

EXPOSURE MANAGEMENT

MANUFACTURING THREAT LANDSCAPE 2026



TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
MANUFACTURING INDUSTRY OVERVIEW 2025	4
MONTHLY ATTACK TRENDS	5
MAIN THREAT ACTORS	6
MAIN ATTACK VECTORS	13
EUROPE	14
UNITED STATES	16
BRAZIL	18
CHINA	19
INDIA	20
RECOMMENDATIONS	21
PREDICTIONS FOR 2026	23
CONTACT US	24

EXECUTIVE SUMMARY

In 2025, the manufacturing sector faced a sharp rise in cyber threats, with ransomware incidents targeting the industry up 56% year-over-year, accounting for roughly half of all global attacks. Key drivers included vulnerable legacy OT systems, complex supply chains, and increasingly sophisticated ransomware-as-a-service operations. Major threat actors included Akira, Qilin, Play, Clop, Safepay, NoName057(16), and Chinafans, employing tactics such as ransomware, double extortion, website defacement, supply chain attacks, and AI-enhanced malware.

Regions most affected were the United States, Europe, India, Brazil, and China, with high operational and financial impacts reported across critical manufacturing processes.

Recommendations focus on implementing Zero-Trust architecture, enhancing OT/IT security, strengthening patching and backup strategies, improving employee training, and mitigating supply chain risks. Threats are expected to escalate in 2026, with AI-driven attacks, faster ransomware campaigns, and data theft replacing traditional encryption-focused operations.





MANUFACTURING INDUSTRY OVERVIEW 2025

The industrial and manufacturing sectors have increasingly become prime targets for cyber threats worldwide, with ransomware, data breaches, and supply chain attacks posing the greatest risks.

In 2025, global ransomware incidents surged 32% year-over-year, reaching 7,419 documented cases, while attacks specifically targeting manufacturing rose 56%, increasing from 937 in 2024 to 1,466 incidents. Manufacturing alone accounted for roughly 50% of all ransomware hits, reflecting its high operational criticality and the substantial financial impact of production downtime, which can cost millions per day. The countries most heavily targeted in 2025 included the United States, India, Germany, the United Kingdom, and Canada, highlighting that both mature and emerging industrial economies were exposed.

Key drivers of this trend included the widespread presence of vulnerable legacy operational technology systems, increased reliance on complex supply chains, and the growing sophistication of ransomware-as-a-service operations that enabled threat actors to scale attacks rapidly across multiple regions.

