked circulatory system extending all the way to external consultants who are supposed to be temporary guardians of data. And when a major artery like a global consulting partner gets nicked, the impact of a leak (no matter how small) can be felt thousands of miles away.

The timeline of the attack

Somewhere on the morning of September 26th which was a Friday, the attack in the form of unauthorized access was first detected by Red Hat. Acting immediately, RedHat blocked access to the data and isolated the server to prevent any further access to the server even from validated sources.

A week later and after a round of internal confirmations, RedHat passed on the information on the breach to Nissan on October 3rd (the Friday after) who immediately reported the breach to Personal Information Protection Commission. In addition, as per Nissan, they also contacted customers who are believed to have been impacted by the breach directly or who data was compromised in the breach. The company also issued an apology on its website.

The impacted server was not known to contain any other information than the breached data as per Nissan.

The anatomy of the Nissan attack and its aftershock

When viewed from a stratospheric level, the news is a standard data breach headline: 21,000 Nissan customers in Japan had their personal details exposed including customers who have (or had) purchased vehicles and entered services at the former Fukuoka Nissan Motor Co., Ltd. (currently Nissan Fukuoka Sales Co., Ltd.)

But the source of the leak wasn't an unsecured or forgotten Nissan server. The incident involved a routed indirect hit on Nissan that possibly originated from a compromised GitLab instance that was used by Red Hat Consulting. The levels of data protection accorded to the server are unknown at this point.

The so called "Crimson Collective" the threat actor behind the breach didn't just steal records. They stole 570GB of "Customer Engagement Reports" (CERs) numbering around 800.

As per the automotive major, Nissan's customer engagement strategy focuses heavily on personalized mobile messaging, a seamless digital-to-dealership experience, and using data analytics to deliver relevant content and services. The company aims to build long-term loyalty and achieve high conversion rates and it is possible that this data was collected and stored as part of this exercise and handed over to Red Hat as part of a project.

The stolen reports contain details such as:

- Verified full names
- Physical addresses
- Phone numbers
- Email addresses
- Customer data used in sales and insurance related operations

The company has claimed that credit card details were not part of the breach. Nissan has also issued an advisory to impacted customers to be careful about responding to suspicious calls about their vehicles.

When blended with other information that could be sourced from stolen databases, this could easily bring the customers a step closer to a breach in a phishing attack. This data could also be used to build a buyer profile of the customer and it's essentially a downhill from here.

The "Consultant Blind Spot"

Nissan had multiple collaborative projects with Red Hat.

As per available information, Nissan had engaged Red Hat with a consultancy opportunity to transform the automotive major into a key player in the software-defined vehicle space. This was a data heavy collaboration. Nissan had in fact announced that it would be using the Red Hat In-Vehicle Operating System to power its next-generation software-defined vehicle platform. As per Red Hat, its new vehicle operating system can support advanced driver-assistance systems, digital cockpits, telematics, infotainment, and cutting-edge AI models.

In addition to this, Nissan had also engaged Red Hat to build a customer management system. Details of this project are not very clear. From available information made available to us and analysed by our research team, it seems that it was this project that was impacted by the breach.

The data leaked was information given to Red Hat's consultants by Nissan for the purpose of working on the customer management system project. Red Hat's consultation division had stored the information on its own internal GitLab instance alongside the project's other artifacts. Unfortunately, this was the very server that was breached. So technically this is not a breach at Nissan.

For years, we have argued that consulting firms are turning into ultimate credential aggregation points. We hire experts to help us scale, but in doing so, we often grant them a level of trust that bypasses our standard Zero Trust protocols. Such a dichotomy in security controls could easily be misused by a threat actor. In fact threat actors do keep an eye out for consultants that handle such data. This is not to blame anyone here in any manner. But this is a standard practice across industries that operates based on the level of trust that exists between the client and the consultant (in some cases the consultant could even be an individual).

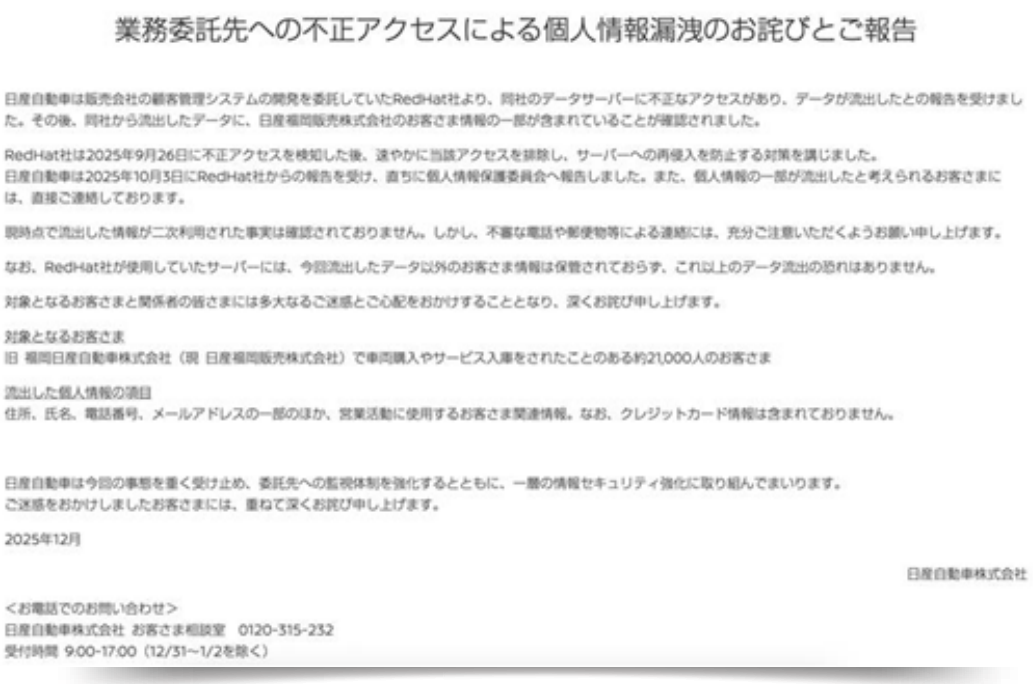
When a consultant creates a "shadow repository" or a test environment to build your next customer engagement management system, that environment could sit well outside the rigorous oversight of your internal CISO or the security team concerned. In some cases, it may not even be subject to the same risk assessment audits that other bits of your infrastructure are subject to. There have been instances in the past when a collaboration ends but the consultant retains the client's data for a while. Sometimes the data is even forgotten in the process.

An additional layer of security for such data and collaboration could go some way in helping in preventing such incidents.

Three lessons for the strategic cybersecurity leader

If you are sitting in a boardroom today, the Nissan-Red Hat event should trigger three immediate shifts in your thinking:

- Start auditing engagements: We spend months vetting a software vendor's product but only minutes signing a SOW for their consultants. We must treat consulting teams as privileged users with "permanent-temporary" access that requires continuous, automated monitoring. The consultant should furnish compliance reports on an ongoing basis for meeting the risk exposure needs of the customer.
- The death of static secrets: Hardcoded secrets in Customer Engagement Reports (CERs) were the primary fuel for this breach. In an era of AI-driven threat hunting, static tokens are a liability. If a secret can be written down, it can be stolen.
- Recognize the extended "Blast Radius": This breach affected Nissan, but the stolen data included reports for over 800 organizations, including government agencies and financial giants. We must map our "blast radius" and know the answer to the question "if our primary consultant is breached tonight, what specific keys to our kingdom do they currently hold"?



業務委託先への不正アクセスによる個人情報漏洩のお詫びとご報告

日産自動車は販売会社の顧客管理システムの開発を委託していたRedHat社より、同社のデータサーバーに不正なアクセスがあり、データが流出したとの報告を受けました。その後、同社から流出したデータに、日産福岡販売株式会社のお客さま情報の一部が含まれていることが確認されました。

RedHat社は2025年9月26日に不正アクセスを検知した後、速やかに当該アクセスを排除し、サーバーへの再侵入を防止する対策を講じました。
日産自動車は2025年10月3日にRedHat社からの報告を受け、直ちに個人情報保護委員会へ報告しました。また、個人情報の一部が流出したと考えられるお客さまには、直接ご連絡しております。

現時点で流出した情報が二次利用された事実は確認されておりません。しかし、不審な電話や郵便物等による連絡には、充分ご注意いただくようお願い申し上げます。

なお、RedHat社が使用していたサーバーには、今回流出したデータ以外のお客さま情報は保管されておらず、これ以上のデータ流出の恐れはありません。

対象となるお客さまと関係者の皆さまには多大なるご迷惑とご心配をおかけすることとなり、深くお詫び申し上げます。

対象となるお客さま
旧 福岡日産自動車株式会社（現 日産福岡販売株式会社）で車両購入やサービス入庫をされたことのある約21,000人のお客さま

流出した個人情報の項目
住所、氏名、電話番号、メールアドレスの一部のほか、営業活動に使用するお客さま関連情報。なお、クレジットカード情報は含まれておりません。

日産自動車は今回の事態を重く受け止め、委託先への監視体制を強化するとともに、一層の情報セキュリティ強化に取り組んでまいります。
ご迷惑をおかけしましたお客さまには、重ねて深くお詫び申し上げます。

2025年12月

日産自動車株式会社

<お電話でのお問い合わせ>
日産自動車株式会社 お客さま相談室 0120-315-232
受付時間 9:00-17:00（12/31~1/2を除く）

A note on the breach put out by Nissan

To gain a deeper and more granular understanding of the impact of cyberattacks across different countries, we incorporated population data into our analysis of cyberattacks. Specifically, we calculated the number of cyberattacks reported per capita, using population figures from Worldometer. This approach highlights the relative burden of cyberattacks on each nation's population, rather than just looking at absolute numbers. Per capita attacks also help us understand the theoretical attack load on each citizen of a country that is being targeted by cyberattacks.

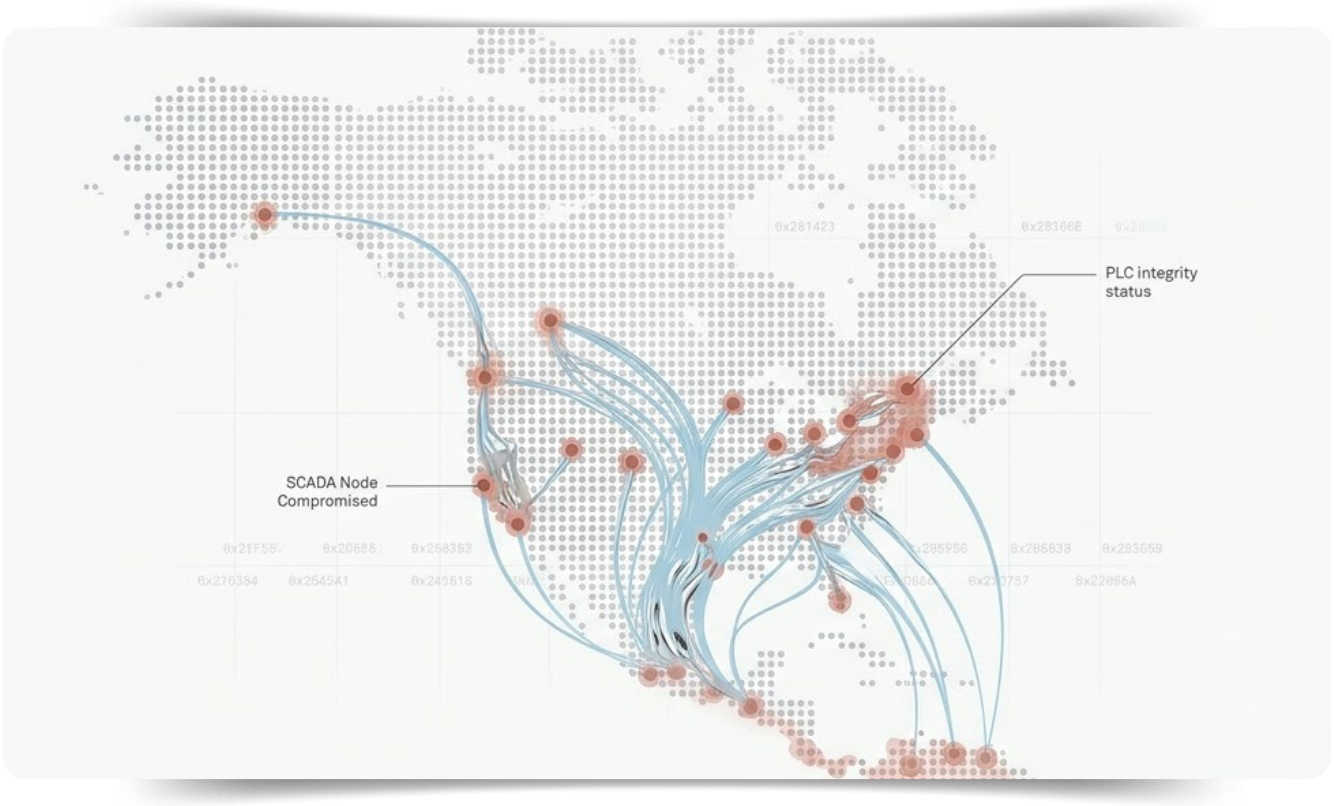
Interestingly, Russian state-affiliated advanced persistent threat (APT) groups appear to have shifted their tactics. Instead of favoring stealth and subtlety, these actors increasingly aim to produce noticeable, disruptive effects. In many cases, they do not attempt to obscure their identity or operations, foregoing even the minimal measures typically used to maintain plausible deniability-except in rare cases where media organizations are the intended targets.

This overt behavior could be attributed to several factors. It might be a manifestation of operational fatigue or desensitization among Russian cyber operators. Alternatively, it could reflect a strategic directive from higher authorities to send a clear, demonstrative signal of cyber capabilities during wartime.

Country	Rank
Ukraine	1
Lithuania	2
Finland	3
Israel	4
Taiwan	5
Belarus	6
Sweden	7
Chile	8
Oman	9
Estonia	10

17. Regional Threat Landscape Analysis

North America



2025 was a year that saw more new attacks than ever within North America. In addition to the existing set of threat actors, new threat actors from Latin America also joined the fray. From disruptions to ransom, every objective was on the table as far as the attackers were concerned. While it is important to underscore the evolving sophistication of the average attack in the region, it is more important to also highlight the rising presence of suspicious payloads turning up in complex OT environments more frequently than in 2024. This includes:

- Broken pieces of suspicious code
- Unknown payloads
- Modified firmware

17.1 Threat landscape characterization

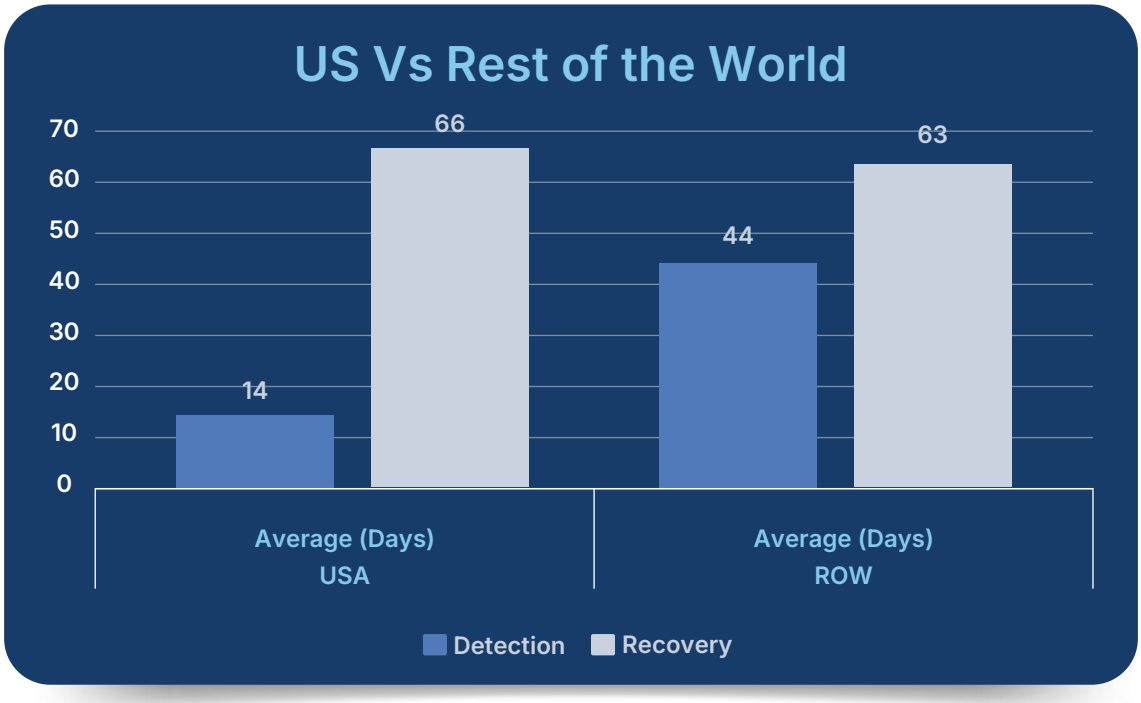
North American operational technology environments experienced a marked escalation in both sophistication and volume of cyberattacks throughout 2025. Threat actors demonstrated an increasingly dangerous willingness to target industrial control systems (ICS), supervisory control and data acquisition (SCADA) platforms, and programmable logic controllers (PLCs) across critical infrastructure sectors.

In 2025, the region witnessed a fundamental shift in the threat landscape characterized by:

- Adversary diversification: Nation-state actors, disgruntled employees, hacktivist groups, and financially motivated cybercriminals are now actively targeting OT environments

"Critical infrastructure in North America attracts more attacks than any other part of the world"

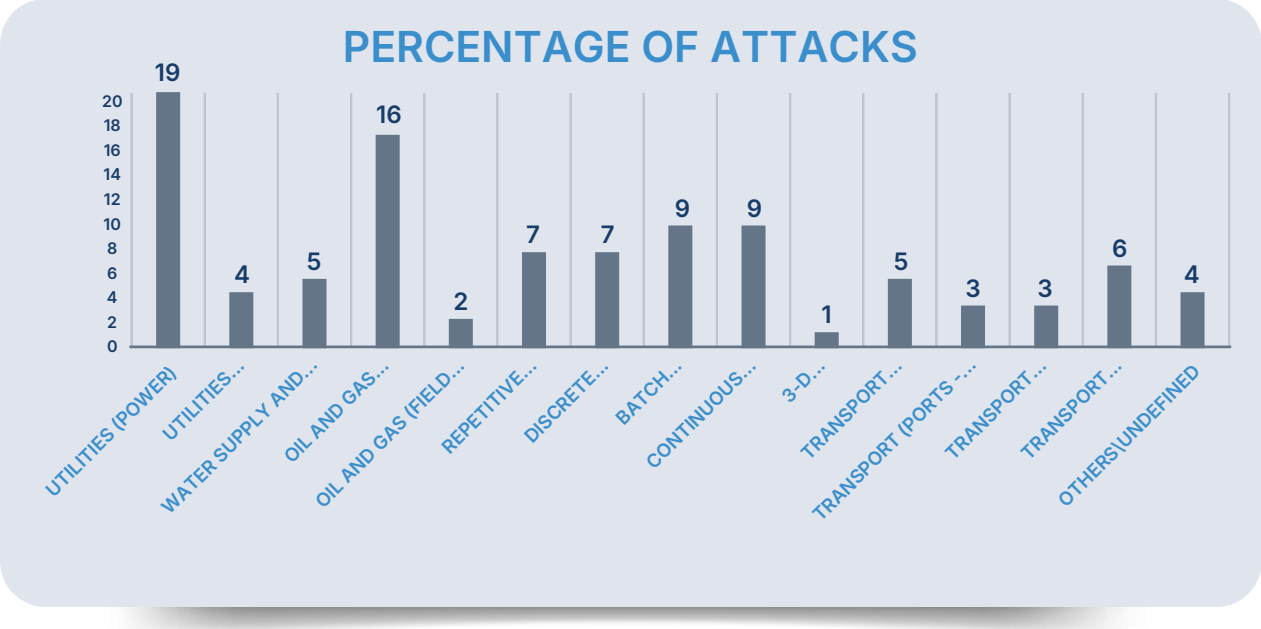
- Payload diversity: North America also attracts a huge diversity of payloads from across threat actors. But unlike other regions, North America is often targeted using very complex and evolved malware. The diversity of payloads stems from an attempt to bypass security mechanisms using multiple tactics.
- Operational evolution: Movement from purely IT-focused ransomware to a more direct OT manipulation and SCADA intrusion
- Sectoral concentration: Water/wastewater systems, energy utilities, and oil and gas systems are bearing the brunt of attacks
- Exploitation simplicity: Successful compromises are often achieved through basic techniques that rely on exploiting poor cyber hygiene rather than advanced persistent threat (APT) toolkits. This is true for most attacks on enterprises. In case of the attacks on critical infrastructure, the threat actors do follow a more circuitous route.
- Qualitative concentration: The number of threat actors that are operational in North America is fewer when compared to other regions. The ratio of average number of threat actors per unit of critical infrastructure in the region is among the lowest when compared to global numbers. So how come US is attracting such a huge volume of attacks? Well this has to do with the large number of attacks mounted by a small set of actors. The threat of prosecution and exposure of threat actors by US regulatory agencies has made threat actors follow a different playbook for the US. In addition to deploying senior threat actors, handlers also do not permit smaller or new groups to target the US directly. Such an approach alone is responsible for the growing sophistication of cyberattacks on US critical infrastructure.



US leads the world in early detection of breaches and attacks. Businesses here also recover faster from incident as compared to the rest of the world.

Sectoral attacks in North America

Sector	Percentage
Utilities (Power)	19
Utilities (Renewables)	4
Water supply and management	5
Oil and gas (Refineries)	16
Oil and gas (Field activity)	2
Repetitive manufacturing (Electronics, toys, confectionery)	7
Discrete manufacturing (Clothing, automotive, firearms, medical devices)	7
Batch manufacturing (Food and beverage, pharmaceuticals, plastics)	9
Continuous manufacturing (Fertilizer production, chemical processing, pharmaceuticals)	9
3-D printing/additive manufacturing	1
Transport (Railway systems of all types)	5
Transport (Ports – inland and sea facing)	3
Transport (Airports)	3
Transport (Pipelines)	6
Others\undefined	4



The growing attacks on utilities and oil and gas are no coincidence. Threat actors are building teams with OT-focused skillsets and while they were merely selling data earlier, now they are also using the exfiltrated data for training AI models (including SLMs) to manage bits and pieces of the attack chain independently. Post-attack negotiations are now being handled by expert negotiators who are operating with a mix of AI-generated scripts and psychological terror tactics to put pressure on the victim.

