DARKTRACE

ANNUAL THREAT REPORT 2026: EUROPE REGIONAL OUTLOOK

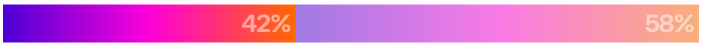
The global cyber threat landscape in 2025 was increasingly defined not by uniform trends, but by regional threat economies shaped by maturity, geopolitics, the speed of digitization, and attacker objectives. This regional breakdown provides a focused analysis of the key threat trends, notable threat actors, and outlook for Europe.

The European cybersecurity market grew by over 10% in 2025 [1], reflecting economic and geopolitical factors such as the introduction of mandatory regulation [2] and increased pro-Russian hacktivists targeting organizations in NATO member states and other countries in opposition to Russia's national interests [3].

REGIONAL TRENDS AND STATISTICS

TOP ATTACK VECTORS

In 2025, cloud account and email compromises accounted for 58% of incidents observed across Darktrace's customer base, significantly exceeding network-based compromises which comprised the remaining 42%.



Attackers are capitalizing on Europe's 'cloud-first' mentality [4] and the corresponding shift of sensitive data to those environments, ongoing challenges securing cloud identities [5] and lack of visibility and control within shared ownership models [6].

MOST IMPACTED SECTORS

Across Europe, the highest share of observed incidents across the Darktrace fleet originated from organizations based in:

- Manufacturing
- Professional scientific and technical activities
- Information and communication
- Financial and insurance
- Construction
- Human health and social work activities

The uptick in attacks on these sectors reflect attackers' shifting focus to the technology stack and infrastructure that underpins operational processes, critical societal functions and permits downstream access to multiple nodes along the supply chain from one source [7].

NOTABLE THREAT ACTORS

Actor	Motivation & Targets	Key Tactics
ShadowPad-linked Chinese state-sponsored actors	**Stealthy persistence;** Manufacturing & critical IT assets	**DNS tunneling** (T1071.004) **SSL C2** (T1071.001) **Privileged credential misuse** (T1078)
Lazarus Group	Democratic People's Republic of Korea (DPRK) state-sponsored Advanced Persistent Threat (APT) known for its dual focus on cyber espionage and financial theft.	Social engineering via **fake recruitment campaigns** Use of **trojanized applications** and npm packages **Credential theft** and cryptocurrency wallet targeting **Deployment of remote access tools** (e.g., AnyDesk) and command-and-control via Telegram Living-off-the-land (LOTL) techniques using **PowerShell and legitimate binaries**
Akira Ransomware	Akira ransomware was first observed in the wild in March 2023 and has since emerged as one of the most active and widely deployed ransomware families across the global threat landscape. Operating under a Ransomware-as-a-Service (RaaS) model, the group consistently leverages double-extortion tactics, demanding payment both for file decryption and to prevent the public release of sensitive data exfiltrated during intrusions. Akira targets organizations across a broad range of sectors, including Manufacturing, Education, and Healthcare, with activity observed across North America, Latin America, Europe, and the Asia-Pacific region.	**Initial Access** Targets remote access services such as RDP and VPN through vulnerability exploitation or stolen credentials. **Reconnaissance** Uses network scanning tools like SoftPerfect and Advanced IP Scanner to map the environment and identify targets. **Lateral Movement** Moves laterally using legitimate administrative tools, typically via RDP. **Persistence** Employs techniques such as Kerberoasting and pass-the-hash, and tools like Mimikatz to extract credentials. Known to create new domain accounts to maintain access. **Command and Control** Utilizes remote access tools including AnyDesk, RustDesk, Ngrok, and Cloudflare Tunnel. **Exfiltration** Uses tools such as FileZilla, WinRAR, WinSCP, and Rclone. Data is exfiltrated via protocols like FTP and SFTP, or through cloud storage services such as Mega.

COUNTRY & SECTOR SPOTLIGHTS

The following section presents an analysis of country- and sector-specific attacks observed by Darktrace in Europe in 2025, focusing on key sectors across each country: Financial Services in the UK, Manufacturing in Germany, and Retail in France.