Top 5 Targeted Countries 2025



USA
713



India
201



Germany
79



UK
65

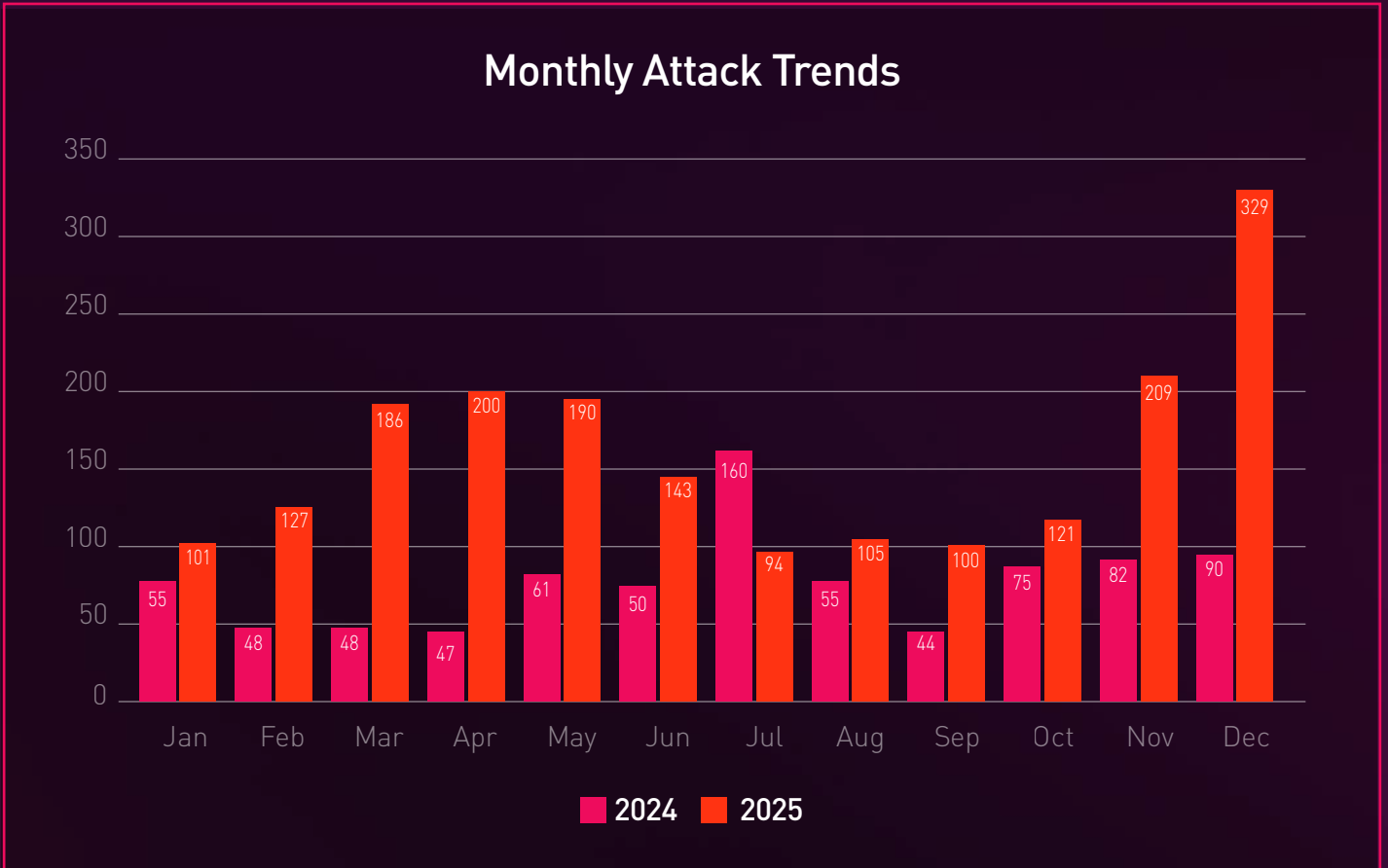


Canada
62

MONTHLY ATTACK TRENDS

In December 2025, the manufacturing sector experienced a noticeable spike in cyber-attack activity, driven by a convergence of year-end operational pressure and attacker opportunism. As manufacturers entered peak production and fulfillment cycles, the financial and operational impact of downtime increased significantly, making organizations more vulnerable to extortion-driven campaigns.

Ransomware groups such as Akira and Qilin intensified targeting during this period, exploiting reduced staffing over the holidays, delayed patching tied to fiscal year transitions, and persistent OT vulnerabilities.





MAIN THREAT ACTORS

Akira

Overview - Akira is a ransomware threat actor group active since March 2023, potentially linked to the defunct Conti ransomware syndicate. It primarily targets small and medium sized businesses but has expanded to larger organizations across sectors including education, critical manufacturing, IT, healthcare, finance, and food/agriculture.

Motives - primarily financial, employing a double extortion model to encrypt data and threaten leaks of exfiltrated information, amassing approximately \$244 million in proceeds by late 2025.

Attack vectors - initial access via VPNs lacking MFA, exploiting CVEs, spearphishing, and RDP.

Notable incidents - In 2025, Akira was involved in a breach at Südkabel, a German cable manufacturer, where 27 GB of data including NDAs, financial records, and employee/customer contacts were exfiltrated, leading to operational disruptions.

Latest IOCs –

MD5	a3bd85eaaa58cec1636d437310c416e8
MD5	97ed9f3ce2f797d92e7104f835bed9c4
MD5	838e852d6730eb31b2a052ef27c6d4f7
MD5	1b09e216fda688b200634cb61db3694e
MD5	a374a3c2bd5e2793afd4a668f50e1123
MD5	6fec53ab6b5a356cc6a53cce75754474
MD5	532c04c73f0d1f07888a61c8cd6eeb0a

MD5	5e9caca257ed66ebab0094fc497c2d19
MD5	3827274b568162409be1dac4d607a662
MD5	d5b8c1cdf094faf3cd74bbaa8f25bc0d
MD5	37bff212fbaa74d5bfc4034ee39275cf
MD5	a26557658ddd4d181eb0d01e78dbe9b3
MD5	71fd1839b927ff4ed094023c944af197

Qilin

Overview - Qilin, also known as Agenda, is a Russia-based ransomware-as-a-service group first observed in 2022, operating through affiliates who use its malware and infrastructure to conduct attacks.

Motives - financial extortion, combining system encryption with massive data theft to pressure victims into paying ransoms, often targeting critical infrastructure for maximum disruption and leverage.

