SHIELDWORKZ

The Global OT & IoT Threat Landscape Assessment and Analysis Report 2025

A Shieldworkz Threat Research Labs initiative

/shieldworkz info@shieldworkz.com https://shieldworkz.com

SHIELDWORKZ

About

Shieldworkz provides comprehensive cyber resilience for the world's most critical industrial, IoT, and infrastructure environments. As a specialist OT/IoT-focused cybersecurity partner, we deliver turn-key, end-to-end program that integrates cutting-edge technology With expert-led services to secure national infrastructure and global manufacturing operations.

Our unified platform provides a single-dashboard view for deep-packet inspection, continuous asset discovery, vulnerability management, and micro-segmentation, all amplified by a proprietary AI engine featuring the OThello™ large-language model for automated alert triage and the OThello™ co-pilot for generating compliance reports and OT-specific penetration testing scripts. For organizations requiring a managed solution, we design, build, and operate captive OT Security Operations Centres (SOCs), providing unified governance and SOAR-driven incident response that aligns with IEC 62443 and other regional mandates.

By integrating this advanced technology with expert-led managed services, Shieldworkz partners with CISOs to build and operate true cyber resilience, safeguarding the world's most critical industrial and infrastructure operations from the plant floor to the cloud.

SHIELDWORKZ

Report Methodology & Data Integrity

The findings and projections in this report are the result of a comprehensive, multi-faceted threat intelligence gathering and analysis process. Our methodology is designed to provide a granular and validated view of the global OT and IoT threat landscape, grounded in real-world data.

Global Honeypot Network

The primary data source is Shieldworkz's global honeypot network, one of the largest of its kind. This network is engineered to attract and analyze malicious activity on an industrial scale.

- Scale and Scope: The network is operational in over 95 cities worldwide and analyzes an average of 39 million attacks each day.
- Strategic Placement: Our honeypots are strategically deployed in locations with specific attributes known to attract high-value threat activity, including geopolitical hotspots, internet traffic hubs, submarine cable landing centers, and cities with a high density of critical infrastructure projects.
- High-Fidelity Emulation: The network comprises over 10,500 physical and virtual devices mimicking real-world industrial deployments, covering more than 1,200 device architectures. This ensures that the attack data collected reflects tactics used against actual ICS and IoT environments.

Infrastructure Scale

10,500+
Emulated OT and IoT Devices

Global Reach

95+
Strategically Placed Cities

Daily Threat Volume

39 Million
Attacks Analyzed Daily

SHIELDWORKZ

Multi-Source Intelligence Corroboration

To enrich and validate our honeypot data, we integrate intelligence from a wide range of other sources:

- The Cybercriminal Underground: We actively monitor and surveil hackers' forums, malware platforms, the Dark Web, and other validated channels where threat actors collaborate. This includes running "dark honeypots" in locations where new attack vectors emerge.
- Institutional and Research Partners: We incorporate data from universities, government agencies, and other reputable sources to provide additional context and validation.

Rigorous Analytical Framework

Every captured attack is systematically fingerprinted, categorized, and analyzed.

- 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.

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.

SHIELDWORKZ

A New Era of Industrial Cyber Risk

The convergence of sophisticated adversaries, weaponized AI, and escalating geopolitical tensions has redefined the threat landscape for critical infrastructure.

The 2025 threat landscape for Operational Technology (OT) and the Internet of Things (IoT) is defined by an unprecedented escalation in the frequency, sophistication, and strategic intent of cyberattacks. Analysis by Shieldworkz Threat Research Labs reveals a pivotal shift: adversaries are not just breaching networks, but systematically weaponizing new technologies, exploiting geopolitical tensions, and industrializing their attack methodologies.

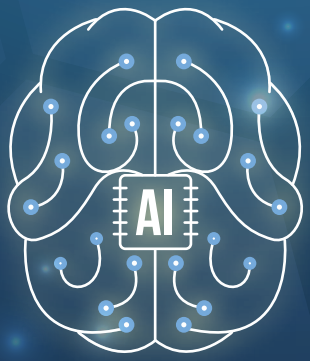
79%

Surge in cyberattacks targeting the energy sector in 2024, making it the most targeted industry globally.

17%

Rise in internet-accessible Industrial Control System (ICS) ports detected between November and December 2024.

SHIELDWORKZ



Key Finding 1
The Industrialization of Cybercrime & The Rise of AI

Advanced hacker groups have evolved into well-structured entities that resemble mature businesses, with streamlined processes for everything from target selection to ransom negotiations. This operational maturity is now supercharged by the integration of Artificial Intelligence, which is being used to automate and enhance nearly every phase of an attack.

AI-Powered Offense:
Adversaries are now using AI to break proprietary protocols , manage large botnets , and create autonomous, self-evolving malware.

Industrialized Operations:
Threat actors have evolved into mature entities resembling businesses , with some even supported by HR and payroll functions.

Recruitment Surge:
Lockbit and RansomHub led affiliate recruitment in 2024, adding 39 new affiliates to their networks.

- AI-Powered Offense: Adversaries now use AI-based tools to break proprietary protocols, autonomously manage compromised botnets, and generate highly convincing phishing emails. Threat groups like RansomHub are actively using AI for target identification, attack deployment, and crunching stolen data.
- Autonomous Malware: We are detecting new forms of "semi-sentient" malware with minimal code that can autonomously evolve within a target network, bypass signature-based detection, and exfiltrate data stealthily.
- Threat Actor Growth: Despite increased reliance on AI, major threat actors expanded their recruitment of human affiliates in 2024, capitalizing on the uncertainty created by global elections.

SHIELDWORKZ

Key Finding 2 Critical Infrastructure is the New Battlefield

State-sponsored Advanced Persistent Threat (APT) groups from nations including Russia, China, North Korea, and Iran are conducting coordinated, multi-year reconnaissance campaigns against Critical Information Infrastructure (CII) in over 100 nations. These operations are designed to establish persistent access and lay dormant implants that can be triggered during geopolitical escalations.

- Geopolitical Targeting: Attacks are increasingly correlated with geopolitical flashpoints. Chinese APTs, operating under the Ministry of State Security (MSS), are running persistent, country-focused campaigns, such as the multi-year breach of India's power grid infrastructure by APT 41.
- Expanding Attack Surface: A 17% rise in internet-accessible ICS ports was detected between November and December 2024. Our scans identified 40,983 accessible ICS ports in North America alone in a single scan.
- Sectoral Hotspots: The energy sector is the most-attacked industry, followed by manufacturing and healthcare. Within the oil and gas sector, 47% of incidents had an "Unknown" impact, indicating severe visibility gaps.

State Sponsored Espionage

APT groups from China, Russia, and Iran are waging multi-year campaigns against critical infrastructure in over **100** nations, seeking to establish persistent access for future disruption.

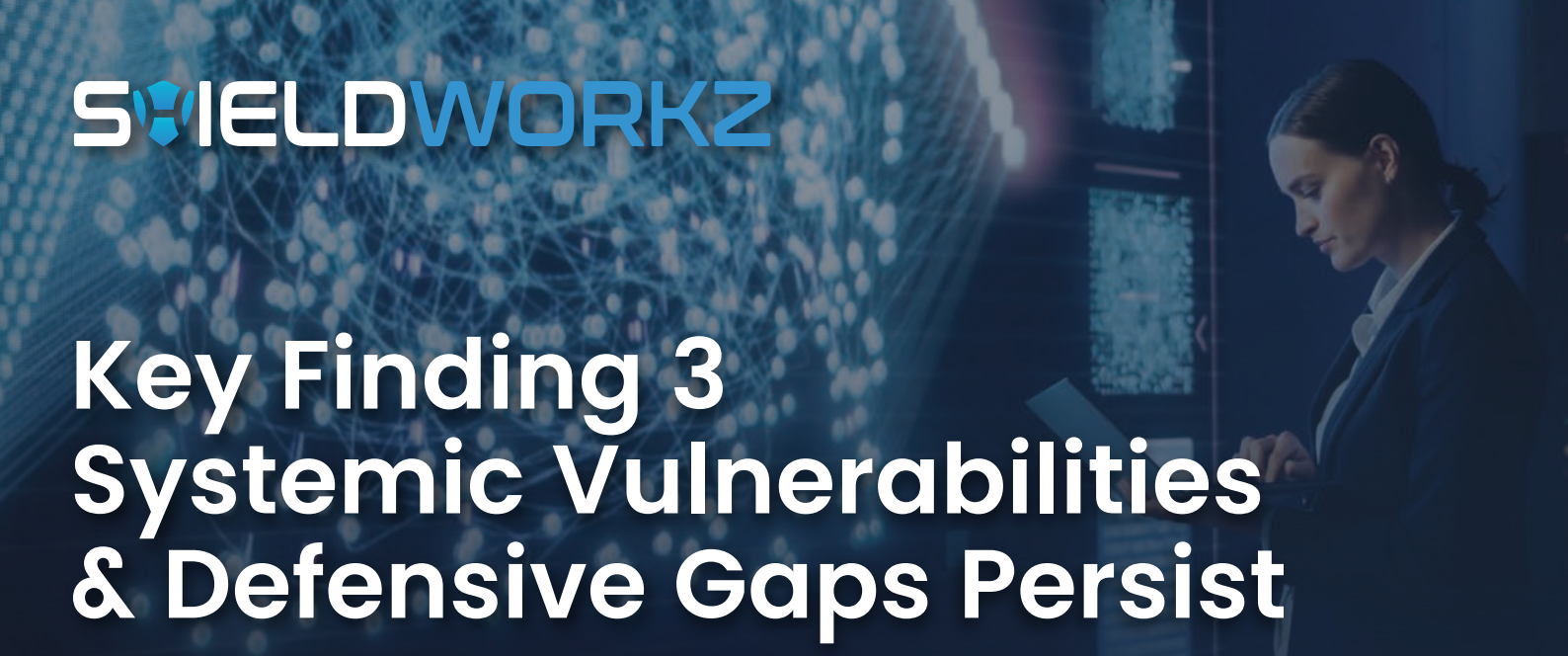
A Vast & Growing Attack Surface

Our research validated over **95,000** internet-accessible industrial ports globally, a **17%** year-over-year increase in the total exposed OT footprint compared to our 2023 study.

Concentrated Sector Risk

With a **79%** surge in attacks, the energy sector is the world's most targeted industry, yet severe blind spots remain, with **47%** of incidents in the oil & gas industry go unclassified, highlighting critical visibility gaps.

SHIELDWORKZ



Key Finding 3 Systemic Vulnerabilities & Defensive Gaps Persist

Despite the escalating sophistication of threats, foundational cybersecurity weaknesses remain dangerously prevalent across industries. These unaddressed gaps provide fertile ground for attackers to succeed with alarming frequency.

- IT-OT Convergence Risk: The convergence of IT and OT is enabling threats to move in both directions. However, many organizations lack a well-architected network that properly segregates risk zones from functional zones, leaving their OT environments highly vulnerable.
- Pervasive Visibility Gaps: Many asset owners are simply unaware that breaches have occurred and impacted their systems. This is compounded by the presence of shadow assets and unmonitored asset behaviors.
- Incident Response Immaturity: The absence of a structured incident response process, a lack of ICS event management specialists, and missing response playbooks significantly amplify the impact of attacks. It is estimated that over 45% of attacks on ICS systems in Asia are currently not reported to any agency outside the enterprise.

13%

Unfixable Flaws

of serious OT vulnerabilities are now considered "Forever Day" threats with no available patch, representing a permanent and unremediated risk to industrial systems

45%

The Silent Breach

Of industrial attacks in Asia go unreported outside the enterprise, crippling collective threat intelligence and hiding the true scale of regional risk.

40%

The Broken Boundary

Of all system attacks specifically target the IT-OT convergence zone, as adversaries exploit weak network segmentation to move laterally from corporate networks into critical operational environments.

SHIELDWORKZ

2025 Projections & Strategic Outlook

The trends observed in 2024 indicate a challenging year ahead. Shieldworkz projects that in 2025, organizations must prepare for the following strategic shifts:

1. Increased Targeting of Remote and High-Value Assets
- Attacks on remote assets, such as those in space and offshore oil rigs, will be targeted more frequently by adversaries.

2. Escalation of Multi-Vector Attack Campaigns
- A rise in multi-layered attacks is anticipated, combining phishing, zero-day vulnerability exploitation, and sophisticated social engineering tactics to maximize efficacy.

3. Heightened Focus on OT Security as a Business Imperative
- OT security will receive heightened attention, with a necessary focus on risk management, vulnerability remediation, and enhanced operational visibility within industrial environments.

The convergence of industrialized cybercrime, state-sponsored aggression, and AI-driven attack tools marks a new and dangerous chapter for OT and IoT security. The findings of this report underscore the urgent need for a paradigm shift in defensive strategies—moving from reactive compliance to proactive, intelligence-led resilience.

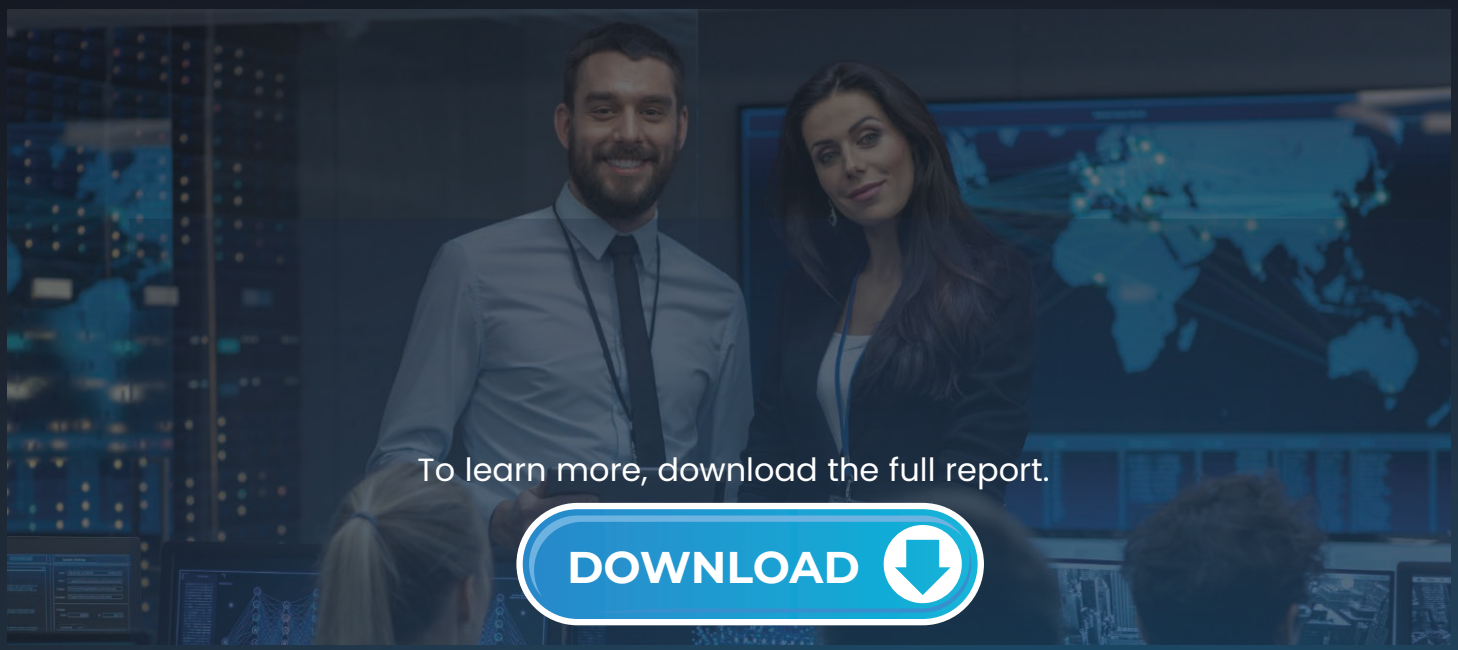


Table Of Contents

The Global OT and IoT Threat Landscape Report 2025

Shieldworkz Threat Research Labs

How this report was created.

1. Our global honeypot network
2. Malware obtained from various sources including forums and shadow networks
3. Universities, government agencies, and other sources of repute
4. Independent threat researchers and other unaffiliated sources

Our vast honeypot network serves as an active sink drawing up to 39 million attacks on an average each day. The nature of attacks varies from simple reconnaissance to sophisticated attacks carried out using complex payloads. Further, we also monitor the interactions between various threat actors in order to track targeted attacks.

This report has been prepared from the threat intelligence gathered by our honeypot network which is today operational in over 95 cities across the world. These cities have at least one of these attributes

01 Host a mix of industries with a diverse spectrum of use cases

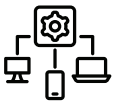
02 Are landing centers for submarine cables

03 Are geopolitical hotspots with ongoing conflicts or are sitting on geopolitical fault lines

04 Are internet traffic hotspots

05 Are targeted by APT groups or other sophisticated hackers

06 House multiple IoT projects with a high number of connected end points



07 House multiple connected critical infrastructure projects

08 Have academic and research centers focusing on IoT and digital transformation

09 Have the potential to host multiple IoT projects across domains in the future

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 10500 physical and virtual devices covering over 1200 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 unsupvised categorization, this data is analyzed thread-bare by our global threat research team. The analysis focuses on these areas

This report provides a context for the evolving threat landscape as well. The context is divided into six parts:

- **Triggers and actors:** what are threat actors up to: analyzed at tactical and strategic levels; how are malware evolving
- **Targets:** what is being targeted and why
- **Enablers:** what institutional gaps are aiding the growth in cyberattacks [with inputs from CISOs and other stakeholders]
- **Impact:** How are such trends impacting cybersecurity and enterprises and governments everywhere
- **Vulnerabilities of interest to hackers**
- **Attack patterns**

Key findings are published by us every year to enable governments, businesses, decision-makers, academicians, students, CISOs, and those interested in cybersecurity to gain a comprehensive understanding of the evolving threat environment that envelops IoT deployments and OT installations and derive appropriate institutional responses to prevent, contain and dissuade such attacks.

Additional resources

To try our IoT and OT threat intelligence feeds for free, please visit this link

For more information on the malware and attacks analyzed in this report, please visit the malware reports section of our website.

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 https://shieldworkz.com

Processed datasets are also available on request.

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.

10 reasons to read this report 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 90 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.
- More information on sector-specific threats and their impact
- Cybersecurity leaders can gain a much deeper understanding of how the threat landscape is evolving and its impacts on their business
- Unlike other reports that cover security trends at a very high level, this report goes into specifics with validated data. We have also attempted to look well beyond reporting attacks. We explore reasons for the rising attacks while contextualizing institutional responses
- 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
- Accurate cyber threat predictions based on a thorough investigation of existing TTP patterns

The year that was: looking back at 2024

In 2024, all sectors witnessed a rise in cyberattacks on Industrial Control Systems. A mix of vulnerabilities, attack sophistication, prevalence of unsecured systems and lack of mature practices contributed significantly to the rise in cyberattacks on OT operators.

Threat actors are now using various flavors of AI to aid in attacks. One incredible use case that came to our notice 2024 is the use of AI-based bots to surveil forums that sell exploit data. Once the bot detects such data, the actor enters into a negotiation with the exploit shop to get the best possible rate for procuring the exploit information. We believe that at least one such exploit was used in the attack on a utility company registered in January 2024.

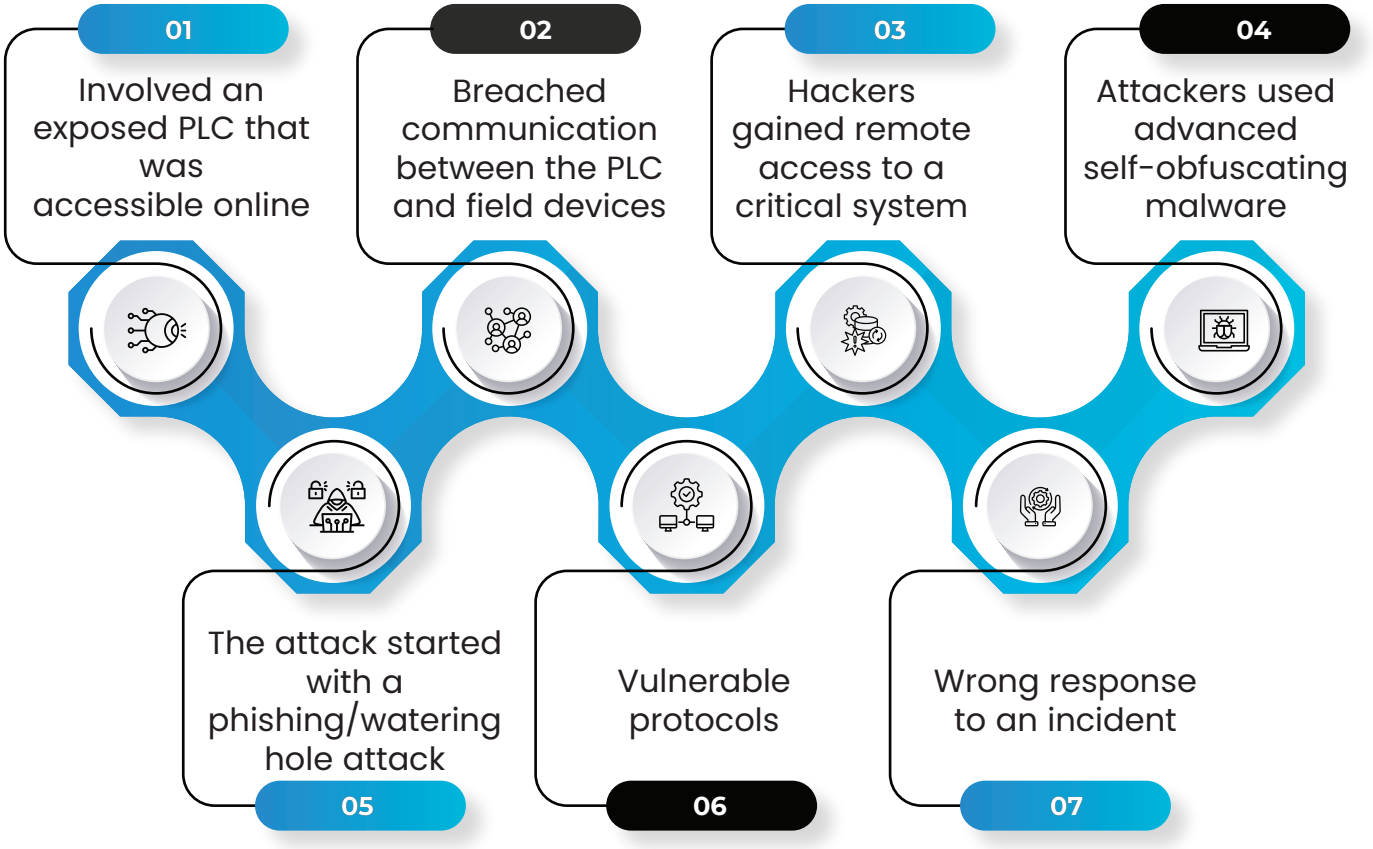
Attacks on ICS systems are still underreported by victims. This could be for various reasons, including ensuring operational confidentiality. Based on verifiable claims, we are able to report that over 45 percent of attacks in Asia are currently not reported to any agency outside the enterprise.

Increasing attack penetration

Since the last 7 years, cyberattacks on OT systems have moved beyond IT-OT converged zones that exist at levels 4 and 5 as per the Purdue model. The nuisance category of attacks often involve little or no precision and the actor tries to use vulnerabilities or lack of adequate defenses to go deeper into the OT network. Such attacks could impact production but can be contained easily as they involve threat actors and TTPs that are not very sophisticated.

Of bigger concern are more advanced attacks that could cover more assets and operations. Such attacks involved tactics specific to OT systems and functions. The actor may impose a hidden recon payload that stays hidden and studies the OT network for a considerable period of time before striking. All actions and attacks paths in such an attack are deliberate and the impact could be potentially devastating for an OT operator Such attacks could also provide hackers with enough experience and learnings to replicate elsewhere.

All major attacks on ICS infrastructure globally in 2024 had at least one of the following characteristics/attack patterns:



Lack of mature cybersecurity practices and employee sensitivity are key internal factors that contribute to a breach.

Major ICS security trends recorded in 2024

- PLCs manufactured by OEMs headquartered in nations that were involved in regional conflicts, but installed in other countries were targeted by APTs. Such attacks have brought a new economic dimension to the ongoing conflicts around the world.

- 'Forever day' vulnerabilities as mentioned by ISA here are becoming a major challenge for OT operators As of December 2024, as per our calculations, at least 13 pecent of serious vulnerabilities have no remediation or patch available which makes these systems vulnerable to a massive strike by threat actors. Furthermore, in many cases, most of the available patches haven't been deployed because of stability issues and or other issues.

- 39 percent of all attacks involve advanced actors. Globally, most attacks involved an APT at some stage With many state actors openly engaging private threat actors, ICS-specific malware and tactics are finding their way into easily accessible malware forums faster. Many APT actors including APT 41, APT 28, APT 33 and a few others are collaborating with independent threat actors to test the potency of their malware. The test versions often carry malware versions that are older with traceable codes and backdoor communication to validate a breach

- Revenge attacks involving disgruntled insiders, vendors, hacktivists, and other actors with some axe to grind are becoming more common. A large manufacturer in South East Asia was breached by an actor who was rejected during an employment interview by the victim organization Almost 13 percent of published attacks studied by us showed a pattern that could be traced back to an agent that had previous interactions with the victim organization

- Lack of visibility into assets continues to present significant challenges to OT asset owners. Based on leaked data being sold on various forums, it is clear that many asset owners are not aware of breaches that have taken place and impacted their systems. The presence of shadow assets, unmonitored asset behaviors, and lack of cyber oversight are all adding to this challenge

- We are seeing a growing footprint of AI in cyberattacks on OT systems. Hackers are using AI-based tools to break proprietary protocols, encryptions, and more. Bad actors are also training SLMs to autonomously hack OT systems like PLCs or to manage large and compromised device constellations turned into botnets. Such tools are also used to generate phishing emails or generate traffic from remote sites that appear legitimate to first level defense mechanisms such as firewalls

- Involvement of insiders is growing. While it is not easy to say whether these insiders were acting out of a lack of knowledge or were volunteering their services to hackers, 7 of the largest breaches in 2024 were traced back to an insider. It is therefore important to ensure training and sensitization of employees

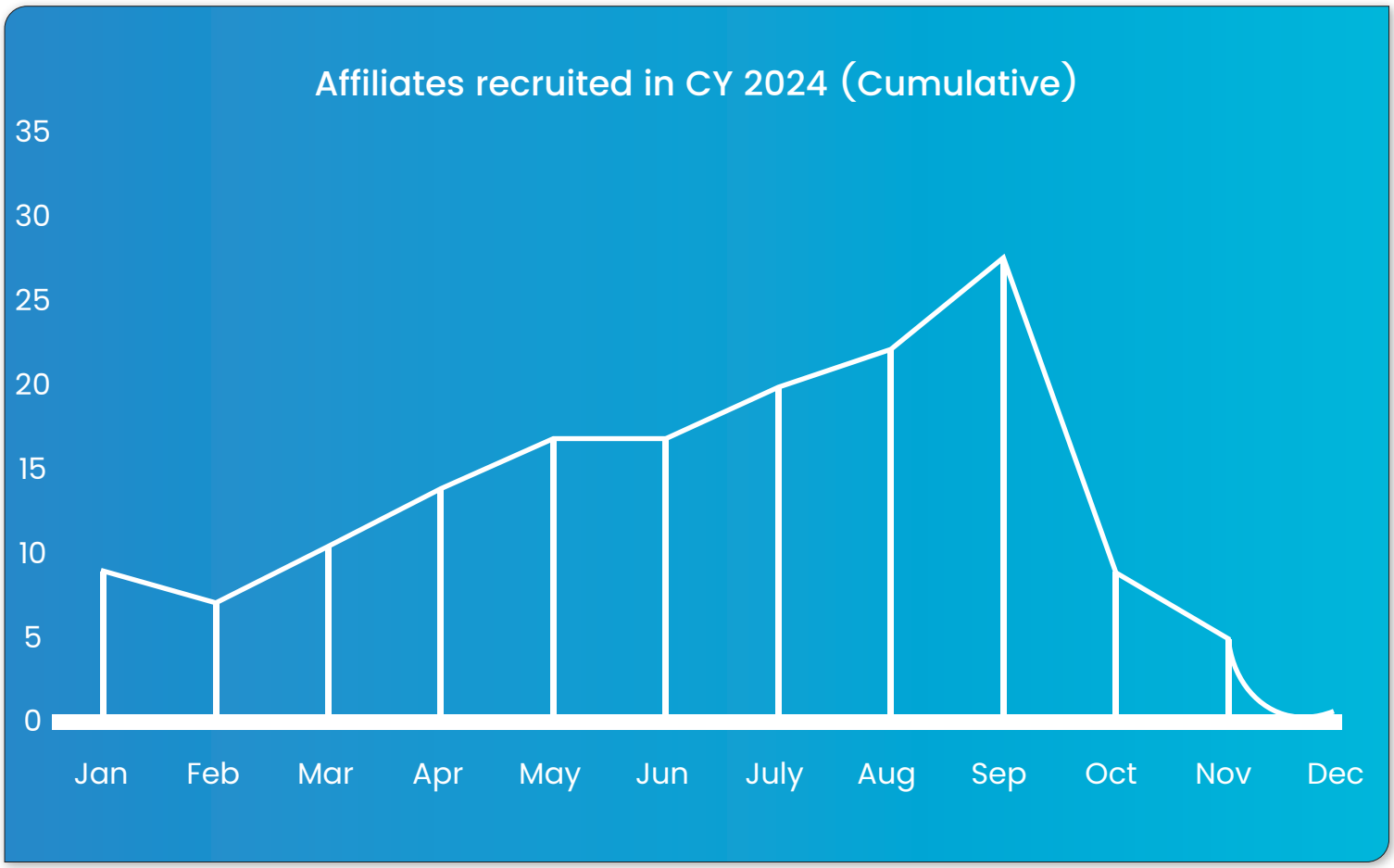
- A large automotive company operating separately in India and Pakistan (under different ownership patterns) was targeted by a new threat actor with links to Iranian APT 33. An interesting aspect of this attack is how the threat actor waited for a year to target the subsidiary operating in Pakistan. Both attacks were carried out using similar tactics starting with a spoofed email sent out on a weekend. The stolen data was sold as separate lots by the same threat actor.

Major ICS security trends recorded in 2024

Threat actor	New affiliates added in 2024
Lockbit and	39
RansomHub	29
Clop (erstwhile)	27
Non-com	23
Blackbasta	18
E-corps	8
Tutor	7

All major threat actors increased their recruitment drives across the globe in 2024. This is despite these groups increasing their reliance on AI tools for executing various phases of their targeting campaigns.

One reason for heighted recruitment of affiliates was the elections in many countries which often creates periods of uncertainty and opens windows for threat actors to exploit.



Countries where elections occurred in 2024

The number of recruits increased in 2024 all the way up to September. The recruitment showed a steep decline from October till December 2024. This aligns well with the elections schedule running across the globe in 2024. The list of nations where elections were held in 2024 is given in the chart below:

It comes as no surprise that many of these nations logged a higher number of cyberat tacks in 2024.

Loose affiliations and loyalty

Change in affiliate behavior : one major change we noticed in 2024 is the lack of exclusivity among affiliates. With major law enforcement action being taken against non-state actors, many affiliates chose to hedge their bets by diversifying their affiliations across groups. This led to a situation where a single affiliate was earning ransom across multiple events using multiple encryptors and decryptors. Several affiliates were also modifying malware on their own unlike before.

Air gaps are hurting

Air gaps, once considered a reliable security measure, are no longer perceived as such for various reasons. For one, they often create a false sense of assurance about an organization's actual security level. Air-gapped networks may convey a sense of security that does not accurately reflect the true risks present on the shop floor. In many instances, networks believed to be air-gapped were, in reality, not fully isolated. Systems were often connected to the internet through mobile hotspots introduced by employees, removable USB drives, or temporary connectivity established during maintenance windows.

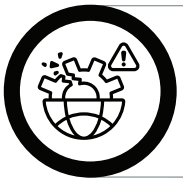
Absence of security acceptance testing

Security acceptance testing is yet to be incorporated as a standard and mandatory cyber hygiene practice in many organizations and this has led to many security challenges arising across the lifecycle of an OT asset such as

Undetected Vulnerabilities – Security flaws in systems, applications, or configurations may go unnoticed, increasing the risk of exploitation by attackers.

Non-Compliance with Security Standards - Organizations may fail to meet regulatory compliance or industry security requirements (e.g., NIS2, ISO 27001, IEC 62443), leading to legal and financial repercussions.

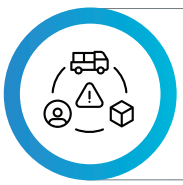
Increased Attack Surface – Without proper testing, insecure configurations, weak authentication mechanisms, and unpatched software could leave systems exposed to cyber threats.



Operational Disruptions – Security weaknesses could be exploited to disrupt critical business operations, leading to downtime, financial losses, or even safety risks in industrial environments.

Data Breaches and Loss – Sensitive data may be compromised due to untested security controls, leading to reputational damage, legal consequences, and loss of customer trust.

Higher Remediation Costs – Fixing security issues post-deployment is often more expensive and complex than identifying and addressing them during the acceptance testing phase.



Supply Chain Risks – If third-party systems and components are not security-tested before integration, they could introduce vulnerabilities into the entire ecosystem.

Unchecked expansion of threat surface: If we go by just the number of exposed and accessible OT and IoT systems and networks (systems and devices accessible from the network), we can conclude with evidence that the threat surface exposed has grown significantly in 2024. Major industries where we recorded this trend are utilities, maritime and manufacturing.

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 Consequences could include loss of data, major rise in blast radius after an incident and risk of long term reconnaissance using stealthy malware.

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.

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.

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.

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.

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.

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.

The increasing sophistication of cyber attacks can also be traced to these trends we are tracking

Increased organization and operational maturity of threat actors

Advanced hacker groups have evolved into well-structured entities with operational models resembling mature businesses. These groups now possess greater financial and technical resources, similar to startups that have undergone multiple funding rounds and business model optimizations. As a result, major threat actors have streamlined processes for target selection, attack execution, breach tactics, ransom negotiations, and fund laundering. In addition, they are now being run on industrial scales supported by HR and Payroll functions akin to regular businesses.

This structured approach has enabled them to make more accurate revenue projections, allowing them to scale operations up or down dynamically based on risk, law enforcement activity, and geopolitical factors.

Expansion of the Cybercriminal Talent Pool

The number of independent hackers has grown significantly, leading to a more diverse and decentralized threat landscape. Based on intelligence gathered from known hacker forums, unique TTP (Tactics, Techniques, and Procedures) analysis, and affiliate behavior tracking, an estimated 9,300 highly skilled hackers entered the cybercrime ecosystem between 2023 and 2024. The proliferation of ready-made exploit kits, compromised credentials, and do-it-yourself (DIY) hacking tools has further lowered the entry barriers for new actors, enabling even less experienced individuals to launch sophisticated attacks.

