CSIS

DELIVERED BY SECALLIANCE

Threat Matrix

European Threat Landscape Report

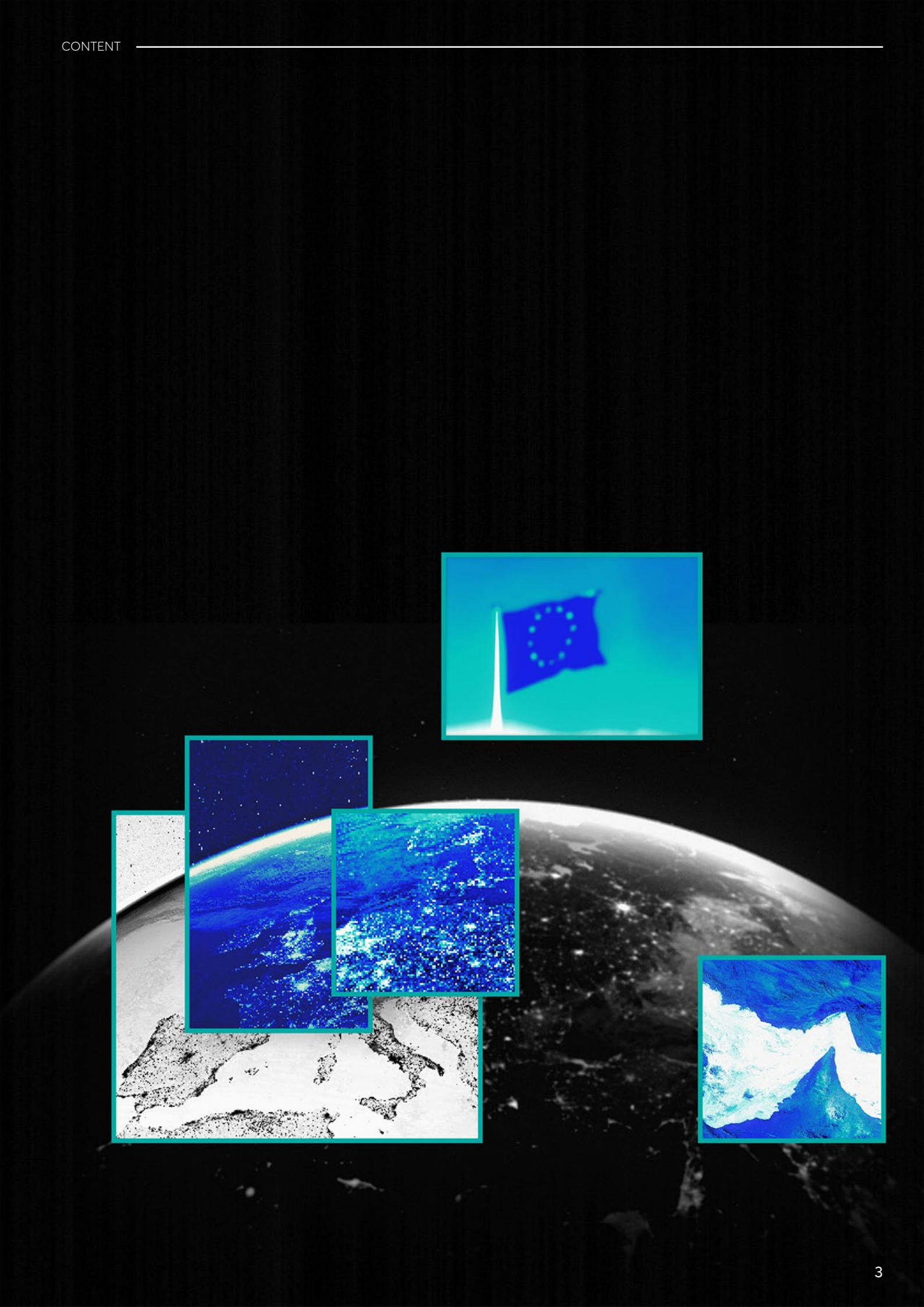
October 2026



csis.com

CONTENT

Foreword	04
Executive Summary	05
Geopolitical Overview	08
Regulatory Updates	12
Event Timeline	16
Metrics	18
Trends	36
Insights	48
Assessments	55
Forecasts	68
Assessment Terminology	73
CSIS Updates	74



FOREWORD

Following growing geopolitical instability in Europe's relations with the US, China and Russia, aligned with increasing technological threats, I made the decision this year that we would look to address these challenges by merging our traditional Threat Matrix report with the Threat Landscape reporting provided by our SecAlliance Intelligence team, thereby creating a new Europe-focused threat landscape report that provides a more holistic view of geopolitical and cyber threats directly affecting Europe. This new report utilises data and perspectives gathered from across Europe and aims to support executive decision making whilst continuing to deliver value across the full spectrum of organisational stakeholders through valuable insights, assessments and predictions.

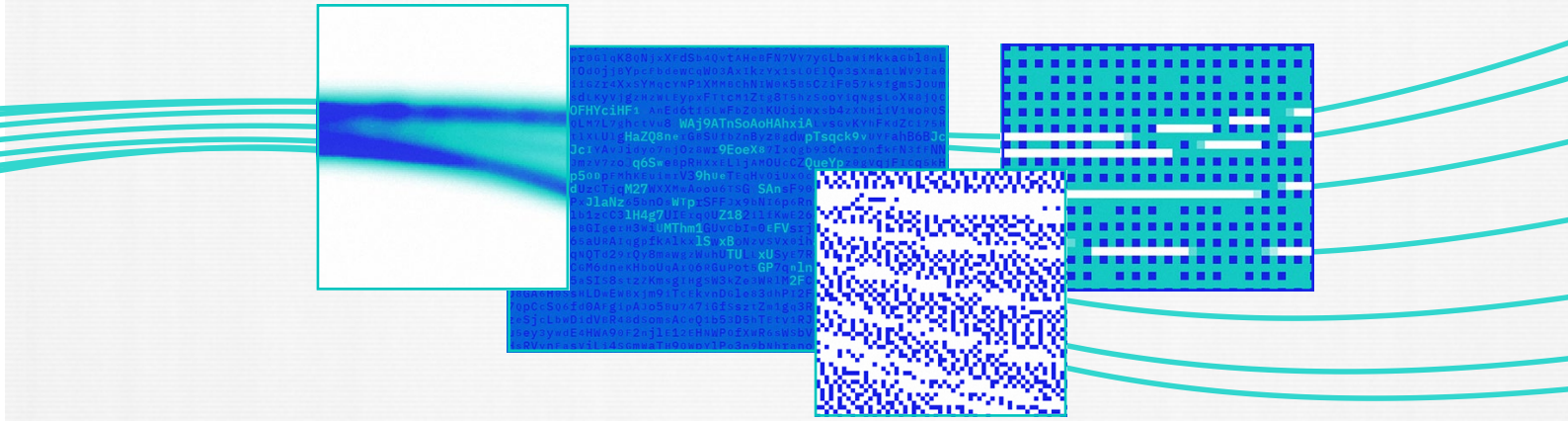
Whilst key drivers for this report are geopolitically focused, the rapid technological development in offensive AI models and Europe's steady push towards greater digital sovereignty are both subjects that could not be ignored as each currently has significant impact on the European Threat Landscape. From a board perspective, the speed at which offensive frontier AI models are now learning to adapt in real time makes it imperative that organisations give greater consideration to their own defensive and resiliency frameworks, and whether they have the capacity and capability to adapt at pace to meet the growing offensive challenge.

Digital sovereignty brings its own concerns from a cyber perspective. Although frameworks and technologies can be developed to counter geopolitical instability, these actions create additional threats from espionage, sabotage and attempts to discredit new capabilities. Organisations moving along this path should thus carefully consider risk factors affecting their own operational resilience profiles before fully committing to any strategic change.

Within the report itself you will find metrics, trends, insights, assessments and predictions all focused on subjects affecting European organisations and delivered by our highly skilled team of analysts who specialise in delivering fully curated intelligence products across the Strategic, Operational and Tactical levels of intelligence.

Should you wish to have a more informed discussion around any of the points raised or would like to learn more about the services we provide, I welcome you to reach out to my teams via the contact details provided at the back of this report.

DANIEL SHEPHERD
CEO, CSIS Security Group



EXECUTIVE SUMMARY

Overview

Throughout 2026 Europe has experienced a worsening security environment shaped by US unpredictability, a persistent and expanding Russia threat, and rising strategic competition with China, especially in cyber and trade.

Since early 2025, US-European relations have steadily deteriorated amid growing doubts about Washington's reliability as a security partner, driven by a more unilateral, coercive, and unpredictable US foreign policy. In response, European states are increasingly considering strategic, technological, and regulatory distancing from the US, including more independent intelligence and security arrangements, although cooperation in areas of shared interest is likely to continue. These tensions are expected to persist in the medium term, and even if US policy softens after 2028, Europe's efforts to reduce dependency are unlikely to reverse. Whilst digital sovereignty may strengthen Europe's strategic independence, if implemented without care it could replace political dependency with new technical, operational, and security risks.

EU-China trade tensions are expected to intensify throughout late 2026 through sector-specific disputes rather than a full trade war, particularly in strategic industries such as green technology, steel, and chemicals. Alongside this, Chinese cyber-espionage against European government, regulatory, and research entities is likely to continue, with intellectual property theft remaining a near-term risk and covert prepositioning for future leverage assessed as likely, even though overt destructive cyberattacks against Europe remain unlikely in the short to medium term.

The war in Ukraine remains intense, with continued missile and drone strikes, failed negotiations, and wider spillover effects across Europe through Russian cyber activity, sabotage, and other grey-zone threats. Despite some internal disagreements, European political, military, and institutional support for Ukraine has remained strong.

Russian grey zone operations show persistent influence activity, increasing use of AI and hybrid cyber-enabled tactics, and the importance of credible amplification rather than sheer volume in determining whether reputational damage becomes significant. Hybrid threats in Europe continue to make normal business operations more uncertain, costly, and politically exposed, with the greatest risk arising from blended, deniable attacks on critical dependencies rather than from any one tactic alone.

Europe's nation-state cyber threat picture is defined above all by Chinese and Russian strategic activity, with other malign states adding more targeted or indirect forms of pressure. The strongest common themes are growing use of deniable access, pressure on critical infrastructure, and the blurring of boundaries between espionage, coercion, and wider geopolitical competition. Russia is expected to continue its focus on Ukraine and Europe, with state-linked actors continuing to target governments, defence, logistics, and critical infrastructure for espionage, disruption, and long-term access, while also using proxies, hacktivists, and information operations to weaken European cohesion and support for Ukraine. Critical infrastructure and political events, especially in Eastern and Northern Europe, are likely to remain key targets.

Cybercrime continues to show a highly connected cyber threat landscape in which phishing, credential theft, fraud, persistent access, and ransomware increasingly operate as stages in the same attack chain. Attackers commonly begin by stealing credentials, payment data, or session information through phishing, then use that access to enter enterprise environments, maintain control, and expand their foothold with remote access tools and command-and-control frameworks. The central conclusion is that identity has become the main point of vulnerability - attackers are increasingly abusing legitimate accounts and session material rather than relying only on obvious malware. Although many incidents are still being detected early, most activity is concentrated in the initial access, persistence, credential access, and command-and-control stages, creating a valuable opportunity for defenders to contain attacks before they escalate.

Europe's ransomware threat now appears to be shifting toward faster, more scalable, AI-enabled extortion built on stolen access and data theft, with defenders needing to prioritise credible threats, supply-chain exposure, and claim validation. CI/CD and software supply chains have become critical attack surfaces in Europe because they allow threat actors to turn one trusted compromise into large-scale downstream access with speed and efficiency.

Predictions

Russia will remain the most immediate escalation risk for Europe, China the most persistent espionage and strategic pre-positioning challenge, and the US relationship will likely remain strained but fundamentally intact in core areas of shared security interest.

On the technology front, it's likely that both AI and digital sovereignty will continue to increase strategic competition: AI will lower barriers to cyber capability and raise the risk of novel incidents, while Europe's push for sovereign capability will likely create new regulatory pressure and possibly new targets for espionage and disruption.

Phishing will continue to be a primary attack vector for cybercrime, ransomware will continue to be the most prevalent attack type, and it's likely that we'll see a steady increase in AI assisted intrusion attempts as frontier models continue to develop at pace.

Russia

Russian grey-zone pressure on Europe is likely to intensify in the short term, including cyber-enabled sabotage against critical national infrastructure. A collapse of the Putin regime and a battlefield rout remain unlikely despite their probabilities increasing; if either were to occur, Russian offensive cyber activity and criminal operations against Europe would almost certainly continue, with a battlefield collapse especially likely to trigger a sharp rise in sabotage, broader grey-zone activity, and possible targeting of assets such as subsea communications cables.

China

EU-China relations are highly likely to worsen in the short term, increasing cyber-espionage pressure on European trade, foreign, and finance ministries, while Chinese cyber-enabled sabotage remains a remote near-term risk although pre-positioning for future disruptive operations is highly likely. Chinese industrial espionage is almost certain to focus on advanced semiconductor manufacturing, AI, robotics, biotechnology, and green technology, with the know-how behind leading-edge chip production standing out as a primary intelligence priority. A Chinese invasion or blockade of Taiwan remains a remote short-term possibility.

United States

Any reduction in EU-US security cooperation is likely to stay limited to specific issues rather than becoming broad-based, with intelligence sharing on mutual priorities such as organised crime and state-linked espionage almost certain to continue. The November 2026 midterm elections are unlikely to materially change the direction of US foreign policy.

Artificial Intelligence

The outlook points to a more volatile and accessible offensive cyber environment, with patch volumes expected to stay persistently high and the cost of effective exploits likely to fall, making advanced attack capability more widely available. Governments are also expected to tighten control over advanced AI models, with the US likely to impose federal assessment and approval requirements for frontier proprietary models and restrict overseas access, while China is likely to take similar steps for advanced open-weight models. At the same time, the risk of AI-driven security incidents is rising, including a likely real-world adaptive LLM-enabled worm in the short-to-medium term and a likely major lawsuit following an accidental LLM-driven intrusion in the short term. A broader global market correction caused by inflated technology stocks remains unlikely in the immediate future.

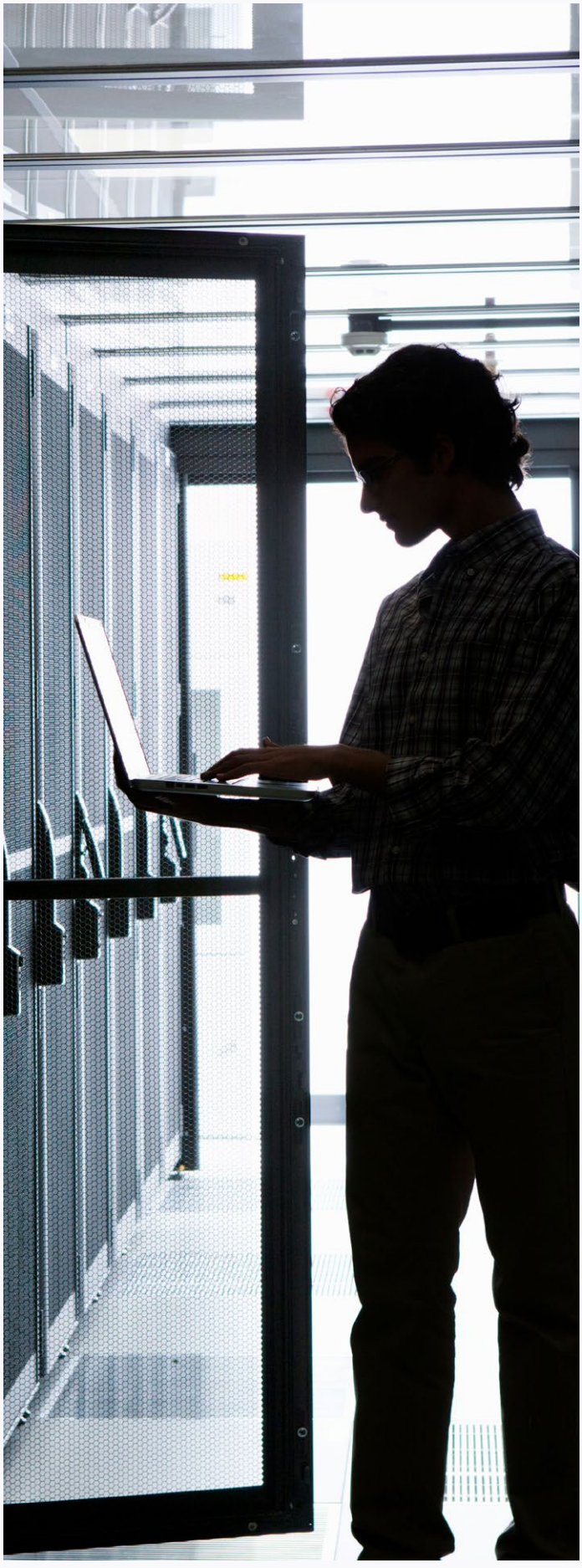
Digital sovereignty

Europe is almost certain to keep building more independent intelligence, security, cloud, and AI structures, but these will themselves become priority espionage targets for hostile states. Foreign cyber operations are also likely to focus more heavily on new EU trade, defence, and diplomatic initiatives, while European-owned digital infrastructure will face growing risks not only to confidentiality through espionage, but increasingly to integrity and availability as adversaries seek to expose weaknesses and undermine confidence. Regulators are expected to push economically significant organisations toward sovereign solutions, beginning with defence and critical infrastructure but extending into technology, finance and healthcare. The shortage of fully sovereign providers will make "operational sovereignty" using extra-jurisdictional suppliers a central regulatory and strategic concern.

Cybercrime

The access-first model currently being experienced is expected to intensify. Phishing will likely remain a primary method of compromise, with attackers continuing to target session cookies, browser-stored secrets, MFA processes, and account recovery mechanisms, making malicious activity look more like normal user behaviour. Infostealers and stolen credentials are also expected to drive faster enterprise intrusions, shortening the time between initial theft and wider disruption. Ransomware will likely remain a major threat, especially in large European economies and important sectors where identity compromise can be turned into broad enterprise access.

The access-first model currently being experienced is expected to intensify. ***Phishing will likely to remain a primary method of compromise****, with attackers continuing to target session cookies, browser-stored secrets, MFA processes, and account recovery mechanisms, making malicious activity look more like normal user behaviour.*



IT worker in a server room.

GEOPOLITICAL OVERVIEW

US-Europe Relations 9

The War in Ukraine 10
Key Cyber Trends 10
Cyber Landscape Outlook 10

EU-China Trade Relations 11



US-Europe Relations

Since the start of the second Trump administration in January 2025, relations between the United States and its European allies have been defined by rising tension as well as uncertainty over Washington's reliability as a security partner. Amid a strategic pivot away from Europe and towards the Western hemisphere and East Asia, US foreign policy has proven both assertive and unpredictable, characterised by the frequent use of tariffs as a coercive instrument, the assertion of territorial ambitions over the sovereign territory of friendly nations and the pursuit of unilateral military action in multiple foreign countries.

In this threat environment, European states are debating how to respond to a perceived weakening of American security guarantees and how to manage the risks arising from a less predictable policy environment in Washington. Should present trends continue, European states are likely to more actively pursue technological, regulatory and strategic decoupling from the US, challenging the sustainability of the transatlantic relationship in its current form [For more details regarding derisking efforts in the area of technical supply chains, see Section on European Digital Sovereignty].

Amid unresolved tensions, including continued US pressure regarding the status of Greenland, there are early indicators that European states are investing in intelligence and security cooperation structures that run parallel to, rather than through, existing transatlantic channels. For instance, the Dutch parliamentary coalition agreement of January 2026 includes an ambition to establish a European 'Five Eyes' equivalent, though the same agreement reaffirms Dutch commitment to bilateral defence and nuclear sharing arrangements with the US.

Public reporting also suggests multiple European countries have already narrowed the scope of intelligence sharing with the United States, citing concerns regarding the legality of US strikes in the Caribbean as well as trust-related concerns around the potential politicisation of intelligence in Washington. European sensitivity to these issues is further informed by an established record of US intelligence agencies conducting signals intelligence collection against partner states. Reporting alleging that US agencies were directed to increase intelligence-gathering operations against Greenland in mid-2025 indicates that such taskings continue in the second Trump administration, reflecting potentially increased risk appetite on the part of Washington in line with strategic priorities.

Curtailment of security cooperation is likely to remain confined to the specific areas outlined above. Bilateral sharing on areas of convergent interest, such as transnational organised crime and state-nexus espionage activity, is likely to persist. Consistent with this, US agencies will almost certainly continue to collaborate with European intelligence and security services, including through joint law enforcement action against cybercriminal infrastructure and the release of joint advisories on China and Russia nexus threat actors. There is, however, a realistic possibility that European services will extend case-by-case restrictions to issues where transatlantic perspectives diverge, which over time could erode the substance of transatlantic intelligence cooperation.

Tensions between the US and Europe are almost certain to persist through the medium-term. Given the extensive foreign policymaking powers of the executive branch, a Democratic victory in the November 2026 midterm elections is unlikely to significantly alter the direction of US foreign policy and could even exacerbate conditions of unpredictability should the administration face greater resistance to its domestic agenda. In the longer term, a change of administration following the 2028 presidential election presents a realistic possibility of a partial reversal in Washington's tone and policy towards Europe. European de-risking efforts are nonetheless unlikely to be reversed, given that increased defence spending commitments, sovereign procurement cycles and industrial policy are driven by the threat from Russia as well as by uncertainty over US commitments.

ASSESSMENT

Almost certain: *US–Europe tensions persist through the medium term.*

Almost certain: *US agencies continue to collaborate with European services, including joint law enforcement action against cybercriminal infrastructure and joint advisories on China- and Russia-nexus threat actors.*

Likely, if present trends continue: *European states more actively pursue technological, regulatory and strategic decoupling from the US.*

Realistic possibility: *European services extend case-by-case restrictions to issues where transatlantic perspectives diverge.*

Unlikely: *a Democratic victory in the November 2026 midterms significantly alters the direction of US foreign policy.*

The War in Ukraine

The conflict remained highly active throughout the reporting period, with Russia and Ukraine sustaining intensive missile and drone strikes and Ukraine making limited territorial gains. Both sides increasingly relied on long-range strikes, while drone warfare continued to expand in scale. Diplomatic efforts remained stalled, with multiple rounds of negotiations failing to produce a breakthrough. Temporary ceasefires collapsed amid mutual accusations of violations, while Russia maintained its territorial demands and Ukraine continued to seek renewed negotiations. The wider conflict also increasingly affected Europe through cross-border drone incidents, cyberattacks, sabotage, and other grey-zone activity, reinforcing concerns over regional security. Despite internal disagreements over financing, European political and military support for Ukraine remained strong. EU member states expanded military assistance, defence cooperation and drone procurement, while further sanctions against Russia were introduced. Discussions on Ukraine's EU accession also progressed, including proposals for greater interim integration into EU structures.

Key Cyber Trends

Based on activity observed over the past six months, the key trends shaping the cyber threat landscape can be summarised as follows:

Ukraine remains Russia's strategic priority: Russian state-linked actors continued to target Ukrainian government, defence and essential service providers for espionage and destructive purposes. European and NATO-linked entities were also extensively targeted, with government, logistics, diplomatic, and defence industrial base organisations remaining the primary focus. Some activity clusters expanded into other sectors, including financial services, likely to collect information related to the conflict and Ukraine's reconstruction efforts.

Increasing destructive targeting of Europe: The Russia-attributed campaign targeting Polish energy facilities during the previous reporting period marked a notable escalation in destructive cyber-enabled activity against European critical infrastructure. Since then, Russia's intelligence-affiliated actors have continued probing European Critical National Infrastructure (CNI), while Russia has maintained the use of recruited proxies to facilitate physical sabotage, disruption and espionage against critical infrastructure across Europe.

Continued state-cybercriminal nexus: Russia-aligned hacktivist activity remained the most visible form of cyber activity directly linked to the conflict, with campaigns targeting organisations perceived to support Ukraine. This activity formed part of a broader pattern of cooperation between Russian state actors, cybercriminal groups and Russia-aligned hacktivist collectives, with evidence of the Russian state increasingly coordinating or managing selected criminal entities to support broader objectives in cyberspace.

Persistent Russian information operations: Russia continued to use influence operations to shape perceptions of the war and undermine Western support for Ukraine. In Europe, activity increasingly targeted political and civic movements in former Soviet states seeking closer ties with the EU. Electoral processes in Hungary, Poland and Germany, alongside major EU and G7 engagements, featured prominently in Russian influence activity. Moscow also leveraged high-profile international events, including the Milano-Cortina Olympics and Eurovision 2026, as opportunities to amplify pro-Russian narratives and undermine Western cohesion.

FOUR TRENDS

1. Ukraine remains Russia's strategic priority

2. Increasing destructive targeting of Europe

3. Continued state-cybercriminal nexus

4. Persistent Russian information operations

Cyber Landscape Outlook

During H2 2026, Russian state-linked cyber operations are highly likely to remain focused on intelligence collection, persistent access and positioning for potential disruptive activity. Russian military intelligence and security services will highly likely continue targeting Ukrainian military and government networks for battlefield-relevant information, while increasingly seeking long-term access to European systems. Critical infrastructure, particularly energy, is likely to remain exposed to both cyber-enabled and physical sabotage, with Poland and the Baltic states facing the highest risk. Intelligence collection is likely to extend deeper into Western Europe, particularly against major EU and NATO members such as Germany and France, as well as against countries that control significant Russian assets, including Belgium.