Attack vectors - deploying ransomware for encryption, exfiltrating terabytes of sensitive data, publicly claiming responsibility on leak sites, and scaling operations via affiliates, with a focus on rapid execution post-compromise.

Notable incidents - In 2025, Qilin targeted a manufacturing and logistics firm, stealing 29,843 files including debtors/creditors lists, bank statements, and internal documents, causing potential supply chain disruptions.

Latest IOCs –

IPv4 Address	216.158.229.74
IPv4 Address	188.119.66.189
IPv4 Address	176.113.115.97
IPv4 Address	176.113.115.209
IPv4 Address	85.209.11.49
IPv4 Address	31.41.244.100

MD5	daec53d5a033d22b522d9fa3973ece16
MD5	e4814c8dc3d6d83ecb0ed32bf1d6f593
MD5	a74c5f1022edb72d1cb39381664809b5
MD5	7ba4c93c6142fd6b1b0c34f92deda07a
MD5	c8d43c18b4b451e1722ebb0adbd924b5
MD5	9394e505be0e7a274cd7431abd53aef1





Play

Overview - Play, also called Playcrypt, is a ransomware group active since June 2022, presumed to be a closed operation emphasizing secrecy, with around 900 affected entities reported by the FBI as of May 2025.

Motives - financial, using double extortion to exfiltrate data before encryption and threaten leaks on a Tor-hosted site, demanding cryptocurrency ransoms without initial specifics in notes, and escalating via emails or calls.

Attack vectors - initial access through abused valid accounts, exploited applications, defense evasion by disabling antivirus with GMER/IOBit/PowerToo, credential access via unsecured creds and impact through intermittent AES-RSA encryption.

Notable incidents - In 2025, Play breached ADC Aerospace, a U.S. manufacturing firm, exfiltrating internal/client documents, budgets, payroll, IDs, and confidential info, which was posted on their dark web site, leading to operational impacts.

Latest IOCs -

SHA256	fc2b98c4f03a246f6564cc778c03f1f9057510efb578ed3e9d8e8b0e5516bd49
SHA256	c316627897a78558356662a6c64621ae25c3c3893f4b363a4b3f27086246038d
SHA256	e1c75f863749a522b244bfa09fb694b0cc2ae0048b4ab72cb74cf73d971777b
SHA256	094d1476331d6f693f1d546b53f1c1a42863e6cde014e2ed655f3cbe63e5ecde
SHA256	d4a0fe56316a2c45b9ba9ac1005363309a3edc7acf9e4df64d326a0ff273e80f
SHA256	c88b284bac8cd639861c6f364808fac2594f0069208e756d2f66f943a23e3022
SHA256	f18bc899bcacd28aaa016d220ea8df4db540795e588f8887fe8ee9b697ef819f
SHA256	e641b622b1f180fe189e3f39b3466b16ca5040b5a1869e5d30c92cca5727d3f0
SHA256	608e2b023dc8f7e02ae2000fc7dbfc24e47807d1e4264cbd6bb5839c81f91934
SHA256	006ae41910887f0811a3ba2868ef9576bbd265216554850112319af878f06e55

AOL011

No information was found about this TA.

NoName057(16)

Overview - NoName057(16) is a pro-Russia hacktivist group created as a Kremlin-backed project by the Center for the Study and Network Monitoring of the Youth Environment, active since March 2022, collaborating with groups like CARR and forming Z-Pentest in 2024.