UNITED KINGDOM

The UK threat landscape in 2025 was shaped by challenges from both foreign actors and native-English-speaking attackers who targeted key supply chain functions and Technology organizations. The activities of Scattered Spider, a threat group with US and UK affiliates, highlighted the UK's exposure to native-English social engineering and underscored critical supply chain vulnerabilities, most notably in the Jaguar Land Rover attack, which reduced UK gross domestic product (GDP) by 0.1% [8].

In 2025, the UK published its Modern Industrial Strategy, in which the Financial Services sector was listed as a key sector to build investment and deliver a competitive regulatory environment that harnesses the UK's global leadership in Fintech [9]. The UK Financial Services market is becoming increasingly targeted by threat actors interested in this sector, such as DPRK-affiliated actors, particularly in response to heightened US scrutiny in 2025.

CASE STUDY

In 2025, Darktrace detected the activities of Lazarus Group in a UK Forex firm and a UK cryptocurrency organization.

Forex Organization: A developer was socially engineered on a third-party social media platform into running malicious code hosted on GitHub, which likely contained malicious npm packages. From there, the Lazarus group accessed the internal network using Astrill VPN, a third-party VPN commonly associated with the group. Subsequent activity indicated the presence of an infostealer, used for further data collection and exfiltration.

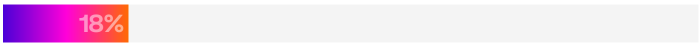
Cryptocurrency organization: Multiple users, including VIPs, were targeted over an extended period by likely Lazarus Group threat actors. In one case, mirroring elements of the group's "Contagious Interview" campaign, a user was approached with a fraudulent job opportunity and instructed to run Terminal commands framed as troubleshooting steps, ultimately installing malicious drivers.

Following infection, the compromised devices executed obfuscated Python scripts designed to retrieve additional payloads from Pastebin, scan for crypto-related information, and download further malware such as the Tsunami Injector for keylogging and credential theft. The malware then exfiltrated collected data to a command-and-control server.

Darktrace's Threat Research team also observed the malware removing itself, underscoring the stealthy and operationally disciplined nature of the activity.

FRANCE

The Retail sector represents 18% of France's GDP [10]. High-end, luxury fashion in particular holds a strong cultural significance in France, with major international brands and conglomerates operating flagship stores in the Paris region [11]. Thus, these are attractive targets to financially-motivated cybercriminals who hope to capitalize on the data of high net worth individuals for secondary attacks [12].



In 2025, several French luxury brands were targeted by ShinyHunters ransomware group. Open-source reporting indicates that the attack likely involved initial access via Salesloft drift and Salesforce account compromise, leading to sensitive customer data exposure [13]. As an example of later stage attacks, Darktrace's Threat Research team detected a Black Friday phishing email campaign attempting to impersonate the luxury fashion brand Louis Vuitton that redirected users to a malicious, newly registered Russian domain.

In another attack, the multinational retail giant Auchan experienced a data breach where the data and Personally Identifiable Information (PII) of thousands of customers was stolen from the company's loyalty program and customer information database [14].

While customer PII is a lucrative financial incentive for threat actors, and data-theft attacks on third-party cloud applications like Salesforce have risen this year [15], threat actors with more strategic objectives often leverage unsecured third-party applications as entry points to the wider network. This behavior was exemplified by Darktrace's pre-CVE detection in SAP Netweaver, which was chained with the Auto-Colour backdoor malware.

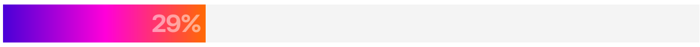
CASE STUDY

In 2025, Darktrace detected multiple SaaS compromises affecting a French Automobile and Retail distributor. In one case, a VIP was targeted by a phishing attack delivered via Microsoft Forms, enabling the attacker to steal the user's credentials. The attacker then logged in using a third-party commercial VPN and created an email rule that redirected financially-related messages to the Spam folder, likely to obscure signs of fraudulent activity.