European elections and major political events will provide further opportunities for Russian espionage and influence operations, with Sweden's September 2026 election a likely short-term target. Pro-Russian hacktivists are almost certain to continue opportunistic targeting of organisations supporting Ukraine, although activity is expected to remain short-lived and low impact. More broadly, Russia is likely to exploit political divisions through sabotage and influence operations, with the US midterms, UN General Assembly, IMF and G20 meetings providing key opportunities to undermine transatlantic cohesion and support for Ukraine.

EU-China Trade Relations

Trade related tensions between European Union and China continue to grow. Although an 'all-out' trade war is assessed as unlikely in the short term, the intensification of sectoral trade disputes is almost certain. This assessment is predicated on the fact that, whilst the EU's trade deficit with China (~€1bn per day) is difficult to sustain, neither party would benefit from a full-scale trade war. The economic impact of a trade war would have significant negative implications for both Europe and China, particularly given the fragility and uncertainty around trade barriers with the US, and other threats to global trade. With regard to sector-specific trade restrictions, Electric Vehicles (EVs), batteries, solar panels and wind power equipment (as well as 'green technology' more generally), steel and chemicals are assessed to be the highest risk sectors.

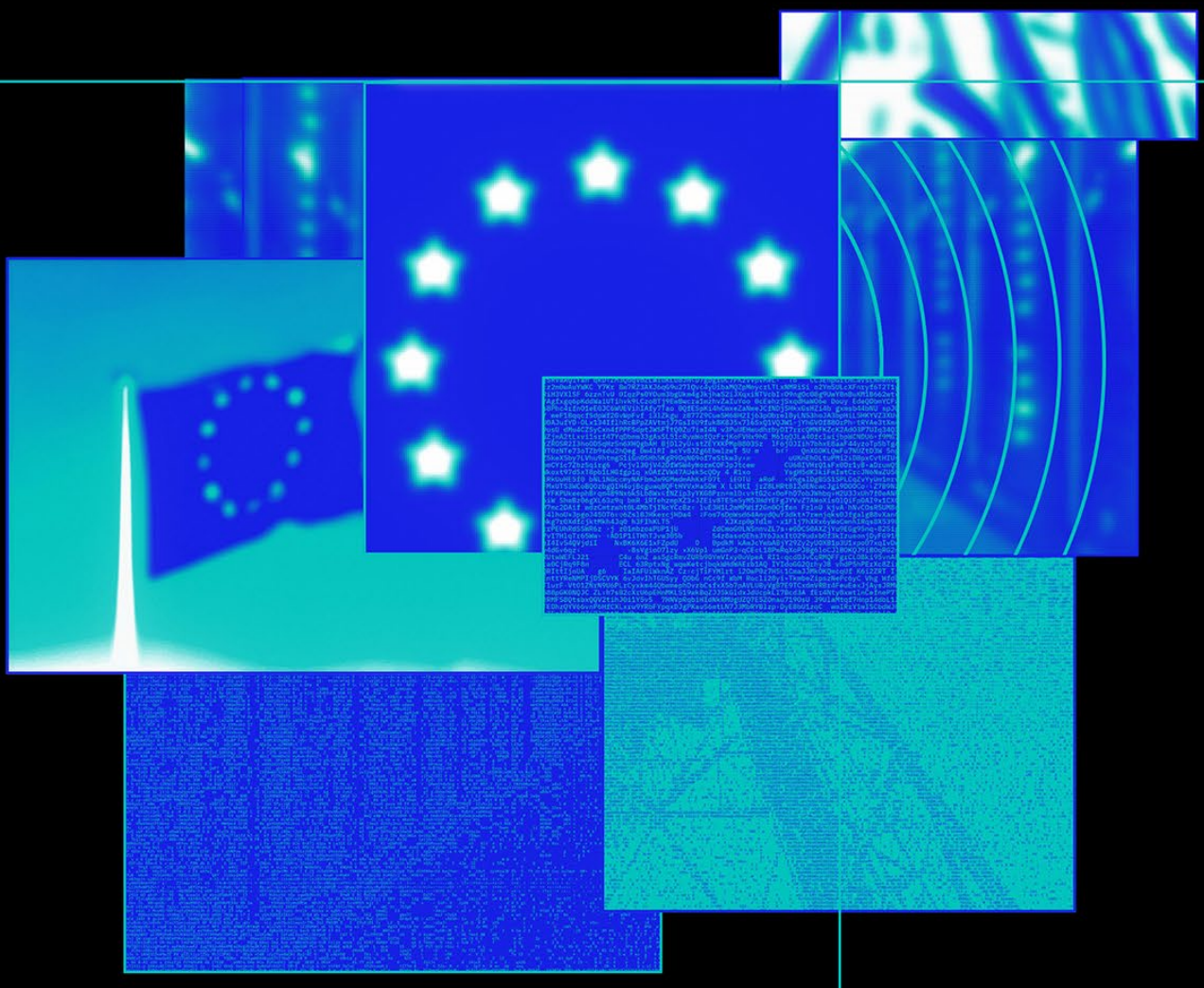
In light of growing tensions over trade, ongoing cyber-espionage activity targeting the EU's decision-making institutions and processes, (and those of European national governments) will continue. In particular, the threat to trade, foreign & finance ministries will continue to rise, alongside bodies responsible for economic security and investment screening, and technical standards setting / regulatory bodies.

Similarly, a continuation of intellectual property (IP) theft operations targeting European research and development centres, is effectively certain in the short term, however this threat is likely to diminish in the longer term, as Chinese domestic R&D capability accelerates further. More generally, given China's rapidly growing capacity for offensive cyber operations, the country has the potential to significantly increase the number of entities targeted in the medium term.

The threat of Chinese disruptive or destructive attacks against European targets is assessed to be very low in the short / medium term, as such behaviour would be significantly counterproductive for China, exacerbating European fears around digital sovereignty, and leading to increased efforts to 'de-risk' the relationship. Pre-positioning activity, designed to enable future cyber-enabled sabotage operations, or potentially to provide leverage as part of Chinese 'sharp power' or 'Weishe' based operations, remains highly likely.

REGULATORY UPDATES

Introduction	13
The Network and Information Security Directive 2 (NIS2) and Critical Entities Resilience Directive (CER)	13
Digital Operational Resilience Act (DORA)	14
Artificial Intelligence Act and Digital Omnibus	14
The Cybersecurity Act (CSA)	14
Digital Services Act (DSA)	14
Cyber Resilience Act (CRA)	15



Introduction

The EU's framework of cybersecurity regulations is increasingly shaped by the following dynamics:

- **Competitiveness vs Regulation:** The EU faces a growing range of cybersecurity threats that potentially warrant increased regulation. This is further shaped by efforts to enhance the bloc's digital sovereignty, reducing the reliance on foreign providers, such as the US and China. Data and system security (key elements of digital sovereignty) can be preserved through robust regulation; however, regulatory 'red tape' may impede Europe's ability to develop world-leading technical enterprises.

- **The EU-US Relationship:** This is further complicated by the EU's high level of dependency on the US. This straddles both defence and the provision of irreplaceable critical technologies, particularly cloud storage, as well as heavy reliance on ubiquitous providers, such as Microsoft. EU efforts to regulate Big Tech are proving to be a source of tension with the US, which views them as anti-competitive and punitive toward US companies.

- **The speed and impact of current developments in AI:** The pace of technological change makes it challenging to develop effective regulation. Intense competition among jurisdictions, many of which view AI development as a zero-sum game, reduces the likelihood of collaborative standard-setting.

These competing pressures are likely to constrain Europe's regulatory agenda in the medium- to long-term future. Attempts to consolidate existing regulations to minimise regulatory burdens and placate Big Tech interests are highly likely. As existing regulations come into force, a shift from new legislation to effective enforcement is also likely; however, in the short term, enforcement may be undermined by US-EU tensions.

ASSESSMENT

Highly likely: *attempts to consolidate existing regulations, to minimise regulatory burdens and placate Big Tech interests.*

Likely: *a shift from new legislation to effectiue enforcement as existing regulations come into force.*

Short-term risk: *enforcement undermined by US-EU tensions.*

The Network and Information Security Directive 2 (NIS2) and Critical Entities Resilience Directive (CER)

NIS2 strengthens cybersecurity requirements for critical sectors, including financial services, energy, healthcare, digital infrastructure, government and transportation. It is now in force across most EU nations, entering into force in Sweden, Estonia, Poland, Austria, Bulgaria, and Luxembourg during the reporting period. The Netherlands will transpose NIS2 into national law on 15 August 2026. In June 2026, reports stated that the European Commission (EC) is preparing to take Spain and France to court for failing to meet the implementation deadline.

The CER aims to strengthen the resilience of critical sectors by addressing physical threats. NIS2 and CER are complementary because of the overlap between physical threats and digital services, such as a physical attack disrupting digital connectivity or a cyberattack disrupting physical service provision. The CER has been implemented in 20 EU states, with the remainder facing a legal challenge from the EC for failing to do so. During the reporting period, Belgium and Germany transposed the CER into national law. As of 17 July 2026, member states are required to have identified and designated critical entities under the CER.

Digital Operational Resilience Act (DORA)

DORA establishes a harmonised legislative framework for financial services entities across the EU to strengthen digital and operational resilience. 19 critical ICT third-party service providers (CTTPs) also fall under DORA's oversight framework.

Although DORA has been in effect since January 2025, its first year of application was largely a grace period to allow institutions time to align with regulatory requirements. In 2026, regulatory bodies have made strides towards enforcement. Non-compliant organisations face penalties of up to EUR 20m, while individuals held liable for violations face fines of up to EUR 5m, with these sums varying across different jurisdictions.

Artificial Intelligence Act and Digital Omnibus

The EU AI Act is designed to regulate AI across four risk levels. Although it is now entering its enforcement phase, it has been subject to re-evaluation and simplification as part of the proposed Digital Omnibus to simplify EU legislation. The EC has published its draft, non-binding guidelines on the classification of high-risk AI systems, although enforcement has been delayed. In August 2026, certain AI Act obligations for general-purpose models, as well as prohibitions on AI practices, came into force.

The Digital Omnibus was proposed in November 2025 as a new digital package designed to simplify rules on AI, cybersecurity and data. Regulations such as the AI Act, NIS2, DORA, Data Act and the General Data Protection Regulation (GDPR) could be affected by changes to reporting requirements or amendments to the acts. Proposed changes have been criticised for their potential to threaten data security, such as changing the definition of personal data and allowing pseudonymised data to be more broadly shared or used to reduce bias in AI systems.

The Cybersecurity Act (CSA)

The CSA was first adopted in 2019. In January 2026, the EC proposed an updated act (CSA2) to improve supply chain security, facilitate compliance with cybersecurity rules, and empower the EU Agency for Cybersecurity (ENISA). The proposal was open for feedback and will now undergo further discussion in the European Parliament.

Digital Services Act (DSA)

The DSA, which came into force in February 2024, regulates online services used by EU individuals, such as social media platforms or online marketplaces. In December 2025, the US announced visa restrictions on EU citizens, including former EU commissioner Thierry Breton, for his role in creating the DSA, citing impositions on free speech. The move is linked to ongoing US opposition to the DSA for its attempts to regulate US tech giants, including a EUR 120m fine on X for breaching transparency requirements.

Cyber Resilience Act (CRA)

The CRA introduces mandatory cybersecurity requirements for manufacturers of products with digital elements (e.g. hardware, software and connected digital devices). It has been in effect since December 2024; however, the Act's main obligations will apply from 11 December 2027, with reporting obligations applying from 11 September 2026. Manufacturers will be required to notify of actively exploited vulnerabilities and security incidents through the CRA Single Reporting Platform.



EU flag in Brussels.

EVENT TIMELINE 2026



1 **03 Jan - US captures Venezuelan president Maduro**
Indicates US foreign policy is less constrained by international norms & conventions.

2 **07 Jan - Trump declines to rule out use of military force to seize Greenland**
Signals shift in US foreign policy, challenging European assumptions about sovereignty, security & trust in the transatlantic alliance.

3 **13 Jan - Poland accuses Russia of cyberattacks on national energy grid**
Reflects significant increase in the Russian sabotage threat, both conventional & cyber-enabled.

4 **20 Jan - Ireland & Germany expand surveillance & interception powers**
Intended to reduce long-term SIGINT dependence on third parties in light of growing threats.

5 **20 Jan - EU plans phaseout of Chinese tech from European CNI**
Action to counter China-linked security risk, but has significant trade & diplomatic implications.

6 **20 Jan - Davos highlights surge in corporate AI investment & employment concerns**
AI spending continues to grow. The extent of impact on employment remains unclear, but likely significant.

7 **22 Jan - France seizes Russian shadow-fleet tanker off Sicily**
Strengthened sanctions enforcement against Russia's shadow fleet.

8 **22 Jan - Trump's Gaza 'Board of Peace' established**
The board's legitimacy, influence & longevity remain unclear & contested.

9 **27 Jan - EU & India sign security & defence partnership**
EU strategic partnerships are extending beyond traditional allies in an increasingly multipolar world.

10 **31 Jan - China revises cybersecurity law, expands state control**
Potential for compliance & operational challenges for European organisations & travellers.

11 **01 Feb - US government shutdowns weaken federal security operations**
CISA shutdown potentially reduces US cybersecurity capacity.

12 **05 Feb - Satellite espionage case highlights growing threat to Euro space sector**
Arrests indicative of growing focus by hostile threat actors.

13 **24 Feb - Pentagon pressures AI firms to allow military use of models**
Dispute between US government & Anthropic highlights concerns around control & misuse.

14 **24 Feb - Four year anniversary of the war in Ukraine**
Front-lines remain largely static, focus shifts to strategic targeting using drones & missiles.

15 **26 Feb - EU sanctions Chinese entities linked to Russia**
The EU's 20th round of sanctions deepen EU-China friction.

16 **28 Feb - US missile strikes on Iran, closure of Strait of Hormuz**
Major disruption to fuel supplies results in significant price increases & some shortages.

17 **02 Mar - Ukrainian 'Deep Strike' campaign targeting Russian energy infra commences**
Campaign is effective in curtailing fuel production, resulting in domestic shortages.

18 **05 Mar - Europol warns of heightened Iran-linked threat in Europe**
Physical and cyber targeting of US & Israeli targets in Europe a concern.

19 **06 Mar - US cyber strategy prioritises offensive cyber & AI**
New doctrine places emphasis on pre-emptive cyber disruption & elevates AI to a strategic national priority.

20 **11 Mar - Handala claims cyberattack on US pharma company Stryker**
Beyond this one opportunistic attack, Iran's cyber response was largely muted & ineffectual.



21 **12 Mar - US briefly eases Russian oil sanctions after disruption**
Geopolitical necessity prioritised over sanctions policy.

22 **16 Mar - Anthropic releases Claude Mythos 5 Preview**
Vulnerability detection capability focussed attention on the practical impact of AI on cyber security.

23 **16 Mar - EU launches counter disinformation & sabotage strategy**
Strategy seeks to bolster protections for critical infrastructure, democratic processes & election security.

24 **09 Apr - UK reports on Russian submarines mapping sub-sea infrastructure**
Highlights vulnerability of sub-sea infrastructure in light of increased Russian sabotage threat.

25 **12 Apr - Hungarian elections open door to closer cooperation with the EU**
Viktor Orbán's defeat removes a significant obstacle to EU support for Ukraine.

26 **24 Apr - Media reporting highlights NATO divisions over Iran strikes**
Reporting indicates the US wishes to 'punish' NATO members who did not support US military action against Iran.

27 **30 Apr - EU signs Mercosur deal with Latin America**
The deal aims to deepen trade & investment ties between the EU & Mercosur by reducing barriers across both regions.

28 **05 May - Germany warns China is closing AI capability gap**
The warning highlights the narrowing Chinese-US AI capability gap, & risks over less transparent development.

29 **13 May - US-China summit**
Summit highlights continued US-China engagement, despite growing Sino-Russian ties.

30 **19 May - EU tightens foreign investment screening in critical sectors**
Strengthens EU oversight of foreign investment across Critical National Infrastructure.

31 **20 May - Russian drone incursions test NATO resilience**
Continued pressure on NATO's eastern flank & a persistent risk of escalation.

32 **27 May - UK & Poland sign defence treaty**
Effort to strengthen European defence cooperation to counter Russian threat.

33 **27 May - UK expands sanctions on Russian oil & technology**
Added pressure on Russian revenue streams & industrial capacity.

34 **03 Jun - EU unveils technological sovereignty package**
Strengthening European autonomy in semiconductors, AI & cloud.

35 **06 Jun - China publishes whitepaper on global governance**
Signals Beijing's intent to shape global governance, including in AI, cyberspace & other emerging domains.

36 **12 Jun - US imposes export control on Anthropic's top-end models**
Short-lived controls raised concerns around digital sovereignty.

37 **15 Jun - G7 reaffirms support for Ukraine, promotes cooperation on critical minerals alliance**
Critical minerals alliance viewed as key to reducing dependence on strategic rivals.

38 **18 Jun - European Council Summit**
Working toward national defence spending of 3% of GDP. Reaffirmed EU support for Ukraine.

39 **30 Jun - EU boosts military & budget support for Ukraine**
€90bn financial support for Ukraine.

METRICS

Implications of Top C2 Telemetry	19
Credentials as an intrusion enabler	20
Ransomware - a defining European Threat	22
Operational detection for defence	29
Phishing as an access and fraud enabler	31
Compromised Cards as Fraud Risk	34



Implications of Top C2 Telemetry

KEY TAKEAWAYS

- *Access theft remains the dominant signal.*
- *Infostealers create identity risk beyond the infected host.*
- *RATs and post-exploitation frameworks indicate active, expanding intrusions.*

CSIS observations of command-and-control infrastructure in H1 2026 show that the most prominent malware families and frameworks align with three persistent attacker objectives: stealing access, maintaining access, and expanding access.

This pattern is reflected in the relative prominence of three categories of tooling:

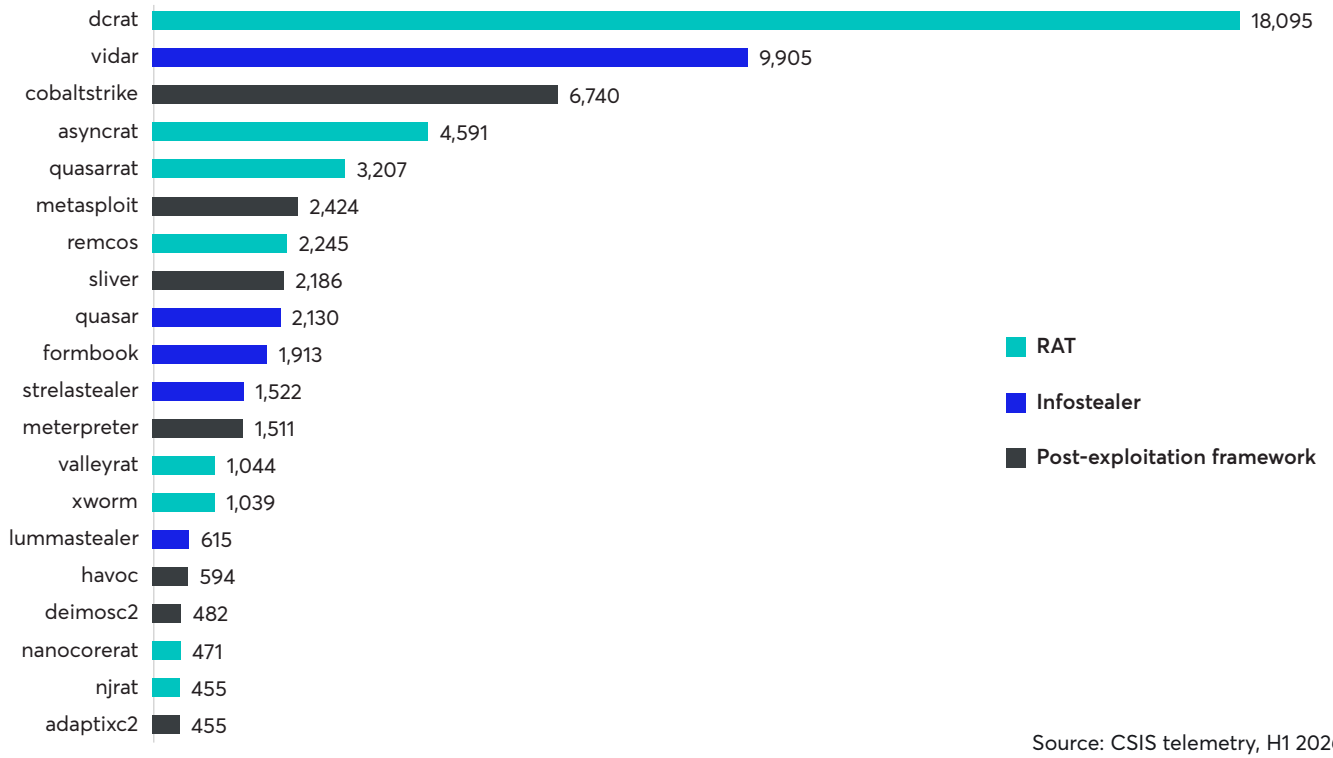
- Infostealers such as Vidar, LummaStealer, and RedLine.
- RATs such as DCRat, AsyncRAT, QuasarRAT, and Remcos.
- Post-exploitation frameworks such as Cobalt Strike, Metasploit, and Sliver.

The strongest signal in the dataset is the continued importance of infostealers. Their prominence reinforces that a substantial share of malicious activity remains focused on credentials, browser-stored secrets, cookies, and authenticated sessions. For defenders, the risk extends well beyond the initially compromised endpoint. Once stolen, these materials can support account takeover and follow-on intrusion even where the original malware has been removed. Infostealer detections should therefore trigger an identity-led response, not solely endpoint containment.

A second important finding is the continued prevalence of RATs. These tools are designed to provide durable remote control over compromised systems and commonly support persistence, command execution, and the staging of additional payloads. In practical terms, RAT activity suggests that an intrusion may still be active and that attackers may retain direct operational access.

Post-exploitation frameworks such as Cobalt Strike and Metasploit are stronger indicators of broader enterprise risk. Their presence is associated with privilege escalation, lateral movement, and preparation for final objectives such as ransomware deployment. Where this tooling is observed, the intrusion has typically progressed beyond initial compromise and should be treated accordingly.

Most prominent C2 malware families, H1 2026



Source: CSIS telemetry, H1 2026.

Credentials as an intrusion enabler

Credential theft remains one of the most critical enablers of modern enterprise intrusion. The H1 2026 dataset contains 192.1 million unique compromised credentials, split relatively evenly between Europe/UK (100.4 million, or 52.2%) and the rest of the world (91.8 million, or 47.8%).

The distribution is highly concentrated:

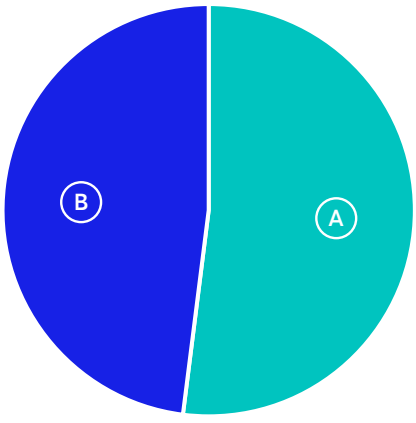
- Global Top 10 (65.5% of total): Japan, Italy, France, Germany, Poland, Russia, Brazil, Spain, and Indonesia.
- Europe/UK Concentration: Italy (22%) and France (22%) are tied as the primary targets in Europe, making up nearly half of the regional total on their own. Germany (13%), Poland (12%), and Spain (6%) follow.

Valid credentials, session cookies, and other access materials remain operationally invaluable because they allow attackers to bypass traditional malware detection points. For defenders, credential theft must be treated as a primary intrusion vector. Infostealer detections should immediately trigger credential resets, session invalidation, and reviews of externally accessible accounts.

KEY TAKEAWAYS

- *Stolen credentials remain a primary route into enterprise environments.*
- *Session material and browser secrets materially increase the risk.*
- *Identity response should begin immediately after infostealer exposure.*

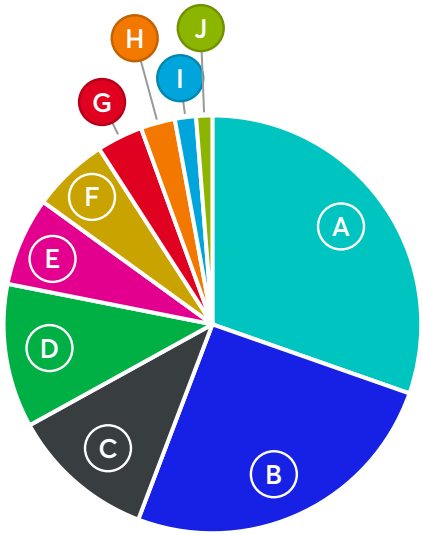
Compromised credentials in Europe/UK



A.	Europe + UK/GB	52%
B.	Rest of world	48%

Source: CSIS telemetry, H1 2026.