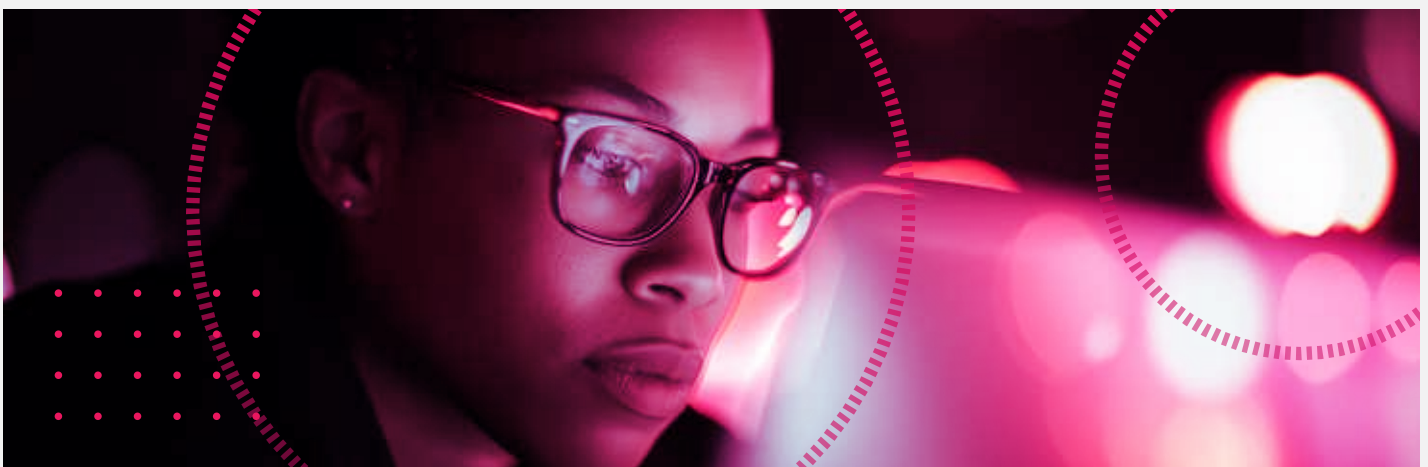
Motives - Ideological and geopolitical, supporting Russia's stance on the Ukraine conflict by targeting entities perceived as hostile to Russian interests, promoting pro-Russia narratives through disruptions.

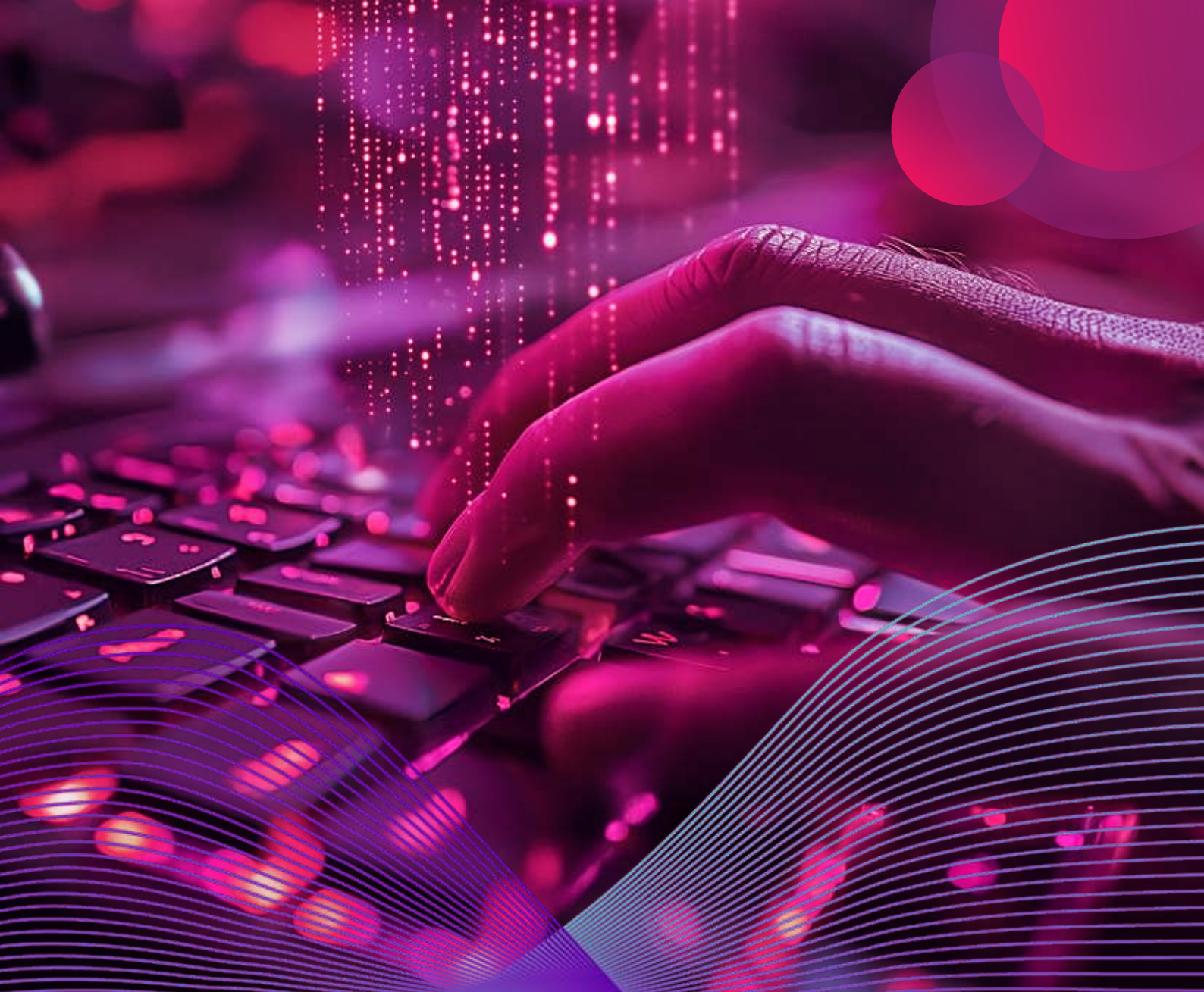
Attack vectors - DDoS using the proprietary DDoSia tool, reconnaissance with Nmap/OpenVAS for VNC services, brute force/password spraying for access, GUI manipulation in OT systems and exaggerated social media claims. they share TTPs via Telegram and GitHub.