This activity reflects sustained phishing efforts and classic business email compromise (BEC) tradecraft aimed at concealing financial fraud while maintaining persistence within the victim's SaaS environment.

GERMANY

Germany hosts Europe's largest industrial economy, generating 29% of the European Union's (EU) gross value, and in Manufacturing alone [16]. Rapid digital transformation in German production has placed its Manufacturing industry at the forefront of Industrial Internet of Things (IIoT) adoption [17]. However, such adoption and resultant IT-OT convergence introduce new vulnerabilities to sensitive OT networks.



The presence of IP and patents within this sector make it attractive to both financially-motivated and state-sponsored threat actors [18]. For instance, China's industrial policy places strategic importance on Germany's core sectors, including automotive and mechanical engineering. China's rapid advancements in the automotive industry and its growing share of industrial machinery exports have now surpassed Germany's declining share [23].

Darktrace's analysis of attacks in Germany in 2025 revealed a threat landscape increasingly shaped by SaaS-centric attacks and growing operational complexity. Hybrid email deployments and legacy configurations continue to create visibility gaps, slowing security teams' response times. Attackers are exploiting multi-factor authentication (MFA) weaknesses and DNS-based channels at higher rates, blending traditional phishing with more advanced persistence techniques.

CASE STUDY

In 2025, Darktrace detected the activities of state-sponsored malware in a German automation solution manufacturer. ShadowPad is a modular remote access trojan (RAT) that has been deployed by Chinese state-sponsored threat groups [20]. Although the exact initial access vector was unknown, Darktrace's previous analysis of ShadowPad activity in the European Manufacturing sector indicated entry via compromised VPN credentials.

The organization's Domain Controllers (DCs) were beaconing to rare external IPs associated with this malicious backdoor's infrastructure over DNS TXT records, likely using this protocol to tunnel data. Further privilege escalation was observed over external NTLM connections and Kerberos login requests for administrative credentials as the attackers probed internally. Organizations should continuously monitor privileged accounts and alert on new administrative credential usage on servers. External VPN logins to DCs should be treated as high-severity precursors and paired with MFA hardening and device baselines.

GOVERNMENT & REGULATORY OVERVIEW

SIGNIFICANT REFORMS TO SECURITY POLICY AND REGULATION ADVANCED ACROSS EUROPE IN 2025:

The European Union's Digital Operational Resilience Act (DORA) came into force on January 16, 2023, with mandatory compliance required by January 17, 2025. This is aimed at enhancing the operational resilience of financial institutions and emphasizes proactive measures over reactive financial compensation.

The NIS2 Directive was implemented in several European member states [21]. This widened the list of sectors defined as "important," placing additional "duty of care" requirements that each organization must follow. This includes both proactive and preventative security measures and improved response and reporting following an active threat. Under NIS2, Manufacturing and larger Retail organizations with an annual turnover of over EUR 10 million, among others, are within scope [22, 23]. While NIS2 will help businesses and services build resiliency, implementation may perpetuate existing resource constraints around budget and security expertise [24].

The UK government's new **Cyber Security and Resilience Bill** was introduced to modernize UK cyber laws, to recognize the risk posed by the supply chain and place industry best-practice, such as the UK National Cyber Security Centre's (NCSC) Cyber Assessment Framework, on firmer footing. Under this, Managed Service Providers and data centers are intended to be added to the scope of regulation to better recognize the increasing reliance on digital services and the vulnerabilities posed by supply chains.

This sets clearer government expectations on technical standards and methods organizations will need to follow to prove their resilience [25], shifting the focus from compliance to resilience [26].

INSIGHTS & OUTLOOK

For Europe, 2026 presents a continuously evolving cyber landscape shaped by economic growth and technological innovation to ensuring Europe's competitive advantage and resilience amidst heightened geopolitical concerns.