Prolonged Breach Detection and Low Prosecution Rates

The increasing gap between initial compromise and breach detection, coupled with low prosecution rates, has emboldened cybercriminals to adopt "hit-and-run" tactics. Attackers rapidly exfiltrate sensitive data and sell it on underground marketplaces before victims even realize a breach has occurred. This data is then weaponized in secondary attacks targeting enterprises, government agencies, and critical infrastructure. The lack of swift legal consequences has further incentivized cybercriminals to operate with impunity.

These trends collectively indicate a rapidly evolving threat landscape where adversaries are not only more skilled but also more systematic, scalable, and resilient against defensive measures

Prolonged Breach Detection and Low Prosecution Rates

Trend	Concern
Lack of incidence response maturity	A poorly developed incident response (IR) capability exposes organizations to significant operational, financial, and reputational risks.
Prolonged malware loiter time	With increasing malware sophistication, delayed detection and containment of malicious payloads can allow adversaries to exfiltrate sensitive data, disrupt operations, and deploy additional payloads such as ransomware.
Residual access points present a threat to victims	In the aftermath of a cyber incident, threat actors can renter previously compromised networks via residual access points.
Lack of well-defined roles, responsibilities, tested responses and playbooks	This could lead to a lack of cohesive approach to enforcing security mechanisms and use of tools in a organized manner leading to confusion and erosion of overall security posture
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.
Externally accessible systems and networks	The number of such systems continues to rise every year indicating a lack of security attention to this basic cybersecurity practice
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.
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
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 read to a breach but long-term risks in terms of litigation and censure and/or fines from regulatory authorities.
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.
High levels of reliance on OEMs	In certain enterprises, Original Equipment Manufacturers (OEMs) are 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.
Lack of adequate supply chain visibility	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.

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.
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 2025.
New mandates to comply	As cyber breaches continue to rise, regulators will 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.

Despite these evolving threats, enterprise security postures remain inadequate to effectively counter the next wave of sophisticated, low-detection ransomware campaigns. Without enhanced monitoring, adaptive threat intelligence, and real-time anomaly detection, organizations risk prolonged exposure and operational paralysis from highly targeted cyberattacks.

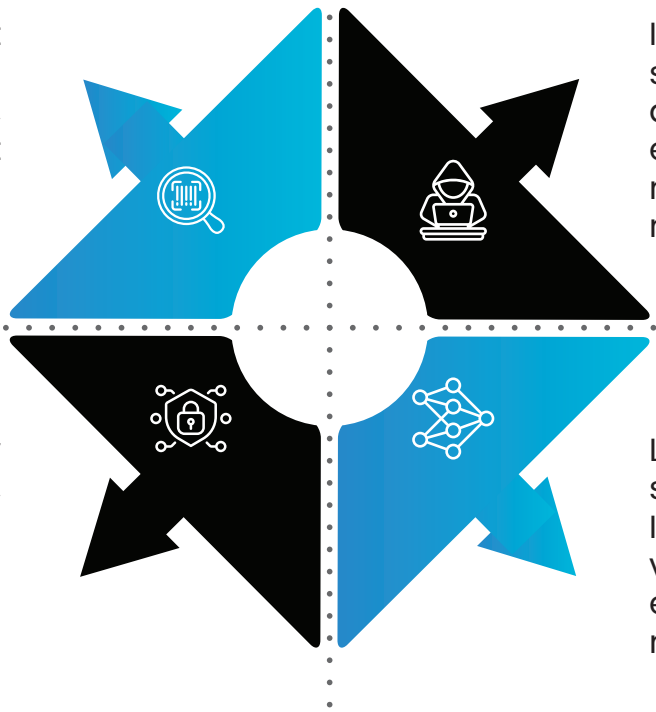
Ongoing security challenges

The presence of unmapped and unpatched legacy systems in power infrastructure introduces severe cybersecurity vulnerabilities, exacerbating the risk landscape that power companies must address urgently. These legacy systems, often running outdated firmware with unpatched vulnerabilities, are susceptible to remote code execution (RCE), denial-of-service (DoS) attacks, and privilege escalation exploits. The lack of visibility into these assets further amplifies the difficulty in implementing proactive security measures, making them prime targets for adversaries leveraging zero-day vulnerabilities and advanced persistent threats (APTs).

The strategic risk posed by cyber threats to the power sector is not confined to operational disruptions but extends to national security and economic stability. A compromised SCADA system or remote terminal unit (RTU) could lead to cascading failures across regional grids, affecting power availability during peak economic activity hours or critical national operations. Threat actors, including state-sponsored groups, have demonstrated capabilities to manipulate grid frequency, trigger load imbalances, and even induce physical damage through cyber-kinetic attacks, as evidenced in past incidents such as Industroyer, Triton, and BlackEnergy.

Field research conducted by our threat intelligence team has revealed significant gaps in cybersecurity posture across multiple power generation and distribution sites. Despite the presence of multi-layered physical security controls, intrusion detection, and access restrictions, cybersecurity defenses were found to be inadequate and misconfigured. Commonly observed security lapses included

Limited or absent anomaly detection mechanisms, preventing early threat identification.



Inconsistent firewall rule sets, with permissive access controls exposing critical ICS networks to lateral movement attacks.

Outdated security configurations in PLCs, RTUs, and HMIs, making them vulnerable to protocol-based exploits.

Lack of network segmentation, allowing IT-OT convergence vulnerabilities to be exploited for cross-do-main attacks.

Data hungry nation-state actors continue to target critical infrastructure

As of December 2024, threat actors from over 7 countries were found to be active throughout the year. These countries include China, North Korea, Russia, Iran, Uzbekistan, Belarus and Pakistan. Living of the land has become a common exploitation tactic for APT threat actors. They achieve this by using multiple tactics to blend into the background operations of target institutions.

Beyond geopolitical flareups in Europe and the Middle East, APT groups from the countries mentioned above launched many campaigns to target critical infrastructure and businesses of interest across the globe these include grids, water treatment plants, oil refineries and pipelines, smart infrastructure, ports and data centers.

With the onset of Large Learning Models, threat actors have become more data hungry than ever before. All attacks on target infrastructure now carry a data element as well. This means that in every attack hackers try to gather data from target networks. Newer variants of complex payloads that the Shieldworkz Threat Research Team intercepted come with more stealth and loiter mode features.

Unlike before when an attack ended with either shutdown of the target infrastructure or exfiltration of data, today attacks serve many purposes including

01 Data harvesting from non-target systems

02 Deciphering the threat response by studying publicly available sources or by engaging personnel from the target organization in conversations on forums

03 All data is used for developing parameters for threat response modeling as well to understand operational and cyber security investment patterns to understand how the target networks and systems will change in the future

04 Data on persons of interest gathered from social platforms and via data exfiltration is used to determine personality traits in order to target them in subsequent attacks

05 The exfiltrated data is also sold to data brokers as well

Malware sentience: Changing role of AI in enabling cyberattacks

Various forms of autonomous malware are being detected frequently on the web now. In 2024, we were able to track an independent threat actor based in Easten Europe that was selling self-learning payloads that came with minimal lines of code but were able to latch on to networks and use data triggers to evolve and indulge in land and expand tactics in target networks. These payloads were more akin to semi-sentient code strands than full fledged operational payloads.

By releasing such strands on a wide scale, hacker groups will increase the chances of a strand making it past defense mechanisms a landing in a target network where it can then use the network resources to autonomously unpack itself and morph into a more potent payload or even a full fledged malware with a capability to bypass signature-based detection systems by blending in fully and generating smaller footprint.

Such payloads can play multiple roles across its lifecycle. From periodic exfiltration of simple data packets all the way to blocking data packets or instructions to systems or other actions designed to slow down or inhibit the operational effectiveness of the system as a whole. In case of critical infrastructure linked to utilities, this can lead to loss of power or water treatment plants coming to a grinding halt.

Such payloads can also be used to exfiltrate data from hand-held devices, HMIs, emails, manuals or even devices.

AI-backed malware/recon campaigns

Autonomous systems can be programed to launch periodic campaigns against targets including systems, networks, key personnel and even OEMs. With increase in data exfiltrated after each round of successful cyberattacks, the volume of data gathered increases and feeds into making the subsequent campaign phase more potent. The entire set-up including malware staging sites, launchpads, phishing campaigns and command and control servers are all managed autonomously across multiple locations to ensure higher redundancy levels.

AI can also help hackers in identifying target employees who may have traits that may prove helpful to them in attaining mission\campaign objectives. Our team did come across an email sent to an employee at a leading manufacturing company in the Middle East by an anonymous entity offering USD 35,000 for sharing their login credentials and information on a specific set of devices that was part of their infrastructure. Such brazen attempts do indicate that hackers are operating with more confidence and lesser chances of being caught or persecuted.

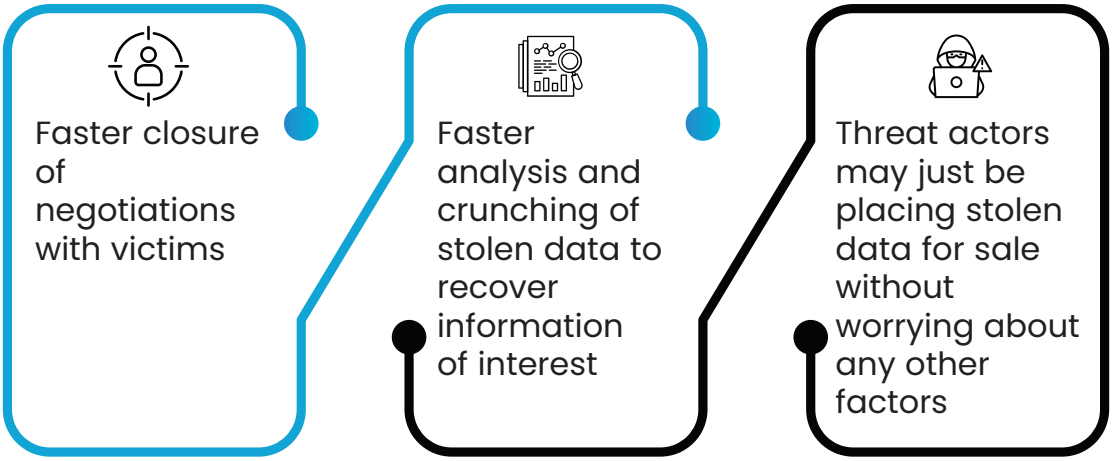
Hackers are also using AI in malware testbeds to improve the malware capabilities across environments. Such tests leads to the development of malware that is not just more stealthy but can also exfiltrate data faster.

Core AI traits being used by hackers today	Evolutionary paths being considered or experimented upon by threat actors
Target profiling (Systems, people and processes)	Polymorphic malware that can modify footprint to evade detection
Campaign management	Independent payload with minimal code that can execute a specific task in the target network
Stealth including mimic the footprint of approved applications, systems and services	Malware that can trick systems into relieving data
Staggered data harboring and exfiltration	Supply chain infiltration in a coordinated manner by tapping into multiple points of entry/exploit
Autonomous malware	
Malware that can reverse engineer protocols	

In addition to the above, Generative adversarial networks (GANs) can simulate real-time OT operations, creating false-positive signals to mask attacks.

Stolen data is being placed for sale faster

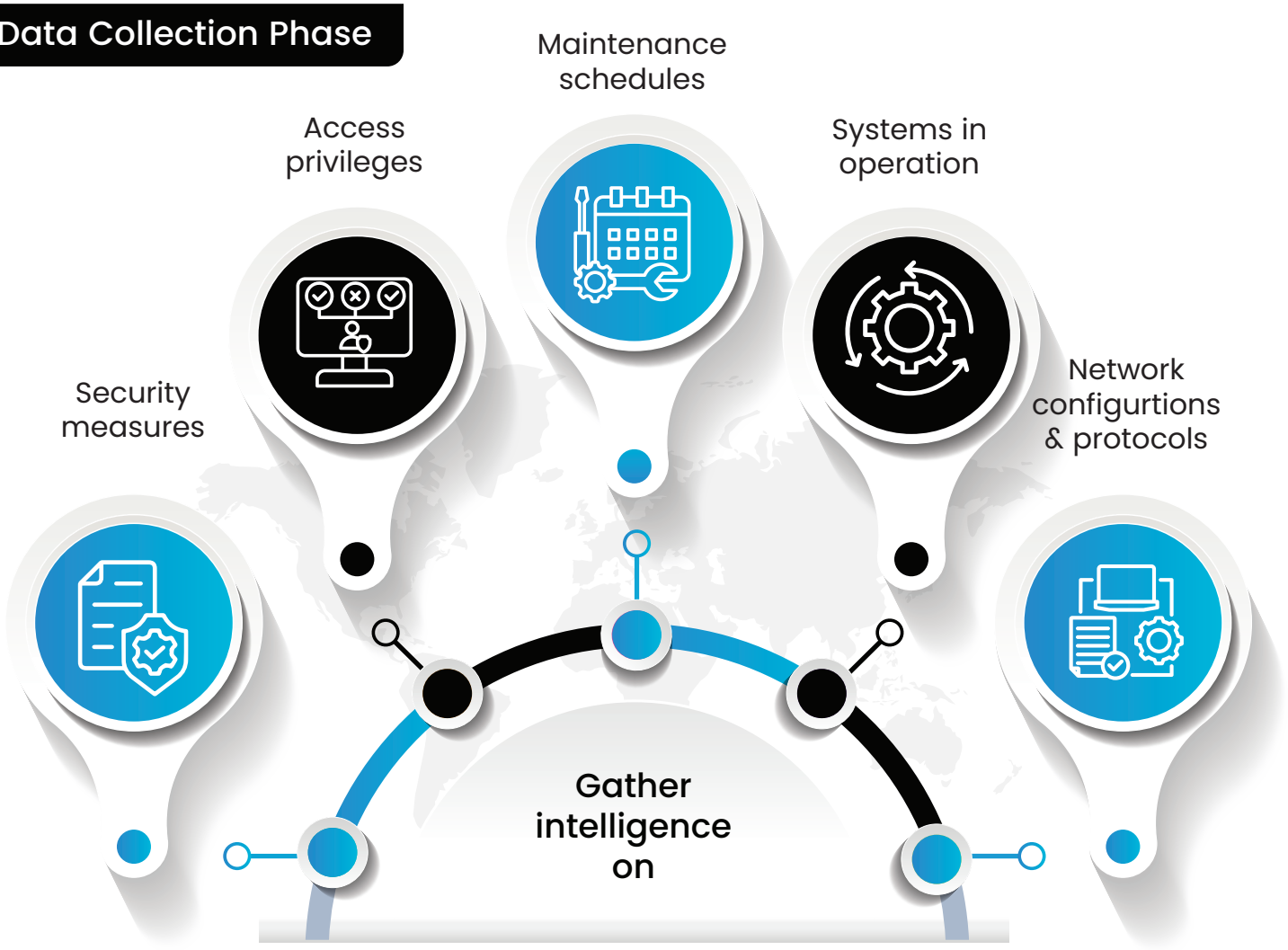
Across 27 major events that our team analysed, the time taken by hackers to place stolen data for sale on various forums has reduced by an average of 3 days in 2024. This could be because of the following reasons



With stolen data being made available for sale faster, more threat actors can get access to information that can be used for improving their ability to target more victims in the future. There have been allegations of LLMs being trained on stolen data in the past. For hackers targeting specific enterprises, data on security measures, access privileges, maintenance timings, systems in operation, network configurations and protocols could potentially be used to frame a model for launching a hacking campaign when a Zero Day becomes available or even in situations where a rogue LLM used by the hackers can frame a campaign using this data.

A campaign that relies on this approach could proceed in the below phases:

Data Collection Phase



Analysis & Modeling

	Use LLMs or AI tools to correlate collected data
	Identify vulnerabilities & high-value targets
	Predict optimal attack windows (e.g., during maintenance or off-hours)

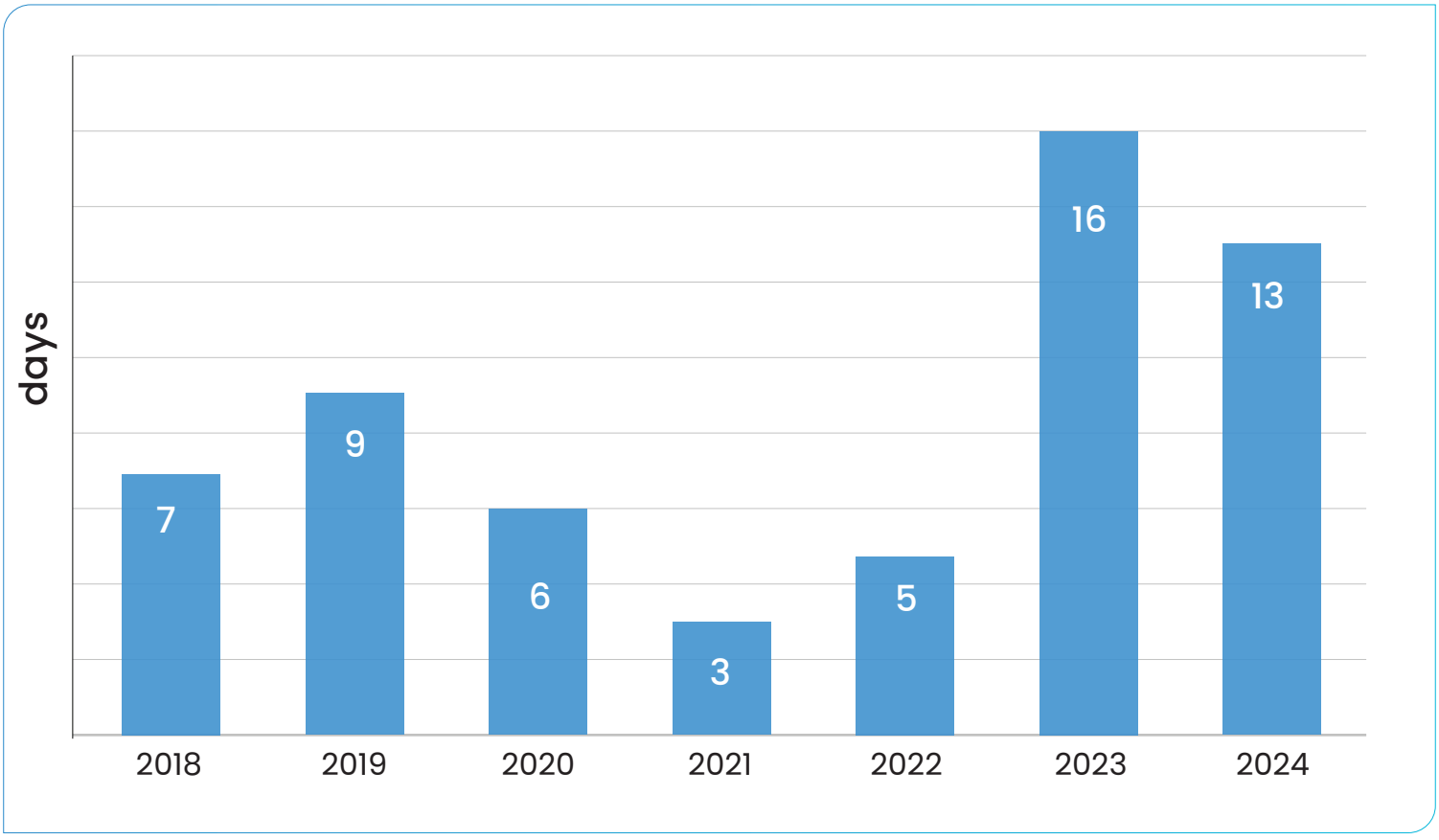
Exploitation Strategy

- Prepare payloads for known vulnerabilities
- Wait for a Zero Day to emerge
- If using a rogue LLM, generate an automated attack playbook

Execution & Attack

- Deploy malware, phishing, or direct exploits
- Establish persistence & escalate access
- Exfiltrate data or disrupt operations

Average number of days taken to place stolen data on sale



Understanding the role of AI in more detail

AI has significantly augmented the data correlation capabilities of malicious actors, enabling sophisticated targeted attacks. Historically, identifying a vulnerable insider required manual data aggregation across heterogeneous online platforms, necessitating extensive breach data parsing and social media scraping.

Contemporary attack vectors leverage AI-driven web crawlers and data mining techniques to automate the extraction of Personally Identifiable Information (PII) from publicly available breach databases and social media APIs. Natural Language Processing (NLP) models are then employed to identify and extract relevant data points, such as contact information, social affiliations, and behavioral patterns, facilitating the construction of comprehensive target profiles.

The output of this automated data synthesis pipeline includes structured data representations of the target, enriched with potential attack vectors such as phishing email templates and deepfake media generated using Generative Adversarial Networks (GANs). These profiles are subsequently integrated into existing attack campaigns or used to initiate novel, highly targeted attacks against strategic assets.

The integration of AI into these workflows represents a paradigm shift, enabling adversaries to achieve a level of automation, precision, and persistence previously unattainable through manual methods.

Threat actors and groups such as RansomHub are already using advanced methods for data exfiltration and encryption. With LLMs coming into the picture, RansomHub is already exploring various paths to using AI in its operations extensively. Based on initital investigations, we have found the group using AI to execute the following tasks

- Identifying targets (based on use of certain systems that are vulnerable or past breaches)
- Deploying targeted means of attack against potential victims (instead of using a method that could fail and alert potential victims, the groups tries to succeed on its first attempt)
- Negotiations with victims including making threatening calls and sending emails with ransom demand from temporary emails
- Crunching stolen data

Data Collection

- Security measures
- Access privileges
- Maintenance schedules
- Systems in operation
- Network configurations & protocols

Analysis & Modeling

- Use LLMs or AI tools to correlate collected data
- identify vulnerabilities & high-value targets
- Predict optimal attack windows Systems in operation

Exploitation Strategy

- Prepare payloads for known vulnerabilities
- Wait for a Zero Day to emerge
- if using a rogue LLM, generate an automated attack playbook

Execution & Attack

- Deploy malware, phishing, or direct exploits
- Establish persistence & escalate access
- Exfiltrate data or disrupt operations

The Convergence of Artificial Intelligence and Malicious Software Development: A Detailed Analysis

The integration of Artificial Intelligence (AI) into the realm of malware development presents a significant and evolving threat landscape. Malicious actors are leveraging AI's capabilities to create sophisticated, adaptive, and evasive malware that challenges traditional security paradigms.

AI-Driven Malware Development: Technical Deep Dive

Adaptive Polymorphism and Metamorphism

AI, particularly machine learning (ML) techniques like reinforcement learning (RL) and generative adversarial networks (GANs), enables the creation of malware that can dynamically alter its code and behavior.

RL: Malware can be trained in simulated network environments to learn optimal evasion strategies. By receiving feedback on its detection rate, it can refine its code to bypass security measures.

GANs: GANs can generate new malware variants that are statistically similar to benign files, making them difficult to detect using signature-based methods.

This results in highly polymorphic and metamorphic malware that can evade static analysis and signature-based detection as mentioned earlier.

This can also be used to change the protocols used by the malware to communicate with command and control servers, making network based detection difficult.

Behavioral Mimicry and Network Blending

AI allows malware to analyze network traffic patterns and system behavior to mimic legitimate processes to minimize its signature and detectability.

By understanding baseline network activity, an AI-based malware can blend its communication and actions, making it appear as normal traffic. This can help in entrenching the malware for months or even years before its activation for a disruptive action by the handler.

For instance, malware can simulate the behavior of a common application or service, making it difficult to distinguish from legitimate activity. While this is commonplace in the IT world, the presence of a plethora of protocols prevented threat actors from targeting OT in the past but that is no longer the case as hackers are deploying AI-based protocol dissectors to read protocol-based data in the OT network.

Malware can also adapt its data patterns to resemble normal data traffic, effectively hiding in plain sight.

Autonomous Operation and Dynamic Adaptation

AI empowers malware to operate autonomously, adapting to changing network conditions and security measures.

This includes the ability to dynamically adjust its attack vectors, encryption algorithms, and communication protocols.

Malware can analyze network encryption techniques and dynamically adapt its own encryption to maintain covert communication.

This can also include the ability for the malware to change its target within a network, if the original target becomes unavailable, or heavily defended.

AI-Powered Target Profiling and Attack Optimization

AI can be used to analyze large datasets of target information, including social media profiles, network configurations, and vulnerability databases.

This allows malware to generate highly targeted phishing attacks, exploit zero-day vulnerabilities, and customize attack payloads for specific victims.

AI can also be used to predict the success rate of different attack vectors, allowing attackers to optimize their strategies.

Automated Vulnerability Discovery and Exploitation

AI can be used to automatically find vulnerabilities in software and hardware.

Tools are being developed that utilize fuzzing and symbolic execution with AI to find zero day exploits, that can then be used in malware.

This can allow for the creation of malware that can exploit vulnerabilities before they are known to security vendors.

Challenges and Limitations

The only factor that is presently slowing down hackers in developing malware that is exponentially more potent is errors in training data emerging from bad storage and data refinement practices.

Another factor that is contributing significantly is the computational power needed to process and generate advanced features in AI-based malware.

Updates on LockBit-NG

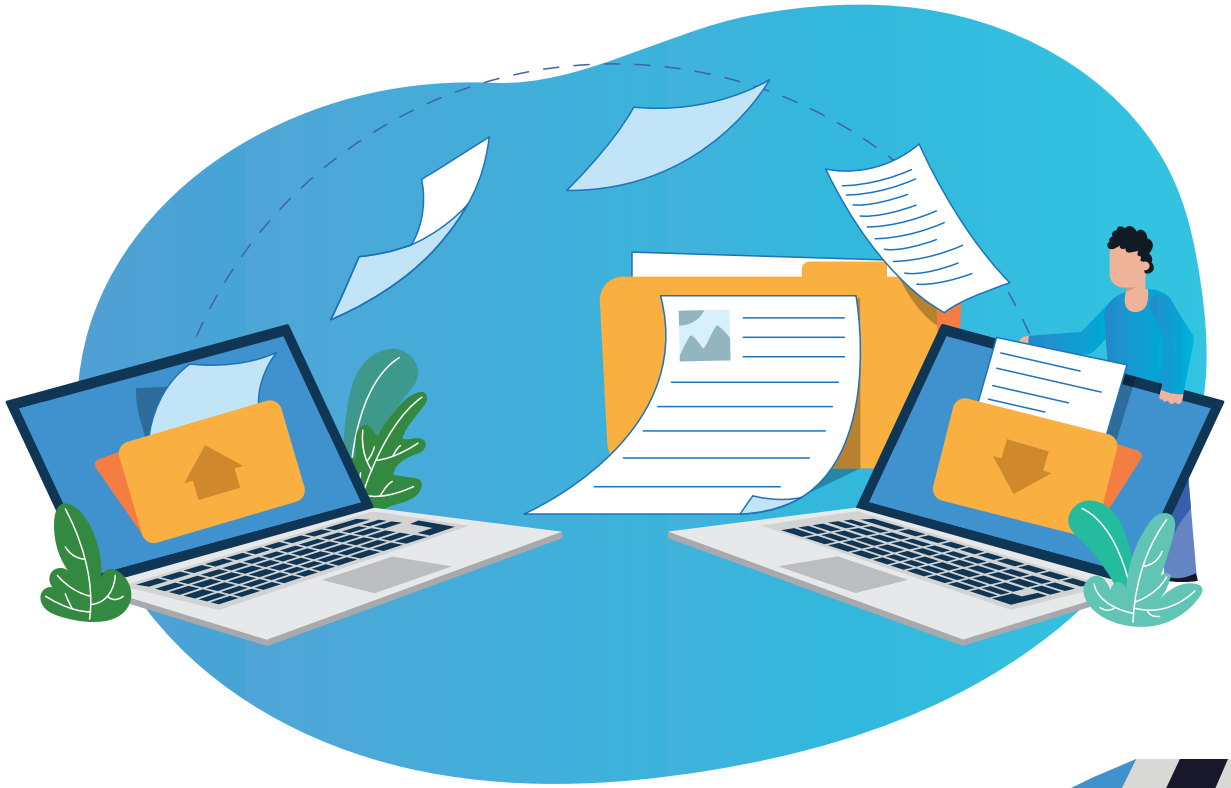
After its takedown in a major operation in early 2024, threat actor LockBit began its attempt to regroup immediately. The group informally launched two new LockBit variants with completely new code bases surfaced within a few months. Thanks to the availability of countries which offer persecution free operations to threat actors, such groups are able to regroup fairly easily and continue building more potent versions of ransomware leveraging institutionalized knowledge and attack tactics.

In December 2024, the threat actor announced its revival with the formal launch of LockBit 4.0 made available in two variants. These two variants were just reworked versions of the variants released after criminal prosecution in early 2024. One reason behind the group releasing two variants so early was its need to hang on to the vast network of affiliates and to preserve its reputation. It even went as far as declaring its support for a candidate in US elections.

Lockbit 4.0's first variant comes with enhanced stealth features with multiple security bypass mechanisms and covered data exfiltration. A key theme of this release is evasion. This variant can even disable security features in the host system while dropping the ransom text note.

Each attack beings with two script initiations. The first one, a slightly altered PoweShell script that initiates a secondary script leading to the deployment of a malicious DLL. The Mitre tactics include Execution, Command and Control, Exfiltration, Credential Access, Privilege Escalation, Persistence, Defense Evasion, Initial Access, Discovery and Impact. LockBit 4.0 also has a ultra-quiet mode that allows file names to be kept unchanged. This reduces the footprint even further.

From all signs, Lockbit 4.0 is in a very early stage of development. The two variants released indicate a possible level of tactical obfuscation and may be an attempt to confuse threat researchers.



Use of AI by APT groups

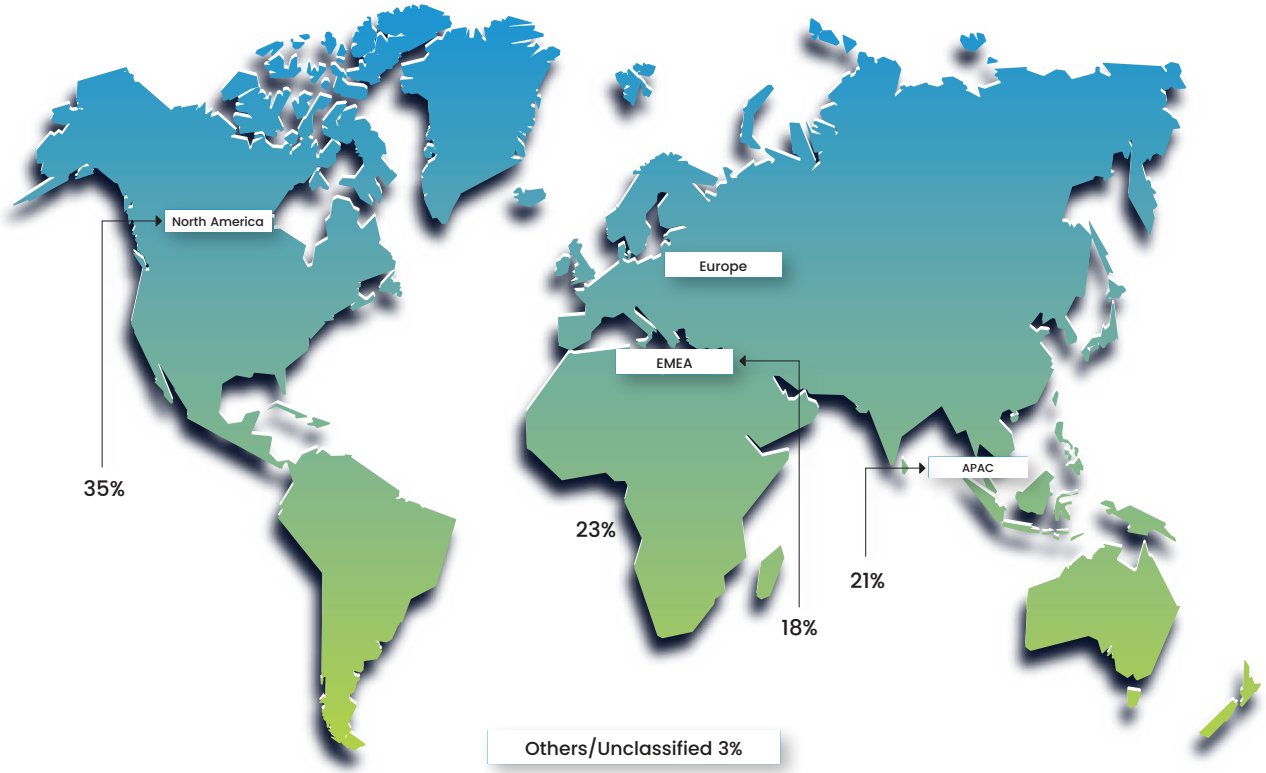
Other than APT groups such as APT 41 based in China, a few other APT groups have also started using AI in some way.

Group	Origin	Targets	Level of maturity and use
Dark Pink/Cicada	South-East Asia	Armed forces, hacktivist groups and government agencies	Evolving. From using AI purely for phishing, this group is now using AI to crawl the web and to select targets
Vixen Panda	China	Middle East and North Africa	Beginner. Web crawling for information gathering
Static Kitten	Iran	US, UK, Australia, UAE, Qatar, Israel, Germany, India, Central and Eastern Europe	Beginner. Using AI-based spiders to crawl target networks
Imperial kitten	Iran	US, UAE, Qatar, Israel, Germany, Saudi Arabia and Egypt	Uses LLM to generate convincing phishing emails and content for fake websites.
Gamaredon	Russia	Ukrainian and NATO targets	Advanced. Is using AI for gathering intelligence on defense targets including individuals.
APT 29	Russia	Targets across Europe and NATO	Advanced. Has developed individual-specific tracking tools to track the digital footprints of high-value targets
Turla	Russia	Diplomatic intel from Eastern European countries	Is known to support many APTs groups in Russia by developing blueprints of espionage tools

The integration of artificial intelligence (AI) within Advanced Persistent Threat (APT) groups varies, influenced by factors such as operational scale, target profiles, and resource availability. Notably, APT groups engaging with targets that possess robust, geographically dispersed infrastructures are increasingly adopting AI-based tools to enhance the efficacy of their cyber operations.

Our analysis has unearthed 61 distinct state backed cyber threat actors who are leveraging AI technologies to enhance their cyber and information warfare strategies. These groups employ AI for most of the tasks listed earlier in addition to stealing malware code bases from other hackers and developing them using AI.

Global distribution of cyberattacks percentage



The level of network accessibility is also playing a key role in hackers targeting OT installations.