Notable incidents - In 2025, while no specific manufacturing breach was directly attributed, the group targeted global critical infrastructure including energy and food/agriculture sectors, with opportunistic DDoS and OT intrusions causing productivity losses.

Latest IOCs –

SHA-256	fb2d227e3e03be19b837ba274cce8f6ad452a94b8cd91518c68e65546e5b3bf9
SHA-256	2110818f824ccc6d25396136f5d4ee066d40bc514136ae8868695bd56c0a08b5
SHA-256	ecc83b1a1864a6f60bb301308b652af9c9f519e2baf92baa903694b02e69b26
SHA-256	411c70b55e1781395b3267dc2aa8c6a38b63030a59f0e6a436bd71ab09add07c
SHA-256	43f5cbfba724aa9f428d7c6d33c52704bf8c8903ae633858a9ca073f6547369c
SHA-256	56be909f3967f9d0491817914c8b8950c65ecafefee3e0572587a2dd9162f65d
SHA-256	c54a3a57a9d8867be5d50fa39fe8cf90ccb8520dab1144a9ee495a86d991d65f
SHA-256	77cc16be9e6f910be9b154981df07ee9e426863e1543e0d84fbd7dc6c9d09f3
SHA-256	1b1eb5652aafcb76fd53ca368d30fc255b5fc495236bfa6a1598caff5502a4aa
SHA-256	550c4c56adfdb9437385373f2a9a7d12cea88601c5d14acde45c614bbf8d07c3





Chinafans

Overview - Chinafans is a hacktivist group active since March 3, 2025, with a primary motivation centered on dominance and ideological messaging, operating at an individual resource level, indicating a small number of actors and minimal technical sophistication. Their activities primarily target Retail, Entertainment, Business Services, and Healthcare sectors across regions including Japan, Indonesia, Malaysia, United States, South Africa, and Vietnam.

Motives - Chinafans exemplifies hacktivist operations that assert ideological objectives through digital vandalism targeting global websites across multiple industries.

Attack vectors - Website defacement through exploiting known web application and CMS vulnerabilities, leveraging insecure configurations and social engineering to manipulate site content, often conveying political statements or disruptive messages. The group maintains a community presence on zone-h.org, announcing defacement operations and providing affected domain details, reflecting engagement with the hacktivist community and notoriety-seeking behaviour.

ClOp

Overview - ClOp is a ransomware group active since 2019, linked to the threat actor FIN11, operating as a public facing entity for campaigns exploiting enterprise software vulnerabilities.

Motives - Profit-oriented, focusing on data theft extortion without always encrypting, using leaks to pressure victims.

Attack vectors - Exploiting CVEs, sending extortion emails to executives, and publishing stolen data on public sites.

Notable incidents - In 2025, ClOp was involved in the Oracle EBS breach affecting a global manufacturing firm, where sensitive data from 9,479 individuals was stolen and leaked after non-payment, disrupting telecom and automotive services.

Latest IOCs –

IPv4 Address	193.118.55.74
MD5	dfd6177cd181f2c8cd9b2bd088a192ba
MD5	75804319cddfb798b3859cb757296f6e
SHA-1	67c93b7f0dbaa2e93b89b297095efa64a84cb448
SHA-1	af4e4be68600ea666144af26f8a8aee6b2520eae
SHA-256	38f0750cbe49b30db326b53b9f752b66c4f5e23cc3bbbd6d1844e2878a19b9a7
SHA-256	3f41e2ceff3a04cd6de6aadce7e7b7c8584940e4320a7db55dd712debb061510
SHA-256	aa43f34c3fa67aea994c1babeb71b46c7b24eccaa0455ae21aa561e251e7cc4d
SHA-256	f6afa84b0847414220bb15517b8b5e2c505b64b53efbba73b753379c66ac5017
SHA-256	bef2d817f1813eb0629222112fd3721865a2a4eb1f4d51ad1f09fd807d4380ab
SHA-256	a702a671b7911a09ccb5b4f42923e8b301e0bbb851443dd52622022959a3055a





x7root

Overview - x7root is an individual hacker or small group primarily known for website defacements, as evidenced by notifications on defacement archives like Zone-H.org.