The volume of attacks targeting utilities demonstrates significant temporal and geographical variability. This fluctuation may correspond with seasonal demand cycles or specific threat actor campaigns designed to exploit operational windows of vulnerability. The variance may also indicate reconnaissance activities preceding larger strategic objectives. Attack patterns on utilities suggest deliberate targeting of operational technology (OT) assets and control systems, particularly during high-load periods or infrastructure upgrades.

Within manufacturing, the concentration of attacks is highly skewed towards complex manufacturing units that rely on proprietary processes and intellectual property (IP) Threat intelligence collected by our research team confirms that adversaries are exhibiting a strong interest not only in the technological processes but also in the personally identifiable information (PII) and credentials of plant personnel most likely as a vector for privilege escalation and lateral movement.

While volumetric IP-related attacks appear relatively low, the strategic nature of the targets suggests a high value-to-volume ratio. Exfiltrated artifacts indicate that the perpetrators operate as part of organized, well-funded groups with ties to nation-state actors. These threat actors are not low-level opportunists but are part of structured IP exfiltration operations with affiliations to advanced persistent threat (APT) groups such as APT41 or darknet-linked data brokering networks.

Both oil and gas and manufacturing sectors face a broad spectrum of threats that span across the supply chain right from upstream component providers to downstream service integrators. The attack surface includes third-party vendors, IoT/IIoT devices, industrial routers, and legacy SCADA systems. This breadth of targeting suggests that threat actors have a deep understanding of sector-specific architectures and are conducting highly granular reconnaissance and exploitation campaigns.

Core ICS elements including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Human-Machine Interfaces (HMIs), and Programmable Logic Controllers (PLCs) are high on the to-attack list of threat actors. SCADA systems are used primarily for geographically dispersed assets, such as electrical grids, water distribution networks, and pipeline systems. DCS platforms are typically deployed in continuous or batch processing environments like chemical plants, refineries, and power generation facilities. HMIs provide visual dashboards and control interfaces for operators, while PLCs act as robust, real-time controllers for specific field

devices and processes. Such systems are identified and marked for remote access by threat actors well before the actual attack takes place. In some instances, the threat actors even know what type of incident response measures will be triggered and whom to negotiate with for faster ransom payout.

17.2 Data theft

Within the United States, sophisticated info-stealing malware have now emerged as a key tool for augmenting data breaches. Information harvested from social media platforms like X and even Reddit was combined to construct detailed breach profiles of employees in sensitive roles and locations. These meticulously crafted profiles, along with exfiltrated credential data, were then fed into nascent AI tools, enabling the automated generation of potential access credentials, frequently leading to devastating business email compromise (BEC) attacks. US-based businesses accounted for an alarming proportion of data hemorrhaged onto the dark web and other illicit online forums.

Of the 9 petabytes of stolen data analyzed, a staggering 2.6 petabytes originated from US entities. This torrent of stolen information witnessed a substantial 41 percent year-on-year increase in 2025. Meanwhile, Canadian businesses experienced a significant 165 percent surge in cyberattacks during the same period, with publicly available information suggesting a concerningly high success rate for these intrusions. Such a huge spike in attacks does point to increasing hacker interest in Canadian businesses.

The presence of persistent access mechanisms and dormant payloads in critical infrastructure suggests a capability for rapid activation during periods of kinetic conflict or heightened political tension. These latent exploits can be triggered to disrupt industrial operations, delay response efforts, or signal geopolitical intent. Such activity underscores the plausibility of cyberattacks being used as a force multiplier during conventional conflict scenarios.

The intelligence gathered from successful attacks is increasingly being used to train large language models (LLMs) and AI engines, enabling adversaries to simulate network behavior, anticipate defensive playbooks, test institutional retention (and muscle memory) and refine intrusion strategies with high precision

The escalating frequency of reconnaissance attacks across critical sectors in North America is a growing concern that demands immediate attention. These operations have evolved far beyond simple network probing; adversaries now actively exfiltrate metadata, credentials, and system configuration details while maintaining persistent surveillance on target environments. This enables them to map digital perimeters, profile defense mechanisms, and wait for exploitable vulnerabilities to emerge.

As mentioned in section on AI, the intelligence gathered from these attacks is increasingly being used to train large language models (LLMs) and AI engines, enabling adversaries to simulate network behavior, anticipate defensive playbooks, test institutional retention and refine intrusion strategies with high precision. This capability shifts reconnaissance from passive observation to an active phase in long-term cyber campaigns. What makes this trend particularly insidious is that many of these attacks are launched from hijacked infrastructure located in geopolitically neutral or non-adversarial countries, masking their true origin and complicating attribution. Coupled with the proliferation of autonomous botnets and AI-driven command-and-control (C2) systems, attackers can now orchestrate global-scale operations with minimal human oversight.

Modern botnets have become significantly more adaptive and evasive. They dynamically rotate through vast IP address pools (linked in some instances to compromised mobile phones), manipulate port activity at random intervals, and employ polymorphic behaviors to evade detection by traditional botnet monitoring tools. These advancements not only increase operational stealth but also allow malicious infrastructure to persist longer within enterprise networks.

17.3 Unique pressure tactics

In one instance involving the threat actor Qilin, negotiators reached out to a water treatment plant claiming that they had quietly exfiltrated almost 45 TB of data during a recent intrusion that according to them went undetected. In order to prove their point, the negotiators shared screenshots of a few documents that were purportedly stolen by Qilin.

In this case Qilin was simply exaggerating their work. Not only was no data stolen, more importantly the screenshots shared were from an insider. The group didn't pay up and asked its employees to ignore all calls. Each employee (and in some cases their family members) was getting almost 3-4 calls a day asking them to ask the management of the company to pay off the ransom else, they will also leak more information including PII of employees.

Such psychological tactics are designed to put pressure on an enterprise to pay a ransom even in cases where no data was actually exfiltrated.

17.4 Automated scripts and fragmented payloads

The quiet probing that lasts as much as 36 months in some instances is often a prelude to an attack. Through automated scripts and via highly fragmented payloads, the threat actors are able to create a clear beachhead and move on to LOTL and other well-known persistence techniques. Now lets take a look at what each category of threat actor is trying to achieve in the region.

17.5 Nation-state actors

APTs with the highest regional footprint in North America

Threat actor	Percentage activity
Volt Typhoon	21
Cyber Av3ngers	19
APT 28 (Russia)	19
Lazarus (North Korea)	7
Others	34

17.5.1 China: Volt Typhoon

Volt Typhoon is a very well-known and notorious threat actor previously connected with attacks on US Navy. The group works by executing small and targeted pre-positioning campaigns that target small and medium-sized U.S. water systems and electric utilities in batches. It is known to have access to at least 130-150 water systems most of which are located in rural areas or close to defense establishments.

This group maintains a very high level of operational readiness and is known to be particularly active during US military exercises in the Indo-Pacific theater managed by USINDOPACCOM. As with all other Chinese threat actors, this one also bears a very high overlap with the Ministry of State Security and its reports are known to be tabled during the meetings of the Chinese Central Military Commission. Volt Typhoon is an extremely dangerous player. An FBI note on Volt Typhoon released in 2024 states:

"Chinese hackers had penetrated deeply into United States' cyber infrastructure" with explicit intent to cause damage to water treatment plants, electrical grid, and transportation systems"

- Strategic Intent: Assessed to be establishing access for potential sabotage during Taiwan Strait conflict scenarios (2027 operational readiness timeline referenced in U.S. intelligence assessments)
- Methodology: Living-off-the-land techniques, persistent access maintenance, minimal detection footprint

17.5.2 Iran (IRGC-affiliated actors / Cyber Av3ngers):

- **Notable Incident**: Municipal Water Authority of Aliquippa, Pennsylvania (2023, continued into 2025 timeframe)
- **Targeting**: Israeli-made Unitronics PLCs controlling water pressure systems
- **Impact**: Forced shutdown of booster station equipment, manual operation implementation
- **Scope**: At least 10+ U.S. water facilities compromised using similar methodology according to federal investigators
- **Tactics**: Exploitation of internet-exposed HMI devices with default credentials

17.5.2 Russia (APT28/GRAPHITE overlap):

- **Infrastructure**: Exploitation of Ubiquiti EdgeRouters for credential harvesting, proxy operations, and C2 infrastructure
- **Targeting**: Electric, oil & gas, water/wastewater, manufacturing sectors
- **Operational Overlap**: Infrastructure sharing between APT28 and historically-tracked threat groups (STIBNITE operations 2020-2021)

17.5.3 Hacktivist Groups

Z-Pentest (Most Active):

- **Emergence**: Established early 2025
- **Alliances**: NoName057(16), CARR (Cyber Army of Russia Reborn), Sector16
- **Activity Level**: Most active hacktivist group targeting ICS throughout 2025
- **Targeting**: Wide range of industrial technologies including HMI systems, SCADA networks
- **TTPs**: VNC brute-forcing, internet scanning for exposed devices, simultaneous DDoS attacks to facilitate SCADA intrusions
- **Evidence**: Video documentation of HMI defacement, system name changes to hacktivist group references

Sector16:

- **Formation**: January 2025 (collaboration with Z-Pentest)
- **Sophistication**: Novice group leveraging shared TTPs from more established partners
- **Focus**: U.S. critical infrastructure with geopolitical messaging

Dark Engine / Infrastructure Destruction Squad:

- **Targeting**: Persistent focus on HMI exposure and manipulation
- **Operational Pattern**: Repeated intrusion attempts against similar target profiles

CISA May 2025 Alert: Government assessment of "unsophisticated cyber actor(s) targeting ICS/SCADA systems within U.S. critical infrastructure sectors (Oil and Natural Gas), specifically in Energy and Transportation Systems." Despite elementary intrusion techniques, poor cyber hygiene and exposed assets enable significant consequences including defacement, configuration changes, operational disruptions, and physical damage potential.

CISA December 2025 Advisory (AA25-343A): Detailed pro-Russia hacktivist TTPs including:

- Scanning for vulnerable devices with open VNC ports (T0883, T1595.002)
- Temporary VPS provisioning for password brute-force operations (T1583.003)
- Exploitation of weak authentication on SCADA networks
- Simultaneous DDoS attacks masking SCADA intrusions (April 2025 confirmed incidents)

17.5.4 Financially-motivated cybercriminals

Ransomware groups:

- **Qilin**: Most prolific ransomware group in 2025. It started its operations by targeting US businesses and expanded to other countries
- **Akira**: Second-most prolific, focusing on construction, manufacturing, professional services
- **Black Basta**: Confirmed targeting of utilities (Southern Water UK data breach, indicating methodology potentially applicable to North American utilities)

Targeting pattern:

- Manufacturing: 600 entities affected
- Healthcare: 477 entities affected (healthcare OT systems including building management, medical device networks)
- Focus on sectors with high operational continuity requirements and lower cybersecurity maturity

17.6 Verified regional incidents

Water and wastewater

American Water (October 2024, impacts extended into 2025)

- **Entity**: Largest regulated U.S. water utility (14 million customers, 14 states, 18 military installations)
- **Discovery**: October 3, 2024
- **Attack Type**: Cybersecurity incident (specifics not publicly disclosed)
- **Response**: Proactive disconnection of MyWater customer portal, suspension of billing systems
- **Impact Assessment**: IT systems compromised; company stated no impact to water/wastewater operations or quality
- **Regulatory**: 8-K SEC filing due to critical infrastructure status
- **Recovery**: Billing systems restored within days; investigation ongoing with law enforcement coordination

This attack demonstrates IT/OT segmentation effectiveness when properly implemented. However, the targeting of the largest U.S. water utility signals strategic adversary interest in high-profile, high-impact targets.

Municipal Water Authority of Aliquippa, Pennsylvania (2023, continued monitoring 2025)

- Attack Attribution: Iran-backed Cyber Av3ngers
- Target: Israeli-made Unitronics PLCs controlling water pressure monitoring
- Impact: Shutdown of booster station monitoring equipment, forced manual operations
- Scope: Federal investigators confirmed at least 10 additional U.S. water facilities compromised using identical methodology

Canadian Water Systems

- Canadian Centre for Cyber Security Assessment (2025-2026 Threat Assessment):
  - "Non-state actors will very likely continue to opportunistically compromise and disrupt internet-exposed water system OT within Canada, especially in connection to major geopolitical events"
  - "Cyber threat to Canada's critical infrastructure is almost certainly increasing"
  - Confirmed awareness of multiple instances of non-state actors attempting to disrupt internet-exposed OT systems in Canada, including water systems

Energy Sector

North American Electric Utility Sector (2025)

- **CISA Assessment**: Unsophisticated actors targeting ICS/SCADA in Energy and Transportation Systems
- **Methodology**: Exploitation of poor cyber hygiene, exposed assets
- **Consequences**: Defacement, configuration changes, operational disruptions, physical damage potential
- **Trend**: 70% increase in cyberattacks on U.S. utility companies from 2023 to 2024

Brute-Force Campaigns Against VPN Infrastructure

- **Targeting**: Electric, oil & gas, water/wastewater, manufacturing sectors in Canada and United States
- **Actor**: Multiple threat groups identified conducting brute-force operations
- **Focus**: Vulnerable remote services, VPNs subject to recently publicized CVEs
- **Infrastructure**: OSINT identified suspicious self-signed X.509 certificates on AWS-hosted infrastructure, indicating coordinated campaign infrastructure

NERC Warning: North American Electric Reliability Corporation documented that electrical grid attack surface expands by approximately 60 susceptible points per day due to increasing digitalization and interconnection.

Manufacturing sector

CISA ICS Advisory Analysis (2024-2025):

- Critical Manufacturing: 45.8% of all affected technologies in ICS advisories
- Energy Systems: 21.3% of affected technologies
- Vulnerability Concentration: Siemens products (1,175 reported ICS vulnerabilities), Schneider Electric (163 vulnerabilities, ~70% high/critical severity)

Attack surface: Manufacturing sector faces compounded risk from:

- Legacy equipment with extended operational lifespans (10-30+ years)
- Specialized control protocols (Modbus, Profinet, EtherNet/IP)
- Continuous uptime requirements limiting patch windows
- Interconnection with supply chain partners and OEM remote maintenance

Local Governments on the radar: A growing threat to counties and public infrastructure

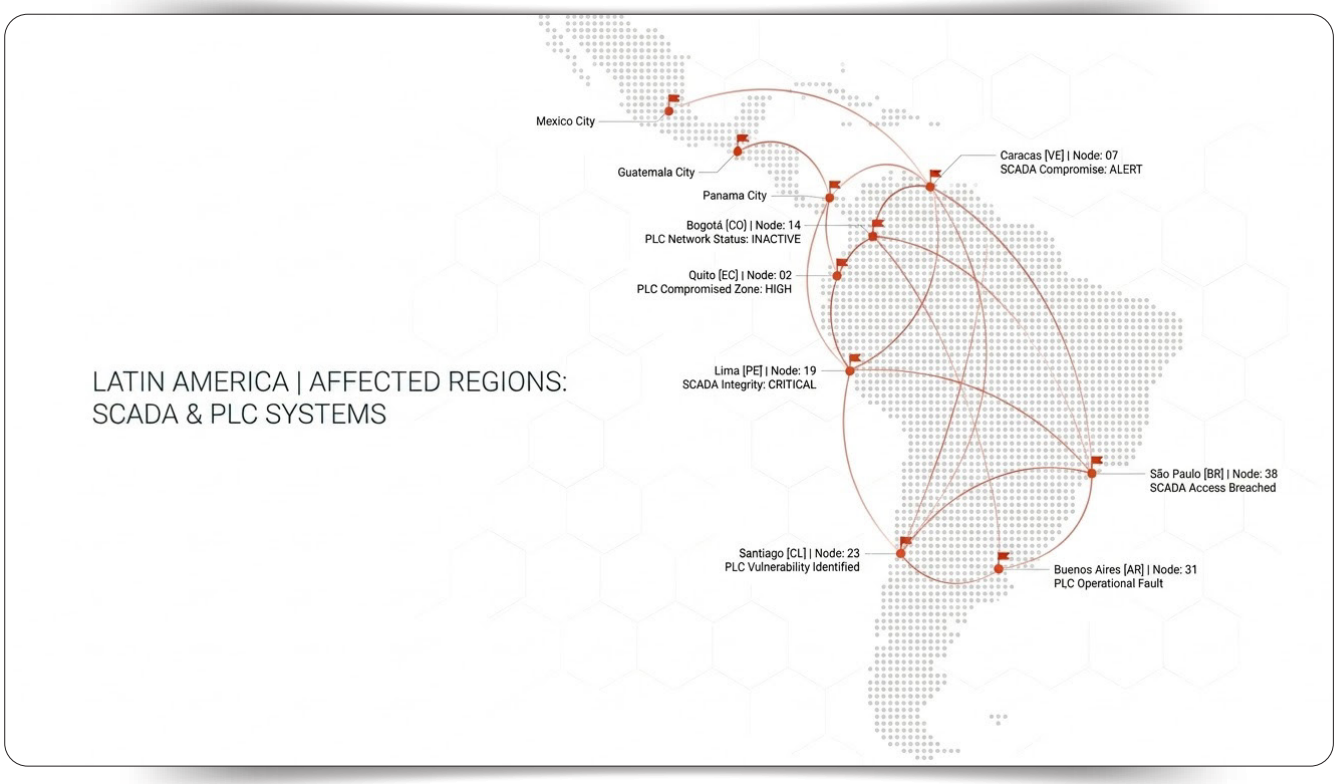
Attacks on U.S. County governments grew by a relatively modest 7 percent in 2025 (as compared to over 300 percent in 2024). While the attacks have declined in terms of absolute numbers, the quality of attacks continues to improve. One of the most common attack vectors observed was brute force login attempts targeting specific public-facing servers and payment gateways. Threat actors are also keeping an eye on officials connected with public counties and their social media profiles.

Between April and December 2025, counties were bombarded with an average of 17,000 login attempts every 72 hours. Such a staggering frequency clearly underscores both the scale and persistence of the threat. Although many of these attempts were blocked by basic security controls, few counties failed to detect or mitigate repeated access attempts, resulting in successful intrusions. Once inside, attackers often attempted to alter or corrupt application files tied to essential public services, severely disrupting operations.

The average cost of recovery for an affected county was approximately $920,000, with a mean downtime of 97 days. In some severe cases, counties attacked in mid-to-late 2024. had not returned to full operational capacity even by June 2025. Overall, cyberattacks on U.S. county systems resulted in 764 cumulative days of citizen service disruption across the year. Pre-negotiation ransom demands averaged $120,000, with a response window of just 48 hours thereby leaving minimal time for victims to react.

18. Regional Threat Landscape Analysis

Latin America



Latin America is turning into a hub for cyberattacks. The region is primarily being used as a conduit for relaying cyberattacks from known geographies to mask their origin. Latin America reported a significant surge in cyberattacks during 2025, with organizations facing an average of 7000-13000 attacks each week. This represents a 29 percent year-over-year increase. Our regional honeypots get swarmed by attacks in waves during periods of geopolitical turmoil elsewhere indicating a very strong link between events elsewhere and cyberattacks in the region.

Latin America's attractiveness as conduit for cyberattacks stems from:

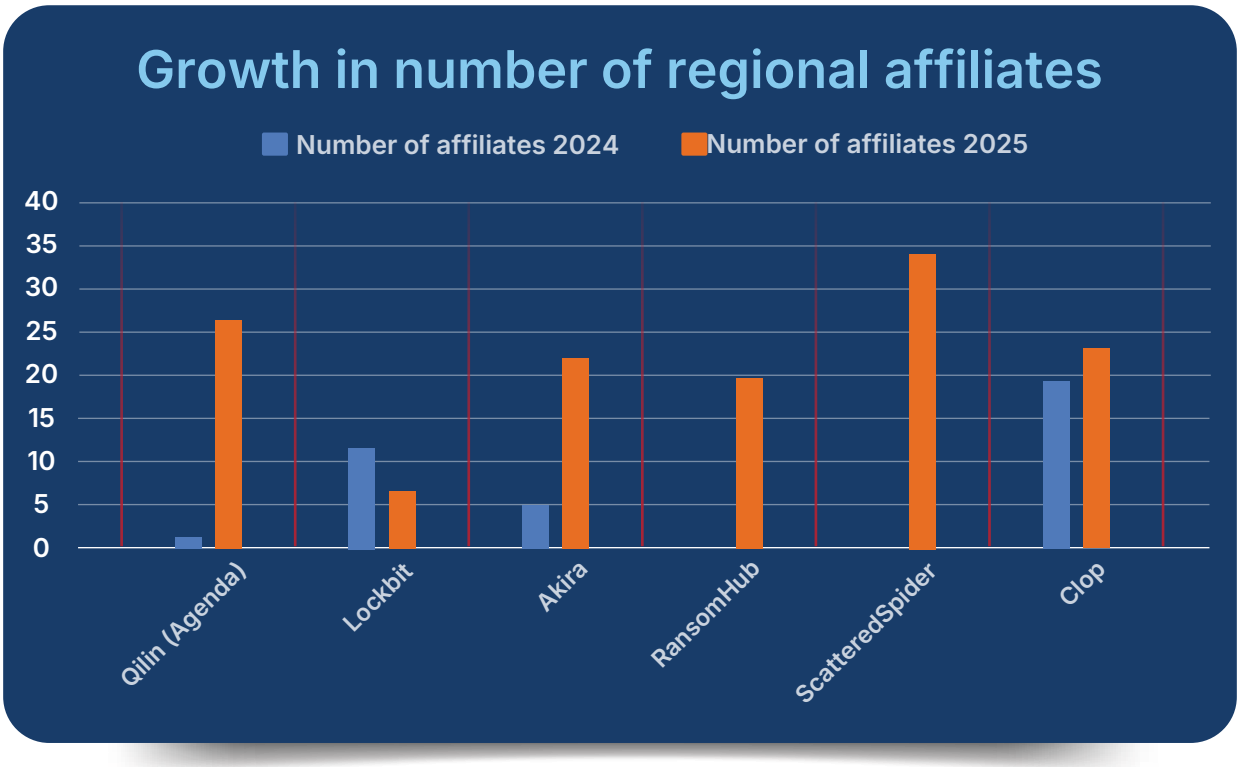
- A massive expansion of regional bot network in the region. This makes it easier to route suspicious traffic and scans through IPs that are native to the region
- Gradual yet significant rise in the number of affiliates recruited by major threat actors who are based in the region now or have moved here
- The increase in the number of digital transformation and automation projects that have taken off in the region

18.1 Ransomware as the Primary OT Threat Vector

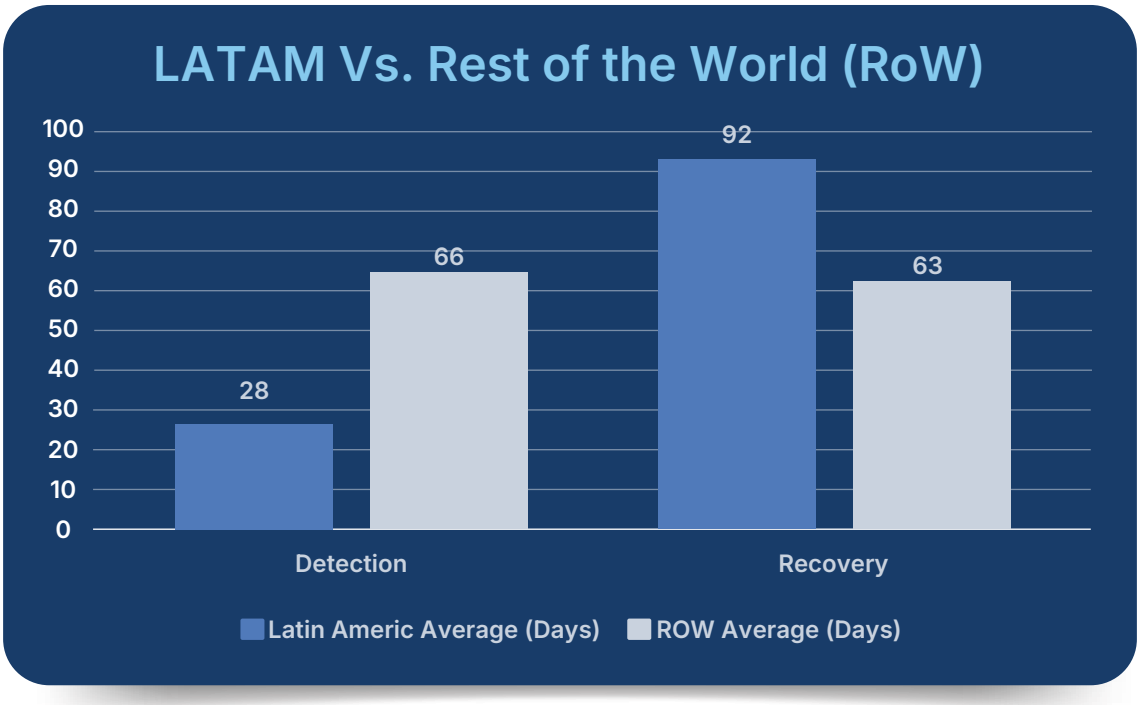
Ransomware has emerged as the dominant threat affecting operational environments in the LATAM region during 2025. As per our analysis, ransomware attacks are growing disproportionally in the region. This includes both ransomware targeting regional businesses and those that are transiting the region through regional botfarms. Brazil, Mexico and Argentina saw major attacks directed towards businesses and critical infrastructure within their borders.

