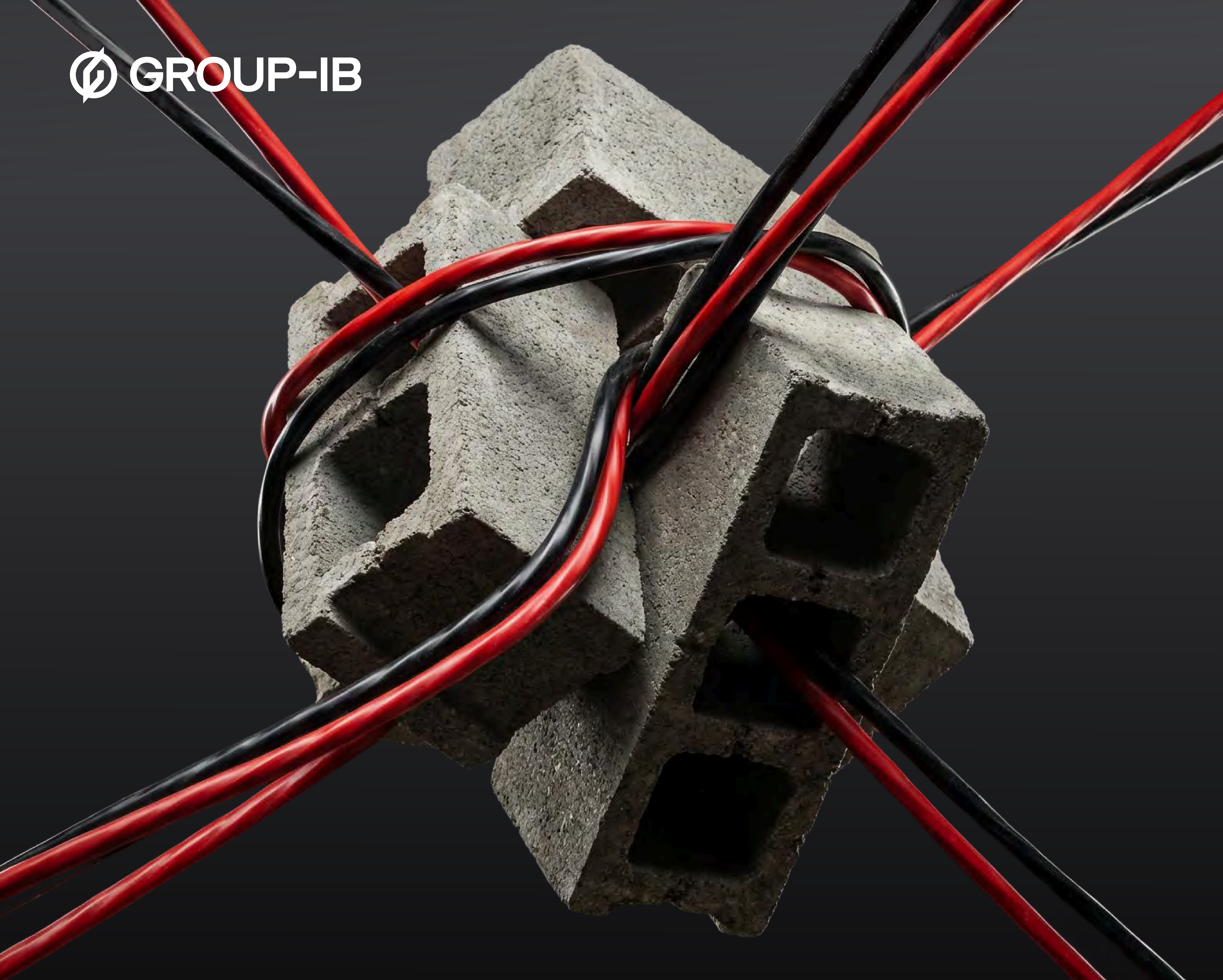




Threat Report

Inside Europe's Manufacturing Cyber Threat Landscape

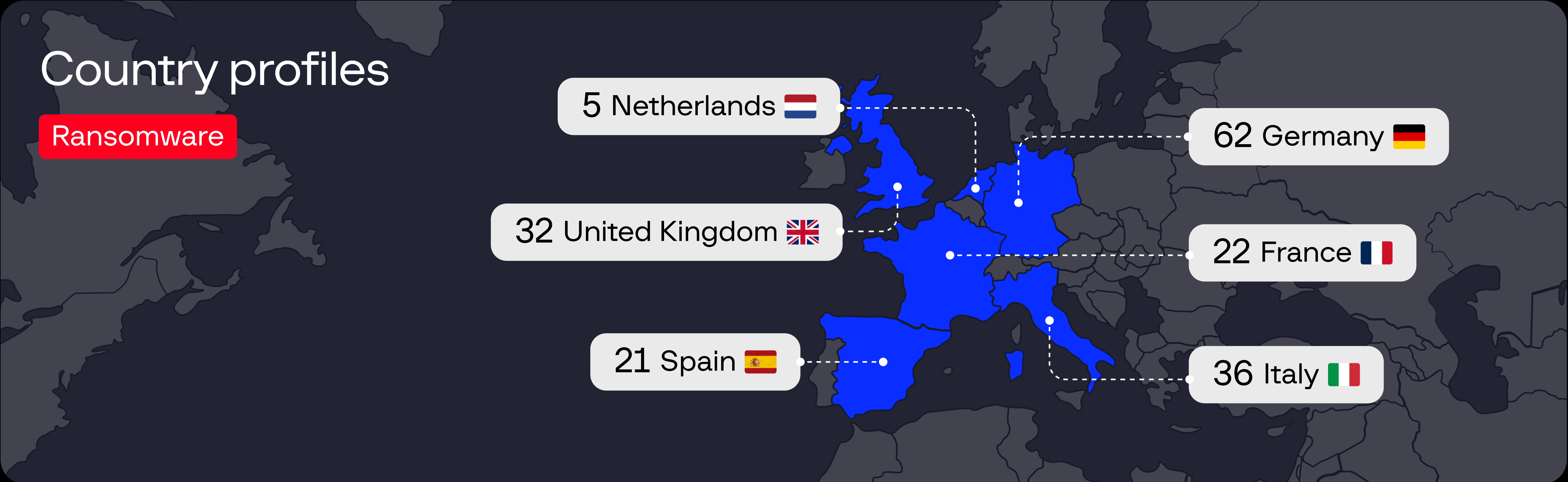
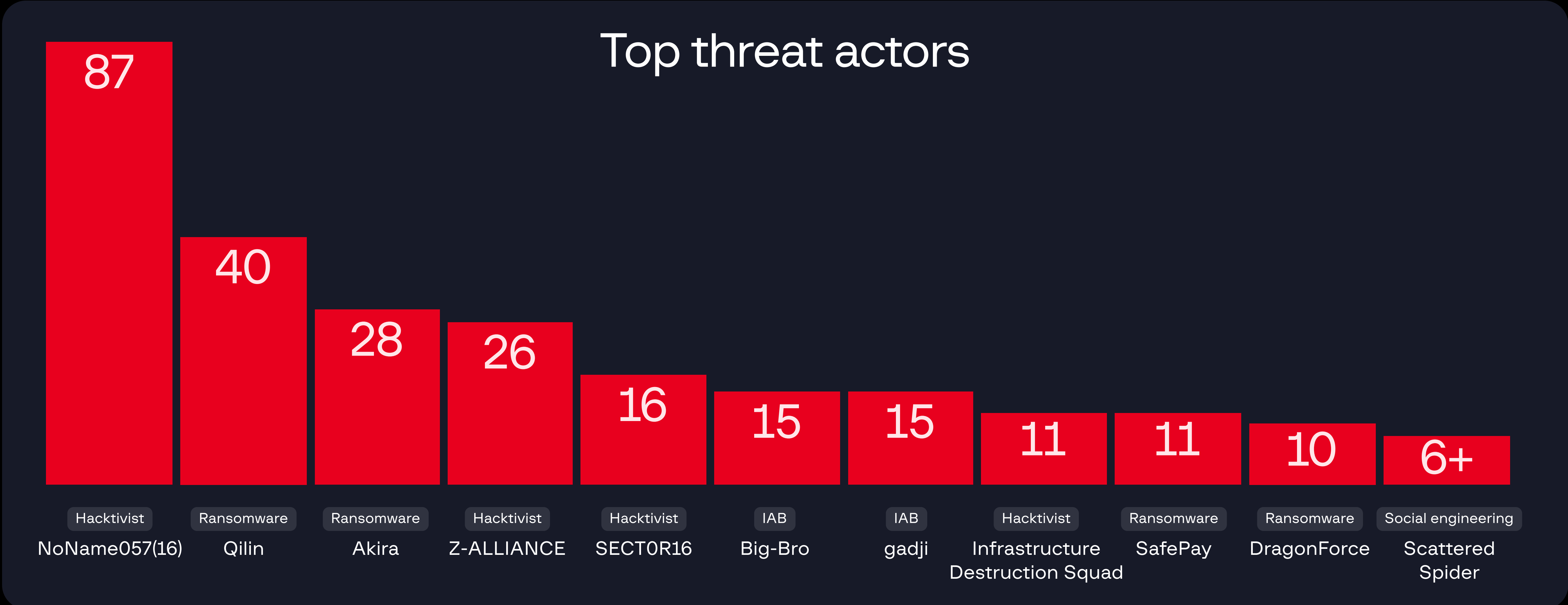
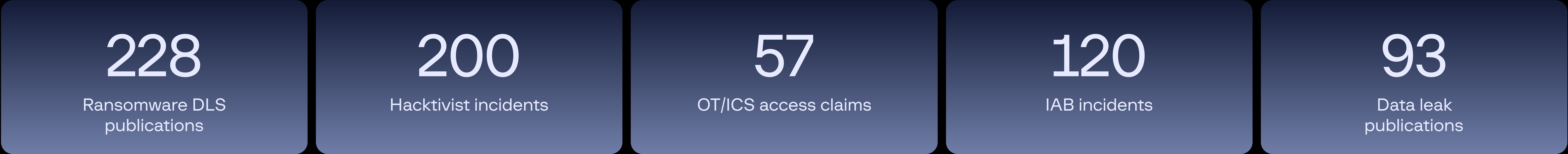
Table of contents

Executive summary	04
MITRE ATT&CK® Heatmap: Global manufacturing threat landscape	05
How this can help European manufacturers	05
How to use this heatmap	06
Initial Access Brokers (IAB)	08
Access to your network may already be for sale	08
Recent case: Phantom Stealer campaign targeting European manufacturers	10
Hacktivism & OT access	11
DDoS is a distraction, OT access is the threat	11
Ransomware activity	13
The defining threat to European manufacturing operations	13
Data leak publications	15
Intellectual property flooding the underground marketplace	15
Threat actor profiles	17
Key adversaries targeting European manufacturing	17
State-sponsored threats: the quiet backdrop	21
Country profiles	23
Six countries, one threat landscape, 2025–2026	23
Recommendations	27
Immediate priorities. Act now	27
Sustained capabilities. Build in 2026	28
Vulnerability management across IT and OT environments	29
How Group-IB addresses each threat category in this report	30

Europe's manufacturing cyber threat landscape

Full-year 2025 with early 2026 updates

Source: Group-IB Threat Intelligence



Trend

25% of all IAB activity is accounted for by Big-Bro and gadji.

Key incident

Scattered Spider

- JLR SAP zero-days
- 5-week shutdown
- \$250M losses

BlackEnergy

30+ Polish sites had their ICS devices destroyed

Trend

Germany

highest incident count

Italy

highest OT access

France

37% of all data leaks

United Kingdom

most targeted by ransomware + IAB

Spain

OT hacktivists proving ground

Netherlands

attacks on irreplaceable vendors

- ASML
- AkzoNobel

What to prepare for in 2026

Ransomware

ERP and SAP exploitation will replace phishing as the primary entry point.

Audit SAP, ERP, and SaaS integrations for zero-day exposure and credential hygiene.

OT access

Hacktivist OT capabilities will spread as groups share TTPs.

Eliminate unsecured remote access to industrial control systems.

Access brokers

IAB-to-ransomware pipeline will accelerate and go private.

Monitor underground forums and private channels for sector-specific IAB activity.

Data leaks

IP theft will expand beyond France as underground markets professionalize.

Monitor for your data on underground markets. Focus on the data itself, not just who sells it.

State-sponsored

APT groups are mapping control loops and pre-positioning for disruption.

Patch perimeter devices on emergency SLAs. Enforce MFA on all VPN. Segment IT from OT.

Supply chain

Supplier VPN and contractor access will remain the preferred entry vector. Time-bound vendor access.