Exposed CPS linked networks

Between November and December 2024, our threat research team conducted a systematic study to assess the extent of Industrial Control Systems (ICS) infrastructure accessible via the public Internet. This research builds on our 2023 analysis, aiming to quantify and evaluate changes in ICS exposure over time. Our latest findings indicate a 17% rise in the number of accessible ports compared to the 2023 study, highlighting a growing attack surface that could be leveraged by threat actors.

Our methodology involved an initial discovery phase using non-intrusive scanning techniques to identify exposed ICS devices, unsecured network perimeters, and open ports that serve no legitimate operational purpose. To eliminate false positives and to further ensure data integrity, we conducted a secondary validation scan, targeting only those ports that remained open 30 days after the initial scan. Another reason for this gap is to see if the OT asset owners or the security teams turn aware of the open port and fix it. Which is what happened in at least some cases as the number of open ports did drop in the subsequent scan.

This two-step verification process helped differentiate persistent exposure from transient connectivity changes, thereby enhancing the reliability of our dataset.

Historical Context: The Evolution of ICS Connectivity

Traditionally, ICS environments were designed as air-gapped systems, meaning they operated in complete isolation from external networks. This was a deliberate security measure, as ICS systems control mission-critical industrial processes, including power grids, water treatment facilities, manufacturing plants, and transportation networks. However, over the past two decades, the increased adoption of Industrial Internet of Things (IIoT), remote monitoring, and cloud-integrated operations has led to a shift away from air-gapped designs.

This shift, while enabling operational efficiencies, has inadvertently expanded the attack surface by introducing external access points into ICS environments. As a result, a growing number of ICS assets are now exposed to the Internet—often unintentionally—due to misconfigurations, legacy systems with hardcoded remote access capabilities, or poorly implemented remote access solutions.

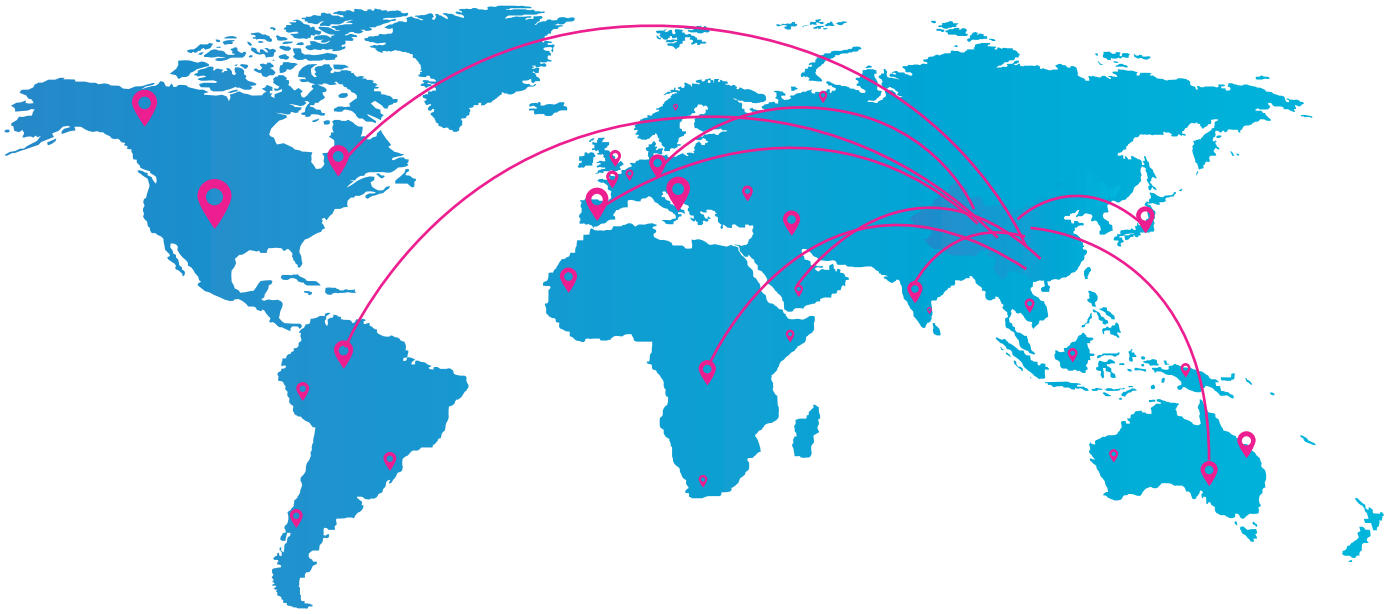
Security Implications of Unprotected ICS Ports

The presence of publicly accessible ICS devices and open ports represents a significant security risk. Threat actors can leverage exposed ports for a variety of malicious activities, including:

- **Reconnaissance and Target Profiling** – Attackers scan for publicly available ICS endpoints to map out vulnerable systems and identify potential entry points.
- **Unauthorized Access and Exploitation** – Exploiting weak authentication mechanisms, outdated firmware, or unpatched vulnerabilities to gain control over ICS components.
- **Manipulation of Industrial Processes** – In extreme cases, attackers could disrupt or alter industrial control logic, leading to safety hazards, production downtime, or even physical damage.
- **Deployment of Malware or Ransomware** – Compromised ICS networks can be used to deploy destructive malware targeting industrial operations, as seen in previous incidents involving Triton, Industroyer, and BlackEnergy.

While our research primarily focuses on identifying the extent of ICS exposure rather than investigating direct exploitation, the findings highlight a growing security gap that must be addressed immediately

Map: Geographical distribution of accessible ports across the globe

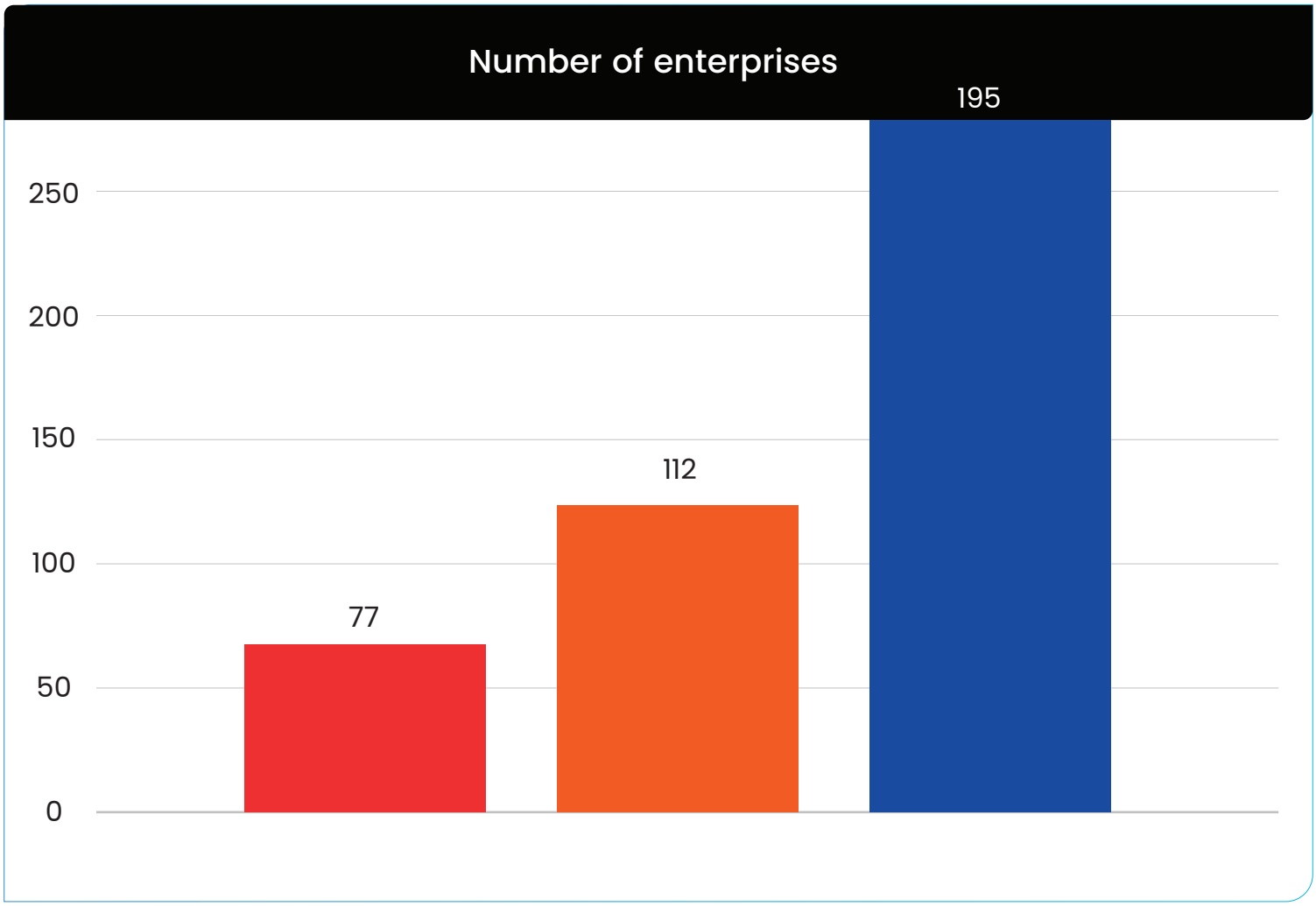


Region-wise accessibility of ICS-linked ports

Region	ICS ports accessible	Validated in repeat scan
North America	40983	39888
Asia	20444	19076
Europe	19873	18453
South America	5854	5400
Africa	1093	877
Australia	2733	2651
Others	10001	9130

First scan on 15th November 2024

Validated on 15th December 2024



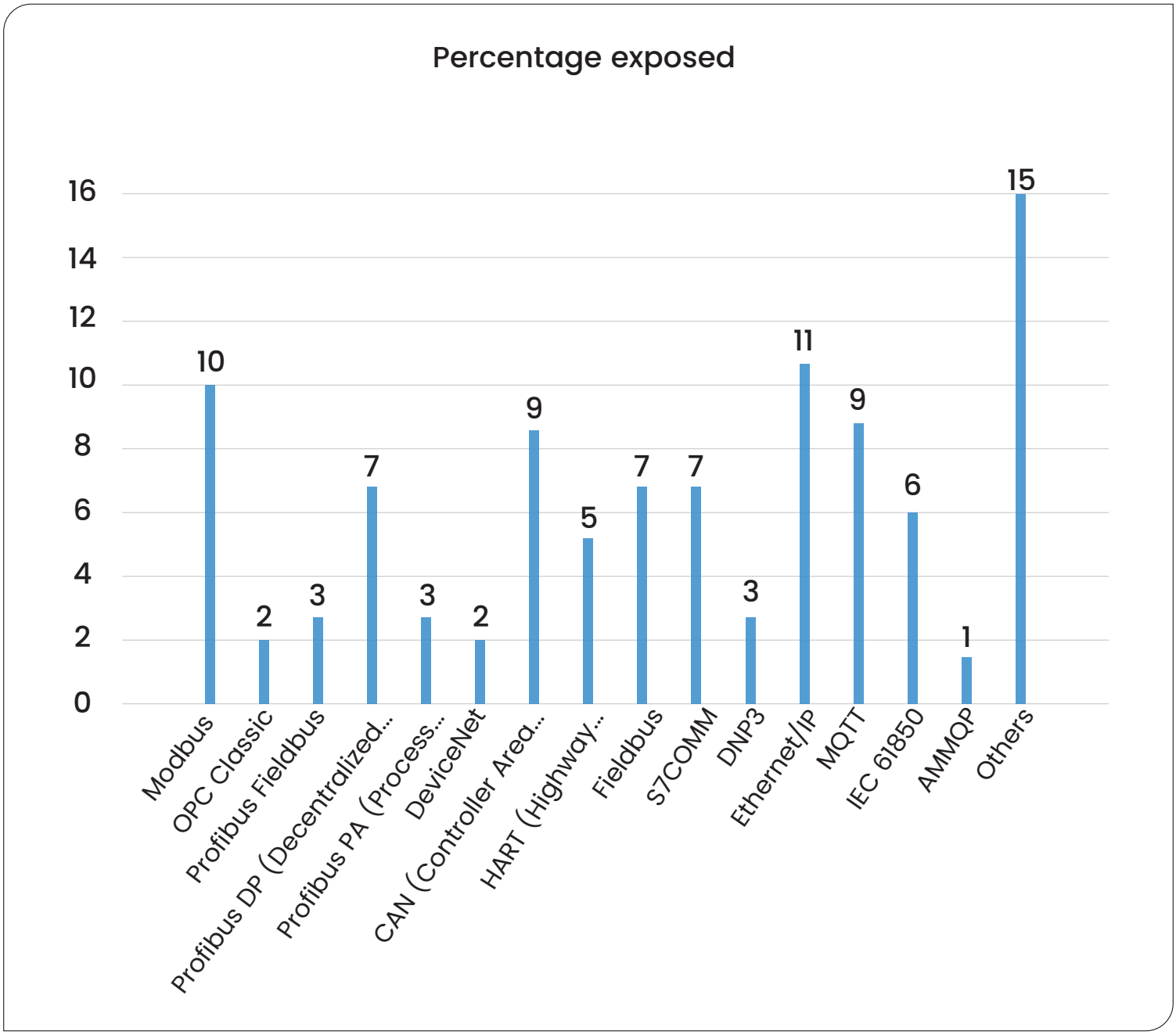
Legend

Red enterprises have 4 or more accessible ports

Orange represents those with between 1-2 ports

Blue enterprises have 1 exposed and accessible port

Percentage of systems linked to common protocols exposed



Major ICS advisories issued by CISA in 2024

Alert Code	Date	Summary	Risk
ICSA-24-354-05	December 19, 2024	ATTENTION: Exploitable remotely/low attack complexity Vulnerability: Unrestricted Upload of File with Dangerous Type	Successful exploitation of this vulnerability could allow an attacker to achieve code execution on the affected device.

Alert Code	Date	Summary	Risk
ICSA-24-354-04	December 19, 2024	ATTENTION: Exploitable remotely/low attack complexity Vulnerability: Heap-based Buffer Overflow	Successful exploitation of this vulnerability could allow an unauthenticated remote attacker arbitrary code execution.
ICSA-24-354-03	December 19, 2024	ATTENTION: Low attack complexity Vulnerability: Deserialization of Untrusted Data	Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code.
ICSA-24-354-02	December 19, 2024	ATTENTION: Exploitable from adjacent network	Successful exploitation of these vulnerabilities
		Vulnerabilities: Origin Validation Error, Incorrect Authorization	could allow an attacker to escalate privileges and access sensitive information.
ICSA-24-354-01	December 19, 2024	• ATTENTION: Exploitable remotely • Vulnerability: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Successful exploitation of this vulnerability could allow an attacker to cause a denial-of-service condition.
ICSA-24-352-04	December 17, 2024	ATTENTION: Exploitable remotely/low attack complexity Vulnerability: Improper Input Validation	Successful exploitation of this vulnerability could lead to a denial-of-service and a loss of confidentiality and integrity in the controller.

Alert Code	Date	Summary	Risk
ICSA-24-352-03	December 17, 2024	ATTENTION: Exploitable remotely/low attack complexity Vulnerability: Unprotected Alternate Channel, Heap-based Buffer Overflow, Classic Buffer Overflow	Successful exploitation of these vulnerabilities could allow an attacker to perform edit operations, create admin users, perform factory reset, execute arbitrary code, or cause a denial-of-service condition.
ICSA-24-352-02	December 17, 2024	ATTENTION: Exploitable remotely/low attack complexity Vulnerability: Improper Input Validation	Successful exploitation of this vulnerability could allow an attacker to cause a denial-of-service condition.
ICSA-24-347-10	December 12, 2024	ATTENTION: Exploitable from adjacent network Vulnerability: Incorrect Synchronization	Successful exploitation of these vulnerabilities could allow an attacker to cause a denial-of-service condition.
ICSA-24-347-09	December 12, 2024	ATTENTION: Low Attack Complexity Vulnerability: Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Write, NULL Pointer Dereference, Use After Free, Stack-based Buffer Overflow	Successful exploitation of these vulnerabilities could allow an attacker to affect confidentiality, integrity, or availability of the affected products.

Alert Code	Date	Summary	Risk
ICSA-24-347-08	December 12, 2024	ATTENTION: Low Attack Complexity Vendor: Siemens Equipment: COMOS Vulnerability: Improper Restriction of XML External Entity Reference	Successful exploitation of these vulnerabilities could allow an attacker to extract arbitrary application files.
ICSA-24-347-07	December 12, 2024	ATTENTION: Low Attack Complexity Vendor: Siemens Equipment: Solid Edge SE2024 Vulnerability: Heap-based Buffer Overflow, Integer Underflow (Wrap or Wraparound)	Successful exploitation of these vulnerabilities could allow an attacker to execute code in the context of the current process.
ICSA-24-347-06	December 12, 2024	• ATTENTION: Low Attack Complexity • Vendor: Siemens • Equipment: Simcenter Femap • Vulnerability: Heap-based Buffer Overflow, Improper Restriction of Operations within the Bounds of a Memory Buffer	Successful exploitation of these vulnerabilities could allow an attacker to execute code in the context of the current process.

Alert Code	Date	Summary	Risk
ICSA-24-347-05	December 12, 2024	ATTENTION: Low Attack Complexity Vendor: Siemens Equipment: Siemens Engineering Platforms Vulnerability: Deserialization of Untrusted Data	Successful exploitation of this vulnerability could allow an attacker to cause a type confusion and execute arbitrary code within the affected application.
ICSA-24-347-04	December 12, 2024	• ATTENTION: Low Attack Complexity • Vendor: Siemens • Equipment: Parasolid • Vulnerability: Out-of-bounds Write	Successful exploitation of this vulnerability could allow an attacker to execute code in the context of the current process.
ICSA-24-347-03	December 12, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Siemens • Equipment: RUGGEDCOM ROX II • Vulnerability: Cross-Site Request Forgery	Successful exploitation of this vulnerability could allow an attacker to perform administrative actions if an authenticated user is tricked into accessing a malicious link.
ICSA-24-347-02	December 12, 2024	• ATTENTION: Low attack complexity • Vendor: Siemens • Equipment: Siemens Engineering Platforms • Vulnerability: Improper Input Validation	Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands.

Alert Code	Date	Summary	Risk
ICSA-24-347-01	December 12, 2024	• ATTENTION: Low Attack Complexity • Vendor: Siemens • Equipment: CPCI85 Central Processing/Communi-cation • Vulnerability: Insufficiently Protected Credentials	Successful exploitation of this vulnerability could allow an attacker with physical access to the device to decrypt the firmware.
ICSA-24-345-03	December 10, 2024	• ATTENTION: Low Attack Complexity • Vendor: Schneider Electric • Equipment: FoxRTU Station • Vulnerability: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Successful exploitation of this vulnerability could allow an attacker to perform remote code execution.
ICSA-24-345-02	December 10, 2024	• ATTENTION: Low Attack Complexity • Vendor: Schneider Electric • Equipment: EcoStruxu-re Foxboro DCS Core Control Services • Vulnerability: Out-of-bounds Write, Improper Validation of Array Index, Improper Input Validation	Successful exploitation of these vulnerabilities could lead to a loss of system functionality or unauthorized access to system functions.

Alert Code	Date	Summary	Risk
ICSA-24-338-05	December 03, 2024	• ATTENTION: Low Attack Complexity • Vendor: Fuji Electric • Equipment: Monitouch V-SFT • Vulnerability: Out-of-bounds Write	Successful exploitation of these vulnerabilities could crash the device being accessed.
ICSA-24-338-06	December 03, 2024	• ATTENTION: Low Attack Complexity • Vendor: Schneider Electric • Equipment: Tellus Lite V-Simulator • Vulnerability: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Successful exploitation of these vulnerabilities could crash the device being accessed.
ICSA-24-338-04	December 03, 2024	• ATTENTION: Low Attack Complexity • Vendor: ICONICS, Mitsubishi Electric • Equipment: ICONICS GENESIS64 Product Suite and Mitsubishi Electric MC Works64 • Vulnerability: Uncontrolled Search Path Element, Dead Code	Successful exploitation of these vulnerabilities could result in remote code execution.

Alert Code	Date	Summary	Risk
ICSA-24-338-02	December 03, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Fuji Electric • Equipment: RUGGEDCOM APE1808 • Vulnerability: Missing Authentication for Critical Function, NULL Pointer Dereference, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Successful exploitation of these vulnerabilities could allow an attacker to gain access to the management web interface or cause a denial-of-service condition.
ICSA-24-331-05	Nov 26, 2024	• ATTENTION: Exploitable remotely • Vendor: Hitachi Energy • Equipment: RTU500 Scripting Interface • Vulnerability: Improper Certificate Validation	Successful exploitation of this vulnerability could allow attackers to spoof the identity of the service.

Alert Code	Date	Summary	Risk
ICSA-24-331-04	Nov 26, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Hitachi Energy • Equipment: MicroSCADA Pro/X SYS600 • Vulnerability: Improper Neutralization of Special Elements in Data Query Logic, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Authentication Bypass by Capture-replay, Missing Authentication for Critical Function, URL Redirection to Untrusted Site ('Open Redirect')	Successful exploitation of these vulnerabilities could allow an attacker to inject code towards persistent data, manipulate the file system, hijack a session, or engage in phishing attempts against users.
ICSA-24-331-03	Nov 26, 2024	• ATTENTION: Exploitable remotely • Vendor: Schneider Electric • Equipment: EcoStruxure Control Expert, EcoStruxure Process Expert and Modicon M340, M580 and M580 Safety PLCs • Vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Use of Hard-coded Credentials, Insufficiently Protected Credentials	Successful exploitation of these vulnerabilities could allow a denial of service, a loss of confidentiality, and threaten the integrity of controllers

Alert Code	Date	Summary	Risk
ICSA-24-331-02	Nov 26, 2024	• ATTENTION: Low attack complexity • Vendor: Schneider Electric • Equipment: PowerLogic P5 • Vulnerability: Use of a Broken or Risky Cryptographic Algorithm	If an attacker has physical access to the device, it is possible to reboot the device, cause a denial of service condition, or gain full control of the relay by abusing a specially crafted reset token.
ICSA-24-331-01	Nov 26, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Schneider Electric • Equipment: PowerLogic PM5500 and PowerLogic PM8ECC • Vulnerability: Weak Password Recovery Mechanism for Forgotten Password, Improper Authentication	Successful exploitation of these vulnerabilities could result in an attacker gaining escalated privileges and obtaining control of the device.
ICS Advisory | ICSA-24-326-06	Nov 21, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Schneider Electric • Equipment: PowerLogic PM5300 Series • Vulnerability: Uncontrolled Resource Consumption	Successful exploitation of this vulnerability could cause the device to become unresponsive resulting in communication loss.

Alert Code	Date	Summary	Risk
ICS Advisory | ICSA-24-326-05	Nov 21, 2024	• CVSS v4 10.0 • ATTENTION: Exploitable remotely/low attack complexity • Vendor: Schneider Electric • Equipment: EcoStruxure IT Gateway • Vulnerability: Missing Authorization	Successful exploitation of this vulnerability could allow unauthorized access.
ICS Advisory | ICSA-24-326-04	Nov 21, 2024	• ATTENTION: Exploitable remotely • Vendor: Schneider Electric • Equipment: Modicon M340, MC80, and Momentum Unity M1E • Vulnerability: Improper Input Validation, Improper Restriction of Operations within the Bounds of a Memory Buffer	Successful exploitation of these vulnerabilities could allow an attacker to tamper with memory on these devices.

Alert Code	Date	Summary	Risk
ICS Advisory | ICSA-24-326-03	Nov 21, 2024	• ATTENTION: Exploitable remotely • Vendor: Schneider Electric • Equipment: Modicon M340, MC80, and Momentum Unity M1E • Vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Authentication Bypass by Spoofing	Successful exploitation of these vulnerabilities could allow an attacker to retrieve password hashes or cause a denial-of-service condition.
ICS Advisory | ICSA-24-319-16	Nov 14, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Hitachi Energy • Equipment: MSM • Vulnerability: Missing Release of Resource after Effective Lifetime, Loop with Unreachable Exit Condition ('Infinite Loop')	Successful exploitation of these vulnerabilities could allow an attacker to impact the confidentiality, integrity or availability of the MSM.
ICSA-24-319-15	Nov 14, 2024	• ATTENTION: Low attack complexity • Vendor: Rockwell Automation • Equipment: Arena Input Analyzer • Vulnerability: Improper Validation of Specified Quantity in Input	Successful exploitation of this vulnerability could allow an attacker to disclose information and execute arbitrary code on the program.

Alert Code	Date	Summary	Risk
ICSA-24-319-07	Nov 21, 2024	• ATTENTION: Exploitable remotely • Vendor: Siemens • Equipment: Siemens Engineering Platforms • Vulnerability: Deserialization of Untrusted Data	Successful exploitation of this vulnerability could allow an attacker to cause a type confusion and execute arbitrary code within the affected application.
ICSA-24-319-04	November 14, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Siemens • Equipment: SINEC NMS • Vulnerability: Improper Input Validation, Improper Check for Unusual or Exceptional Conditions, Out-of-bounds Write, Uncontrolled Resource Consumption, HTTP Request/Response Splitting, Missing Encryption of Sensitive Data, Out-of-bounds Read, Improper Certificate Validation, Missing Release of Resource after Effective Lifetime, Improper Validation of Certificate with Host Mismatch, Allocation of Resources Without Limits or Throttling, Incorrect Permission Assignment for Critical Resource	Successful exploitation of this could allow an authenticated medium-privi-leged attacker to write arbitrary content to any location in the filesystem of the host system.

Alert Code	Date	Summary	Risk
ICSA-24-284-20	October 10, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Rockwell Automation • Equipment: ControlLogix • Vulnerability: Improper Input Validation	Successful exploitation of this vulnerability could allow an attacker to send a specially crafted CIP message and cause a denial-of-service condition on the affected device.
ICSA-24-284-11	October 10, 2024	• ATTENTION: Exploitable remotely • Vendor: Siemens • Equipment: RUGGEDCOM APE1808 • Vulnerability: Incorrect Authorization	Successful exploitation of this vulnerability could allow an attacker to cause a limited denial-of-service condition, data loss, or information disclosure.
ICSA-24-284-02	October 10, 2024	• ATTENTION: Low Attack Complexity • Vendor: Siemens • Equipment: Simcenter Nastran • Vulnerability: Heap-based Buffer Overflow, Improper Restriction of Operations within the Bounds of a Memory Buffer	Successful exploitation of these vulnerabilities could allow an attacker to execute code in the context of the current process.

Alert Code	Date	Summary	Risk
ICSA-24-284-01	October 10, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Siemens • Equipment: SIMATIC S7-1500 and S7-1200 CPUs • Vulnerability: Open Redirect	Successful exploitation of this vulnerability could allow an attacker to make the web server of affected devices redirect a legitimate user to an attacker-chosen URL.
ICSA-24-261-03	September 17, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Yokogawa • Equipment: Dual-redundant Platform for Computer (PC2CKM) • Vulnerability: Unchecked Return Value	Successful exploitation of this vulnerability could allow an attacker to perform a denial-of-service.
ICSA-24-289-02	October 15, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Schneider Electric • Equipment: Data Center Expert • Vulnerability: Improper Verification of Cryptographic Signature, Missing Authentication for Critical Function	Successful exploitation of these vulnerabilities could allow an attacker to access private data.

Alert Code	Date	Summary	Risk
ICSA-24-284-20	October 10, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Rockwell Automation • Equipment: ControlLogix • Vulnerability: Improper Input Validation	Successful exploitation of this vulnerability could allow an attacker to send a specially crafted CIP message and cause a denial-of-service condition on the affected device.
ICSA-24-284-18	October 10, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Rockwell Automation • Equipment: Compact GuardLogix, CompactLogix, ControlLogix, GuardLogix, 1756-EN4TR • Vulnerability: Uncontrolled Resource Consumption	Successful exploitation of this vulnerability could allow an attacker to cause a denial-of-service on the affected products.
ICSA-24-284-18	October 10, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Rockwell Automation • Equipment: Compact GuardLogix, CompactLogix, ControlLogix, Guard-Logix, 1756-EN4TR • Vulnerability: Uncontrolled Resource Consumption	Successful exploitation of this vulnerability could allow an attacker to cause a denial-of-service on the affected products.

Alert Code	Date	Summary	Risk
ICSA-24-261-01	September 17, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Siemens • Equipment: SIMATIC S7-200 SMART Devices • Vulnerability: Uncontrolled Resource Consumption	Successful exploitation of this vulnerability could allow an attacker to cause a denial-of-service condition.
ICSA-24-256-20	September 12, 2024	• ATTENTION: Low attack complexity • Vendor: Rockwell Automation • Equipment: ADvance Trusted SIS Workstation • Vulnerability: Improper Input Validation	Successful exploitation of these vulnerabilities could result in an attacker executing code within the context of a current process.
ICSA-24-256-15	September 12, 2024	• ATTENTION: Exploitable remotely • Vendor: Siemens • Equipment: Industrial Edge Management OS (IEM-OS), SINEMA Remote Connect Server, SINUMERIK ONE • Vulnerability: Signal Handler Race Condition	Successful exploitation of this vulnerability could allow an unauthenticated remote attacker to achieve remote code execution with high impact on the affected system.

Alert Code	Date	Summary	Risk
ICSA-24-256-08	September 12, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Siemens • Equipment: Industrial Products • Vulnerability: Improper Input Validation	Successful exploitation of this vulnerability could allow a remote attacker to cause denial-of-service condition in the affected products.
ICSA-24-256-01	September 12, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Siemens • Equipment: SINEMA Remote Connect Server • Vulnerability: Session Fixation	Successful exploitation of this vulnerability could allow a remote attacker to circumvent the additional multi-factor authentication for user session establishment.
ICSA-24-228-01	August 15, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Siemens • Equipment: RUGGEDCOM RM1224, SCALANCE M-800 Family • Vulnerability: Uncontrolled Resource Consumption, Improper Input Validation, Exposure of Data Element to Wrong Session, Insertion of Sensitive Information into Log File	Successful exploitation of these vulnerabilities could allow an authenticated attacker to execute arbitrary code, escalate privilege, forge 2FA tokens of other users, or cause a denial-of-service condition.

Alert Code	Date	Summary	Risk
ICSA-24-205-02	July 23, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Hitachi Energy • Equipment: AFS650, AFS660, AFS665, AFS670, AFS675, AFS677, AFR677 • Vulnerability: Type Confusion, Use After Free, Double Free, Observable Discrepancy	Successful exploitation of these vulnerabilities could allow an attacker to create a denial-of-service condition.
ICSA-24-198-01	July 16, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Rockwell Automation • Equipment: Pavilion 8 • Vulnerability: Incorrect Permission Assignment for Critical Resource	Successful exploitation of this vulnerability could allow an attacker to create new users and view sensitive data.
ICSA-24-193-08	July 11, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Siemens • Equipment: Mendix Encryption • Vulnerability: Use of Hard-coded, Security-relevant Con-stants	Successful exploitation of this vulnerability could allow an attacker to decrypt any encrypted project data.

Alert Code	Date	Summary	Risk
ICSA-24-191-05	January 16, 2025	• ATTENTION: Exploitable remotely/Low attack complexity • Vendor: Johnson Controls Inc. • Equipment: Software House C CURE 9000 • Vulnerability: Incorrect Default Permissions	Successful exploitation of this vulnerability may allow an attacker to access credentials used for access to the application.
ICSA-24-165-07	June 13, 2024	• ATTENTION: Low Attack Complexity • Vendor: Siemens • Equipment: PowerSys • Vulnerability: Improper Authentication	Successful exploitation of this vulnerability could allow a local attacker to bypass authentication, thereby gaining administrative privileges for the managed remote devices.
ICSA-24-158-03	June 06, 2024	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Mitsubishi Electric • Equipment: CC-Link IE TSN Industrial Managed Switch • Vulnerability: Allocation of Resources Without Limits or Throttling	Successful exploitation of this vulnerability could allow an attacker to cause a temporary denial-of service (DoS) condition in the web service on the product.

Alert Code	Date	Summary	Risk
ICSA-24-058-01	January 16, 2025	• ATTENTION: Exploitable remotely/low attack complexity • Vendor: Mitsubishi Electric Corporation • Equipment: Multiple Factory Automation products • Vulnerability: Insufficient Resource Pool	Successful exploitation of this vulnerability could allow a remote attacker to cause a temporary denial-of-service (DoS) condition for a certain period of time in the product's Ethernet communication by performing a TCP SYN Flood attack.

The Shieldworkz research team not only analyzed open ports but also monitored attempts to exploit known CVEs associated with IoT systems. These exploitation attempts were recorded across our lab environments and real-world deployments under our observation.

The frequency and sophistication of these attacks indicate a strong awareness among threat actors of these vulnerabilities and their exploitation methods. While some of these CVEs are dated, many remain unpatched, leaving IoT projects exposed. Once an attacker gains access, they can pivot to other connected devices and systems, expanding their reach. Compromised devices are often repurposed into botnets—a frequent and concerning outcome.

Vulnerability	Total attempts
CVE-2017-17215	26355
CVE-2023-26801	987
CVE-2019-12780	1,844
CVE-UNAS-SIGNED-2020-Zyxel-CPE-Command-Injection-RCE-01	365
EDB-41471	843

Vulnerability	Total attempts
CVE-2014-8361	646
CVE-2017-18368	365
CVE-2016-10372	936
CVE-2018-10562	1992
EDB-25978	298
EDB-39596	811
CVE-2015-2051	98
EDB-31683	12
CVE-2018-9995	23
EDB-44760	11
OPENVAS-1361412562310107187	834
CVE-2016-6277	776
CVE-2020-8515	83
CVE-2009-0545	98
CVE-2019-7192	22
CVE-2019-17270	992

Vulnerability	Total attempts
CVE-2022-2488	875
CVE-2022-2486	222
CVE-2020-15920	134
CVE-2021-36260	887
CVE-2020-5847	983
CVE-2021-21805	187
CVE-2021-27561	927
CVE-2014-3206	22
CVE-2017-14135	132

Cost of ransom declines for the first time

This decline, can be explained by and attributed to many factors including:

- Increasing competition among affiliates.
- Easy access to compromised accounts through APT groups
- Cost of hacking kits and tools and tools has fallen
- AI has automated many stages of the attack reducing the cost of attack
- There have been instances where decryptors were provided by a rival hacker group for a lesser ransom payment

The number of incidents studied has reduced because we have amended the criteria to consider more complex attacks.

Cost per GB of data as demanded by hackers Vs. what was paid by the victim businesses*

Year	The approximate ransom demanded by hackers per GB (Demand) (USD)	Cost per GB (Paid by the victim organization)	Sample size* (Number of incidents)
2016	4975	4900	23
2017	7600	7000	26
2018	10,000	9000	35
2019	14,567	12000	41
2020	27,340	22,045	49
2021	50,000	39,000	51
2022	54,990	49,044	82
2023	63,711	53,001	97
2024	59,001	41,000	99

* Number of incidents studied where the information was sufficient to arrive at the ransom numbers

^ The ransom demand varies according to the threat actor, size of the data, victim, and complexity of the malware used

Sectoral attacks

In 2024, Shieldworkz researchers conducted on-site assessments of power plants and power distribution infrastructure across North America, Latin America, the Middle East, and South Asia. Our goal was to investigate the rising attacks on critical infrastructure and evaluate how the sector was responding to these escalating threats.