To understand the growth in attacks, we need to understand how the affiliate networks associated with major global threat actors have grown in the last 5 years in the region. Groups like ScatteredSpider and Qilin have logged impressive growth in the number of affiliates added. There may be overlaps between affiliates working for multiple groups. This growth indicates that these affiliates are drawing enough regional business from the groups they are affiliated to. It is possible that some of these groups are targeting enterprises in countries outside the region and are simply hiding here. But when one connects the growth in the number of botfarms and the growing number of regional cyberattacks with the growth in affiliates, a pattern emerges.

This growth has a clear link with the rising cyberattacks in the region. Not only are these affiliates engaging targets outside the region but they are also targeting businesses within the region as well. It is also possible that some of these affiliates have moved into the region to target businesses here and conduct post-breach activities.



What distinguishes 2025 from previous years is the extended recovery times in Latin America compared to other regions. While organizations elsewhere often recover within days, South American entities frequently require months to restore operations, magnifying economic and operational impacts. In fact, both the detection and recovery times are very high in Latin America when compared to the rest of the world. On an average, businesses here continue for almost 9 additional working days without detecting a breach as compared to the global average.



18.2 Targeted sectors and attack surface

Industrial sectors have become primary targets. In Brazil, Mexico, Chile, and Argentina, industrial companies ranked among the top five categories suffering cyberattacks. This pattern reflects the presence of critical infrastructure in these countries:

- **Brazil and Argentina**: Leading positions in regional mining and mechanical engineering
- **Chile**: World's leading copper producer
- **All four nations**: Well-developed chemical processing and energy sectors

The convergence of IT and OT networks has dramatically expanded the attack surface. Legacy SCADA systems, poorly segmented networks, and outdated ICS equipment create vulnerabilities that attackers systematically exploit.

Sectoral attacks in LATAM

Sector	Percentage
Utilities (Power)	15
Utilities (Renewables)	1
Water supply and management	8
Oil and gas (Refineries)	26
Oil and gas (Field activity)	2

Sector	Percentage
Repetitive manufacturing (Electronics, toys, confectionery)	1
Discrete manufacturing (Clothing, automotive, firearms, medical devices)	7
Batch manufacturing (Food and beverage, pharmaceuticals, plastics)	7
Continuous manufacturing (Fertilizer production, chemical processing, pharmaceuticals)	5
3-D printing/additive manufacturing	1
Transport (Railway systems of all types)	9
Transport (Ports – inland and sea facing)	4
Transport (Airports)	4
Transport (Pipelines)	4
Others\undefined	6

18.3 Attack origins and threat actors

State-Sponsored Activity: Chinese APT groups including APT 41 expanded operations across Brazil, Argentina, and Mexico during 2025. These groups employed adversary-in-the-middle techniques and custom VPN tools to infiltrate government and industrial networks. China is retaining a very high level of interest in both businesses and government entities in the region. Most of the attacks on key sectors in LATAM can easily be traced back to Chinese threat actors or their unmarked affiliates.

Another country that maintains a high level of digital surveillance on businesses here is Russia. LATAM has been on GRUs radar since 2018. APT 28 and 29 lead the pack when it comes to most active days registered. Incidentally, both Russian and Chinese threat actors do not seem to make an active attempt to hide their activities in the region.

Chinese interest in the region could also be explained by the low level of "construction engagement" this region has received in China's Belt and Road Initiative (BRI). As per a report by the China Global South Project, "Chinese investment in Latin America this decade, as the vast loans from China's state-owned policy banks that defined BRI engagement in the 2010s have faded to almost zero. The large-scale infrastructure projects that such financing supported have declined". This means that China's influence in the region as expressed by the declining construction engagement may have caused some heartburn in Beijing and that may have translated into more cyber attention from Chinese threat actors.

18.4 Who is keeping an eye on the region?

Threat actor	Country	Observation	Targets
APT 41	China	Active approx. 200 days a year; Has a strategic presence	Targeting critical infrastructure and data centers
APT 31	China	Operates in tandem with APT 41	Enterprises and businesses
APT 30	China	Is found across the region	IOCs found across all types of businesses including not-for-profit entities.
APT 28	Russia	Active throughout the year	Targets oil and gas entities specifically

Threat actor	Country	Observation	Targets
APT 29	Russia	Keeps an eye on government communication	Targets government department and ministries
APT 35	Iran	Is active occasionally across campaign cycles tied to geo-political events	Target government entities, financial institutions, mineral extraction and oil and gas companies

In terms of the targets, these APT groups are targeting a diverse set of targets across the region. Strategic APTs such as APT 41 and APT 28 are spearheading campaigns targeting key sectors. The goal is to ensure a high level of surveillance on government communications and commodity production and selling by regional companies.

Regional threat actors: The South American APT (APT-C-36) group BlindEagle conducted multiple campaigns between late 2024 and early 2025, targeting Colombian government entities and judicial institutions. While the exact affiliation of this group is not known, it seems to have an understanding with multiple APT groups from the countries listed in the table.

Pro-Russian affiliates launched DDoS attacks against Latin American infrastructure throughout 2025 using regional botfarms.

Financially motivated groups: Ransomware groups operating broadly under the RaaS model (including variants like Global Group, Play, and newly emerged operations) conducted broad campaigns across the region. Brazil featured prominently as a target for multiple ransomware families. Brazil's diversified industrial infrastructure and its prominent geopolitical influence make it an attractive target for APT groups and other unaffiliated threat actors.

Country-wise breakdown of attack percentage

Country	Percentage of attacks
Brazil	25
Argentina	19
Mexico	15
Chile	6
Colombia	5
Others	30

18.5 Critical infrastructure vulnerabilities

Energy and utilities infrastructure in LATAM faced persistent threats, though verified OT-specific incidents remain sparse in public reporting. The rising attacks registered by our regional honeypots points to rising interest in regional infrastructure. The global trend of attacks on operational technology affected LATAM, with specific concerns around:

- **Water treatment facilities**: Vulnerable due to outdated control systems
- **Oil and gas**: Extraction, transport and refining especially in Brazil and Argentina
- **Energy sector**: Grid management and distribution systems targeted
- **Manufacturing**: Production lines increasingly targeted for maximum disruption leverage

18.6 Attack methodologies

The technical approach to compromising OT environments in 2025 followed established patterns:

- **Initial access**: 79 percent of oil and gas and utility sector incidents began with phishing; 81 percent involved exploitation of remote services
- **Lateral movement**: Poor network segmentation between IT and OT allowed attackers to pivot from compromised email systems to industrial control systems
- **Persistence**: Threat actors established long-term access in target networks, sometimes maintaining presence for months before detection
- **Role of botfarms**: Bot farms that deflect payload bearing traffic to mimic remote sites or other legitimate traffic sources
- **This region is also home to new malware test beds**: This is where new payloads are tested before being used for attacks around the world

18.7 The geopolitical dimension

Unlike targeted campaigns against North American and European infrastructure, South American OT attacks appear more opportunistic rather than strategically coordinated. The exception involves Chinese and Russian state-sponsored groups that are conducting espionage operations aligned with economic and political interests in the region as mentioned before.

Threat actors are building a presence for the long term.

18.8 Detection and response challenges

Organizations in South America face unique obstacles:

- **Resource constraints**: Limited cybersecurity budgets and scarce OT security expertise
- **Security posture**: In many cases is not aligned to the threat environment surrounding these enterprises.
- **Detection delays**: A majority of successful attacks in OT environments took almost a month to discover. The average recovery time is almost 90 days
- **Visibility Gaps**: Organizations estimate that most of the OT environment attacks go completely undetected

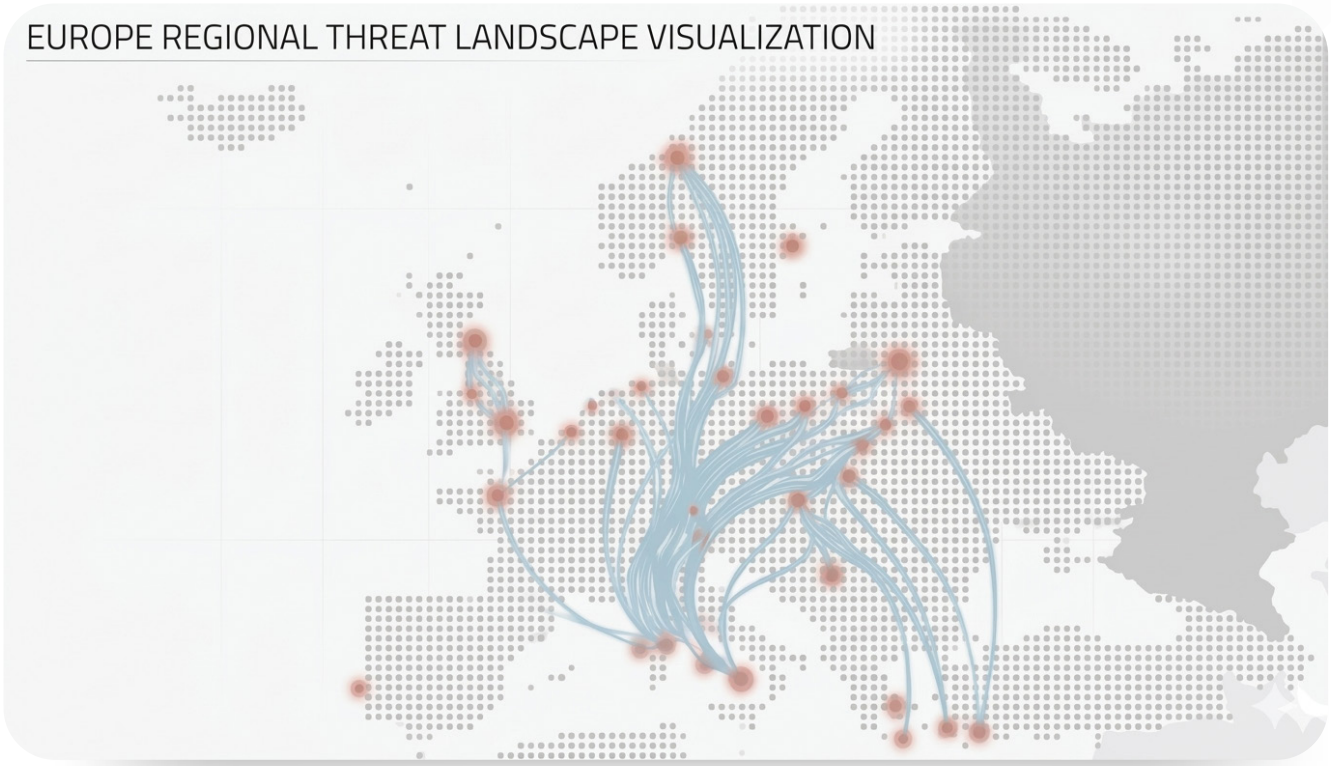
18.9 Key takeaways from an OT perspective

The 2025 threat landscape in South America is characterized by volume over sophistication in most cases. Rather than advanced, targeted OT attacks with physical consequences, the region primarily faces ransomware campaigns that impact industrial operations through encryption and service disruption rather than direct manipulation of physical processes.

The critical vulnerability lies not in novel attack techniques but in fundamental security hygiene-unpatched systems, poor segmentation, inadequate visibility, and insufficient expertise to detect and respond to threats before they cause operational disruption.

However, we must emphasize: the scarcity of detailed, verified public data on specific OT incidents in South America during 2025 suggests either under-reporting, lack of disclosure requirements, or limited investigation into the operational technology aspects of reported incidents. This data gap itself represents a significant challenge for the region's OT security maturity.

19. Regional Threat Landscape Analysis Europe

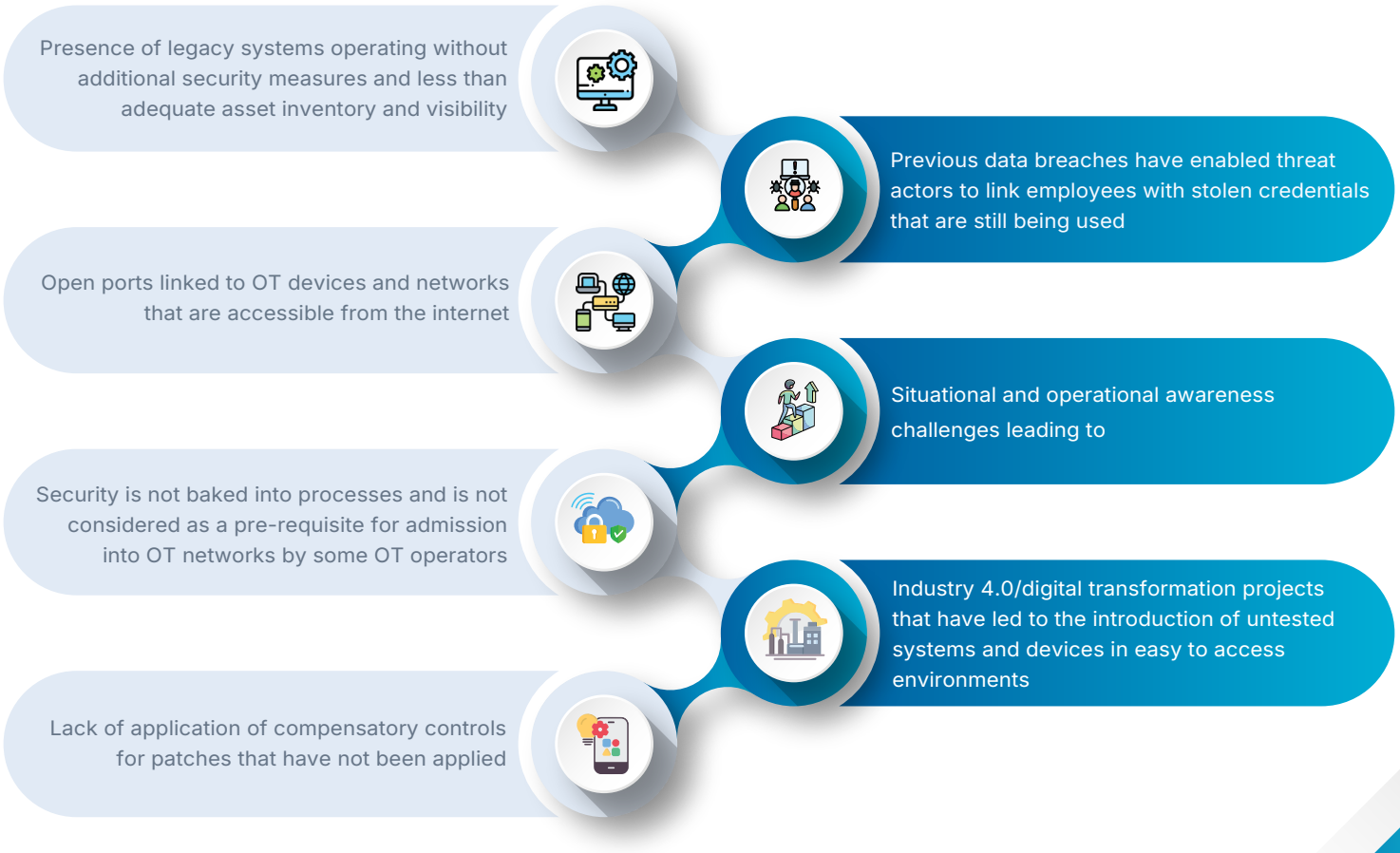


Just like North America and LATAM, the number of attacks logged in Europe rose significantly in 2025. One defining feature of the threat landscape in the region is the high levels of attention this region is receiving from threat actors from countries such as Iran, Russia, China and North Korea. While the first three are chiefly working to disrupt infrastructure and exfiltrate IP and defense information, the last one is working to steal bitcoins and data to sell. Europe is today home to a growing number of threat actors and affiliates. Most of these actors are active and engaged within a larger network of enablers.

Focused attacks on OT in the region witnessed a 70 percent increase in 2025 and there are various reasons for this. Most of the attacks were concentrated on few key sectors.

Our research shows that most of the attacks on OT in the region succeed because of these reasons:





19.1 Unique challenges in Europe

The presence of large clusters where similar facilities are located is helping threat actors and hacktivists focus their geographical targeting efforts. This also triggers a chain of targeting activities that threat actors can initiate. Consider for instance the information in this table where we have three clusters that are home to some of the biggest chemical plants. For hackers this presents a unique opportunity to target the manufacturing capacity of a country through targeted attacks.

- Elevated AI-powered phishing campaigns run in association

Port of Antwerp-Bruges	Antwerp, Belgium	Europe's largest integrated chemical cluster home to 7 of the world's top 10 chemical companies.
Ludwigshafen Complex	Ludwigshafen, Germany	The world's largest integrated chemical site, operated by BASF, with 200 plus plants.
Rotterdam	Rotterdam, Netherlands	Enormous hub with 45plus chemical companies and 5 oil refineries.

Further, in some instances, factories located in such clusters may also:

- Use the same ISP: Factories within the same industrial park or cluster often utilize the same Internet Service Provider (ISP) or local infrastructure, leading to them being assigned adjacent or identical public IP ranges. Hackers use automated scanners to probe these ranges for open ports and services.
- They may be provisioned under the same enterprise WAN contract
- They could also be part of a shared industrial park network
- They use centralized MPLS or SD-WAN backhaul

In such cases, the Public IP blocks may be contiguous, the ASN (Autonomous System Numbers) could match and reverse DNS could even up revealing naming conventions. Hacktivists are known to use such means to identify and target specific factories. The methods used in such attacks could be Passive DNS analysis, BGP route mapping and WHOIS ASN clustering which forms the foundational layer for an attack.

Another way in which threat actors can take such gaps to another level is through the use of OT Metasearch Engines. Specialized tools like Shodan or Censys act as search engines for the Internet of Things (IoT). They index exposed Industrial Control Systems (ICS) and SCADA devices by their IP addresses, often including screenshots of control panels that identify the specific facility and its vulnerabilities.

Factories located within the same clusters could also end up sharing supply chains. This makes it easier for hackers to enter multiple targets by moving laterally across identified networks. A less secure vendor in the chain could compromise a big part of the cluster itself this way.

As mentioned in the report on internet accessible systems, legacy protocols such as Modbus or BACnet can easily be discovered by sniffing network traffic. This allows attackers to identify the specific hardware (such as controllers) used across a cluster and use unpatched vulnerabilities in the devices to target the network and the infrastructure.