Route through monitored jump hosts. Log all third-party sessions.

Executive summary

In September 2025, a cyberattack [forced Jaguar Land Rover](#) to shut down assembly lines across four countries. The attack halted production for five weeks, caused \$250 million in direct losses, and contributed to a measurable dip in UK GDP. The attackers never touched a single production line controller. They got in through the enterprise IT layer.

This is just one example of the attacks that European manufacturers are facing from multiple angles simultaneously. The sector is the most heavily targeted by ransomware in Europe, with the United Kingdom, Germany, and Italy absorbing more than half the regional total. In parallel, hacktivist groups are reaching industrial control systems and publishing video proof. And network access to European factories is being sold on underground forums to anyone willing to pay.

Over the past decade, European manufacturing organizations have made significant progress in securing industrial environments. Factories in major industrial economies have invested heavily in asset inventories, industrial network segmentation, and anomaly detection capabilities. These internal security disciplines form the technical backbone of many OT security programs and support compliance with frameworks such as [IEC 62443](#) and the [NIS2 Directive](#).

But as internal defenses have matured, the attack surface has expanded in a different direction. Production networks are increasingly connected to enterprise IT infrastructure, supplier ecosystems, and remote maintenance services. This convergence improves operational efficiency, yet it also introduces exposure points outside the factory perimeter that attackers routinely exploit.

Today, there is a critical mismatch between where attacks begin and where security programs focus.

While OT security prioritizes internal production networks, the earliest indicators of compromise appear outside the factory perimeter. Attackers gain initial access through internet-facing systems, compromised credentials traded on underground forums, and exposed remote access services. From there, they pivot into production environments.

On top of that, supply chain attacks have become the go-to model for scalable intrusion. Attackers compromise vendors, SaaS platforms, and open-source ecosystems to inherit trusted access across customer networks. For manufacturers, a breach at a supplier can quickly become a breach at your plant. [NIS2 Article 21 directly requires](#) organizations to assess the supply chain risk, but many haven't yet turned that requirement into concrete controls over third-party remote access.

This report is designed to help organizations address these challenges. It covers the full-year 2025 threat landscape and key incidents and emerging threats from early 2026 across six European manufacturing economies: Germany, France, Italy, Spain, the Netherlands, and the United Kingdom.

The report provides CISOs, OT security leaders, SOC teams, and threat intelligence practitioners the visibility they need into the actors, methods, and ecosystems targeting the manufacturing sector. All data is sourced from [Group-IB Threat Intelligence](#).

MITRE ATT&CK®

Heatmap: Global manufacturing threat landscape

This heatmap presents a MITRE ATT&CK® matrix illustrating the most frequently observed tactics and techniques used by threat actors targeting the manufacturing sector in 2025 and early 2026. It provides a unified view of the current threat landscape on a global scale.

The color-coded matrix highlights the prevalence and frequency of specific adversarial methods across the full attack lifecycle — from Initial Access to Impact — helping organizations understand how attackers operate when targeting manufacturing infrastructure.

How this can help European manufacturers

While the statistics reflect a global perspective, cybercriminal syndicates and advanced persistent threats (APT) groups are highly agile. The threat actors driving these trends can pivot and target European organizations at any moment. The tactics, techniques, and procedures (TTPs) dominating the global stage today are the exact blueprints they will deploy if they shift their focus toward Europe. European manufacturers must be ready.

Based on observed threat actor activity, several critical patterns emerge:

01. Destructive Impact

The vast majority of attacks culminate in operational disruption. Data Encrypted for Impact is the most widely used technique, followed by Network Denial of Service. These statistics confirm that ransomware and service disruption remain the primary objectives of attacks against the manufacturing sector.
02. Initial Compromise & Persistence

Attackers heavily rely on External Remote Services to breach networks and establish persistence. Abuse of compromised credentials — Valid Accounts at both domain and local level — is a major driver for unauthorized access and privilege escalation.
03. Data Theft

When exfiltrating intellectual property or sensitive data, adversaries predominantly utilize Exfiltration Over Web Service and Exfiltration Over C2 Channel.
04. Lateral Movement

To navigate through manufacturing networks, attackers frequently exploit the Remote Desktop Protocol (RDP).

How to use this heatmap

This matrix is designed as a strategic tool for security operations centers (SOC), threat hunters, threat intelligence analysts, and risk management teams within the manufacturing industry. By focusing on the “hot spots” identified here, defenders can prioritize their security controls, sharpen detection rules, and allocate resources toward the most probable and impactful attack vectors.

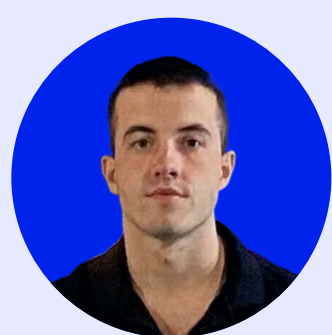


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1133 External Remote Services	T1059 Command and Scripting Interpreter	T1133 External Remote Services	T1078.002 [Valid Accounts → Domain Accounts]	T1078.002 [Valid Accounts → Domain Accounts]	T1110 Brute Force	T1082 System Information Discovery	T1021.001 [Remote Services → Remote Desktop Protocol]	T1213 Data from Information Repositories	T1219 Remote Access Tools	T1567 Exfiltration Over Web Service	T1486 Data Encrypted for Impact
T1078.002 [Valid Accounts → Domain Accounts]	T1059.001 [Command and Scripting Interpreter → PowerShell]	T1078.002 [Valid Accounts → Domain Accounts]	T1078.003 [Valid Accounts → Local Accounts]	T1078.003 [Valid Accounts → Local Accounts]	T1555 Credentials from Password Stores	T1083 File and Directory Discovery	T1210 Exploitation of Remote Services	T1114 Email Collection	T1090 Proxy	T1041 Exfiltration Over C2 Channel	T1498 Network Denial of Service
T1078.003 [Valid Accounts → Local Accounts]	T1053.005 [Scheduled Task/Job → Scheduled Task]	T1078.003 [Valid Accounts → Local Accounts]	T1078 Valid Accounts	T1078 Valid Accounts	T1555.003 [Credentials from Password Stores → Credentials from Web Browsers]	T1057 Process Discovery	T1021.005 [Remote Services → VNC]	T1560.001 [Archive Collected Data → Archive via Utility]	T1105 Ingress Tool Transfer	T1048 Exfiltration Over Alternative Protocol	T1491 Defacement
T1078 Valid Accounts	T1204.002 [User Execution → Malicious File]	T1078 Valid Accounts	T1053.005 [Scheduled Task/Job → Scheduled Task]	T1036 Masquerading	T1003 OS Credential Dumping	T1087 Account Discovery	T1021.004 [Remote Services → SSH]	T1005 Data from Local System	T1071 Application Layer Protocol	T1020 Automated Exfiltration	T1490 Inhibit System Recovery
T1566.004 [Phishing → Spearphishing Voice]	T1059.003 [Command and Scripting Interpreter → Windows Command Shell]	T1543.003 [Create or Modify System Process → Windows Service]	T1547.00 [Boot or Logon Autostart Execution → Registry Run Keys / Startup Folder]	T1562.001 [Impair Defenses → Disable or Modify Tools]	T1056 Input Capture	T1018 Remote System Discovery	T1021.007 [Remote Services → Cloud Services]	T1213.003 [Data from Information Repositories → Code Repositories]	T1071.001 [Application Layer Protocol → Web Protocols]	T1030 Data Transfer Size Limits	T1561 Disk Wipe
T1566.001 [Phishing → Spearphishing Attachment]	T1053 Scheduled Task/Job	T1053.005 [Scheduled Task/Job → Scheduled Task]	T1053 Scheduled Task/Job	T1027 Obfuscated Files or Information	T1003.001 OS Credential Dumping → LSASS Memory	T1033 System Owner/User Discovery	T1021.002 [Remote Services → SMB/Windows Admin Shares]	T1113 Screen Capture	T1571 Non-Standard Port	T1567.004 [Exfiltration Over Web Service → Exfiltration Over Webhook]	T1485 Data Destruction
T1190 Exploit Public-Facing Application	T1059.006 [Command and Scripting Interpreter → Python]	T1112 Modify Registry	T1055 Process Injection	T1070 Indicator Removal	T1552.003 [Unsecured Credentials → Shell History]	T1016 System Network Configuration Discovery	T1021 Remote Services	T1560 Archive Collected Data	T1573 Encrypted Channel	T1529 System Shutdown/Reboot	T1529 System Shutdown/Reboot
T1195.001 [Supply Chain Compromise → Compromise Software Dependencies and Development Tools]	T1204 User Execution	T1543 Create or Modify System Process	T1543.003 [Create or Modify System Process → Windows Service]	T1497 Virtualization/Sandbox Evasion	T1552.001 [Unsecured Credentials → Credentials In Files]	T1046 Network Service Discovery	T1021 Remote Services	T1530 Data from Cloud Storage	T1001 Data Obfuscation		T1489 Service Stop
T1566.002 [Phishing → Spearphishing Link]	T1569 System Services	T1505.003 [Server Software Component → Web Shell]	T1068 Exploitation for Privilege Escalation	T1140 Deobfuscate/Decode Files or Information	T1056.001 [Input Capture → Keylogging]	T1497 Virtualization/Sandbox Evasion		T1056 Input Capture	T1573.001 [Encrypted Channel → Symmetric Cryptography]		
	T1106 Native API	T1574.001 [Hijack Execution Flow → DLL]	T1574.001 [Hijack Execution Flow → DLL]	T1070.004 [Indicator Removal → File Deletion]	T1558 Steal or Forge Kerberos Tickets	T1518.001 [Software Discovery → Security Software Discovery]		T1119 Automated Collection	T1102.002 [Web Service → Bidirectional Communication]		
				T1055 Process Injection							

Initial Access Brokers (IAB)

Access to your network may already be for sale

For European manufacturers, Initial Access Brokers (IABs) represent a critical upstream risk as they do not announce themselves through IDS alerts or anomalies in the OT network. By the time an IAB listing appears on Exploit.in or XSS.is, the initial compromise has already happened. The victim organization typically does not know until weeks later, when the buyer deploys ransomware or begins exfiltrating data.