Across nearly all the facilities we visited, digitization initiatives were underway at various stages. However, many organizations struggled with unfilled security positions dating back to 2021, and a significant portion of legacy infrastructure remained operational without dedicated security controls or risk-mitigation policies.

The attack surface within utility firms continues to expand, with many systems remotely exploitable. Since most plants and distribution networks lack layered security defenses against persistent and sophisticated adversaries, attackers can move laterally, seize control of systems, escalate privileges, modify or crash operations, and exfiltrate sensitive data.

At one power distribution company, we discovered that smart meter consumption data was accessible via the web, making it possible to manipulate or reset meter readings—posing a serious risk to billing integrity and grid stability.

In 2024, the energy sector saw a staggering 79% surge in cyberattacks, making it the most targeted industry globally. Meanwhile, the healthcare sector also faced increasing threats, largely driven by the rapid recruitment of cybercriminal affiliates and widespread security gaps across medical institutions.

The Escalating Threat Landscape in Manufacturing: A Deep Dive into Cyberattacks

The manufacturing sector is experiencing a significant surge in cyberattacks, driven by a confluence of factors that have created a vulnerable environment. This vulnerability stems from

- **Increased Asset Complexity :** Modern manufacturing facilities are integrating a diverse range of sophisticated assets, expanding the attack surface for malicious actors.

- **Convergence of IT and OT :** The increasing integration of Information Technology (IT) and Operational Technology (OT) networks, while enhancing efficiency, also creates interconnected vulnerabilities.

- **Neglecting security legacy assets :** Older, legacy assets often lack robust security measures, making them prime targets for exploitation.

This combination of factors has rendered the manufacturing sector, particularly smart factories, highly susceptible to a wide spectrum of cyber incidents.

Targeting Smart Factories: A Global Phenomenon

As smart factories increasingly adopt automation technologies and integrate Industrial Internet of Things (IIoT) devices, they have become high-value targets for cyber adversaries. These interconnected, data-driven environments offer enhanced efficiency and productivity but also introduce complex security challenges.

In 2024, our expanded global honeypot network—purpose-built to simulate smart factory conditions—detected 906 unique threat signatures. This marked a significant increase from previous years and underscored the growing focus of threat actors on industrial environments. Notably, the majority of these threats were aimed at process-based manufacturing organizations operating across multiple geographic regions. This trend reflects the strategic significance of these facilities within global supply chains and the high impact potential of a successful cyberattack.

The sharp rise in detected threats can be directly attributed to the scale and sophistication of our monitoring infrastructure, which now more effectively captures the tactics, techniques, and procedures (TTPs) used by adversaries targeting smart manufacturing environments.

Motivations Behind Cyberattacks on Smart Factories

The drivers behind these cyberattacks are varied and often interlinked. Key motivations include:

- **Intelligence Gathering :** Threat actors are actively probing industrial networks to understand the evolving landscape of operational technology (OT), including the introduction of new machines, protocols, and digital control systems. This reconnaissance enables them to craft more precise and effective attack strategies in future operations.

- **Intellectual Property (IP) Theft :** Nation-state and Advanced Persistent Threat (APT) groups are increasingly targeting smart factories to exfiltrate sensitive intellectual property. This includes proprietary manufacturing processes, engineering designs, software algorithms, and R&D data—assets that are vital to maintaining technological and competitive advantage.

- **Exploitation of Security Gaps in Emerging Technologies** : The rapid integration of new devices—often without comprehensive cybersecurity validation—presents a significant attack surface. Devices may harbor undocumented features, misconfigurations, or backdoors that adversaries can exploit. Attackers are particularly focused on identifying these weak points in real-time production environments, where any disruption can have severe operational consequences.

- Ransom
- Training other hackers
- Selling network access to other hackers or groups

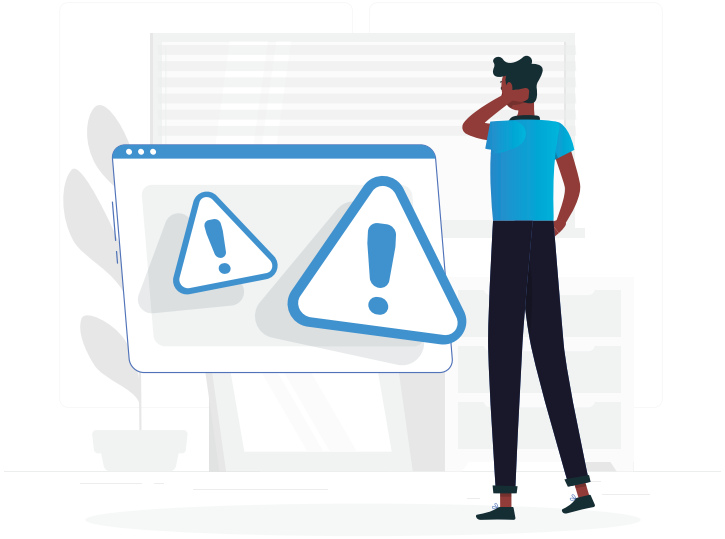
The Under reported Threat of IP Theft

A critical but often overlooked aspect of cyberattacks on manufacturing is the theft of intellectual property. The precise nature of data compromised in cyber incidents is frequently undisclosed, making it difficult to quantify the extent of IP loss including those linked to years of R&D. However, analyzing major attacks on industrial giants reveals a consistent pattern suggesting that IP theft is a significant objective. Such IP may even end up in the hands of state-backed actors who may then use it to further the economic goals of their backers.

The long term damage caused by IP theft can be devastating to a company. Loss of IP can demotivate R&D spending and force businesses to instead invest in incremental development of IP rather than looking at massive innovations that could alter processes ushering in a reduction of energy usage or even improving the quality of end product.

With such attacks, the entire supply chain linked to manufacturing loses.

Disclosure	Target	Ransom paid	Data leaked
April	Auto Major	No	Yes
July	Large food and beverage co.	No	Yes
Mid-August	Aerospace co.	No	No
Mid-November	Utility entity	No	No



Data Monetization Strategies Used by Threat Actors

In the context of large enterprises, cyber extortion does not always culminate in ransom payments. In scenarios where victims refuse to pay, threat actors pivot to alternative monetization strategies. One of the most prevalent approaches involves data exfiltration and resale. Exfiltrated datasets are sold on darknet marketplaces or via private channels to data brokers, cybercriminal syndicates, or competitive entities seeking strategic advantage.

When intellectual property (IP)—such as proprietary formulas, engineering schematics, software source code, or product designs—is involved, the data is often sold directly to state-sponsored Advanced Persistent Threat (APT) groups or indirectly to industry competitors through proxy actors. These entities are willing to pay a premium for access to high-value industrial intelligence that can accelerate their innovation cycles or inform geopolitical agendas.

Non-conventional data being sold

- Volume of production data including daily/weekly fluctuations
- Data on new employees added/existing employees promoted
- Information on configuration of systems and versions of software
- Data on rejectedstock/batch (es)

If the data cannot be monetized through direct sale or ransom, it is repackaged and repurposed for training AI models as mentioned earlier—particularly large language models (LLMs) or specialized machine learning systems that benefit from exposure to niche, domain-specific information. In such cases, threat actors either build internal tooling or sell the datasets to underground AI development operations that lack access to legitimate training data.

Regardless of the monetization pathway, victim organizations suffer long-term consequences. The exfiltrated datasets frequently include sensitive categories such as

- Customer Personally Identifiable Information (PII)
- Internal pricing models and margin analysis
- Product development roadmaps
- Strategic market research
- Legal assessments and contract terms
- Technical R&D documentation

These datasets are highly sought after in cybercriminal ecosystems. Data brokers often aggregate, sanitize, and repackage this information for resale to malicious buyers in regulated and unregulated industries alike.

Moreover, in situations where the victim lacks robust backup and disaster recovery mechanisms, the stolen data itself becomes a commodity. Threat actors may offer to resell the original data back to the victim—often at a premium—especially if the stolen datasets include irreplaceable intellectual assets or operational blueprints. In some instances, attackers simultaneously sell the data to the victim and external buyers, maximizing profit with minimal additional effort.

The fear of regulatory sanctions, legal liability, and reputational damage often drives victims to enter into negotiations—either directly or through third-party intermediaries. This is especially true in jurisdictions with stringent data protection regulations (e.g., GDPR, CCPA, NIS2), where breach disclosures can trigger compliance investigations or lawsuits.

We can say with a high level of confidence that every bit of data stolen by hackers and put on sale has a buyer.

Stolen data continues to be on sale 4 years later

In November 2020, a large Indian online grocery delivery service was hacked leading to the leakage of approximately 20 million user records containing personal information such as emails, names, hashed passwords, birthdates and phone numbers were leaked. and hashed passwords.

As late as December 2024, two unconnected mid-sized travel firm and another firm in the consumer durables sector were running campaigns using this very data. Both these firms claimed to have a promotional tie-up with the victim online grocery delivery service to offer packages to the customers of the victim. They were running a national tele-calling campaign to reach out to the customers sharing stolen data to prove the tie up with the online grocery retailer was a genuine one.

When this brought to the attention of the victim online grocery delivery service, they denied any link with these firms and promised to investigate the matter.

A threat actor named ShinyHunter is still selling the data as of November 2024.

Targeted Threat Landscape: Oil and Gas Sector

The oil and gas industry remains a high-priority target for both financially motivated and nation-state adversaries. While opportunistic cybercriminals focus on extortion and data resale, APT actors consistently target this sector for its geopolitical and economic significance.

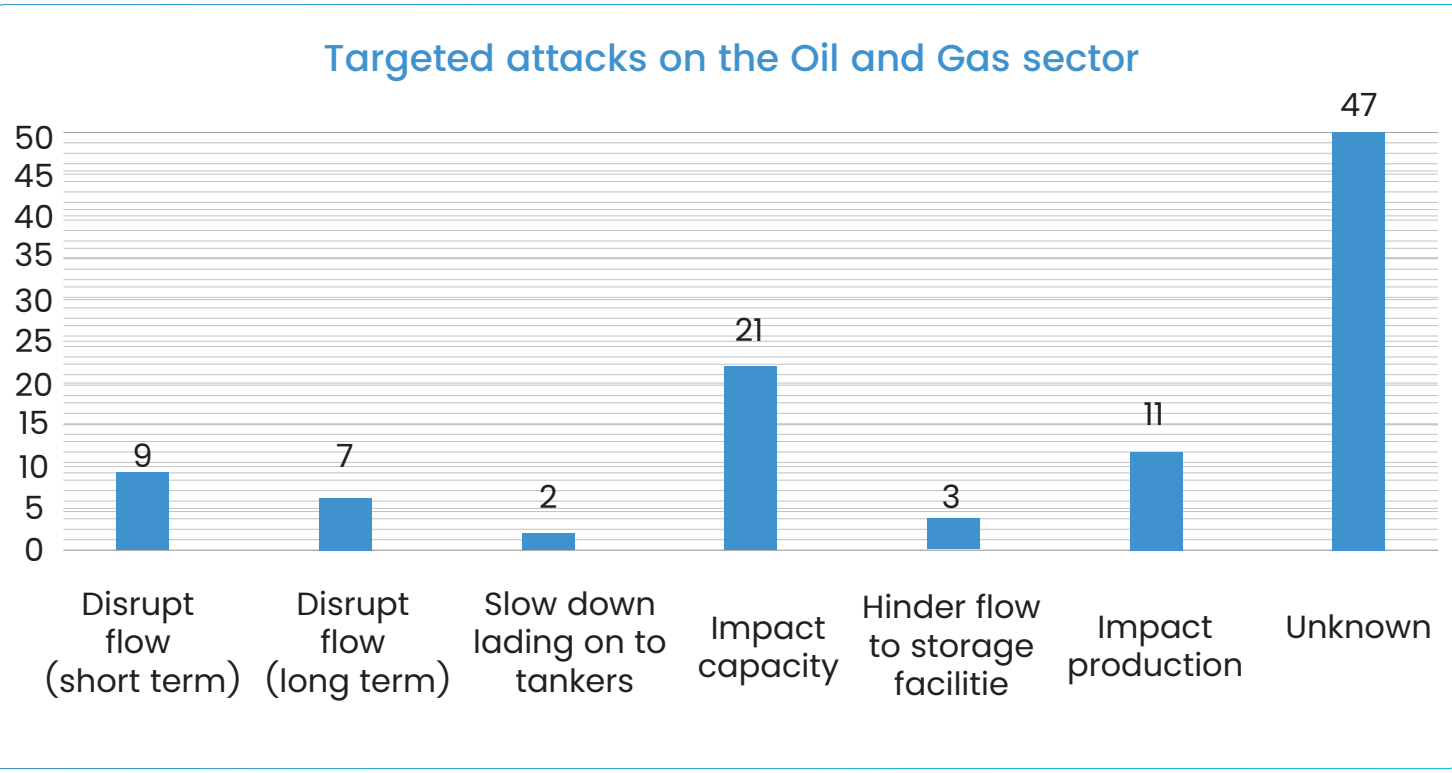
In 2024, a substantial portion of cyberattacks in this domain were directed toward oil transportation infrastructure, with particular focus on

- Subsea and offshore pipeline systems
- Remote sites with significant infrastructure
- Storage terminals and logistics hubs
- Strategic market research
- Refined product distribution networks
- Interconnected OT/ICS environments used in processing and transport

These attacks often aim to degrade capacity utilization, reduce flow efficiency, or cause sustained operational disruption—tactics intended to influence global energy prices and create supply chain instability. Adversaries exploit vulnerabilities in both legacy ICS components and newly introduced IIoT devices, leveraging weak segmentation, outdated firmware, and inadequate real-time monitoring.

The sector's strategic importance makes it a preferred target for supply chain compromise, pre-positioning for future sabotage, and long-term intelligence gathering.

It is possible that some of these attacks are carried out to influence the global oil prices which are often impacted by news related to cyber attacks on oil infrastructure. Even in a situation where the impacted percentage of output is less than one percent of the daily or monthly average production depending on which oil entity is impacted, oil prices can rise or fall. Further since most oil and gas companies are listed on the national stock exchanges, such attacks also impact the bourses as well. Such factors add another dimension and motivation to the attacks on oil companies.



Threat actors are also targeting non-OPEC oil producers

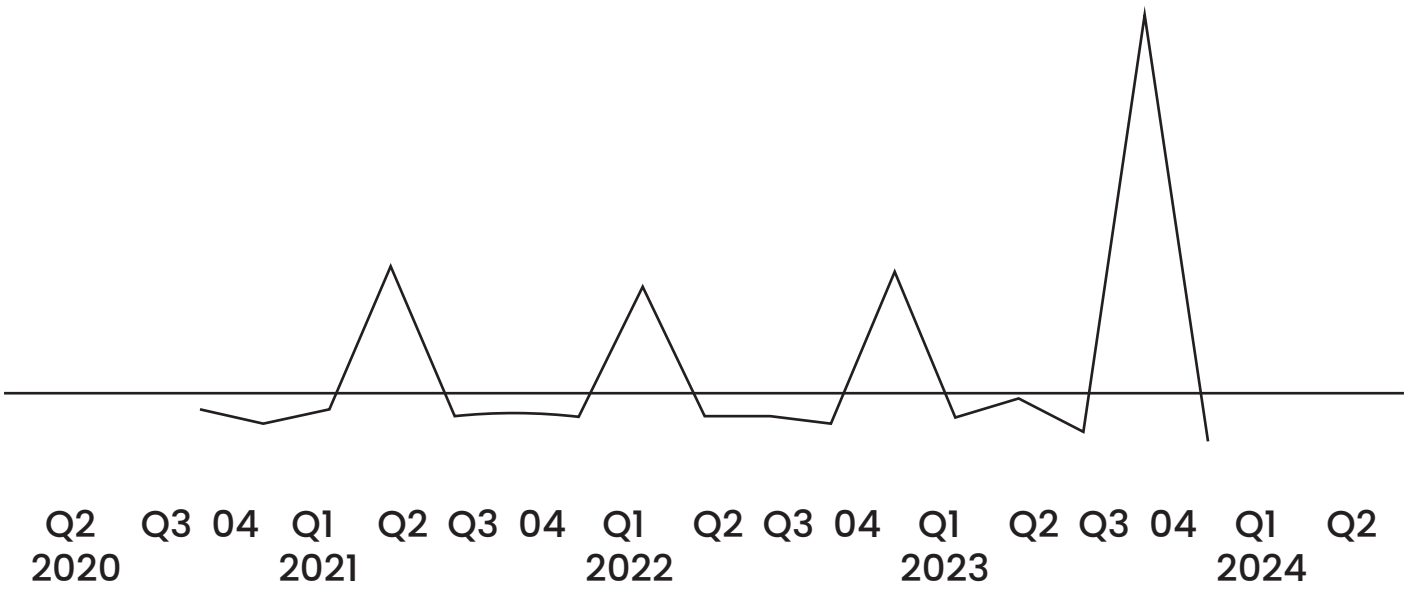
As per a report by US Energy Information Administration, "monthly crude oil prices in 2024 remained between $70/b and $90/b. Sluggish demand and relatively high supply outside of the OPEC+ countries contributed to the relatively narrow trading range for crude oil4". With non-OPEC nations stepping up oil production, the oil output from these nations has served as a stabilizing factor as far as global oil prices are concerned.

Prominent among the non-OPEC+ countries that have been increasing oil output include United States, Canada, Brazil, and Guyana. As the influence of these nations on the global o&g prices increases, the sectoral attacks on the oil and gas companies in these nations is expected to grow significantly. Further, in addition to APT groups, conventional actors and unorganized threat actors, hacktivists are also targeting oil and gas firms across OPEC+ and non-OPEC+ countries as well.

Spear phishing, ransomware, loiterware and supply chain attacks have been used by hackers in the past to steal sensitive information and demand a ransom. In 2025, we expect this trend to continue as oil and gas companies expand their infrastructure. As per GlobalData5 analytics, "despite a 35% decline in mentions of cybersecurity in global oil and gas company filings in Q224 compared to the previous quarter, mentions for the full year will surpass those of 2023 in the next month or two to hit an all-time high". Attacks on oil and gas entities continued for the rest of 2024 as threat actors continued their attacks.

Company filings mentions related to cybersecurity in the global oil & gas industry, Q2 2020 - Q2 2024

- QoQ change



Source: Global Data Company Filings Analytics

In August 2024, a large global O&G company admitted that it's systems have been breached and data exfiltrated. Stolen data from O&G companies also finds ready buyers in the market. Such data can be used to gauge production levels, operational challenges, production forecasts for the upcoming months and any regulatory issues that the O&G company may be facing. Overall, such data helps analyse a company's health which in turn has a bearing on its stock prices and (if big enough) the impact on global O&G prices Such data can be also be priceless for trader who indulge in speculative buying and selling of oil.

Oil companies can also be held for ransom against release of such data.

IEC 62443-based challenges specific to the oil and gas sector

Challenge	Mapped to	Implication
Cybersecurity governance	IEC 62443-2-1	Governance issues often encountered in this sector include lack of clear governance policy around cyber physical system security, lack of clarity on roles and responsibilities and lack of a policy based incident response plan
Risk assessments	IEC 62443-2-1, 3-2	Identification of assets based on security risk and patch status is mostly done on an ad hoc basis. Risk assessments and audits are biased towards IT assets and networks. OT systems are often audited by third-parties that are not fluent in OT systems and their unique cybersecurity needs.
Defining zones and conduits	IEC 62443-3-2	Logical security zones even when created are not backed by appropriate communication conduits.
Supplier and vendor component security	IEC 62443-4-1, 4-2	System vendors and integrators have started following secure lifecycle development processes but legacy systems in place today were not development in compliance with such processes

Attacks logged by target stages crude oil handling and processing stages

Attacks	Target Phases
Data exfiltration	Drilling, refining, transport and distribution
Ransomware	Across operations
Sabotage	Transport and refining, offshore drilling
Listening	Drilling, operations and refining
Payload testing	Drilling, refining, and transport

Top target systems in inbound attacks	Percent
PLCs	15
Generic IT	11
SCADA workstations	13
Firmware	9
Well performance analysis systems	1
Process optimization and control	4
Safety instrumented systems/disable safety	9
Smart pumps	1
Pipeline monitoring	1
Directional drilling guidance system	5
Automated integrated drilling system	6
System state change	4

Cyber physical monitoring systems	6
Production management systems	3
Impair process control	2
Unspecified HMI systems	3
ERP	2
Unknown	5

Hacking kits

Today, there are at least 25 generative AI-powered kits (often referred to as GPT kits) designed to create malware or modify existing malicious code. These kits have significantly lowered the entry barrier for cyber attackers by automating and simplifying complex tasks.

- Sniff network traffic,
- Extract and correlate usernames and passwords from breached databases,
- Scan for open ports,

Some kits even offer "trial-mode cyberattacks", allowing users to simulate a full attack chain:

- Launch non-destructive payloads on target systems,
- Move laterally across network segments, including zones hosting critical infrastructure,
- And finally, withdraw the payload—mimicking real-world cyber reconnaissance without triggering major alarms.

This demonstrates how threat actors can test and refine their attacks with minimal risk, often at very low cost or even free of charge

Beyond AI-driven tools, a variety of basic hacking kits are openly shared on underground forums These include tools to

Hacking kit	Function	Price in USD (2024)
Spyden	Open port crawler	1-3
Xintas	Password match algorithm	1
Anormus	Network stealth level tracker	9
Elephus	Network stealth level tracker	8-16
Access sale	Access to compromised networks	35 (Depends on victim entity)
Gordata	Data sampler	2-10
Composite kit	Most of the above functions	12
Sniffer	Data interception	4

Dark Web ecosystem and the commoditization of cybercrime

The widespread availability of these kits is fuelled by thriving underground ecosystems—forums and marketplaces that facilitate:

- Sale and exchange of malware strains,
- Faster access to complex malware without investing in R&D
- Access credentials to breached systems,
- Zero-day vulnerabilities,
- And as-a-service offerings like ransomware-as-a-service (RaaS) and phishing kits.

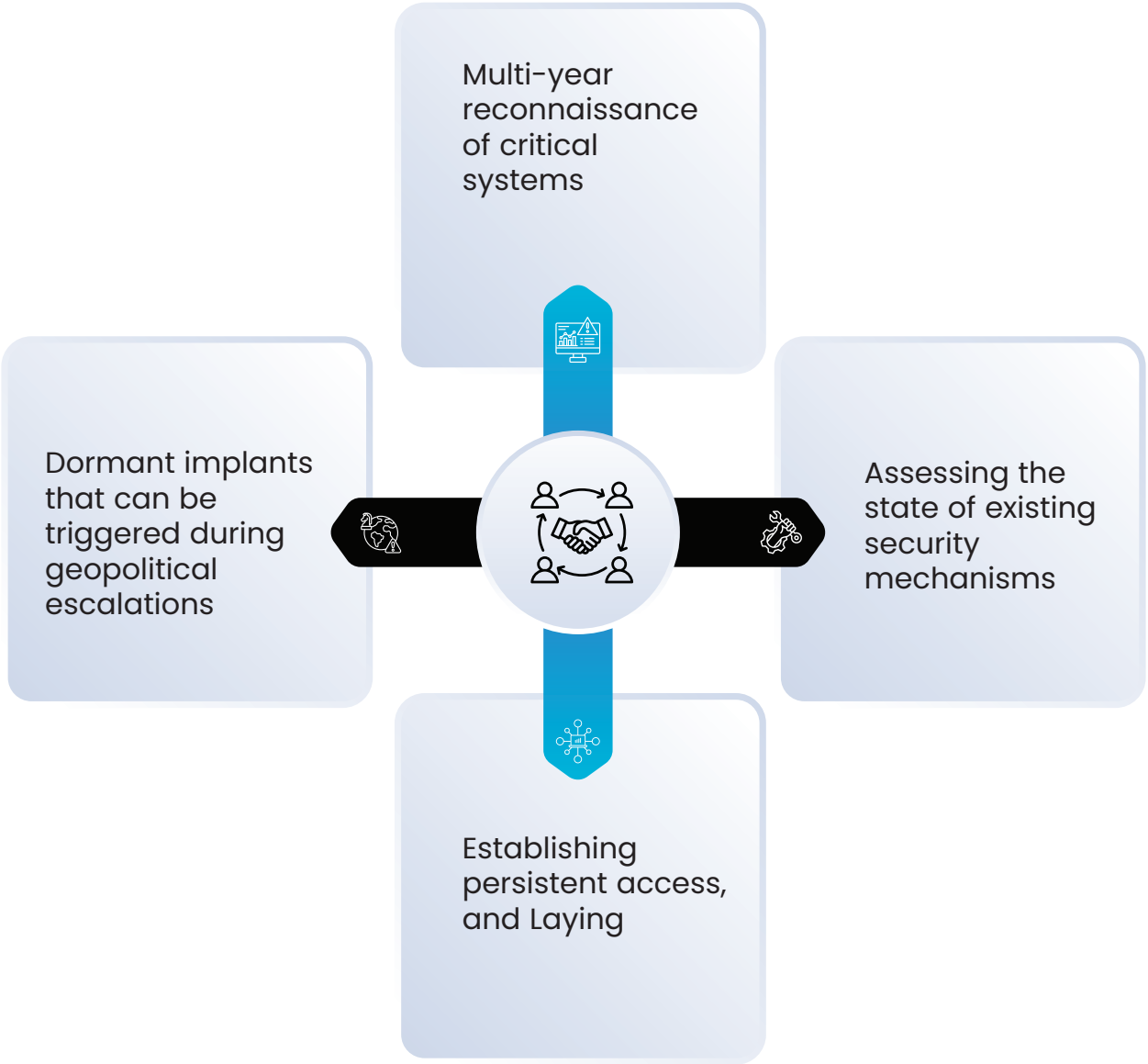
This commoditization of cybercrime has enabled a surge in mass-scale, opportunistic, and targeted attacks across geographies and sectors. The ease of access to such resources means that even low-skill actors can launch sophisticated campaigns, posing a significant challenge to defenders.

Interestingly, not only does Dark Web facilitate attacks on entities, it also serves to connect data buyers with brokers and other interested entities.

Critical infrastructure faces sustained targeting

State-sponsored threat groups—particularly from Russia, China, North Korea, and Iran—are actively conducting coordinated operations against Critical Information Infrastructure (CII) across more than 100 nations. These attacks have increased in frequency, sophistication, and strategic intent over the past four years.

APT (Advanced Persistent Threat) groups associated with these states are engaging in



Sectors under frequent attack include

- Energy (Oil & Gas),
- Utilities,
- Maritime and port operations,
- Transport infrastructure,
- Data centers, and
- Governmental institutions.

These operations are not purely disruptive in nature—they aim to maintain a long-term foothold that can be leveraged for strategic impact during crises, including infrastructure sabotage, data manipulation, and denial-of-service scenarios.

Reconnaissance as a Precursor to Full-Spectrum Attacks

The past two years have seen a marked increase in targeted scanning activity against industrial systems. These scans are designed to extract critical telemetry, such as:

- Network architecture and segmentation flaws,
- Open ports and exposed services,
- Lack of updated asset inventory
- Credential reuse and weak access policies
- Asset identification and traffic baselines,
- And vulnerabilities in protocol handling or device firmware.

Even in the absence of immediate exploitation, sustained scanning introduces latency, strains system resources, and adds operational risk. Furthermore, reconnaissance data can be used in attack simulations to test payload behavior before launching an actual campaign.

Real-World Case Study: Recon to Attack Transition

In November 2024, Shieldworkz threat research team observed a targeted cyberattack on a power plant decoy facility that illustrates the transition from passive reconnaissance to active exploitation.

- The attacker began with automated vulnerability scanning, fingerprinting exposed ICS/IIoT devices.
- Within weeks, three remote code execution (RCE) vulnerabilities were exploited to deploy a stager—a lightweight program designed to establish a C2 channel.
- The payload's beaconing behavior was customized to reduce detection probability, including randomization of intervals and protocol mimicry.

This resulted in:

- Compromise of IIoT endpoints
- Unauthorized access to CCTV infrastructure
- The eventual use of those compromised devices to launch a coordinated nighttime attack on a power sector component manufacturer—likely intended as a distraction or test run for broader disruption.

Major cyber events in 2024

December 2024: Chinese hackers breached a third-party vendor for the U.S. Treasury Department to gain access to over 3,000 unclassified files. The documents related to principles such as Secretary Janet Yellen, Deputy Secretary Wally Adeyemo, and Acting Under Secretary Brad Smith, in addition to the Committee of Foreign Investment in the United States and the Office of Foreign Assets Control.

December 2024: Russian hackers infiltrated a Pakistani hacking group, exploiting their infrastructure to access sensitive information stolen from South Asian government and military targets.

December 2024: Cyberattacks on Indian government entities increased by 138% between 2019 and 2023, rising from 85,797 incidents in 2019 to 204,844 in 2023, according to the Indian Ministry of Electronics and IT.

December 2024: Russian hackers targeted Romania's election systems with over 85,000 cyberattacks and leaked credentials on Russian hacker forums. The attacks came just before Romania's presidential vote, with attacks persisting through election day.

December 2024: Russian hackers launched a phishing campaign targeting Ukrainian armed forces and defense enterprises. The attackers deployed remote access tools to infiltrate military systems and steal credentials from platforms like Telegram and local networks.

December 2024: China's national cybersecurity agency accused a U.S. intelligence agency of conducting cyberattacks on two Chinese tech firms since May 2023, targeting an advanced materials research unit and a high-tech company specializing in intelligent energy and digital information. The attacks reportedly led to the theft of substantial trade secrets, coinciding with heightened U.S.-China tensions over export controls on semiconductors and AI technologies.

November 2024: The United Kingdom's National Cyber Security Center found a three-fold increase in the most significant cyberattacks compared to a year ago. NCSC provided support for 430 cyberattacks, 89 of which were "nationally significant," and listed China, Russia, Iran, and North Korea as "real and enduring threats."

November 2024: Chinese hackers, dubbed Salt Typhoon, breached at least eight U.S. telecommunications providers, as well as telecom providers in more than twenty other countries, as part of a wide-ranging espionage and intelligence collection campaign. Researchers believe the attack began up to two years ago and still infects telecom networks. Attackers stole customer call data and law enforcement surveillance request data and compromised private communications of individuals involved in government or political activity.

November 2024: Chinese spies planted a chip in a former U.S. three-stars general's conference name tag to track his every move during his time serving in the Indo-Pacific.

November 2024: Iranian hackers have been targeting aerospace, defense, and aviation industries in Israel, the UAE, Turkey, India, and Albania, according to Israeli reports. Hackers pose as recruiters on LinkedIn and distribute malware to victims through fake lucrative job offers to spy on targets and steal sensitive data starting in 2023. The malware and tactics are similar to those of a North Korean hacking group that targeted cryptocurrency exchange-traded funds.

December 2024: South Korean officials accused pro-Russian hackers of attacking civilian and government website, following South Korea's decision to monitor North Korean troops in Ukraine. Several pro-Russian hacktivists have claimed the attacks, but no final attribution has been made.

October 2024: Russian agents sent emails about bomb threats to nearly 60 Ukrainian embassies worldwide, as well as media outlets and state agencies.

October 2024: Iranian agents are increasing their espionage efforts against government agencies in the United Arab Emirates. Attackers deployed a backdoor to exfiltrate sensitive credentials

October 2024: Russian cybercriminals sent information-stealing malware to an unknown number of Ukrainian draft-age men to undermine Ukraine's military recruitment efforts.

October 2024: Australia introduced its first national cyber legislation, the Cyber Security Bill 2024. It is the country's first attempt to codify security standards for ransomware reporting and smart devices and proposes a framework for managing the impact of significant cyber incidents.

October 2024: Chinese hackers have breached at least twenty Canadian government networks over the last four years, according to the Canadian Cantre for Cyber Security (CCCS). CCCS reported that the objectives of the breach include espionage, IP theft, malign influence, and translational repression. The statement comes after CCCS revealed a Chinese threat actor was conducting surveillance scans of Canadian parliamentary and political networks.

October 2024: Russian hackers sent compromised emails disguised to appear as if they were sent from Amazon or Microsoft to infiltrate Ukrainian state and military devices and steal credentials from victims. The scope of the campaign is unknown.

October 2024: Chinese hackers hacked cellphones used by senior members of the Trump-Vance presidential campaign, including phones used by former President Donald Trump and JD Vance as well as people affiliated with the Harris-Walz campaign. It is unclear what data may have been accessed. The FBI is investigating the incident.

October 2024: New reporting reveals Chinese-backed hackers have been conducting large data exfiltration operations against Thailand's government institutions. Hackers first gained access in 2023 through a brute force attack on a local area network before gaining privileged access and beginning data exfiltration.

October 2024: Ukrainian hackers attacked Russia's state media company and electronic court document management system on Putin's birthday. The attack prevented Russian courts from filing lawsuits or viewing court hearing schedules for several days, and it interrupted all streaming services of prominent TV and radio stations in Russia.

September 2024: Chinese hackers have been conducting an ongoing cyber espionage campaign against Middle Eastern government entities that published human rights studies related to the Israel-Hamas War. The campaign was discovered in June 2024 after researchers discovered malware implants that were designed to ultimately deliver a malware implant. interrupted all streaming services of prominent TV and radio stations in Russia.

September 2024: Russian cyber spies conducted an espionage campaign against Mongolia's Ministry of Foreign Affairs and Cabinet websites. The spies added malicious code to the websites to exfiltrate a victim's browser cookies. Attackers used the same exploits as those sold by commercial surveillance vendors such as NSO Group and Intellexa, but it is unknown if these companies knowingly sold their exploits to the Russian government, according to reports.

August 2024: U.S. government officials blamed Iranian hackers for breaking into Donald Trump's presidential campaign. Hackers also attempted to break into the then-Biden-Harris campaign, then offered to share the stolen Trump campaign documents with the campaign, but were ignored. The attack comes as U.S. officials raise warnings about potential foreign interference in the upcoming U.S. election from Russia, China, Iran, and North Korea.

August 2024: The United Nations unanimously approved its first treaty on cybercrime. The treaty will face a General Assembly vote in the fall.

August 2024: Russian cyber criminals are deploying malware against diplomats through a used-car email scheme. The attackers embed a file supposedly with images of a used car in their email, but the file contains backdoor malware that established persistent access for attackers to engage in for follow-on data theft, reconnaissance, and surveillance activities.

July 2024: South Korea's military is investigating the leak of highly sensitive information on Seoul's espionage activities and issued an arrest warrant for a suspect. The information included personal data on Seoul's non-official agents conducting undercover espionage overseas. The information was transferred to the suspect's personal laptop before being leaked. Lawmakers said the leak was first discovered in June and was not the result of a hack.