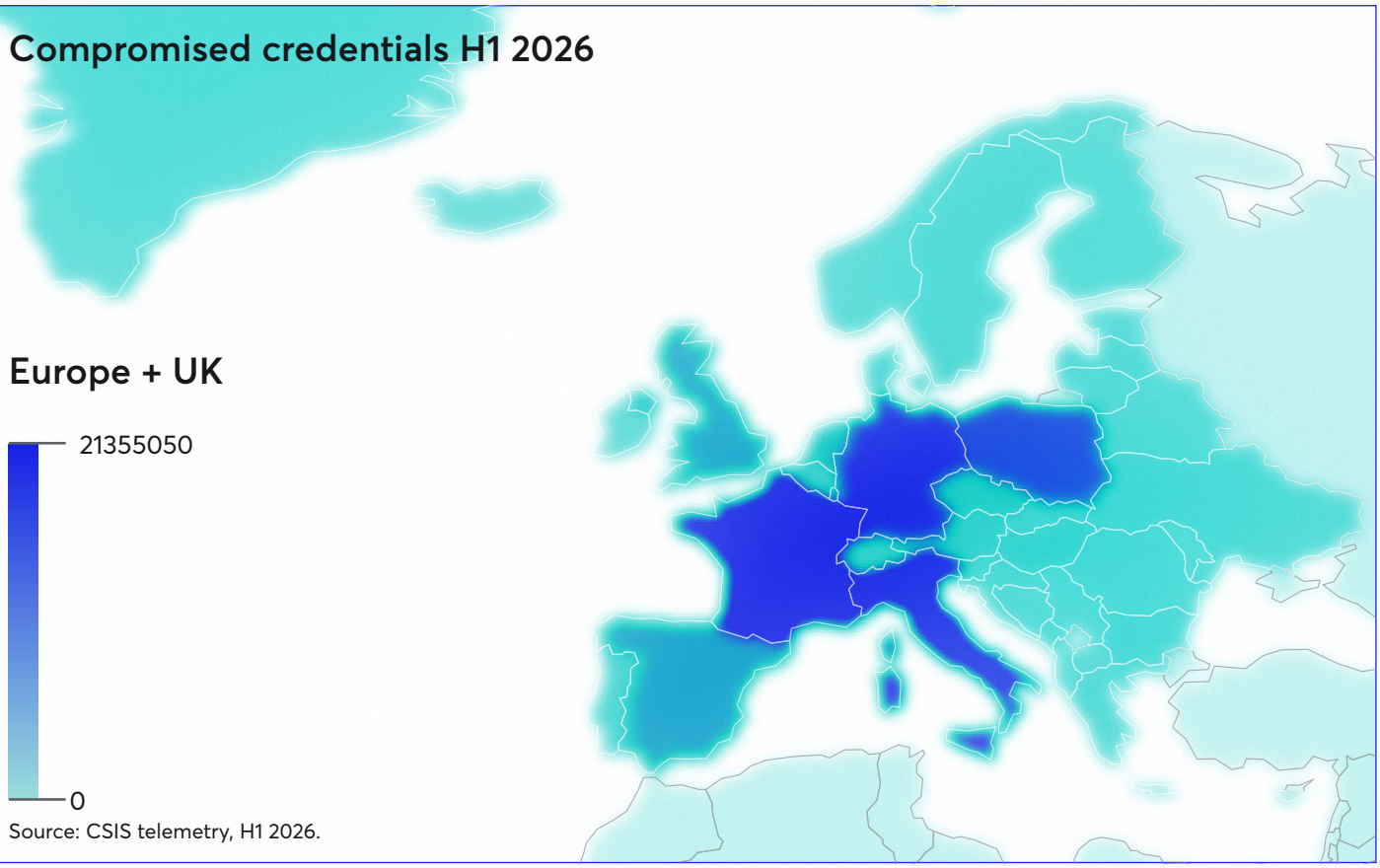
Compromised credentials: global top 10



A.	FR	30%	**F.**	ES	6%
B.	IT	25%	**G.**	NL	4%
C.	DE	11%	**H.**	CZ	3%
D.	PL	11%	**I.**	HU	2%
E.	GB	7%	**J.**	AT	1%

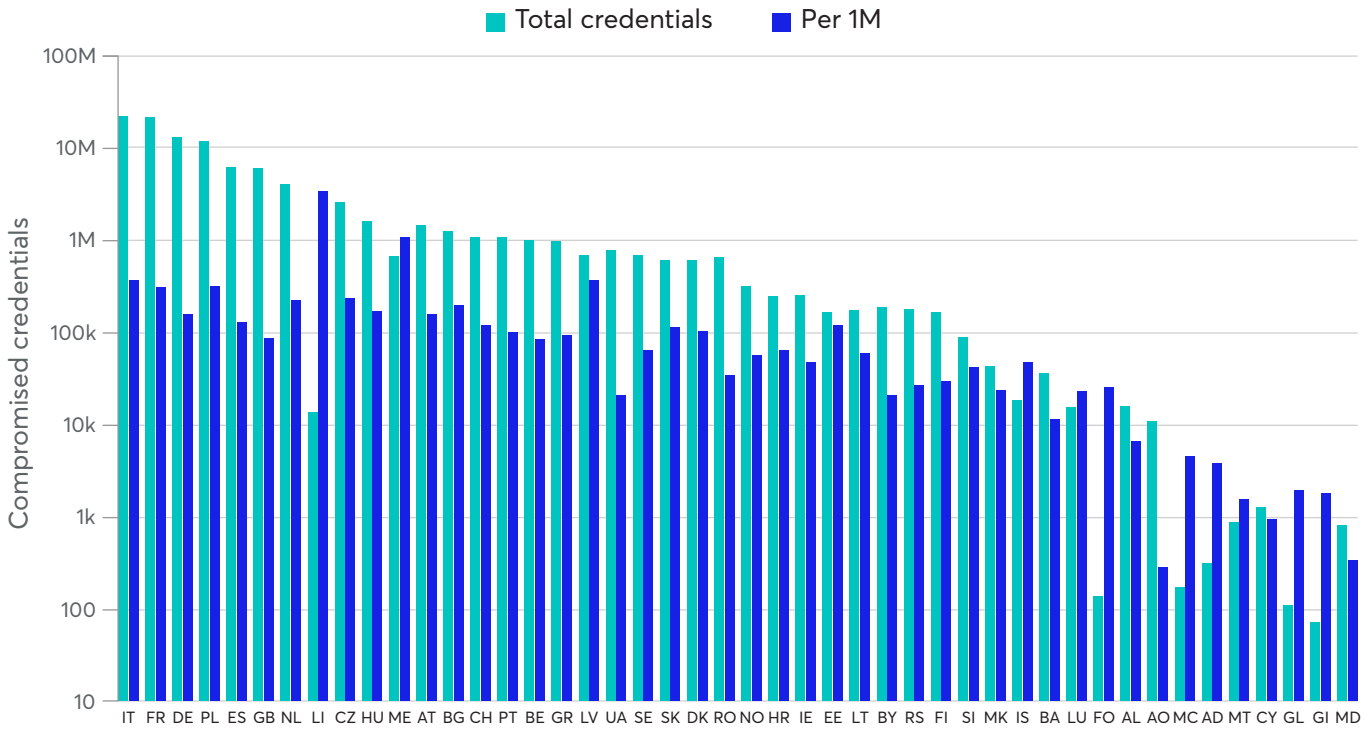
Source: CSIS telemetry, H1 2026.

Compromised credentials H1 2026



Source: CSIS telemetry, H1 2026.

Distribution including population adjustment



Source: CSIS telemetry, H1 2026.

Ransomware - a defining European threat

KEY TAKEAWAYS

- *Ransomware remains the highest-impact outcome in the intrusion chain.*
- *Pressure is concentrated in major economies and key sectors.*
- *A relatively small set of actors accounts for a large share of incidents.*

Ransomware is often the high-impact outcome of the intrusions built on stolen credentials and persistent footholds. In H1 2026, there were 1,213 confirmed leak cases across Europe.

Activity is heavily concentrated in Europe's largest economies:

- Germany: 261 cases.
- United Kingdom: 242 cases.
- France: 134 cases.
- Italy: 130 cases.
- Spain: 102 cases.

When adjusted for population, Northern Europe emerges as the most exposed region at 3.08 leaks per one million people, ahead of Central Europe (2.28) and Western Europe (2.10).

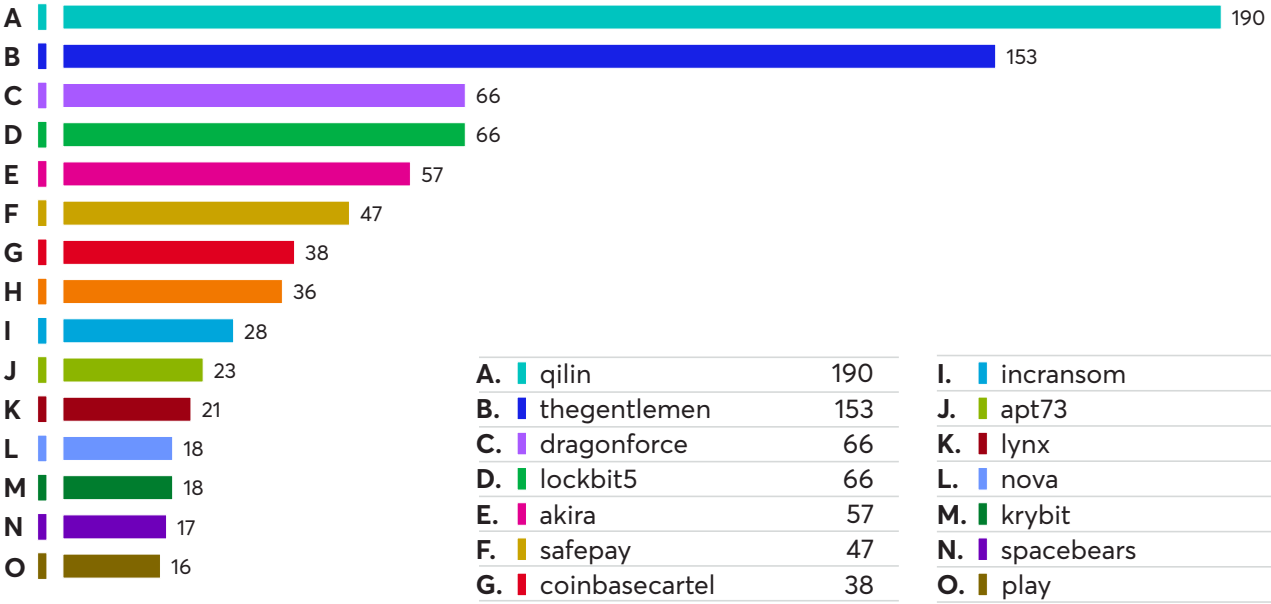
Sector discrepancies

Europe faces a distinct pattern of ransomware pressure compared to the rest of the world. Europe over-indexes in manufacturing (16.35% of cases against 12.84% globally). Technology, consumer services, and business services also show elevated weighting in Europe, indicating that European ransomware is disproportionately oriented towards industrial operations, supply chains, and the real economy.

Actor landscape

The European threat environment is heavily concentrated among a smaller number of actors. Qilin and The Gentlemen account for 31.3% of total Europe and UK incidents, compared to just 22.6% globally. Groups like Safepay and LockBit5 also show clear European weighting, whereas groups like Incransom, Clop, and Play carry greater relative weight globally.

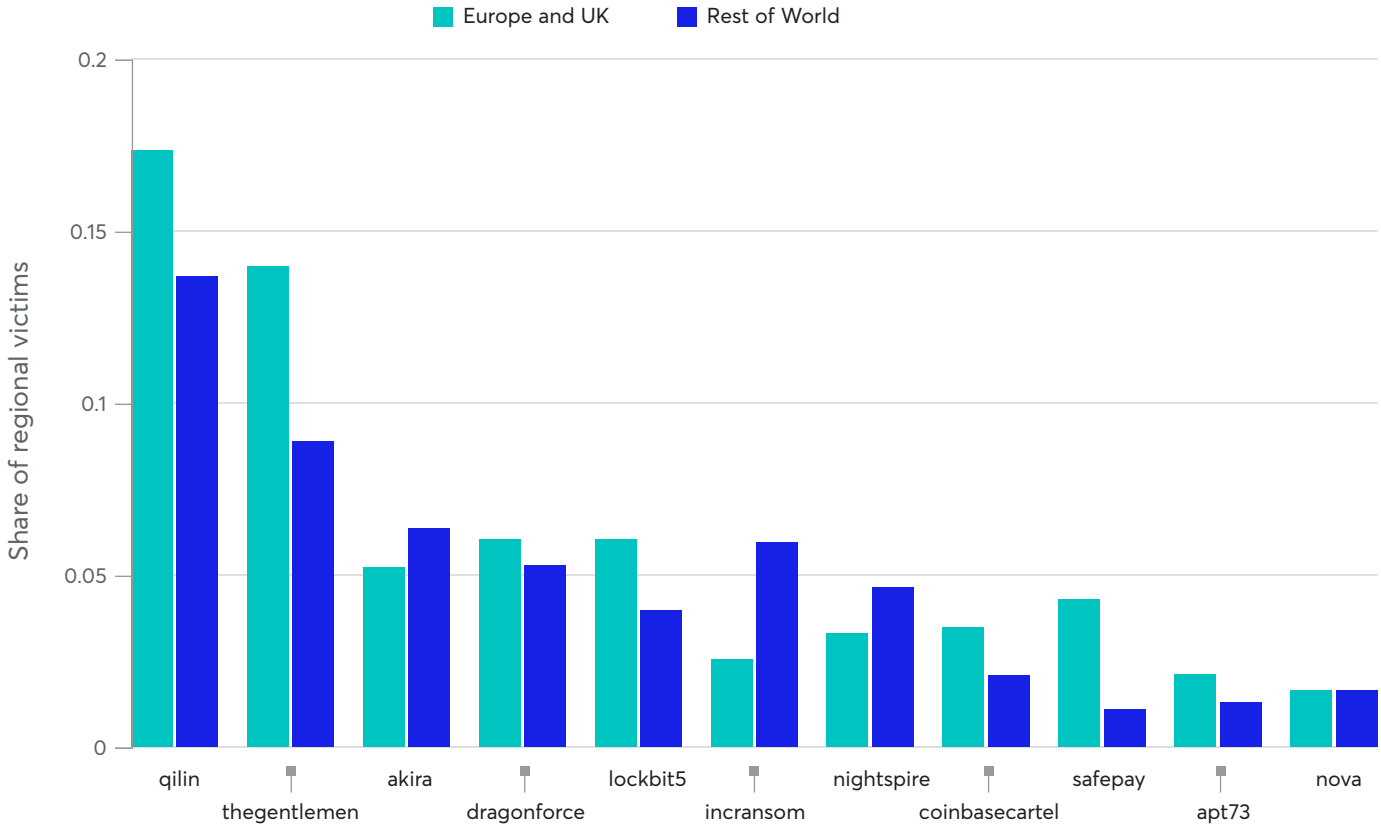
Top ransomware groups targeting Europe/UK



A.	qilin	190
B.	thegentlemen	153
C.	dragonforce	66
D.	lockbit5	66
E.	akira	57
F.	safepay	47
G.	coinbasecartel	38
H.	nightspire	36
I.	incransom	28
J.	apt73	23
K.	lynx	21
L.	nova	18
M.	krybit	18
N.	spacebears	17
O.	play	16

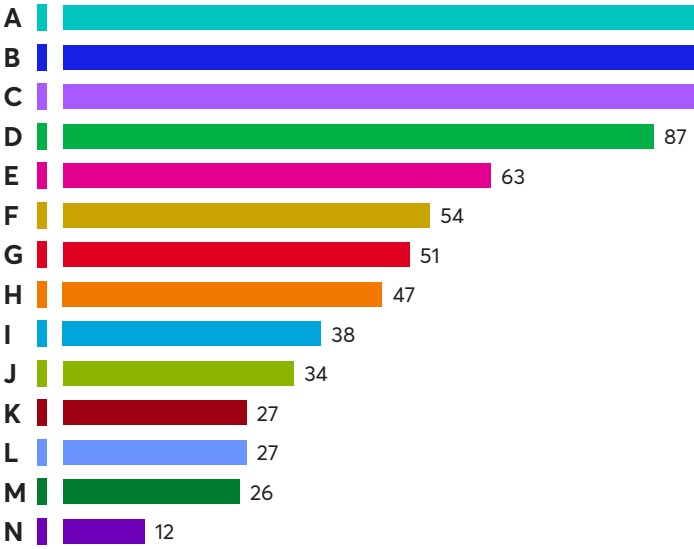
Source: CSIS telemetry, H1 2026.

Group share: Europe/UK vs rest of world



Source: CSIS telemetry, H1 2026.

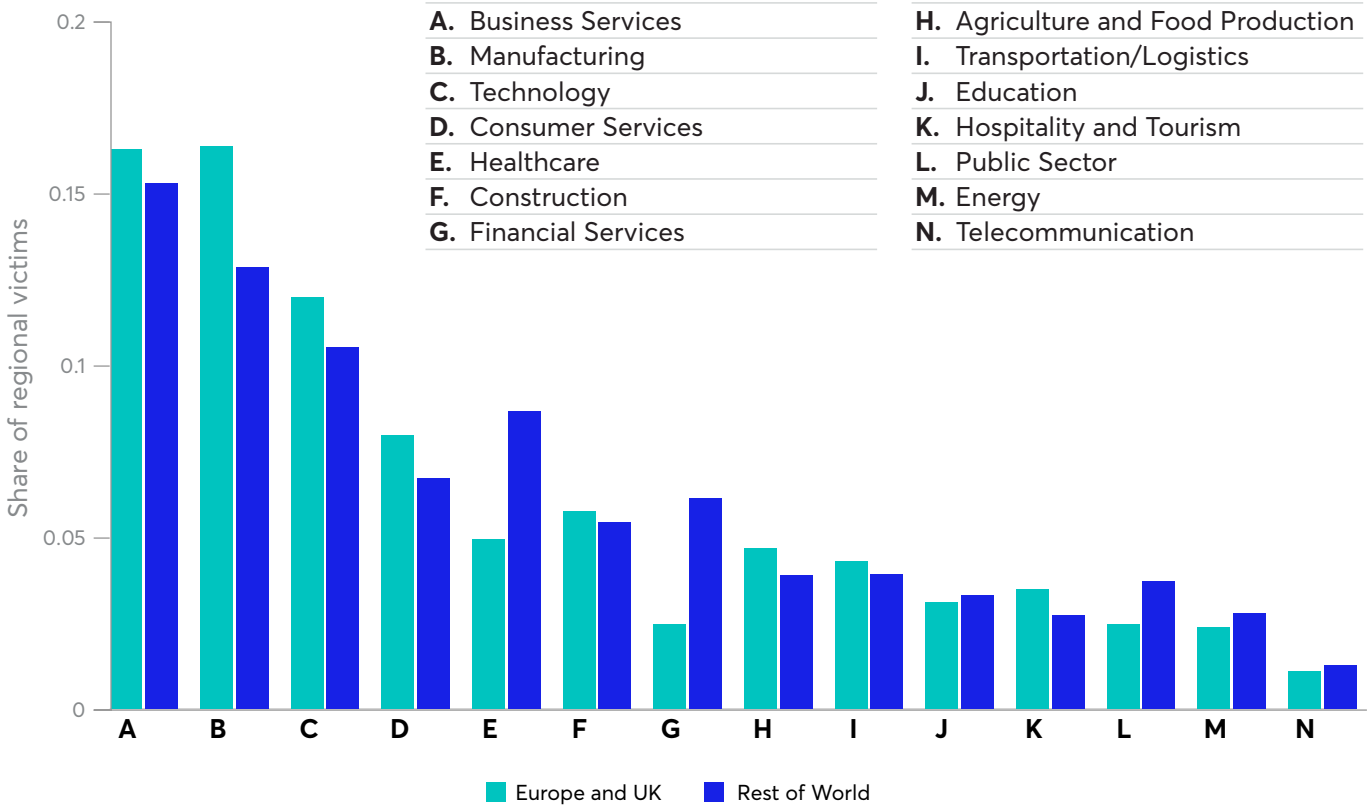
Top ransomware sectors in Europe/UK, H1 2026



A.	Manufacturing	179
B.	Business Services	178
C.	Technology	131
D.	Consumer Services	87
E.	Construction	63
F.	Healthcare	54
G.	Agriculture and Food Production	51
H.	Transportation/Logistics	47
I.	Hospitality and Tourism	38
J.	Education	34
K.	Financial Services	27
L.	Public Sector	27
M.	Energy	26
N.	Telecommunication	12

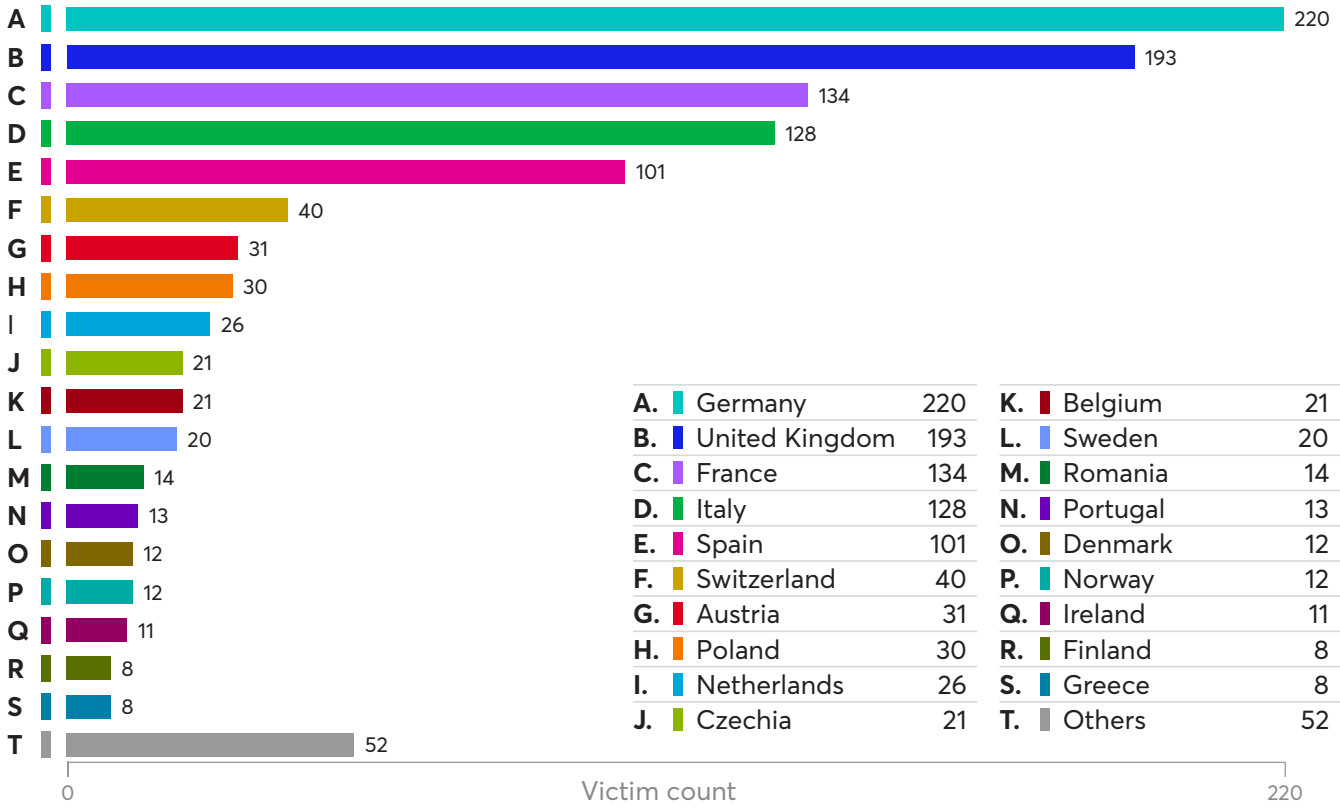
Source: CSIS telemetry, H1 2026.

Sector share: Europe/UK vs rest of world



Source: CSIS telemetry, H1 2026.

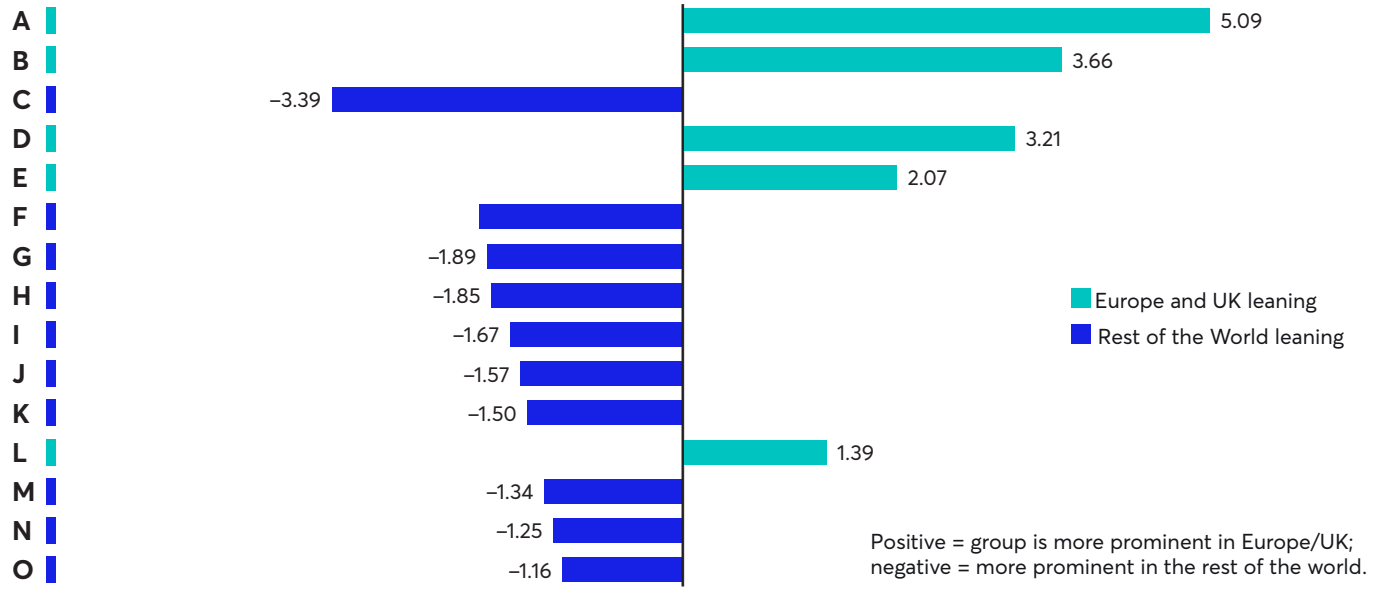
Europe/UK ransomware victims by country



A.	Germany	220	K.	Belgium	21
B.	United Kingdom	193	L.	Sweden	20
C.	France	134	M.	Romania	14
D.	Italy	128	N.	Portugal	13
E.	Spain	101	O.	Denmark	12
F.	Switzerland	40	P.	Norway	12
G.	Austria	31	Q.	Ireland	11
H.	Poland	30	R.	Finland	8
I.	Netherlands	26	S.	Greece	8
J.	Czechia	21	T.	Others	52

Source: CSIS telemetry, H1 2026.