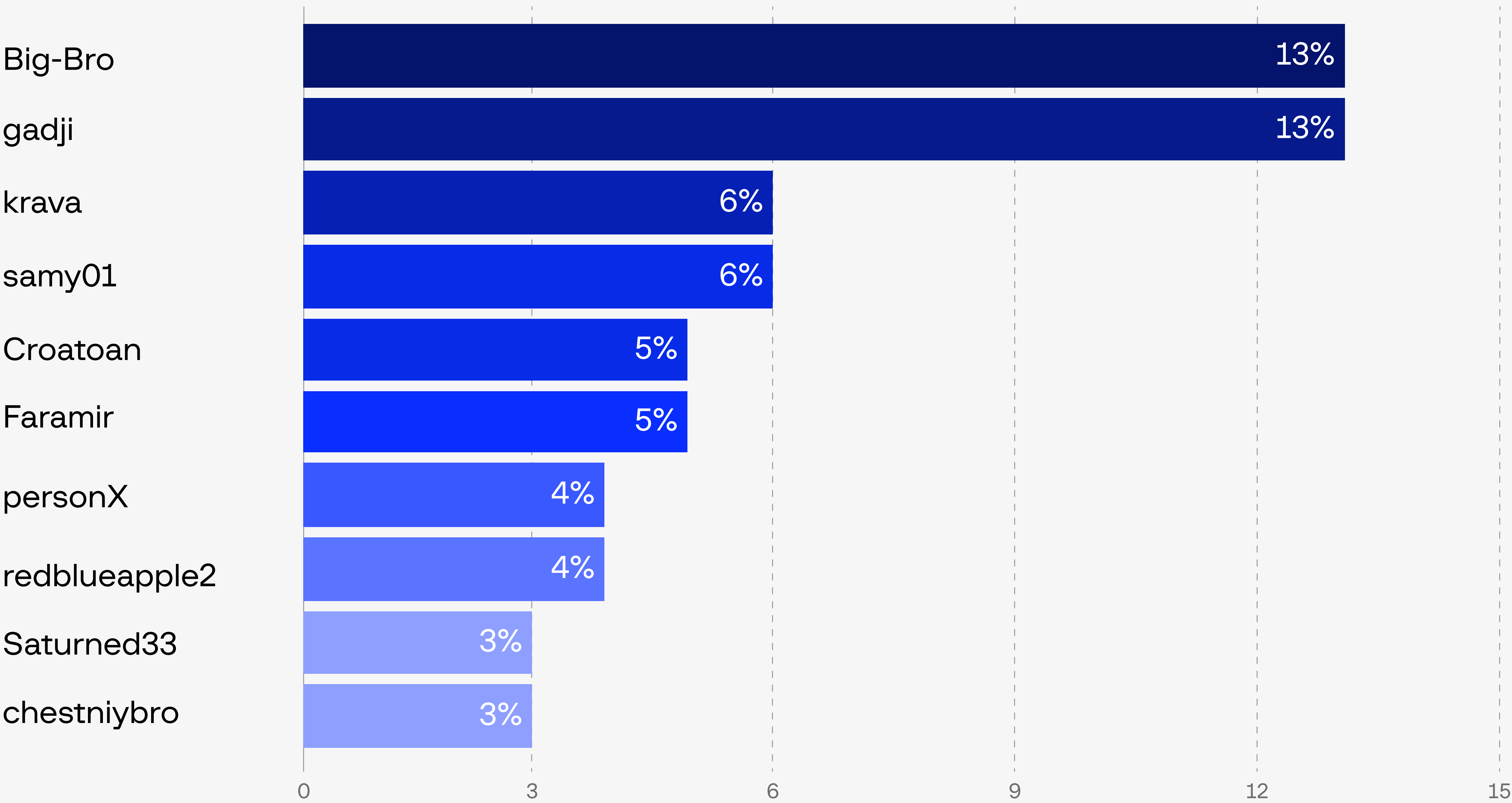


Xabier Eizaguirre,
Threat Intelligence
Analyst, Group-IB

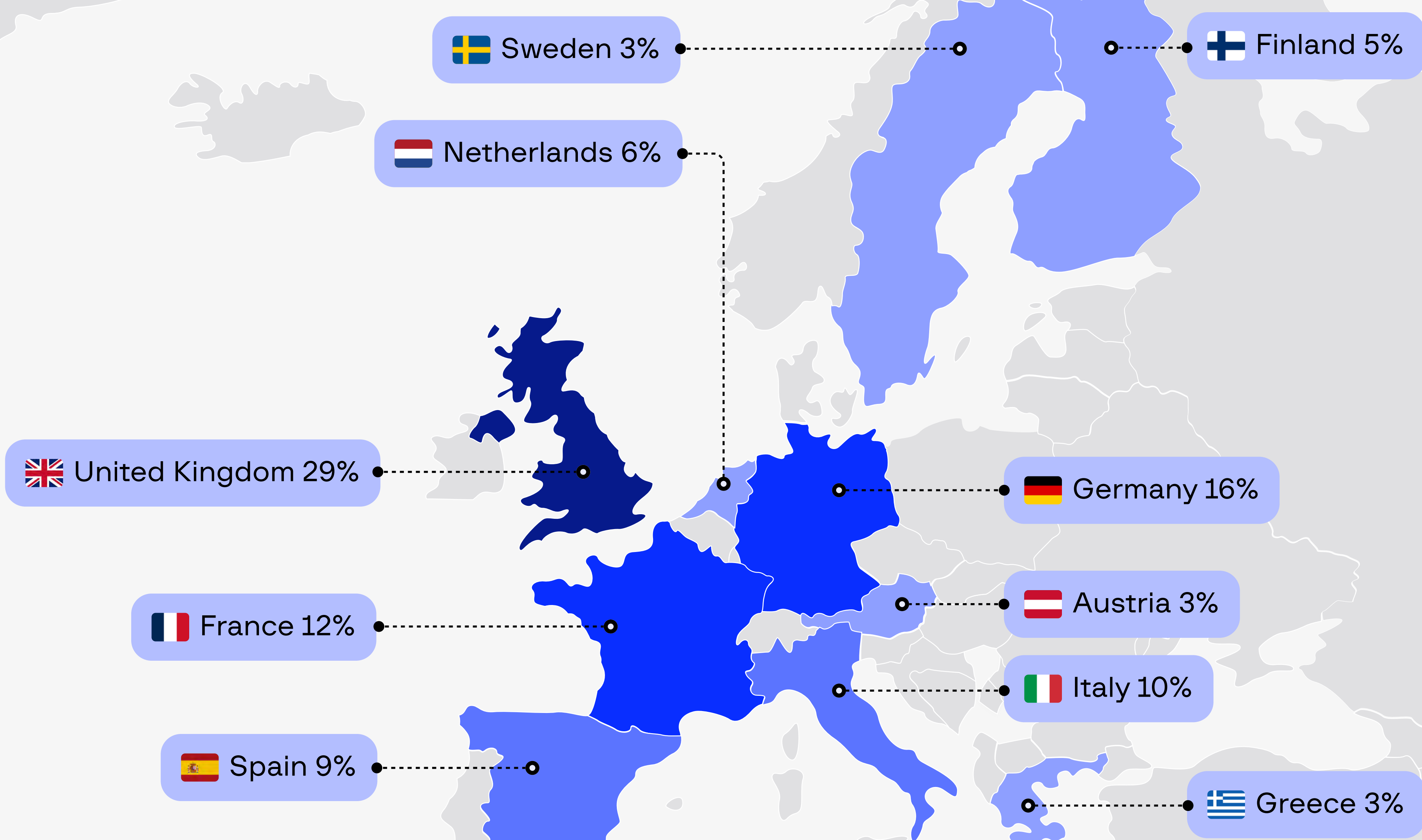
In 2025, Group-IB recorded **120 IAB incidents** targeting European manufacturers. Every one of those listings represented a network that had already been breached and was being sold to the next attacker. Many victim organizations were unaware.

Initial access broker activity targeting European manufacturing (2025)

Top IAB actors

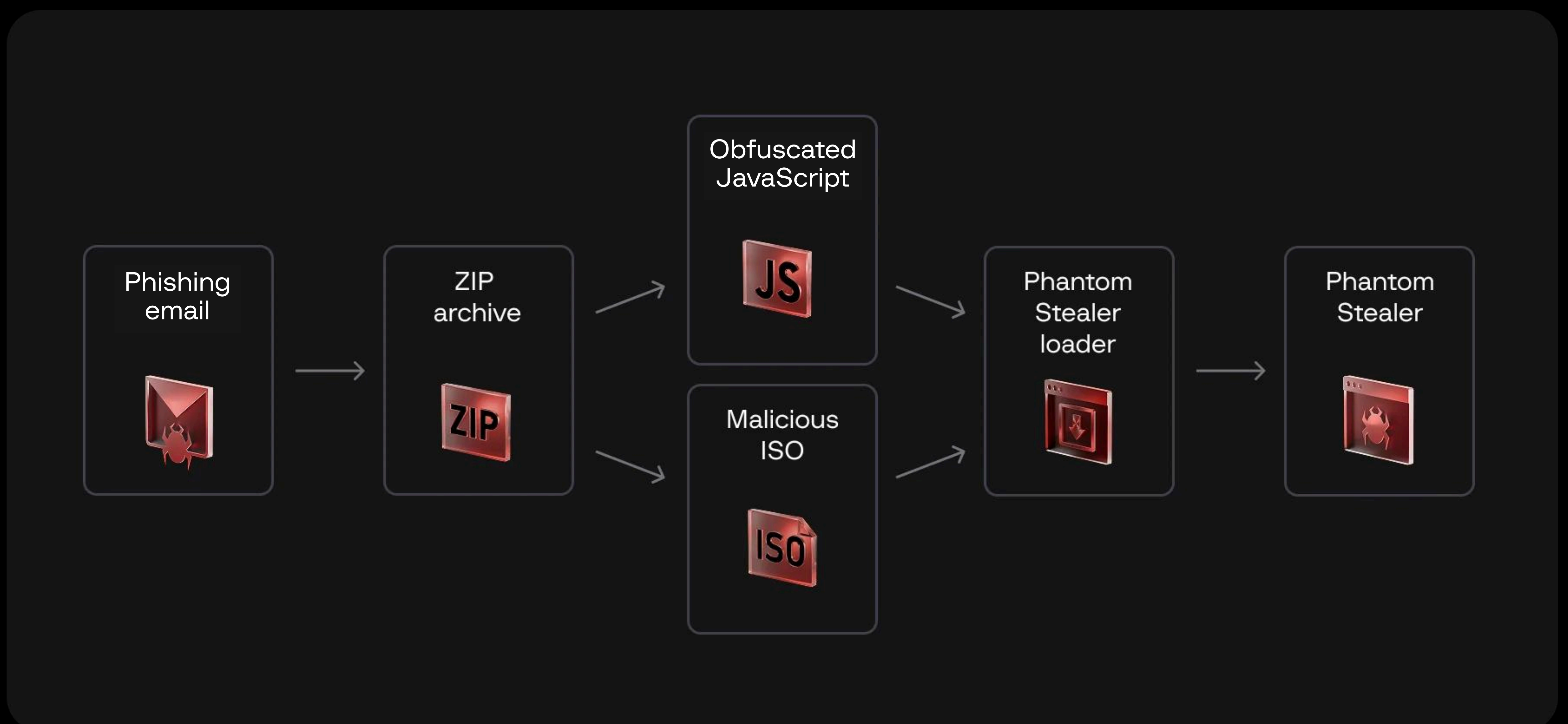


IAB incidents by country



Recent case: Phantom Stealer campaign targeting European manufacturers

Between November 2025 and January 2026, [Group-IB Business Email Protection](#) detected and blocked a sustained Phantom Stealer delivery campaign targeting European logistics, manufacturing, and technology organizations. The campaign ran in five distinct waves, with the threat actor targeting multiple unrelated companies on the same day, a spray pattern characteristic of stealer-as-a-service operations.



Every email impersonated the same legitimate equipment trading company, using procurement-themed subject lines (RFQ, INQ, PO# references) and short quotation-request bodies followed by elaborate signature blocks to evade text-based classifiers. Each carried an archive attachment containing an obfuscated JavaScript dropper or malicious executable. All emails were blocked before reaching end users. Had they not been, the harvested credentials would likely have appeared on underground forums within weeks — exactly the access that IABs in this report sell to ransomware operators and APT groups.

Learn more about
Phantom Stealer

Hacktivism & OT access

DDoS is a distraction, OT access is the threat

200

hacktivist incidents
targeting European
manufacturers

In 2025, Group-IB recorded **200** hacktivist incidents targeting European manufacturers. The majority were DDoS campaigns: loud, visible, and designed to make headlines rather than cause lasting damage.

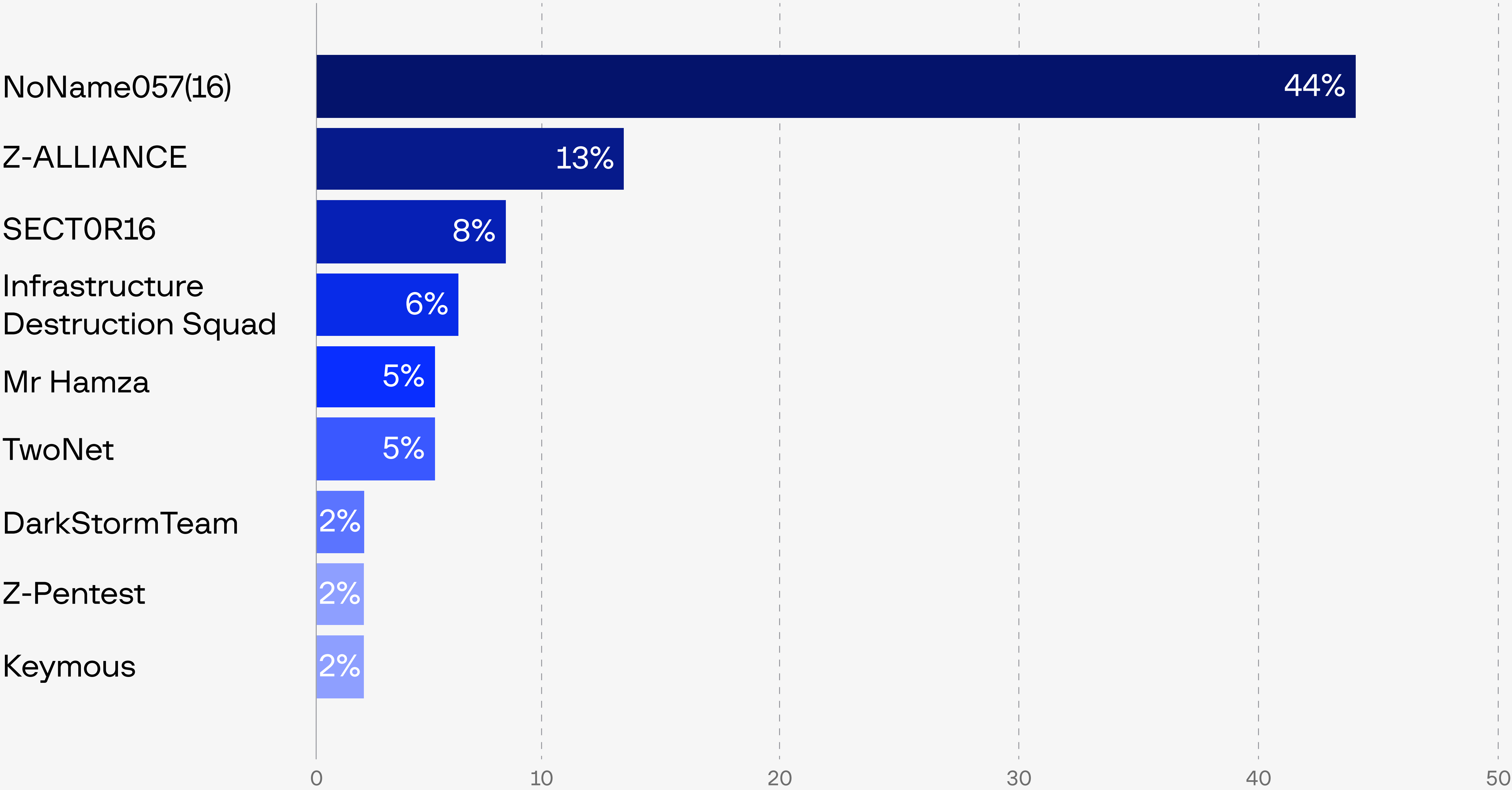
But **57** of those incidents were something different entirely. In those cases, hacktivist actors didn't just disrupt websites but claimed they had reached industrial control systems, including PLCs, SCADA interfaces, and HMI panels that govern physical production processes. These operations are quiet, targeted, and aimed at physical safety.