July 2024: A faulty software update for Microsoft Windows issues by cybersecurity firm CrowdStrike caused a global IT outage that disrupted airline and hospital operations. It affected approximately 8.5 million machines and cost Fortune 500 companies $5.4 billion, according to reports.

July 2024: Germany accused China of directing a "serious" cyberattack against Germany's Federal Office for Cartography and Geodesy (BKG), which conducts precision mapping of the entire country, in 2021. The findings come at the end of a three-year investigation into the incident and as Germany plans a rip-and-replace project for Chinese telecommunications infrastructure in Germany over security concerns.

July 2024: Australia, the United States, Canada, the United Kingdom, Germany, Japan, South Korea, and New Zealand issued a warning about malicious Chinese state-sponsored cyber activity in their networks. It marked the first time South Korea and Japan joined with Australia to attribute malicious cyber actions to China, and the first time Australia led a cyber attribution effort against China.

June 2024: Japan's space agency has suffered a series of cyberattacks since last year, according to the Japanese government. Japan's Chief Cabinet Secretary claimed the targeted networks did not contain sensitive rocket or satellite information, and that the attackers were "from outside of Japan."

June 2024: Hackers deployed ransomware in Indonesia's national data center which briefly disrupted a variety of immigration services, including immigration document management services at airports, and deleted information that was not backed up. The attack prompted Indonesia's Director General of Informatics Applications at the Communications and Informatics Ministry to resign and initiated and a nation-wide audit of Indonesia's national data centers.

June 2024: Belarusian state-sponsored hackers launched an espionage campaign Ukraine's Ministry of Defense and a Ukrainian military base. The attackers sent targets phishing emails with drone image files a malicious Microsoft Excel spreadsheet.

June 2024: Germany's main opposition party, the Christian Democratic Union, suffered a cyberattack just ahead of European Parliamentary elections. Germany's interior ministry did not disclose the extend of the attack or the suspected perpetrator, but acknowledged it was "serious." The attack occurred shortly after Germany's Social Democratic party was attacked by Russian hackers. The party briefly took down parts of its IT service as a precaution.

June 2024: The government of Palau accused Chinese hackers of stealing over 20,000 government documents shortly after the island nation signed a 20-year economic and security deal with the United States in March 2024. Palau's president said this was the first major attack on government records that the island has seen.

May 2024: A new report from Canada's Communications Security Establishment detected Chinese espionage activity against eight members of Parliament and one senator starting in 2021. The spies likely attempted to obtain information from the targets' personal and work devices but were unsuccessful, according to the report. The Parliamentarians were members of Canada's Inter-Parliamentary Alliance on China, which focuses on how democracies should approach PRC-related issues. The report also mentioned this activity was similar to activity against 19 European countries dating back to 2020.

May 2024: Recent media reports stated Pakistani cyber spies deployed malware against India's government, aerospace, and defense sectors. The group sent phishing emails masquerading as Indian defense officials to infect their targets' devices and access sensitive information. The attack's extent is unknown.

May 2024: Chinese hackers hit Britain's Ministry of Defense with a cyberattack that exposed sensitive information on every troop apart from the UK's special forces. The attackers targeted a third-party contractor to access names and bank details of current and former members of the armed forces. The UK Minister of Defence stopped short of publicly naming China as the culprit.

May 2024: Poland and the Czech Republic accused Russian cyber spies of targeting government and infrastructure networks. Both countries claim the attacks occurred around the same time Russian hackers attacked the German government. Hackers gained access by exploited a Microsoft Outlook vulnerability, and the extent of the compromised data is currently unknown.

May 2024: Germany accused Russian hackers of breaking into the emails of Germany's Social Democrats, the leading party in its governing coalition, and recalled its ambassador from the country. The campaign started in March 2022 when hackers exploited vulnerabilities in Microsoft Outlook to target the party's executive committee, as well as German defense and aerospace companies.

April 2024: Ukraine's military intelligence agency launch a cyberattack against Russia's ruling United Russia party the same day Russia hosted its Victory Dictation. Attackers launched a barrage of DDoS attacks against United Russia's servers, websites, and domains to make them inaccessible. United Russia publicly admitted to suffering from a "massive" DDoS attack.

April 2024: Belarusian pro-democracy hackers, known as the Belarusian Cyber-Partisans, crippled the website of Belarus' main security service agency for over two months. The hackers also published a list of website administrators, its database, and server logs on its Telegram channel. This is the latest in a series of attacks against the Belarusian government by the group.

April 2024: Police in the United Kingdom are investigating a series of "honey trap" attacks against British MPs. Attackers sent explicit messages allegedly of themselves over WhatsApp to their target for the apparent purpose of acquiring compromising images of the target. The perpetrators of these attacks are currently unknown.

April 2024: Germany plans to create a cyber military branch as part of its military restructuring. Germany's defense minister, Boris Pistorius, stated the new Cyber and Information Domain Service (CIR) would help deter increasing cyber aggression from Russia against Germany and its NATO allies.

April 2024: Hackers attacked El Salvador's national cryptocurrency wallet Chivo and exposed over 144 GB of sensitive personal information of millions of Salvadorians. The hackers also released Chivo's source code publicly. The Salvadorian government has not released an official public statement on the attack.

March 2024: A "massive" cyberattack disrupted the African Union's systems for over a week and infected over 200 user devices, according to the deputy chair of the AU Commission. The cause of the cyberattack is unknown.

March 2024: Iranian hackers compromised an IT network connected to an Israeli nuclear facility. Hackers leaked sensitive facility documents but did not compromise its operational technology network.

March 2024: Russian hackers launched phishing attacks against German political parties. Hackers concealed ransomware in a fake dinner invitation from Germany's Christian Democratic Union to install a backdoor in their victim's computer.

March 2024: India's government and energy sectors was breached in a cyber espionage campaign. Hackers sent a malicious file disguised as a letter from India's Royal Air Force to offices responsible for India's electronic communications, IT governance, and national defense. Researchers have not yet determined who conducted the attack.

March 2024: A U.S. Department of Justice indictment revealed Chinese hackers targeted several EU members of the Inter-Parliamentary Alliance on China and Italian MPs. The attack was designed to detect IP addresses and the targets' locations.

March 2024: Canada pulled its financial intelligence system FINTRAC offline after a "cyber incident" by a currently unidentified attacker. FINTRAC claims the attack does not involve its intelligence or classified systems but declined to disclose further details of the incident.

March 2024: Russian hackers leaked an intercepted conversation between German military officials about the country's support for Ukraine. In the call, the head of Germany's Air Force discussed the possibility of supplying Taurus missiles to Ukraine and commented on German Chancellor Olaf Scholz's hesitance to send the missiles. Germany announced it would investigate the incident and believes the leak was intended to inflame divisions in Germany.

March 2024: Switzerland's National Cyber Security Centre (NCSC) confirmed that leaded data from a May 2023 breach included 65,000 documents from the Federal Administration. The documents contained sensitive personal data, classified information, and passwords, and were from Switzerland's federal police, judiciary, and migration offices. Swiss officials had originally assessed that breach only impacted non-government documents.

March 2024: Microsoft claims Russian hackers stole its source code and are continuing to gain unauthorized access to its internal systems as part of their November 2023 campaign to spy on senior Microsoft executives. Microsoft also said attackers increased the volume of their "password spray" attacks by nearly tenfold between January and February 2024. The company did not disclose further details on the source code access or breached internal systems.

February 2024: Russian hackers launched an espionage campaign against the embassies of Georgia, Poland, Ukraine, and Iran beginning in 2023. Hackers exploited a bug in a webmail server to inject malware into servers at the embassies and collect information on European and Iranian political and military activities.

February 2024: Roughly 190 megabytes of data from a Chinese cybersecurity company were exposed online, revealing the company's espionage efforts on the governments of the United Kingdom, India, Indonesia, and Taiwan. The leak's source is unknown.

February 2024: The Royal Canadian Mounted Police suffered a cyberattack against its networks. The RCMP stated it is investigating this "alarming" incident and does not believe it had an impact on its operations or the safety and security of Canadians. It is so far unclear who is behind the attack and if it was a data breach or security incident.

February 2024: U.S. officials hacked an Iranian military spy ship that was sharing intelligence with Houthi rebels who have been firing on ships in the Red Sea. According to U.S. officials, the attack was part of the Biden administration's response to an Iranian drone stroke that killed three U.S. soldiers in Jordan.

February 2024: A data breach of French health insurance companies in January 2024 affected 33 million French citizens, or nearly half the country's population. The attack compromised sensitive birth date, social security, and marital status information, but not medical history. The French data protection agency opened an investigation to determine if the companies complied with cybersecurity guidelines under the EU's General Data Protection Regulations.

February 2024: Chinese spies places malware in a Dutch military network in 2023. The network was not connected to the defense ministry's main network, which reduced damage. This is the first time the Netherlands has publicly accused China of cyber espionage.

January 2024: Hackers breached Global Affairs Canada's secure VPN in December 2023, allowing hackers to access sensitive personal information of users and employees. It affected staff emails, calendars, and contacts. It's unclear if classified information was compromised or lost. The hacker's identity is currently unknown.

January 2024: Russian hackers launched a ransomware attack against Sweden's only digital service provider for government services. The attack affected operations for 120 government offices and came as Sweden prepared to join NATO. Sweden expects disruptions to continue for several weeks.

January 2024: Microsoft announced that Russian hackers broke into its corporate systems. Hackers used a "password spray attack" to steal emails and documents from accounts of Microsoft's senior leadership, cybersecurity, and legal teams back in November 2023.

January 2024: Russian hackers attacked 65 Australian government departments and agencies and stole 2.5 million documents in Australia's largest government cyberattack Hackers infiltrated an Australian law firm that worked with the government to gain access to government files.

January 2024: The Australian government identified and sanctioned Aleksandr Ermakov as the Russian hacker who breached Medibank, the country's largest private health insurance provider, in 2022. He stole information from 9.7 million current and former Medibank customers. This is the first time Australia has issued cyber sanctions against an individual since the framework was established in 2021. The U.S. and UK also sanctioned Ermakov.

January 2024: Russian agents hacked residential webcams in Kyiv to gather information on the city's air defense systems before launching a missile attack on Kyiv. Hackers changed the cameras' angles to gather information on nearby critical infrastructure facilities and stream the footage on YouTube. Ukraine has since ordered webcam operators in the country to stop live broadcasts.

Global APT activity in 2024

In 2023, nearly all Advanced Persistent Threat (APT) groups tracked by our threat intelligence teams exhibited heightened operational activity. This surge was closely correlated with a series of geopolitical flashpoints and conflicts, which significantly intensified the threat landscape in cyberspace.

APT actors associated with Iran, North Korea, China, and Russia conducted a broad spectrum of cyber operations, ranging from targeted espionage and surveillance to disruption and sabotage. These campaigns were directed not only at Critical Information Infrastructure (CII) but also at non-critical sectors, including manufacturing, logistics, and financial services—indicating a strategy aimed at destabilization, coercion, and strategic advantage

Chinese APTs

To understand the operations of Chinese APT groups, it is essential to understand the workings of the Chinese Ministry of State Security. The PRC's Ministry of State Security (MSS) is the mother ship for almost all APT groups operating from China.

The Ministry of State Security (MSS) and its affiliated state security bureaus have actively pursued covert cyber and human intelligence operations to collect a wide array of sensitive information—primarily targeting political, economic, military, and technological domains that could impact the strategic interests of the People's Republic of China (PRC).

Can the MSS be seen as just a controlling government agency? The answer is no, In addition to being the controlling agency for all cyber espionage operations in China, the MSS is also involved in almost every aspect of inter APT coordination including assigning timelines for various espionage projects. The MSS also ensures the most efficient use of mission bandwidth while preventing duplication of work. In addition to getting espionage targets from the Chinese leadership, the MSS also gets work allocated from other wings of the Chinese government as well.

In addition, the MSS is known to align with the military and industrial goals of China while being responsible for the success of China's espionage and corporate spying initiatives.

In the past at least of one instance, the MSS had also published a training calendar for various APT groups operating under its umbrella. Going by its past success, we have no reason to believe the enormous power and responsibility that the MSS enjoys will not change any time soon. The MSS is listed in all internal propaganda of the CCP as an "irreplaceable arm" of the Chinese government.

Key operational objectives

Exfiltration of intelligence related to foreign policy, particularly from nations such as the United States, to shape or anticipate diplomatic stances unfavourable to the PRC. Surveillance and influence operations targeting politicians, analysts, and institutions perceived as critical of PRC policies, often through a combination of cyber-enabled espionage and disinformation campaigns.

Acquisition of proprietary scientific and technical data, especially intellectual property that could offer competitive or economic advantage to PRC-based state-owned and private enterprises.

These activities often blend cyber intrusion, human intelligence (HUMINT), and psychological operations (PSYOP) as part of a coordinated strategy to support economic espionage, policy manipulation, and long-term geopolitical positioning.

China's strategic espionage doesn't distinguish between adversaries and friendly nations. Its APT groups keep track of and spy on many nations and entities that are considered allies by the Chinese g overnment. In addition, groups like APT 41 spy on other countries using the infrastructure of ally nations. Such extensive use of SIGINT is unprecedented and when seen in the light of advances made in AI, is certainly a matter of concern.

Key tactics

Among all the threat actors originating from China, APT 41 is easily among the most sophisticated ones. APT 41 is known to blend and modify its threat activities and TTPs extensively as per the needs of the environment or potential victim being targeted. APT 41 has a huge appetite for data with geopolitical and\or economic undertones.

APT 41 is often known to exfiltrate data across targets and then hand them over to fellow APT groups for analysis and refining. That said, APT 41 is also known to run a large scale data refining facility of its own consisting of co-opted cloud infrastructure from private sector entities in China. The private sector entities do not have a choice when it comes to saying no to the MSS. Entities that say no or do not meet data refinement targets are served penalties and their licenses cancelled.

APT Group	Scans	Supply chain	VPN	Watering hole	Data theft	Data sale
APT41	Yes	Yes	No	Yes	Yes	No
APT22	Yes	Yes	Yes	Unknown	Yes	Yes (Internal)
APT10	Yes	Yes	Yes	Yes	Yes	Yes
APT18	Yes	Yes	No	No	Yes	Yes
APT27	Yes	Yes	Yes	Yes	Yes	Yes

Country focused campaigns

Since 2022, China's APT 41 has been running country focused campaigns targeting critical infrastructure. In one such campaign, APT 41 targeted the power grid infrastructure in India. The fact that this campaign is not bound by time brings another level of complexity to the fore.

Indian power grid infrastructure was breached in 2020 and 2023 as part of the same campaign. The sub-group of APT 41 responsible for this campaign is known to run multi-year reconnaissance cycles targeting the same infrastructure. Such campaigns involve thedeployment of a malicious payload that sits undetected in the victim's network till an order is released to create havoc in the network andsystems it is linked with.

APT 41 is certainly showing a significant appetite for targeting critical infrastructure. Such an approach is inspired by a tactical blackout campaign run by Russian threat actor Sandworm targeting Ukraine last decade. The focus in on maintaining access to the breached infrastructure for the longest period of time while retaining the ability to strike during a period of geopolitical tension or during an unrelated event.

The APT 41 subgroup will certainly seek to create more disruption in the future through a subsequent attack.

APT 41 which includes many sub-threat actors operating with similar TTPs is the frontline threat actor linked to the Chinese Ministry of State Security (MSS). With offensive and deceptive capabilities, APT 41 operates under the specific instructions of the MSS and maintains a higher degree of links with it. APT 41's mandate includes targeting civilian and military infrastructure in countries across the Indo-Pacific. APT 41 also carries out extensive reconnaissance and listening operations to locate communications and assets of interest.

Shieldworkz has isolated IOCs connected with APT 41 from across Japan, the USA, India, Germany, Estonia, Norway, Sweden, the UK, UAE, Malaysia, Singapore, and South Korea. Unlike APT 17 which is another group operating with a higher degree of interaction with the MSS, APT 41 is more active throughout the year and hoards data including confidential information. APT 17 is a feeder threat actor and more of a launchpad for testing new trainees and works closely with other MSS threat actors on a project-to-project basis. APT 41 enjoys a higher level of autonomy in operations but not in the selection of targets which is decided by the MSS.

The repeated attacks on power grids in India (see box) are a case study of Chinese threat actors trying to attain multiple geo-political objectives through a single axis of attack. The targets have been chosen carefully not just to deliver a message but also to showcase the capabilities of Chinese threat actors. The pattern of attacks and the level of disruption targeted also points to a degree of desperation in MSS to push a certain geopolitical agenda within a short time.

"It is also clear that China's MSS is not worried about the repercussions of weaponizing cyberspace. If the MSS was concerned about a potential fallout of its activities, it wouldn't have pursued cyberattacks at such scales in such a brazen manner."

Both APT 41 and 17 connect to a shell technology company Lixia district of Jinan province in China. The local agency here is believed to be known as the Jinan Bureau. APT 41 ran 21 known campaigns this year targeting entities in the countries mentioned earlier. Unlike the hit-and-run operations run by other Chinese APT groups, APT 41 maintained a higher degree of loiter time sometimes waiting for nearly 39 days before exfiltrating data from a target in Japan.

APT 41 has multiple listening stations across China that tap into communications originating from its targets. In 2023, many of its campaigns were focused on deploying payloads on networks connected with ports, power grids, railway networks and defense infrastructure. Power grids are among the most favored targets of the group with evidence coming in from as many as 9 countries.

The connection with the Belt and Road project

While the other APT groups operating under MSS maintain a relatively low profile and footprint, we have reasons to believe that some of them are tasked with maintaining a vigil on countries that are part of the China-led Belt and Road (BRI) project. China retains a very high level of interest in learning how the BRI project is being perceived in the countries that have opted for it. Thus, such countries are surveilled to a very high extent with GBs of strategic intelligence being transferred through digital espionage every year.

Sometimes, the MSS pits threat actors against each other by asking one group to validate the findings of the other independently. This double-blind exercise ensures the collection of high-value data that feeds into the diplomatic maneuvers that the Chinese government undertakes. In the case of the BRI, in addition to monitoring political sentiments, Chinese APT groups also target data gathered by the intelligence agencies belonging to these states by targeting loose ends. For instance, in the case of a South East Asian country, a Chinese threat actor accessed embassy communications belonging to the target nation. The embassy located in a European nation was preparing for a media briefing by a high-ranked government official and was exchanging classified material via regular emails.

There are also instances of Chinese APT groups working together to steal feeds from military infrastructure in friendly nations. APT 22 is known to vacuum TBs of data from defense facilities belonging to close allies (one in South Asia and the other in Africa). It is not known whether the nations involved are aware of this espionage. But it is certainly clear that MSS relies heavily on exfiltrated data much more than Humint or what it is told by government officials.

"We can say with a very high degree of confidence that China is retaining a very high level of surveillance interest in BRI countries."

Documented APT 41 activity in 2023

APT Group	Scan instances	Data exfiltration attempts	Communication monitoring	Spam messaging
North America	11,453	3400	1392	103
South America	7843	932	465	18
Africa	13999	1033	102	10
Europe	23384	14011	6453	99
Asia	77098	39001	11452	177
Australia	9777	1090	79	11

Russian APT groups - pushing the frontiers

APT 29 is one of the frontline Russian APT groups. Also known as 'Cozy Bear', this group is known to go after high-value targets such as the US government and Fortune 500 businesses around the world. This group is known to retain a very high level of situational awareness about the unique security and operational features of its target networks. This group also masks traffic using routers to obfuscate origin and to evade IP-based traffic filters. APT 29 is just one of the many threat actors that are run by Russia.

In terms of tactics, targets, and quality of attacks, Russian APT actors display a remarkable level of maturity. Russian APTs are among the most experienced threat actors in the world. They operate at diplomatic, military, industrial, political, and economic levels. The same actor may engage a target at all these levels. Data exfiltration is a baseline motive.

All Russian APT actors work to support Russian state security policy objectives. Because of a lack of support from local cloud service providers, Russian APT groups are not able to scale their data crunching operations which leads to plenty of exfiltrated data being wasted. This is quite unlike their Chinese counterparts where every KB of exfiltrated data is sorted and analyzed.

This is also why Russian APT groups run very targeted campaigns as they do not want to collect data that they are not interested in. When it comes to targets, Russian APT groups are more focused on critical infrastructure, media, diplomatic communication, research bodies, and global leaders. APT 29 is the most sophisticated actor in Russia and uses techniques such as API manipulation, token theft, password spray, long-term reconnaissance, and employee targeting to gain access to data of interest.

APT 29 was behind the Solar Winds attack. The group has also been known to exploit CVE-2021-34523 and CVE-2021-34473. Since March 2023, this group has been targeting senior NATO officials and Members of the European Parliament through a long-drawn campaign. The group also ran campaigns themed on Think Tank jobs, used automobiles, and conflict updates. These campaigns were used to target high-value targets by luring susceptible individuals to download malware.

In addition to supporting state and diplomacy aims, Russian APT groups also indulge in economic espionage and are known to have links with independent hacker groups like Lockbit. These links are only leveraged for specific projects involving attacks on government agencies such as those in Canada and US.

Strategic Cyber Espionage Across the Indo-Pacific and Beyond

APT 41 is a highly sophisticated Chinese state-sponsored threat group known for its dual mandate: supporting both civilian and military intelligence objectives. Operating under the broader direction of China's Ministry of State Security (MSS), the group has conducted wide-ranging cyber operations across the Indo-Pacific and beyond, targeting critical infrastructure and strategically important assets.

APT 41 engages in extensive reconnaissance, intelligence gathering, and prolonged listening campaigns to identify and monitor high-value communications and digital assets. Unlike many other Chinese threat groups, APT 41 is characterized by its persistence, operational flexibility, and data hoarding tendencies, often maintaining a long-term presence within victim networks before executing data exfiltration.

Global Reach and Indicators of Compromise (IOCs)

Our researchers have identified IOCs linked to APT 41 from operations in multiple countries, including the United States, Japan, India, Germany, Estonia, Norway, Sweden, the United Kingdom, the United Arab Emirates, Malaysia, Singapore, and South Korea. The group's campaigns are notable for their geographical spread, strategic targeting, and continuity throughout the year.

APT 41 vs. APT 17: Operational Differences

APT 41 is often contrasted with APT 17, another MSS-affiliated group. APT 17 functions more as a feeder or training platform for emerging operators, typically engaging in shorter-term projects in coordination with other MSS entities. APT 41, by comparison, operates with greater autonomy in terms of tactics and execution, though its strategic targeting remains under the direct influence of the MSS. This semi-independent model allows APT 41 to maintain a sustained and methodical approach to long-term intelligence objectives.

Being posted in APT 41 is considered as a major career advancement and APT 41 agents often get to work on complex projects, are compensated well and get to serve for longer periods well past their retirement as consultants to other threat groups.

Indian Power Grid Attacks: A Case Study in Strategic Disruption

A series of attacks on Indian power grids exemplifies how Chinese cyber operations serve multiple geopolitical objectives through a single axis of attack. These incidents were not only designed to demonstrate capabilities and signal intent but also aimed to disrupt critical infrastructure in ways that align with China's broader regional strategy. Through these attacks, the Chinese establishment is also sending a clear geo-strategic message to other nations in the region.

The targeted nature and timing of these attacks suggest an urgent push by the MSS to meet specific geopolitical goals, potentially indicating internal pressures within the Chinese intelligence apparatus

Command Infrastructure and Operational Behaviour

Both APT 41 and APT 17 are linked to a shell technology company based in the Lixia district of Jinan, Shandong Province. This company is believed to serve as a front for the local MSS unit, known as the Jinan Bureau. In 2024 alone, APT 41 is confirmed to have launched at least 61 cyber campaigns across its targeted geographies.

A distinctive aspect of APT 41's operations is its use of extended loiter times. In one documented case, the group remained inside a Vietnamese network for 39 days before initiating data exfiltration, demonstrating a patient and deliberate operational tempo uncommon among many Chinese APTs, which often employ hit-and-run tactics.

Focus on Critical Infrastructure

APT 41 has established multiple listening posts within China and among its projects in other nations to intercept and analyze communications from its targets.

In 2024, many of its campaigns focused on embedding malware and payloads in networks linked to ports, power grids, railway systems, and defense infrastructure. Power grids, in particular, have emerged as a priority target, with documented incidents at least nine countries.

The connection with China's strategic ambitions in APAC and beyond

As a major tool in the hands of China's leadership, APT 41 is essentially a Swiss Army knife in terms of its utility. In addition to managing a strategic presence in networks across allies and adversaries alike, APT 41 is enabling the promotion of strategic Chinese government goals around the world.

Russian APT Groups: Expanding the Boundaries of State-Sponsored Cyber Operations

Russian Advanced Persistent Threat (APT) groups remain at the forefront of global cyber-espionage activity, characterized by highly targeted, sophisticated, and state-aligned operations. Among them, APT 29, also known as Cozy Bear, stands out as a premier threat actor. This group has consistently targeted high-value entities such as U.S. government agencies, Fortune 500 companies, global diplomatic institutions, and critical infrastructure operators.

APT 29 is notable for its exceptional situational awareness of the operational and security nuances of its target environments. It routinely leverages anonymization techniques, such as router chaining and traffic masking, to evade detection and bypass IP-based filtering systems. The group's operations are emblematic of Russia's broader cyber doctrine, which emphasizes stealth, persistence, and strategic intelligence collection. Strategic Objectives and Campaign Characteristics

Russian APT actors, including APT 28 (Fancy Bear), Turla, and Sandworm, function as key instruments of state power. Their objectives span diplomatic, military, industrial, political, and economic domains, often blurring the lines between espionage, influence operations, and sabotage. A single group may conduct campaigns across multiple domains simultaneously, with data exfiltration serving as a foundational goal.

Unlike their Chinese counterparts—who focus on mass data collection and analytical exploitation—Russian APTs are selective and surgical in their approach. Due to limited support from domestic cloud service infrastructure, Russian actors face challenges in storing and processing large volumes of stolen data. As a result, they prefer highly targeted operations, aimed at extracting only data of strategic value.

Russian APT groups commonly target

- Critical infrastructure sectors (energy, defense, transportation)
- Think tanks
- Media and information outlets
- Diplomatic channels and government communication platforms
- Research institutions and think tanks
- High-ranking political and military officials

APT 29 is widely regarded as Russia's most technically sophisticated cyber actor. It employs advanced techniques such as

- API manipulation and token theft
- Password spraying and brute-force attacks
- Persistent reconnaissance and employee profiling
- Use of legitimate cloud platforms and social engineering lures

The group was responsible for the SolarWinds supply chain compromise, one of the most significant cyber-espionage campaigns in recent history. It has also exploited vulnerabilities such as CVE-2021-34523 and CVE-2021-34473, enabling it to bypass authentication controls in Microsoft Exchange environments.

Since June 2024, APT 29 has been engaged in a prolonged targeting campaign against senior NATO officials and Members of the European Parliament. These operations have featured cleverly themed phishing lures—such as fake job listings at think tanks, updates on the Russia-Ukraine conflict, and classified automobile sales—to entice high-value individuals into downloading malware-laden documents or visiting malicious sites.

Beyond formal state operations, Russian APT groups have demonstrated tactical coordination with independent cybercriminal entities, including ransomware groups like Lockbit. These collaborations are typically opportunistic and project-based, particularly for missions targeting Western government agencies in Canada, the U.S., and Europe. While Russian APTs operate under strict state control, this cooperation provides them with extended reach, alternative capabilities, and plausible deniability.

Once inside target networks, the group is known to wipe out all signs of its presence in a meticulous manner.

Industrial Control System (ICS) Cyberattacks Attributed to Russian APT Groups

The emergence of sophisticated malware targeting Industrial Control Systems (ICS) poses a significant threat to critical infrastructure. Notably, the CosmicEnergy malware, exhibiting advanced capabilities, has been identified targeting systems associated with power generation and distribution entities across Europe and other regions. This malware is attributed to threat actors with established links to at least two Russian Advanced Persistent Threat (APT) groups, including APT 29.

CosmicEnergy's design deviates from conventional malware, focusing on the potential for large-scale disruptions capable of causing national or regional grid failures. This represents an evolution in Russian cyber warfare tactics, emphasizing the development of sector-specific and outcome-oriented malware. While generic malware remains a concern, the trend indicates an increasing prevalence of tailored malware designed for specific industrial sectors and operational objectives.

North Korean Advanced Persistent Threat Activity

North Korean threat actors demonstrate persistent and adaptable capabilities across diverse incident types and targeted sectors. A notable development is the documented attempt by a North Korean threat actor to engage with threat analysts and researchers via fabricated social media profiles, a tactic distinct from those employed by Chinese, Iranian, and Russian APT groups.

The primary objective of North Korean APT groups, particularly APT 38, is to generate revenue in hard currency. Research indicates the presence of multiple subgroups, potentially seven, operating under the umbrella of APT 38.

APT 38 and the Reconnaissance General Bureau (RGB)

APT 38 is subordinate to the 110th Research Center, 3rd Bureau of the Reconnaissance General Bureau (RGB). The Third Bureau's mandate encompasses technical surveillance and comprehensive cyber operations, including data exfiltration, persistent surveillance, and targeted harassment of individuals critical of the North Korean government.

The RGB serves as the central agency for malicious cyber activities within North Korea. Its operations extend beyond cyber warfare, encompassing support for other government initiatives such as arms trafficking, currency smuggling, agent infiltration into South Korea, disinformation campaigns, and commodity trading.

APT 37 and the Ministry of State Security

The Ministry of State Security operates APT 37, a strategically oriented threat actor with objectives aligned with the directives of its parent organization, reporting directly to Kim Jong Un. This group utilizes tools such as SlowDrift, Blue Whistle, and M2RAT. APT 37 is characterized by its long-term reconnaissance capabilities, employing advanced obfuscation techniques. Its arsenal includes zero-day exploit capabilities and highly effective spear-phishing campaigns.

Operational Scope and Impact

In 2023, Shieldworkz observed the global footprint of both APT 37 and APT 38. APT 37 targeted embassies, oil companies, defense contractors, defectors, and government entities, while APT 38 focused on financial institutions (banks and stock exchanges), NGOs, and enterprises.

Enterprises face a heightened risk from North Korean APT groups due to their broad operational objectives. This expansive targeting scope renders virtually any business a potential target.

Combined, APT 37 and 38 account for a substantial proportion of global malicious cyber activity. These groups exhibit advanced capabilities in executing year-round scams.

Analysis of Advanced Persistent Threat Activities: North Korean and Iranian Groups

North Korean APT Activity: Escalated Campaigns and Targeted Exfiltration

During June and July 2023, North Korean Advanced Persistent Threat (APT) groups, specifically APT 37 and APT 38, exhibited a notable escalation in their global campaigns, focusing on the exfiltration of sensitive documents and information from numerous Asian and European nations. This surge in activity targeted critical sectors, including research institutions, strategic think tanks, and enterprises with affiliations to nuclear power generation facilities. These campaigns demonstrate a strategic focus on acquiring data related to advanced technologies and critical infrastructure.

Furthermore, North Korean APT groups have consistently engaged in targeted cyber operations against media outlets, government officials, and influential entities that express dissent against the North Korean regime. This activity highlights the dual-purpose nature of these groups, combining economic espionage with political objectives.

Iranian APT Activity: Evolved Threat Landscape and Strategic Targeting

While the operational footprint of Iranian APT actors may appear less extensive compared to their Chinese, Russian, and North Korean counterparts, their capabilities and persistence are significant. APT 35 (aka "Magic Hound") and APT 34 (aka "OilRig") are prominent actors within the Iranian cyber threat landscape. Their targeting focus encompasses critical sectors such as aviation, oil and gas, financial services, manufacturing, critical infrastructure, and aerospace. This selection of targets suggests a strategic imperative to bolster Iran's domestic technological capabilities and enhance its competitive standing in key industries, particularly in the oil and gas sector.

Beyond these core sectors, Iranian APT groups have demonstrated an expanded targeting scope, including financial services and healthcare. However, these sectors are not prioritized to the same degree. In the manufacturing sector, these groups exhibit a pronounced interest in intellectual property related to industrial processes, raw material inputs, and automation technologies.

Although Iranian APT groups represent a smaller fraction of the overall APT threat landscape, their activity levels have experienced a substantial increase since 2021. Initially, around April 2013, their operations were confined to a limited number of countries. However, their operational reach has expanded globally across diverse sectors.

These groups are capable of launching high-volume attacks against targeted entities within compressed timeframes. Notably, in November 2023, a 900% surge in Iranian APT activity was observed across the Middle East within a 21-day window (November 4 to November 25). This spike suggests a correlation with concurrent geopolitical events in the region, underscoring the opportunistic nature of Iranian cyber operations.

Technical Tactics and Operational Persistence

Iranian APT groups frequently employ watering hole attacks as a primary intrusion vector, minimizing the need for direct exploitation. This tactic allows for stealthy compromise of target networks through infected websites frequented by intended victims.

These groups demonstrate exceptional persistence in targeting critical infrastructure. APT 35, for example, is known to maintain prolonged network presence, often for months, awaiting opportune moments for malicious action. Within compromised networks, Iranian threat actors exhibit an aggressive reinfection cycle, typically attempting to re-establish access within 48 to 105 hours, ensuring persistent control and data exfiltration. This level of persistence and reinfection highlights a sophisticated understanding of network operations and a commitment to maintaining long-term access.

Country	Percentage of attacks logged
Israel	41
USA	15
Sweden	11
Saudi Arabia	6
UAE	6
Jordan	1
Others	20

The observed trend of increased Iranian APT activity directed towards critical infrastructure indicates a strategic shift in their operational priorities. Ongoing analysis suggests that Iran, in conjunction with its regional proxy actors, will remain a persistent threat to these systems.

The potential for synergistic cyber capability development between Iran and Russia, given their evolving strategic partnership, requires detailed technical assessment and mitigation strategies. .

APT Group	Scans	Supply chain	VPN	Watering hole	Data theft	Data sale	Vulnerability exploitation
APT 33	Yes	No	No	Yes	Yes	No	Yes
APT 34	Yes	Yes	Yes	Yes	Yes	No	Yes
APT 35	Yes	Yes	Yes	Yes	Yes	No	No

Cyber Threat Projections for 2025: Evolving Tactics and Strategic Shifts

While a general prediction of increased cyberattack volume and sophistication can be readily made, a more nuanced forecast necessitates the identification of key trends and actors shaping the 2025 threat landscape. This analysis aims to provide a refined perspective on the emerging threat environment, considering the interplay of relevant factors.

The following trends are projected to significantly influence the cyber threat landscape in 2024

- Organized threat actors to continue expanding with new tactics and affiliates
- Attacks on remote assets such as those in space and offshore oil rigs will be targeted more frequently
- Attacks on crypto wallets will gain momentum in 2025 and will remain the single biggest threat to businesses as actors will use the stolen funds to improve targeting and tactics
- Other than AI-based attacks, data refined by AI will pose a more persistent threat to business

Enhanced Encryption and Data Obfuscation

o Threat actors will employ increasingly robust encryption techniques to prolong data inaccessibility for victims. This strategy will complicate data recovery efforts and potentially increase ransom demands.