CRITICAL CLUSTER EXPOSURE POINTS SUMMARY



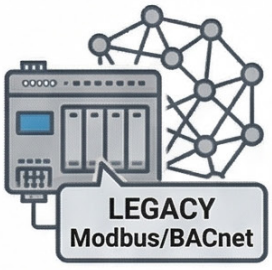
SHARED ISP & IP RANGE



SHARED ENTERPRISE WAN

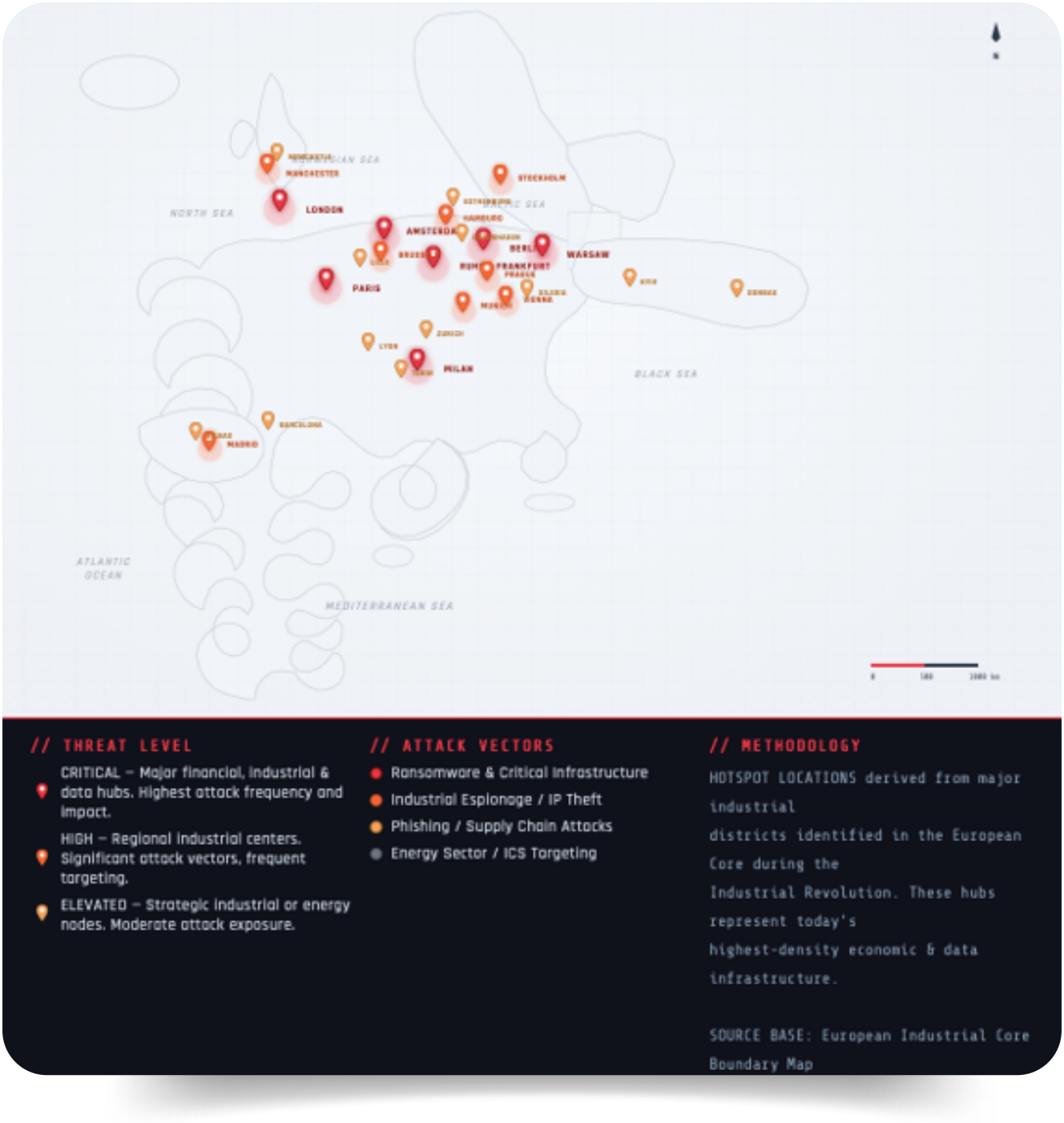


OT METASEARCH ENGINES



LEGACY PROTOCOLS DISCOVERY

19.2 Cluster level attacks logged in European honeypots



The presence of attack hotspots close to major industrial clusters reveals the nature of attention that such clusters are receiving from hackers. The high level of probing is indicative of interest and confidence that hackers are investing in these regions. State-backed actors that are participating in such scans may be eyeing future attacks at times of geo-political stress.

Attacks on such clusters could also indicate investments in speculation by threat actors. When refining (and/or mineral processing capacities, for instance, are taken offline, the threat actor gets to profit from speculating on the prices of commodities. We have pointed this out before.

19.3 What motivates threat actors in Europe?

Motivation	Percentage
Geo-politics	18
Geo-economics	10
Ransom	18
Disruption	6
Malware testing	2
Access sale	9
Reconnaissance	17
Data exfiltration	15
Unknown	5

In addition to conventional motivations such as geopolitics and geo-economics, threat actors are maintaining a very high level of surveillance on the region. With clear geopolitical faultlines, cyberspace here is reflecting the geopolitical realities the region faces today. In addition to having a large volume of threat actors of all hues, Europe is also home to a large number of newer threat actors and affiliates turning active every year.

Percentage attacks on sectors

Sector	Percentage
Utilities (Power)	14
Utilities (Renewables)	7
Water supply and management	3
Oil and gas (Refineries)	18
Oil and gas (Field activity)	4
Repetitive manufacturing (Electronics, toys, confectionery)	1
Discrete manufacturing (Clothing, automotive, firearms, medical devices)	7
Batch manufacturing (Food and beverage, pharmaceuticals, plastics)	7
Continuous manufacturing (Fertilizer production, chemical processing, pharmaceuticals)	6
3-D printing/additive manufacturing	3
Transport (Railway systems of all types)	7
Transport (Ports – inland and sea facing)	5
Transport (Airports)	7
Transport (Pipelines)	4
Others\undefined	7

19.4 Detection vs recovery: Europe Vs RoW

	Europe	ROW
	Average (Days)	Average (Days)
Detection	19	66
Recovery	77	63

19.5 Critical infrastructure: Regional sector risk profiles

Sector	Current Risk Level	Threats
Energy and Utilities (Power Generation, Oil and Gas, Water /Wastewater):	Very high	Presence of complex threat actors with newer versions of malware and modified stealthy payloads increases the risk. Availability of stolen data that can be used to craft targeted phishing and asset-level attacks on enterprises
Manufacturing and industrial	high	Attacks on clusters and targeted attacks on specific manufacturers. These attacks are highly complex, sophisticated, multi-modal and targeted.
Transportation and Logistics (Rail, Maritime, Aviation)	high	Supply chain issues and due to threat actors targeting large scale disruption. With extended supply chains, the visibility of components becomes opaque making it easier for poisoned components to enter extended supply chains
Healthcare and Life Sciences (Medical IoT)	Medium	Mostly due to independent threat actors who are after data or ransom
Smart Buildings and facilities management	Medium	Due to the large number of threat actors targeting this sector.

19.6 Cross-sector risk interdependencies and cascading failure scenarios

In addition to unique threats to sectors, there is also the possibility of threats moving across sectors causing a cascading failure. For instance, through a multi-modal payload, both a building management system as well as a sub-station or power distribution infrastructure can be targeted through the same campaign (if they share a network). While instances of such attacks are low right now, as cyberattacks improve in sophistication, such scenarios will become commonplace. However, if critical infrastructure operators resort to putting IEC 62443-based zones and conduits in place, cross sector attacks and the risk from lateral movements can be minimized.

19.7 Common regional attack vectors and exploitation pathways

The commonly observed and documented pathways that threats are taking in OT environments in the region are as below:

Initial access vectors specific to OT/IoT Environments

Type of attack	Current Risk Level	Commonly seen in
Remote Access abuse (VPNs, Jump Hosts, Remote Desktop Protocol)	Attackers use stolen credentials to log in through legitimate entry points like VPNs or Remote Desktop Protocol, allowing them to bypass the perimeter and move laterally as "trusted" users.	Oil and gas, manufacturing and utilities and in sectors with remote sites separated by vast distances
Spear-phishing targeting engineering and OT personnel	Highly personalized (and timed) work-related emails crafted to exploit the specific technical roles of engineers, often containing malicious attachments or links designed to harvest credentials or drop ICS-specific malware.	Across all sectors
Exploitation of Internet -Exposed HMIs and Engineering Workstations	Involves targeting Human-Machine Interfaces (HMIs) that are mistakenly left reachable from the public internet, allowing attackers to directly manipulate industrial processes without needing complex exploits.	Oil and gas, process-oriented manufacturing and utilities and in sectors with remote sites separated by vast distances
Supply chain compromise (Firmware, Software Updates, Third-Party Vendors)	Attackers inject malicious code into official software updates or hardware components at the source, turning a trusted vendor into an unwitting delivery vehicle for a "Trojan horse."	Across all sectors
Exploitation of Known CVEs	Adversaries take advantage of publicly disclosed software vulnerabilities	Across sectors
Misuse of removable media	Infected USB drives or portable devices are used to bridge "air-gapped" networks, introducing malware directly into isolated systems that have no connection to the outside world.	Manufacturing and utilities
Exploitation of known CVEs	Adversaries take advantage of publicly disclosed software vulnerabilities	Across sectors
Misuse of maintenance windows	Threat actors time their malicious activities to coincide with scheduled downtime, as security alerts during these windows are often ignored or dismissed by staff as "noise" from testing.	Manufacturing, maritime, oil and gas and utilities
Insertion of decoy systems	In an offensive context, the attacker deploys rogue devices or "man-in-the-middle" hardware that mimics legitimate controllers to provide false data to operators while the real process is being sabotaged.	Manufacturing, maritime, oil and gas and utilities

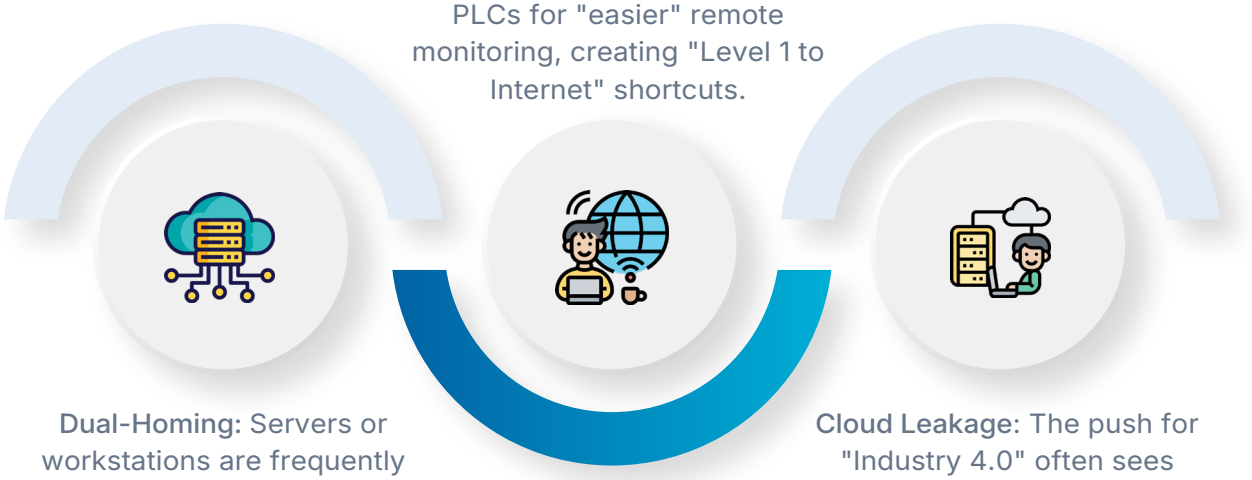
19.8 Lateral movement: Crossing the IT/OT Boundary

While most OT operators in Europe have deployed measures to prevent lateral movement of threats, because of the lack of adherence to cyber hygiene measures, threats are able to move laterally and cover a larger portion of the infrastructure. Here are some of the commonly observed security gaps in the region that are enabling lateral movement.

19.9 Purdue Model violations in practice

If the Purdue Model is strictly adhered to, then the data should only flow between adjacent layers through managed interfaces. However, this is not so in practice because of the following violations:

Shadow OT: Engineers bypass security to install cellular modems or direct-to-internet gateways on PLCs for "easier" remote monitoring, creating "Level 1 to Internet" shortcuts.



Dual-Homing: Servers or workstations are frequently configured with two Network Interface Cards (NICs), one for the OT network and one for the IT network, effectively bridging the gap and bypassing all firewall controls.

Cloud Leakage: The push for "Industry 4.0" often sees sensors (Level 0) sending telemetry directly to a cloud provider, bypassing the entire security stack.

19.10 DMZ traversal and historian exploitation

The Industrial DMZ (iDMZ) is supposed to be a "buffer zone" where IT and OT never meet (directly) face-to-face. However, Data Historians often turn into the most common weak point in this defense. This has been observed consistently in repetitive, discrete and process -based manufacturing and oil and gas sectors. Because Historians must collect data from the factory floor and serve it to business analysts, they often have specific or diluted "allow" rules in both the IT and OT firewalls. If an attacker compromises the Historian through an unpatched vulnerability or stolen credentials, they gain a "trusted" platform inside the iDMZ. From here, they can traverse "South" into the control network by piggybacking on the legitimate polling connections the Historian uses to talk to PLCs thereby breaking the Purdue Model.

19.11 Living-off-the-Land (LOTL) in OT Environments

Once an adversary is inside, they rarely use custom malware (which can be easily detected). Instead, they use Living-off-the-Land tactics that use the legitimate tools already present in the environment to perform malicious acts.

- **Engineering software**: Attackers use the actual vendor software (like TIA Portal or Studio 5000) to push malicious logic to controllers. To a security monitor, this looks like a standard update.
- Native Protocols: They use built-in protocols like Modbus, EtherNet/IP, or OPC UA to send "Stop" or "Write" commands. Since these protocols lack inherent authentication, the device simply obeys.

- Admin Tools: Using wmiexec, PowerShell, or SSH to move laterally across the network without ever dropping a single malicious file on the disk.

19.12 Lack of Zones and network breaks

The absence of internal segmentation (zones) is the primary reason localized incidents become site-wide disasters.

- The "Flat Network" Problem: In many plants, once you are past the perimeter firewall, there are no internal "network breaks." Every device can talk to every other device (East-West traffic).

- Facilitating movement: Without Micro-segmentation, an attacker who compromises a single HMI in the packaging area can easily reach the safety controllers (SIS) in the chemical processing area. There are no "speed bumps" to trigger alerts or slow the progression of an attack.

Purdue Model breaks are also responsible for a lag in threat detection. As the threat moves laterally and accesses more parts of the infrastructure, the blast radius also increases once the payload is executed or the ransomware triggered.

19.13 The firmware challenge

Firmware implants and bootkits also provide deep persistence in systems by embedding malicious code at the hardware-firmware level, surviving OS reinstalls and resets. PLC logic manipulation alters industrial control systems for sabotage, while rogue device implantation introduces hardware threats for long-term access.

Firmware Implants

Firmware implants target low-level components like UEFI/BIOS, TPM modules, or peripherals (e.g., network cards, monitors). They modify boot processes or SMRAM to execute code before the OS loads, using techniques like polymorphic encryption to evade detection and signature spoofing to bypass verification. These survive BIOS flashes, hardware swaps, or full rebuilds via "firmware cross-contamination," where infected peripherals reinfect clean systems.

Bootkit Techniques

Bootkits hook into the boot chain, patching bootloaders, option ROMs, or device initialization for pre-OS execution. Persistence relies on nonvolatile storage like SPI flash or management controller images, restoring payloads across power cycles without disk files. Advanced variants use hardware rootkits, such as microscopic FPGAs added during manufacturing, enabling data exfiltration via subtle signals like monitor power modulation.

PLC Logic Manipulation

Attackers modify PLC ladder logic or data manipulation instructions (such as arithmetic, comparisons, PID loops) to alter control processes like temperature or flow regulation. Techniques include injecting false sensor data, changing setpoints via BCD inputs, or exploiting data type conversions for unintended outputs like activating valves out of sequence. This enables sabotage in ICS environments, with persistence through reprogrammed firmware or sealed logic that ignores external resets.

Rogue device implantation

Rogue devices, like compromised USBs or physically implanted hardware (such as FPGA on controller boards), gain initial access and maintain footholds. They exploit supply chains for pre-infection or use badUSB emulation to inject bootkits. Persistence comes from self-replicating firmware that hooks drivers or modulates hardware signals for covert C2, surviving firmware updates.

19.14 Continuing impact of the Ukraine-Russia war on cyberspace

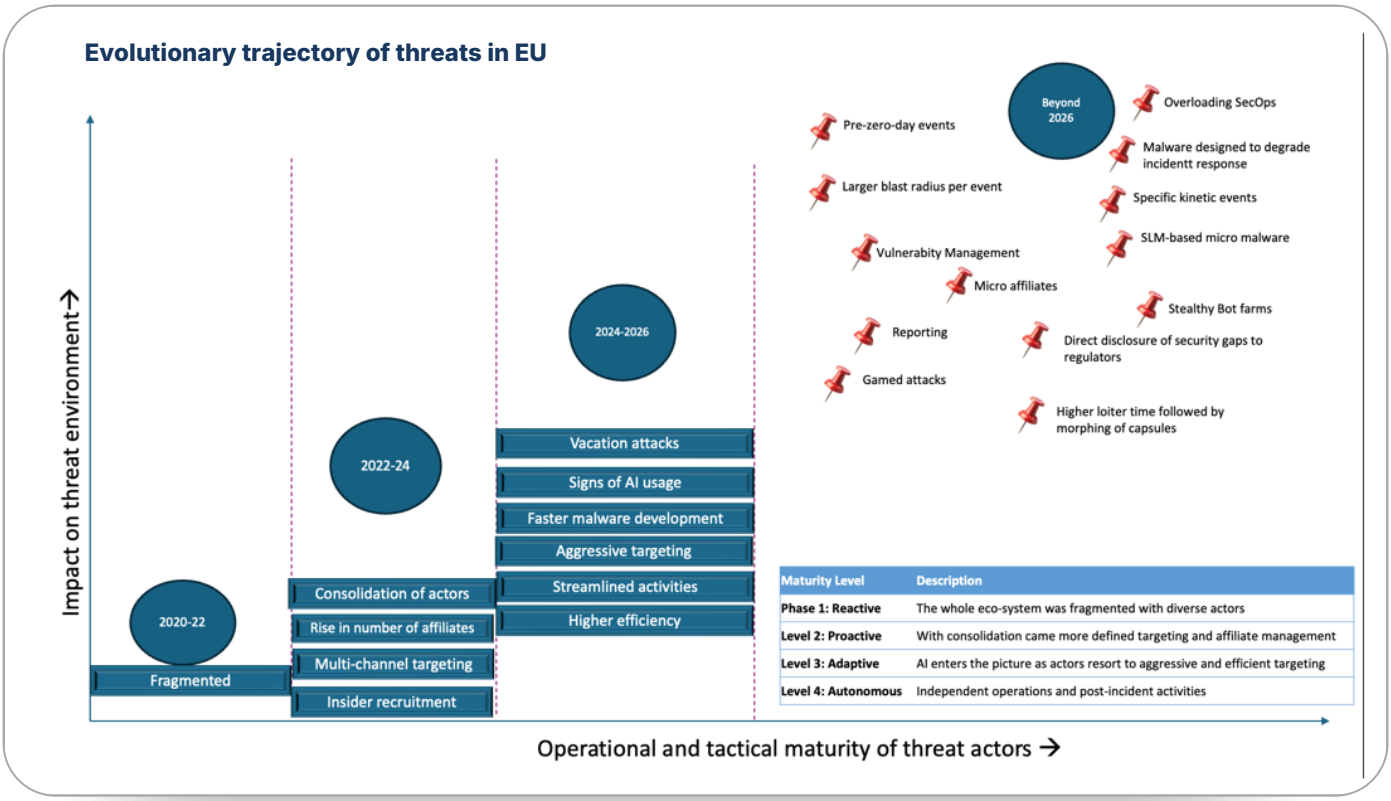
Among all war zones, the conflict in Ukraine is the one that has had significant implications on cyberspace. Right from the earliest attacks on Ukrainian infrastructure in the middle of the last decade all the way to the highly targeted attacks on Ukrainian utilities and defense establishments, this war has contributed in a multitude of ways to the evolution of complex threats and TTPs. It is important to contextualize the evolution of threats with this ongoing conflict. The primary impact of this conflict was evident across the following areas (with global implications):

- Operational changes: Changes in the affiliate models that state-backed actors were relying on
- Malware development cycles: Faster malware development cycles timed to match events on the battlefield
- Kinetic attacks: Such attacks are no longer a no-go
- **Multi-level correlation:** Threat actors have started co-relating target-related data from multiple platforms
- **Stolen data:** is channeled to intelligence agencies rather than being released on the dark web
- **Posturing:** Threat actors are pretending to be after ransom while the real objective is data or access to a system of interest. Masking of intentions may lead to CERT teams and regulators not assigning the right level of security interest to a threat actor

While some of these changes (as we have indicated earlier) are part of the overall evolution of threats, the conflict has expedited the evolution. Such changes have put an additional evolutionary pressure on the cybersecurity teams defending critical infrastructure and enterprises. Driving these pressures are three key factors: unpredictable threat environments, accelerating threat evolution, and the non-linear nature of modern incidents that typically involve multiple escalations occurring in parallel (case in point, Jaguar Land Rover incident).

Europe has entered an era where it is now a primary target of most malware development activities occurring within the boundaries of the region itself. By the end of this decade, the evolving interplay between sophisticated threat actors and emerging attack vectors is likely to give rise to a new tier of geopolitical risk. We are talking of a risk that will articulate itself by holding enterprises hostage at scale. This translates into a large blast radius involving multiple enterprises that may share a common supply chain, host similar systems (and/or architectures), follow similar security practices or are at a similar stage of cyber maturity.

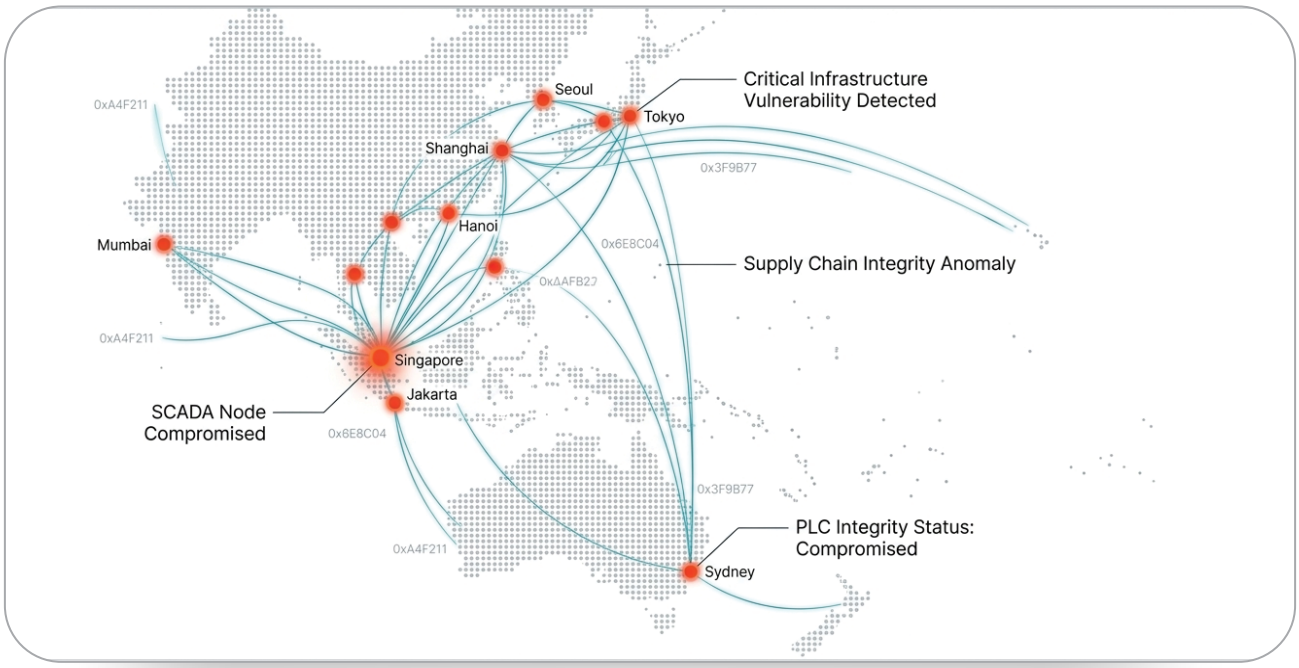
When the conflict started, the elements supporting such a trend were already in place. There were evolved threat actors, malicious payloads being developed, massive affiliate recruitment programs being run and smaller breaches that were exposing data and information on security tactics adopted by enterprises. Nearly half a decade on, we have watched the entire cycle mature and evolve into a far more structured, and formidable, threat landscape.