Italy recorded the highest number of OT access events, followed by Spain and Poland. Germany bore the heaviest overall hacktivism load, driven almost entirely by NoName057(16), which accounted for nearly half of all European hacktivist incidents.

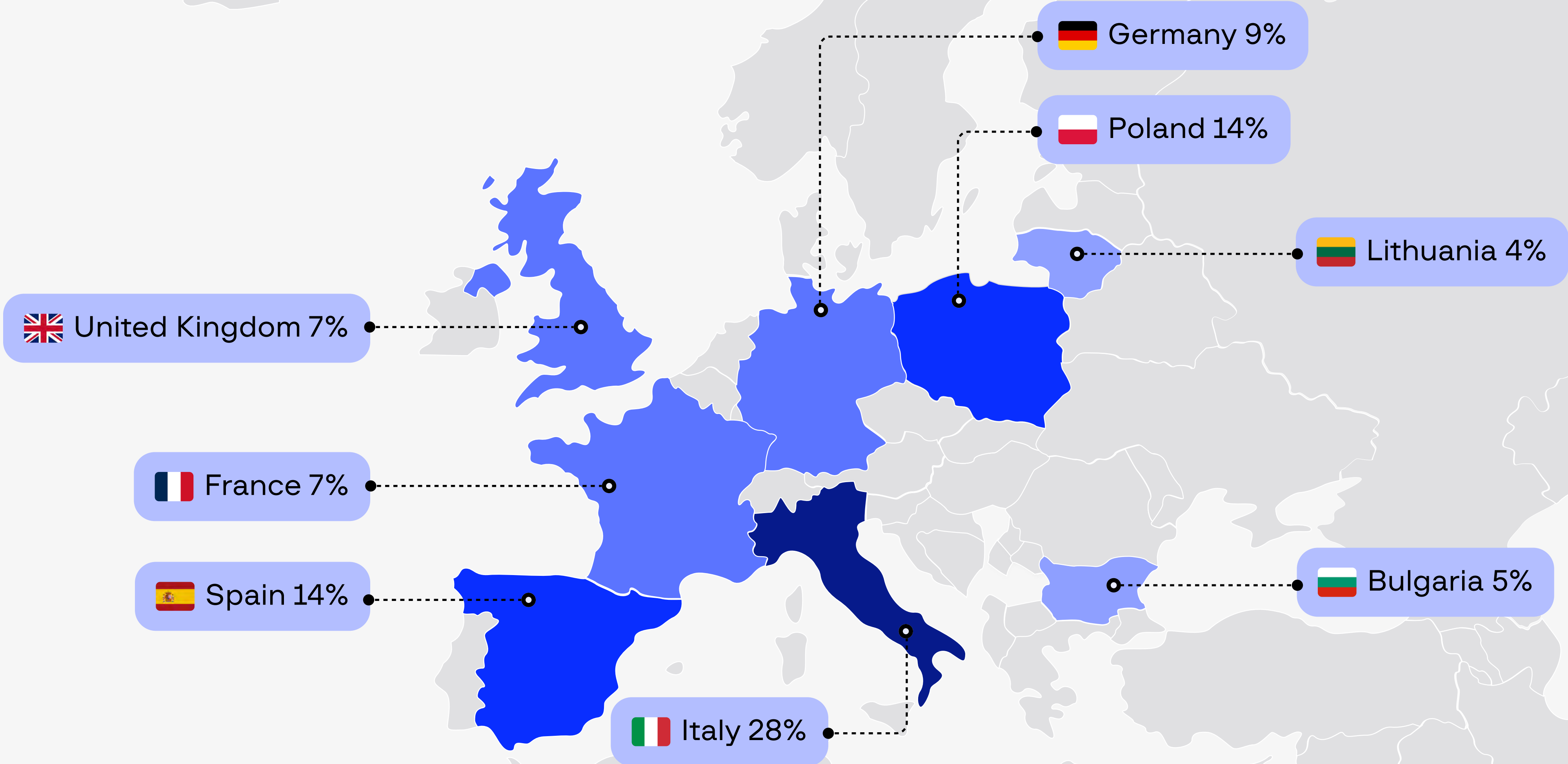
The concern is that groups capable of both DDoS and OT access may use one as a smokescreen for the other. A wave of DDoS attacks generates noise and media attention, while behind that noise, a quieter operation reaches the control systems that actually run the factory. These incidents can lead not only to business disruption but also to prolonged operational downtime, with consequences that extend far beyond those of typical DDoS attacks.

Hacktivism and OT access targeting European manufacturing (2025)

Top hacktivist actors



OT access claims by country



Ransomware activity

The defining threat to European manufacturing operations

Ransomware remains the highest-impact threat category for European manufacturers, and the ecosystem behind it has industrialized. In 2025, Group-IB detected **228 dedicated leak site posts** targeting this industry. Ransomware-as-a-Service groups like Qilin operate with sophisticated affiliate structures that let them scale across multiple manufacturing verticals simultaneously. Smaller operators are filling niches left by disrupted groups, keeping overall pressure high even as individual syndicates rise and fall.

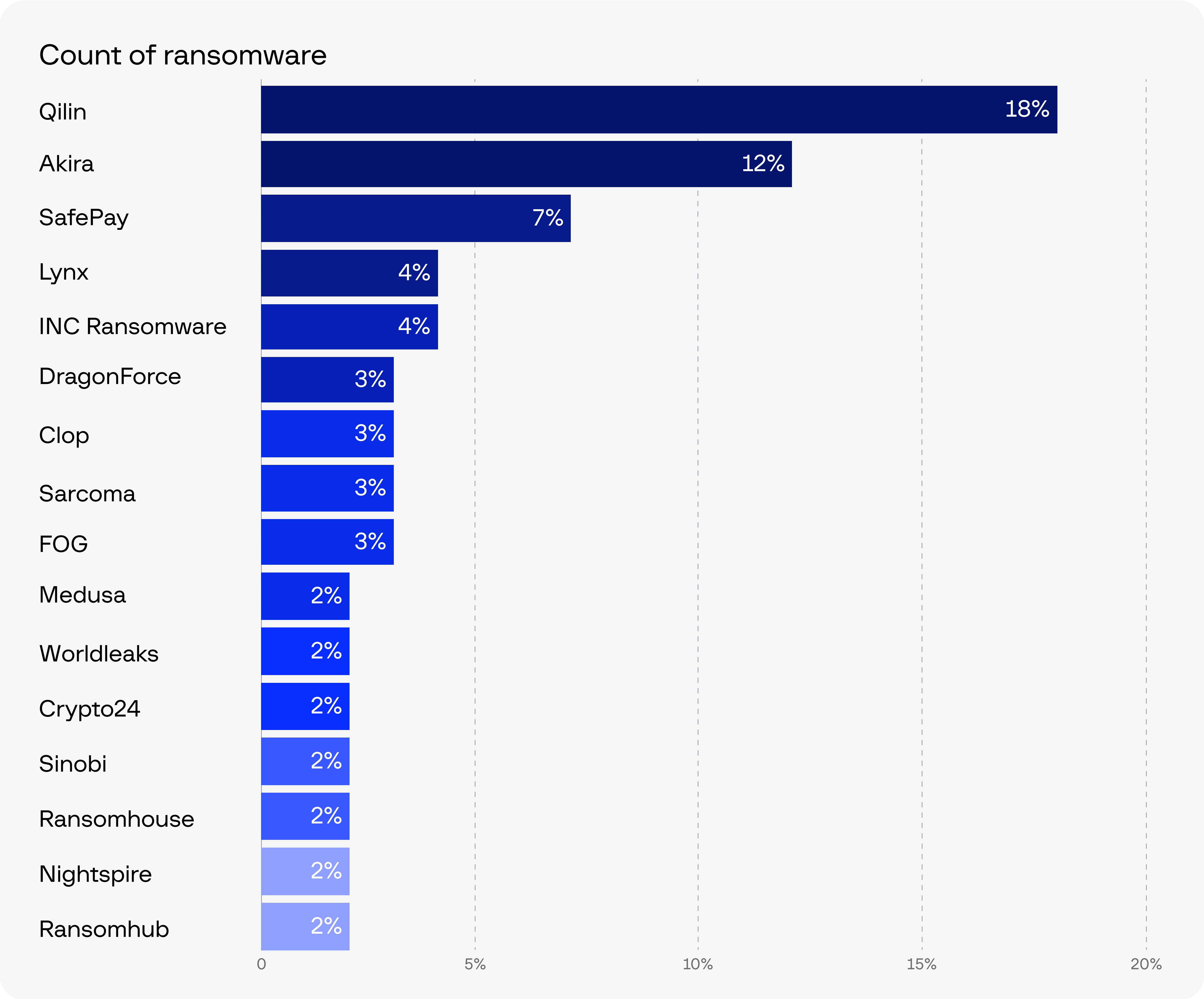
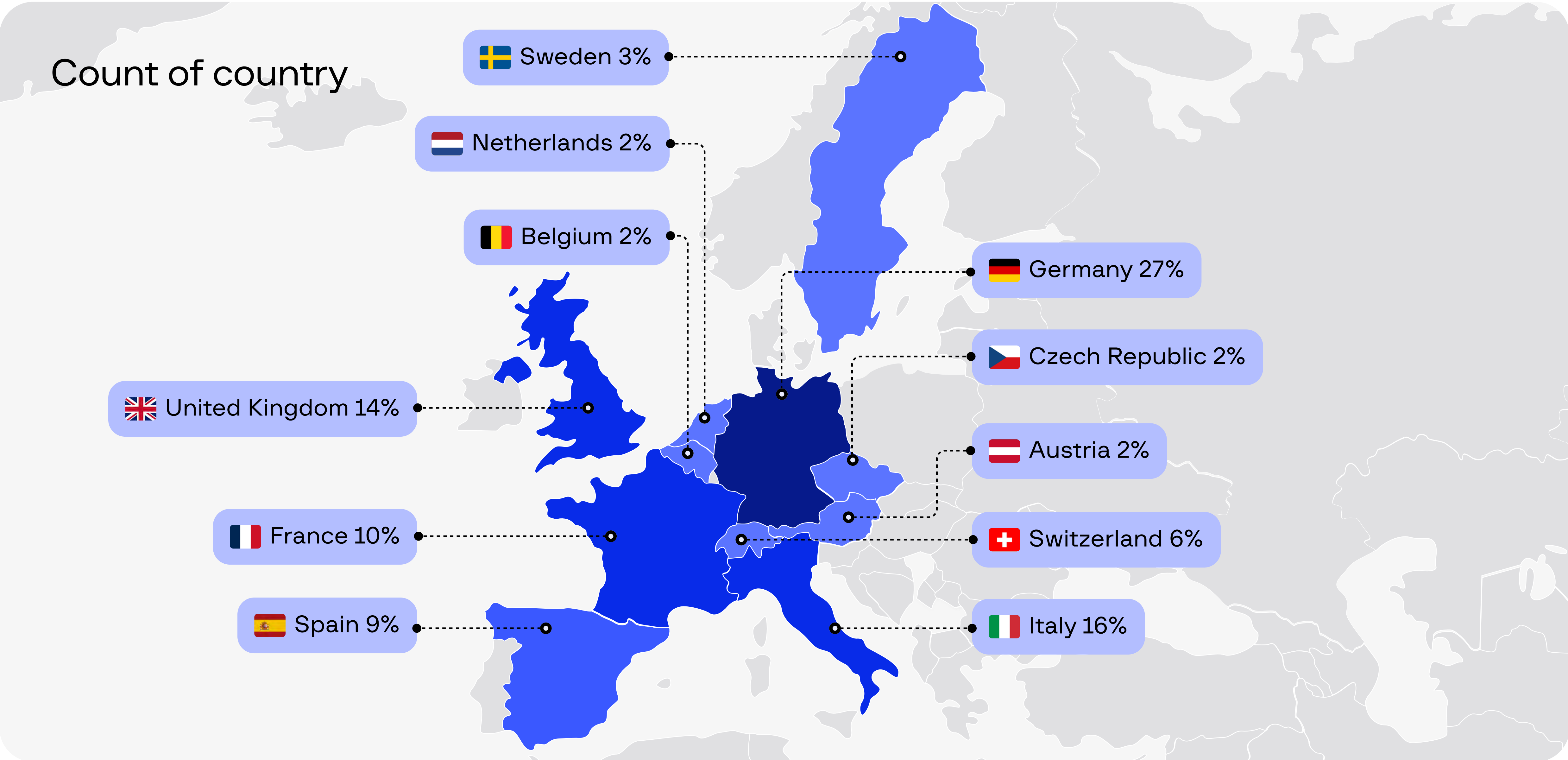
As documented in the IAB section above, many of these ransomware events began with access that was already being sold on underground forums weeks earlier. Monitoring IAB activity is the earliest available warning signal.