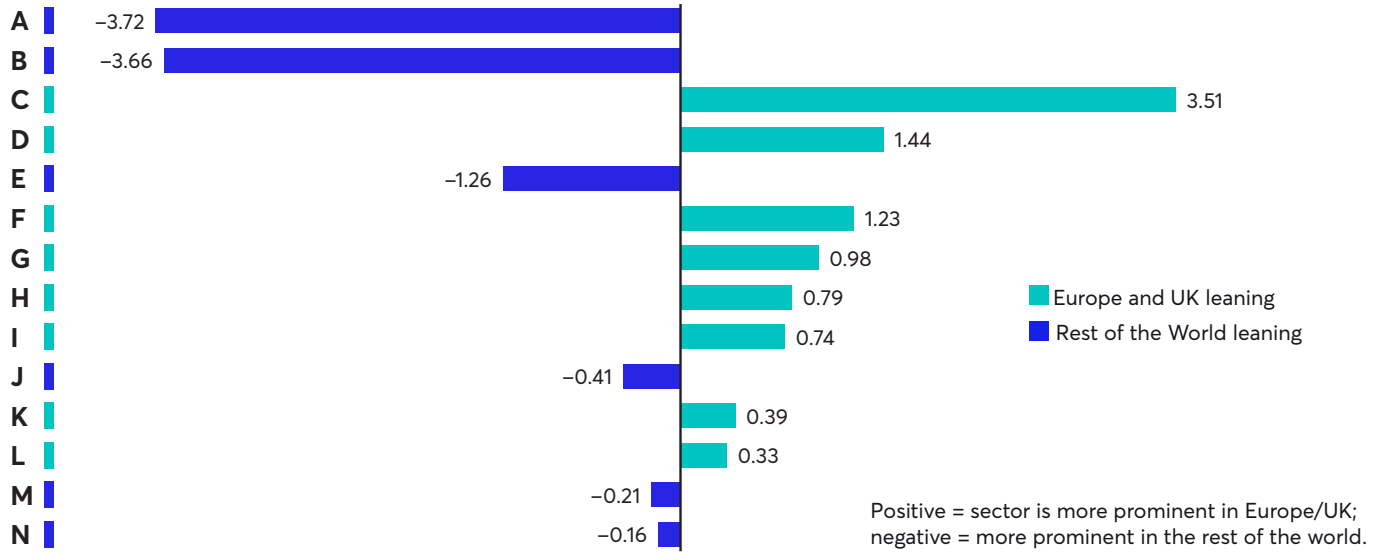
Group share: Europe/UK minus rest of world



A.	thegentlemen	5.09 %
B.	qilin	3.66 %
C.	incransom	−3.39 %
D.	safepay	3.21 %
E.	lockbit5	2.07 %
F.	play	−1.97 %
G.	sinobi	−1.89 %
H.	clop	−1.85 %
I.	handala	−1.67 %
J.	genesis	−1.57 %
K.	shinyhunters	−1.50 %
L.	coinbasecartel	1.39 %
M.	nightspire	−1.34 %
N.	pear	−1.25 %
O.	akira	−1.16 %

Source: CSIS telemetry, H1 2026.

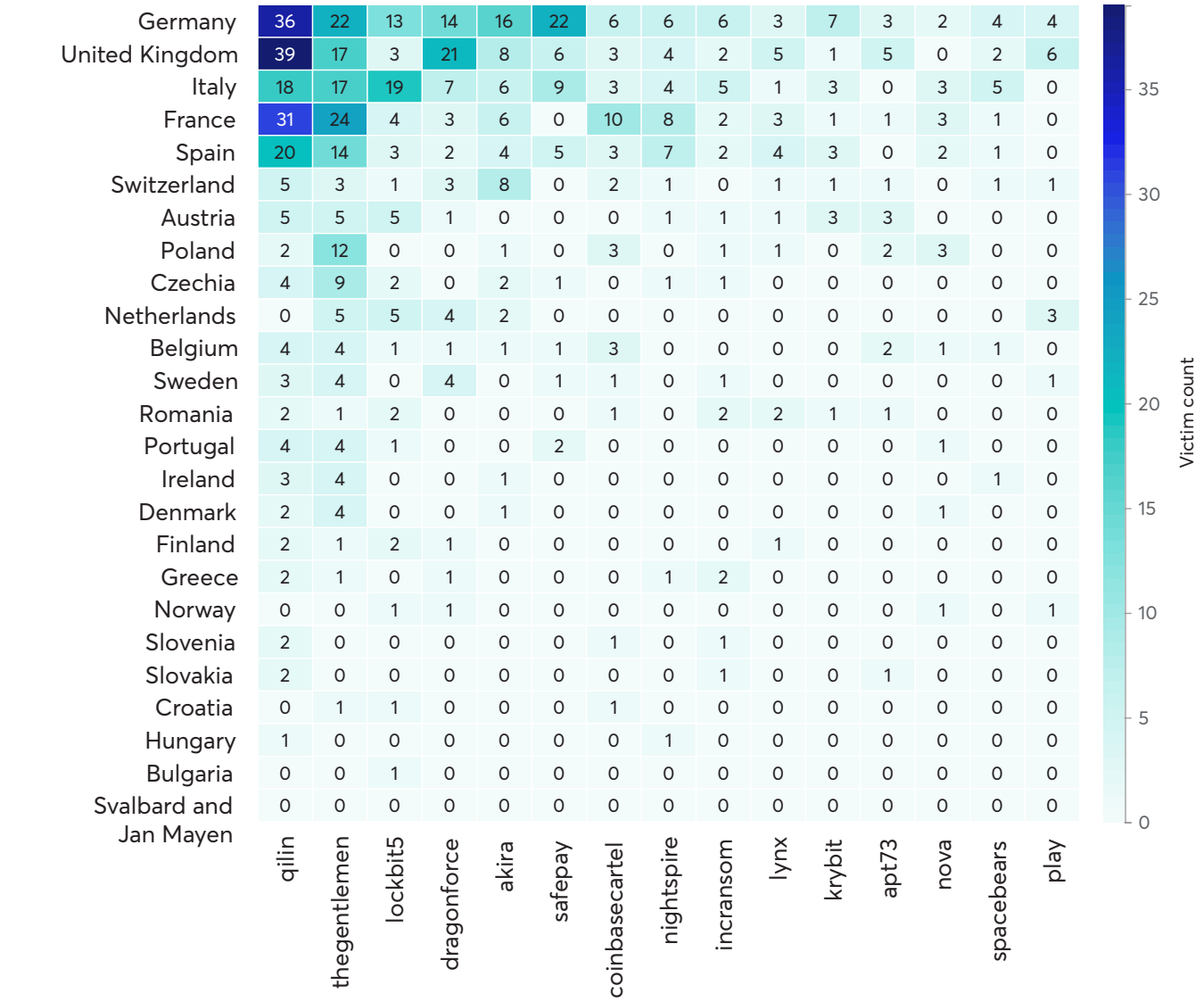
Sector share: Europe/UK minus rest of world



A.	Healthcare	−3.72 %
B.	Financial Services	−3.66 %
C.	Manufacturing	3.51 %
D.	Technology	1.44 %
E.	Public Sector	−1.26 %
F.	Consumer Services	1.23 %
G.	Business Services	0.98 %
H.	Agriculture and Food Production	0.79 %
I.	Hospitality and Tourism	0.74 %
J.	Energy	−0.41 %
K.	Transportation/Logistics	0.39 %
L.	Construction	0.33 %
M.	Education	−0.21 %
N.	Telecommunication	−0.16 %

Source: CSIS telemetry, H1 2026.

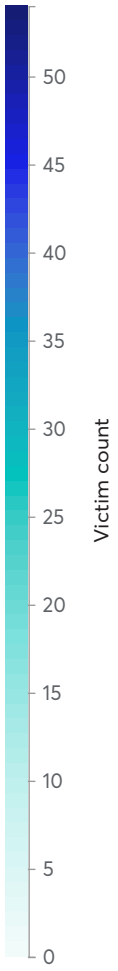
Europe/UK ransomware victims: country x group, H1 2026



Source: CSIS telemetry, H1 2026.

Europe/UK ransomware victims: country x sector, H1 2026

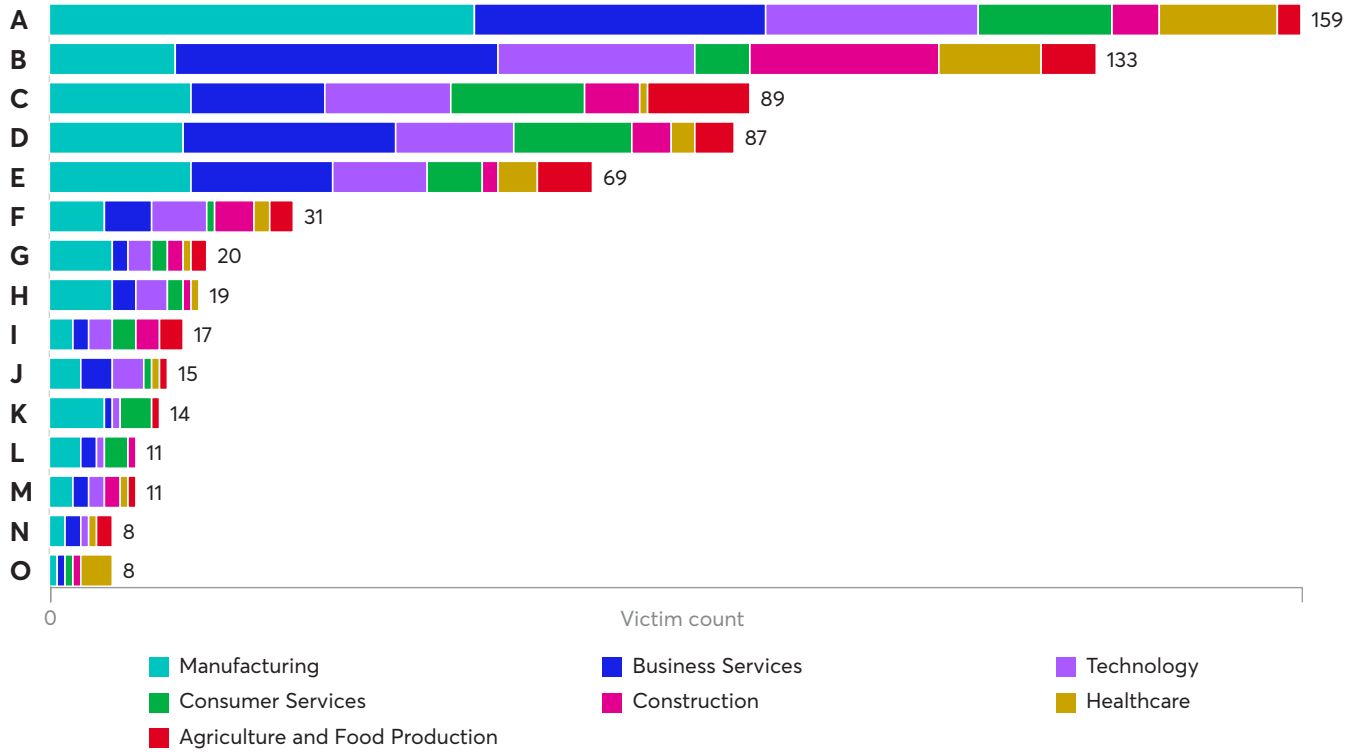
	Manufacturing	Business Services	Not Found	Technology	Consumer Services	Construction	Healthcare	Agriculture and Food Production	Transportation/Logistics	Hospitality and Tourism	Education	Financial Services	Energy	Public Sector	Telecommunication
Germany	54	37	31	27	17	6	15	3	7	3	5	5	3	6	1
United Kingdom	16	41	18	25	7	24	13	7	8	5	9	7	7	3	3
France	17	27	11	15	15	5	3	5	5	12	3	2	5	7	1
Italy	18	17	26	16	17	7	1	13	6	1	1	0	3	1	1
Spain	18	18	15	12	7	2	5	7	4	6	2	2	1	2	0
Switzerland	7	6	2	7	1	5	2	3	2	1	0	3	1	0	0
Austria	8	2	4	3	2	2	1	2	3	0	1	3	0	0	0
Poland	8	3	3	4	2	1	1	0	1	0	4	1	0	0	2
Netherlands	3	2	4	3	3	3	0	3	1	0	2	1	0	1	0
Czechia	4	2	2	1	3	1	0	0	0	1	2	1	2	1	1
Belgium	4	4	4	4	1	0	1	1	1	0	0	0	0	1	0
Sweden	7	1	2	1	4	0	0	1	2	2	0	0	0	0	0
Romania	3	2	0	2	0	2	1	1	0	0	1	0	2	0	0
Portugal	2	2	3	1	0	0	1	2	0	1	0	0	1	0	0
Norway	2	1	4	1	0	0	0	0	1	1	0	0	0	1	1
Denmark	1	1	1	0	1	1	4	0	1	1	0	0	0	1	0
Ireland	1	2	1	2	1	2	0	0	0	1	1	0	0	0	0
Finland	1	1	2	1	1	2	0	0	0	0	0	0	0	0	0
Greece	0	3	1	1	0	0	0	0	2	0	0	1	0	0	0
SJM*	0	1	1	1	0	0	3	1	0	0	0	0	0	0	0
Slovenia	0	0	1	1	0	0	0	1	0	0	1	0	1	0	0
Bulgaria	0	0	1	0	2	0	0	0	0	1	0	0	0	0	0
Croatia	0	0	2	0	0	0	0	0	0	1	0	0	0	1	0
Serbia	0	0	0	1	0	0	0	0	1	0	1	0	0	0	1
Slovakia	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1
Hungary	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0



SJM* = Svalbard and Jan Mayen

Source: CSIS telemetry, H1 2026.

Ransomware victims by sector: top countries in Europe/UK, H1 2026



A.	Germany	159	**I.**	Netherlands	17
B.	United Kingdom	133	**J.**	Belgium	15
C.	Italy	89	**K.**	Sweden	14
D.	France	87	**L.**	Czechia	11
E.	Spain	69	**M.**	Romania	11
F.	Switzerland	31	**N.**	Portugal	8
G.	Austria	20	**O.**	Denmark	8
H.	Poland	19			

Source: CSIS telemetry, H1 2026.

Operational detection for defence

KEY TAKEAWAYS

- *Most observed activity appears before end-stage impact.*
- *Identity abuse is prominent throughout the intrusion lifecycle.*
- *Speed of response remains decisive.*

CSIS Managed Detection and Response data adds an operational layer to this report, showing the actual behaviours most prominent in live intrusions. Activity is heavily weighted towards the early and middle stages of the attack lifecycle.

This is reflected clearly in the MITRE ATT&CK tactic distribution:

- Initial Access: 397 observations (24%).
- Persistence: 275 observations (17%).
- Credential Access: 259 observations (16%).
- Command and Control: 178 observations (11%).

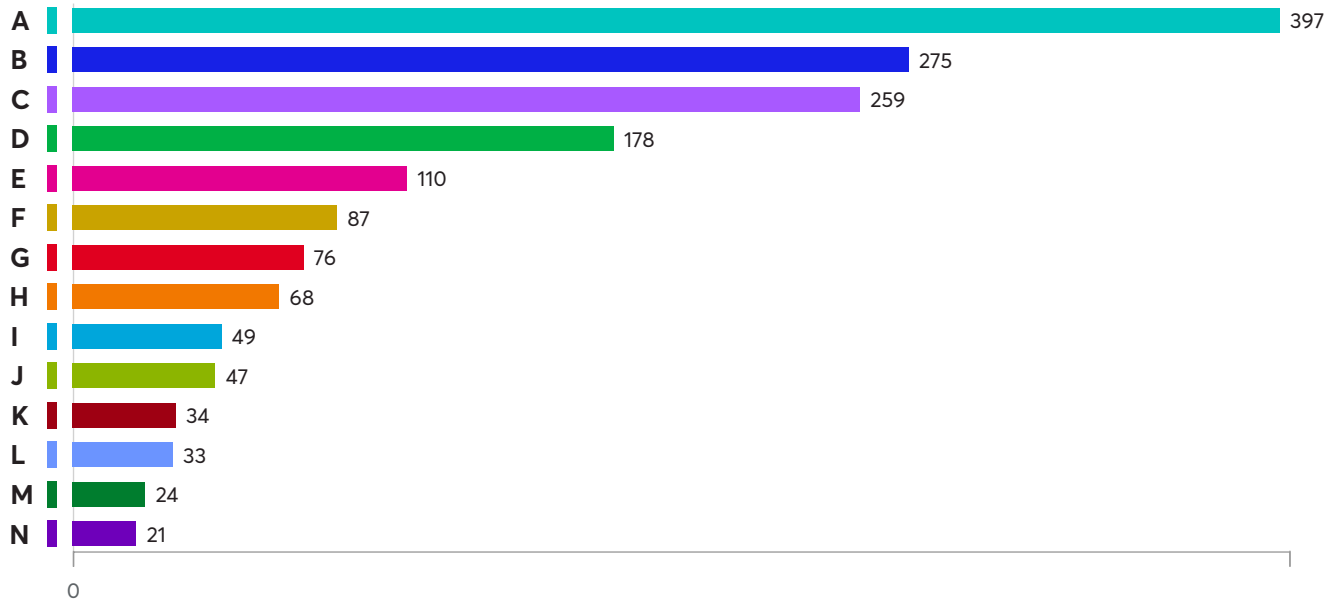
The prominence of Credential Access techniques — such as OS Credential Dumping, Credentials from Password Stores, and Steal Web Session Cookie — shows that attackers are targeting identities in parallel with system access.

For Initial Access, the most prominent technique is Phishing: Spearphishing Link (T1566.002), supported by the heavy use of Valid Accounts (cloud and local), Password Spraying, and Exploit Public-Facing Application.

For command and control and persistence, techniques like Application Layer Protocol, Dynamic Resolution, Account Manipulation, and Create Account indicate that once access is obtained, attackers work quickly to make it durable and low-noise.

The lower relative volumes for Exfiltration (3%) and Impact (1%) in the MDR dataset indicate a positive defensive reality: there is still an opportunity to disrupt attackers before they reach the stages associated with data loss or destructive ransomware, provided defenders act rapidly on early identity and C2 telemetry.

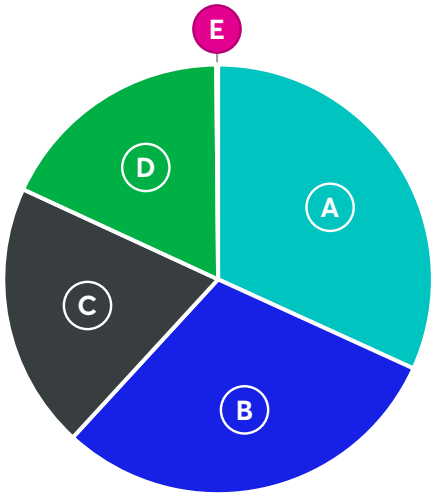
MDR MITRE Tactic findings H1 2026



A.	Initial Access	397	**F.**	Privilege Escalation	87	**K.**	Collection	34
B.	Persistence	275	**G.**	Defense Evasion	76	**L.**	Reconnaissance	33
C.	Credential Access	259	**H.**	Execution	68	**M.**	Resource Development	24
D.	Command and Control	178	**I.**	Lateral Movement	49	**N.**	Impact	21
E.	Discovery	110	**J.**	Exfiltration	47			

Source: CSIS telemetry, H1 2026.

MDR alert severity



A.	Low	690
B.	Medium	651
C.	Info	435
D.	High	390
E.	Critical	3

Source: CSIS telemetry, H1 2026.

MDR MITRE ATT&CK Techniques: top 50 - H1 2026



A.	T1566.002	Phishing: Spearphishing Link	276
B.	T1078	Valid Accounts	155
C.	T1078.004	Valid Accounts: Cloud Accounts	145
D.	T1110	Brute Force	101
E.	T1190	Exploit Public-Facing Application	96
F.	T1041	Exfiltration Over C2 Channel	93
G.	T1098	Account Manipulation	90
H.	T1595	Active Scanning	90
I.	T1008	Fallback Channels	88
J.	T1071	Application Layer Protocol	88
K.	T1090	Proxy	88
L.	T1133	External Remote Services	88
M.	T1568	Dynamic Resolution	88
N.	T1583	Acquire Infrastructure	88
O.	T1587	Develop Capabilities	88
P.	T1590	Gather Victim Network Information	88
Q.	T1557	Adversary-in-the-Middle	76
R.	T1110.001	Brute Force: Password Guessing	68
S.	T1110.003	Brute Force: Password Spraying	67
T.	T1566	Phishing	61
U.	T1539	Steal Web Session Cookie	60
V.	T1048	Exfiltration Over Alternative Protocol	58
W.	T1059.001	Command and Scripting Interpreter: PowerShell	57
X.	T1562	Impair Defenses	45
Y.	T1036.005	Masquerading: Match Legitimate Name or Loc…	34
Z.	T1204.001	User Execution: Malicious Link	34
AA.	T1003	OS Credential Dumping	32
AB.	T1555	Credentials from Password Stores	28
AC.	T1070.004	Indicator Removal on Host: File Deletion	24
AD.	T1102	Web Service	22
AE.	T1021	Remote Services	21
AF.	T1046	Network Service Discovery	19
AG.	T1555.003	Credentials from Password Stores: Credentials f…	19
AH.	T1555.004	Credentials from Password Stores: Windows Cre…	19
AI.	T1562.001	Impair Defenses: Disable or Modify Tools	18
AJ.	T1059	Command and Scripting Interpreter	17
AK.	T1204	User Execution	17
AL.	T1485	Data Destruction	16
AM.	T1020	Automated Exfiltration	15
AN.	T1114	Email Collection	15
AO.	T1087.002	Account Discovery: Domain Account	14
AP.	T1562.006	Impair Defenses: Indicator Blocking	13
AQ.	T1119	Automated Collection	12
AR.	T1217	Browser Information Discovery	12
AS.	T1136	Create Account	11
AT.	T1021.004	Remote Services: SSH	10
AU.	T1018	Remote System Discovery	9
AV.	T1547.001	Boot or Logon Autostart Execution: Registry Ru…	9
AW.	T1005	Data from Local System	8
AX.	T1210	Exploitation of Remote Services	8

Source: CSIS telemetry, H1 2026.

Phishing as an access and fraud enabler

KEY TAKEAWAYS

- *Phishing continues to enable both fraud and intrusion.*
- *Global and European targeting patterns differ markedly.*
- *Trusted cloud and hosting infrastructure is increasingly part of the delivery model.*

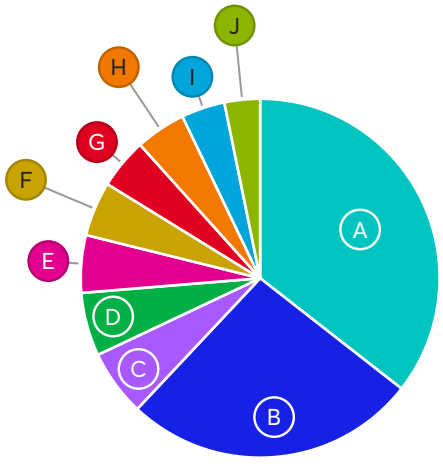
CSIS analysis reinforces that phishing remains a core mechanism for access theft and payment fraud. The dataset reveals a stark geographic divide: European brands account for only 11% of targeted brands, while the rest of the world accounts for 89%.

Attackers rely heavily on brand-driven lures, with distinct differences between global and European targeting:

- Global leaders (tech and social): globally, Facebook is the most targeted brand (36%), outpacing Microsoft (26%). Scotiabank (6%), FedEx (6%), and WhatsApp (5%) round out the top five. Attackers favour brands with large user bases and direct links to identity and account recovery workflows.
- European leaders (gambling and crypto): in Europe, the targeting profile is vastly different. The gambling site Bet365 is the top targeted brand (33%), followed heavily by cryptocurrency hardware wallets Ledger (20%) and Trezor (13%). Traditional banking follows with HSBC (10%) and Santander (7%).
- Financial services focus: looking strictly at Europe and UK financial targeting, crypto assets dominate traditional banking. Ledger (34%) and Trezor (23%) make up over half of all financial targeting, expanding the threat model beyond conventional credential harvesting into direct digital asset theft.

Furthermore, adversaries increasingly leverage trusted infrastructure. A large share of observed phishing activity sits behind major cloud, CDN, or hosting providers, including Cloudflare, Microsoft, Google, Amazon, Fastly, Akamai, and Oracle. Phishing should not be treated as a narrow email filtering problem; it is a multi-channel fraud mechanism requiring stronger identity controls and resilient MFA processes.

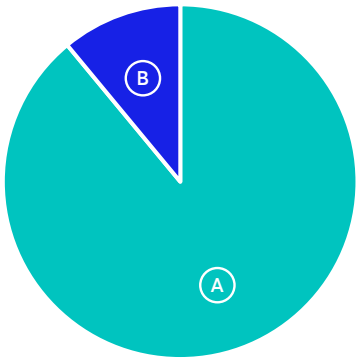
Top 10 brands targeted H1 2026



A.	Facebook	36%	**F.**	PayPal	5%
B.	Microsoft	26%	**G.**	Bet365	5%
C.	Scotiabank	6%	**H.**	Roblox	5%
D.	FedEx	6%	**I.**	Netflix	4%
E.	WhatsApp	5%	**J.**	Coinbase	3%

Source: CSIS telemetry, H1 2026.