Maturity Level	Description
Phase 1: Reactive	The whole eco-system was fragmented with diverse actors
Level 2: Proactive	With consolidation came more defined targeting and affiliate management
Level 3: Adaptive	AI enters the picture as actors resort to aggressive and efficient targeting
Level 4: Autonomous	Independent operations and post-incident activities

20. Regional Threat Landscape Analysis Indo-Pacific

The Indo-Pacific region in the context of this report refers to a region comprising the following countries:



- Australia
- Bangladesh
- Brunei
- Cambodia
- China
- Cook Islands
- Fiji
- French Polynesia
- India
- Indonesia
- Japan
- Kiribati
- Laos
- Malaysia
- Maldives
- Marshall Islands
- Micronesia
- Myanmar (Burma)
- Nauru
- New Zealand
- Singapore
- Thailand
- Vietnam

There are many variations of the definition of Indo-Pacific but we felt that it is best to group the above countries together to cover the broader Asia-Pacific region.

The region's geopolitical landscape shifted significantly in 2025 as latent fault lines fractured into active, kinetic conflict. Most notable were the renewed escalations between India and Pakistan and the brief but intense border war between Thailand and Cambodia. The former led to a major activation of regional cyberspace while the latter conflict was mostly restricted to the war zone itself.

In addition to these conflicts, this region is also home to the entire cyber firepower of China's Ministry of State Security. As mentioned earlier, China is utilizing its APT groups to target specific countries and regional groupings such as ASEAN. China's APT groups dominate the regional cyberspace followed by those linked to Russia and Iran. China's APT groups are registering their presence across segments. China could also be maintaining a watch on diplomatic exchanges and defense procurement priorities through compromised servers stealthily present in environments linked to such activities.

The Indo-Pacific region also serves as a testing ground for TTPs and malicious payloads linked to Chinese APT groups. China also played a major role in the Indo-Pakistan conflict as well. The expanded role of Chinese APT groups also aligns with the larger geo-political ambitions China is nurturing as well as its attempt to project power across the globe. This approach mirrors the geo-political playbook maintained by the Soviet Union (and Russia continues to maintain). The only part that China has refined is the higher level of surveillance China is maintaining on countries like Pakistan that are considered to be friendly to China.

The communications snooping in the region is a diversified activity. Telecommunications and internet providers are used to steal data and track targets in the region. In addition to laptops and mobile phones, these groups target switches and firewalls running with unpatched CVEs.

20.1 Specific TTPs observed in the region

Chinese Advanced Persistent Threat (APT) actors have been seen to employ a multi-layered approach to network penetration, focusing on stealth and the exploitation of inherent trust within enterprise architectures in corporate environments in the Indo-Pacific region. Such an approach also covers businesses that are not immediate targets but may serve as a conduit to access target networks in other enterprises or to mask traffic.

20.2 Breaching perimeter defense

To overcome perimeter defenses, these actors prioritize the compromise of edge devices including firewalls, routers, and even VPN concentrators that often lack the same level of logging and endpoint protection as internal servers.

By seizing control of these assets, they leverage the trusted relationships that are associated with these assets to utilize:

Private interconnections: They target provider-to-provider or provider-to-customer links (such as MPLS or dedicated peering lines).

Administrative tunnels: By moving through established pathways, their malicious traffic appears as legitimate internal data, allowing them to pivot into "island" networks that are otherwise air-gapped from the public internet.

Deferred throttling: This involves a sudden spike in activities initiated by the latent threat during specific windows (such as maintenance or lean staffing periods) which could be a payload or triggering of a firewall rule to allow certain types of traffic.

20.3 Network traffic manipulation and monitoring

Once deep within the infrastructure, the actors transform the compromised network hardware into a passive data collection platform. They manipulate routing tables and enable advanced monitoring features to gain total visibility without alerting traditional security software. This is achieved by:

- Traffic mirroring: By enabling SPAN (Switch Port Analyzer), RSPAN, or ERSPAN, they can clone all data passing through a switch and send it to a controlled destination and gain a high level of awareness on the asset topology and traffic characteristics.

- Routing modification: They may implement static routes to redirect sensitive traffic flows, ensuring that high-value data passes through a point where it can be intercepted or exfiltrated.

20.4 Extended network access and stealthy data exfiltration

To maintain long-term access and hide their command-and-control (C2) communications, these actors wrap their activities in standard protocols to blend in with encrypted traffic.

- Encapsulation: They frequently configure Generic Routing Encapsulation (GRE) or IPsec tunnels

- The objective: Create a secure "private" path for stolen data to leave the network without detection, often masked as routine site-to-site administrative traffic. This effectively turns the organization's own infrastructure against itself, using authorized protocols to bypass Data Loss Prevention (DLP) systems.

20.5 Large scale exploitation and persistence

Unlike "smash-and-grab" cybercriminals, these APT groups operate on an industrial scale with plenty of patience:

- Wide-scale vulnerability scanning: They simultaneously target large numbers of Internet -exposed devices across vast IP ranges, looking for unpatched vulnerabilities in common network appliances. Since this region is home to a large number of internet exposed devices, it becomes easier to locate and target such devices.

- Recurrent access: Even after a system is cleaned, these actors often return to re-compromise the same systems using alternative backdoors or stolen credentials, ensuring they maintain a persistent foothold for follow-on intelligence gathering operations.

The net result is the same. The risk to enterprises increases manifold within a short period of time. However, the actual risk exposure of enterprises varies as per many factors. Delayed deployment of patches and other security gaps often contribute to such risks as well.

A lack of updated asset inventory and architecture diagram hits regional enterprises in two ways:

- Threat actors are able to insert digital decoys without being detected
- During an incident, lack of adequate asset information leads to entire assembly lines or pipelines or substations being shut to prevent the propagation of the attack as well as to ascertain the blast radius

The prevalence of APT groups, hacktivists and corporate espionage driven threat actors creates a complex threat environment where attacks occur in short yet intense cycles. The same victim may be breached by multiple threat actors who have different objectives or maybe targeting different parts of the infrastructure. Some of the threat actors may lay low before surfacing with an event while others may make their present apparent in the short-term.

The line between APT groups and independent threat actors is very thin in this region which leads to a situation wherein actors exchange sides in a jiffy and attribution becomes a complex affair.

Threat chains exist with hacktivists and corporate spies at one end and an APT actor at the other with each actor contributing in some way to the targeting, hacking, compromise and data exfiltration/ransom collection. Such chains also enable APT groups to recruit and train highly skilled talent. Threat actors commonly exchange individual team members based on suitability to the specific projects undertaken by the group.

20.6 What motivates threat actors in Indo-Pacific?

Motivation	Percentage
Geo-politics	30
Geo-economics	4
Ransom	15
Disruption	9
Malware testing	1
Access sale	7
Reconnaissance	14
Data exfiltration	14
Unknown	6

It comes as no surprise that attacks motivated by geopolitical considerations dominate the motivation table. With the Chinese APT engines firing on all cylinders and with major contributions from Iran and Russian, the threat landscape converges around APT groups from these countries. While Indo-Pacific was being used as a testbed for new malware and variants as late as February 2025, Latin America has now emerged as the new leader in that space. With a significant increase in affiliate groups in Latin America, these groups have started using the regional cyberspace as a test bed for new malware as we have indicated before.

The scale at which activities such as access sale and data exfiltration are carried out has not reached levels that we are seeing elsewhere. The presence of geo-political faultlines amplifies the role of APT groups who may themselves be playing the role of regular hackers by accessing and selling data. North Korean APT groups are experts in monetizing stolen data.

Percent attacks on various sectors

Sector	Percentage of overall attacks
Utilities (Power)	25
Utilities (Renewables)	1
Water supply and management	1
Oil and gas (Refineries)	16
Oil and gas (Field activity)	1
Repetitive manufacturing (Electronics, toys, confectionery)	7
Discrete manufacturing (Clothing, automotive, firearms, medical devices)	9
Batch manufacturing (Food and beverage, pharmaceuticals, plastics)	10

Sector	Percentage of overall attacks
Continuous manufacturing (Fertilizer production, chemical processing, pharmaceuticals)	11
3-D printing/additive manufacturing	1
Transport (Railway systems of all types)	6
Transport (Ports – inland and sea facing)	2
Transport (Airports)	4
Transport (Pipelines)	1
Others\undefined	5

The large volume of attacks on utilities and oil and gas infrastructure reinforces the active presence of APT groups in Indo-Pacific. Manufacturing is also a sector of interest though attacks on manufacturers are dominated by non-APT actors most of whom are affiliates linked to some of the groups we have already mentioned in the first half of this report. However, from the data available, one could come to the conclusion that affiliates in Indo-Pacific enjoy a greater degree of freedom in:



The region has fewer affiliates than other regions which makes it tough to ensure loyalty and this also forces major ransomware groups to offer concessions beyond what is offered elsewhere.

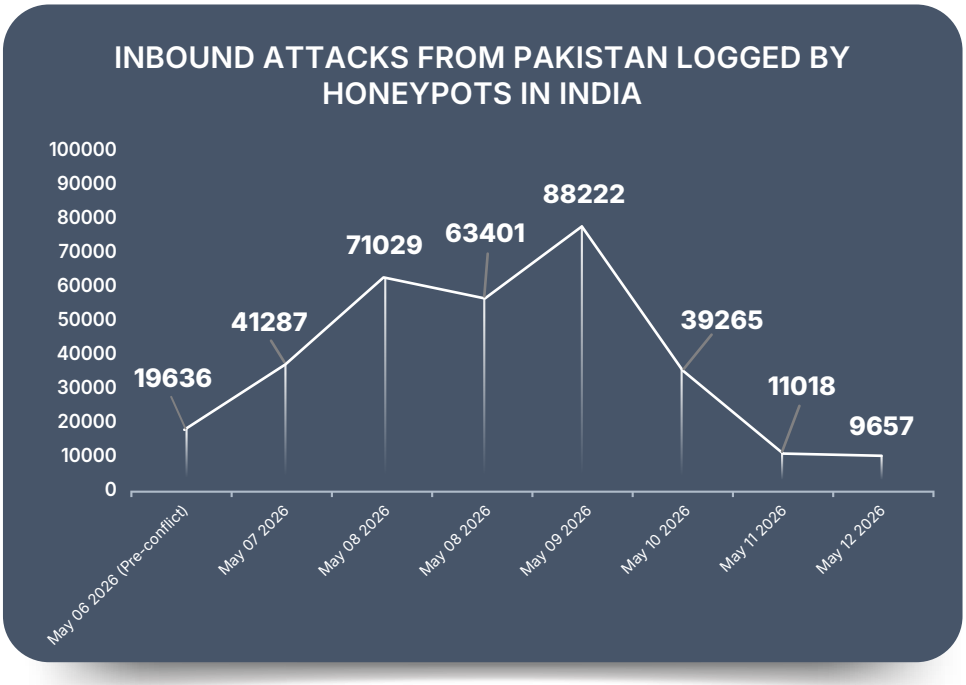
20.7 The Indo-Pakistan conflict spills over into cyberspace

As per the Stimson Center "following a terrorist attack on April 22, India launched punitive strikes on Pakistan on May 7. This began a four-day conflict between India and Pakistan from May 7-10". This conflict and the one preceding it in 2019, triggered regional cyberspace in a big way. There seems to be an established pattern to the way Pakistan activates its cyber threat actors and affiliates during a conflict.



The observed and recorded patterns associated with Pakistani threat actors during the conflict is as under:

- Operational activation window: 3-7 Hours after any major geopolitical incident
- In the first phase of attacks, Pakistani threat actors targeted websites associated with the India central and state government agencies and civic bodies. These attacks were meant to deface the sites in numbers that are sufficient enough to keep incident response and security teams busy and distracted. Most of these attacks were carried out by new recruits or even students who were assigned specific projects by their handlers
- The second phase involved targeting defense facilities and the most critical infrastructure through phishing campaigns at scale. Such attacks were carried out from multiple geographies using bot farms located within and outside Pakistan. Pakistani cities such as Karachi, Lahore, Islamabad, and Quetta are known to host large volumes of compromised or sold network access panels. Some of these bot farms also moonlight as click farms for promotional and propaganda activity on social media
- In the last phase, an intense follow-up campaign was run to test the compromised networks as well as to target the facilities that resisted comprise in the last two phases.



Since India responded rapidly to block the IPs and contain any intrusion, there was little to no impact of this campaign on Indian cyberspace or infrastructure except for a spike in traffic. Pakistani threat actors are primed towards volume-based attacks. Which translates into 1000s of attacks with the assumption that one of them will be successful and deliver the payload or results they want.

The steep deescalation seen on the evening of May 10th also points to something unique about the Pakistani cyber threat actors. Some of the key members were members of the armed forces who were pulled back into their respective units as the war entered its final phases and Pakistan wanted to avoid its cyber threat teams from being targeted by revenge attacks from India which had started peaking at this time. Pakistan had also shifted into a very high decibel campaign to prove that it had "successfully hacked into many Indian establishments and leaked sensitive data". No evidence whatsoever was provided for this claim at any point of time during the operations or after that.

In addition to the inbound attacks, spoofing attacks were carried out from various domains using themed emails and messages.

Category	Phishing / C2 Domain	Mimicked Entity / Lure
Government Spoofing	zohidsindia[.]com	Likely targeting ZOHO/Gov mail users
	nationaldefensecollege[.]com	National Defence College (NDC)
	nationaldefencebackup[.]xyz	Defence backup services
	jkpolice[.]gov[.]in[.]kashmirattack[.]exposed	Jammu & Kashmir Police
	iaf[.]nic[.]in[.]ministryofdefenceindia[.]org	Indian Air Force / MoD
	email[.]gov[.]in[.]modindia[.]link	Government Email Service (Kavach)
	email[.]gov[.]in[.]indiangov[.]download	General Government login
	email[.]gov[.]in[.]drdosurvey[.]info	DRDO Survey/Feedback
Event-Based Lures	pahalgamattack[.]com	News/Reports on the Pahalgam attack
	operationsindoor2025[.]in	Fake "Official" Operation reports
	sindoor[.]website	Information on the military operation
	sindoor[.]live	"Live updates" on the conflict
Malware Delivery	fogomyart[.]com/random.php	Macro-based web query redirect

Domain information about operationsindoor2025.in, one of the malicious URLs used in the phishing campaign. It is worth noting that this domain was registered on May 7th the day the conflict began.

Domain Information

Domain:	operationsindoor2025.in
Registered On:	2025-05-07
Expire On:	2027-05-07
Updated On:	2025-05-30
Status:	clientUpdateProhibited clientDeleteProhibited serverHold clientRenewProhibited clientTransferProhibited
Name Servers:	ns10.domaincontrol.com ns09.domaincontrol.com

IP address	Associated Malware	Notes
167.86.97.58	**Crimson RAT**	Port 17854. Used for primary data exfiltration.
164.215.103.55	**Go-based Spyware**	Port 8080. Targeted Linux (BOSS) systems.
93.127.133.9	**Crimson RAT**	Ports 12345 / 54321. Identified in late-stage lures.
91.215.85.21	**Eliza RAT**	Frequently reused infrastructure for Gov targeting.
45.153.241.15	**Transparent Tribe**	General C2 node for phishing redirects.
2.56.10.86	**CapraRAT**	Primarily used for targeting Android devices.

20.8 Malicious phishing and payload URLs

Payload Delivery:

- seemysitelive[.]store (Hosted Go-droppers for Linux)
- aeroclubofindia[.]co[.]in (Spoofed aviation site hosting MSI installers)
- trade4wealth[.]in (Used by SideCopy for .NET loader delivery)
- indiangov[.]download (Spoofed NIC mail portal)

Macro-Triggered Redirects:

- fogomyart[.]com/random.php (The primary "phone home" URL for .xlam lures)
- zohidsindia[.]com (Mimicking Zoho/Gov infrastructure)

Themed Lures (2025 Specific):

- pahalgamattack[.]com
- operationsindoor2025[.]in
- sindoor[.]live

20.9 Strategic context

Overall, Pakistan's cyber threat playbook is designed to be highly reactive and episode oriented. Pakistan deployed this playbook during its conflict with India. Indian cyberspace and critical infrastructure started receiving huge volumes of diverted and compromised traffic from 17 IP clusters within the first four hours of the conflict. In addition to unleashing its core APT groups, Pakistan also launched cyberattacks through its proxies and affiliates some of which have IP addresses linked to few Not-for-profit organizations Karachi, Quetta, Sukkur and Peshawar.

The high level of inbound traffic from Pakistan into Indian cyberspace was further routed through compromised device clusters in various parts of South East Asia and Latin America as well. Such routing was meant to mask the origin of the traffic, beat firewalls where specific IP ranges were blocked and create enough noise to tie down and tire out cybersecurity teams.

Pakistani bot farms and malicious payloads were not known to possess certain capabilities that were demonstrated during the conflict. It is possible that Chinese APT groups were offering targeting guidance and degraded malware versions to their Pakistani counterparts. The appearance of many variants of known malware within a short period of time (without any precedent or alignment with known capabilities of Pakistani APTs, lack of detection of test variants of such malware as well as lack of alignment with known malware development cycles of Pakistani threat actors) during the duration of the conflict. Such a collaboration is not rare Chinese APT 41 is known to work with North Korean APT groups.

The collaboration with China is the most strategically consequential and underappreciated layer of Pakistan's cyber threat posture. The evidence here comes from credible institutional sources and should be treated seriously. Carnegie Endowment for International Peace notes that China and Pakistan have been alleged to be implicated, at times jointly, in cyber incidents aimed at undermining India's strategic and economic interests. The i-Soon leaks of early 2024 provided insight into China's hacking industry and highlighted this potential link, with Chinese state-affiliated groups targeting India's defense, telecommunications, and government networks.

RUSI explicitly flags that for India, the prospect of deepening cyberspace collaboration between Pakistan and China adds another layer to the already robust defense partnership between the two countries.

At the formal policy level, Pakistan and China recently agreed to enhance cooperation in intelligence sharing and cybercrime prevention, with the understanding reached during a meeting between Pakistan's Federal Interior Minister and China's Ambassador.

The operational convergence is significant even without a formal joint cyber operations framework. China benefits from Pakistani APT groups targeting India because it reduces operational exposure for Chinese groups on the most sensitive targets. Pakistan benefits from Chinese cyber tradecraft, tool development, and intelligence that could be shared through the broader CPEC security framework. Both countries have a convergent interest in keeping India's strategic planners occupied and its defense networks penetrated.

Lastly, Pakistan and China are also known to be collaborating on a project to enhance the strength of GPS spoofing signals to confuse aircrafts.

20.10 A primer on Pakistani cyber threat actors

APT36 / Transparent Tribe (also: Earth Karkaddan, Mythic Leopard, Storm-0156, COPPER FIELDSTONE, ProjectM)

This is Pakistan's most documented, persistent, and strategically significant APT group. APT36 has been active since at least 2013, with an overarching goal of cyber espionage primarily towards institutions and individuals related to strategic interests of South Asia, specifically India. Unlike ransomware actors seeking financial gain, APT36 is an intelligence -gathering operation for the long haul, where the attacker wants the victim to remain unaware of the attack for as long as possible.

The group's evolution is instructive. Between 2010 and 2014, Pakistani hackers primarily conducted website defacements and basic phishing. From 2015 to 2019, APT36 matured toward credential theft, malware infiltration, and sustained surveillance of India's defense and diplomatic networks. From 2020 to 2024, the group developed Android malware targeting Indian military personnel through fake applications and deployed advanced Windows-based trojans with layered obfuscation. By 2025, the focus moved to Linux-specific targeting, particularly against India's indigenous BOSS Linux system thereby signaling dedicated research capacity and a state-backed commitment to penetrating critical digital infrastructure.

Their targeting profile against India is comprehensive. Primary targets include the Indian government, military, defense contractors, and diplomatic missions. Beyond traditional spear phishing using malicious Office documents and PDFs, APT36 has refined malvertising by registering domains closely resembling official Indian government sites and using paid search ads to drive targeted traffic. Their malware toolkit now spans Crimson RAT, CapraRAT (Android), ElizaRAT, Poseidon (Linux), ObliqueRAT, and cross-platform loaders written in Python, Golang, and Rust. Time zone checks are embedded in binaries to execute only on Indian systems, reducing exposure.

APT36's opportunistic exploitation of geopolitical events is a defining TTP. Following the Pahalgam terror attack of April 2025, APT36 deployed Pahalgam-themed PDF documents to target Indian government and defense personnel, leveraging both credential phishing and malicious payloads including Crimson RAT, with fake domains impersonating Jammu & Kashmir Police and the Indian Air Force.

In December 2024, the group had deployed CurlBack RAT, Spark RAT, and Xeno RAT against Indian government agencies, defense contractors, maritime operations, and academic institutions, demonstrating both technical adaptability and broad operational reach.

A particularly notable intelligence indicator: forensic analysis of a malicious PDF dropped in an APT36 campaign found that the document was created in Pakistan's +5:00 time zone and authored on a laptop from Pakistan's Prime Minister Youth Laptop Scheme - a telling clue of the campaign's origins.