Xabier Eizaguirre,
Threat Intelligence
Analyst, Group-IB

The United Kingdom, Germany, and Italy together accounted for **57% of all ransomware DLS posts** targeting European manufacturers in 2025. The concentration of high-value industrial intellectual property and aging OT infrastructure in these countries creates a particularly attractive target profile.

Ransomware targeting European manufacturing (2025)



Data leak publications

Intellectual property flooding the underground marketplace

Underground data leak publications are sales of stolen corporate data by leak brokers operating on forums and specialized marketplaces. The buyers include competitors, nation-state actors, and further downstream threat groups who use the data to refine targeting, enable impersonation, or conduct fraud.

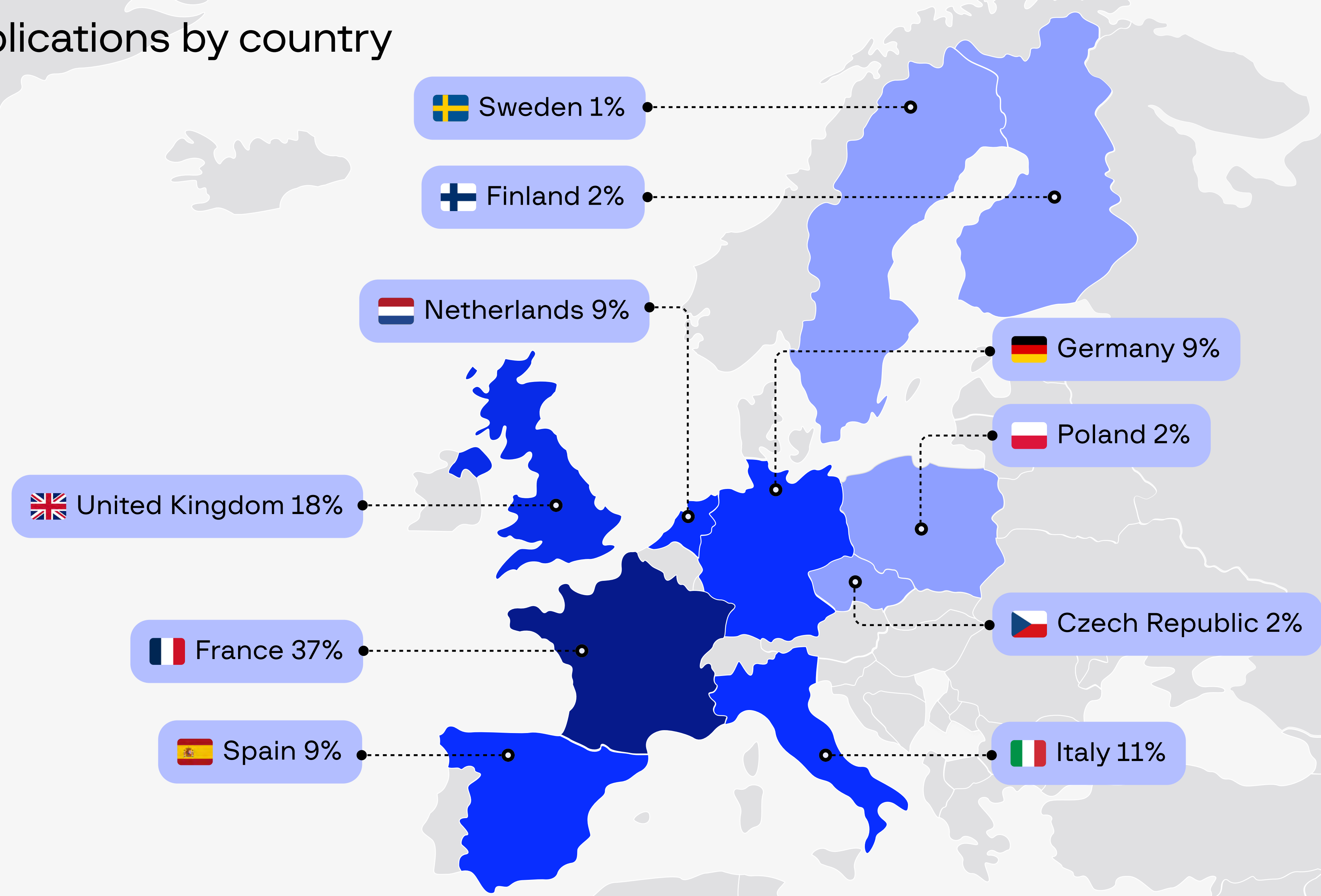


Xabier Eizaguirre,
Threat Intelligence
Analyst, Group-IB

In 2025, Group-IB recorded **93 data leak publications** targeting European manufacturers. France is the standout finding: **34 incidents**, accounting for 37% of the European total followed by the United Kingdom with **17 incidents**.

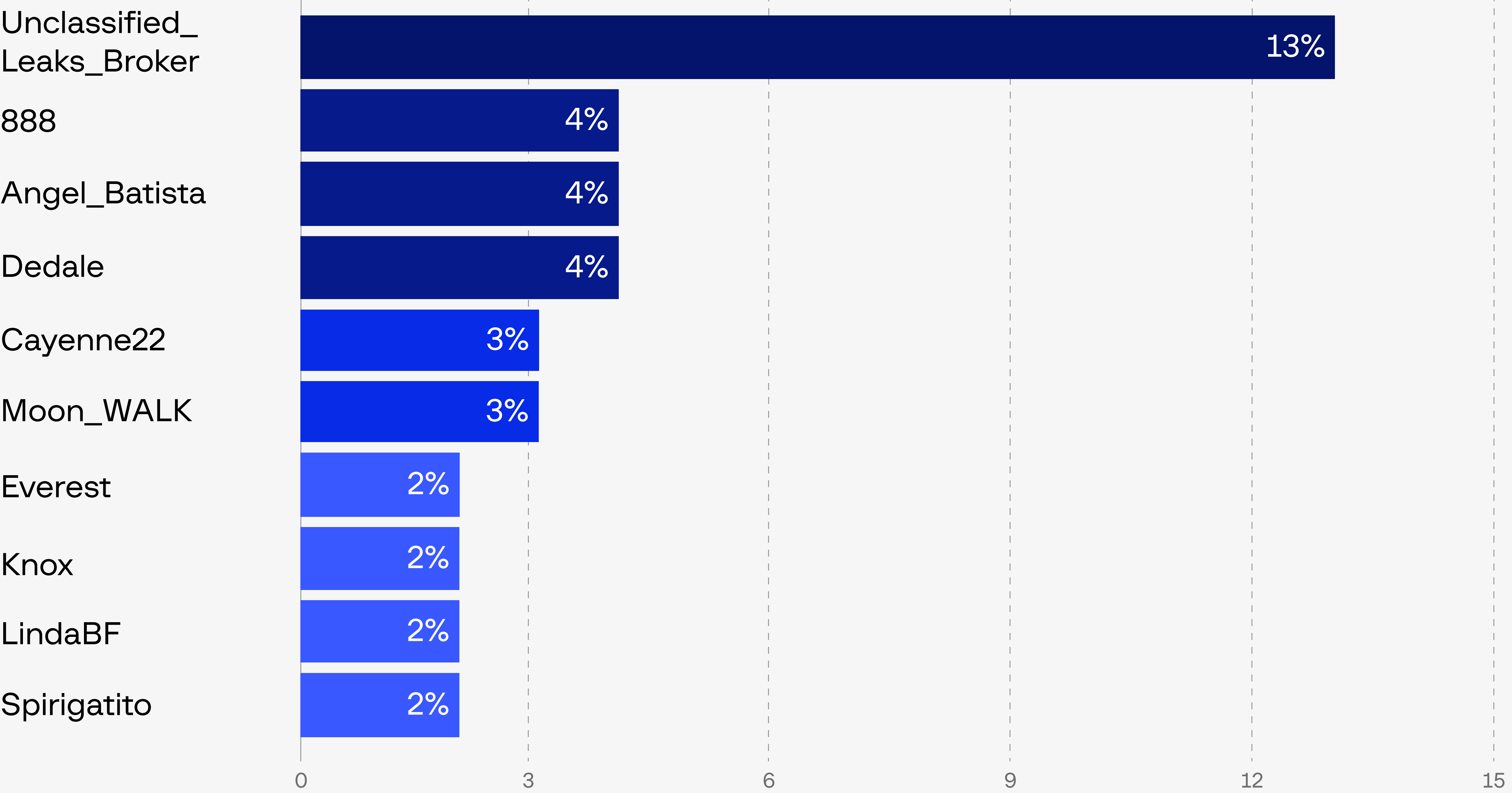
Manufacturing volume alone doesn't explain the number. France hosts a concentration of high-value intellectual property across aerospace, defense, vehicle manufacturing, shipbuilding, and luxury goods, exactly the categories that command premium prices underground. The presence of dual-use industrial and defense-adjacent companies makes French manufacturing data particularly attractive to state-affiliated buyers as well as organized crime groups.

Leak publications by country



Data leak publications targeting European manufacturing (2025)

Top leak actors



Threat actor profiles

Key adversaries targeting European manufacturing

The following profiles represent the most significant threat actors targeting European manufacturing, selected based on incident volume, operational impact, and capability escalation over the past year. They span ransomware, hacktivism, initial access brokerage, and social engineering, which reflects the multi-vector nature of the current threat landscape.



NoName057(16)

Active since
July 2022

Hacktivist DDoS collective

About

The most active threat actor targeting European manufacturing by incident count in 2025, NoName057(16) is a hacktivist group that built a crowdsourced DDoS army. Through Telegram channels and a tool called DDoSia, the group recruits volunteers who contribute their devices to coordinated attack waves. Before each campaign, it publishes a message naming the target country and framing the attack as a political act, turning its follower base into an amplifier.

Targets are chosen strategically: parliaments, ports, banks, and the industrial manufacturers that keep European economies running. In April 2025, the group ran #OpGermany, hitting Guhring, Sennebogen Maschinenfabrik, and Voith in a single coordinated wave, publishing verification links as proof of impact. By early 2026 it had expanded to UK manufacturing, targeting GKN and British drone manufacturers.

NoName057(16) has also claimed to have gained access to OT environments and control panels, which means a significant escalation in the group's potential impact.

Activity in 2025

87 incidents

T1498 Network Denial of Service T1499 Endpoint Denial of Service T1491 Defacement



Why it matters

European manufacturers are being selected as targets not because of their vulnerabilities but because of their economic visibility. If your factory is a recognizable part of a European industrial supply chain, you're on the list.



Qilin

Active since
July 2022

Ransomware RaaS

About

The leading ransomware operator targeting European manufacturing by case volume, Qilin first appeared in July 2022 under the name Agenda, rewrote its payload in Rust, and relaunched as a Ransomware-as-a-Service operation in February 2023. Group-IB analysis of its operations revealed a mature double-extortion machine: affiliates exfiltrate data before detonating encryption, then run a three-stage process of negotiation, public announcement, and data release.