Motives - Seem to revolve around gaining notoriety, demonstrating skills, or hacktivism, common among defacers who publicize breaches to showcase vulnerabilities rather than financial gain.

Attack vectors - Exploiting content management system vulnerabilities, such as those in WordPress for brute-force attacks and shell uploads, leading to site defacements and file placement.

Top 10 Threat Actors



Akira
121



Qilin
118



Play
77



AOLO11
77



NoName057(16)
72



Chinafans
67



Clop
63



Safepay
47



Mr. BDKR28
45



x7root
42

More information on threat actors mentioned in this report is available in Check Point Exposure Management (Formerly Cyberint) Threat Actor Intel Module.

MAIN ATTACK VECTORS

Ransomware remains the dominant threat, comprising nearly half of manufacturing breaches. Key attack vectors include:

- **Exploited Vulnerabilities** - The leading entry point, 32% of incidents, often targeting legacy operational technology systems or zero-day flaws like the Windows Common Log File System. For example, ClOp ransomware surged due to exploits in Cleo Managed File Transfer.
- **Phishing and Malicious Emails** - Responsible for 23% of attacks, often enhanced with AI for more convincing social engineering. Nation-state actors, like Chinese groups, use spear-phishing to target supply chains in sectors like semiconductors.
- **Compromised Credentials and Brute-Force Attacks** - Credentials for industrial firms sell for \$4,000-\$70,000 on the dark web. Trojans like W32.Worm.Ramnit spiked 3,000% in Q1 2025 for stealing OT credentials.
- **Supply Chain Attacks** - Nearly doubled in 2025 - 297 incidents vs. 154 in 2024), exploiting vendors to access larger targets. Examples include breaches via HR software or OAuth tokens.
- **Double Extortion and Extortion Only Tactics** - Data theft combined with encryption or theft without encryption. Groups threaten to leak data on dedicated sites.
- **EDR Evasion and AI-Driven Malware** - Tools like RansomHub's EDRKillshifter bypass defenses; AI enhances phishing and malware.
- **Abuse of Remote Access and IoT/OT Exploitation** - SSH tunneling for ESXi ransomware, targeting interconnected IoT devices in smart factories.
- **Denial-of-Service (DoS) and Data Manipulation** - Used in nation-state attacks to disrupt ICS such as deleting data or causing outages.

Attack Vectors 2025



Ransomware
890



Defacement
526



Information-System-Disruption
345



Breach & Leak
144



EUROPE

Europe recorded significant ransomware activity in the industrial sector, with manufacturing bearing the brunt. In Q3 2025, industrial ransomware attacks climbed 13% to 742 globally, with Europe seeing 162 incidents—second only to North America. Manufacturers accounted for 72% of these hits, reflecting a broader trend where 80% of firms still harbor critical vulnerabilities in legacy operational technology (OT) systems. Ransomware demands averaged \$1.16 million, more than double the previous year's figure. The European Union Agency for Cybersecurity (ENISA) highlighted ransomware as a prime threat, often leading to data breaches or system downtime.

Notable incidents:

- **Volkswagen Group France (October 2025)** - Qilin ransomware stole 150 GB of data, including vehicle owner information.
- **Collins Aerospace (September 2025)** - Ransomware disrupted multiple European airports, highlighting supply chain vulnerabilities.

Main Threat Actors - Europe 2025



NoName057(16)

57



Qilin

35



Safepay

20



x7root

20



Akira

19



Chinafans

15



Mr. Hamza

14



Incransom

12



Keymous +

8



worldleaks

7

Attack Vectors 2025 - Europe 2025



Ransomware

198



Information-System-Disruption

122



Defacement

86



Breach & Leak

28





UNITED STATES

The USA was the top global target for ransomware, 21% of incidents, with manufacturing as the most attacked industry for the fourth year. Ransomware comprised nearly half of manufacturing breaches, with median costs at \$500,000. In 2025, 1,929 documented attacks hit industrial sectors, with manufacturing and construction each at 21%. Legacy OT systems and supply chains were key vulnerabilities.