The most recent development signals further capability expansion. In campaigns codenamed "Gopher Strike" and "Sheet Attack" identified in September 2025, researchers assessed with medium confidence that the activity might originate from a new subgroup or a closely aligned Pakistan-linked group operating in parallel with APT36. Both campaigns shared APT36 TTPs, used new tools, and showed potential use of generative AI in malware development - suggesting either evolution of APT36 or the emergence of a new but coordinated actor.

SideCopy

SideCopy began as what appeared to be a subdivision or sub-cluster of APT36 but has progressively demonstrated independent operational sophistication. Analysis of an open directory found it hosting malware linked to both APT36 (Golang-based Linux payloads) and SideCopy (HTA stagers for Windows), with the C2 server used by SideCopy's RAT payloads sharing the same Common Name typically associated with APT36. APT36 focuses majorly on Linux systems while SideCopy targets Windows systems, adding new payloads to its arsenal - suggesting deliberate division of labor rather than overlap.

SideCopy has targeted Indian Air Force installations, shipyards, and ports. The Stimson Center notes that APT36 and SideCopy are publicly treated as Pakistan-linked and have conducted cyber espionage particularly in India and Afghanistan. Critically, the Stimson Center also flags a severe attribution complication: Russian state-linked group Turla allegedly compromised a network of Pakistan-based SideCopy to spy on Indian networks, creating a false impression and shifting the blame toward Pakistan - reiterating that sophisticated false flag techniques can obscure true threat actor identity. This means Indian attribution to SideCopy carries a non-trivial margin of error, even for technically sophisticated analysts.

Cosmic Leopard / Operation Celestial Force

In the second quarter of 2024, multiple Pakistani-linked threat groups targeting India were reported using Android-based malware. These include Operation Celestial Force, tracked as Cosmic Leopard, and another new group leveraging WhatsApp to deliver SpyNote RAT. Cosmic Leopard represents a mobile-first espionage capability, consistent with ISI's known interest in monitoring Indian military and intelligence personnel through their personal devices.

Hacktivist Clusters as Force Multipliers

Beyond state-linked APTs, Pakistan deploys what are effectively proxy hacktivist groups that provide deniability while expanding the attack surface. India's Maharashtra Cyber agency, in its May 2025 "Road of Sindoor" report, identified seven threat actor groups active against India: APT36, Pakistan Cyber Force, Team Insane PK, Mysterious Bangladesh, Indo Hacks Sec, Cyber Group HOAX 1337, and National Cyber
Crew - employing tactics including malware campaigns, DDoS attacks, GPS spoofing, and website defacement.

Pro-Pakistan groups like Team Insane Pakistan claimed to have compromised the High Court of Andhra Pradesh, allegedly leaking judicial records. The scale during Operation Sindoor was significant: following India's military response in May 2025, over 1.5 million cyberattacks reportedly targeted Indian infrastructure, with DDoS attacks peaking at seven attacks per hour on May 7th. However, the success rate was strikingly low - of approximately 1.5 million attempted attacks on Indian systems, only around 150 were reported as successful.

Assessing Pakistani Cyber Capabilities: A Scorecard

What Pakistan's APT ecosystem is focused on:

Sustained, long-dwell espionage against Indian defense and government targets. APT36 has maintained access to Indian networks for over a decade.

Social engineering calibrated to Indian geopolitical events - the Pahalgam attack lures are a textbook example of rapid operationalization.

Cross-platform malware development across Windows, Linux (including India's MayaOS and BOSS), and Android

Abuse of legitimate cloud infrastructure (Google Drive, Firebase, Telegram, GitHub) for C2, making network-level blocking extremely difficult.

Mobile surveillance operations targeting Indian military and diplomatic personnel.

Infrastructure sharing and coordination between APT36, SideCopy, and emerging clusters that suggest centralized direction, possibly from ISI.

Where capabilities remain limited:

In the second quarter of 2024, multiple Pakistani-linked threat groups targeting India were reported using Android-based malware. These include Operation Celestial Force, tracked as Cosmic Leopard, and another new group leveraging WhatsApp to deliver SpyNote RAT. Cosmic Leopard represents a mobile-first espionage capability, consistent with ISI's known interest in monitoring Indian military and intelligence personnel through their personal devices.

No confirmed destructive attacks on Indian critical infrastructure (power grids, financial systems) at the level demonstrated by Russian or Iranian actors.

The sheer volume of hacktivist attacks during Operation Sindoor (1.5 million) with a success rate of roughly 0.01% suggests that the bulk of Pakistan-aligned cyber activity remains noisy and low-sophistication.

Carnegie notes that India's offensive cyber capacity is likely equal or superior to that of Pakistan.

Pakistan's cybersecurity governance is still evolving and faces legal, normative, and capacity gaps. Pakistan's CERT was only formed in March 2024, while India's CERT-In is a member of the global Forum of Incident Response Teams (FIRST).

Attribution discipline is weak. Pakistani APT operators have left operational security errors including timezone metadata, PMYLS laptop artefacts, and reused infrastructure, all of which have aided forensic attribution.

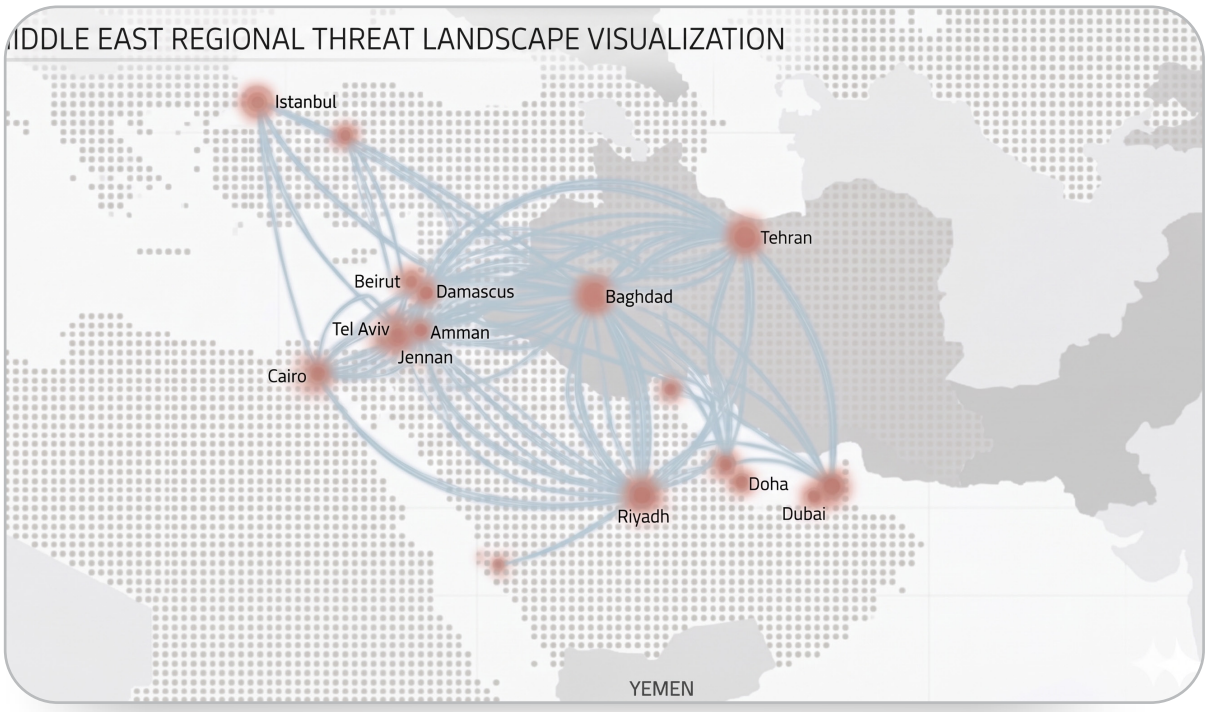
The Attribution Problem

Any intelligence note on this topic must flag the attribution challenge honestly. India and Pakistan do not have a formal attribution policy, making it difficult for independent analysts to assess the validity of their institutional processes. The process involves a loose network of agencies coordinating technical and intelligence findings, raising concerns about the lack of consistent and verifiable evidentiary standards. The Turla-SideCopy false flag incident is a reminder that sophisticated adversaries, including Russia that have actively exploited this ambiguity.

Summary Assessment

Pakistan's APT ecosystem is best characterized as a persistent, ISI-directed intelligence collection operation against India, with a capability ceiling below that of Tier-1 state actors (China, Russia, USA) but well above that of most regional players. The most sophisticated capability is long-dwell espionage rather than destructive cyber warfare. The deepening China-Pakistan alignment on both cyber governance and operational cooperation presents a structural amplification risk for India - not because Pakistani groups will suddenly gain Chinese capability levels, but because the two countries share intelligence, targets, and an interest in keeping India's attention divided across two cyber-active frontiers simultaneously.

21. Regional Threat Landscape Analysis Middle East



The Middle East witnessed another year of increased attacks on all flavors of infrastructure. The cyber dimension of various regional conflicts have now actively moved in scale from observer -reconnaissance into active weaponization and exploitation. They key players in the region are all well known actors. Iranian state-aligned APTs, alongside Russian and Chinese SIGINT collection units, conducted operations targeting Gulf/MENA networks throughout the year. The key activities observed include credential theft via phishing, payload obfuscation on supply chains, lateral movement using Living off the Land Binaries (LOLBins), and persistent access establishment ahead of potential geopolitical escalation. These threat actors are also using Wipers to remove any evidence of their activities.

Geopolitical motivation (including hacktivism) accounts for 34% of all attributed incidents - a proportion consistent with a region experiencing persistent interstate tension. Combined with reconnaissance activity (21%), over half of all attacks carry a state-nexus or pre-positioning signature, indicating that many incidents are not isolated events but components of longer-term strategic campaigns.

The Gulf region is a global data-traffic hotspot due to the convergence of undersea cable infrastructure, cloud service hubs, data centers and multinational enterprise operations. This concentration of digital infrastructure along with strategically important data and persons enables threat actors to blend malicious traffic with legitimate data flows, complicating detection and attribution efforts. The region is also home to several smart city projects and test-beds making it highly lucrative for threat actors to engage infrastructure in the region.

In 2025, many regional conflicts led to a multidimensional confrontation with significant cyber implications for the region as a whole. Escalating political rhetoric and military signaling from various states and their fronts have correlated directly with an observable increase in cyber operations across the region.

21.1 Chief threat actors

Actor	Role	Cyber Posture
Iran	Primary adversary and most active actor	Active throughout the year but turns kinetic in batches. Active offensive operations via MOIS-linked APTs; credential theft, wiper pre-positioning, supply chain targeting
Russia	Opportunistic collector	Multi-modal intelligence collection clandestine operations that blend under Iranian operational noise and cover
China	Strategic collector	Salt Typhoon-linked cluster activity telecom and infrastructure intelligence collection

Iranian threat actors are among the most active ones in the region. Just like its counterpart in the armed forces, Iran's cyber threat wings operate via a mosaic model. This means that teams have a certain level of functional autonomy and operate through a tiered leadership structure. In addition, the members of Iranian APT groups are spread across the country and follow well tested operational playbooks that define actions to be taken when connectivity fails. Iranian cyber teams are well aware of the possibility of connectivity failure impacting operations during a war and they have gamed this very scenario into their operational resilience models. This represents a high level of evolution, operational awareness and residual strike capability (the ability to bounce back when cornered).

Russian and Chinese interest

Known Iranian APT actors and their mandate

The following table summarizes the principal Iranian APT groups and our assessment of the mandates assigned to them

APT / Group	Sponsor	Primary Mandate
APT33 (Refined Kitten)	IRGC	Destructive malware, critical infrastructure sabotage, prolonged recon
APT34 / OilRig	MOIS	Espionage, data and credential theft, long-dwell access
APT35 / Charming Kitten	IRGC-IO	Spear-phishing, social engineering, DDoS, credential harvest
APT42	IRGC-IO	Targeted surveillance of various persons of interest
MuddyWater	MOIS	Core group, espionage against regional govts, critical infrastructure, telecoms, energy
Cotton Sandstorm (ASA)	IRGC	Influence ops, hack-and-leak, IO amplification, operates in association with MuddyWater to expand the intelligence gathered from hacking operations
Cyber Av3ngers / IRGC -CEC	IRGC-CEC	ICS/OT attacks, PLC exploitation, DDoS and possible involvement with Bot farms

These groups represent the width and depth of Iran's cyber capabilities which support Iran's hybrid warfare aspirations.

Iran's cyber army is architected in a very unique way. Unlike its counterparts in Russia and China which are operationally managed exclusively by state entities, Iranian APT groups have a redundant leadership layer that is triggered during times of conflict or emergency. During such situations, this leadership layer that comprises a mix of veteran state-backed hackers and former intelligence agents offers transitionary leadership to ensure operational continuity.

Such a distinction matters enormously for defenders. The IRGC runs groups that are fundamentally oriented toward sabotage, critical infrastructure access, network manipulation and psychological operations. MOIS serves as a collector of intelligence for the state intelligence apparatus. Both these actor clusters share tooling, infrastructure, and in some cases even targets. When you hear about MuddyWater establishing initial access at a regional energy entity, there is a documented pattern of OilRig trailing behind to conduct sustained exfiltration or to cover the tracks.

21.2 Threat actor profiles: The active players

As of this writing, the following groups represent the most operationally active and tactically relevant actors in the current crisis environment:

OilRig (APT34) aka Helix Kitten / Earth Simnavaz / Cobalt Gypsy

Affiliation: MOIS

Iran's most persistent espionage arm. Active since 2014, OilRig targets energy, government, and financial sectors across the Middle East with a long-dwell, intelligence-collection mandate. By 2025, the group shifted significantly into cloud-native attack paths, using compromised Microsoft 365 accounts and Azure persistence mechanisms to maintain access. Their tooling now includes four new custom downloaders viz., OilBooster, OilCheck, ODAgent, and SC5k.

They are all using legitimate Microsoft cloud APIs (OneDrive, Graph, Exchange EWS) as covert C2 channels. The deliberate abuse of trusted cloud services makes detection extraordinarily difficult without behavioural analytics.

MuddyWater

Affiliation: MOIS

The most operationally active Iranian group in the current crisis window. Their TTPs blend living-off-the-land (LOtL) techniques PowerShell, RDP abuse, Mimikatz with legitimate tools such as SimpleHelp and Atera RMM for persistent remote access. The Aclip backdoor, which abuses the Slack API for C2, represents their willingness to weaponize trusted SaaS platforms.

APT42 / Charming Kitten aka TA453 / Mint Sandstorm / Educated Manticore

Affiliation: IRGC-IO

The human intelligence collection machine. APT42 doesn't go broad - it goes deep. Journalists, researchers, policy experts, academics, and diaspora activists are targeted through months -long relationship cultivation before any technical intrusion occurs. Check Point Research observed multi-channel social engineering campaigns leveraging messaging apps to funnel targets into credential-harvesting kits. In the current environment, this group is actively targeting individuals with privileged access: journalists covering the conflict, analysts at defense contractors, and anyone with proximity to decision-makers.

CyberAv3ngers aka Shahid Kaveh / IRGC Cyber Electronic Command

Affiliation: IRGC-IO

The OT specialist. CyberAv3ngers represents Iran's most direct capability against industrial control systems. Previously linked to attacks against Unitronics PLCs at U.S. water utilities, they have recently re-used C2 infrastructure associated with the IOCONTROL malware framework - a custom OT-focused tool designed to interact with PLCs, HMIs, and SCADA components. Flashpoint intelligence documents claimed breaches of a Jordanian grain silo company, including alleged manipulation of temperature controls and weighing systems. Whether fully realized or partly fabricated, the targeting intent against OT is unmistakable.

Cotton Sandstorm aka Haywire Kitten / Emennet Pasargad / MarnanBridge

Affiliation: IRGC

The fast-reaction influence operator. Cotton Sandstorm's playbook combines website defacement, DDoS, email hijacking, and data theft with immediate information operation amplification. Their custom infostealer WezRat is delivered through spearphishing campaigns masquerading as urgent software updates. In some Israeli-targeting cases, intrusions were followed by deployment of WhiteLock ransomware. This group moves fast - it is designed for tempo, not stealth.

[Hacktivist Proxy]

Evil 33

Formed on February 28, 2026 just hours after the first strikes Evil33 serves as a coordination hub for pro-Iranian hacktivist cells. This group, linked to MOIS, blends data exfiltration with operational targeting of Israeli energy, manufacturing, defense, and healthcare organizations.

Analysis of Telegram messages across 150 groups shows attack timing synchronized with kinetic events on the ground and we can say with a fairly high level of confidence that this is not spontaneous activism.

Tactics, Techniques and Procedures

Iranian APT TTPs have evolved considerably ,becoming more sophisticated since the Shamoon era. The shift is now toward cloud abuse, LOtL techniques, and AI-assisted operations. Such tactics represent a deliberate adaptation to modern defensive environments while increasing the chances of success.

Initial access (MITRE TA0001)

TECHNIQUE	ACTOR	DETAILS	MITRE ID
Spear phishing with credential harvesting	APT42, MuddyWater, APT34	Fake login pages mimicking Microsoft 365, Google Workspace, VPN portals. Multi-step trust-building before payload delivery.	T1566.002
VPN / Edge device exploitation	Fox Kitten, APT33	Exploitation of known CVEs in Pulse Secure, Fortinet, Citrix, and Palo Alto GlobalProtect. SSH tunnelling for persistence post-access.	T1190
Social engineering via professional platforms	APT42, Tortoiseshell	Fake recruiter personas on LinkedIn, fake interview invitations, months-long relationship cultivation before delivering malware-laced files.	T1566.003
Watering hole attacks	APT35, APT39	Compromising websites frequented by target demographics (policy institutes, diaspora news sites, academic portals).	T1189

Persistence and command plus control (MITRE TA0003 / TA0011)

TECHNIQUE	ACTOR	DETAILS	MITRE ID
Legitimate cloud services as C2	OilRig, MuddyWater	Microsoft OneDrive, Graph API, Exchange EWS API, Slack API used for covert C2 and data exfiltration. Effectively blends into legitimate traffic baselines.	T1102, T1567
Commercial RMM tools for persistence	MuddyWater	Abuse of SimpleHelp, Atera, and ScreenConnect for persistent remote access. Near-impossible to block without policy controls.	T1219
Web shell deployment	OilRig, MuddyWater	Web shells installed on internet-facing Exchange and IIS servers as secondary ingress points after initial compromise	T1505.003
DNS tunnelling	OilRig	Custom payloads use DNS queries for C2 communication, bypassing many perimeter controls.	T1071.004

The toolkit

TOOL / MALWARE	ACTOR	CAPABILITY	MITRE ID
Shamoon / MeteorExpress	APT33-linked	Destructive disk wiper. MeteorExpress added volume shadow deletion and Active Directory abuse. Still the reference architecture for Iranian wiper development.	T1485
WezRat	Cotton Sandstorm	Custom modular infostealer delivered as fake software updates. Keylogging, screenshot capture, credential harvest, clipboard monitoring.	T1056, T1113
IOCONTROL	CyberAv3ngers	Modular OT-focused malware designed to interact with PLCs, HMIs, SCADA systems. Communicates via MQTT over TLS. Previously deployed against Unitronics PLCs.	T0831, T0836
WhiteLock Ransomware	Cotton Sandstorm	Deployed post-WezRat compromise against Israeli targets. Primarily a destructive/coercive tool rather than financially-motivated ransomware.	T1486
PowGoop / Thanos variants	MuddyWater	Backdoor loader using PowerShell obfuscation. Thanos variant used as pseudo-ransomware for destructive effect with deniability.	T1059.001
Foudre + Tonnerre	Infy (Prince of Persia)	Long-lived surveillance implant pair. Tonnerre v50 detected September 2025. Targets Telegram on compromised hosts.	T1204.002

Multiple investigations have confirmed that CyberAv3ngers uses GPT models specifically for conducting PLC research, querying programmable logic controller documentation, attack surfaces, and firmware vulnerabilities. AI is actively accelerating the pace at which less technically sophisticated operators can develop OT-capable intrusion capabilities. The democratization of ICS attack research is a structural shift, not a temporary trend.

21.3 Targeting OT systems

OT and ICS targeting remains a signature capability and strategic priority. The IRGC-affiliated group CyberAv3ngers compromised at least 75 Unitronics PLCs across U.S. water, energy, healthcare, and food manufacturing sectors between November 2023 and January 2024, exploiting internet-facing devices using factory-default passwords. Updated CISA and FBI guidance issued in December 2024 documented new TTPs including manipulation of engineering and diagnostic tools, direct targeting of HMIs and operator workstations, and exploitation of vendor and third-party maintenance access.

In June 2025, the group Marshtreader, associated with MOIS, was observed scanning Israeli networks for vulnerable cameras in apparent intelligence-gathering activity ahead of potential targeting during the regional conflict.

21.4 Most targeted countries

UAE, Israel, Saudi Arabia and Kuwait are among the most targeted countries in the region. Regional oil producers are targeted by groups such as APT 27 (China), CyberAv3ngers, Xenotime, CyberVolk and OverFlame are now to target oil and gas entities in the region. Some of these threat actors are also working with groups indulging in speculation on oil prices. The interest in oil prices could be from a consumption standpoint (APT 26 and 27) or from a profit /ideology standpoint (CyberAv3ngers and CyberVolk). Either way, the extraordinary interest in numbers linked to production and refining output indicates a strategic curiosity and we won't be surprised if these threat actors are monetizing such information by working with groups making a profit out of oil price speculation.

21.5 Average number of incidents

The consistent growth in the average number of cyber incidents indicates a steady increase in cyber intrusions and of cyber threat actors improving their targeting methods in the region. Almost a quarter of the attacks are on the oil and gas sector which is primarily because of two reasons:

- The presence of diversified and widespread oil and gas infrastructure in the region
- Strategic importance of the sector to the regional economy
- Incident counts in the Middle East display a clear, near-monotonic upward trend (Figure 1). Three distinct growth phases are discernible:
- **Phase I** – Emergence (2018–2020): Volume tripled from 1 to 6 per month. This period aligns with the proliferation of TRITON/TRISIS (targeting Safety Instrumented Systems in Saudi Arabia) and broader geopolitical escalation in the Gulf.
- **Phase II** – Consolidation (2021–2023): Growth moderated, stabilising near 10 incidents per month. Threat actors were likely refining access and tooling rather than escalating externally visible activity - a reconnaissance-heavy period consistent with the motivation data.
- **Phase III** – Acceleration (2024–2025): A renewed upswing to 2–14 per month suggests operational campaign deployment, potentially driven by evolving ransomware targeting of energy infrastructure and continued state-sponsored activity.