Across Europe, escalating geopolitical threats have highlighted the risks of dependence on US and Chinese providers of cloud, Telecommunications and AI infrastructure. Global competition to achieve 6G technology has placed concerns around the role of Chinese vendors in European infrastructure and their risk [27]. As the EU pushes for physically and logically separate infrastructure [28,29], organizations should continue to adopt a "trust-but-verify" model, where less trusted areas of the supply chain are continuously assessed and mitigated with risk-based controls.

In the UK, the Government's National Payments Vision and plans to create scalable digital verification and identity calls for more partnerships between the public and private sectors and presents challenges associated with blending variations of centralized and decentralized verification and secure information sharing amongst customers and institutions [30]. Lessons learned from enterprises around securing Identity will be a crucial factor to this.

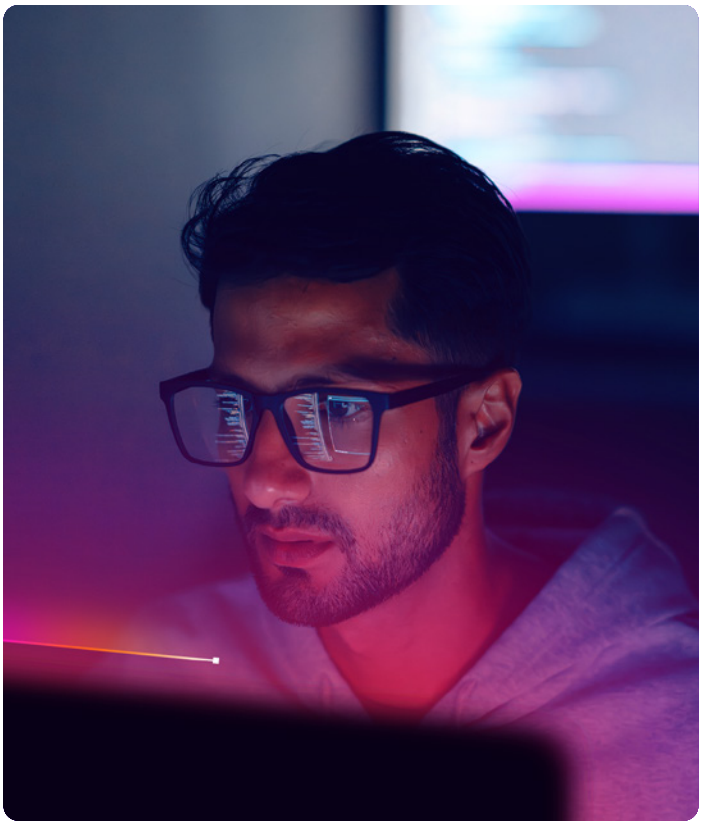
Taken together, cyber resilience for Europe has become a critical enabler for economic competitiveness, technological leadership and geopolitical stability. Europe's external dependence on governed cloud, Telecommunications, and AI infrastructure has elevated supply chain security from an operational concern to a strategic risk, driving policy shifts toward infrastructure separation, sovereignty, and assurance by design.

Successfully delivering these ambitions will depend on sustained public-private collaboration, interoperable design, and the application of enterprise-grade identity security practices at national scale.

Ultimately, Europe's ability to navigate this evolving cyber landscape will be defined by how effectively it balances openness with resilience—leveraging innovation while systematically managing geopolitical and supply-chain risk to preserve trust in its digital future.

REGIONAL ANALYSIS METHODOLOGY:

It is important to note that while the analysis is relevant and broadly representative of wider global trends, it is also influenced by the geographic distribution of Darktrace's customer base. For example, within the AMS region, the US represents the largest share of Darktrace customers, meaning insights in this section may be weighted more heavily toward US-based activity.



[1] [Online]. Available: https://www.mordorintelligence.com/industry-reports/europe-cybersecurity-market.

[2] [Online]. Available: https://www.enisa.europa.eu/news/whats-driving-cybersecurity-investments-and-where-lie-the-challenges.