The ransom note is clear in what is taken: manufacturing diagrams in SolidWorks format, employee personal data, network credentials, financial records. Entry typically comes through Fortinet edge devices exploiting CVE-2024-21762 and CVE-2024-55591, with lateral movement aided by Mimikatz, PsExec, and NlBrute. Access vectors, however, continuously evolve, which is why it’s important to monitor the cybercrime ecosystem in real time using Threat Intelligence solutions.

Confirmed European manufacturing victims include Cambridge Fluid Systems (UK, April 2025), Lipapromet (October 2025), and Albany Pumps (UK, March 2026).

Activity in 2025

40 incidents

- T1190 Exploit Public-Facing Application
- T1486 Data Encrypted for Impact
- T1078.002 Valid Accounts: Domain Accounts
- T1190 Remote Desktop Software
- T1021.001 Remote Services: RDP
- T1021.002 Remote Services: SMB



Why it matters

Qilin knows exactly what manufacturing data is worth. If your plant's intellectual property is accessible from the network edge, your next ransom note will itemize it.



Big-Bro

Active since
February 2023

Initial Access Broker

About

The most active initial access broker targeting European manufacturing, Big-Bro operates accounts across multiple underground forums including Exploit.in, XSS, RAMP, and BreachForums. Their business model is: breach enterprise environments through valid credential abuse and exploited remote services, then sell administrative-level network access to whoever will pay.

Big-Bro doesn't deploy ransomware itself. It sells the keys to groups that do. What makes this actor particularly difficult to track is evidence suggesting it functions as a reseller, aggregating access from multiple upstream sources rather than conducting every initial compromise itself. This means the real breach may predate the listing by weeks, and the victim may not know access has been sold. In European manufacturing, documented access sales for UK, Germany, and France manufacturers ran consistently throughout 2025 and into early 2026.

Activity in 2025

15 incidents

- T1133 External Remote Services
- T1078.002 Valid Accounts: Domain Accounts
- T1021.001 Remote Services: RDP
- T1219 Remote Desktop Software



Why it matters

For European manufacturers, the real danger is not only the ransomware itself, but the fact that network access may have been sold weeks before the attack begins. If your RDP or VPN credentials are compromised, they're already on a price list.



Z-ALLIANCE

Active since
June 2025

Hacktivist OT access

About

The actor behind the highest number of confirmed OT access operations against European manufacturing in 2025 with 21 OT access claims, Z-ALLIANCE is a hacktivist group that bypasses corporate networks entirely and goes straight for PLCs, SCADA interfaces, and HMI panels that control physical production processes, with Italy and Spain as primary target countries.

The campaign ran at peak intensity between September and October 2025, hitting facilities across Italy, Poland, the UK, Germany, Spain, Romania, the Netherlands, and Lithuania in rapid succession. At Ranieri Impiantistica in Italy, the group gained administrative control over boiler systems, refrigeration units, and heating valves. At ARSYSTEM's paint booth facility in Poznan, Poland, attackers controlled ventilation, air pressure, and temperature regulation across all production phases. At HENSTER in Poland, an unsecured VNC connection let the group block biomass fuel supply, activate emergency alarms, and force boiler automation into failure state. At Kaserei Zeltuurner in Germany, cheese production control systems were compromised. In each case, the group published video evidence via Telegram.

Activity in 2025

26 incidents

- T1133 External Remote Services
- T1078.002 Valid Accounts: Domain Accounts
- T1021.001 Remote Services: RDP
- T1219 Remote Desktop Software

Why it matters

European manufacturers with unsecured remote access to industrial control systems are no longer facing potential OT risks. Attackers are already inside boiler systems, ventilation controls, and production line automation.



Akira

Active since
April 2023

Ransomware

About

The most prolific and geographically consistent ransomware operator targeting European manufacturing in 2025, Akira has built a mature infrastructure with Windows and Linux variants, structured negotiation portals, and extortion calibrated to victims' cyber insurance coverage. Akira is known for fast encryption cycles and a strong SME manufacturing focus, targeting organizations with valuable OT infrastructure but limited dedicated security resources.

Initial access typically comes through critical vulnerabilities in edge infrastructure: CVE-2024-37085 in VMware ESXi, CVE-2023-27532 in Veeam Backup, and CVE-2023-20269 and CVE-2024-40766 in Cisco VPN appliances. From there, affiliates deploy BumbleBee Loader for persistence, Cobalt Strike for command and control, and LaZagne for credential harvesting before encrypting data. These TTPs are subject to change, therefore staying current with the evolving threat landscape using Threat Intelligence is essential for effective defense.

Switzerland emerged as a concentration point: ABECO Zumtech Drucklufttechnik AG, Keller Laser AG, and J. SCHNEEBERGER Maschinen AG were all breached in 2025, the latter two on the same day in September. PIBOR ISO SA and Vardeco extend the confirmed European victim list. None had data published on Akira's leak site at time of writing, which reflects the group's extortion logic: the threat of publication is the leverage, not the release itself.

Activity in 2025

28 incidents

- T1190 Exploit Public-Facing Application
- T1486 Data Encrypted for Impact
- T1078.002 Valid Accounts: Domain Accounts
- T1219 Remote Access Tools

Why it matters

Swiss, German, French, and Italian manufacturers are firmly in Akira's crosshairs. The group calibrates ransom demands to cyber insurance coverage, meaning your policy isn't protection, it's the price tag.





Scattered Spider

Active since
May 2022

Cybercriminal

Social engineering

About

Scattered Spider was behind the most operationally significant manufacturing incident in Europe in 2025. It is an English-speaking, financially motivated group that built its reputation on social engineering: operators impersonate IT helpdesk staff, execute SIM swaps to bypass MFA, and build phishing infrastructure replicating Okta and enterprise SSO portals with enough fidelity to fool security-aware employees. The toolkit includes STONESTOP and POORTRY for defense evasion, AMOS and Vidar for credential harvesting, and AnyDesk and TeamViewer for persistent access.

In September 2025, the group attacked Jaguar Land Rover via CVE-2025-31324 and CVE-2025-42999, a chain of SAP NetWeaver zero-days that gave access to JLR's ERP environment and forced complete production shutdowns at Halewood and Solihull lasting nearly five weeks. The extortion ran via Telegram, with data release thresholds tied to subscriber milestones. The same campaign period saw the group targeting LVMH, Dior, KLM, Brainlab SE, AutoScout24, Charlotte Tilbury, and The Sage Group across France, Germany, and the Netherlands. The JLR attack also connected to the August 2025 Salesloft/Drift OAuth token campaign, which compromised over 700 organizations.

Activity in 2025

6+ incidents

T1598.003 Spearphishing Link

T1598.004 Spearphishing Voice

T1656 Impersonation

T1195 Supply Chain Compromise

T1219 Remote Access Tools

Why it matters

The JLR attack proved that European automotive and luxury manufacturers are now targets for zero-day exploitation, not just social engineering. A five-week production shutdown and \$250 million in losses is the new benchmark for what a supply chain breach can cost a European manufacturer.



State-sponsored threats: the quiet backdrop

The threat actors profiled above are the most active against European manufacturing by incident volume. But more secretive yet very disruptive threats are state-sponsored groups who seek persistent access, operational intelligence, and the ability to disrupt physical processes on command. Two groups have clearly demonstrated this capability against European manufacturing over the past year.



BlackEnergy

Active since
at least 2010

APT

OT/IT destructive operations

About

BlackEnergy is a sophisticated state-sponsored threat actor primarily focused on the energy, government, military, and telecommunications sectors.

In December 2025, BlackEnergy executed coordinated destructive operations against Poland's energy and manufacturing sectors, targeting over 30 wind and solar farms, a combined heat and power (CHP) plant serving nearly half a million customers, and a manufacturing company. The group exploited internet-exposed FortiGate VPN appliances configured with static credentials and no multi-factor authentication to gain administrative access to operational technology at renewable energy grid connection points.

The group destroyed industrial control devices at scale. Hitachi RTU560 controllers were disabled by corrupted firmware uploads that triggered reboot loops. Mikronika RTUs had system files deleted via SSH root access. Hitachi Relion 650 protection relays were wiped through default FTP accounts. Moxa NPort serial device servers were factory-reset with unreachable IP addresses. Devices were targeted in ascending IP order, which indicates automated tooling designed for scale.

At the manufacturing target, the group deployed LazyWiper, a PowerShell-based wiper distributed via Group Policy Object. At the CHP plant, BlackEnergy had been inside since at least March 2025, conducting reconnaissance of SCADA systems, extracting Active Directory databases, and exfiltrating FortiGate configurations before deploying DynoWiper malware to over 100 machines.

Activity in 2025

Multiple incidents

T1561 Disk Wipe

T0881 Service Stop

T1021.002 Remote Services: SMB

T0888 Remote System Information Discovery

T0836 Modify Parameter



Why it matters

BlackEnergy demonstrated capability to permanently disable RTUs, protection relays, and HMIs across 30+ sites simultaneously using default credentials on internet-exposed VPN appliances. European manufacturers with FortiGate perimeter devices, unsecured remote access to OT networks, or industrial equipment from Hitachi, Mikronika, or Moxa should treat this actor as a direct threat to their own infrastructure.



TAG-100

aka RedNovember

Active since
2024

APT

Cyber-espionage

About

TAG-100 is a Chinese state-sponsored group conducting cyber-espionage operations against government, defense, aerospace, and manufacturing organizations in Europe and beyond. What makes the group particularly dangerous is its speed: TAG-100 weaponizes public proof-of-concept exploits within days of release and targets internet-facing security appliances at scale, including SonicWall, Cisco ASA, F5 BIG-IP, Palo Alto GlobalProtect, Fortinet FortiGate, and Ivanti Connect Secure VPN instances.

In March 2025, TAG-100 conducted reconnaissance and likely compromised a European engine manufacturer by targeting SonicWall VPN devices and F5 BIG-IP login pages. The group also targeted a UK defense contractor's SonicWall instance and reconnoitered a UK cable harnessing company serving aerospace, military, defense, and medical sectors. In April 2025, TAG-100 targeted a European space research center and conducted spearphishing operations against US defense contractors. The group uses open-source tools including the Go-based backdoor Pantegana, Cobalt Strike, and SparkRAT, and maintains operational security through ExpressVPN and Warp VPN infrastructure.

Activity in 2025

Multiple incidents

T1190 Exploit Public-Facing Application

T1505.003 Server Software Component: Web Shell

T1571 Non-Standard Port

T1567.002 Exfiltration to Cloud Storage

T1566.001 Spearphishing Attachment

Why it matters

TAG-100 has already targeted European engine manufacturers, defense contractors, and aerospace supply chain companies. Manufacturers relying on SonicWall, Palo Alto, Fortinet, or Ivanti perimeter devices with delayed patching cycles are directly exposed. The objective is long-term access and intellectual property theft, and victims may never know they were compromised unless they actively look.

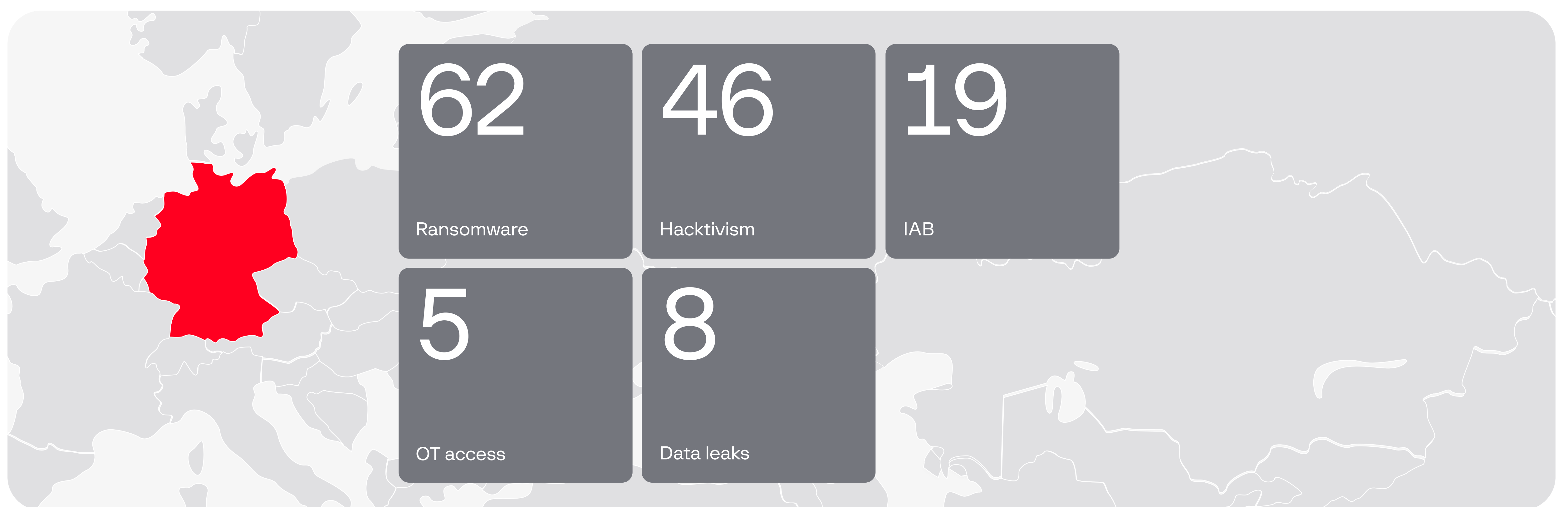


Country profiles

Six countries, one threat landscape, 2025–2026

Germany

Highest hacktivism load. Second in ransomware and IAB. Under pressure from every actor type.