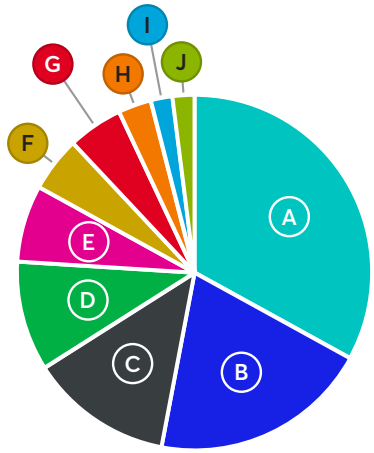
European brands targeted vs rest of the world H1 2026



A.	Rest of world	89%
B.	Europe	11%

Source: CSIS telemetry, H1 2026.

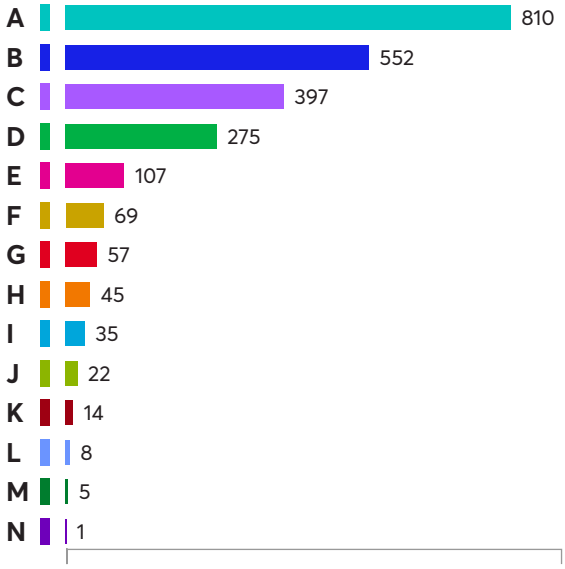
Top 10 targeted brands Europe



A.	Bet365	33%	F.	Booking.com	5%
B.	Ledger	20%	G.	DHL	5%
C.	Trezor	13%	H.	ING	3%
D.	HSBC	10%	I.	BT	2%
E.	Santander	7%	J.	BBVA	2%

Source: CSIS telemetry, H1 2026.

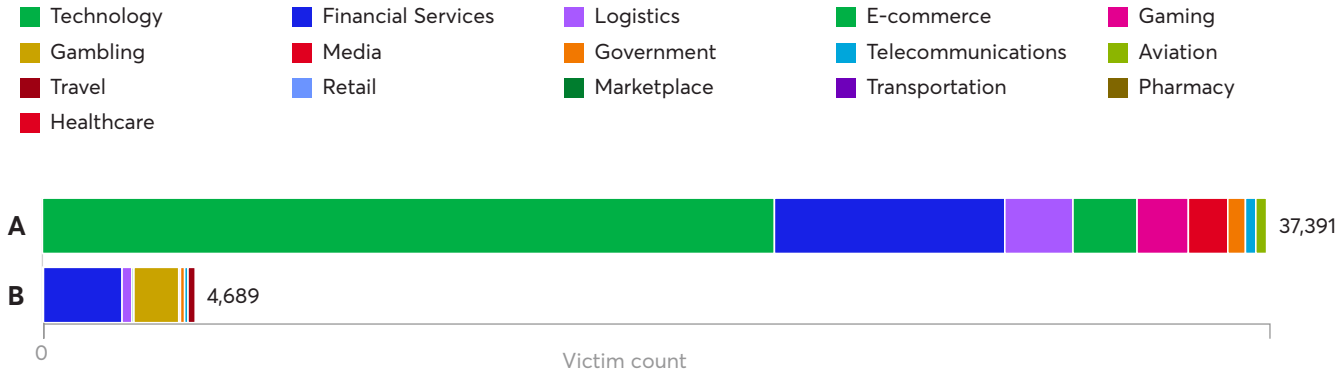
Europe/UK financial services targeted H1 2026



A.	Ledger		H.	S-Pankki	
B.	Trezor		I.	Barclays	
C.	HSBC		J.	BankID	
D.	Santander		K.	Lloyds Bank	
E.	ING		L.	DKB	
F.	BBVA		M.	Nickel	
G.	Credit Agricole		N.	Luminor	

Source: CSIS telemetry, H1 2026.

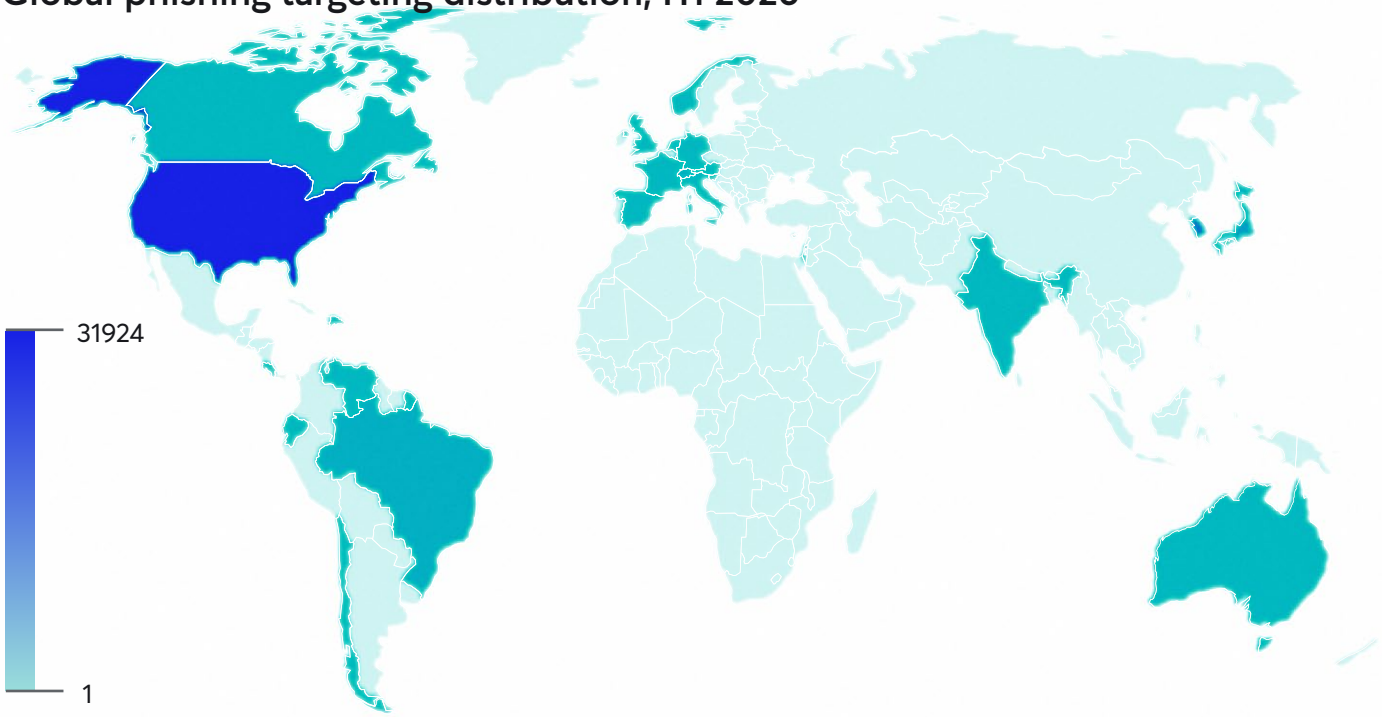
Sectors targeted Europe vs rest of the world



A.	Rest of world	37,391
B.	Europe	4,689

Source: CSIS telemetry, H1 2026.

Global phishing targeting distribution, H1 2026



Source: CSIS telemetry, H1 2026.

Compromised cards as fraud risk

KEY TAKEAWAYS

- *Card theft is a monetisation outcome rather than a standalone event.*
- *Exposure is heavily concentrated by geography.*
- *Payment integrity monitoring remains essential.*

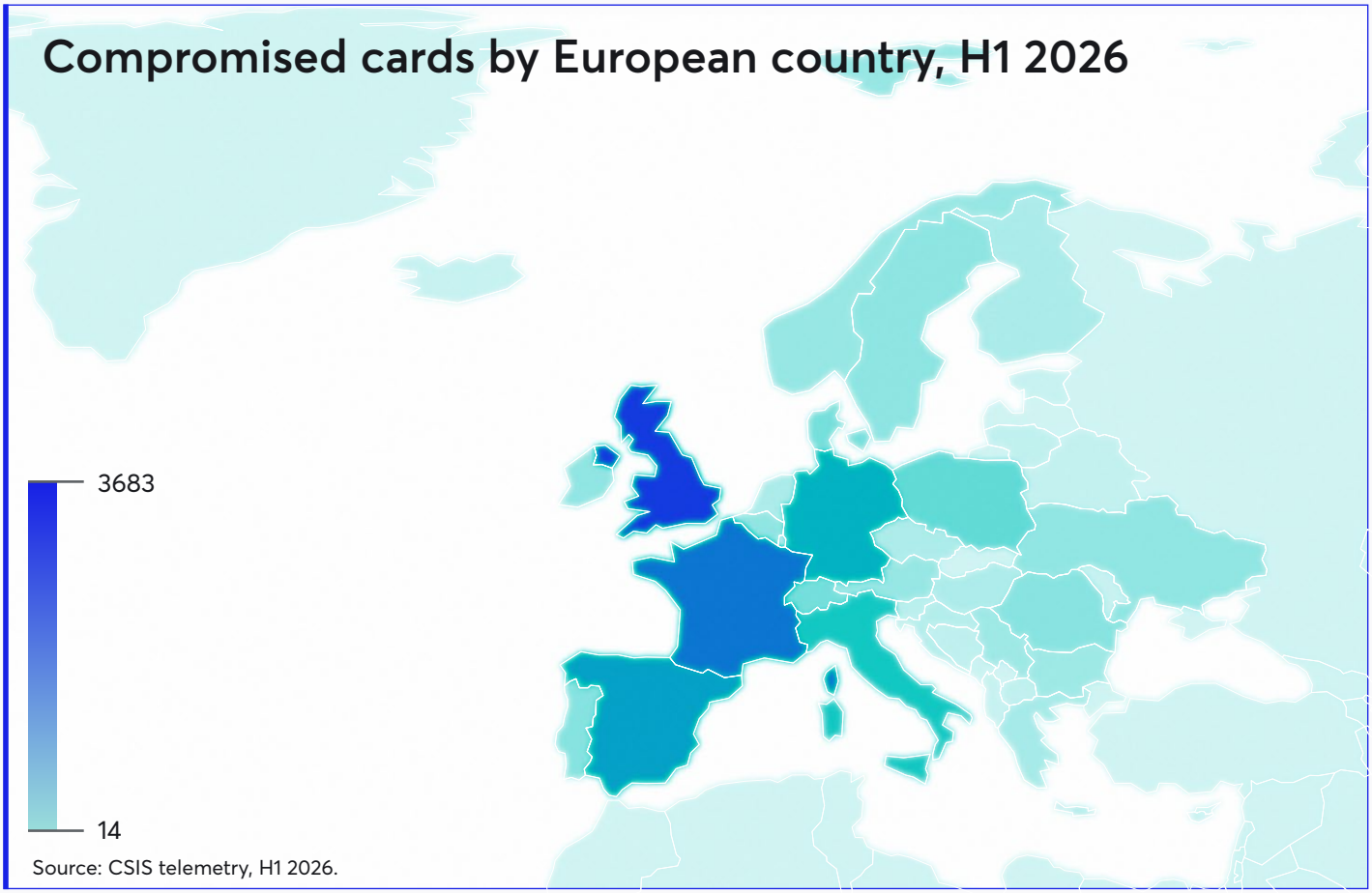
Compromised cards represent the fraud-oriented, downstream expression of the phishing activity described above. While compromised credentials are tied to access-enabled intrusion, compromised card data reflects digital skimming, e-commerce compromise, and malware-enabled theft.

The geographic distribution of compromised cards in H1 2026 is highly concentrated:

- Europe (60% of the European Top 20): The United Kingdom leads the region (18%), closely followed by France (14%), Spain (11%), Germany (9%), and Italy (8%).
- Global (81% of the Global Top 20): The global picture is overwhelmingly dominated by the United States (55%), standing far apart from Japan (12%), India (6%), Canada (4%), and Brazil (4%).

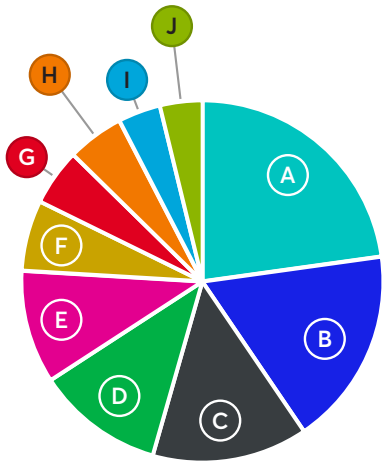
Card theft is typically part of a monetisation chain. Threat actors obtain card data and convert it into fraud, resale, or further criminal use. Defenders need visibility into payment page integrity, third-party web dependencies, and anomalous transaction testing.

Compromised cards by European country, H1 2026



Source: CSIS telemetry, H1 2026.

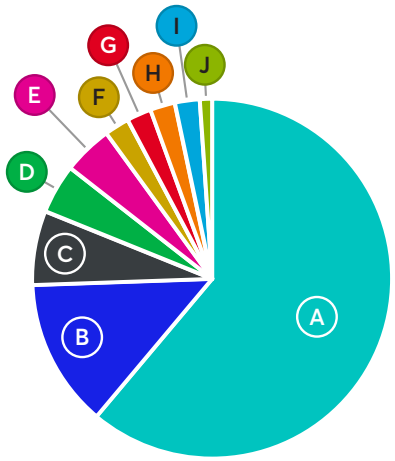
Compromised cards: European top 10



A.	GB	23%	**F.**	PL	6%
B.	FR	18%	**G.**	CH	5%
C.	ES	14%	**H.**	DK	5%
D.	DE	11%	**I.**	PT	4%
E.	IT	10%	**J.**	RO	4%

Source: CSIS telemetry, H1 2026.

Compromised cards: rest of the world



A.	US	61%	**F.**	CN	2%
B.	JP	13%	**G.**	KR	2%
C.	IN	7%	**H.**	TR	2%
D.	CA	4%	**I.**	AR	2%
E.	BR	4%	**J.**	MX	1%

Source: CSIS telemetry, H1 2026.

TRENDS

Geographic Attack Trends 37

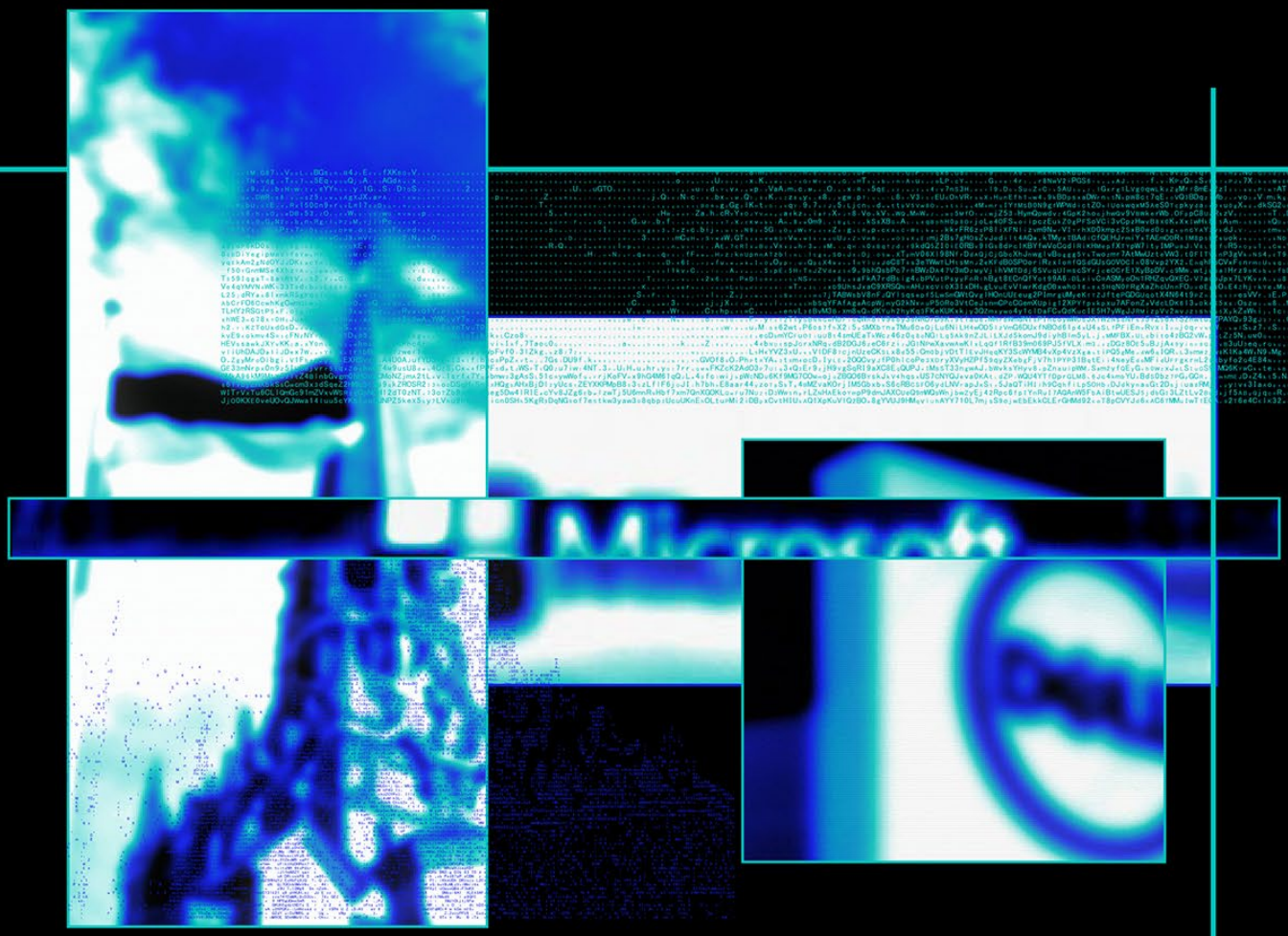
Tactics, Techniques and Procedures (TTPs) Trends 39

- AI-enabled activity 39
- Identity Pipelines and Identity Access Management 39
- Cloud and Software-as-a Service (SaaS) 40
- Ransomware and Extortion 41
- Hacktivism 41

Targeted Product/Vendor Trends 42

Common Vulnerabilities and Exposures (CVE) Exploitation Trends 44

Common Weakness Enumeration (CWE) Trends 46



Geographic Attack Trends

CSIS incident response data indicate that phishing remains the primary attack vector in Europe, particularly for access theft and fraud attempts [See: Metrics]. European phishing campaigns are also skewed towards betting and crypto-related lures, despite tech and banking brands remaining the focus globally.

In March 2026, Europol disrupted the Phishing-as-a-Service (PhaaS) operation Tycoon2FA, seizing 330 domains tied to phishing pages and control panels. This incident highlights the crucial importance of Phishing-as-a-Service (PhaaS) operations. These services offer multi-factor authentication (MFA) Bypass and Adversary-in-the-Middle (AitM) capabilities that enable them to evade conventional defensive strategies while offering efficient ways to scale and deliver their campaigns.

Another key initial access method in Europe is the use of valid accounts. CSIS Managed Detection and Response (MDR) data identified 100.4 million unique compromised credentials for Europe and the United Kingdom, with distribution concentrated in Italy and France (22% each) [See: Metrics]. These intrusions mainly targeted public-facing endpoints and applications through password-spraying techniques. This observation is further supported through reporting, such as Finland's Cyber Security Centre, which highlighted the June 2026 "FortiBleed" campaign, which compromised data from twenty Finnish firms.

During the reporting period, CSIS MDR also detected 1,213 confirmed ransomware cases across Europe. H1 2026 has seen double extortion, involving data theft and encryption, become the norm with some actors such as Cl0p and BianLian now primarily focused on data theft. Germany (261 cases) and the UK (242 cases) were the most targeted countries. This likely reflects the size of these countries as well as their concentration of high-value, commonly targeted sectors, notably German manufacturing and British professional services. Additionally, on a per-capita basis, Northern Europe emerges as the most extortion-exposed region, with 3.08 leaks per million people, ahead of Central Europe (2.28) and Western Europe (2.10).

Russian-language affiliate-driven Ransomware-as-a-Service operations Qilin and The Gentlemen account for roughly a third of extortion incidents in Europe, highlighting the continuing prevalence of Russian-language threat actors. Both groups target construction, healthcare and manufacturing entities, with Qilin also showing a focus on professional services. Notable recent breaches include the Spanish defence company Indra Group by The Gentlemen and the Austrian aviation firm Avcon Jet, both in June 2026. Qilin and The Gentlemen both favour the use of vulnerabilities for initial access via edge devices, moving within the network using default tools, and engaging in techniques to inhibit recovery and analysis like shadow-copy deletion and deleting logs.

January to June 2026 also saw threat actors place greater emphasis on 'Living off the Land' (LotL) techniques, where adversaries use pre-installed tools and applications to conduct attacks. This activity has included the use of trusted services abuse to avoid detection and disguise command-and-control (C2) communications. This has been highlighted in nation-state APT activity over the reporting period. For instance, in January 2026, APT28 targeted Ukrainian government agencies and European defence, transportation, and diplomatic entities using a critical vulnerability in Microsoft Office. The campaign used Microsoft Outlook for C2 communications using the NotDoor backdoor malware, which executed commands when it detected trigger phrases contained within emails.

In terms of hacktivism, this remains primarily driven by pro-Russian groups, such as NoName056 and its affiliates in the DDoSia project. Between January and June 2026, these groups have engaged in generally low-impact DDoS attacks against websites belonging to European local government, transport, and defence-related entities perceived to be of strategic interest.

ASSESSMENT

***Likely**: phishing and the exploitation of network perimeter endpoints remain the main routes for initial access in Europe over the next six months.*

***Likely**: adversaries increasingly attempt to abuse AI agents to automatically scan for and deploy exploits and tooling, especially with the release of cheaper open-weight models.*

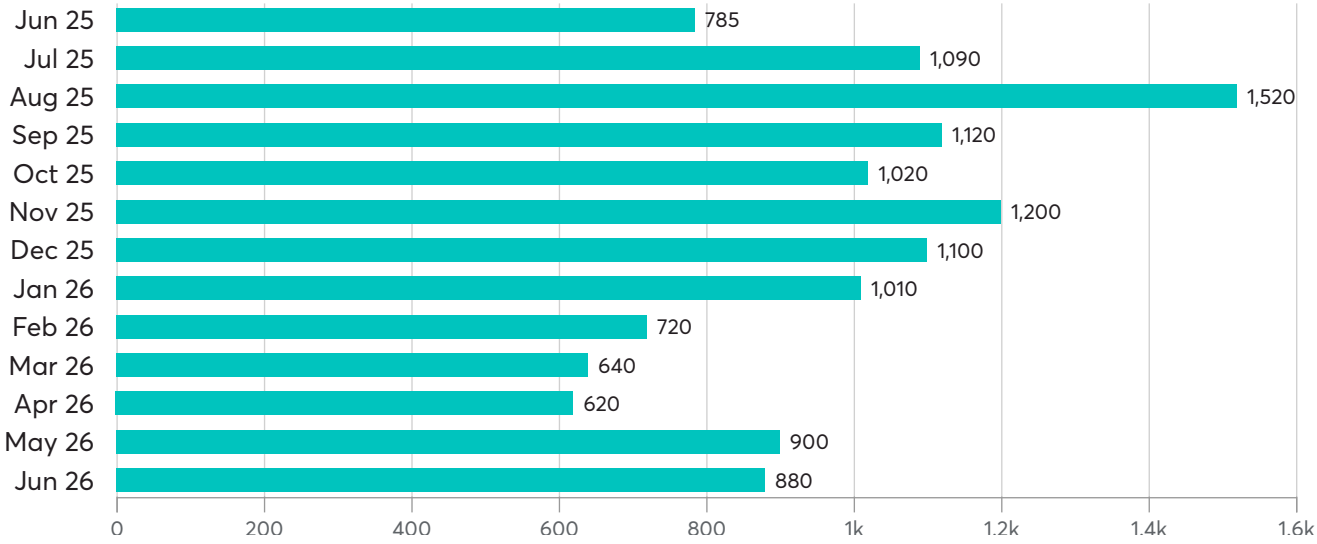
***Likely**: geopolitical risk to Europe from the Russo-Ukraine war remains elevated through H2 2026.*

***Highly likely**: disruptive targeting of OT technologies by hacktivist entities continues.*

These groups have also increased their attacks against Industrial Control Systems (ICS) in water utilities, agricultural facilities and energy plants. Threat actors have released screenshots of supervisory control and data acquisition (SCADA) and programmable logic controller (PLC) systems, though these claims have not generally been independently corroborated or led to significant public disruption. Nonetheless, the attacks highlight an increasing intent by pro-Russian activists to cause potentially significant physical disruption.

Over the next six months, these trends are likely to remain consistent, with phishing and exploitation of network perimeter endpoints as the main routes for initial access in Europe. While generative AI has been effectively used to improve phishing lures, adversaries are likely to increasingly attempt to abuse AI agents to automatically scan for and deploy exploits and tooling, especially with the release of cheaper open-weight models such as Kim K3. Geopolitical risks to Europe from the Russo-Ukraine war are also likely to remain elevated for H2 2026, with disruptive targeting of OT technologies by hacktivist entities highly likely to continue.