[3] [Online]. Available: https://www.ncsc.gov.uk/news/ncsc-issues-warning-over-hacktivist-groups-disrupting-uk-organisations-online-services.

[4] [Online]. Available: https://dtpgroup.co.uk/insight/50-cloud-computing-statistics.

[5] [Online]. Available: https://www.bankinfosecurity.com/cloud-identity-exposure-a-critical-point-failure-a-29924.

[6] [Online]. Available: https://sitsi.pacanalyst.com/part-6-cloud-security-shared-responsibility-and-real-accountability/.

[7] [Online]. Available: https://industrialcyber.co/reports/businesses-and-manufacturing-bear-brunt-of-36-ransomware-spike-as-government-and-healthcare-see-declines/.

[8] [Online]. Available: https://minipip.co.uk/details/news/jaguar-land-rover-cyber-attack-costs---200-million-and-hits-uk-gdp.

[9] [Online]. Available: https://www.gov.uk/government/calls-for-evidence/financial-services-growth-and-competitiveness-strategy/outcome/financial-services-growth-and-competitiveness-strategy-overview.

[10] [Online]. Available: https://transfer.lc/french-retail-market/.

[11] [Online]. Available: https://www.chooseparisregion.org/industries/fashion-luxury.

[12] [Online]. Available: https://www.kelacyber.com/wp-content/uploads/2022/10/KELA-RESEARCH_France-Threat-Landscape-Report_-Luxury-Industry.pdf.

[13] [Online]. Available: https://www.symmetry-systems.com/blog/what-we-know-so-far-about-salesloft-and-other-recent-salesforce-breaches/.

[14] [Online]. Available: https://www.securityweek.com/hundreds-of-thousands-affected-by-auchan-data-breach/.

[15] [Online]. Available: https://cloudprotection.com/blog/salesforce-attacks-in-2025/.

[16] [Online]. Available: https://www.gtai.de/en/invest/business-location-germany/market-germany-europe-s-economic-hub#toc-anchor—1.

[17] [Online]. Available: https://senzemo.com/iot-solutions-for-the-german-market-key-industry-conferences.

[18] [Online]. Available: https://www.bitkom.org/EN/List-and-detailpages/Press/German-business-losses-more-than-220-billion-euros-per-year.

[19] [Online]. Available: https://www.dw.com/en/china-puts-pressure-on-german-car-chemicals-engineering-industry/a-71919309.

[20] [Online]. Available: https://www.sophos.com/en-gb/research/shadowpad-malware-analysis.

[21] [Online]. Available: https://www.darktrace.com/blog/nis2-compliance-interpreting-state-of-the-art-for-organisations.

[22] [Online]. Available: https://www.logisticsit.com/articles/2023/07/05/a-look-at-new-in-the-nis2-directive?__cf_chl_tk=gKfPKYT7K1P1OMrRMIEzWO6LDFFt35OPyE6_bZ359vo-1768949517-1.0.1.1-0IZrxZJ4_zcMFBoc4dyBuSK-0NyBSYIf65t6FtFDeUEc.

[23] [Online]. Available: https://secomea.com/blog/compliance/nis2-scope-essential-important-entity/.

[24] [Online]. Available: https://www.darktrace.com/resources/7-steps-to-get-ahead-with-nis2.

[25] [Online]. Available: https://www.darktrace.com/blog/modernising-uk-cyber-regulation-implications-of-the-cyber-security-and-resilience-bill.

[26] [Online]. Available: https://www.darktrace.com/blog/uk-cyber-security-and-resilience-bill-what-it-means-for-organizations .

[27] [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757633/EPRS_BRI(2024)757633_EN.pdf.

[28] [Online]. Available: https://www.youtube.com/watch?v=7CVz57sLVPw&t=15s.

[29] [Online]. Available: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en.

[34] [Online]. Available: https://www.theglobalcity.uk/insights/thought-pieces/scaling-digital-verification-solutions.

About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit www.darktrace.com.