Multi-Vector Attack Campaigns

o A rise in multi-layered attacks is anticipated, combining phishing campaigns, zero-day vulnerability exploitation, and sophisticated social engineering tactics. This integrated approach aims to maximize attack efficacy and compromise diverse attack vectors.

Strategic Objectives: Ransom, Exfiltration, and Reconnaissance

o Threat actors will maintain a focus on three primary objectives ransomware deployment, data exfiltration and subsequent sale, and long-term reconnaissance for strategic intelligence gathering.

o Kinetic cyberattacks are projected to remain predominantly driven by geopolitical motivations rather than independent cybercriminal activities. Independent cybercriminals generally prioritize financial gain through ransom or data monetization, and avoid attacks with high potential for physical harm.

Operational Technology (OT) Security Prioritization

o OT security will receive heightened attention in 2024, with a focus on risk management, vulnerability remediation, and enhanced operational visibility and control within industrial environments.

o Comprehensive OT system documentation and specialized security training will become essential for mitigating emerging threats.

Increased Activity by Independent Threat Actors

o Independent cybercriminals utilizing modified tools derived from larger threat actor and APT arsenals will play a more prominent role.

o Increased law enforcement scrutiny against major threat actors in the US, EU, and other regions may incentivize smaller actors to target SMEs for scalable ransomware operations.

o Independent actors are likely to leverage distributed infrastructure across multiple jurisdictions, including mixed data processing capabilities, to maintain a low digital footprint while executing large-scale attacks.

Malware and Malicious Payload Trends: Obfuscation, Diversification, and Critical Infrastructure Targeting

Malware Source Attribution Challenges

In 2024, a notable increase in unidentified malware sources presented significant challenges to attribution efforts. This phenomenon indicates several key trends

Geopolitical Conflict and Advanced Malware Development

o A correlation exists between the proliferation of sophisticated malware and regions experiencing active geopolitical conflict. The observed malware originating from conflict zones, such as Ukraine, Israel, and Armenia, underscores the weaponization of cyber capabilities in contemporary warfare.

Advanced Obfuscation Techniques by Level Two Actors

o Enablers and level two threat actors are employing sophisticated obfuscation techniques, including header manipulation and property alteration, to conceal malware origins. However, proprietary detection methodologies employed by our research team have successfully identified these covert activities.

Enhanced Operational Security and Anonymization

o Threat actors are prioritizing operational security and anonymity, implementing comprehensive measures to obscure their digital footprints throughout the attack lifecycle.

Emergence of Undiscovered Malware Forums

o Hidden malware forums are facilitating the exchange of complex malware and exploit tools, contributing to the diversification of the threat landscape.

Independent Threat Actor Activity and Critical Infrastructure Targeting

Independent threat actors maintained a high level of operational activity throughout 2023. The execution of high-profile attacks, targeting gas pipelines, utility infrastructure, project management software, and other critical applications, suggests a strategic effort to establish persistent network access for malware deployment and long-term surveillance. Critical Infrastructure Vulnerabilities and Operational Technology (OT) Security

OT Availability and Legacy System Vulnerabilities

• Operational technology (OT) environments, particularly within critical infrastructure sectors, prioritize system availability and uptime. The prevalence of legacy systems lacking robust vulnerability assessment, patching, access management, and control mechanisms creates significant disruption risks.

• The inherent constraints of OT environments, where system downtime can result in severe consequences (e.g., power outages, water supply disruptions), contribute to the persistence of vulnerable legacy systems.

• The maturity of current OT security programs is inadequate. Immediate prioritization must be placed on improving cyber-physical system protection.

Enabler Role in Malware and Intelligence Exchange

o Enablers function as third-party conduits, facilitating the exchange of advanced malware, vulnerability intelligence, and stolen data. These entities also support the transfer of malware and breach tactics between affiliated APT groups, enabling plausible deniability and operational distance.

Malware origin

Possible Source	Percentage detected
Dark web	15
Procured via malware forums	28
Mixed	6
Military-grade	6
Academic\research labs	5
Unknown	40

Advanced Malware Analysis and Emerging Development Trends: A Research Laboratory Perspective

Within our specialized research laboratories, a multi-faceted analytical approach has been implemented to achieve granular malware segregation and characterization. This methodology encompasses

Observed Trait Analysis : Categorization based on discernible behavioral patterns and operational characteristics.

- **Deep Content Inspection :** Examination of binary and executable structures to identify embedded malicious code and payloads.

- **Multi-Layer Inspection and Analysis :** Sequential analysis across various layers of the malware, including network, application, and kernel levels, to detect hidden functionalities and communication protocols.

- **Code Slicing :** Examination of binary and executable structures to identify embedded malicious code and payloads.

- **Dual Sandboxing :** Utilizing redundant sandboxing environments to observe malware behavior in controlled and isolated settings, mitigating the risk of escape and lateral movement.

- **Proprietary Behavioral Analysis and Stealth Evaluation Techniques :** Employing in-house developed methodologies to assess malware behavior, including evasion techniques, persistence mechanisms, and covert communication channels.

Through this comprehensive analysis, we have consistently observed that while malware properties exhibit dynamic variations, the fundamental characteristics of stealth and persistence remain constant across all samples. These core attributes are essential for malware to achieve its objectives, which include establishing covert network access, exfiltrating sensitive data, and maintaining long-term control over compromised systems.

A significant development this year has been the discovery of a substantial cache of malware exhibiting characteristics indicative of development within academic or research facilities. This attribution is based on the presence of code inserts and unique traits that do not align with known malware development laboratories. The observed anomalies suggest a distinct development environment and potentially a different set of objectives.

The collaborative nature of malware development is well-established, involving multiple actors and shared resources. It is increasingly evident that malware developers are leveraging base code and components originating from academic institutions or government-affiliated research facilities. This practice enables the rapid development of sophisticated malware, potentially introducing novel attack vectors and obfuscation techniques. The utilization of research-derived code also contributes to the diversification of the threat landscape, making attribution and mitigation more challenging. This trend underscores the importance of stringent security measures within research environments to prevent the inadvertent or intentional leakage of potentially weaponizable code.

Port	Attacks in million
23 -Telnet	877
445 - SMB	634
22 SSH	542
1433 MSSQL	300
3306 MySQL	600
80 - HTTP	728
7547 - CWMP	109
25 - SMTP	65
20 FTP	32
Others	22

Types of attacks and frequency

Types	Percentage occurrence
Integrity violation with malicious code Injection	19
Brute force attacks	13
Phishing emails	2/week/org
Privilege abuse	11
DoS and variants	8
Simple reconnaissance	18
Persistent reconnaissance	8

Port/asset scan/TCP dump (specific recon)	10
Firmware downgrade attempts (corrosion)	7
Crypto mining/jacking	9

Key traits observed in malicious payloads detected around the world (sample size 10909 unique samples)

Trait	Trait detection rates (in percentage)	Geographic distribution or focus	Verticals targeted
Persistence	High 58 Med 32 Low 10	North America, Western Europe, and SE Asia	Manufacturing and critical infrastructure projects
High levels of stealth	76	Global	Defense, healthcare-connected vehicles, and manufacturing
Faster deployment	81	Global	Almost all verticals
Crypto mining	29	All except Latin America	Smart cities and manufacturing
High network mobility plus Lateral movement	65	Global	Manufacturing, smart cities, Defence, telecom

Attacks on key sectors

Sector	Trend (in percentage)
Energy	↑ 172
Healthcare	↑ 98
Manufacturing	↑ 91
Oil and gas	↑ 87
Education	↑ 65
Banking and Finance	↑ 65
Defense	↑ 57
Retail	↑ 49
Smart devices	↑ 48
Critical infrastructure excluding energy/utilities and oil and gas pipeline and infra	↑ 39
Others including agriculture, public safety, unspecified projects, and telematics projects not falling under the above categories	↑ 70

Common IEC 62443 control deficiencies heightening the risk exposure

In the year 2024, Shieldworkz' Risk and Gap Assessment team carried out multiple assessments across the globe. As an outcome of this exercise, the team pointed out multiple security controls that were lacking across sites and even industries in some instance. A compressed version of the findings along with the SR information is provided in the below table.

The result of such gaps could include

Key SRs	Deficiency	Risk	Commonly encountered in which industry
Identification and Authentication Control (IAC)			
SR 1.1 – Human user identification and authentication	Use and privilege controls do not exist or controls do not allow users to be identified	Insider threat, challenges with Root Cause Analysis after an event (RCA), session user mismatch	Manufacturing, ports

Key SRs	Deficiency	Risk	Commonly encountered in which industry
SR 1.2 - Software process and device identification and authentication	Devices and processes are triggered and function at random without being tracked	Rogue devices could be introduced unauthorized processes may run in the background without being detected	Manufacturing, utilities, ports, airports
SR 1.3 - Account management	Inadequate controls and excess privileges; lack of role- and need-based privileges	Unauthorized users could misuse privileges	Manufacturing, oil and gas, utilities, ports, airports
SR 1.4 - Identifier management	Lack of awareness of user, group, role, or control system interface identifiers must be supported.	Challenges in linking action to a specific user or user group	Manufacturing, oil and gas, utilities
SR 1.5 - Authenticator management	Lack of mechanism or oversight or both to ensure authenticators (such as passwords) are unique, not transmitted or stored in clear text, shared among employees.	Possibility of breach	Manufacturing, oil and gas, utilities
SR 1.6 - Wireless access management	Wireless access is not regulated; wireless is used for accessing	Misuse of wireless third party may access systems or misuse them	Manufacturing
SR 1.7 - Strength of pass-word-based authentication	Use of weak passwords that are present in breached Dark Web records	Threat actors can gain access to systems from accessible systems (with exposed IPs)	Manufacturing, oil and gas, utilities, ports, airports

Key SRs	Deficiency	Risk	Commonly encountered in which industry
Use Control			
SR 2.1 - Authorization enforcement	Weak authentication controls; Lack of ability to set a complete system setting, right down to a specific individual level enforcement setting corresponding to an individual object	Credential misuse	Manufacturing, ports, oil and gas, utilities
	Wireless networks are not set up with the	Misuse of wireless	Manufacturing, oil and gas,
SR 2.2 - Wireless use control	capability to authorize, monitor, and enforce usage restrictions according to commonly accepted security industry practices.		utilities, airports
SR 2.4 - Least privilege	Misuse of privileges and lack of privilege control	Misuse of wireless third party may access systems or misuse them	Manufacturing, oil and gas, utilities, ports, airports
SR 2.6 - Remote session termination	Lack of capability to set up remote sessions in a manner that they terminate automatically after a specified duration of inactivity- timeout, or using manual termination by the initiator.	Extended sessions could render networks vulnerable to data hijacking or remote access by threat actors	Manufacturing, oil and gas, utilities, ports, airports
SR 2.7 - Concurrent session control	Lack of controls related to concurrent session	Threat actor could use concurrent sessions to hijack processes and systems	Manufacturing, oil and gas, utilities, ports, airports

Key SRs	Deficiency	Risk	Commonly encountered in which industry
System Integrity (SI)			
SR 3.1 - Communication integrity	Lack of controls to prevent exfiltration of data. Protect against information tampering during transmission.	Data breach	Manufacturing
SR 3.2 - Malicious code protection	Lack of measures to identify code modification and execution of malicious codes without impacting IACS real-time behavior	Trojan codes added by unauthorized entities can be triggered remotely or insitu to cause disruption	Manufacturing, oil and gas, utilities, ports, airports
3.8 Session integrity	Session-based protocols are not protected in a way that causes the rejection of invalid session IDs	Session manipulation	Manufacturing, oil and gas, utilities, ports, airports
Data Confidentiality (DC)			
SR 4.1 - Information confidentiality	Confidential information is not secured in such a way that it is protected when it is at rest. No or less than adequate measures in place to protect confidential information	Data breach, leakage of credentials	Manufacturing, oil and gas, utilities, ports, airports
Data Flow Restrictions			
SR 5.1 - Network segmentation	Network segments are not logically isolated Traffic from one segment ends up intermixing with traffic from other segments No barriers in place to prevent mixing of control-system network and non-control system network traffic	Lateral movement of malware and threats	Manufacturing, oil and gas, utilities, ports, airports

Key SRs	Deficiency	Risk	Commonly encountered in which industry
SR 5.2 - Protection of zone boundary and network integrity	Lack of barriers and boundary protection around zones; network susceptible to breach due to mixing of traffic	Same as above Same as above	Manufacturing
SR 5.3 - Partitioning of data flows	Same as above. Mixing of traffic with different intend across networks enabling migration of threats	Data breach, threats can move across the network to target crown jewels	Manufacturing, oil and gas, utilities, ports, airports
Additional Protection			
SR 7.1 – Denial of service protection	IACS doesn't harbor the means to request information from or be notified by boundary devices, or otherwise detect an ongoing cyberattack. IACS also cannot operate in a degraded mode post detection.	Disruption of operations	
Reporting	Lack of event reporting capabilities	Compliance challenges	Manufacturing, oil and gas, utilities, ports, airports
Response	Network segments are not logically isolated Traffic from one segment ends up intermixing with traffic from other segments No barriers in place to prevent mixing of control-system network and non-control system network traffic	Lateral movement of malware and threats	Manufacturing, oil and gas, utilities, ports, airports
Resource Availability			
Redundancy	Lack of redundancies	Disruption and extended recovery phase	Manufacturing, oil and gas, utilities, ports, airports

Countries where malware was first spotted as a percentage of overall detections

Country	percentage of overall detection
China	19
North Korea	17
Russia	16
Iran	16
Malaysia	1
Vietnam	1
Unknown	30

Most attacked countries in cyberspace

USA still remains the most attacked nation in cyberspace (based on the volume of cyberattacks). The ranking remains largely unchanged except for a few nations moving up or down. When one views the rankings based on the quality of the attack, there is an entirely different view that emerges. In this list, while US is still number one, it is followed by Ukraine and Belgium. While Ukraine is in the midst of an ongoing conflict, Belgium and Estonia are attracting cyberattacks of higher quality as they are home to strategic agencies and intergovernmental bodies.

Most attacked countries (volume)

Country	Rank
USA	1
Germany	2
United Kingdom	3
Canada	4
France	5

Ukraine	6
India	7
Australia	8
UAE	9
South Korea	10

Most attacked nations (quality and sophistication of cyberattack)

Country	Rank
USA	1
Ukraine	2
Belgium	3
UAE	4
Germany	5
Israel	6
Norway	7
Estonia	8
Saudi Arabia	9
Vietnam	10

For the above calculation, we assign weightage on the basis of the below table

Parameter	Weightage
Attack sophistication	10
Threat actor rank (involved in the attacks studied)	10
Volume of attacks unconnected with geopolitical events	5
Percentage of attacks drawn from non-conventional threat actors	15
Volume of verified yet undisclosed attacks	10
Overall attack volume	20
Attacks on CII	20
Other parameters	10

Most targeted nations (based on the number of sites/countries of origin of attacks)

Country	Country	Verified attacks originating from
USA	1	70009 IP clusters across 51 countries
UK	2	39902 IP clusters across 47 countries
Germany	3	20092 IP clusters across 44 countries
Israel	4	19092 IP clusters across 37 countries
France	5	18963 IP clusters across 35 countries
India	6	15666 IP clusters across 33 countries
UAE	7	14087 IP clusters across 29 countries

Ukraine	8	10873 IP clusters across 21 countries
Vietnam	9	70009 IP clusters across 51 countries
Philippines	10	39902 IP clusters across 47 countries

Most attacked countries on a per capita basis

To gain a deeper understanding of the impact of cyberattacks across different countries, we incorporated population data into our analysis. 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.

According to this metric, Ukraine ranks as the most affected country. This result is not unexpected, given the ongoing conflict and geopolitical tensions. However, it's important to note that cyberattacks on Ukraine are not evenly distributed over time. They tend to surge during periods of intense military activity, such as heavy shelling or significant troop movements along the front lines.

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.

Table - Countries drawing maximum cyberattacks on a per capita basis

Country	Rank
Ukraine	1
Lithuania	2
Finland	3
Israel	4

Taiwan	5
Belarus	6
Sweden	7
Chile	8
Oman	9
Estonia	10

Most attacked cities

An examination of the cities most frequently subjected to cyberattacks reveals the undeniable influence of geopolitics in cyberspace. The consistent ranking of several East European cities within the top 10 in 2022, 2023 and 2024 is certainly a telling indicator. These cities were prime targets for sophisticated persistent threat (APT) groups believed to be associated with Russia, China, and Iran. The statistic that over 60 percent of cyberattacks on Vilnius and Tallin were traced to Chinese APT actors is particularly significant. It is possible that Chinese APT groups are maintaining a high level of vigil across this region.

While direct cooperation among these APTs cannot be definitively established, the geopolitical context strongly suggests the underlying motivation for these attacks.

City	Rank in 2024	Rank in 2023
New York	1	3
Kiev	2	6
Tokyo	3	-
Talin\Prague	4	-
New Delhi	5	5
Vilnius	6	-

Dubai	7	7
Oslo	8	-
London	9	2
Washington D.C	10	1

Threat landscape across regions

North America

The digital landscape of North America, a global epicenter for innovation and transformation, faced an unrelenting barrage of cyberattacks, painting a stark picture of the escalating threats in the digital age. In 2024, the region witnessed a staggering 301 billion attacks, a monumental 299 percent surge compared to the previous year, underscoring a rapidly intensifying cyber battlefield.

Regional snapshot

Total Attacks: 301 billion

Complex attacks: 21 billion

Attacks on CII: 71 billion

Reconnaissance load: 192 billion

Growth in attacks over 2023: 299 percent

Within this immense volume, 21 billion were sophisticated, complex attacks, demonstrating the increasing skill and resources of malicious actors. Critical infrastructure, encompassing vital utilities and water treatment facilities, became a significant target, absorbing 71 billion attack attempts, highlighting the potential for widespread disruption. Even the initial probing and reconnaissance efforts reached an astounding 192 billion instances, revealing the persistent and pervasive nature of threat actor activity.

This relentless cyber onslaught disproportionately impacted key sectors driving the North American economy and societal well-being. Manufacturing, healthcare, education, the foundational critical infrastructure, burgeoning start-ups, and the energy-rich oil and gas industries all found themselves in the crosshairs. Organizations managing intricate technological ecosystems, blending traditional IT with operational technology (OT), industrial control systems (ICS), and the burgeoning Internet of Things (IoT), proved particularly vulnerable to this escalating tide of attacks.

At the heart of this cyber storm stood the United States, consistently ranking as the most targeted nation globally. Its digital frontiers faced constant probing and active attacks originating from a diverse spectrum of threat actors, ranging from well-established and highly resourced Advanced Persistent Threat (APT) groups to smaller, less sophisticated entities. The digital arteries of the US were under persistent scrutiny from state-sponsored and non-state-sponsored groups emanating from Iran, North Korea, China, Russia, and even less conventionally recognized cyber threat origins.

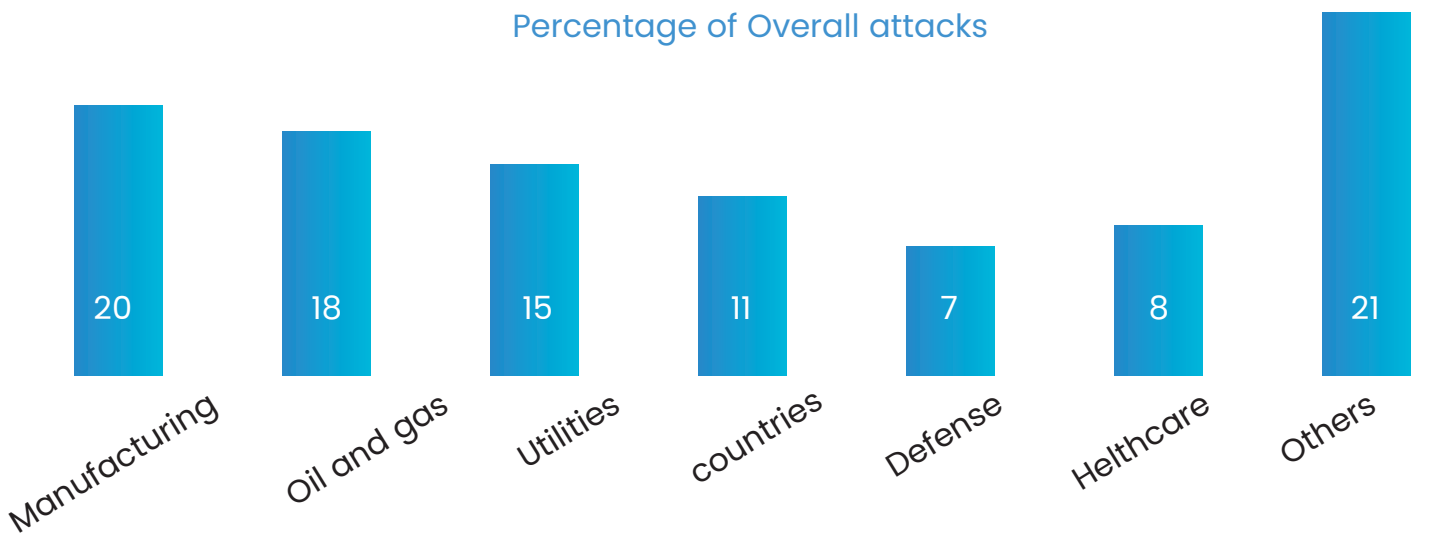
Dominating the threat landscape in North American cyberspace during 2024 was the notorious Lockbit ransomware group, responsible for a staggering 21 percent of all reported cyber incidents. Through its network of affiliates, Lockbit established a pervasive and damaging footprint across the region, with a particular predilection for the often-underfunded education and healthcare sectors. Lockbit's operational patterns in North America offer a revealing glimpse into the evolution of cybercriminal enterprises over the past half-decade.

Since its emergence in 2019, Lockbit rapidly expanded its malicious reach, extorting billions of dollars in ransom payments and inflicting substantial downtime and recovery costs on victims worldwide. Throughout the early 2020s, Lockbit affiliates aggressively targeted entities across various industries in the US and Canada, successfully breaching some of the region's largest and most prominent organizations.

The absence of robust and adaptive regulatory measures inadvertently facilitated Lockbit's remarkable ability to repeatedly reshape its criminal business model. Initially focused on a select number of high-value targets, Lockbit's affiliates by the end of 2022 adopted a far more indiscriminate approach, launching attacks across the digital landscape, often targeting even entities with limited capacity to pay ransoms, including vulnerable educational institutions and small healthcare providers.

Within the United States, sophisticated info-stealing malware emerged as a key tool for augmenting data breaches. Information harvested from social media platforms like Twitter 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 7 petabytes of stolen data analyzed, a staggering 2.6 petabytes originated from US entities. This torrent of stolen information witnessed a substantial 39 percent year-on-year increase in 2024. Meanwhile, Canadian businesses experienced a significant 323 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.



Ongoing threat activity in manufacturing and oil & gas sectors

Manufacturing and oil and gas sectors continue to experience a disproportionately high volume of cyberattacks within the region. These sectors remain primary targets due to their strategic and economic importance, operational complexity, and their integration of legacy systems with modern digital infrastructure. Attack telemetry and incident reporting indicate that high-value assets within these industries are being systematically targeted, often through sophisticated, multi-stage attack campaigns.

Utilities and Sectoral Attack Variability

In contrast, the volume of attacks targeting utilities demonstrates significant temporal 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.

Targeted interest in high-value manufacturing

Within manufacturing, the concentration of attacks is skewed towards high-end and heavy 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—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.

Supply chain and downstream exploitation

Both oil and gas and manufacturing sectors face a broad spectrum of threats that span across the supply chain—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.

Geostrategic dimensions of threat activity

The persistent and well-coordinated attacks against critical infrastructure sectors—especially manufacturing, utilities, and oil and gas—are indicative of a broader geopolitical agenda. Intelligence from attack forensics and infrastructure telemetry points to a pre-conflict phase of hybrid warfare, with adversarial nations engaging in deep reconnaissance and access provisioning. The intent appears to be to degrade resilience and sow confusion in the event of geopolitical escalation.

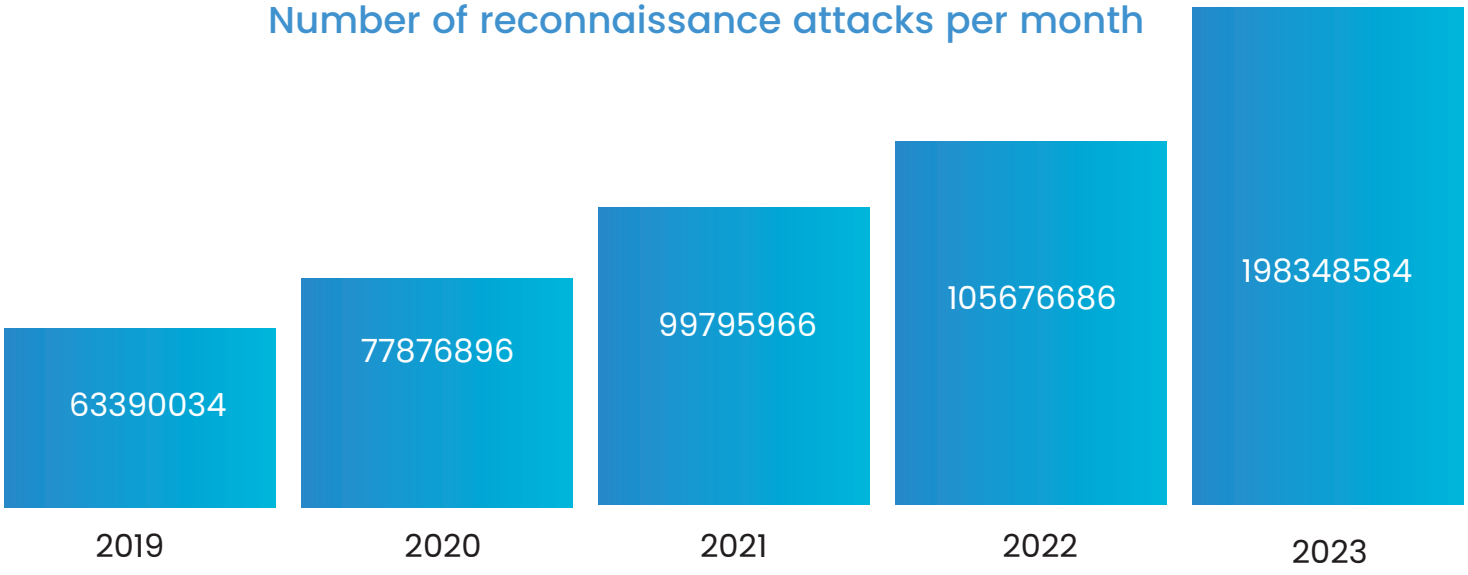
Attribution and threat actor behavior

Multiple nation-state actors are likely involved in these campaigns. Our analysis traces the origin of attacks to infrastructure spanning at least two continents and three countries. Russia and China employ layered obfuscation tactics, routing attack traffic through compromised home and industrial IoT devices to mask attribution. Their focus remains on persistent access, long-term reconnaissance, and large-scale data exfiltration. In contrast, Iranian campaigns are more overt and disruptive, frequently targeting operational continuity in utilities and manufacturing plants.

Latent threats and escalation potential

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.

Number of reconnaissance attacks per month



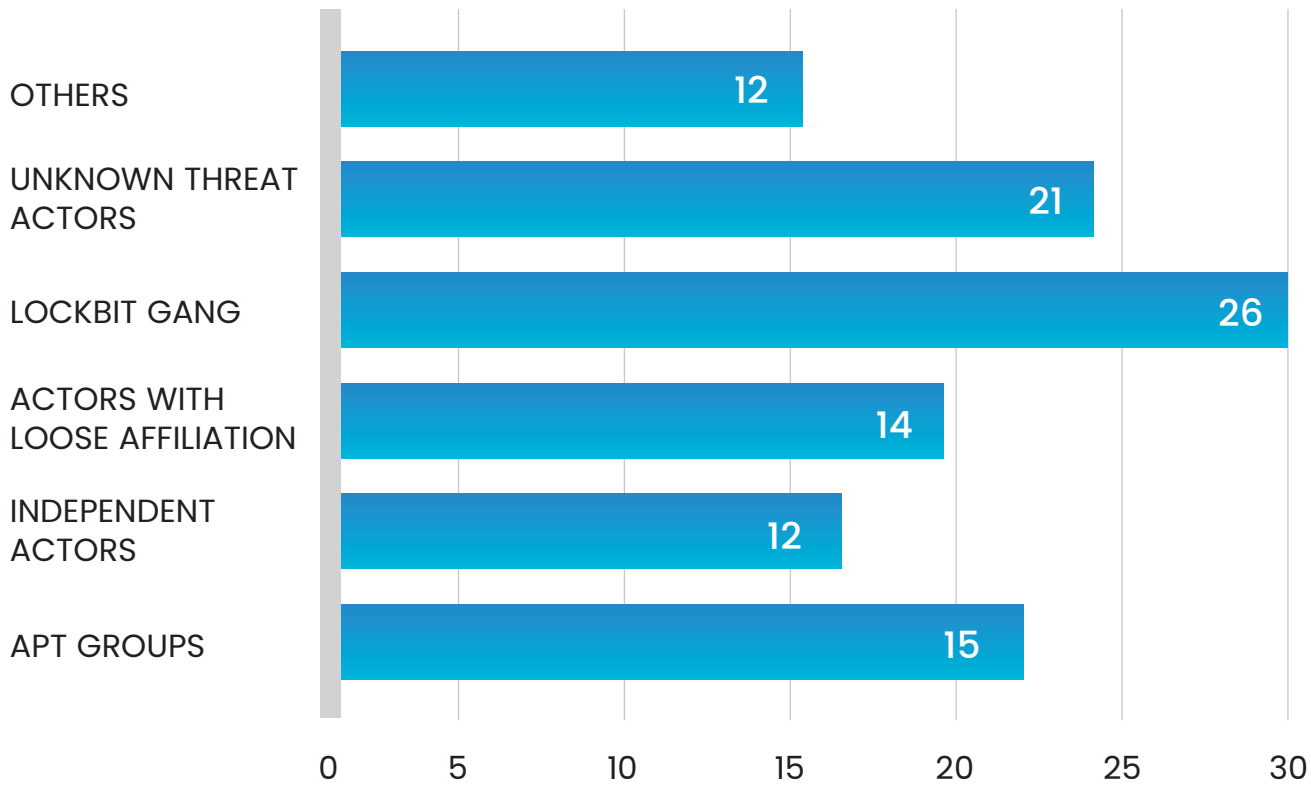
The escalating frequency of reconnaissance attacks across critical sectors in North America is a growing concern that demands immediate attention. These operations have evolved far beyond simple network probing; adversaries now actively exfiltrate metadata, credentials, and system configuration details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

Alarmingly, 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, 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 also become significantly more adaptive and evasive. They dynamically rotate through vast IP address pools, 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.

Who is attacking North America?



Attacks on critical infrastructure

A significant cyberattack in 2024 was conducted by a pro-Russian hacktivist group that targeted critical infrastructure across the United States. The group compromised multiple water treatment plants and also claimed responsibility for attacks on two dairy facilities Their primary method of intrusion involved exploiting multiple unsecured, internet-facing human-machine interfaces (HMIs) to access industrial control system (ICS) components remotely.

In January 2024, the group successfully infiltrated two water facilities in Texas, where they altered pump settings and alarm thresholds—ultimately causing storage tanks to overflow. Then in April 2024, the attackers released video footage showing themselves remotely manipulating HMI screens within wastewater treatment systems and an unnamed energy company, highlighting the ongoing risks of poor ICS network segmentation and inadequate authentication mechanisms.

Between January 2024 and June 2024, at least 49 cyberattacks targeting industrial control system infrastructure were publicly reported across the United States. Among these, 33 were attributed to the Iranian-linked hacktivist group Cyber Av3ngers, while 9 were claimed by a pro-Russian group linked to their flagship APT group. These campaigns affected a wide geographic area, spanning at least 16 states—including California, Colorado, Florida, Georgia, Illinois, Indiana, Minnesota, Montana, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Pennsylvania, South Carolina and Texas.

The targeted attacks impacted a broad array of sectors, such as water and wastewater treatment, agriculture, energy, healthcare, education, telecommunications, state and municipal governments, and private-sector manufacturing. This distribution underscores the systemic and cross-sectoral vulnerabilities within the operational technology (OT) landscape in North America.

Industrial control systems, a critical component of OT infrastructure, enable the automated and remote management of physical processes. Unlike information technology (IT), which focuses on data processing and communication, ICS components interface directly with sensors, actuators, and machinery to control real-world outcomes. Core ICS elements include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Human-Machine Interfaces (HMIs), and Programmable Logic Controllers (PLCs). 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.

Exploiting Local Governments: A Growing Threat to Counties and Public Infrastructure

Attacks on U.S. county governments have surged by 137% in 2023, exposing a critical vulnerability in local governance IT infrastructures. One of the most common attack vectors observed was brute force login attempts targeting specific public-facing servers. Between April and December 2023, counties were bombarded with an average of 14,000 login attempts every 78 hours—a staggering frequency that underscores both the scale and persistence of the threat.

Although many of these attempts were blocked by basic security controls, several 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 2023 had not returned to full operational capacity even by January 2024. 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—leaving minimal time for victims to react.