Year-wise breakdown of cyber incidents (average)

Year	Average number of cyber incidents per month in ME
2018	1
2019	3
2020	6
2021	7
2022	10
2023	10
2024	12
2025	14

21.6 What motivates these attacks

Motivation	Percentage of overall attacks attributed
Geo-politics	28
Geo-politics (Hacktivism)	6
Ransom	19
Disruption	3
Malware testing	1
Access sale	7
Reconnaissance	21
Data exfiltration	10
Others\Unknown	5

Understanding attacker motivation is central to effective threat modelling. The distribution of motivations in the Middle East OT/ICS dataset (Figure 3) reflects a sophisticated and multi-vector threat environment rather than a single dominant actor type.

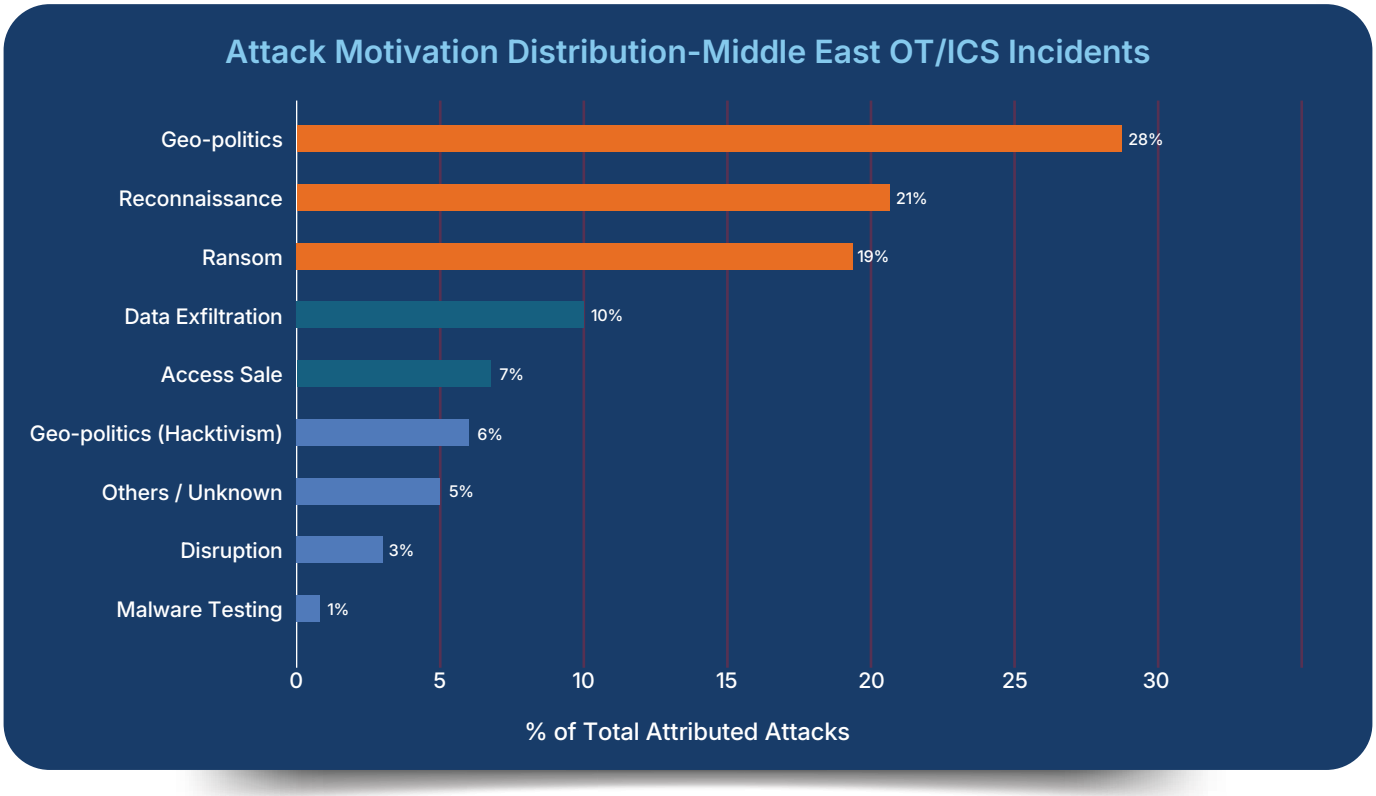


Figure 3 – Attack Motivation Distribution (% of Attributed Incidents)

21.7 Geopolitical drivers (34% Combined)

The combined geopolitical category - comprising direct state -interest operations (28%) and hacktivist proxies (6%) - is the single largest motivation cluster. This is consistent with the Middle East's role as the epicentre of several active geopolitical conflicts and proxy rivalries. Nation-state actors targeting OT environments typically seek one or more of the following: long-term persistent access, intelligence collection on industrial processes, or pre-positioning for potential destructive effect.

- The 28% direct geopolitical share is notably high by global standards; in most other regions, financial motivation (ransomware) tends to dominate.
- Hacktivist activity at 6%, while comparatively modest, is often underreported and may be used as a cover designation for state-sponsored operations with plausible deniability requirements

21.8 Reconnaissance (21%)

Reconnaissance as a standalone motivation category at 21% is a significant signal. In mature threat actor campaigns, reconnaissance is not an end goal - it is a preparatory phase. The high incidence of reconnaissance-coded events suggests that a substantial portion of current activity represents investment in future offensive capability rather than immediate impact.

Organisations experiencing elevated reconnaissance activity should treat this as an indicator of elevated risk within a 12–24 month horizon.

21.9 Financial motivations: Ransom and access sale (26%)

Ransomware operators (19%) and initial access brokers (7%) together account for more than a quarter of all incidents. This financial motivation tier reflects the professionalisation of cybercrime ecosystems targeting OT environments. Several ransomware groups - most notably those deploying variants capable of crossing the IT/OT boundary - have identified energy and transport infrastructure in the Gulf as high-value targets, where operational downtime creates immediate economic and reputational pressure to pay.

The risk
The 7% access sale figure is particularly consequential: initial access brokers sell footholds into industrial networks to third parties, creating a potential amplifier effect where a single intrusion event funds multiple downstream campaigns.

21.10 Data Exfiltration (10%)

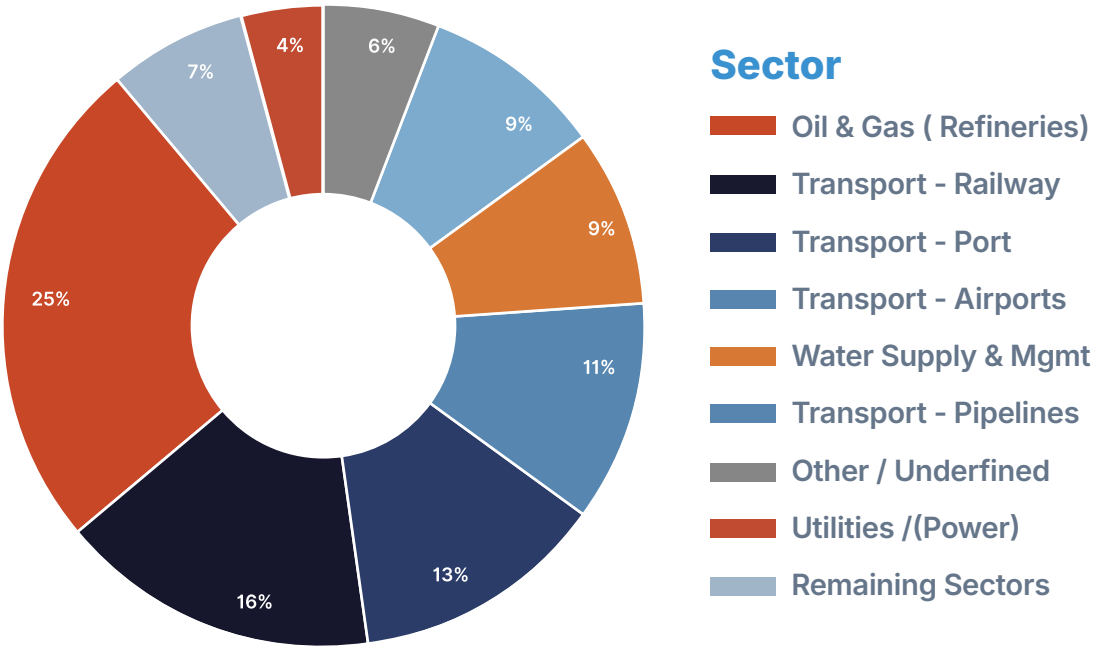
Data exfiltration at 10% points to intellectual property theft and operational intelligence gathering. In the energy sector context, exfiltrated data may include process schematics, operational parameters, maintenance schedules, and safety system configurations - all of which have strategic value to both state and commercial rivals.

21.11 Disruption, Malware Testing, and Others (9%)

Disruption-coded events (3%) represent direct attempts to impair operational continuity. While numerically modest, each disruption event in a critical infrastructure context carries outsized economic and public safety consequences. The 1% malware testing attribution is notable: it indicates adversaries are using live industrial environments as test ranges for novel tooling, confirming that some Middle East OT networks are effectively serving as sandboxes for next -generation attack development.

21.11 Sector-wise analysis

The sector distribution (Figure 4) reveals a pronounced concentration on high-consequence critical infrastructure. Three macro-clusters emerge: hydrocarbon energy, multi-modal transport, and utilities.



Incident breakdown by industry

21.12 Oil and gas (26%)

Refineries account for 25% of all incidents - the single largest sector share in the dataset. This finding is consistent with the region's economic exposure: Middle Eastern refinery output accounts for a material share of global petroleum product supply, and any operational disruption carries immediate market implications. Field activity, at 1%, is likely underreported given the remote and often less instrumented nature of upstream operations.

- The TRITON/TRISIS attack on a Saudi petrochemical facility's Safety Instrumented Systems remains the most operationally significant precedent for this sector targeting pattern.
- Threat actors with energy sector expertise and custom OT toolkits (notably those attributed to Iranian and Russian state campaigns) show persistent interest in refinery process environments.

Transport infrastructure (49%)

The transport cluster - railways (16%), ports (13%), airports (11%), and pipelines (9%) collectively represents the largest targeting sector at 49% of all incidents. This is a strategically rational target selection: Middle Eastern transport nodes serve as critical chokepoints for both regional supply chains and global trade routes.

Railway systems (16%): Increasingly digitised rail networks, including metro systems in the UAE and Saudi Arabia, present a growing OT attack surface. Many deployments combine SCADA systems with passenger information and safety systems on shared or proximate networks.

Ports (13%): Port logistics systems integrate OT (crane automation, vessel traffic management) with IT (cargo management, customs systems). The 2020 Shahid Rajaee port disruption in Iran demonstrated the economic leverage available through port-targeted cyberattacks.

Airports (11%): Aviation OT environments include baggage handling, runway lighting, fuel systems, and ATC ground systems - all potential targets for disruption-motivated actors.

Pipelines (9%): Cross-border and domestic pipeline infrastructure represents both a strategic target and an intelligence collection opportunity. Convergence of IT and OT in pipeline SCADA environments, accelerated by remote monitoring adoption, has materially expanded the attack surface.

21.13 Water supply and management (9%)

Water systems at 9% rank as the third most targeted sector. Attacks on water infrastructure carry disproportionate public health and civil unrest potential relative to the technical complexity of execution, which partly explains their attractiveness to both state and ideologically motivated actors. Desalination infrastructure - uniquely critical in the Gulf region - presents a specific and high-value sub-target.

21.14 Power utilities and manufacturing (9%)

Power generation - conventional (4%) and renewable (1%) - and the various manufacturing sub-verticals (1% each) collectively represent a secondary targeting tier. The relatively low manufacturing share likely reflects the sector's lesser strategic profile in the Middle East relative to global comparators, where manufacturing represents a larger share of the OT estate. The growing renewable energy sector, currently at 1%, should be monitored as a rising risk surface as Gulf nations accelerate solar and wind deployments.

21.15 Overall assessment

The region Is a primary theatre, not a secondary target

The data confirms what experienced practitioners have long assessed: the Middle East is not experiencing a spillover from global OT/ICS threat activity - it is a primary theatre. The region's incident growth rate, the dominance of geopolitical motivation, and the concentration on hydrocarbon and transport sectors all point to deliberate, sustained targeting by sophisticated actors with specific strategic objectives. Defensive postures calibrated to global norms are likely to be materially insufficient.

The reconnaissance signal demands attention

Twenty-one percent of incidents coded as reconnaissance represents a significant pending isk materialisation. In threat actor campaign models, reconnaissance events precede exploitation by weeks to months. organizations in the energy and transport sectors that have detected unusual network scanning, credential harvesting, or HMI probing activity in recent periods should treat the current environment as elevated-risk rather than business-as-usual.

The IT/OT convergence dividend is becoming an IT/OT convergence liability

The breadth of sector targeting - spanning refineries, railways, ports, airports, pipelines, and water systems - reflects the expanding OT attack surface created by digital transformation programs across the region's critical infrastructure. Remote monitoring, predictive maintenance, and digital twin deployments all introduce IP connectivity into historically air-gapped environments. The incident data suggests adversaries are exploiting this convergence faster than many asset owners are defending it.

Access brokers are a force multiplier risk

The 7% access sale category, while appearing modest in isolation, has outsized risk amplification potential. A single access broker sale can result in multiple downstream campaigns by buyers with diverse motivations - including ransomware deployment, data exfiltration, and destructive payload staging. Asset owners who detect a single intrusion event in OT environments should assume the possibility of multiple simultaneous campaigns rather than a single-actor scenario.

Targeted sector breakdown: Total incident share

Sector	Percentage
Utilities (Power)	4
Utilities (Renewables)	1
Water supply and management	9
Oil and gas (Refineries)	25
Oil and gas (Field activity)	1
Repetitive manufacturing (Electronics, toys, confectionery)	1
Discrete manufacturing (Clothing, automotive, firearms, medical devices)	1
Batch manufacturing (Food and beverage, pharmaceuticals, plastics)	1
Continuous manufacturing (Fertilizer production, chemical processing, pharmaceuticals)	1
3-D printing/additive manufacturing	1
Transport (Railway systems of all types)	16
Transport (Ports – inland and sea facing)	13
Transport (Airports)	11
Transport (Pipelines)	9
Others\undefined	6



22. OT Security in 2026

Operational Technology (OT) security is no longer a niche discipline confined to process engineers and SCADA specialists. It has become a board-level risk management priority. The convergence of IT and OT networks, the proliferation of Industrial Internet of Things (IIoT) devices, and the demonstrated willingness of nation-state actors and ransomware syndicates to target industrial infrastructure have collectively transformed the threat landscape beyond recognition from even five years ago.

The incidents cataloged across the 2018–2025 period - from TRITON/TRISIS targeting Saudi Arabian safety instrumented systems, to ransomware attacks paralysing pipeline operations, to destructive malware propagating from corporate IT into plant-floor OT networks - share a common thread: they exploited security debt accumulated during decades of air-gap assumption, where isolation was treated as a substitute for security architecture. That assumption is now comprehensively invalidated.

CONTEXT

These recommendations are grounded in the threat intelligence findings from the accompanying OT/ICS incident dataset (2018–2025) and reflect established frameworks including IEC 62443, NIST CSF, NIST SP 800-82, and the MITRE ATT&CK for ICS knowledge base. They are designed for global enterprise asset owners across energy, utilities, transport, manufacturing, and water sectors.

The recommendations are structured across six domains: Governance & Risk Management; Network Architecture & Segmentation; Asset Visibility & Inventory; Identity & Access Management; Threat Detection & Response; and Supply Chain & Third-Party Risk. Each domain carries tiered recommendations coded by urgency. The totality of these recommendations constitutes a comprehensive OT security programme architecture applicable to global enterprises regardless of sector.

Domain 1 – Governance, Risk Management & Compliance

Effective OT security begins with governance - the organizational structures, policies, accountabilities, and risk frameworks that determine how security decisions are made and resources are allocated. In the majority of OT security incidents investigated over the past decade, governance failures were either a root cause or a significant contributing factor: unclear ownership, absent policies, and risk frameworks calibrated to IT rather than operational contexts.

1.1 CRITICAL

Establish a Dedicated OT Security Function

Create a dedicated OT/ICS security team, separate from or operating as a distinct practice within the broader IT security function. This team must include individuals with domain knowledge of industrial control systems, SCADA environments, and sector-specific operational processes - not merely IT security generalists with OT exposure. The team should be embedded within, or have direct reporting lines to, operations and engineering eadership, not just IT.

Why it matters: *OT environments have unique availability, integrity, and safety requirements that generic IT security frameworks do not adequately address. Decisions made without OT domain expertise routinely create new vulnerabilities while appearing to remediate existing ones.*

1.2 CRITICAL

Define OT-Specific Risk Appetite and Tolerance Thresholds

Develop a formal OT risk framework that defines risk appetite specifically for operational technology environments, with explicit thresholds for availability impact (acceptable downtime windows), integrity impact (sensor data manipulation tolerances), and safety impact (zero-tolerance thresholds). This framework must be validated by both cybersecurity leadership and operational/engineering leadership and approved at board level.

Why it matters: *OT environments prioritise availability and safety over confidentiality - the inverse of most IT risk models. Applying IT-calibrated risk thresholds to OT decisions consistently produces either over-restrictive controls that impair operations or under-restrictive decisions that create unacceptable safety risk.*

1.3 HIGH

Align to IEC 62443 as the Primary OT Security Standard

Adopt IEC 62443 (Industrial Automation and Control Systems Security) as the governing standard for OT security architecture and operations. Conduct a formal gap assessment against IEC 62443-2-1 (Security Management System) and IEC 62443-3-3 (System Security Requirements) as the baseline. Supplement with NIST SP 800-82 (Guide to ICS Security) for policy and procedural alignment. Avoid attempting to directly apply ISO 27001 or SOC 2 frameworks to OT environments without significant adaptation.

Why it matters: *IEC 62443 is purpose-built for industrial environments. It accounts for the unique constraints of OT - legacy systems, real-time requirements, safety system dependencies - that generic IT security standards do not. Using the wrong framework creates a compliance illusion while leaving substantive gaps.*

1.4
HIGH

Integrate OT Risk into Enterprise Risk Management Reporting

OT cyber risk should appear as a named risk category in enterprise risk registers, with quantified impact estimates (operational, financial, safety, regulatory) reported to the Board Risk Committee on at least a quarterly basis. Establish KRIs (Key Risk Indicators) specific to OT: mean time to detect OT anomalies, percentage of OT assets with known vulnerabilities, coverage of OT environments by monitoring tooling, and patch compliance rates by ICS zone.

Why it matters: *Risk that is not visible at board level does not attract budget. The majority of OT security underinvestment in global enterprises traces to OT risk being invisible or underrepresented in enterprise risk reporting - a governance failure with operational consequences.*

1.5
MEDIUM

Conduct Annual OT Security Maturity Assessment

Commission an independent OT security maturity assessment on at least an annual basis, using a recognized maturity model (IEC 62443 Security Level assessment, or the DHS CSET tool adapted for sector). Assessments should cover all sites globally, not just flagship facilities. Maturity scores should be trended over time and used to drive programme prioritisation and investment decisions.

Why it matters: *Without external, independent assessment, OT security programmes tend toward self-referential improvement — optimising against known gaps while blind to unknown ones. Annual cadence ensures the programme keeps pace with an evolving threat landscape.*

Domain 2 – Network Architecture & Segmentation

Network architecture is the single most consequential security control in OT environments. The absence of proper segmentation — or the existence of segmentation that exists on paper but has been eroded by operational workarounds and unmanaged connectivity - is the primary enabler of lateral movement in the vast majority of significant OT security incidents. TRITON, NotPetya, Colonial Pipeline, and the Oldsmar water treatment incident all exploited segmentation failures as a primary attack vector.

EXPERT
NOTE

The Purdue Model provides a useful reference architecture for OT network layering, but it was designed for operational efficiency, not security. In modern environments, the Purdue Model must be adapted and hardened - not blindly applied. Critically, the IT/OT DMZ is not a substitute for zone-based segmentation within OT networks.

2.1
CRITICAL

Enforce Network Segmentation Based on Security Zones and Conduits (IEC 62443)

Design and implement OT network segmentation using the zone-and-conduit model defined in IEC 62443-3-2. Each zone should be defined by its security level requirements and the trust relationships between zones. Conduits - the controlled communication channels between zones - must be explicitly defined, documented, and enforced through technical controls (firewalls, unidirectional gateways). The IT/OT boundary must be a hardened DMZ, not a flat network junction.

Why it matters: *Zone-based segmentation limits lateral movement. An attacker who gains access to one zone should be unable to pivot to higher-criticality zones without traversing a controlled conduit - buying time for detection and response.*

2.2
CRITICAL

Deploy an OT fluent NDR

Enterprises require OT-native NDR to gain deep-packet visibility into non-IP and industrial proprietary protocols (e.g., S7, EtherNet/IP) that standard IT tools cannot parse. By leveraging deterministic modeling rather than just probabilistic signatures, these solutions baseline "known-good" industrial logic and east-west traffic patterns.

Why it matters: *OT fluent NDR allows for the detection of unauthorized PLC ladder logic changes, firmware manipulation, and anomalous set-point variations-critical indicators of compromise that precede physical kinetic impact or catastrophic downtime.*

2.3
CRITICAL

Eliminate All Direct Internet Connectivity from OT Networks

Conduct a comprehensive audit of all OT network connectivity and eliminate any direct or indirect internet-facing exposure for OT systems. This includes: remote vendor access connections, historian replication channels, condition monitoring platforms, and any IoT/IIoT device with cloud telemetry. All remote access to OT environments must be channelled through a hardened jump server or PAM (Privileged Access Management) solution in a DMZ, with session recording.

Why it matters: *Direct internet connectivity from OT networks is the single highest-risk configuration in industrial environments. The attack paths for ransomware and state-sponsored actors overwhelmingly begin with internet-exposed OT endpoints or IT-to-OT pivots via poorly segmented remote access infrastructure.*

2.4
HIGH

Implement OT-Specific Firewall Rule Management

Establish a formal change management process for OT firewall rules, including peer review and approval by OT security and engineering leadership. Conduct quarterly firewall rule audits to identify and remove stale, overly permissive, or undocumented rules. Firewall policies should enforce default-deny (whitelist) postures between all zones, with explicit permit rules for each approved communication flow.