Claimed pro-Russian hacktivist DDoS activity on European entities, Jun 2025 - Jun 2026



Source: CSIS. Note: methodology changed between January and February 2026, removing duplicate claims by NoName057 and DDoSia Informer channels.

Tactics, Techniques and Procedures (TTPs) Trends

Threat actor TTP trends have broadly followed the availability of attractive targets while fundamental security principles remain extant. Large Language Models (LLMs) have amplified existing TTPs across the threat actor spectrum. The time required to achieve a discrete objective has decreased. The understanding of what constitutes an effective adversarial outcome has likely shifted: for example, stealing partial data, rather than taking full control over a segmented environment. This has meant that where a threat actor can complete an objective with noisy but fast techniques, they will opt to do so if a 'smash and grab' could be considered sufficient to achieve an effect. Meanwhile, threat actors aiming to maintain persistence have likely benefitted from an increased volume of immediate activity across the board.

ASSESSMENT

Almost certain: *initial access through stolen or socially engineered credentials remains the most common method used by threat actors.*

Highly likely: *for state-sponsored actors with established pipelines of operational capability, LLMs have decreased the time-to-exploit for N-day vulnerabilities.*

Likely: *criminal extortion has permanently moved away from ransomware that locks up data as its main method, towards extortion based on data stolen.*

Almost certain: *effective compromise of ICS systems is a highly desired but generally aspirational objective for longer-running hacktivist groups.*

AI-enabled activity

The proliferation of LLMs has directly and indirectly been observed to benefit attackers (T1588.007 – Obtain Capabilities: Artificial Intelligence). For state-sponsored actors with established pipelines of operational capability, LLMs have highly likely decreased the time-to-exploit for N-day vulnerabilities. This means that the development of viable exploits by experienced teams 'diff'ing' patches, focused on browsers or privileged (security) appliances at the network edge, has broadly dropped from a median 1 week in 2025 to 1 day in 2026.

While LLMs have lowered barriers to entry for attackers, the use of these models has also created challenges for them. Vibe-coded malware which is ineffective, or leaks attacker information, has resulted in partially completed attacks and counter-intelligence opportunities. Nonetheless, the ability to understand and attempt to operate against appliances and architectures such as SCADA or ICS that would have previously been out of range, is likely to encourage and accumulate experience and eventually, efficacy.

Generative AI has primarily been useful for financially-motivated state-sponsored actors and to some extent, hacktivism groups (T1683 – Generate Content). Threat actors originating from the DPRK, but physically operating globally, have used GenAI extensively to acquire IT worker positions in western organisations.

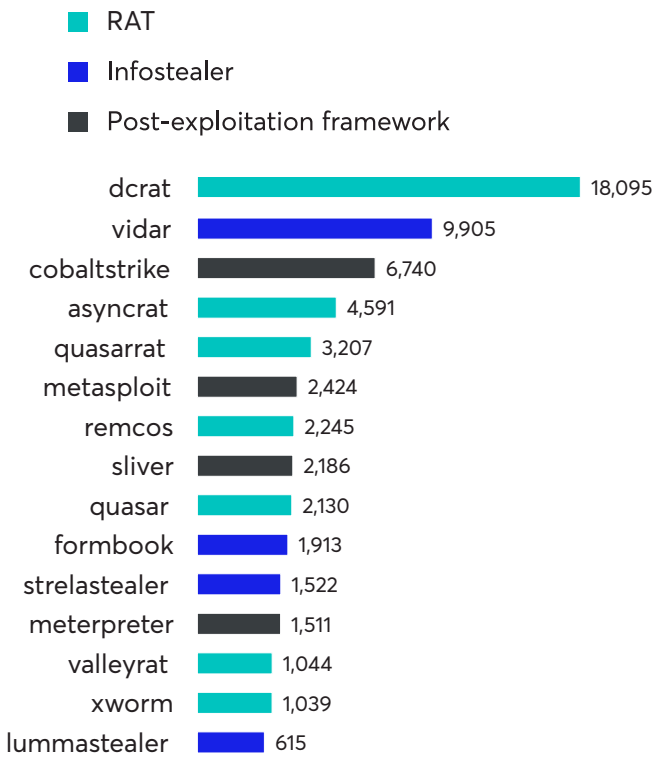
Identity Pipelines and Identity Access Management

Initial access through stolen, or socially engineered credentials, almost certainly remains the most common method used by threat actors.

Infostealers such as Vidar were prevalent across telemetry during H1. Follow on, or alternate, installation of remote access trojans such as DCRat were also used to support endpoint compromise.

Individual endpoints, i.e. laptops, were principally leveraged as a means to steal secrets, tokens, or credentials in order to gain access to wider organisational infrastructure, particularly cloud and SaaS. Lateral access to internal messaging systems, where trust between participants is usually higher, also afforded sight of confidential information.

Most prevalent C2 families by category



Source: CSIS telemetry, H1 2026.

Cloud and Software-as-a-Service (SaaS)

Changes to infrastructure have almost certainly afforded threat actors opportunities to take advantage of implementation and integration challenges. Lateral movement and persistence from a single endpoint, into and across an estate has remained a standard operating procedure. Increasingly, access to cloud and SaaS environments was achieved directly through social engineering.

Access to a cloud or SaaS environment means that a threat actor is highly likely to be able to use the tools present in those environments, install others directly, or locate another account which can do what is required.

Default configurations, misconfigurations, over-permissioned accounts, flat data shares, stored secrets/credentials, API vulnerabilities, and third-party integrations are commonly understood as viable, if not reliable, vectors to access confidential data.

The shared responsibility models (SRMs) used in disparate cloud environments can be difficult to interpret and effectively manage. Security boundaries where SaaS entities are integrated were significantly challenged in 2026. Trust in third-party and supply-chain integrations was highly likely to have been over-permissioned, and those gaps were readily exploited.

File management SaaS platforms are attractive to all threat actors. Code repositories were increasingly compromised. Email and messaging systems were explicitly targeted by established nation-state actors.

A significant advantage for threat actors aiming to exfiltrate data is to leverage the fast and wide, upload and download capabilities within a SaaS environment. This means that where previously, a threat actor might stage data for exfiltration in archived chunks, now threat actors can often export en masse, with platform-native functionality to their own, adjacent assets. Even with moderate levels of logging and controls, the proliferation of signals through an interconnected ecosystem means that threat actors are working inside a defender's effective response time.

ATT&CK techniques which are most closely associated with the breadth of current threat actor cloud activity are listed in the following table:

T1078.004	Valid Accounts: Cloud Accounts
T1110.003	Password Spraying
T1110.004	Credential Stuffing
T1133	External Remote Services
T1021.007	Remote Services: Cloud Services
T1528	Steal Application Access Token
T1550.001	Use Alternate Authentication Material: Application Access Token
T1606.002	Forge Web Credentials: SAML Tokens
T1098.001	Additional Cloud Credentials
T1098.003	Additional Cloud Roles
T1136.003	Create Account: Cloud Account
T1548.005	Temporary Elevated Cloud Access
T1671	Cloud Application Integration
T1526	Cloud Service Discovery
T1538	Cloud Service Dashboard
T1619	Cloud Storage Object Discovery
T1530	Data from Cloud Storage
T1114.002	Remote Email Collection
T1114.003	Email Forwarding Rule
T1537	Transfer Data to Cloud Account

Ransomware and Extortion

Criminal extortion operations have likely diverged permanently from a primary use of ransomware affecting availability (T1486 – Data Encrypted for Impact) to extortion due to data stolen (T1567 – Exfiltration Over Web Service). Immutable data storage platforms across multiple regions have made writing/encrypting/destroying data increasingly difficult for an adversary. Transferring confidential and proprietary data out has become easier by using the tools and infrastructure the data is hosted on.

Exceptions to this trend are still reflected in the most commonly impacted sectors. This is likely due to a prevalence of on-site infrastructure co-located with operations. In particular, the manufacturing sector briefly dropped from most affected sector by incident volume in May 2026 after consistently holding that position since June 2024.

Successful groups, such as theGentlemen, have focused capability development onto replayable methods to defeat Endpoint Detection and Response tools, so-called 'EDR killers' (T1685 – Disable or Modify Tools). These kits are mostly bundles of existing bring-your-own-vulnerable-driver techniques, rather than bespoke, quieter and per-vendor/version exploits (T1687 – Exploitation for Defence Impairment).

Third-party compromises, breached data recycling, synthetic (AI) generated data, metadata misrepresentation, and other false claims were increasingly demonstrated by groups into 2026.

Hacktivism

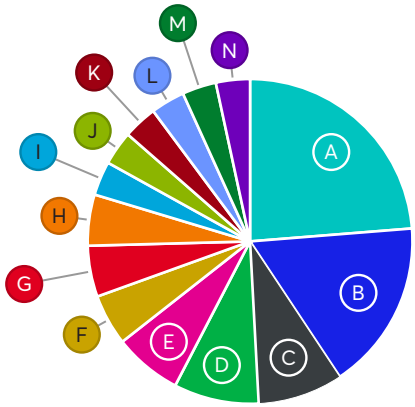
Crossover between hacktivist and criminal groups has likely increased in 2026. Several DDoS-for-hire groups (T1498 – Network Denial of Service) present as aligned with varying hacktivist groups while advertising time on their botnets. Hacktivist groups compete with extortion criminals for viable credentials. Destructive malware (wipers) were sporadically employed. The effective compromise of ICS systems is almost certainly a highly desired but generally aspirational objective for longer-running groups.

For the majority of hacktivist groups, particularly those on Telegram, there is likely value in perceiving their activity as performative. In other words, the majority of their activity is a means to increase awareness of, participation with and reinforcement of messaging, while giving participants a sense of movement.

Targeted Product/Vendor Trends

The following represents the most targeted products/vendors based on CISA KEV CVE additions in H1 2026. The data includes CVEs disclosed prior to 2026, but which were first added to the CISA KEV in 2026.

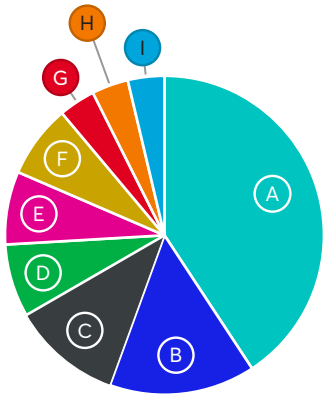
Most targeted technologies based on CISA KEV entries



A.	Microsoft	14	**H.**	Ubiquiti	3
B.	Cisco	10	**I.**	Adobe	2
C.	Google	5	**J.**	Langflow	2
D.	Ivanti	5	**K.**	LiteLLM	2
E.	Joomla Ecosystem	4	**L.**	LiteSpeed	2
F.	Fortinet	3	**M.**	Palo Alto Networks	2
G.	SolarWinds	3	**N.**	SmarterTools	2

Source: CSIS telemetry, H1 2026.

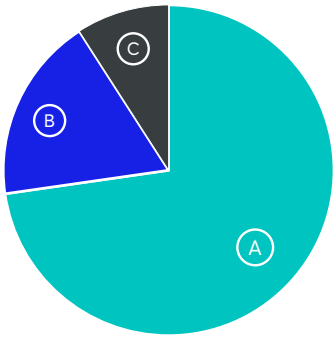
Most targeted Microsoft Technologies



A.	Windows	11	**F.**	SharePoint	2
B.	Office	4	**G.**	Configuration Ma..	1
C.	Defender	3	**H.**	DirectX	1
D.	Exchange Server	2	**I.**	VBA	1
E.	Internet Explorer	2			

Source: CSIS telemetry, H1 2026.

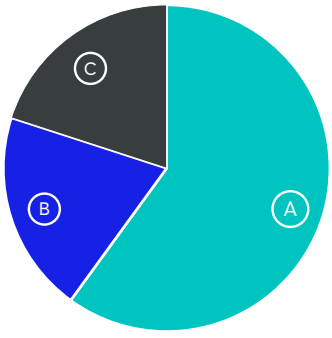
Most targeted Cisco technologies



A.	Catalyst SD-WAN products	8
B.	Unified Communications Manager	2
C.	Secure Firewall Management Center (FMC)	1

Source: CSIS telemetry, H1 2026.

Most targeted Ivanti technologies



A.	Endpoint Manager Mobile (EPMM)	3
B.	Endpoint Manager (EPM)	1
C.	Sentry	1

Source: CSIS telemetry, H1 2026.

ATTACK VECTORS

Network edge devices remain a major route for initial access.

Identity and access management tools, including single sign-on and MFA, are targeted.

Developer tooling and package repositories are being compromised.

The primary Cisco target being Cisco Catalyst SD-WAN products demonstrates the continued targeting and threat actor attention on network edge devices, such as VPNs, firewalls, network access controllers, and SD-WAN infrastructure.

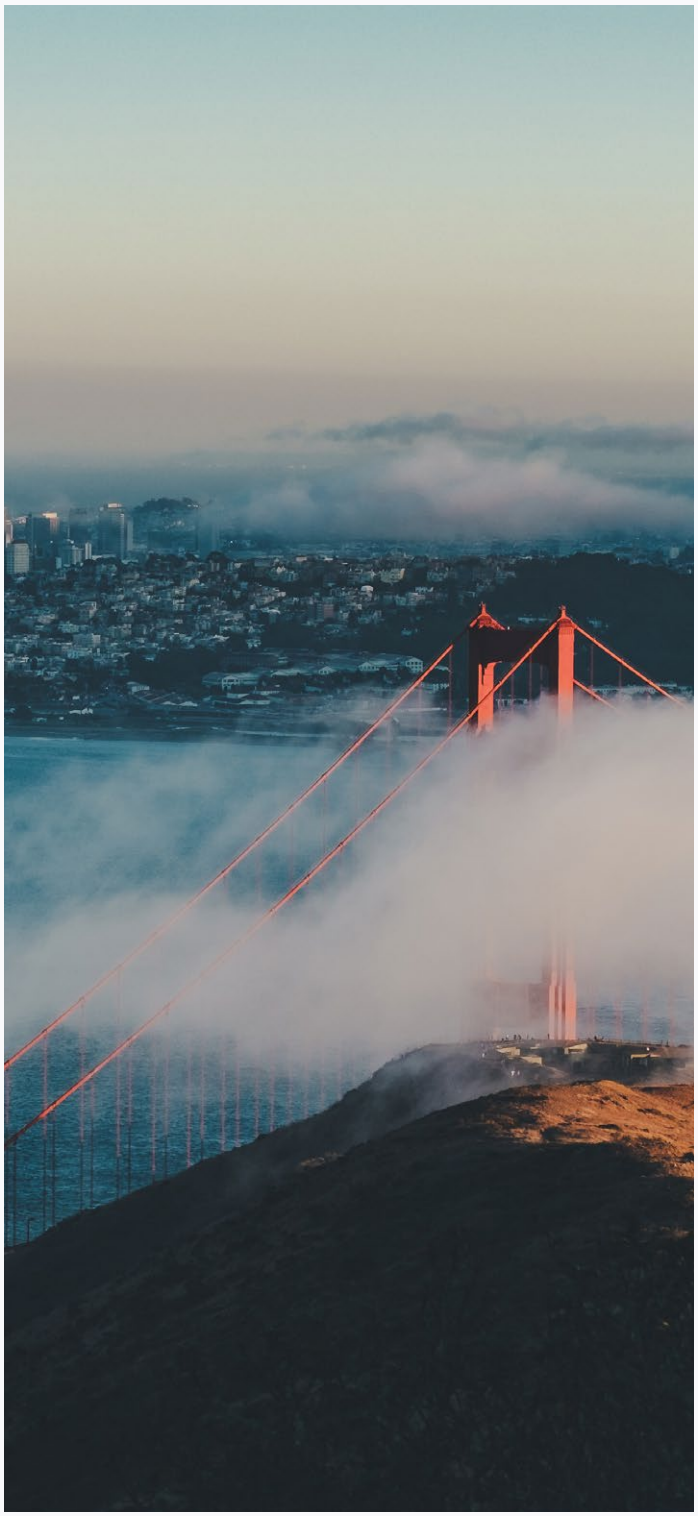
In 2025, edge-device exploitation had an eightfold increase, representing 22 percent of initial-access cases. In H1 2026, this trend continued, with Fortinet, Cisco, Palo Alto Networks, and Ivanti products appearing most frequently in exploitation campaigns.

Another significant trend is the targeting of Identity and Access Management (IAM) solutions such as single sign-on (SSO), multi-factor authentication (MFA), or cloud identity platforms, in addition to vulnerabilities that allow for IAM credential exfiltration, with such compromises providing threat actors access to multiple connected systems.

Notable related threat actor activity includes ShinyHunters and their targeting of Okta and Microsoft Entra ID SSO accounts, facilitating data theft. ShinyHunters continue to effectively impersonate IT support and call centre employees to steal credentials and MFA codes to gain access to SSO accounts.

Another major, ongoing targeting theme is the exploitation and compromise of developer CI/CD (Continuous Integration and Continuous Delivery) tooling, including AI infrastructure platforms and developer package repositories, with such instances frequently containing network access and API credentials for cloud services. Most significant in this regard was TeamPCP's 'Mini Shai-Hulud' supply-chain attack, which compromised over 160 npm packages, allowing the threat actors to steal credentials and secrets from developer machines and CI/CD runners.

Recent compromises have highlighted the inherent trust placed in such repositories, the package maintainers, and the use of automatic updates. Multiple vendors have since taken steps to combat the exploitation of automatic updates and compromised packages to spread malware. Visual Studio Code (VS Code) now applies a two-hour delay before automatically updating integrated development environment (IDE) extensions. Similarly, GitHub announced that npm v12 introduces changes aimed at preventing supply chain attacks, with install scripts no longer running automatically.



Golden Gate Bridge.

Common Vulnerabilities and Exposures (CVE) Exploitation Trends

The most significant vulnerabilities which were exploited over the reporting period include:

CVE-2025-55182 (CVSS 10.0 (v3.1)). **React Server Components (React2Shell).**

A pre-authentication remote code execution vulnerability in React Server Components. The vulnerable code unsafely deserializes payloads from HTTP requests to Server Function endpoints.

CVE-2025-55182 is notable as it also impacts the next, react-router, waku, @parcel/rsc, @vitejs/plugin-rsc, and rwsdk React frameworks and bundlers. Exploitation attempts of CVE-2025-55182 by multiple China state-nexus threat groups, including Earth Lamia and Jackpot Panda, have been reported. Large-scale, automated and opportunistic exploitation attempts of React2Shell were also reported. Researchers also reported a slow migration of this CVE into Mirai and other botnet exploitation kits, with 77,664 IP addresses vulnerable to React2Shell detected.

CVE-2025-55182 exploitation was also conducted by the threat actor tracked as CL-STA-1015, an initial access broker (IAB) with suspected ties to China's Ministry of State Security. Post-exploitation, the threat actors were identified utilising the SNOWLIGHT dropper malware on compromised Linux hosts to download and execute the VShell trojan. Additionally, the researchers noted the use of a bash reverse shell, connected to a probable Cobalt Strike server.

Additional exploitation activity by North Korea-linked threat actors was used to deliver EtherRAT. React2Shell exploitation has also led to the deployment of the MINOCAT tunneler, SNOWLIGHT downloader, HISONIC backdoor, COMPOOD backdoor, and XMRIG cryptocurrency miners. This exploitation was further attributed to multiple China-nexus threat actors, including Earth Lamia and Jackpot Panda, as well as financially motivated actors.

Additional reporting identified exploitation that led to the deployment of VShell and EtherRAT, SNOWLIGHT downloader, ShadowPAD, and XMRig. Additionally, the RondoDox Botnet now includes CVE-2025-55182 exploitation capabilities.

A large-scale automated campaign to steal credentials via CVE-2025-55182 was identified, which was attributed to a threat cluster tracked as UAT-10608. During the observed activity, 766 hosts across various cloud providers and geographies were compromised, with the threat actors collecting environment variables and secrets (API keys, database credentials, GitHub/GitLab tokens), SSH keys, cloud credentials (AWS/GCP/Azure metadata, IAM credentials), Kubernetes tokens, Docker/container information, command history as well as process and runtime data.

CVE-2025-61882 (CVSS 9.8 (v3.1)). Oracle E-Business Suite.

Vulnerability in the Oracle Concurrent Processing product of Oracle E-Business Suite. Allows unauthenticated attacker with network access via HTTP to compromise Oracle Concurrent Processing. Successful attacks allow remote unauthenticated threat actors to perform remote code execution and achieve a full system takeover.

CVE-2025-61882 is notable due to its exploitation by Cl0p during a large-scale corporate extortion campaign that claimed numerous victims.

Reporting identified that threat actors exploited what may be CVE-2025-61882 as a zero-day vulnerability against Oracle EBS customers as early as 09 August 2025, and potentially before that on 10 July 2025. The campaign utilised a multi-stage, fileless malware framework, including GOLDVEIN.JAVA, SAGEGIFT, SAGELEAF, and SAGEWAVE, to evade file-based detection. Google did not formally attribute the campaign to a threat actor, citing that the Cl0p ransomware and branded infrastructure were previously used by at least one other threat actor, and not exclusively by Cl0p (FIN11).

On 16 October 2025, Cl0p shared 24.9 GB of stolen data from American Airlines for download on its Tor data leak site. On 17 October 2025, following the publication of 24.9 GB of American Airlines data by Cl0p, the group announced that American Airlines' subsidiary, Envoy Air, had also been affected by the Oracle breach. A spokesperson for the brand announced that they "are aware of the incident involving Envoy's Oracle E-Business Suite application."

Cl0p then shared 8TB of data related to the Oracle EBS breach on its Tor leak site. It is highly likely that this does not refer to new information but refers to the total data volume so far for companies impacted by the incident, such as Schneider Electric, Emerson, and American Airlines, and Logitech.

CVE-2026-21509 (CVSS 7.8 (v3.1)). Microsoft Office.

Reliance on untrusted inputs in a security decision in Microsoft Office allows an unauthorised attacker to bypass a security feature locally.

CVE-2026-21509 is notable due to its exploitation by the Russian state-sponsored threat actor, APT28 in espionage campaigns targeting government, military, and transportation organisations in Poland, Ukraine, Turkey, Greece, the UAE, and other Eastern European nations.

Exploitation of CVE-2026-21509 has been attributed to APT28, a Russian state-sponsored threat actor. An identified campaign involved phishing emails that delivered malicious DOC files themed around EU COREPER consultations and impersonated Ukrainian government entities. Opening the documents triggered a WebDAV-based infection chain leveraging COM hijacking, a malicious DLL, embedded shellcode concealed within an image file, and a scheduled task to deploy the COVENANT framework, which uses the Filen cloud storage service for command-and-control (C2). Further investigation identified three additional malicious documents targeting EU-based organisations, indicating that the campaign extends beyond Ukraine.

Additional details of an APT28 campaign, dubbed 'Operation Neusploit', were released, in which exploitation of CVE-2026-21509 targeted users in Ukraine, Slovakia, and Romania to deliver MiniDoor or PixyNetLoader payloads.

CVE-2026-22769 (CVSS 10.0 (v3.1)). Dell RecoverPoint for Virtual Machines.

An unauthenticated remote attacker with knowledge of the hardcoded credentials could potentially exploit this vulnerability, leading to unauthorised access to the underlying operating system and root-level persistence.

CVE-2026-22769 is notable due to its exploitation as a zero-day vulnerability by a suspected China-linked espionage group, tracked as UNC6201 since at least mid-2024.

Exploitation allowed the threat actors to deploy a SLAYSTYLE web shell and establish persistent access using BRICKSTORM and the newer GRIMBOLT backdoor. The campaign also involved stealthy lateral movement into VMware environments through Ghost NICs and iptables-based Single Packet Authorisation. The activity was identified during incident response engagements after compromised appliances were observed communicating with command-and-control infrastructure associated with BRICKSTORM and GRIMBOLT.

CVE-2026-20127 (CVSS 10.0 (v3.1)). Cisco Catalyst SD-WAN.

A vulnerability in the peering authentication in Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, and Cisco Catalyst SD-WAN Manager, allows an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system.

CVE-2026-20127 is notable, with exploitation attributed to UAT-8616, and malicious activity dating back to at least 2023. The vulnerability allowed threat actors to escalate to administrator privileges as an internal non-root user account and create a rogue peer joined to the network control plane of an organisation's SD-WAN. Several proofs-of-concept (PoC) have been found for the vulnerabilit. The threat actors then leveraged the built-in update mechanism to downgrade to an earlier version, further escalate to the root user via CVE-2022-20775, then restore the software to its original version. The actor likely used a publicly available proof-of-concept exploit for this vulnerability to run commands as the root user.

CVE-2025-40551 (CVSS 9.8 (v3.1)). SolarWinds Web Help Desk.

SolarWinds Web Help Desk was found to be susceptible to an untrusted data deserialization vulnerability that could lead to remote code execution which would allow an attacker to run commands on the host machine. This could be exploited without authentication.

CVE-2025-40551 is notable due to its exploitation alongside another WHD vulnerability, CVE-2025-26399[31] (CVSS 9.8 (v3.1)), to deploy legitimate tools for remote access. These include an outdated version of the incident response tool Velociraptor for command-and-control, and a Zoho ManageEngine Remote Monitoring and Management agent for persistence, with the campaign likely beginning on 16 January 2026.