Root Causes Behind County-Level Vulnerability

- Weak foundational security hygiene, especially poor password management and lack of MFA
- Understaffed and underfunded IT teams, often lacking specialized cybersecurity personnel
- Accumulated exposure from prior reconnaissance operations, leaving digital footprints and misconfigured systems vulnerable
- Inadequate data protection and storage security, including insufficient encryption and lack of asset visibility

Smart Cities Under Siege: IoT Attacks on the Rise

Cyberattacks targeting Internet of Things (IoT) infrastructure and smart city initiatives have continued to escalate, particularly in mid-sized urban centers. These attacks are typically categorized into several vectors

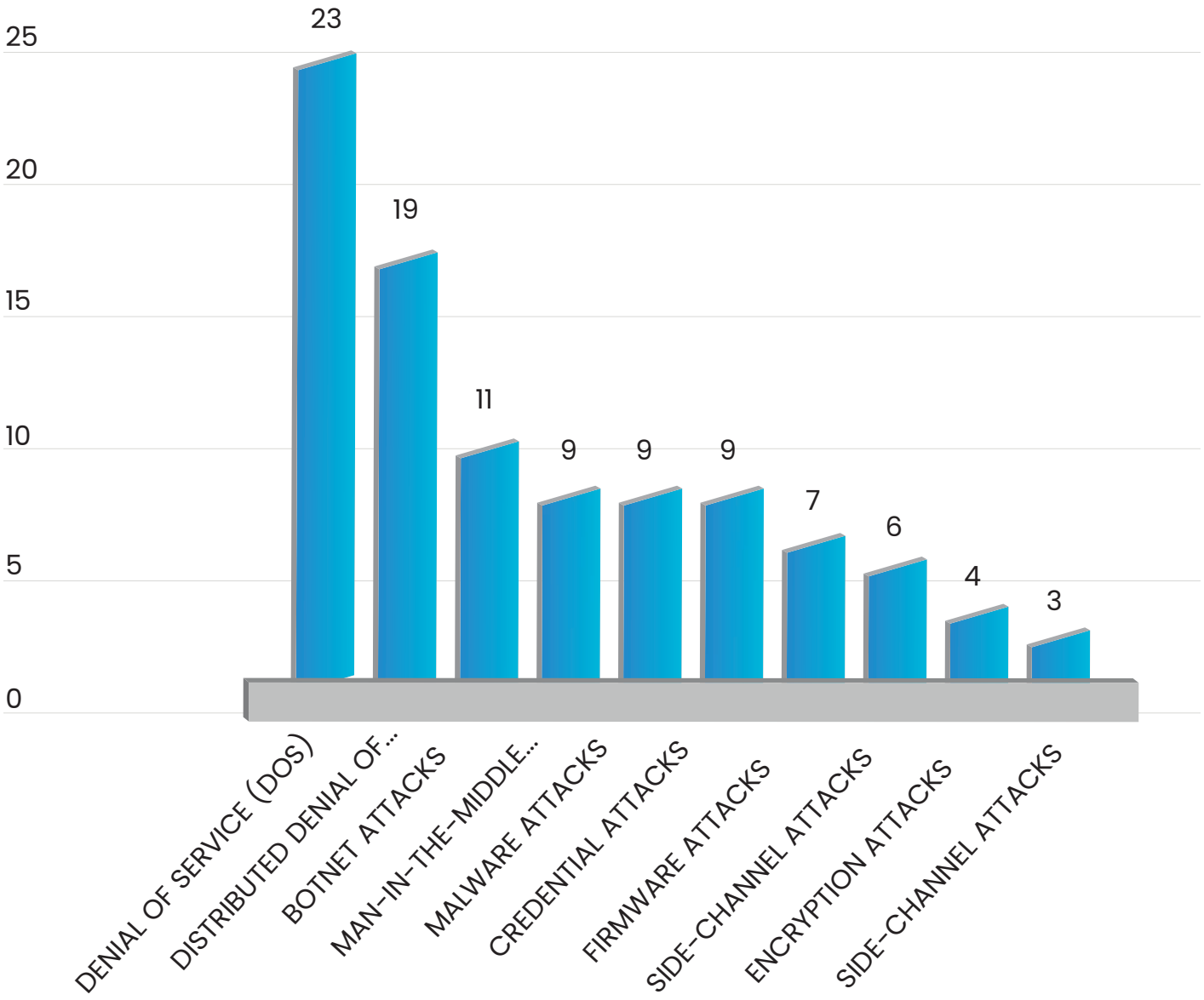
- Denial of Service (DoS) / Distributed DoS (DDoS)
- Botnet-based command and control takeovers
- Man-in-the-Middle (MitM) attacks
- Malware injection
- Credential stuffing and brute force password attacks
- Firmware manipulation and side-channel attacks
- Exploitation of weak or absent encryption protocols

While DDoS attacks remain the most common due to ease of deployment and impact, MitM and malware-based attacks have resulted in greater long-term damage, including data exfiltration, surveillance, and operational disruption.

Across 14+ U.S. cities, IoT systems experienced sustained, low-intensity attack pulses—indicating the use of AI-augmented automation tools. These tools can maintain attack thresholds over time, probing for weaknesses with minimal human oversight. This "drip-feed" tactic allows attackers to stay under detection thresholds while steadily increasing the attack surface.

A major risk factor is the frequent integration of new, untested IoT devices and third-party applications. Each addition creates a new potential vulnerability, often without proper security vetting or patch management. Threat actors are acutely aware of this and are betting on configuration drift and poor lifecycle management to eventually gain access.

Smart Cities Under Siege: IoT Attacks on the Rise



South and Central America

Latin America's expanding cyber threat landscape a 2023 deep dive

In 2024, South and Central America experienced an unprecedented surge in both the volume and sophistication of cyberattacks, marking the region's highest-ever level of cyber threat activity. This dramatic increase is driven by a convergence of factors: rapid digital transformation, integration into global supply chains, and heightened attention from state-sponsored adversaries—most notably Russian and Chinese APT groups.

Regional snapshot

Total Attacks: 28 billion

Complex attacks: 1.1 billion

Attacks on CII: 93 million

Reconnaissance load: 124 million

Growth in attacks over 2024: 19 percent

Digital acceleration driving threat surface expansion

Over the past several years, Latin America has seen widespread adoption of digital infrastructure across sectors. This includes

- Broadband penetration and mobile internet expansion
- Increased use of digital tools in industrial production, agriculture, and mining
- Rapid automation across logistics and commodity management
- Widespread adoption of cloud services and SaaS platforms

These developments, while economically beneficial, have drastically expanded the regional attack surface—often without proportional investments in cybersecurity infrastructure or expertise. The result is a landscape rich with unprotected assets, misconfigured systems, and exposed endpoints that serve as low-hanging fruit for threat actors.

APT activity on the rise

The region has become a strategic interest zone for multiple nation-state actors, including

- APT41 (China) – known for espionage, intellectual property theft, and targeting critical infrastructure
- APT29 (Russia) – focused on long-term infiltration and geopolitical intelligence
- APT35 (Iran) – targeting public sector and foreign policy domains
- Lazarus Group (North Korea) – blending financial motivation with state-aligned disruption campaigns

These groups are not merely probing but establishing operational footholds, expanding C2 infrastructure, and testing malware variants across Latin American targets, often leveraging existing vulnerabilities within the region's immature cyber defense ecosystems.

High-impact incidents and supply chain attacks

Cyberattacks in Latin America are increasingly indiscriminate of organizational size, and supply chain compromises are becoming more frequent. A notable example was the October 2023 Rorschach ransomware attack on Chilean telecommunications provider GTD, which impacted 3,500 downstream organizations, highlighting both the interdependence of digital infrastructure and the fragility of unsegmented networks.

Strategic geopolitical relevance fueling risk

Latin America's geopolitical value is rising as nations such as the U.S., EU, and China court the region for trade, rare earth minerals, energy, and nearshore manufacturing. This increasing global integration draws the region deeper into the crosshairs of geopolitically motivated cyber operations, often used to signal influence or disrupt strategic interests of rival states.

Additionally, proximity to North American markets makes Latin America a favorable region for hosting production hubs, thereby elevating its cyber risk profile in the global digital ecosystem.

Alarming success rates and systemic vulnerabilities

Perhaps the most concerning trend is the attack success rate in Latin America. As of July 2024, the region recorded a peak cyberattack success rate of 0.05%—a significant figure given the scale of attempted intrusions. This vulnerability stems from several key challenges

- Shortage of skilled cybersecurity professionals
- Limited or poorly enforced cybersecurity regulations
- Fragmented response mechanisms across public and private sectors
- Lack of standardized cyber hygiene practices

Rise of regional bot farms and hijacked infrastructure

Latin America is also emerging as a hotbed for botnet operations. Many of these bot farms are built by compromising both industrial infrastructure and personal devices, creating sprawling, hijacked digital ecosystems. While only 10% of the bot traffic is directed at regional businesses, the rest is used for

- Reconnaissance and scanning
- Testing malware payloads
- Running campaigns for threat actors operating globally

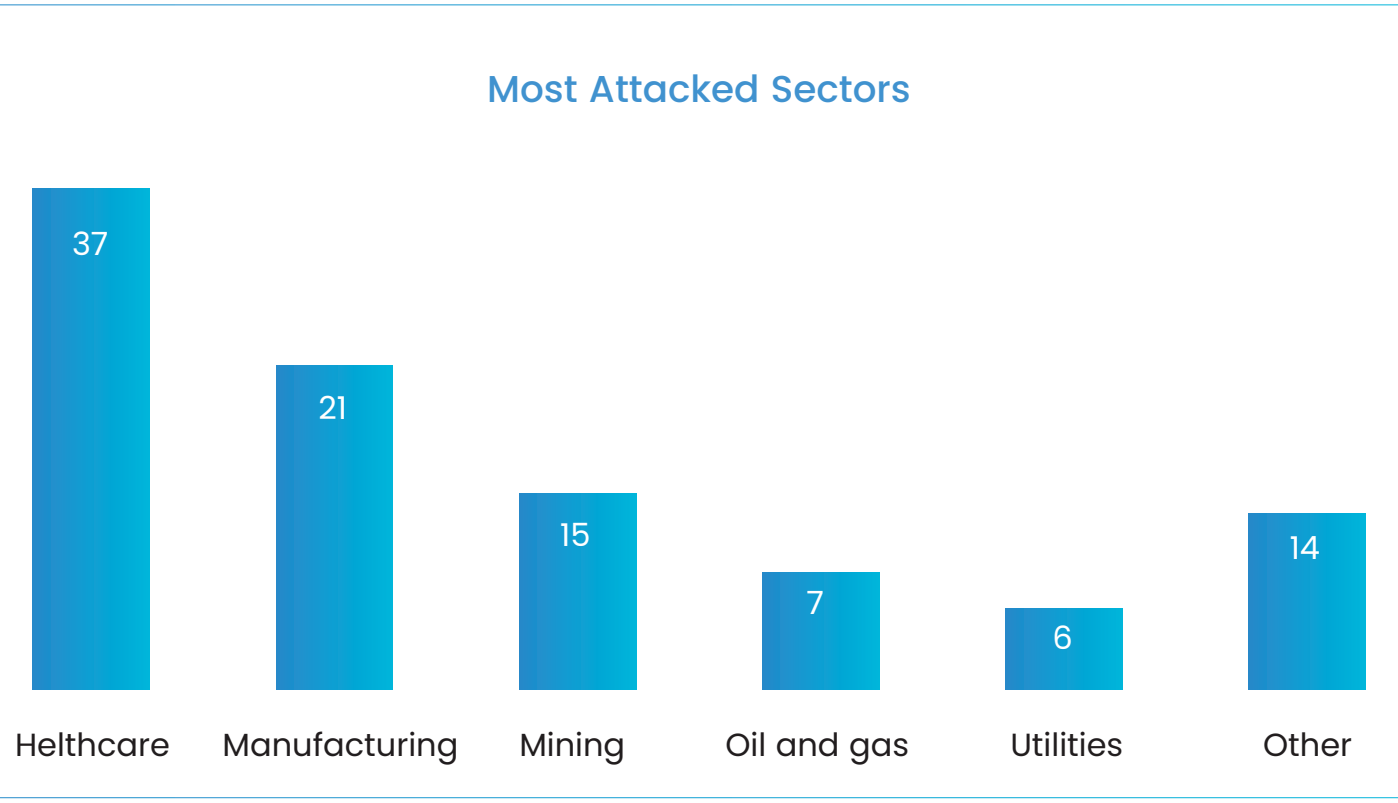
Brazil and Colombia remain unique cases where attackers continue to exploit traditional SMS phishing (smishing) to compromise mobile users—indicative of a wider range of attack vectors tailored to local infrastructure.

Evolution of botnet capabilities

Botnet operations in the region have become significantly more advanced over the past five years. In 2020, Latin American botnets were relatively limited, mostly used for low-scale DDoS attacks. Today, they serve multiple offensive functions

- Credential harvesting
- Cloud brute-forcing
- Command-and-control staging
- Distributed payload delivery

The growing ease with which attackers can access and maintain these bot farms—combined with weak endpoint protections—makes them a powerful force multiplier for cyber adversaries operating in or through the region.



The high volume of cyberattacks observed in the healthcare and manufacturing sectors in Latin America during 2024 reflects the differing motivations and operational tactics of distinct threat actor groups.

In the manufacturing sector, attacks are being carried out by a diverse set of independent actors, including financially motivated ransomware groups, cybercriminal collectives, and potential state-aligned entities. These actors exploit common vulnerabilities in industrial control systems (ICS), supply chain software, and enterprise IT infrastructure. Targets often include small-to-medium enterprises with limited cybersecurity maturity, as well as larger manufacturers involved in strategically significant industries such as automotive, defense, and critical materials processing.

In contrast, cyberattacks on the healthcare sector have been dominated by affiliates of the LockBit ransomware-as-a-service (RaaS) ecosystem. These groups frequently employ double extortion tactics, encrypting sensitive health records and threatening to leak patient data unless ransom demands are met. The healthcare industry's dependence on outdated IT infrastructure, combined with a high sensitivity to service interruptions, makes it an attractive and vulnerable target.

Beyond healthcare and manufacturing, there is increasing cyber interest in the critical minerals sector, particularly in countries across Latin America. The region is a major producer of lithium and copper—two essential inputs for energy transition technologies. Lithium is a core material for rechargeable batteries used in electric vehicles and grid storage systems, while copper is indispensable for the expansion of renewable energy infrastructure and electrical grids. Moreover, Latin America holds significant untapped potential in other strategic materials such as rare earth elements (needed for permanent magnets in EV motors and wind turbines) and nickel, a key component in high-energy-density battery chemistries.

The intensifying global competition for these resources—led in part by China—has made the region a strategic focus for geopolitical and economic cyber espionage. This geopolitical context may explain the heightened activity of Chinese state-linked cyber actors in Latin America. These groups are suspected of engaging in long-term intelligence-gathering campaigns targeting mining companies, government agencies responsible for resource regulation, and logistical supply chains. Their tactics often include advanced social engineering, spear phishing, and the cultivation of insider access within critical organizations.

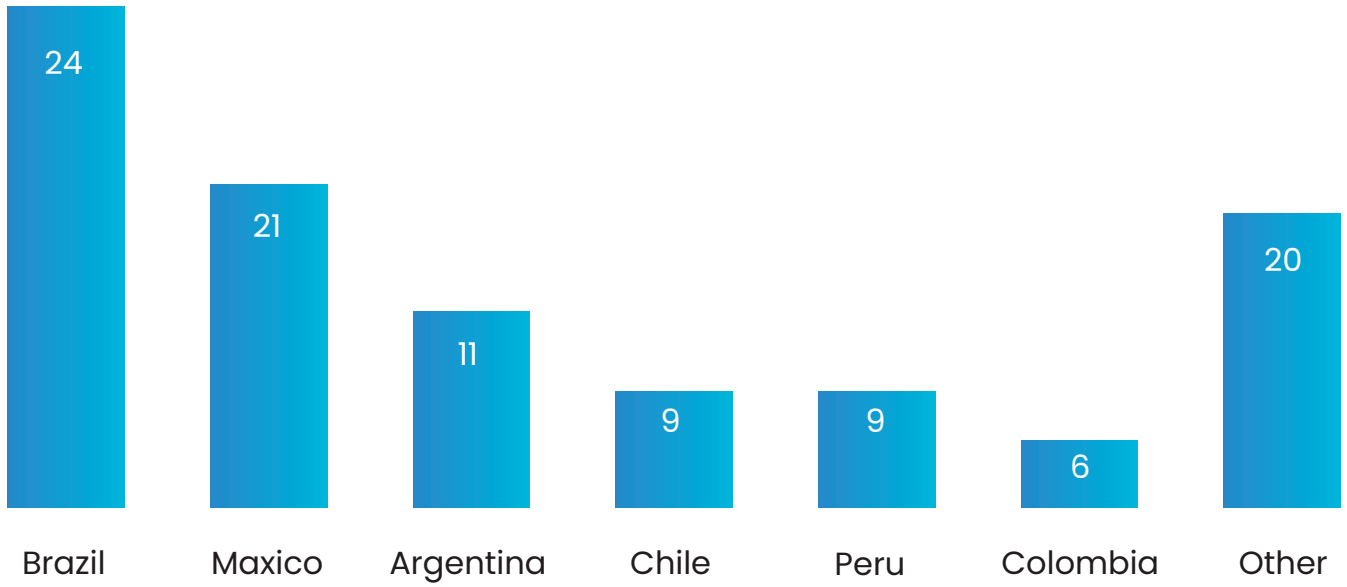
Concurrently, there has been a notable rise in low- and mid-sophistication attacks such as credential harvesting, business email compromise (BEC), and phishing campaigns aimed at both public and private sector entities. The prevalence of these techniques suggests that threat actors are not only seeking immediate financial gain but are also establishing persistent access footholds for future strategic exploitation.

Attacks on regional critical infrastructure

Threat actors targeting ICS environments in the region typically exploit a combination of architectural weaknesses, unpatched CVEs and cyber hygiene gaps. A prevalent initial access vector involves scanning for internet-exposed ICS assets—especially HMIs and SCADA interfaces—often lacking proper authentication, encrypted communications, or network segmentation. Unpatched firmware, default credentials, and improperly air-gapped networks further increase attack surfaces. Once access is obtained, adversaries may manipulate process parameters (e.g., altering pump speeds, disabling alarms, or modifying chemical dosing rates), disable safety interlocks, or cause unauthorized equipment shutdowns. In more coordinated attacks, lateral movement through flat network architectures allows for broader disruption and persistence.

The use of multiple and commonly used ICS platforms and vendors across facilities also introduces a unique monoculture risk – that of such systems that are vulnerable yielding to a domino attack. Successful exploits developed for one system can often be reused or slightly modified to compromise similar environments elsewhere. As demonstrated in many regional campaigns, threat groups are increasingly leveraging open-source intelligence (OSINT), automated scanning tools, and customized ICS malware to carry out opportunistic and ideologically motivated attacks. This evolution emphasizes the urgent need for sector-specific hardening, real-time monitoring, and cross-domain threat intelligence sharing to mitigate risks to critical infrastructure.

Most Attacked Nations in South America



Brazil has emerged as the most attacked country in the region closely followed by Mexico. In addition to their strategic geographic presence, both nations are home to multiple industries of economic significance for the whole region (in addition to North America as well since many supply chains that emerge in these two nations ends up in USA and Canada). The next two Argentina and Chile are significant from a financial standpoint in addition to being among the largest producers of Lithium in the world.

Surprisingly, some patterns of the attack we have logged in Argentina, Chile, and Bolivia to some extent have also been logged in some parts of Australia which is another major producer of the same set of minerals. Cyberattacks on oil and gas entities in Mexico and Brazil have already been correlated with those of other OPEC countries in the last edition of our Threat Landscape Report. This year, we were able to do a much deeper dive into cyberattack correlations and found that a set of threat actors including a few state-backed actors are behind cyber attacks on the commodity sector. Such attacks target the entire value chain including extraction, processing, trade, shipping and buying entities.

On the critical infrastructure side, utilities and ports are among the most attacked targets in South America.

Reasons behind the increasing number of successful cyberattacks in the region

- Hackers are using the region to train bigger groups of hackers

- The number of citizen-facing services that have been digitized has grown exponentially since the pandemic years and this has led to a vast increase in the volume of unsecured threat surface in the region.
- The emerging state of cybersecurity policy and deficiency of institutional response mechanisms
- Hackers interested in manipulating the prices of minerals are keeping an eye on the region
- Growing number of botnets in the region comprising of hijacked devices with poor security

Dismantling the botnet infrastructure in the region along with the adoption of basic cyber hygiene practices could go a long way in reducing the volume of successful cyberattacks In terms of the attacks on IoT projects, the region didn't show much of a deviation from the global average. This once again indicates the involvement of threat actors that are using AI or some form of automated attack generation applications and infrastructure to carry out these attacks.

Regional convergence in threat activity

Notably, forensic and telemetry analysis from recent campaigns revealed that several attack patterns observed across Argentina, Chile, and Bolivia—particularly those targeting critical mineral supply chains—mirror tactics, techniques, and procedures (TTPs) also logged in parts of Australia, another major producer of lithium, copper, and rare earth elements. This geographic overlap in TTPs suggests a coordinated or copycat operational model, likely targeting commodity-producing nations to achieve economic disruption, strategic espionage, or financial manipulation.

Further, cyberattacks on oil and gas entities in Mexico and Brazil have shown strong tactical and infrastructural correlations with intrusion sets previously documented in other OPEC-aligned countries, as noted in the previous edition of our Threat Landscape Report. In 2024, deeper threat correlation analysis and infrastructure clustering allowed us to attribute many of these intrusions to a defined group of adversaries—some with known or suspected ties to state-sponsored entities. These threat actors are targeting the entire commodity value chain: from upstream extraction and midstream processing, to downstream trade, logistics (including maritime shipping), and procurement platforms. Techniques observed include supply chain compromise, targeted spear-phishing of logistics managers and traders, manipulation of market-relevant telemetry data, and ransomware campaigns aimed at halting physical operations.

Persistent targeting of critical infrastructure

On the cyber-physical front, critical infrastructure such as utilities and maritime ports remain among the most frequently targeted sectors in South America. Electric power distribution networks, water utilities, and port management systems have been hit by both opportunistic ransomware and more targeted ICS-specific threats. Several incidents included lateral movement from IT to OT environments via improperly segmented networks or poorly configured remote access tools—an attack pathway still prevalent in the region.

Factors driving increased attack volumes in South America

Several interlinked factors contribute to the growing frequency and success rate of cyberattacks in the region

Adversary training grounds

There is growing evidence that certain adversary groups—especially ransomware operators and cybercrime-as-a-service (CaaS) entities—are using South America as a live-fire environment to train and iterate their tools, techniques, and affiliates before deploying them in higher-security markets.

Post-pandemic digital expansion

The rapid and unregulated expansion of digitized, citizen-facing services since the COVID-19 pandemic has exponentially increased the exposed digital footprint. Many services lack adequate encryption, identity verification, and access controls, leaving significant surface area for exploitation.

Evolving cybersecurity governance

The lack of mature national cybersecurity policies, limited sector-specific regulations, and weak institutional response capabilities (e.g., underfunded CERTs and CSIRTs) further amplify the risk landscape.

Strategic economic espionage

Threat actors with an interest in manipulating global mineral pricing and supply chain integrity are actively surveilling and intruding into South American mining ecosystems. These efforts may involve long-term access operations rather than immediate disruption.

Rise in regional botnet infrastructure

An increasing number of compromised IoT and legacy devices with poor or no security configurations are being absorbed into botnets used for credential stuffing, DDoS, proxy relay, and malware delivery campaigns.

Disrupting regional botnet infrastructure—through coordinated takedowns and international cooperation—alongside the widespread adoption of baseline cyber hygiene (e.g., MFA, regular patching, and network segmentation) could drastically reduce the attack surface and incident success rate.

From an IoT security perspective, the region's incident rate aligned closely with global averages in 2024. This consistency suggests that many of the IoT attacks were conducted using automated platforms powered by AI-driven attack generation or machine-learning-optimized scanning infrastructure. These platforms do not discriminate by geography but target devices based on exposure, misconfiguration, or known vulnerabilities—further indicating that threat actors are increasingly automating the reconnaissance and exploitation phases of their campaigns.

Europe

The Russia-Ukraine conflict continues to exert significant influence on cyberspace across Europe. As of November 2023, the region has witnessed an unprecedented and sustained phase of advanced persistent threat (APT) activity lasting over two years. With the kinetic conflict showing signs of entering a protracted or "frozen" state, Russian APT groups have escalated their cyber operations, using the digital domain to sustain strategic pressure on both Ukraine and its allies.

This heightened threat environment is not limited to traditional players. Alongside established Russian APT groups, threat intelligence reports have confirmed operational visibility of new threat actors from Iran and two Turkish APTs. These actors have broadened the threat matrix, targeting both governmental and private-sector organizations across a wide range of industries.

Unlike earlier campaigns in 2022 and 2023—where urban centers hosting NATO assets were prioritized—2024 saw a strategic shift toward more distributed and sector-specific targeting. APT operations extended deeper into national infrastructure networks, economic sectors, and civilian service platforms.

Indicators of escalation in 2025

Threat correlation and behavioral analytics strongly suggest that APT actors are laying the groundwork for large-scale operations in 2024. This assessment is based on several converging indicators

Increased Targeted Reconnaissance and Lateral Movement

across all EU member states, particularly those with critical infrastructure tied to defense, finance, and manufacturing.

Surging Demand for Infrastructure Intelligence

on dark web and illicit forums, particularly regarding utility grids, transport systems, and data exchange nodes.

Multiple Confirmed Breaches

involving data exfiltration, likely enabling persistent surveillance and situational mapping of high-value targets.

Widening Threat Footprint

across banking, governance, e-mobility, EV charging infrastructure, healthcare, and education—suggesting prepositioning for systemic disruption.

A Record Number of New Malware Variants

specifically built or adapted for European systems, highlighting heightened attacker investment in the region.

Sectoral focus and adversarial intent

The manufacturing sector has emerged as one of the highest-value targets, with attacks characterized by high persistence, multi-stage compromise, and deliberate sabotage intent. The sophistication of intrusion sets—often leveraging zero-day exploits, firmware-level persistence, and supply chain compromise—points to well-funded actors with defined strategic goals.

The Israel–Hamas conflict has also catalyzed cyber spillover into Europe. Since late October 2023, a surge in activity by hacktivist groups—including those based within Europe—has been observed. These groups prioritize high-impact, high-visibility targets such as oil and gas, public utilities, and transport infrastructure. Their operations are increasingly coordinated and involve multi-channel surveillance (technical, social, and open-source), creating what can be described as multi-tier digital containment frameworks for their targets.

Interestingly, these sectors—oil & gas and utilities—have become a convergence zone for APT actors, financially motivated cybercriminals, and ideologically driven hacktivists, often working in parallel, if not in direct coordination.

China strategic industrial espionage

Chinese APTs have intensified their cyber operations targeting European manufacturers, with a focus on intellectual property theft. On average, a single successful breach results in the exfiltration of upwards of 97,000 data records, often involving proprietary research, engineering blueprints, or manufacturing process data.

Germany remains a prime target due to its concentration of high-tech firms involved in semiconductors, renewable energy, defense, space, and automotive innovation. These cyber intrusions align with China's broader geopolitical strategy of accelerating domestic innovation by acquiring foreign IP—an approach that blurs the line between economic competition and digital warfare.

China's operations span multiple organizational layers

- Private sector front companies
- Freelance and contracted cyber operatives
- University-affiliated researchers
- State-owned enterprises with embedded collection mandates

This layered architecture offers operational redundancy and plausible deniability. Should an asset be compromised, only a fragment of the broader campaign is exposed—limiting operational fallout.

Chinese threat actors also extend their targeting to individuals, including

- Exiled Uyghur and Tibetan activists

- Patent holders and innovators with dual-use technologies These intrusions are often politically motivated, supporting broader state objectives in both internal suppression and strategic advancement.

North Korea financial and technological warfare

North Korean cyber operations in Europe are primarily driven by three objectives

Monetary Gain

Through ransomware, cryptocurrency heists, and extortion schemes aimed at replenishing foreign currency reserves amidst tightening sanctions.

Technology Acquisition

Targeting European universities, aerospace firms, and nuclear technology supply chains to support its defense programs.

Strategic Messaging

Using exfiltrated data to bolster its bargaining position and project technological parity or superiority to both regional and global adversaries.

Forum analysis linked to DPRK threat actors reveals deep concerns over

- Potential degradation of its defense infrastructure through Western coalition cyber or kinetic strikes
- Systematic exclusion from technological ecosystems due to sanctions
- Total economic collapse if current sanctions are maintained or escalated

Cyberattacks emanating from North Korean infrastructure are thus designed to address all three risks by conducting

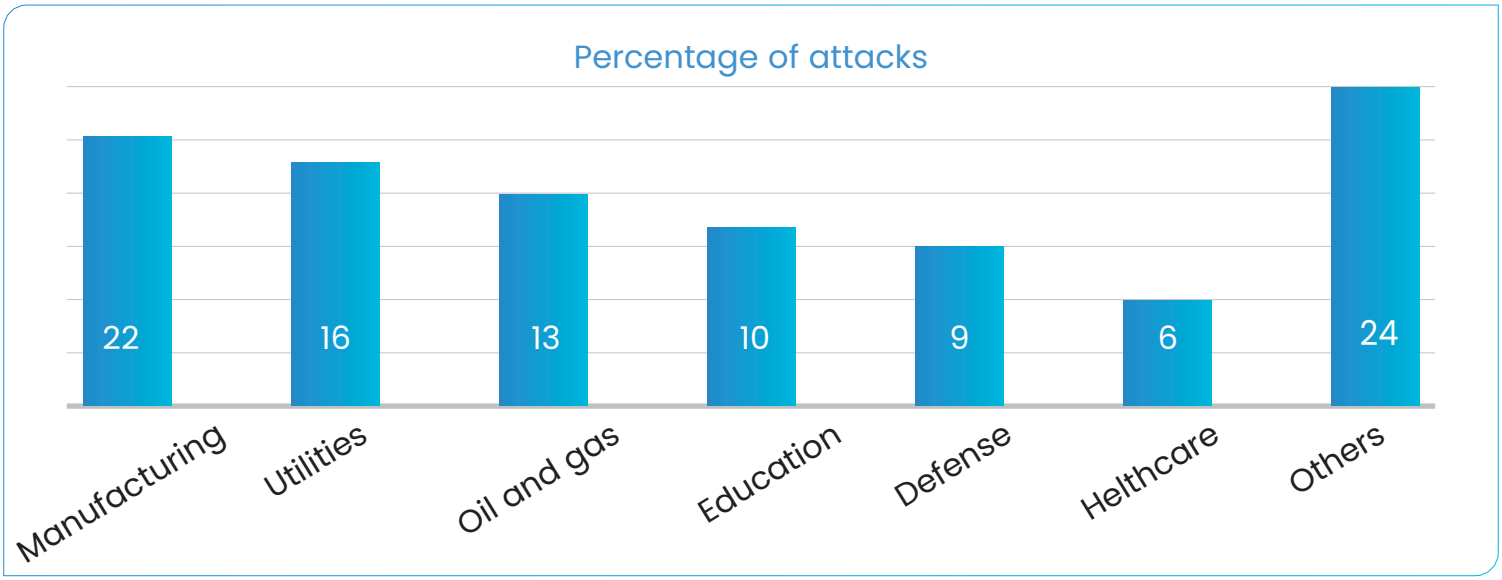
- Espionage operations for defense R&D

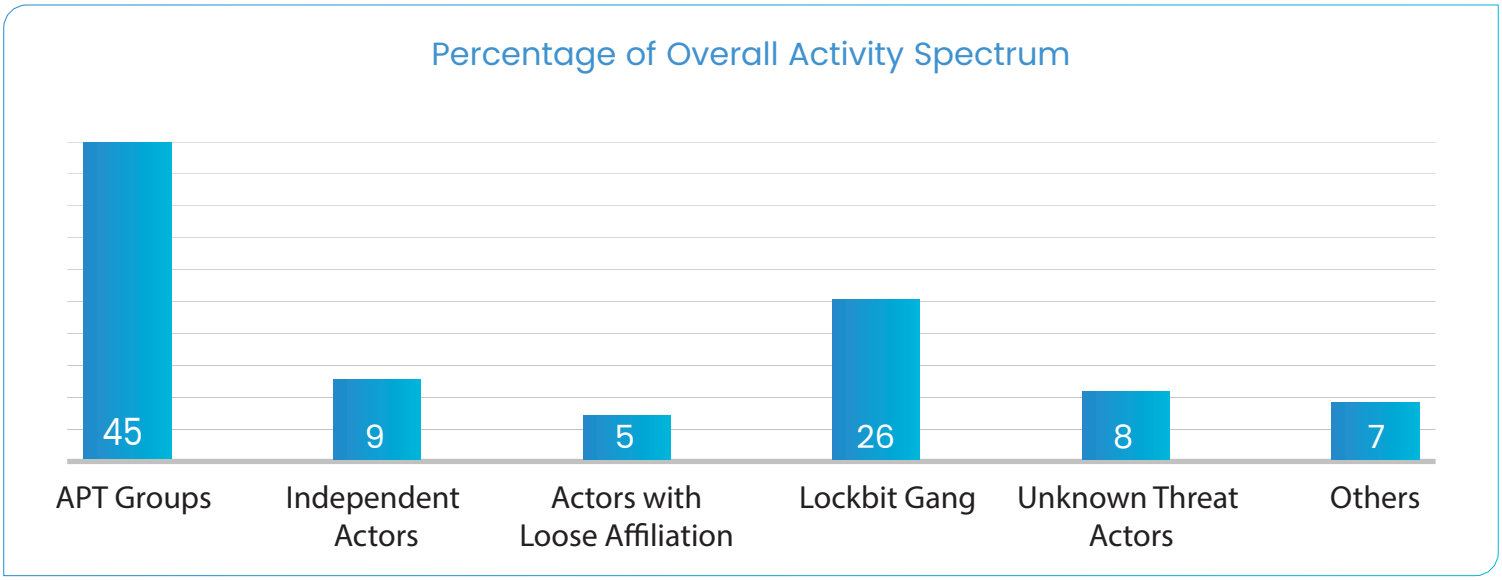
- Illicit digital asset transfers (e.g., crypto laundering)
- Cyber extortion and disinformation campaigns

To Pyongyang, the European Union is not just an economic target—it is viewed as an extension of the U.S.-led threat matrix and is treated as such in its cyber operations.

Outlook

The cyber threat landscape in Europe for 2025 is expected to remain volatile and complex, with increasing convergence between strategic, economic, and ideological adversaries. Multi-vector campaigns involving APTs, cybercriminals, and hacktivists will continue to test the resilience of Europe's digital infrastructure, particularly in sectors critical to national security and economic stability.