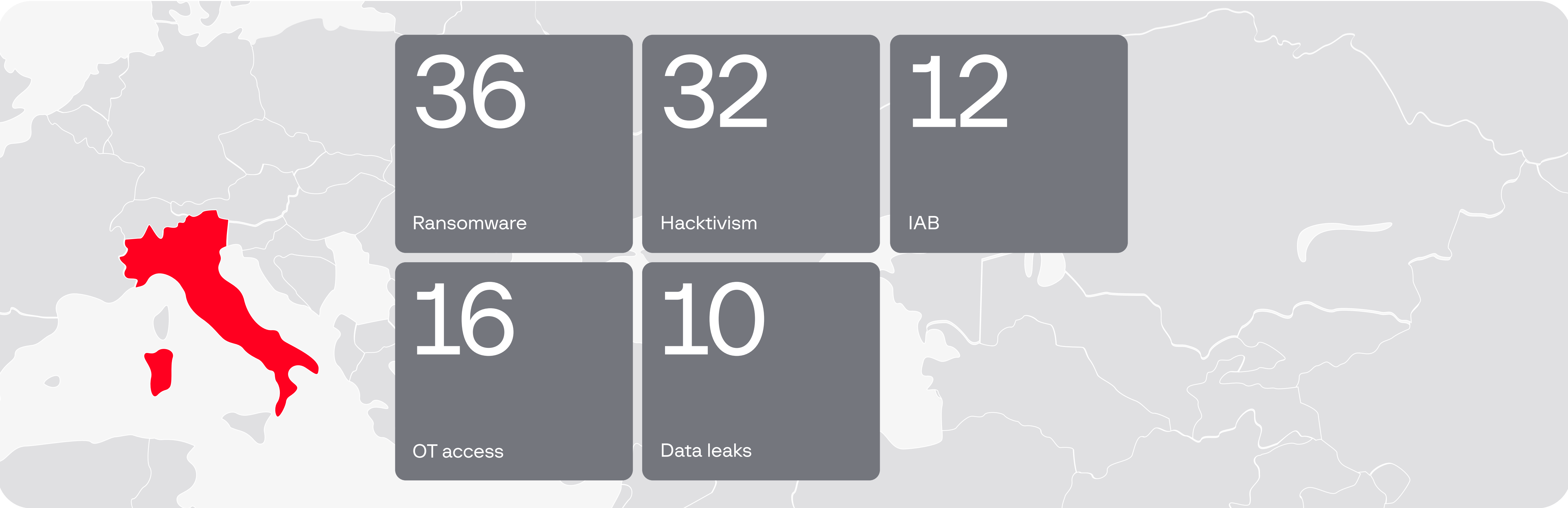


Key incidents

- + **#OpGermany:** Guhring, Sennebogen, and Voith targeted in coordinated DDoS attacks
- + **SafePay ransomware:** attack on SETEX Textil GmbH
- + **Scattered Spider:** targeted Brainlab SE and AutoScout24
- + **Stillnet:** equipment disruption at Lauber Trocknungstechnik and WesaTec
- + **Z-ALLIANCE:** compromised production systems at Kaserei Zeltuurner

Italy

Digital attacks with physical consequences.
OT access at scale.

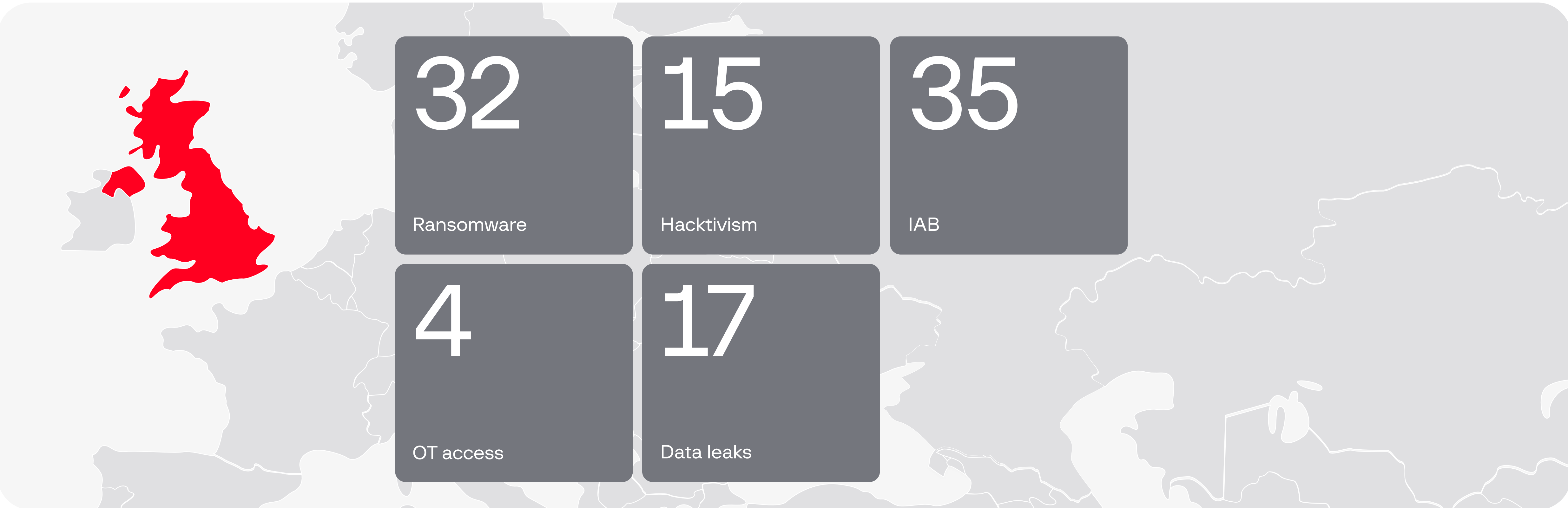


Key incidents

- + **NightSpire:** Giaroli sas (March 2026)
- + **The Gentlemen:** Silvi Srl (March 2026)
- + **Qilin:** 15+ attacks including Csv Group, Callipo Group, Sacca Industrie
- + **DragonForce:** Ponzini S.p.A., Autorotor, Framon Spa
- + **Z-ALLIANCE:** gained control of boiler and refrigeration systems at Ranieri Impiantistica
- + **Sauron of Eye:** documented control over pasteurization and fire protection at a dairy facility
- + **NoName057(16):** HVAC control system access at industrial facility (Feb 2026)

United Kingdom

Most targeted by ransomware and IAB activity. Enterprise platform attacks against industrial brands.

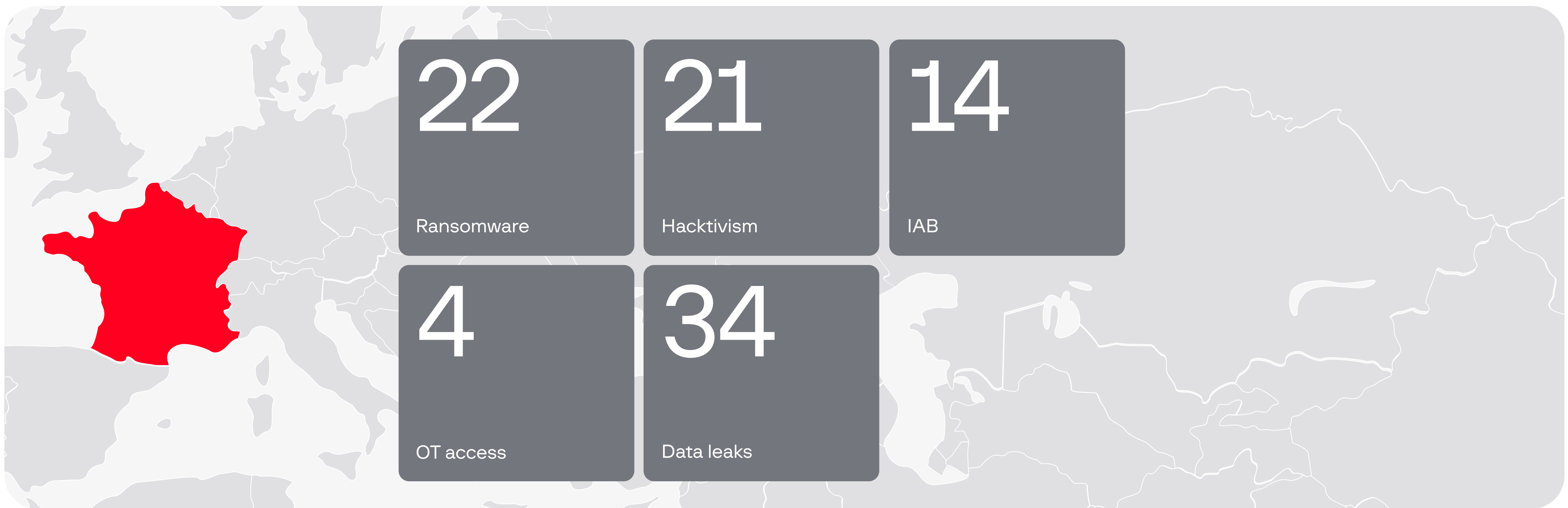


Key incidents

- + **The Gentlemen:** Nenplas Ltd (March 2026)
- + **Qilin:** 20+ attacks including Albany Pumps (March 2026), Moontown, Gtech, Mainetti
- + **Scattered Spider:** JLR SAP NetWeaver zero-days, five-week shutdown, ~\$250M losses; Charlotte Tilbury and The Sage Group
- + **AiLock ransomware:** attack on FUJIFILM Speciality Ink Systems
- + **DragonForce:** Adelphi, Caramel Ltd, GPC Industries
- + **Z-ALLIANCE:** MPAC Automation & Controls OT access

France

Systematic theft of strategic intellectual property. Espionage-grade interest meets cybercriminal methods.

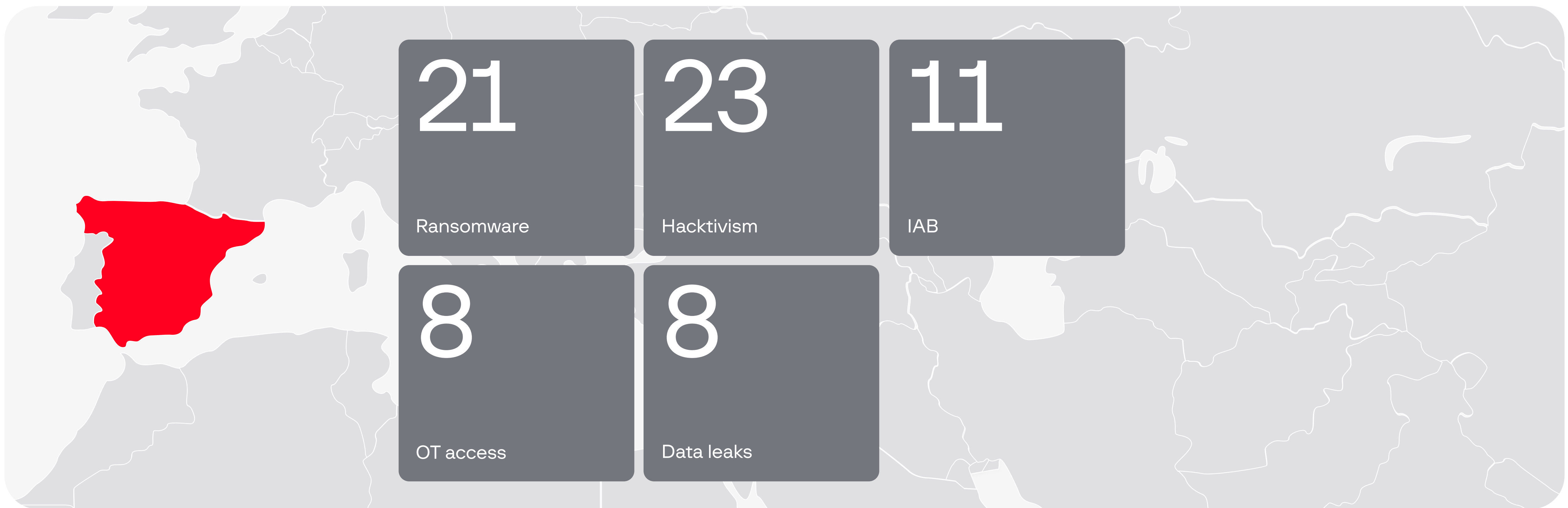


Key incidents

- + **Scattered Spider:** credential harvesting campaigns targeting LVMH and Dior
- + **Lockbit:** CTI-Bat (March 2026)
CI0p: Ransomware attacks hit Schneider Electric and Michelin
- + **The Gentlemen:** ransomware attacks on Sodimatel (March 2026), Hafa, Saelen France
- + **Aerospace/defense targets:** Safran, Thales Group, Naval Group
- + **NoName057(16):** OT access to Chalvignac Prulho Distillation

Spain

OT hacktivist proving ground. Several groups are actively testing capabilities against Spanish infrastructure.