Notable incidents:

- **May 2025** - A large North American Steel Producer halted production after detecting unauthorized access.
- **April 2025** - Medical device manufacturer faced network disruption, delaying manufacturing and shipments, suspected ransomware.
- **2022, ongoing fallout** - Aerospace manufacturer paid \$1.75 million settlement after Conti ransomware leaked employee data.
- **October 2023** - Building materials firm offline for months, likely ransomware, causing stock drops.

Main Threat Actors - USA 2025



Akira
86



Play
70



Qilin
57



Clop
47



Unknown
32



Chinafans
23



Lynx
22



Dark Storm Team
22



Ransomhub
20



Dragonforce
19

Attack Vectors 2025 - USA 2025



Ransomware
482



Defacement
105



Information-System-Disruption
83



Breach & Leak
53





BRAZIL

Brazil faced 248 ransomware incidents in 2024-2025, with 166 directly targeting the country, manufacturing represented 20.56% of attacks, the highest among sectors. Credentials for industrial firms fetch high prices (\$4,000-\$70,000) on dark web markets due to potential production disruptions. In Q1 2025, Brazil led South America with 22 incidents, focusing on food and beverage manufacturing. Supply chain attacks amplified risks, with criminals exploiting vendor systems.

Notable incidents:

- **JBS Foods (2021, ongoing impact)** - The world's largest meat processor, based in Brazil, paid \$11 million in ransom after an attack shut down plants in North America and Australia, disrupting global supply chains.
- **MedicSolution (September 2025)** - KillSec ransomware targeted healthcare software, exposing lab results and patient data from multiple institutions, indirectly affecting industrial health tech integrations.
- **C&M Software (July 2025)** - Supply chain breach used client credentials to access financial systems, highlighting risks to connected industrial payment infrastructures.

Top Threat Actors - Brazil 2025



Belief
3



Chinafans
3



Goku Exploits
2



Simsimi
2

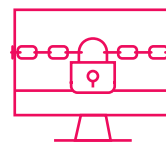


EbRaHiM-VaKeR
2

Attack Vectors - Brazil 2025



Defacement
22



Ransomware
7

CHINA

Data on attacks against China's industrial sector is limited, as reporting often focuses on China as a cyber aggressor. However, ransomware groups claimed 90 victims in China in 2025-2026, including manufacturing firms. Manufacturing remains vulnerable to global trends, with 71% surge in threat actor activity targeting the sector.

Notable incident:

- **Luxshare Precision Industry Co. Ltd. (December 2025)** - Major electronics manufacturer hit by Ransomhouse, with client data stolen.

Top Threat Actors - China 2025



x7root

2



MR.QLQ

2



1352eFwp3n

1



888

1



Sinobi

15



BROKENPIPE

1



Worldleaks

1



Chinafans

1



303

1



kiki88888

1

Attack Vectors 2025 - China 2025



Defacement

6



Ransomware

2



Breach & Leak

4

INDIA

India became APAC's ransomware epicentre in 2025, with 65% of hit companies paying ransoms, average \$1.35 million. Manufacturing and critical IT services were hardest hit, with Qilin leading assaults. A massive, alleged attack in 2025 targeted energy, railways, and gas infrastructure, wiping servers and databases.

Notable incidents:

- **Deck India Engineering Pvt. Ltd. (Recent)** - Tengu ransomware targeted the heat treatment firm, exposing sensitive data.
- **Raymond Limited (Q1 2025)** - Fabric manufacturer faced IT denial via ransomware.
- **AIIMS Delhi (2023, ongoing impact)** - Ransomware disrupted health services, indirectly affecting industrial medical supply chains.

Top Threat Actors - India 2025



AOLO11

67



XYZ

13



EbRaHiM-VaKeR

6



Chinafans

5



ynR!

5



Mr.Falcon

5



Mr. BDKR28

5

Attack Vectors 2025 - USA 2025



Defacement

163



Ransomware

16



Information-System-Disruption

13



Breach

9



RECOMMENDATIONS

Implement Zero-Trust Architecture Across IT and OT

Adopt strict identity verification, least-privilege access, and continuous validation for all users, devices, and remote/third-party connections. Segment networks to isolate OT from IT, preventing lateral movement during breaches. This is emphasized as essential for smart factories and legacy systems.