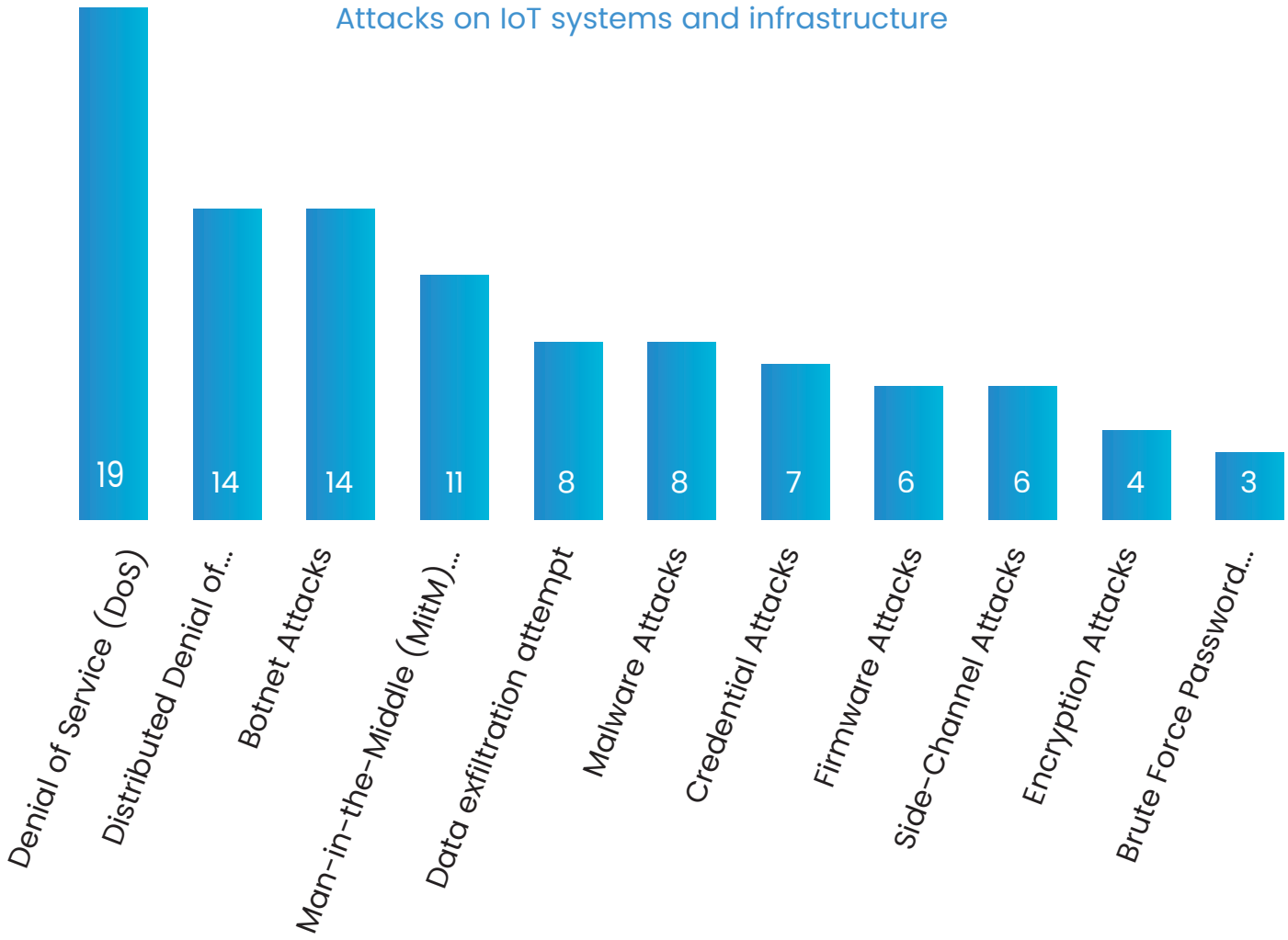
Where are the cyber threats to Europe coming from?

Country of origin	Main actors	Percentage
Russian	1	3
China	2	6
Iran	3	-
Turkey	4	-
Pakistan	5	5
North Korea	6	-
Others		34

Most attacked countries

Country	Rank
United Kingdom	1
France	2
Ukraine	3
Germany	4
Finland	5

France and the UK are drawing a huge volume of sophisticated attacks on their manufacturing infrastructure linked to defense. While Ukraine is in the third position, attacks on Ukraine rose by as much as 371 percent in 2023 which is more or less aligned with the growth in cyberattacks we registered in Ukraine in 2022. Ukraine, Lithuania, and Finland top the list of most attacked nations in Europe on a per capita basis.



In addition to DoS and DDoS, Europe is also witnessing a large volume of attacks designed to steal data.

The Indo-Pacific region - a growing cyber threat theatre

The Indo-Pacific region encompasses 40 countries and economies, including Australia, Bangladesh, Bhutan, Brunei, Cambodia, the Democratic People's Republic of Korea (DPRK), India, Indonesia, Japan, Laos, Malaysia, Maldives, Mongolia, Myanmar, Nepal, New Zealand, the Pacific Island Countries, Pakistan, the People's Republic of China (PRC), the Philippines, the Republic of Korea (ROK), Singapore, Sri Lanka, Taiwan, Thailand, Timor Leste, and Vietnam. Indo-Pacific is home to some of the most sophisticated threat actors including those from China, North Korea, Iran and Pakistan.

This region is rapidly emerging as a geopolitical flashpoint, with China's assertive actions—both physical and cyber—reshaping regional threat dynamics. Beyond territorial disputes and maritime encroachments, China is weaponizing cyberspace to advance its national objectives, secure its global narrative and to curtail the growth of its adversaries.

China also exerts heavy digital surveillance across its sphere of influence, including extensive monitoring of strategic partners like Pakistan. Chinese state-backed threat actors have targeted India's power infrastructure, with operations often routed through compromised IPs in countries such as Vietnam, Thailand, Cambodia, Brunei, and Slovenia—masking origins while exploiting third-party infrastructure. Similar tactics have been used in attacks on critical infrastructure in Australia and South Korea.

In parallel, Pakistani group APT36 (also known as K-2) continues to evolve, transitioning from targeting Indian critical infrastructure websites to launching multi-phase reconnaissance attacks. These intrusions appear designed to maintain persistent access, ready to be activated during geopolitical tensions or as instruments of economic pressure.

China's cyber investments are concentrated on building four core capabilities

- Intercepting and analyzing high-value communications
- Disrupting critical civilian infrastructure to impair crisis response capacity
- Sustaining long-term surveillance of geopolitical targets
- Maintaining a steady tempo of low-intensity cyberattacks during diplomatic friction

China's doctrine appears to favor "keeping cyberspace warm"—aggressive enough to exert pressure, but calculated to avoid triggering open cyber conflict.

Our threat intelligence indicates that countries participating in China's Belt and Road Initiative (BRI) are somewhat less likely to be targeted by disruptive cyberattacks. However, this does not shield them from pervasive surveillance campaigns. China's APT groups are also improving operational stealth and evasion, complicating attribution efforts for security analysts.

In 2024, China's cyber posture in the Indo-Pacific region became more aggressive, deliberate, and tactically refined—particularly in its targeting of critical infrastructure and cyber-physical systems (CPS). With growing geopolitical tensions over Taiwan, the South China Sea, and expanding security alliances like the Quad and AUKUS, the Chinese state escalated its use of cyberspace as a tool of coercion, disruption, and strategic espionage.

Surge in attacks on critical infrastructure

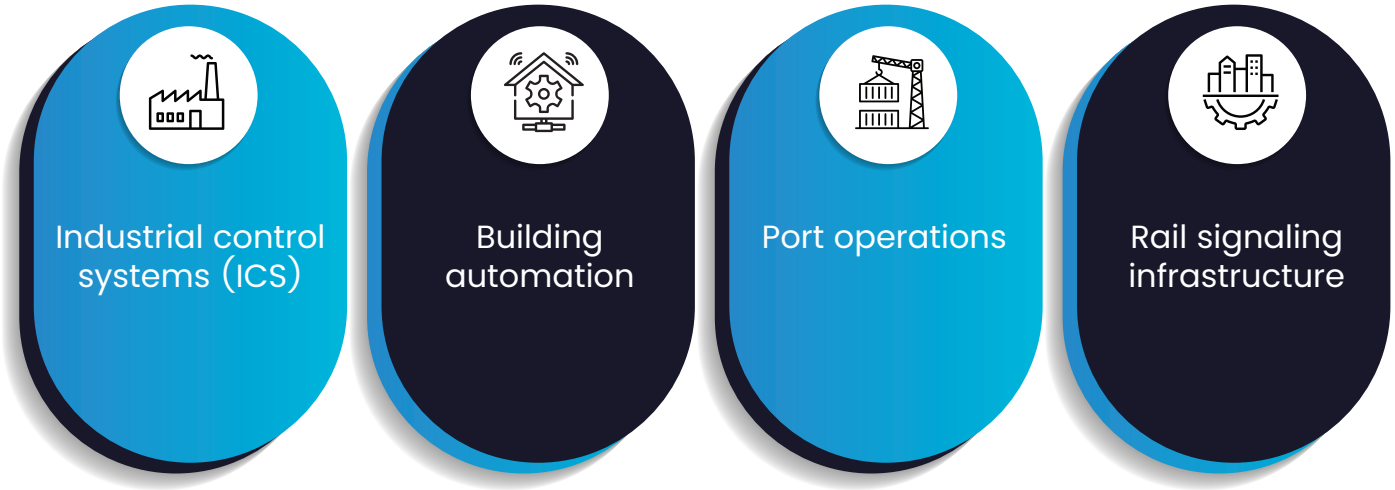
Chinese state-backed Advanced Persistent Threat (APT) groups such as APT41, APT27, and RedEcho significantly expanded operations targeting critical infrastructure across the Indo-Pacific. These attacks were no longer limited to reconnaissance or data exfiltration—they increasingly included pre-positioning of malware in operational environments, enabling potential disruption during times of crisis.

Key sectors targeted

- Power grids and energy distribution in India, Vietnam, and Australia
- Telecommunication infrastructure in Taiwan, the Philippines, and Papua New Guinea
- Water treatment facilities and transport control systems in South Korea and Malaysia

In India, a notable campaign attributed to APT41 targeted the supervisory control and data acquisition (SCADA) systems of state-owned power utilities. The attackers deployed modular malware capable of silently observing operations and uploading encrypted payloads for future command-and-control (C2) activation. While no kinetic disruption was observed, the breach demonstrated China's intent to retain the option of degrading India's critical services during periods of elevated tension.

Chinese APTs have also turned their attention to cyber-physical systems, which bridge IT and operational technology (OT). Throughout 2024, threat activity focused on



In Southeast Asia, ports in Singapore and Vietnam reported anomalous behavior in logistics management systems, which investigators later traced to malware with code similarities to tools used by a known Chinese APT. These operations appeared aimed at gathering intelligence on shipping schedules and creating latent disruption capabilities in logistics chokepoints.

In South Korea, Chinese actors probed the firmware of smart sensors used in high-speed rail networks—an early indication of interest in manipulating real-world processes. These campaigns show a growing interest in blending cyber and physical effects, where control system tampering could have real-world safety or economic consequences.

Targeting of Government Institutions

In parallel, Chinese cyber campaigns in 2024 stepped up espionage efforts against government ministries, defense agencies, and diplomatic missions across the Indo-Pacific.

Confirmed or strongly suspected intrusions included

- Ministry of Defense servers in Australia and Japan
- Foreign Affairs and Intelligence services in Taiwan and Indonesia
- Defense Research Organizations in India and Malaysia

In Taiwan, Chinese actors deployed custom backdoors hidden in compromised Microsoft Exchange servers. These backdoors allowed long-term access to sensitive policy and defense planning documents. Taiwanese investigators found strong evidence of lateral movement toward systems managing national critical infrastructure assessments.

In Indonesia, a multi-month campaign was uncovered targeting the Presidential Office's IT department. It involved the deployment of credential harvesting tools, extensive email surveillance, and attempts to map the country's secure government communications infrastructure.

In Australia, the Home Affairs department confirmed a breach linked to China's APT40, aimed at gathering data on immigration enforcement and maritime patrol planning in the Pacific—a region where Beijing has been aggressively courting influence.

evasion and attribution tactics

Throughout 2024, Chinese cyber units demonstrated increasing operational maturity. Their attacks featured

- Multi-jurisdictional routing of traffic to obscure origin
- Use of third-party infrastructure in neutral countries
- Fileless malware and memory-only implants
- Living-off-the-land (LotL) techniques using native tools like PowerShell and WMI

Notably, Chinese operators expanded the use of AI-generated decoys in phishing and social engineering, including deepfake videos of officials, synthetic job offers, and fake security alerts—increasing initial access rates across government and critical infrastructure organizations.

Strategic Intent and Future Outlook

The pattern of targeting suggests a clear intent: to gain persistent, stealthy access to the region's most sensitive and mission-critical systems—ensuring that China can gather intelligence, exert economic pressure, and, if needed, disrupt the capabilities of adversaries during crises.

While direct disruption has been minimal so far, 2024 has shown that China is laying the technical groundwork for a digital battlefield—preparing access points that can be weaponized swiftly if geopolitical tensions escalate.

As the Indo-Pacific nations continue to digitize their critical services and defense postures, China is positioning itself as both a watcher and potential saboteur—exploiting the region's uneven cyber maturity, fragmented security policies, and growing attack surface.

A complex and escalating threat landscape

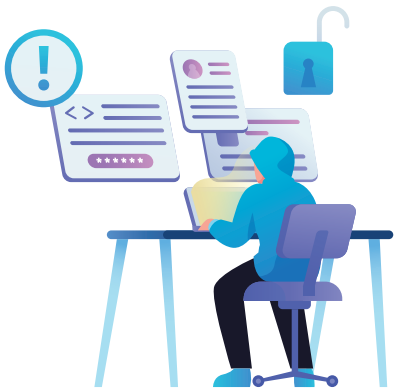
The Indo-Pacific, much like Europe, has become a proving ground for advanced cyber threats and emerging malware strains. In fact, it registered the highest surge in cyberattack volumes in 2023. Multiple factors contribute to this vulnerability

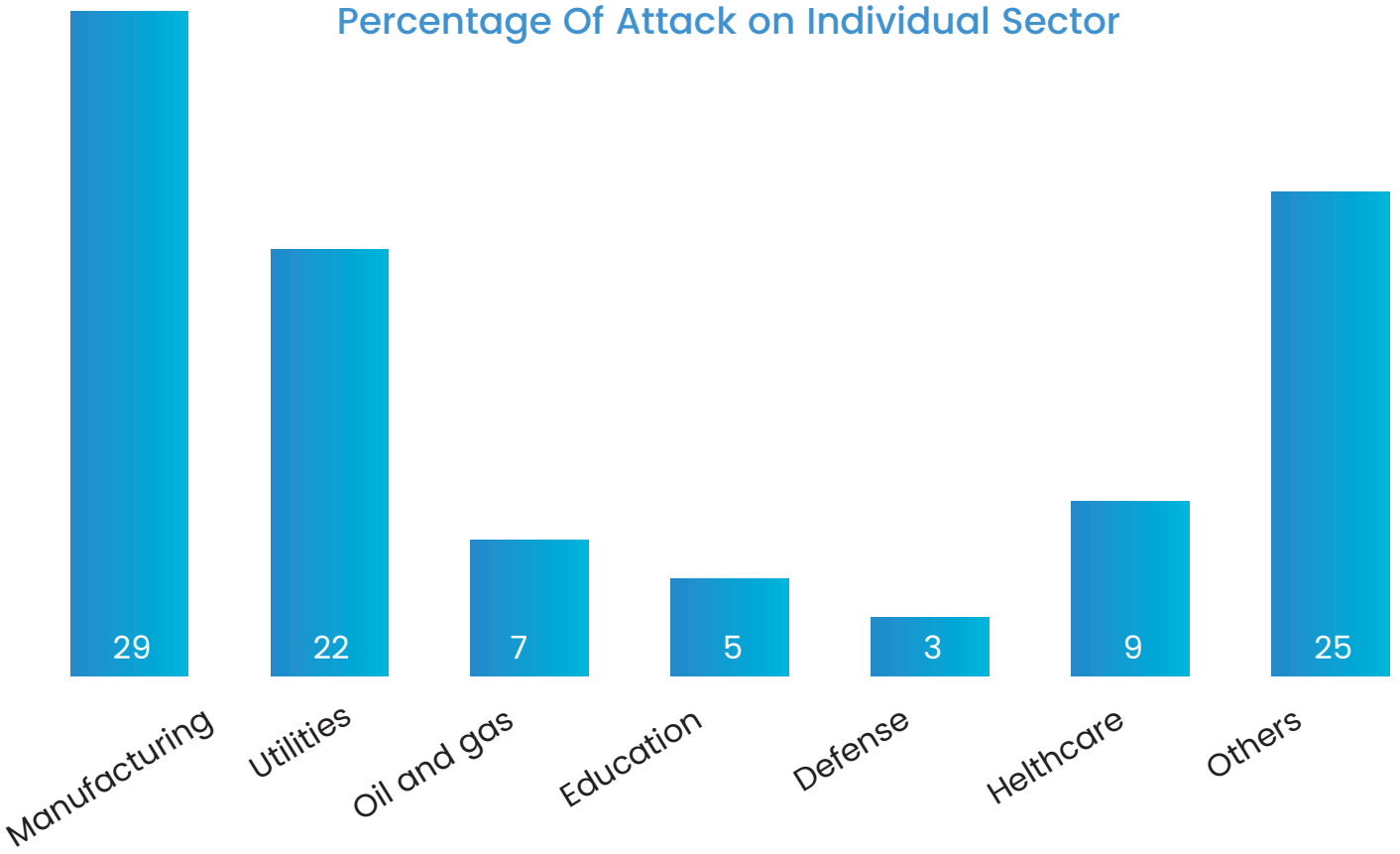
- Lack of clear OT cybersecurity policies and regulations
- Limited visibility and control in industrial environments
- Poor patch management discipline
- Infrequent security audits and risk assessments
- Absence of detailed documentation on plant architecture
- No standardized security testing before deploying new industrial equipment
- Continued reliance on unsecured legacy systems

Sectoral threat focus

The manufacturing sector tops the list as the most attacked vertical in the Indo-Pacific. However, when clubbing together utilities, oil and gas, and defense under the critical infrastructure umbrella, this segment accounts for roughly 32% of all attacks in the region. The maritime sector also deserves attention, comprising nearly 6% of all cyberattacks—a significant figure considering the region's vital role in global shipping and commerce.

Manufacturing plants in the region increasingly incorporate connected machinery running on legacy systems, Operational Technology (OT), and the Internet of Things (IoT). While digitization has advanced rapidly, cybersecurity posture has not kept pace. This has created exploitable security gaps. Threat actors are leveraging these vulnerabilities to infiltrate shop-floor systems, pivot into corporate networks, and deploy malware or exfiltrate sensitive data.





In terms of the threat actors that are active in the region, APT groups and Lockbit affiliates dominate the landscape. We feel that the 'unknown' and 'others' category also contain threat actors with state affiliations. Chinese threat actors also maintain a very high level of active interest in surveilling other threat actors in the region.

Attacks on countries

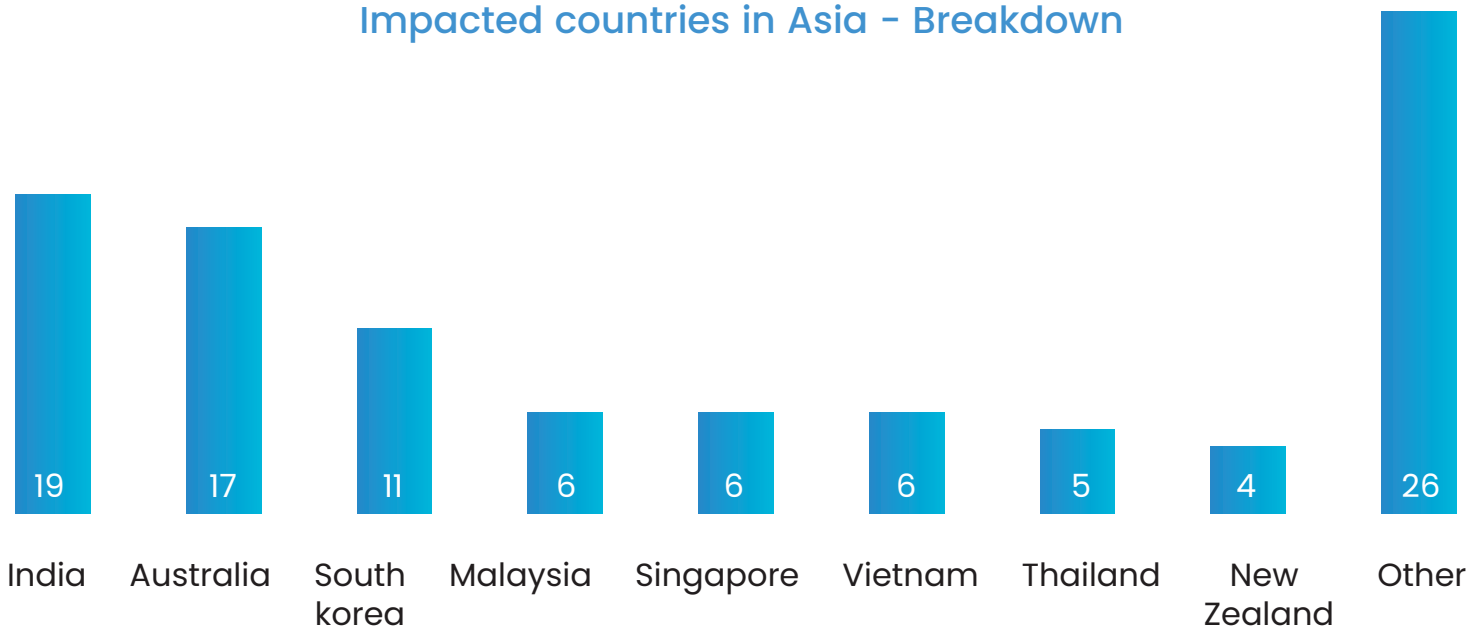
India, Australia and South Korea are among the most attacked countries in the region. It is the critical infrastructure in these countries that is getting attacked at volumes and scale that have made them top the ranks. India faces attacks from both China and Pakistan. The attacks from China target utility companies, defense entities and manufacturers while Pakistan through two actors is attacking India's armed forces, government departments, and research organizations.

A high volume of attacks from Pakistan are targeted at websites as well. The attacks from Pakistan may be a distraction intended to keep Indian security planners away from sectors and targets of interest to China. In the past, we have seen at least two instances of collaboration between Chinese and Pakistani threat actors. The latest instance of this was during the month of September when a summit of G 20 leaders was organized in New Delhi. In the days leading up to the summit, Indian cyberspace was targeted by actors from Pakistan and China. While actors from Pakistan were mostly working to deface

websites, Chinese threat actors targeted Indian critical infrastructure, especially in the country's capital where the summit was taking place.

From a preliminary round of forensic analysis and TTP tracking, we were able to conclude that these attacks were planned well in advance to coincide with the summit. The attacks were conducted at a much larger scale than planned possibly because China decided not to participate in the event which made things easier for the hackers to go all out in attacking diverse targets in India.

South Korea is witnessing a high volume of attacks against its manufacturing infrastructure and government bodies. The attacks are seasonal but of very high quality. Primarily, South Korea is targeted by China and North Korea which is also the case with Malaysia, Singapore, Vietnam, and Thailand. These countries are also targeted through huge volumes of business email compromise attacks as well.



Middle East and Africa

In 2024, the Middle East experienced a sharp escalation in cyberattacks, with threat actors focusing heavily on critical infrastructure, cyber-physical systems, and government networks. The region's strategic importance, coupled with rapid digitization, geopolitical volatility, and ongoing regional conflicts, has made it a high-priority target for both state-sponsored actors and cybercriminal groups.

Critical Infrastructure Under Sustained Attack

Energy production and distribution, water management systems, transportation, and financial services remained top targets throughout the year. Major oil-producing nations such as Saudi Arabia, the UAE, Iraq, and Qatar saw repeated cyber campaigns aimed at breaching and surveilling their national infrastructure.

Notable attack vectors included

- Ransomware and wiper malware targeting oil refineries and logistics systems
- ICS-focused malware designed to disrupt SCADA and PLC environments in power and desalination plants
- Credential harvesting and supply chain compromise involving contractors and IT vendors servicing government-linked infrastructure

One of the most significant incidents involved a ransomware variant with destructive capabilities deployed against a national oil company's data center in the Gulf. The malware not only encrypted business data but also disabled multiple operational control systems, briefly disrupting oil loading schedules at one port.

Iran-based groups such as Charming Kitten and Agrius, as well as suspected Russian-speaking criminal syndicates, were linked to attacks targeting energy and logistics infrastructure in the UAE, Bahrain, and Oman. These campaigns often combined phishing, watering hole attacks, and zero-day exploits against industrial software.

Exploitation of Cyber-Physical Systems (CPS)

The region's accelerating adoption of smart infrastructure and industrial IoT (IIoT) has created a growing attack surface. In 2024, cyber actors increased their focus on

- Smart grid systems and remote monitoring of electrical substations
- IoT-based building automation in airports and industrial zones
- Autonomous oilfield sensors and drone telemetry systems

In Kuwait and Egypt, attackers targeted smart metering infrastructure, seeking to manipulate energy billing and siphon operational data. In several cases, compromised IoT devices such as smart valves and SCADA-linked pressure sensors were discovered to be transmitting data to external C2 servers located outside the region.

In the Red Sea corridor, cyber actors linked to Iranian and pro-Houthi groups probed maritime port systems and container tracking software, likely in an effort to create digital pressure points during regional tensions.

Government Networks and Political Espionage

Government entities—particularly ministries of foreign affairs, defense, and interior—saw a surge in political cyber espionage campaigns. Threat actors from Iran, Turkey, Israel, and China, along with independent mercenary hacking groups, were involved in these intrusions.

Tactics observed included

- Credential theft from diplomats and senior civil servants
- Supply chain compromises involving government IT service providers
- Fake news campaigns launched via social media hijacks or embedded in state websites

In Jordan, a major breach in the Ministry of Defense was traced back to a campaign that used deepfake voice impersonations in spear-phishing calls. Meanwhile, Lebanon and Iraq reported backdoor deployments in government procurement systems, likely aimed at long-term surveillance and corruption of digital workflows.

Several Gulf nations experienced wiper malware attacks targeting judicial and law enforcement networks, designed to erase records and create systemic delays. These were often accompanied by disinformation campaigns to amplify political instability or unrest.

Emerging trends and tactical shifts

- Loiterware and dormant implants: Increasing use of malware that remains undetected and inactive for months, signaling intent to activate during periods of political crisis.
- Use of AI to evade detection: Adversaries began deploying AI-enhanced evasion tools, including polymorphic malware that changes signatures to bypass traditional defenses.

Cross-border infrastructure probing: Many attacks originated from one Middle Eastern country but used compromised infrastructure in neighboring nations to obscure attribution.

Compromise attempts logged

Type	Percentage occurrence*
VPN exploit	12
CCTV feed exfiltration	8
Connected device manipulation (remote)	4
Workstation RAT injection/scans	11
IoT device manipulation	2
Spear phishing	6
Phased DDoS (inbound)	7
Data exfiltration through rogue devices and twining	2
Insider targeting	15
Brute force email compromise	1
Safety instrumentation modification	6
Code injection attempts	5
Reconnaissance (long term)	21
*As a total of the overall attacks logged	100

What is getting attacked?

Sector	Percentage
Utilities	31
Manufacturing	31
Oil and gas	14
Financial services	6
Government	6
Healthcare	6
Others including Not for Profit bodies	7

Motivation factor for bad actors

Factor	Percentage
Geo-political intent	71
Monetary considerations	13
IP/Data Theft	10
Rogue insider	3
Unknown	3

Top APT groups in the region

Name(s)	Country of origin	Target countries
APT 34 OilRig, Helix Kitten, GreenBug, IRN2	Geo-political intent	71
APT 35 Newscaster, Rocket Kitten, Phosphorus, Charming Kitten, Saffron Rose	Monetary considerations	13

APT 39 – Chafer	Iran	Middle East
APT 41	China	Middle East
APT 28	Russia	UAE, Saudi, and Egypt

Throughout 2023, Chinese state-affiliated threat actors mounted extensive and strategic campaigns targeting data centers belonging to oil and gas enterprises, financial institutions, and utility providers across the Indo-Pacific. These attacks appear to be driven not only by the pursuit of sensitive data but also by the desire to exploit the strategic network positioning of these facilities—many of which serve as central hubs connecting multiple enterprises, remote assets, and operational networks.

In a review of 15 major attacks investigated by our Threat Research Team during the year, we found repeated instances of infostealer malware and loiterware—malicious tools specifically designed to remain undetected within networks for extended periods, awaiting remote activation based on strategic intent or geopolitical developments.

While oil and gas ranks third in terms of the number of reported cyberattacks, it stands out as the sector most frequently targeted by advanced and persistent threat campaigns These attacks include

- Long-term surveillance operations on core operational networks
- Deep lateral movement across environments to establish durable persistence
- Exfiltration of industrial data and infrastructure schematics
- Insertion of modular malware components that can be remotely updated or configured IoT and firmware-level backdoors

Our investigation uncovered alarming evidence of pre-infected Internet of Things (IoT) devices, many of which were compromised at the firmware level. These devices—especially smart cameras, fire alarms, and connected medical sensors—were found to contain embedded trojans and remote-access backdoors enabling full control by external operators.

This class of attack poses two critical challenges

- Low detection probability: The randomized placement of these backdoors across device batches reduces the chances of discovery during routine vulnerability assessments or device testing.

- Exploitation via AI-driven threat bots: We have identified a rising use of AI-coordinated sequential botnets—clusters of compromised IoT devices that participate in attacks asynchronously. These devices operate across varying IP ranges and attack intervals, making them exceptionally difficult to attribute or detect through conventional monitoring.

This evolving IoT threat landscape significantly amplifies the risks for sectors dependent on Industrial IoT (IIoT) and Internet of Medical Things (IoMT) ecosystems.

Rising threats to smart infrastructure and cps

In parallel, we observed a growing volume of attacks on intelligent subsystems particularly those embedded in smart infrastructure and cyber-physical systems (CPS). These subsystems, which often aggregate and transmit telemetry data from sensors to centralized data lakes, are being routinely scanned from rotating IP addresses—a hallmark of reconnaissance activity by advanced actors.

In projects across the energy, transportation, and construction sectors, the deployment of IoT gateways has introduced new vulnerabilities into legacy infrastructure. The increased integration of these gateways into critical power and backup systems is degrading the security posture of the broader infrastructure stack, offering new ingress points for attackers.

Systemic attacks in the region

System	Percentage attacks
IT-OT	40
IT-IoT	19
IIoT	14
IoMT	8
Others	19

Most attacked countries in the region

Country	Rank
UAE	1
Saudi Arabia	2
Oman	3
Kuwait	4
Egypt	5
Nigeria	6
Kenya	7

On a per capita basis, Kuwait was the most attacked country in the region. Kuwait drawing a disproportionate volume of attacks is chiefly due to the presence of facilities connected with the oil and gas sector.

Targeted attacks on utilities and oil and gas

Attacks on oil and gas and the utility sector in the region target almost all aspects of operations in these two sectors. Repeated incursions designed to cause sub-kinetic physical disruption in 2020 have now turned into more complex attacks designed to control sub-systems and use that control to unleash mayhem. Many of these attacks were discovered because of sheer carelessness on the part of the hacker. For instance, during one episode, the hacker (Witchetty group AKA APT 10) coded the wrong activation time for the vector to perform file and directory actions possibly due to a time zone difference and the malware was triggered during work hours and the anomalous activity was detected and neutralized. In another case, the C&C server address was wrong.

One is not sure why an actor as mature as APT 10 did these mistakes. But there is certainly a need to rapidly improve security practices in the region else we may see some of these attacks evolve and create more disruption and chaos, especially in the oil and gas sector where such attacks could also be coupled with airborne strikes by drones to create an even bigger impact. In the utility sector, bad actors are working to shut down critical systems and subsystems at will and to time such shutdowns to geopolitical triggers.

References

1. https://time.com/6550920/world-elections-2024/

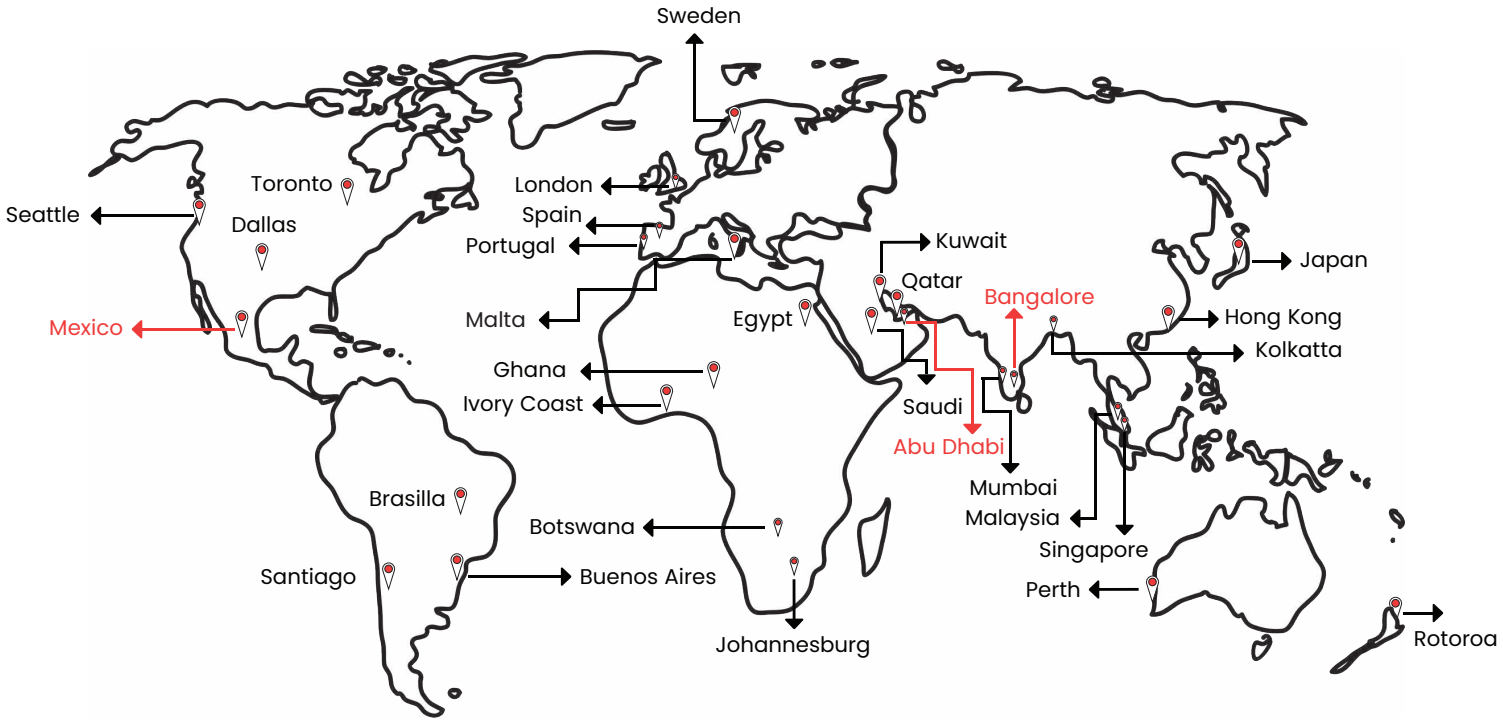
2. https://www.cisa.gov/news-events/cybersecurity-advisories

3. https://www.csis.org/programs/strategic-technologies-programsignificant-cyber-incidents

4. https://www.eia.gov/todayinenergy/detail.php?id=64304

5. https://www.globaldata.com/newsletter/details/cybe atacks-a-growing-threat-for-oil-and-gas-driven-by-geopolitics-extortion_229782/

About Shieldworkz



ISOC and 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.