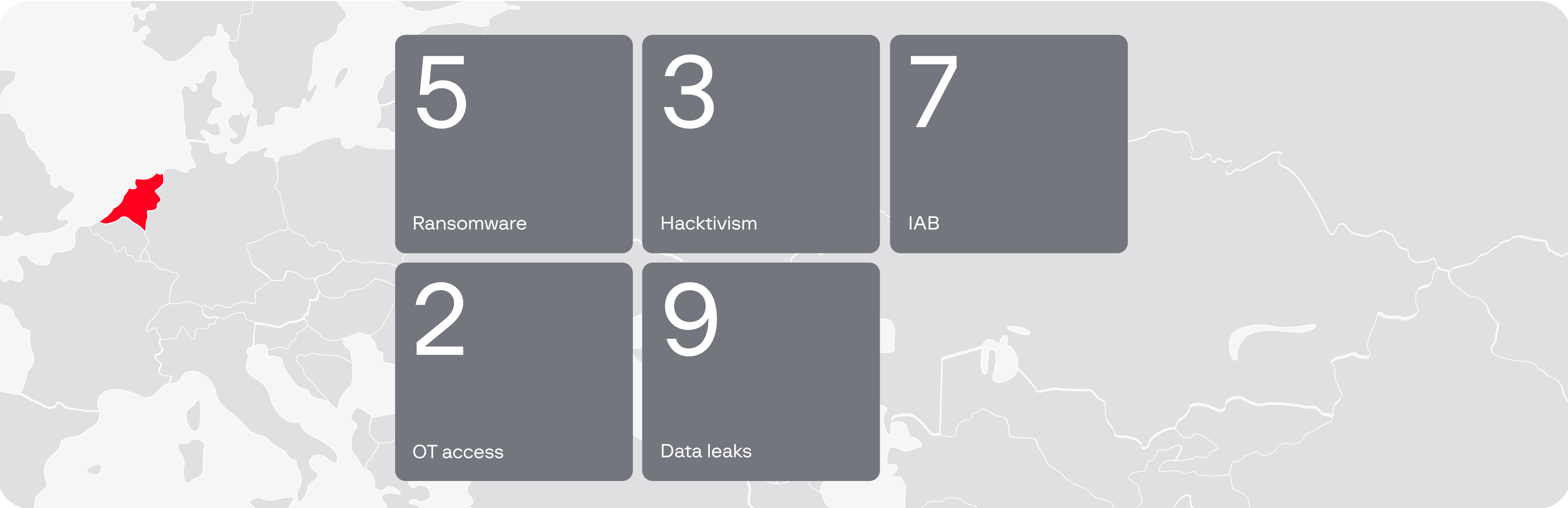


Key incidents

- + **Akira:** AGME, Ste Group, Arcusin, Ondunova
- + **Qilin:** José Combalía SA, Gaviota, Atarfil Geomembranes
- + **Z-ALLIANCE:** claimed OT access to industrial refrigeration and control systems
- + **Z-Pentest:** Topinstal S.L. OT access
- + **NoName057(16):** Metalica Arroyo S.L
- + **Big-Bro:** 7+ manufacturing access sales
- + **Ferrovial database** sold on underground forums

Netherlands

Small sector, globally irreplaceable targets.
Semiconductor and chemical supply chain
chokepoints



Key incidents

- **ASML:** 154 databases allegedly compromised including disk encryption keys (Jan 2026)
- **Anubis ransomware:** AkzoNobel (March 2026)
- **Z-ALLIANCE:** OT access to automotive plant and industrial palletizer in Bergschenhoek
- **Big-Bro:** 6+ manufacturing access sales
- **Scattered Spider:** KLM targeted in Salesforce credential harvesting campaign
- **Perfetti Van Melle:** 13,500 employee records leaked

Recommendations

Shifting from reactive OT patching to preemptive external intelligence

Immediate priorities.
Act now

01. Monitor underground forums for IAB activity

Track active IAB campaigns targeting your sector and region before access is sold to ransomware operators. IAB activity is typically visible weeks before a ransomware attack materializes, and that window is your earliest opportunity to act. Some access listings never appear on public forums and circulate instead in private markets or closed communities. That is why visibility into the broader underground ecosystem is essential.

02. Audit externally accessible OT and IT infrastructure

Internet-exposed industrial services, supplier VPN accounts, and forgotten infrastructure should be the first priority. The majority of OT access events documented in this report originated from externally accessible systems, not from internal OT network compromises. Recent JLR attacks demonstrate that IT infrastructure is critical to OT security. Beyond serving as a network pivot point, IT environments often act as intelligence gateways that attackers leverage to map internal OT structures. Consequently, both environments must be audited.

03. Close the segmentation gap between IT and OT

Poor IT/OT network segmentation remains the most common architectural weakness in manufacturing environments. When corporate and industrial networks share domains or allow lateral movement without restriction, a single compromised credential can propagate from an email inbox to a PLC. Group-IB recommends enforcing logical or physical segmentation between IT and OT zones, implementing Zero Trust architecture for cross-zone traffic, and restricting remote access to industrial systems through monitored jump servers with just-in-time privileged access controls.

04. Determine if your environment is already compromised

Every IAB listing in this report represents a network that was already breached, and without a dedicated assessment, you simply don't know if you're already in scope.

Sustained capabilities. Build in 2026

01. Build ransomware group intelligence into security planning

Understand which ransomware groups are currently active in your region and sector. Qilin, Akira, and DragonForce have distinct targeting preferences, TTPs, and affiliate patterns that can inform defensive prioritization. Understanding how these threat groups evolve is crucial for prioritizing your defenses.

02. Treat hacktivist OT access claims as physical safety risk

57 OT access claims in 2025 represent a real and growing capability among politically motivated actors. OT security teams in Italy, Spain, and Germany should treat Z-ALLIANCE and other hacktivist groups as physical-impact threat actors.

03. Eliminate default and weak credentials across OT environments

Default or vendor-supplied credentials on industrial equipment remain a low-effort path to unauthorized access. While the prevalence of default credentials has declined in recent years, weak password practices, credentials stored in human-readable formats, and shared accounts continue to give attackers a foothold once they reach the OT network. Every credential used for remote access to industrial systems should be unique, rotated, and protected by multi-factor authentication.

04. Deploy endpoint protection where it matters most

Use up-to-date Managed XDR on jump servers and systems within the OT DMZ to protect critical access points without disrupting operational systems, and complement this with OT-aware network monitoring capable of detecting industrial-specific threats that signature-based tools miss.

05. Establish continuous external data footprint monitoring

Understand what intellectual property has already been exfiltrated and where it is circulating. This is especially critical for French and British manufacturers, where data leak volumes are disproportionately high.

Vulnerability management across IT and OT environments

The attacks documented in this report share a common entry point: unpatched perimeter devices. Throughout 2025, adversaries actively exploited vulnerabilities in Ivanti Connect Secure, Palo Alto PAN-OS, Fortinet FortiOS, F5 BIG-IP, and Cisco ASA/FTD, often using public proof-of-concept exploits within days of disclosure.

For manufacturers, vulnerability management must account for two realities. Internet-facing devices (VPN gateways, firewalls, remote access systems) need emergency patching SLAs because they are where attacks start. OT systems deeper in the network often cannot be patched without operational disruption, making compensating controls, segmentation, and continuous monitoring the practical alternative.

Prioritization should go beyond CVSS scores. What matters is whether a vulnerability is externally reachable, whether a public exploit exists, and whether the affected system bridges IT and OT or directly influences physical processes. Asset inventories should explicitly track internet-exposed devices, cellular gateways, and vendor-managed systems, which are often the blind spots that attackers reach first. Remediation efforts should focus on reducing externally reachable attack surfaces and limiting the feasibility of control-loop mapping, unauthorized access, and downstream operational manipulation.

[Group-IB Attack Surface Management](#) continuously discovers and maps these blind spots: the internet-exposed OT interfaces, forgotten infrastructure, and vendor-managed systems that your internal asset inventory may not cover. [Group-IB Threat Intelligence](#) tracks which vulnerabilities are being actively exploited by the threat actors profiled in this report and which proof-of-concept exploits are circulating in underground channels, so your patching priorities reflect what attackers are actually targeting.

Learn more about Group-IB Solutions for Vulnerability Management

How Group-IB addresses each threat category in this report

Network access to your organization may already be for sale

[Group-IB Threat Intelligence](#) gives manufacturing security teams continuous visibility and expertise into underground markets where access to their networks is sold, ransomware affiliate channels and chats where targeting decisions are made, and hacktivist channels where the next country campaign is announced. **Prevyn AI**, the cognitive core of Group-IB products, accelerates this work by orchestrating specialist agents that hunt across dark web forums, profile threat actor TTPs, and correlate findings into structured intelligence reports in minutes rather than hours. [Group-IB Attack Surface Management](#) maps the external attack surface: OT interfaces, supplier connections, and shadow infrastructure that threat actors are already enumerating.

You may already be compromised

[Group-IB Compromise Assessment](#) scans for indicators of IAB activity, ransomware pre-staging, and advanced persistent access that conventional security tools do not surface. It combines enterprise-wide endpoint sweeps, network analysis, and dark web intelligence to uncover active and past breaches. For manufacturers in Germany, France, or Italy, where IAB incidents are highest, this answers the question: has it already happened to us?

Ransomware is staging in your network

[Group-IB Managed XDR](#) provides 24/7 detection and response across IT and OT-adjacent infrastructure, identifying ransomware staging, lateral movement, and credential abuse in the window between initial access and encryption. For manufacturing environments where downtime is measured in production weeks, early detection determines the scale of the impact.

Your defenses may not have been tested against real attacker tradecraft

[Group-IB Red Teaming](#) uses proprietary threat intelligence (TTPs, access vectors, vulnerabilities) to simulate intrusions grounded in what is happening to European manufacturers right now. It mimics the attack chains documented in this report, from exposed perimeter devices through credential harvesting and lateral movement into OT-adjacent systems, to answer the question: where does your segmentation actually fail under real pressure?

Your intellectual property is circulating on underground markets

[Group-IB Digital Risk Protection](#) monitors underground markets for data belonging to your organization: leaked credentials being traded, intellectual property being sold, and broker activity that signals your data has already left your environment. The platform's three-stage takedown process ensures that malicious resources are quickly identified and eliminated, which reduces risks to European manufacturers at early stages.

Your team may not be prepared for this scenario

When a ransomware operator encrypts sensitive information at 2am on a Friday, can your IT security team, OT engineers, plant managers, and crisis leadership coordinate a response without disrupting running production processes? [Group-IB Tabletop Exercises](#) simulate realistic manufacturing intrusion scenarios based on adversary TTPs from Group-IB's Threat Intelligence.

An attack is underway

[Group-IB Incident Response](#) provides 24/7 expert containment with OT/ICS specialization across European jurisdictions, designed to limit operational downtime and contain the breach before data reaches a leak site. For manufacturing environments, this means reconstructing attack timelines across I T and OT boundaries, identifying persistence mechanisms in industrial environments, and coordinating remediation without introducing additional risk to running production processes.

About Group-IB



Global partnerships



Recognized by top industry experts



Fight Against Cybercrime