Common Weakness Enumeration (CWE) Trends

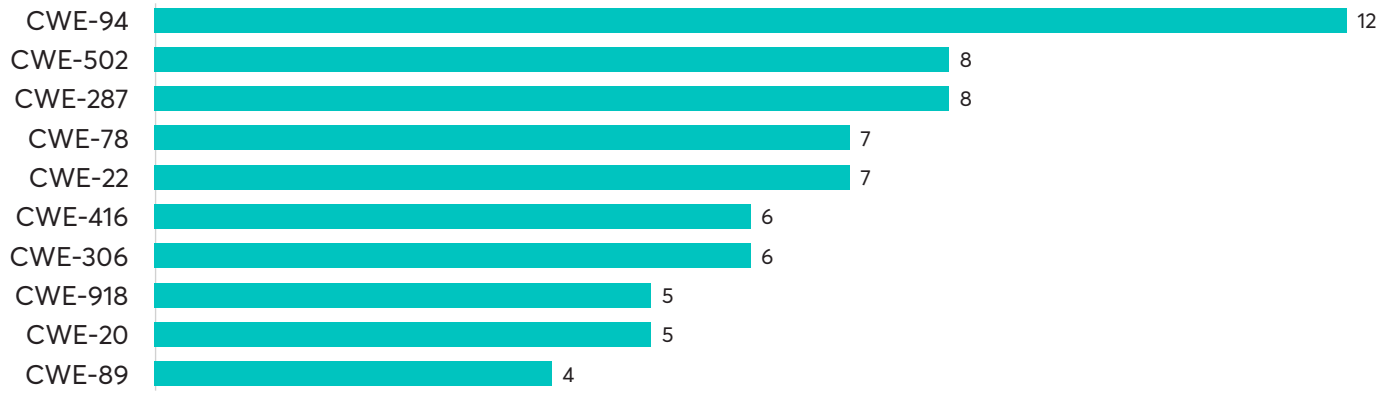
In 2025, the top ten CWE (Common Weakness Enumeration) software weaknesses were as follows:

CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-416	Use After Free
CWE-787	Out-of-bounds Write
CWE-306	Missing Authentication for Critical Function
CWE-502	Deserialization of Untrusted Data
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-122	Heap-based Buffer Overflow
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Based on CISA KEV CVE additions in H1 2026, the current top ten CWE software weaknesses are as follows:

CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-502	Deserialization of Untrusted Data
CWE-287	Improper Authentication
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-416	Use After Free
CWE-306	Missing Authentication for Critical Function
CWE-918	Server-Side Request Forgery (SSRF)
CWE-20	Improper Input Validation
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Top 10 CWE software weaknesses in CISA KEV entries, H1 2026



Source: CSIS telemetry, H1 2026.

Vendors and software developers are ultimately responsible for the CWE weaknesses present within their software. Whilst threat actors have no direct control over their root cause, they seek to identify those that will yield the most impactful outcomes, such as code injection, path traversal, use-after-free, out-of-bounds write, and buffer overflow weaknesses.

Additionally, AI-accelerated vulnerability discovery has changed the scale and speed at which these weaknesses are discovered. Vendors are now leveraging the same AI capabilities to aid vulnerability discovery and remediation.

Based on the CISA KEV entry data, in H1 2026, the most prevalent CWE software weakness was CWE-94: Improper Control of Generation of Code ('Code Injection'). CWE-94 allows threat actors to execute arbitrary code and access resources that they would otherwise be prevented from accessing.

In 2025, CWE-94 was the 7 most common CWE, with seven related entries in the CISA KEV catalogue. The twelve CWE-94 CISA KEV entries in H1 2026 mark a 58% increase.

Recent examples of CWE-94 vulnerabilities include CVE-2026-20045 in Cisco Unified Communications Manager (Unified CM), CVE-2025-37164 in Hewlett Packard Enterprise (HPE) OneView, and CVE-2026-1281 and CVE-2026-1340 in Ivanti Endpoint Manager Mobile (EPMM), all of which are known to be exploited in the wild.

It is likely that the upward trend in CWE-94 weaknesses will continue in H2 2026, as threat actors and AI capabilities continue to identify the most destructive outcomes.

INSIGHTS

AiTM – A Targeted BEC Campaign 49
- Problem 49
- Investigation 49
- Solution 50

The Increasing Pace of AI Evolution 51
- AI-assisted vulnerability discovery 51
- AI-assisted exploitation 51
- Agentic and AI-assisted cyberattacks and defence 51
- Targeting of internal AI systems 52
- Access to AI 52

Open-source Component Attacks 53
- TeamPCP 53
- North Korea 53
- AI 53
- Downstream impact 54



AiTM – A Targeted BEC Campaign

Investigating a months-long AiTM compromise of a Microsoft 365 account and targeted BEC campaign

Problem

A private-sector professional services organisation was compromised without malware, a breached endpoint or a new interactive sign-in that obviously looked hostile. The attacker appears to have stolen a valid Microsoft 365 session token through an adversary-in-the-middle (AiTM) phishing flow and replayed that already authenticated session from unmanaged infrastructure. Because the token represented a completed authentication event, multi-factor authentication did not provide the expected barrier.

The intruder then treated the tenant as a long-term intelligence source. Over several months, the attacker monitored email, accessed sensitive SharePoint and OneDrive material, and learned the language, timing and participants of a genuine commercial dispute. That knowledge was eventually used to impersonate a legitimate third party and pursue invoice fraud against a major institutional customer. The incident exposed confidential business and personal information, created fraud risk and triggered regulatory assessment obligations. Its cloud-only nature also left traditional endpoint-focused controls with little to see.

Investigation

CSIS incident responders set out to answer four practical questions: when the intrusion began, how access was obtained, what the attacker reached and whether the fraud was opportunistic or targeted. The team correlated the available Microsoft 365 sign-in and audit trail with mailbox configuration, message activity, cloud-file access and the fraudulent correspondence. This joined a series of individually low-signal events into a defensible incident timeline.

The earliest confirmed malicious cloud activity occurred at the start of the observable timeline, although the token was probably stolen beforehand. The pattern was consistent with AiTM-enabled session theft: the same authenticated cloud context was reused over time from changing, unmanaged infrastructure. No original lure was recovered, so the precise phishing step could not be proven; the conclusion remained a high-confidence assessment based on access behaviour, not an unsupported claim.

The earliest confirmed malicious cloud activity occurred at the start of the observable timeline, although the token was probably stolen beforehand. The pattern was consistent with AiTM-enabled session theft: the same authenticated cloud context was reused over time from changing, unmanaged infrastructure. No original lure was recovered, so the precise phishing step could not be proven; the conclusion remained a high-confidence assessment based on access behaviour, not an unsupported claim.

Early abuse included changes to Outlook Web Access mailbox or calendar settings. Repeated mailbox access followed, allowing the attacker to track conversations, payment themes and the status of the real dispute. Reconnaissance later expanded to SharePoint and OneDrive content associated with multiple employees, including financial, contractual and dispute-related material. This was not a quick smash-and-grab: the attacker waited until the business context could support a convincing pretext.

Shortly before the fraud attempt, malicious inbox rules were created to divert, delete or silently mark replies as read. Attacker-controlled sender infrastructure was added to trust settings, and fraudulent drafts were staged inside the victim's mailbox. The outgoing messages used a lookalike domain and authenticated email, making them technically credible while remaining fraudulent. By suppressing replies, the attacker isolated the compromised user from the conversation and reduced the chance of discovery.

CSIS concluded that the activity was deliberate and highly targeted. A substantial volume of business communications and cloud documents had been exposed, and the incident required both technical scoping and regulatory review. Crucially, discovery came through security review rather than an automated prevention or detection control. That gap explained how a valid session could remain useful for months while producing no malware alert and no endpoint forensic trail.

Solution

Containment focused first on invalidating the attacker's cloud access. Compromised identities were remediated, active sessions were revoked, authentication material was reset, and the malicious mailbox rules and trust-list changes were removed. Related accounts and cloud assets were reviewed for parallel abuse, while relevant audit data was preserved so containment did not destroy the evidence needed to understand scope and impact.

The response then separated three workstreams that are often blurred in BEC cases. The identity workstream established how the session was replayed and where access persisted. The fraud workstream traced drafts, sent mail, suppressed replies and lookalike infrastructure so affected counterparties and payment processes could be handled through trusted channels. The data-impact workstream mapped accessed messages and files to confidentiality and regulatory obligations. This disciplined structure gave decision-makers a single, evidence-led view instead of competing fragments.

Longer-term remediation addressed the conditions that gave the stolen token value. Exchange Online and webmail access should be restricted to managed or compliant devices; Entra ID token protection should be enabled where supported; and continuous access evaluation, risk-based revocation and stronger reauthentication should shorten the useful life of a hijacked session. Microsoft 365 audit data should be centralised, with detections for access from unmanaged devices, anomalous session reuse, unusual SharePoint or OneDrive activity, destructive inbox rules, trust-list changes and fraudulent drafts.

The investigation demonstrates the value of CSIS's cross-disciplinary response model: cloud forensics, fraud analysis, containment guidance and management-ready documentation were brought together by one team. Organisations can extend that readiness through CSIS Emergency Response, use Managed Detection & Response for continuous expert-led monitoring and remediation, and apply a Cloud Security Assessment to identify the Microsoft 365 configuration gaps that make BEC and session replay easier.

Lessons learned

- MFA is a checkpoint, not a guarantee. A stolen live session can let an attacker operate as an already authenticated user.
- Cloud-only does not mean low impact. No malware or endpoint persistence was needed to expose data and execute fraud.
- Mailbox rules are an anti-forensics tool. Small configuration changes can hide replies, erase warning signs and extend the fraud window.
- Patience makes fraud persuasive. Weeks of document and email reconnaissance enabled the attacker to mirror a real dispute and billing context.

Recommendations

- Constrain session replay. Require managed or compliant devices, deploy token protection where supported, and use continuous evaluation and risk-based reauthentication.
- Detect identity and mailbox manipulation. Alert on unmanaged access, anomalous session reuse, new destructive rules, trust-list changes and suspicious draft activity.
- Watch the data layer. Baseline access to sensitive SharePoint and OneDrive content and investigate deviations from normal business workflows.
- Prepare for the business response. Maintain an incident-response retainer and require out-of-band verification for payment changes, new bank details and dispute-related invoices.

The Increasing Pace of AI Evolution

AI-assisted vulnerability discovery

As AI has been increasingly integrated into vulnerability discovery processes, the number of released security updates from vendors has broken records, increased security bulletin release frequencies, and threatened to overwhelm security teams with patches. If the number of releases continue to increase, or remain at current levels, security teams will struggle to implement all patches, lengthening existing fix timescales further still. With the mean time-to-exploit negative on the Zero-Day Clock for 2026 at time of writing, compared with 2.3 years in 2018, this highlights an urgent disparity between attackers and defenders.

While AI-assisted discovery will almost certainly keep patch volumes high in the immediate-to-short term, in the medium-term these volumes will likely be sustained, but could reduce, as AI-enabled testing may usher in an era of more secure software, with vulnerabilities discovered and remediated before products are released. Awareness of AI-assisted vulnerability discovery may spur products development to prioritise security-by-design further, however the use of AI in 'vibe coding' could also result in increasingly insecure product releases.

As vendors and projects also become overwhelmed by the number of submitted bug reports, more may move to limit the number of permitted submissions, and end bug bounty programs. As vendors themselves struggle to act on the volume of submissions, it is possible that they may attempt to pressure researchers not to publicly disclose vulnerabilities in the future, instead of remediating the issues.

A greater emphasis on prioritisation of vulnerabilities will need to be adopted, already highlighted by the US National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) announcing a new risk-based prioritisation model to manage the influx of Common Vulnerabilities and Exposures (CVE) submissions. AI can aid defenders with prioritisation efforts and assist during fix proposal and validation. It can also be leveraged for automated patch management and implementation itself.

ASSESSMENT

Almost certain: *AI-assisted discovery keeps patch volumes high in the immediate to short term.*

Likely: *those volumes are sustained in the medium term, though they could reduce if AI-enabled testing produces more secure software.*

Highly likely: *AI facilitates the creation of polymorphic malware, and gives agents a dynamic, adaptable approach that allows fast failure correction.*

Possible: *vendors overwhelmed by submissions attempt to pressure researchers not to disclose vulnerabilities publicly, rather than remediating them.*

Possible: *mass access to offensive AI tooling "democratises" attacks, spreading money more thinly across the cybercriminal ecosystem if the supply of tooling increases relative to demand.*

AI-assisted exploitation

While vulnerability prioritisation is a helpful defensive solution, AI-tooling will also make it easier for threat actors to exploit lower severity vulnerabilities, by assisting in the creation of more complex exploit chains. AI will also lower the proficiency barrier and shorten the timescale for creating working exploits. In addition to prioritisation, defensive resources may be increasingly directed towards alternative techniques to combat cybercrime, such as stronger legal regulations around paying ransoms, and more focus on law enforcement operations to combat malicious activity.

Agentic and AI-assisted cyberattacks and defence

AI has already been integrated into real-world attacks. AI-assisted phishing incidents have successfully tricked people and systems, and AI-assisted malware aids the development of malicious code, as attacks begin to shift towards more agentic implementations. A proof-of-concept self-sustaining agentic computer worm has been demonstrated.

It is highly likely that AI will facilitate the creation of polymorphic malware, and provide agents with a dynamic, adaptable approach, allowing fast failure correction. In addition to the integration of AI models into real-world threat actor campaigns, it has become obvious that the capability of autonomous AI agents has substantially increased in recent months. Alongside a spate of model evaluation security incidents, agentic AI ransomware has been observed in the wild [2]. Access to agentic AI will continue to be further leveraged by threat actors. A possible consequence of mass access to offensive AI-tooling could be the "democratisation" of attacks, distributing money more thinly across the cybercriminal ecosystem if a supply of tooling increases relative to demand. However, this also means mass-access of exploits by bad actors. Access to models and compute could become a more important factor in launching complex, sustained AI attacks, leaving well-resourced cybercriminals and nation state APTs able to better execute the most large-scale, sophisticated AI campaigns. Ultimately, many AI-assisted attacks will target lower-sophistication system weaknesses, highlighting the importance of fundamental cyber hygiene practices for target organisations. Defenders can leverage the behaviour of offensive AI threats to aid with detection. For example, LLM self-narration can provide the goals and actions taken by agents within the payloads themselves.

AI can itself be used defensively, with AI firewalls providing dynamic, adaptable evaluations and responses to threats, analysing contextual patterns over static rules and signatures. Defensive Agentic AI could be used to manage vulnerabilities and patching, aid high-volume triaging, and perform countermeasures after evaluation of alerts.

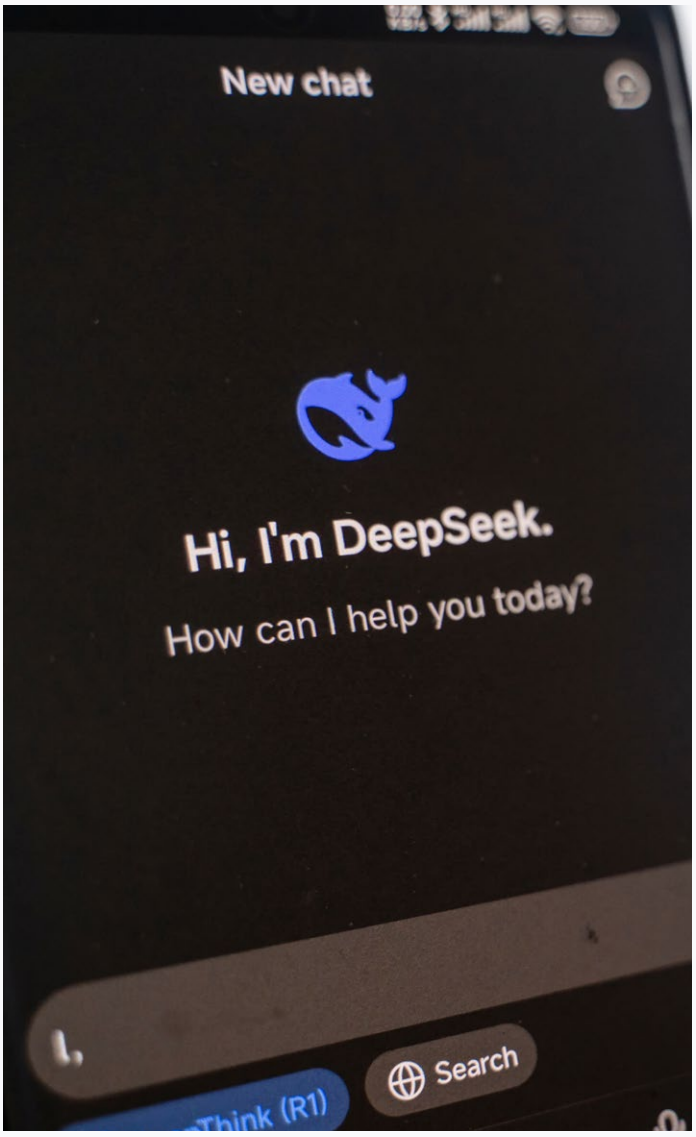
Targeting of internal AI systems

Internal AI models also present an attack surface in companies. The Open Worldwide Application Security Project (OWASP) ranks Prompt Injection as the top risk for LLM applications. Companies may also be exposed via 'shadow AI' applications, where AI tools are utilised by employees without awareness or approval from IT teams.

Access to AI

Factors limiting the use of offensive and defensive AI tooling include access to advanced models and compute. Proprietary US frontier AI models have been subject to, or voluntarily submitted to, export controls or limited previews due to safeguard concerns, before being redeployed or released. However, open-weight, or jailbroken models, present attackers with opportunities to bypass or remove safeguards altogether.

Open-weight models have consistently improved with the most advanced closed-weight models, albeit with a small capability gap, with the leading closed-weight edge driven by US AI labs, and the leading open-weight edge driven by Chinese AI labs (see Section: State Nexus – China for discussion of Chinese AI development, adoption, and implications). Alongside economic considerations, businesses may choose to host open-weight internal models for customisability, and data privacy concerns. Leveraging open-weight models defensively can also avoid wrongly blocked requests from safety guardrails.



Chinese DeepSeek prompt window.

Open-source Component Attacks

In H1 2026, open-source supply chain attacks targeting Continuous Integration and Continuous Delivery/Deployment (CI/CD) pipelines and developer ecosystems continued the escalation first seen in September 2025. Payloads evolved to become more modular and evasive against industry defences, expanded trust-abuse techniques, expanded exfiltration targets from npm tokens to cloud and CI/CD credentials, and self-propagated using stolen credentials.

The initial Mini Shai-Hulud wave targeting Aqua Security's Trivy vulnerability scanner marked the start of the H1 software supply chain attack spike. The Trivy attack enabled the threat actor TeamPCP to use stolen secrets to compromise multiple packages downstream in the supply chain, including Checkmarx KICS. TeamPCP also compromised the LiteLLM and Telnyx PyPI days later, both of which use Trivy in their CI/CD pipeline. The self-propagating worm logic and credential theft enabled recursive waves of compromises down the supply chain.

The speed of intrusions is notable; the threat actors prioritised opportunistic collection of all exposed secrets and fast exits. In the Checkmarx compromise, stolen npm tokens were operationalised within 24 hours for the Bitwarden downstream attack.

TeamPCP

On 12 May, TeamPCP released the Mini Shai-Hulud source code on BreachForums, enabling waves of copycat campaigns using the code and mimicking their TTPs. In June, researchers reported a new variant of Shai-Hulud dubbed Miasma targeting the RedHat Cloud Services npm namespace. Shortly after, the Hades variant, identified as the PyPI branch of Miasma, targeted bioinformatics, graph machine learning, and Model Context Protocol (MCP) libraries. It is realistically possible that the variants are a direct result of the source code release, although this made it difficult to attribute attacks to distinct threat actors.

Besides (Mini) Shai-Hulud, TeamPCP was responsible for other impactful campaigns, such as CanisterSprawl and Megalodon, the latter of which compromised over 5,500 GitHub repositories.

"The speed of intrusions is notable; the threat actors prioritised opportunistic collection of all exposed secrets and fast exits"

North Korea

Meanwhile, North Korea-linked actors (i.e., BlueNoroff) focused on cryptocurrency theft were attributed to the Axios and Mastra attacks. TeamPCP is loud and boisterous, but North Korean threat actors have abused the software supply chain for years (i.e., Contagious Interview) and scaled dramatically in late 2025 by embracing automation. One technique illustrating this is the abuse of VS Code's tasks function to auto-run malicious code when users open a repository, which has been mirrored by TeamPCP and variant clusters.

AI

A few compromised packages had a significant blast radius, especially when developers used AI-enabled automation workflows that merged malware within minutes without human review, thereby amplifying exposure windows. In the LiteLLM compromise, PyPI detected and removed packages within 46 minutes, but during that window, the malicious versions had been downloaded 47,000 times.

AI tools also expand the attack surface. In a Miasma campaign, attackers designed their malicious commit to execute upon opening of the repository in an AI coding tool. JetBrains IDE plugins posed as AI coding assistants to trick users into entering API keys, indicating threat actors' active intent to target popular AI tools.

AI has likely enabled both TeamPCP and North Korean threat actors to accelerate and scale their operations, leading to the spike in attacks in H1 2026.

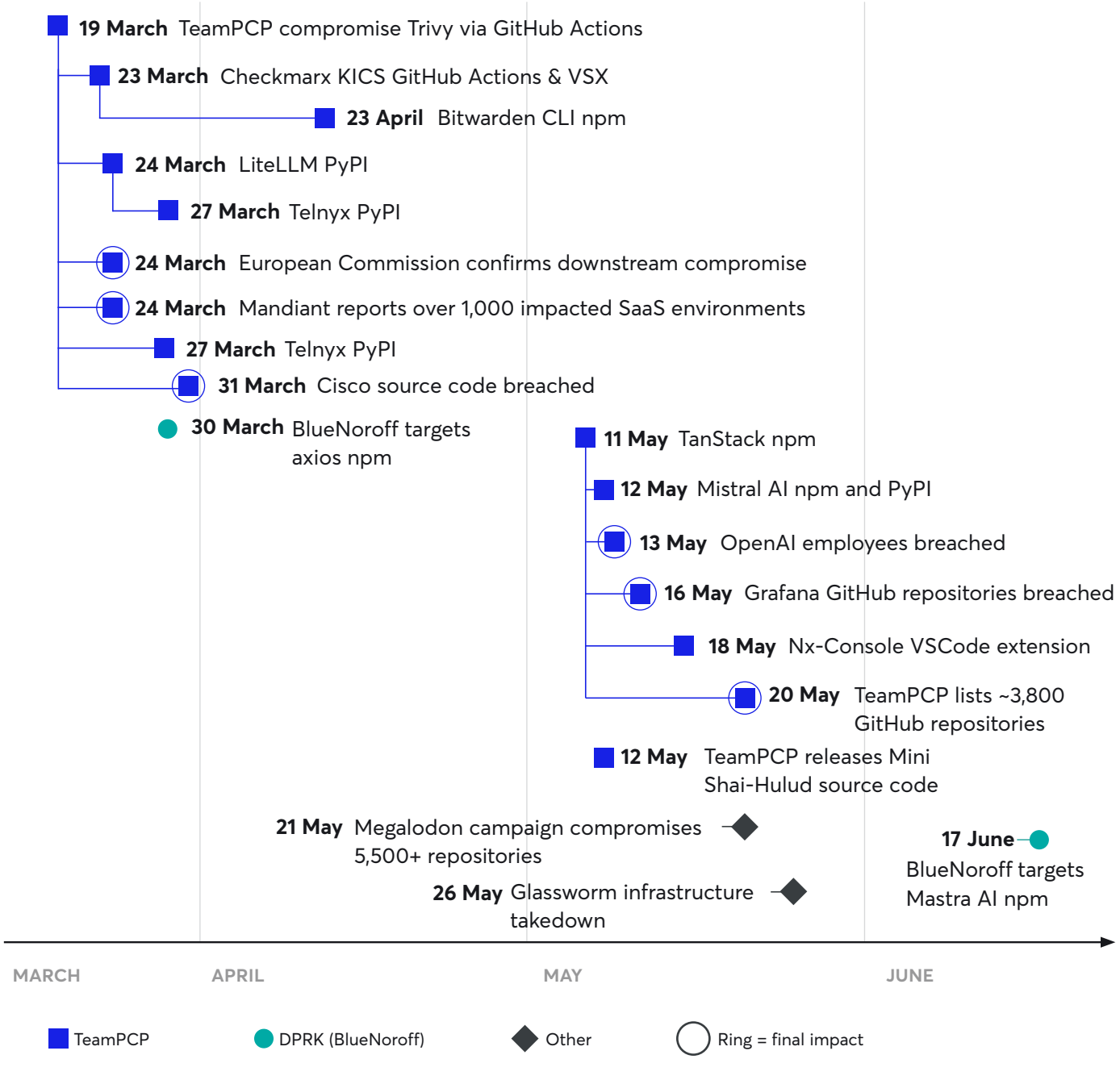
Downstream impact

The initial wave of Mini Shai-Hulud attacks targeting Trivy had a significant blast radius, impacting over 1,000 SaaS environments, including the European Commission. Other major downstream impacts included the TanStack and Axios attacks, which each led OpenAI to rotate potentially compromised code-signing certificates, and the LiteLLM PyPI compromise, which led to a 4TB data breach at Mercor, an AI startup.

While the exact blast radius of each campaign is difficult to quantify, incidents with publicly reported downstream incidents throughout H1 2026 have been visualised below:

Just one device compromised via a malicious artefact in the software supply chain can enable threat actors to steal CI/CD credentials, cloud credentials, keys, and repository secrets, enabling secondary attacks directly on your organisation.

Selected examples of high-profile software supply chain attacks and their downstream impact in H1 2026



ASSESSMENTS

State-Nexus Operations and Regional Threats to Europe 56
- China 56
- Russia 57
- United States 58
- North Korea 58
- Iran 59
- Commercial Spyware Vendors (CSV) 60

Hybrid Threats in Europe 61

Influence Operations Targeting Europe 62
- Likely threat actors 62
- Recent evolution in approach and TTPs 63

European Digital Sovereignty 64

Ransomware and Extortion in Europe 65

European Supply Chain Targeting 67



State-nexus operations and regional threats to Europe

China

Over the course of the reporting period, there were four key themes in reporting concerning the Chinese cyber threat to Europe.