Strengthen Vulnerability Management and Patching

Prioritize rapid patching of known vulnerabilities especially in public-facing apps, VPNs, and ICS/OT components. Use automated patch management and maintain an up-to-date asset inventory to reduce exploitation risks, which remain a top entry point.

Enhance Backup and Recovery Strategies

Maintain offline, immutable, and regularly tested backups to enable quick restoration without paying ransoms. Focus on protecting backups from tampering, as attackers increasingly target them.

Build OT/IT Convergence Security

Treat OT environments with the same rigor as IT - Apply endpoint detection/response, network monitoring, and visibility tools tailored to industrial protocols. Conduct regular risk assessments for PLCs, SCADA, and IoT devices to address the growing attack surface.

Improve Employee Training and Phishing Defences

Roll out ongoing awareness programs, simulated phishing exercises, and multi-factor authentication. With AI-enhanced social engineering on the rise, train staff to recognize advanced lures targeting manufacturing credentials.

Strengthen Supply Chain and Third-Party Risk Management

Vet vendors rigorously, enforce contractual security requirements, and monitor third-party access. Conduct supply chain audits and limit privileges to reduce cascading impacts from vendor breaches.

Leverage AI Defensively While Monitoring Risks

Use AI for automated threat hunting and response but implement controls to prevent AI misuse by attackers.





PREDICTIONS FOR 2026

Cyber threats targeting the industrial and manufacturing sector are expected to continue escalating throughout 2026, with ransomware remaining the primary risk driver. The sector's increasing digitalization, reliance on operational technology (OT), and dependence on complex supply chains make it an attractive target for financially motivated and geopolitically aligned threat actors. Disruption to manufacturing operations, even for short periods, can result in significant financial losses, safety risks, and downstream impacts across critical supply chains.

Key Anticipated Trends

- **AI-powered ransomware acceleration** - Threat actors are increasingly leveraging artificial intelligence to enhance the scale, speed, and precision of ransomware campaigns. AI-assisted phishing and social engineering are expected to become more convincing and targeted, increasing the likelihood of credential compromise among both IT and OT personnel. Additionally, AI-driven tooling will improve payload delivery and enable more sophisticated evasion techniques, allowing malicious activity to bypass traditional endpoint protection, email security, and behavioural detection controls.
- **Shift from encryption to data theft and extortion** - Ransomware groups are anticipated to further reduce their reliance on full system encryption in favour of data exfiltration and extortion-based tactics. By threatening to leak sensitive operational, proprietary, or customer data, attackers can apply pressure while minimizing operational effort and risk. Manufacturing, logistics, food production, and industrial supply chains are expected to remain high-value targets due to their time-sensitive operations and limited tolerance for downtime or reputational damage.
- **Growth in supply chain and SaaS-targeted attacks** - Attackers are increasingly exploiting weaknesses in third-party vendors, managed service providers, and SaaS platforms to gain indirect access to industrial environments. These compromises can enable wide-scale, cascading impacts across interconnected industrial ecosystems, allowing threat actors to affect multiple organizations through a single point of entry. The growing reliance on cloud-based management, monitoring, and collaboration tools further expands the attack surface for the sector.
- **Faster attack execution and reduced dwell time** - Ransomware and intrusion campaigns are expected to progress more rapidly, with threat actors minimizing dwell time between initial access and impact. Increased automation and pre-packaged attack frameworks will limit opportunities for early detection and response, placing greater pressure on organizations to identify and contain threats in near-real time. This trend increases the likelihood that attacks will reach critical operational stages before defensive measures can be fully activated.

CONTACT US

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomom Kotohira Tower 25F,
1-2-8, Toranomom Minato-ku, Tokyo 105-0001

ABOUT CHECK POINT EXPOSURE MANAGEMENT

Check Point's exposure management changes the game.

We combine billions of internal telemetry points with billions of external signals from the open, deep, and dark web to deliver a unified intelligence fabric. This provides clear visibility across the full attack surface, including brand risk.

The industry is moving from fragmented feeds to real context and real priorities. We support that shift through active threat validation, confirmation of compensating controls, and deduplication across tools, so teams can focus on what actually matters.

With safe-by-design remediation, fixes aren't just assigned, they're implemented. Every fix is validated before enforcement, enabling measurable risk reduction without downtime.

Gartner predicts organizations adopting continuous threat exposure management with mobilization will see 50% fewer successful attacks by 2028. We're leading that shift with action, not just tickets, and Fortune 500 organizations across major industries already rely on Check Point Exposure Management.

For more information visit: checkpoint.com/exposure-management

© Check Point, 2026. All Rights Reserved.