Why it matters: *Firewall rule sprawl is endemic in long-lived OT environments. Rules added for temporary purposes, vendor visits, or forgotten projects accumulate over years into a swiss-cheese segmentation posture that resembles but does not deliver zone isolation.*

2.5
HIGH

Wireless Security in OT Environments

Any wireless network serving OT environments - including Wi-Fi for field devices, handheld terminals, or maintenance laptops - must be isolated on a dedicated VLAN with no direct connectivity to the process control network. Use WPA3-Enterprise with certificate-based authentication. Conduct regular RF surveys to detect rogue access points. Consider prohibiting wireless connectivity entirely in highest-criticality zones.

Why it matters: *Wireless networks in OT environments have historically been deployed for operational convenience with minimal security consideration. They routinely provide an out-of-band pathway around carefully constructed wired segmentation controls.*

Domain 3 – Asset Visibility & Vulnerability Management

You cannot protect what you cannot see. OT asset inventories are consistently the most significant data quality gap in enterprise OT security programs. Many organizations have incomplete, outdated, or non-existent inventories of their OT assets - a situation that persists because active scanning of OT networks carries availability risk, passive discovery has historically required specialised tooling, and OT assets have lifecycles measured in decades rather than years, making records stale by default.

3.1
CRITICAL

Build and Maintain a Comprehensive OT Asset Inventory

Deploy passive OT asset discovery tooling across all OT network segments. Supplement passive discovery with engineering documentation review, vendor asset registers, and manual verification at scheduled maintenance windows. The resulting asset inventory must capture: asset type, make, model, firmware version, OS version, network address, zone assignment, communication dependencies, and criticality classification. Review and update the inventory at minimum quarterly.

Why it matters: *Every vulnerability assessment, patch program, and threat detection capability is bounded by the completeness of the underlying asset inventory. Unknown assets are unmonitored assets — and unmonitored assets are the preferred beachhead of sophisticated adversaries.*

3.2
HIGH

Classify OT Assets by Criticality and Consequence

Establish a formal OT asset criticality classification framework with at minimum three tiers: Safety-Critical (SIS, emergency shutdown systems), Process-Critical (primary control systems, historians, engineering workstations), and Supporting (ancillary systems, peripheral networks). Security controls, patch urgency, monitoring coverage, and incident response procedures should be differentiated by tier. Classification must incorporate consequence analysis - the impact of compromise on safety, production, regulatory compliance, and public/environmental exposure.

Why it matters: *Treating all OT assets as equally critical is operationally unworkable and resource-inefficient. Consequence-based classification ensures that the highest-impact assets receive the most intensive controls and monitoring, without imposing disproportionate constraints on lower-consequence environments.*

3.3
HIGH

Implement an OT-Specific Vulnerability Management Programme

Establish a vulnerability management programme calibrated to OT constraints. This programme should: subscribe to vendor security advisories and ICS-CERT alerts for all asset types in the inventory; assess each disclosed vulnerability against the asset inventory and criticality classification; evaluate exploitability and compensating controls before patch deployment; and conduct risk-based patch prioritisation rather than blanket patch timelines. Recognize that patching in OT environments requires coordination with operations, engineering, and safety teams, and often requires maintenance window scheduling.

Why it matters: *OT vulnerability management cannot be a copy-paste of IT patch management. Deploying a patch to an ICS component without testing and operational coordination can cause process disruption equivalent to the incident it was intended to prevent.*

3.4
HIGH

Address End-of-Life and Legacy System Risk

Conduct a formal End-of-Life (EOL) assessment of the OT asset inventory. For assets running unsupported operating systems (e.g., Windows XP, Windows 7) or with discontinued vendor support, document compensating controls (network isolation, application whitelisting, enhanced monitoring) and establish a lifecycle roadmap for replacement or upgrade. EOL assets carrying unacceptable residual risk after compensating controls must be prioritised for capital replacement planning.

Why it matters: *Legacy systems are disproportionately represented in OT breach investigations. The combination of unpatched vulnerabilities, absent vendor support, and operational constraints against replacement creates a persistent high-risk profile that compensating controls can mitigate but not eliminate indefinitely.*

Domain 4 – Identity, Access Management & Human Factors

Access management in OT environments is frequently characterised by shared accounts, generic credentials, vendor access that was never revoked, and a cultural assumption that physical access to a control room equates to implicit trust. These practices, understandable in an era of air-gapped systems, are wholly inadequate in a converged IT/OT world and represent low-effort, high-impact attack vectors for adversaries.

4.1
CRITICAL

Eliminate Shared and Generic Accounts in OT Environments

Audit and remediate all shared or generic accounts across OT systems - including 'admin', 'operator', 'engineer', and vendor-default accounts. Each individual with OT system access should be assigned a unique, personally attributed account. Where OT systems technically cannot support individual accounts (legacy PLCs, older SCADA components), document this as a risk exception with compensating controls and a remediation timeline.

Why it matters: *Shared accounts eliminate accountability and make forensic investigation of incidents impossible. In the absence of individual attribution, detection of unauthorized access in OT environments becomes dependent on behavioural anomaly - a significantly weaker control than access governance.*

4.2
CRITICAL

Implement Privileged Access Management (PAM) for All Remote OT Access

Deploy a PAM solution - such as CyberArk, BeyondTrust, or Delinea - as the mandatory gateway for all remote access to OT environments, including vendor and contractor access. PAM capabilities required: session recording, just-in-time access provisioning, credential vaulting, and real-time session monitoring. All vendor remote access sessions should be explicitly approved before initiation, time-limited, and reviewed post-session.

Why it matters: *Remote access is the most frequently exploited initial access vector in OT environments. PAM transforms uncontrolled, persistent, unmonitored vendor access into audited, time-bounded, accountable sessions - dramatically reducing both the attack surface and the forensic gap in the event of an incident.*

4.3
HIGH

Apply Least-Privilege Principles Across All OT System Accounts

Review and remediate account permissions across all OT systems to enforce least-privilege: each account should have only the permissions required for its defined function, nothing more. This applies to human accounts, service accounts, and application-to-application communication accounts. Conduct a permissions audit at minimum annually, and as part of every OT system change or upgrade.

Why it matters: *Over-provisioned accounts are an attacker's force multiplier. A compromised account with broad permissions enables rapid lateral movement and privilege escalation. Least-privilege enforcement limits the blast radius of any single credential compromise.*

4.4
MEDIUM

Establish and Enforce OT-Specific Security Awareness Training

Develop an OT-specific security awareness program targeting all personnel with access to OT environments: operators, engineers, maintenance technicians, and relevant managers. Training must cover: recognising social engineering targeting OT staff, safe use of portable media and engineering laptops, reporting abnormal system behaviour, and safe remote access procedures. Training cadence should be annual at minimum, with targeted refreshers following significant incidents or threat intelligence updates.

Why it matters: *OT environments have historically been exempt from cybersecurity training programmes, with awareness efforts focused exclusively on IT users. This leaves OT-facing personnel - who often have the most direct access to critical systems - without the knowledge to identify and report threat actor activity.*

Domain 5 – Threat Detection, Incident Response & Resilience

Detection and response capabilities in OT environments lag significantly behind their IT counterparts. The combination of proprietary protocols, specialised vendor tooling, real-time operational constraints, and a historical absence of monitoring infrastructure creates environments where sophisticated adversaries can operate for months before detection - as demonstrated by the multi-year dwell times observed in several landmark ICS intrusion cases.

5.1
CRITICAL

Deploy OT-Native Network Detection and Response (NDR) Tooling

Implement continuous OT network monitoring using tooling capable of passive, protocol-aware inspection of industrial communications (Modbus, DNP3, IEC 61850, EtherNet/IP, OPC-UA, and others relevant to the installed asset base). Monitoring must cover all OT network segments, not just the IT/OT boundary. Alerts should feed into a SOC with OT-trained analysts or a specialist OT-MSSP.

Why it matters: *Generic IT network monitoring tools do not understand OT protocols and cannot identify OT-specific attack techniques such as process value manipulation, unauthorized engineering commands, or exploitation of proprietary industrial protocols. OT-native tooling is non-negotiable for meaningful detection capability.*

5.2
CRITICAL

Develop and Exercise OT-Specific Incident Response Plans

Develop OT-specific incident response playbooks covering at minimum: ransomware impacting OT/IT convergence zones; destructive malware targeting process control systems; unauthorized command injection (e.g., rogue engineering workstation activity); safety system compromise or manipulation; and supply chain-delivered malware in OT components. Playbooks must define OT-specific containment options that account for availability and safety constraints - including deliberate safe-state transitions and manual operation modes.

Why it matters: *IT-generic incident response plans consistently fail when applied to OT incidents. The decision to isolate a compromised system - straightforward in IT - may trigger production shutdown, safety system activation, or regulatory notification in OT. OT-specific playbooks must pre-authorise and document these decisions before an incident occurs.*

5.3
HIGH

Conduct Annual OT Red Team / Tabletop Exercises

Commission annual adversarial exercises against OT environments: full red team exercises (physical and cyber combined) for highest-criticality sites, and tabletop exercises for all sites. Red team scope should include IT-to-OT lateral movement, exploitation of remote access infrastructure, and physical-cyber attack combinations. Tabletops should involve operations, engineering, HSE, legal, communications, and executive leadership - not just IT/OT security teams.

Why it matters: *OT security programmes that are never tested under adversarial pressure carry a dangerous illusion of effectiveness. Red team exercises identify gaps that compliance assessments systematically miss - including the operational and human decision-making failures that determine whether an incident becomes a catastrophe.*

5.4
HIGH

Implement OT-Specific Backup, Recovery and Safe-State Procedures

Establish and test backup and recovery procedures specific to OT environments: golden image backups of engineering workstations and HMI configurations, offline backups of PLC logic and historian data, and documented manual operation procedures for all critical processes. Backups must be stored offline (air-gapped from both IT and OT networks) and tested for recoverability at minimum annually. Safe-state transition procedures - the operational steps to bring a process to a known-safe condition in the event of a cyber incident - must be documented, trained, and accessible without network connectivity.

Why it matters: *OT ransomware incidents have demonstrated that without tested, accessible backups and documented manual procedures, recovery timelines extend from days to weeks. The Colonial Pipeline incident - where a ransomware attack on IT systems caused voluntary OT shutdown due to billing system loss - illustrates the cascading operational dependency that proper resilience planning must address.*

5.5
MEDIUM

Subscribe to OT Threat Intelligence and Sector ISAC

Subscribe to relevant OT/ICS threat intelligence feeds and participate in sector-specific Information Sharing and Analysis Centres (ISACs): E-ISAC (electricity), ONG-ISAC (oil and gas), WaterISAC, A-ISAC (aviation), Maritime ISAC, and equivalent bodies in operating jurisdictions. Consume and operationalise ICS-CERT advisories, and sector regulator threat bulletins. Assign responsibility for intelligence consumption and dissemination to the OT security team.

Why it matters: *Threat intelligence transforms security from reactive to anticipatory. Sector ISACs provide early warning of campaigns targeting specific industrial verticals before they manifest as incidents at individual organizations - intelligence that generic commercial feeds frequently lack.*

Domain 6 – Supply Chain & Third-Party Risk

The supply chain represents one of the most significant and systematically underaddressed risk vectors in OT security. Industrial control systems components - from PLCs and DCS platforms to engineering software and safety system firmware - are developed by a concentrated set of global vendors, creating systemic risk concentration. Supply chain compromises in OT (SolarWinds extended to OT networks; compromised firmware in industrial devices; malicious updates in engineering software) have demonstrated the catastrophic potential of this vector.

6.1
HIGH

Implement OT Vendor Security Assessment Programme

Establish a formal security assessment process for all OT technology vendors and system integrators. Assessments should cover: software development lifecycle (SDL) practices, vulnerability disclosure and patch release processes, incident notification obligations, remote access security requirements, and supply chain integrity controls (software bill of materials - SBOM). Tier vendors by criticality and conduct assessments accordingly - annual for Tier 1 (safety and primary control system vendors), biennial for Tier 2.

Why it matters: *OT asset owners bear the security consequences of their vendors' security decisions but rarely assess those decisions. A vendor delivering a compromised firmware update or a system integrator with poor credential hygiene can negate years of investment in perimeter and detection controls.*

6.2
HIGH

Require and Validate Software Bill of Materials (SBOM) for OT Components

Require OT component vendors to provide Software Bill of Materials (SBOMs) for all software and firmware delivered into OT environments. Validate SBOMs against known vulnerability databases (NVD, ICS-CERT) upon receipt and as part of ongoing vulnerability management. For components where SBOMs are not available, conduct binary composition analysis where feasible or apply compensating controls (network isolation, enhanced monitoring).

Why it matters: *The Log4Shell and XZ Utils vulnerabilities demonstrated that critical open-source components are embedded throughout the enterprise software stack - including in OT systems. Without SBOM visibility, organizations cannot assess their exposure to such vulnerabilities or respond effectively when they are disclosed.*



6.3
CRITICAL

Control and Audit All Third-Party Physical and Logical Access to OT Systems

Implement and enforce a formal process for all third-party access to OT environments - both physical (site access for field engineers, vendor technicians) and logical (remote diagnostic sessions, software updates). Requirements: pre-approved access request; escort for physical access to OT areas; PAM-mediated, session-recorded remote access; verification of contractor cybersecurity posture before access grant; post-session audit review. Terminate all access immediately upon completion of authorized activity.

Why it matters: *Third-party access is the most common initial access vector in OT environments globally. The combination of legitimate credentials, privileged access, and minimal monitoring of vendor activity creates an ideal attack pathway - exploited by both external adversaries who compromise vendors and malicious insiders within vendor organizations.*

6.4
MEDIUM

Apply Hardware and Firmware Integrity Verification

Establish procedures for verifying the integrity of OT hardware and firmware before deployment. This includes: validating firmware hashes against vendor-published checksums for all firmware updates; inspecting hardware for tampering indicators upon receipt; maintaining a record of authorized firmware versions per asset; and conducting periodic integrity checks against baseline for highest-criticality assets.

Why it matters: *Hardware and firmware tampering in the OT supply chain - whether through nation-state interdiction or vendor compromise - is a documented attack vector. The NSA's ANT catalogue and subsequent revelations demonstrated that hardware-level compromise can survive software-level remediation entirely.*

Implementation Roadmap

The recommendations across the six domains should be implemented in a phased program that prioritises risk reduction over administrative completeness. The following roadmap provides a sequenced implementation pathway for global enterprise OT security programs.

Phase	Timeline	Priority Focus Areas	Key Deliverables
1 – Establish	0–90 days	Governance, Visibility, Critical Gaps	OT security team, asset inventory, network audit, PAM for remote access, eliminate shared accounts, internet connectivity audit
2 – Harden	90 days – 12 months	Architecture, Detection, Response	Zone segmentation, OT NDR deployment, IRP development, unidirectional gateways for SIS, vendor access programme, IEC 62443 gap assessment
3 – Optimise	12–24 months	Maturity, Resilience, Supply Chain	Red team exercise, tabletop programme, SBOM programme, threat intel integration, EOL asset roadmap, training programme
4 – Sustain	24+ months ongoing	Continuous Improvement	Annual maturity assessments, threat intelligence operationalisation, regulatory alignment, board-level OT risk reporting cadence

Maturity Benchmarks: Where Should You Be?

The following table provides a self-assessment guide calibrated to IEC 62443 Security Levels (SL 0–4) across key capability areas. Most global enterprises targeting sound operational security should aim for SL 2 as a minimum across all domains, with SL 3 for highest-criticality environments within 24 months.

Capability Domain	SL 0 (None)	SL 1 (Basic)	SL 2 (Target - 12 mo)	SL 3 (Advanced - 24 mo)
Asset Inventory	No inventory	Manual/ partial list	Passive discovery, 90%+ coverage, versioned	Real-time inventory with auto-discovery, 100% coverage
Network Segmentation	Flat network	Basic IT/OT separation	Zone-conduit model implemented, DMZ in place	Unidirectional gateways for SIS, micro-segmentation
Access Management	Shared accounts, no MFA	Individual accounts, basic ACLs	PAM for remote access, least privilege enforced	JIT access, full session recording, behavioural analytics
Threat Detection	No OT monitoring	Perimeter firewall only	OT NDR deployed, SOC visibility	OT-specific threat hunting, threat intel operationalised
Incident Response	No OT IRP	Generic IT IRP applied	OT IRP developed, tabletop conducted	Annual red team, playbooks tested, manual procedures ready
Supply Chain	No vendor controls	Contract clauses only	Vendor assessment program, PAM for vendor access	SBOM programs, firmware integrity verification



Closing Advisory

OT security is not a project with a completion date. It is a sustained capability that must evolve in lockstep with an adversary community that is itself continuously developing. The threat data presented in the accompanying incident analysis report confirms that the Middle East - and by extension the global energy, utilities, and transport sectors - is experiencing a structural and permanent increase in OT-targeted threat activity, not a temporary spike.

The twenty-one recommendations in this advisory collectively constitute a comprehensive OT security program architecture. No single recommendation is sufficient in isolation, and the interdependencies between domains - governance enabling asset management, asset management enabling effective detection, detection enabling proportionate response - mean that program sequencing matters as much as program content.

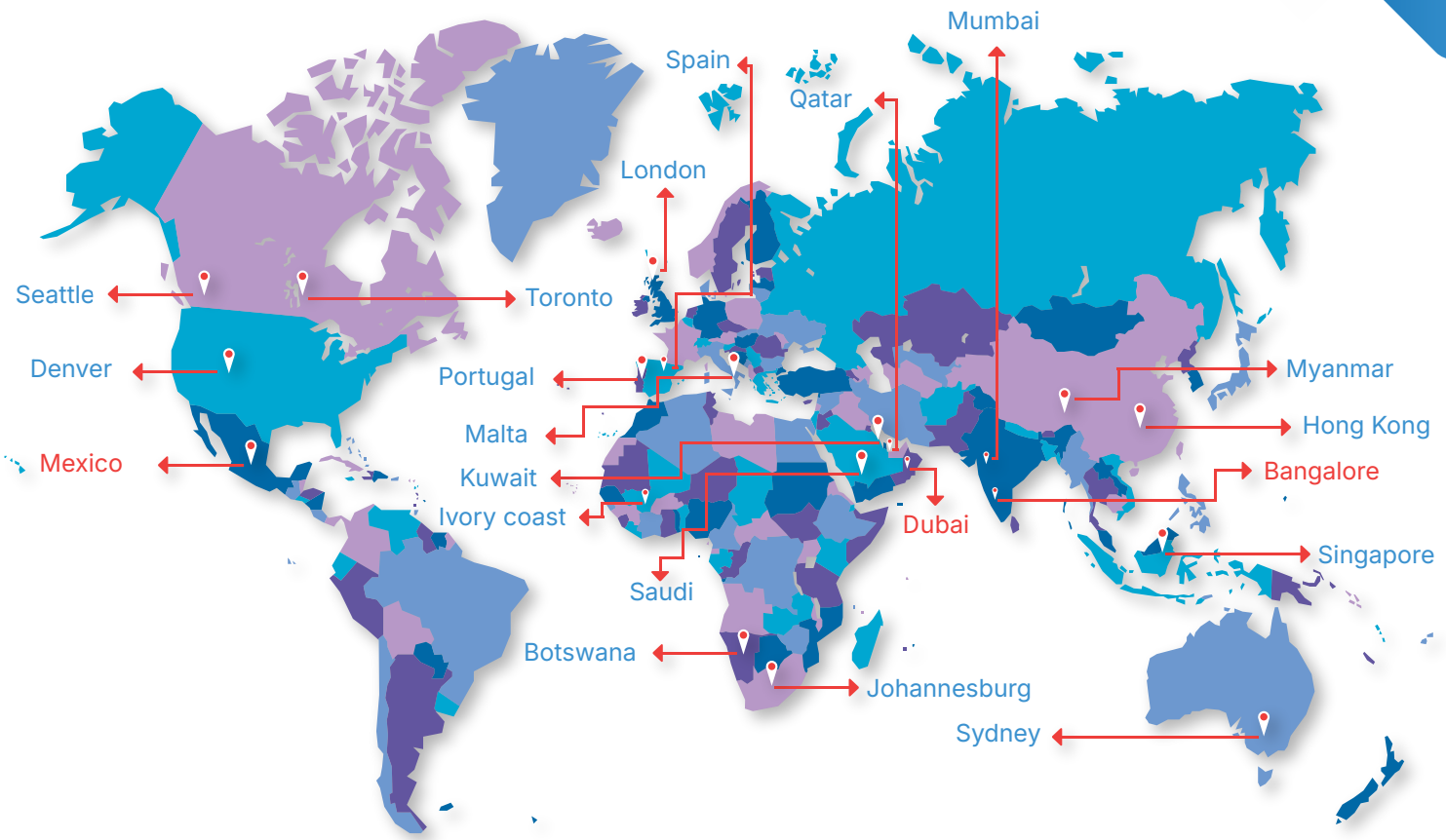
FINAL NOTE

The most common failure mode in OT security program is not technical - it is organizational. Programs that lack clear ownership, executive sponsorship, and integration with operational decision-making consistently underperform their technical investment. The governance recommendations in Domain 1 are therefore not a bureaucratic preliminary; they are the foundation on which all other capability depends.

Organizations that invest in the capabilities described here will not become invulnerable - no security programme achieves that. What they will achieve is a materially improved capacity to detect adversary activity earlier, contain the impact of incidents more effectively, recover more rapidly, and demonstrate to regulators, insurers, and stakeholders that operational risk is being managed with genuine rigour.



About Shieldworkz



ISOC and Level One Honeypot Locations

Honeypot Locations

Security Operations Center

Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

Talk to us today!

Contact Us



6160 Warren Pkwy Ste 100
Frisco, TX 75034

+1 972-418-2948

americas@shieldworkz.com



396 Old Colony Road
Richmond Hill,
ON L4E 5A5 Canada

+1 (437) 223-7770

americas@shieldworkz.com



Tenth floor,

Abu Dhabi,
United Arab Emirates,
FAB Business Center

+971 56 660 5200

middleeast@shieldworkz.com

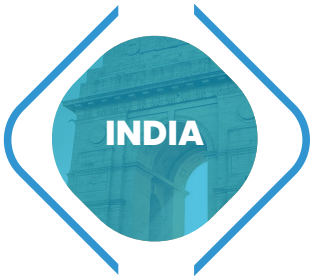


Fritz-Schäffer-Street 1,
4th floor

Bonn, 53113, Germany

+49 (0) 228 / 929 39210

europe@shieldworkz.com



Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli

Bengaluru,
Karnataka 560093

+91 9059620557

apac@shieldworkz.com



Copyright @ 2026, Shieldworkz - All rights Reserved.