- In January, it was reported that Salt Typhoon had been detected targeting UK telecoms networks as part of a long-running espionage campaign. Subsequent reporting, in April, indicated that the same threat actor may also have targeted Italian telecoms networks. Chinese targeting of telecoms networks has been an established theme for over a decade, impacting multiple jurisdictions. Given the unparalleled access that targeting such networks can provide, such attacks are almost certain to remain a constant threat for the near future.

- In March, the EU imposed sanctions on Chinese companies and individuals for conducting cyber-attacks against EU member states. These sanctions relate to activities that occurred in 2022-23 but signal the EU's willingness to publicly address the Chinese espionage threat, despite the potential for retaliation by China, amid growing trade tensions.

- In April, a joint advisory published by several national intelligence agencies, including several European countries, highlighted a 'widespread shift in TTPs, towards networks of compromised infrastructure' based on 'externally provisioned, large-scale networks of compromised devices' by Chinese nation-state threat actors. The development of these networks has occurred over several years; therefore, this cannot be considered a 'new' threat. However, it represents a major evolution in tradecraft and operational infrastructure with significant implications for the ability of the Chinese state to conduct operations at a greater scale, with greater persistence and enhanced deniability. In addition to the espionage threat, the advisory noted that these networks had facilitated pre-positioning of offensive cyber capabilities on critical national infrastructure (CNI).

- In April, it was reported that Mustang Panda had re-focused its targeting on Europe, after a hiatus of several years. EU institutions and diplomatic missions, NATO organisations and European national governments were all targeted in the campaign, potentially indicating an increased intelligence focus on Europe. This change in targeting is likely driven by a combination of factors, including increasing European responsibility for the conduct of the war in Ukraine (a matter of significant geopolitical interest to the Chinese Communist Party (CCP)) and increasing tensions between the EU and China over trade and security.

Based on the 15th Five-Year Plan, the focus of Chinese commercial espionage in the near term is likely to be on AI (especially the manufacture of advanced semiconductors, innovative large language models (LLMs), and industrial AI applications), Quantum technology and 6G communications. More broadly, robotics, connected electric vehicles (EVs), and biomedicine are likely to remain priority areas for commercial intelligence collection. As it becomes increasingly clear that AI holds the key to much of future economic growth, military power, and geopolitical influence, obtaining information to achieve supremacy in this field is almost certainly amongst Beijing's priority intelligence requirements.

In the longer term, however, as China closes the innovation gap with the West, the country's focus on intellectual property (IP) theft is likely to recede, potentially freeing up significant resources to support other intelligence requirements.

As the reporting above indicates, China's capability and capacity to deliver cyber operations at speed and scale are growing, supported by an expanding private sector cyber industry and a dedicated ecosystem. As friction with Europe over regulation, 'de-risking' and market access continues, and as the United States presses Europe to take primary responsibility for its own security and defence, it is assessed as likely that the EU will continue to see an increase in Chinese espionage activity, pre-positioning within CNI and cyber-enabled influence operations.

Long-term concerns over the implications of Chinese military action over Taiwan persist. A Chinese embargo or naval blockade of Taiwan would have significant supply chain implications for Europe, particularly regarding semiconductors, and a Chinese military action would almost certainly result in even greater disruption to global trade and security. Whilst the threat of an embargo / military action is assessed to be slowly increasing in the longer term, there are indications that the immediate/ short-term threat is reduced as President Xi continues to make changes within the senior echelons of the Chinese military.

Russia

Russian nation-state operations continued to target critical national infrastructure, almost certainly to enable disruptive or destructive attacks. Hybrid campaigns paired physical sabotage with influence operations, primarily intended to weaken support for Ukraine, amplify social and political divisions, and exacerbate pre-existing social fault lines (see The War in Ukraine Section for further details). State and criminal cyber infrastructure converged further as intelligence services outsourced operations to cheaper, deniable proxies. Targeting of Ukraine's weapons supply chain persisted through attacks on transport and logistics operators. Throughout, this activity ran in parallel with cease-fire diplomacy, demonstrating that threat levels remain largely independent of the progress of peace talks. The most significant development within H1 is assessed to be deepening state-criminal convergence, which is lengthening attribution timelines and eroding the evidential basis on which the collective European response depends.

Three factors have the potential to significantly alter the Russian threat to Europe in the short- to medium-term: the strategic battlefield situation in Ukraine, domestic issues within Russia, and the potential for further Russian military operations outside Ukraine.

Looking at the battlefield situation in Ukraine, it is assessed as highly likely that front lines will remain largely static in the near term and the war of attrition will continue. A Russian battlefield collapse, stemming from effective Ukrainian strikes on Russian military supply chains (the 'Deep Strike' and 'Mid-Strike' campaigns), is increasingly likely, though still a remote possibility. If such a battlefield 'rout' occurs, however, it is almost certain that Russia would be far less constrained in targeting Europe, with both cyber-attacks and physical attacks against CNI. In such a situation, sabotage of undersea communications cables becomes significantly more likely. Other destructive capabilities held in reserve, including NotPetya-style self-propagating malware, may also be deployed as strategic caution is eroded.

"Three factors have the potential to significantly alter the Russian threat to Europe in the short- to medium-term: the strategic battlefield situation in Ukraine, domestic issues within Russia, and the potential for further Russian military operations outside Ukraine"

Domestically, within Russia, the removal of President Putin is assessed as highly unlikely in the near term; however, there is some evidence that the likelihood is increasing, albeit from a very low baseline. Such a scenario would not necessarily decrease the cyber threat to Europe. The most likely course of action would be a short-term reduction in Russia's offensive cyber operations as the new leadership evaluates its posture.

However, a contested succession could fragment the Russian security services, leading to a power struggle, erosion of strategic control, and associated threats. In the longer term, it is assessed as likely that Europe's cyber threat will remain elevated under any succession outcome, as Russian hostility is structurally rooted in geography, confrontation with NATO, and strategic objectives that outlast any individual leader. European organisations should therefore treat signs of elite fracture in Moscow as indicators of heightened near-term risk, rather than as prospects for de-escalation.

As outlined above, Russian 'grey zone' operations (coercive, disruptive, or hostile actions designed to weaken an opponent whilst falling short of full-scale war) are increasing. It is assessed as unlikely that Russia will instigate a conventional military confrontation with Europe, outside of Ukraine. However, this likelihood is increasing, and there is significant potential for unplanned escalation due to grey-zone operations. Such an expansion of military operations would almost certainly result in a significant increase in cyber threats, like the one described above regarding a Russian battlefield collapse.

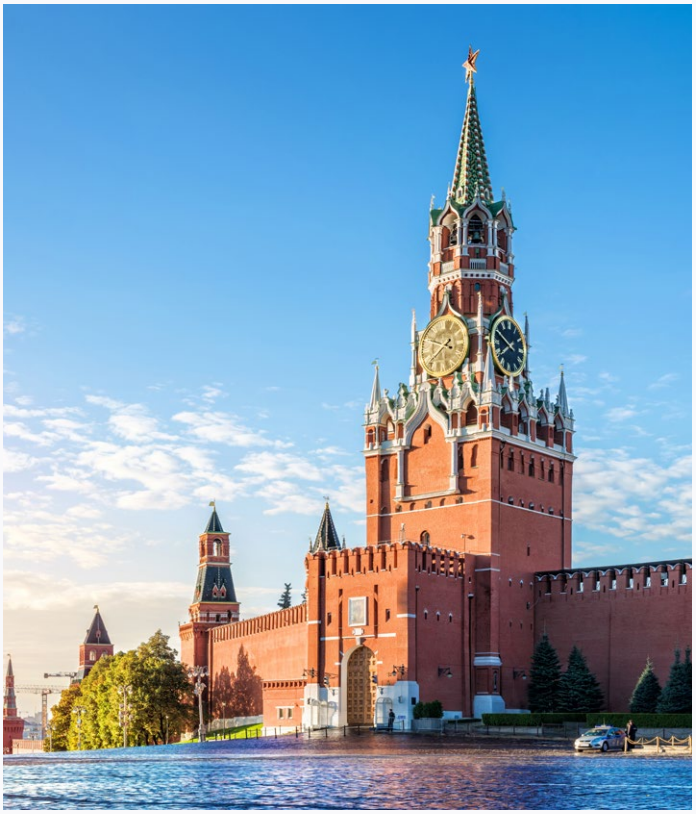


Photo of the Spasskaya tower.

United States

The United States cyber posture was primarily shaped by the decisive shift toward more openly acknowledged offensive operations in H1 2026, as highlighted by the 28 February strikes on Iran and the March 2026 National Cyber Strategy. The strategic implication of the US moving towards more offensive kinetic and cyber operations extends beyond Iran; the public acknowledgement of state cyber effects against critical infrastructure lowers the global threshold for such operations and furnishes adversaries with a legitimising precedent for comparable actions, with potential implications for European CNI.

The US is known to have conducted cyber enabled intelligence collection operations against allies, including the EU, for over a decade. Some increase in this activity is assessed as likely as a result of territorial disputes over strategic geographic assets like Greenland, trade, and European foreign policy, with intelligence collection focussed on elements of the EU and component national governments which are focussed on foreign policy, defence and trade (see Section on US-Europe relations). Two factors have the potential to alter the US cyber threat to Europe in the short- to medium-term: the outcome of the 2026 midterm elections and the medium- to long-term trajectory of US policy beyond the current administration under President Trump.

The midterms are unlikely to significantly constrain the extensive foreign policymaking powers of the executive branch, making a significant change in the direction of US cyber policy highly unlikely. There is, however, the potential for these elections to increase volatility in the short term. A change of administration following the 2028 presidential election presents a realistic possibility of moderation in Washington's cyber approach (see Section XX: US-Euro relations). This would be unlikely to eliminate the underlying threat: US collection against allied government and industry predates the current administration and reflects enduring intelligence priorities rather than the posture of any given single American presidency.

> *"The midterms are unlikely to significantly constrain the extensive foreign policymaking powers of the executive branch, making a significant change in the direction of US cyber policy highly unlikely"*



Photo of the statue of liberty.

North Korea

(DPRK / Democratic People's Republic of North Korea)

North Korean cyber activity in H1 2026 remained focused on financial gain rather than the pre-positioning and espionage that characterise Russian and Chinese operations. Its activity is opportunistic and revenue-driven, with Europe treated as an opportunity rather than a strategic priority. Recruitment-based operations persisted and expanded, including campaigns such as Contagious Interview, which used fake job offers to compromise software developers. Software supply chain targeting also continued, again focusing on developers and open-source infrastructure as access points. This tradecraft appears increasingly sophisticated, using compromised packages and repositories to reach downstream victims. North Korea's focus on cryptocurrency targets also continued, with wider implications as crypto-based transaction systems, including the proposed digital euro, become more mainstream. Across these activity strands, artificial intelligence is acting as a force multiplier, helping close capability gaps such as foreign-language fluency, improving social engineering at scale. Two factors are likely to shape the North Korean threat to Europe over the near- to medium-term: greater use of AI in operations and the expansion of workforce infiltration into European organisations.

On AI-enabled operations, North Korean actors are highly likely to increase the speed and scale of attacks by integrating AI more fully into existing workflows. The developer ecosystem is likely to face more intensive targeting, with a shift towards compromising individuals rather than organisations. Corporate controls are stronger than those of individual developers, who present a broader attack surface and a more accessible route to downstream compromise. The result is an expanded target set at a lower operational cost.

On workforce infiltration, the placement of fraudulent North Korean IT workers in Western companies is highly likely to expand further into Europe over the next reporting period. Enforcement pressure in the United States has pushed the scheme towards European employers, aided by local facilitators, stolen or forged identities, and the normalisation of fully remote hiring. Although this is better understood as an insider threat than a network intrusion, it still underscores the need for stronger organisational security.

Placed workers generate sanctions-evading revenue through salaries, and in some cases, their exposure has led to data theft and extortion. European organisations should treat identity verification in remote hiring as a core security control rather than an administrative formality.



Photo of Juche Tower.

Iran

Iran's cyber threat posture in H1 was driven primarily by regime survival. The US and Israeli strikes on 28 February degraded Iran's cyber command and fractured its regional proxy network, narrowing Tehran's objectives to retaliation, deterrence and the suppression of domestic and diaspora opposition. Activity against Israel surged in volume through the period but remained overwhelmingly low in sophistication, dominated by DDoS attacks, defacements, and opportunistic intrusion.

One development of significant concern was operational technology (OT) targeting, in which Iranian-affiliated actors exploited internet-connected industrial control equipment across the water, energy, and government sectors, causing real operational disruption. This is significant for Europe, given the ubiquity of the affected equipment, though the tradecraft remained opportunistic rather than engineered, and Iran's targeting rationale prioritises Israel and the USA above Europe.

"One development of significant concern was operational technology (OT) targeting, in which Iranian-affiliated actors exploited internet-connected industrial control equipment across the water, energy, and government sectors"

Nonetheless, Iran's most effective coercion remained non-cyber, resting on kinetic threats to shipping and some indications of intent to target individuals on European soil. Iran remains a second-tier actor, not comparable in capability to Russia or China, with much of the Western alarm it has generated reflecting a reaction to noise rather than to demonstrated effect. Whilst the direct cyber threat to Europe from Iran is limited, there is clearly potential for significant disruption to global supply chains as a result of the threats to traffic in the Strait of Hormuz and, potentially, the Bab el-Mandeb.

Houthi attacks on shipping through the Strait of Hormuz and the Bab el-Mandeb remain the most effective physical arm of Iranian pressure on European interests. Should these chokepoints remain contested, supply chain disruption and its economic knock-on effects in Europe are highly likely to persist and could escalate, carrying risks of civil unrest and, in extreme cases, the physical targeting of executives linked to US or Israeli interests. Should the straits reopen and de-escalate, the main factor of Iranian pressure on Europe recedes with them. Further opportunistic targeting, similar to the attack on the US medical equipment company Stryker, remains a possibility, and there is potential for Iranian

state sponsored threat actors to shift from opportunistic exploitation toward deliberate, engineered manipulation of Industrial Control Systems (ICS) potentially enabling a disproportionately significant real-world impact.

The current leadership in Tehran is assessed as weakened and its succession increasingly contested since the February strikes that confirmed the death of Supreme Leader Ayatollah Khomeini. Regime change is assessed as unlikely in the immediate / short term. In such an event, the most likely result would be a near-term decline in state-directed operations as new leadership consolidates its position. However, a fractured succession has the potential to unleash less-restrained proxy and hacktivist activity without centralised control, raising near-term volatility even as Iran's strategic cyber capability is severely reduced.



Photo of Milad Tower in Tehran.

Commercial Spyware Vendors (CSV)

Two key themes are assessed to be of significance regarding the deployment of commercial spyware over the reporting period, neither of which is entirely new.

Firstly, the market for commercial spyware continues to grow, with an increasing number of nation-states using these capabilities. Confirmed deployments have targeted journalists, civil society figures, and political entities across EU member states, with Predator and Pegasus infections continuing to be identified on devices belonging to European targets during the period. Secondly, whilst quantifiable reporting is unavailable, there are indications that commercial entities are being targeted more frequently, likely reflecting the growing use of these tools by private firms, potentially for competitive intelligence.

More broadly, the offensive cyber ecosystem is becoming harder to map as spyware vendors, exploit brokers, and infrastructure providers collectively lower the barrier to entry for states without mature cyber capabilities, and potentially for other, non-state actors. As Europe consolidates its position at the centre of a rules-based trading bloc, it is likely to attract greater attention from a broad spectrum of second-tier threat actors, meaning that targeting with CSV products is almost certain to grow. Two factors are likely to shape this threat over the short- to medium-term: the effectiveness of international efforts to constrain the market and the expanding pool of states able to buy commercial spyware.

Initiatives such as the Pall Mall process seek to establish norms and frameworks to limit the misuse of these technologies. However, such efforts are unlikely to slow market growth. The international environment remains fragmented, enforcement is weak, and demand continues to outpace supply. Vendors can also relocate or rebrand faster than policymakers can respond within national jurisdictions. The market is therefore likely to keep growing despite efforts to restrict it.

Regarding the expanding pool of state clients, it is assessed as likely that European government, industrial, and civil society targets will face increased attention from this widening set of actors as they pursue objectives tied to trade, regulation and diaspora communities. For European organisations. For European organisations, the implication is clear: the threat is no longer confined to a small number of highly capable states, because capability can now be purchased.

Hybrid Threats in Europe

Hybrid and grey-zone operations are now a persistent feature of the European business environment, rather than a set of isolated national-security incidents. The principal pattern over the past year is a Russia-linked campaign that blends sabotage, cyber activity, information manipulation, election interference, proxy recruitment, maritime shadow-fleet activity, drone incursions and exploratory targeting of critical infrastructure. The purpose is strategic: to raise the cost of European support for Ukraine, weaken public confidence in institutions, expose gaps in NATO and EU response thresholds, and create disruption while avoiding a clear act of war.

The Baltic and North Seas have become the clearest theatre for infrastructure-focused grey-zone activity. Repeated incidents involving undersea communications, electricity and energy infrastructure have highlighted how exposed European business operations are to systems that are difficult to monitor, expensive to repair and often privately owned.

A major subsea cable attack occurred on 31 December 2025, when Finnish authorities responded to damage affecting a Helsinki-Tallinn fibre-optic cable and boarded the vessel Fitburg in one of many attacks showing a clear pattern of disruption since the start of Russia's war. The wider concern is that Russia's shadow fleet is no longer solely as a sanctions-evasion mechanism. There are indications that it is also functioning as a sustained hybrid-warfare platform, enabling suspected undersea cable damage and drone activity around military, airport and other critical infrastructure sites across the Baltic and North Sea region.

> ***"Fundamentally, hybrid operations are designed to make normal business activity feel uncertain, costly and politically exposed"***

Russia-linked sabotage activity in Europe has also become increasingly decentralised with the intent to frustrate attribution. Russia is waging an unconventional campaign involving sabotage, vandalism, espionage, covert action and cyber activity against European critical infrastructure and other targets. The campaign exploits legal and investigative opportunities by using low-cost proxies, criminal intermediaries and online recruitment, allowing the sponsor to generate disruption while maintaining plausible deniability.

HIGHEST-RISK SECTORS

Energy · Telecoms · Transport and logistics · Finance · Cloud services · Defence supply chains · Ports · Aviation · Media · Data centres · Companies with government or Ukraine-linked roles

Election interference remains central to the strategic purpose of hybrid operations because it can influence policy, polarise societies and weaken confidence in democratic institutions without requiring a kinetic attack. Moldova's 28 September 2025 parliamentary election provides a recent and relevant case. Reporting and analysis describe Russian foreign information manipulation and interference, illicit financing, vote-buying, Telegram networks, cryptocurrency-linked payment methods, paid protests, cyber activity and deepfakes aimed at shaping Moldova's geopolitical direction and undermining its pro-European trajectory.

Cyber operations are increasingly connected to physical effects, reconnaissance and influence activity. The UK NCSC's 2025 review warned that cyber risk is now a boardroom issue because incidents can halt operations, disrupt production, expose customer data and create financial, legal and reputational consequences. Industry reporting similarly argues that Russian-linked hybrid activity is blending cyber and physical tactics, including attempted access to infrastructure systems, claims by pro-Russian hacktivists, and activity around utilities and critical sites.

Hybrid threat activity will almost certainly continue through 2026 and will remain deliberately ambiguous. The EU has reaffirmed its intention to use sanctions, the cyber diplomacy toolbox, the hybrid toolbox and cooperation with the private sector to deter activity affecting democratic processes, critical infrastructure and societal resilience. NATO is also moving from a reactive model towards deeper private-sector partnerships, including cyber providers, utilities and energy companies, to improve warning and response.

The immediate corporate priority is dependency mapping. Boards should understand which telecoms providers, cloud regions, subsea routes, ports, rail lines, energy suppliers, managed-service providers and critical vendors could create single points of failure. Resilience exercises should test a combined outage, cyber compromise, physical incident and disinformation event, rather than treating each risk separately. Critical sites should review perimeter security, CCTV coverage, drone reporting procedures, contractor vetting, suspicious-approach reporting and escalation routes to law enforcement.

Fundamentally, hybrid operations are designed to make normal business activity feel uncertain, costly and politically exposed. The highest-risk sectors are energy, telecoms, transport and logistics, finance, cloud services, defence supply chains, ports, aviation, media, data centres and companies with government or Ukraine-linked roles. However, second-order effects will likely reach far wider to shared utilities.

Influence Operations Targeting Europe

Influence operations are coordinated, often deceptive efforts to shape perceptions or behaviour, including foreign information manipulation and interference, covert influence, and cyber-enabled activity. Key themes in reporting over the H1 2026 are as follows:

- Influence operations present a moderate-to-high reputational risk to prominent European organisations, especially those whose authority depends on public trust, including governments, election bodies, media, universities, NGOs, defence firms and major consumer brands. Over the next 12-24 months, targeting will remain high-volume, event-driven, and increasingly localised.
- Russia and its aligned influence ecosystem will almost certainly remain the principal threat actor. China is likely to pose a narrower but still significant risk, focused on defending core political and economic interests.
- The main risk is not sudden reputational collapse but cumulative erosion of confidence, reflected in greater scrutiny, weaker partnerships and higher legal, compliance and communications costs.
- Serious damage is most likely when hostile narratives exploit genuine weaknesses, incorporate authentic or stolen material, or are amplified by credible domestic actors.
- Threat actors will highly likely continue combining established methods with cyber intrusion and AI-enabled content production. AI is highly likely to improve scale, speed and localisation more than persuasive effect.

> *"Greater European disruption of known networks will likely encourage actors to use disposable domains, rotating personas and smaller outsourced networks"*

Likely threat actors

Russia and Russian-aligned networks: Russia will almost certainly remain the most active and persistent state-linked threat. Its objectives are likely to include weakening European cohesion, reducing support for Ukraine, discrediting democratic institutions and exploiting divisions over migration, defence, energy, sanctions and living costs. Its advantage lies in a broad ecosystem of state, proxy and quasi-independent channels able to sustain repeated and deniable operations.

China: China is likely to remain the second most significant state actor, though more selective than Russia. Likely targets include governments, universities, media organisations, technology firms, think tanks and NGOs involved in China policy, Taiwan, human rights, critical technology or strategic investment. Chinese activity is more likely to seek narrative control and reputational pressure than broad societal disruption.

Other state and state-aligned actors: Belarus is likely to reinforce Russian-aligned narratives, particularly on migration, border security, Ukraine and NATO, though with limited independent reach. Iranian actors present a narrower, more event-driven threat, especially to diaspora groups, opposition movements, Persian-language media and organisations connected to Israel or sanctions policy.

IMPACT OF AI

The principal change has been the scaling, concealment and faster deployment of influence operations, rather than a wholly new ability to persuade European audiences.

Generative AI is now routinely used to produce and translate text, images, audio and video.

The EEAS identified AI-related techniques in 27% of the incidents it examined during 2025.

Much of that content remained low-quality and attracted limited organic engagement.

Recent evolution in approach and TTPs

Over the past six months, the principle change to information operations targeting European organisations has been the scaling, concealment, and faster deployment of influence operations, rather than a wholly new ability to persuade European audiences. Generative AI is now routinely used to produce and translate text, images, audio, and video. The EEAS identified AI-related techniques in 27% of the incidents it examined during 2025, up from 41 cases in 2024 to 147 in 2025. However, much of this content remained low-quality and attracted limited organic engagement. AI has therefore increased the volume of hostile material and the burden on organisational communications teams more than its intrinsic capability.

Operations have also become more covert. Approximately 9.5% of the recurrent channels mapped by the EEAS were covert, state-aligned, or unattributed rather than overt state sources. States increasingly outsource activity to proxy media, contractors, influencers and commercial amplification networks. This provides plausible deniability and increases the risk that targeted organisations respond too slowly or make premature attribution.

Threat actors are reusing established networks of fabricated websites, personas, and amplification accounts across different countries and events. These assets can be localised or directed within days, allowing actors to exploit the information gap immediately after a leak, cyberattack, accident, or controversial announcement. Recent Russian operations have combined AI-enabled productions, cross-platform amplification, information laundering, and the manipulation of official statements.

Information manipulation is also increasingly integrated with cyber and physical activity. Phishing, account compromise, DDoS attacks, website defacement and selective leaks can create a newsworthy event around which a reputational narrative is constructed. The EU consequently assesses information manipulation as part of broader hybrid campaigns rather than an isolated communications threat.

Despite this evolution, most operations still fail to generate significant organic engagement. The critical escalation point remains uptake by credible domestic journalists, politicians, employees, or influencers. The main recent change is therefore an increase in the speed and frequency of reputational challenges, not a universal increase in their impact.

Over the next 12-24 months, influence operations against European organisations are likely to remain high-volume, event-driven, and increasingly localised. Organisations connected to elections, Ukraine, defence, sanctions, migration, energy, and critical technology will almost certainly face the greatest exposure.

Greater European disruption of known networks will likely encourage actors to use disposable domains, rotating personas and smaller outsourced networks. AI-generated content will improve, but credible amplification and a connection to genuine organisational weakness will remain more important than technical sophistication.



Close-up of fibre-optic lines

Key indicators include:

- Registration of local-language domains resembling the organisation or established media.
- Dormant or newly created accounts beginning coordinated discussion of the organisation.
- Increased phishing or unusual interest in employees and internal documents.
- Identical narratives appearing across several languages or platforms within hours.
- Synthetic media or leaked material emerging immediately after a breaking event.
- Coordinated activity by proxy outlets, influencers, and hacktivist channels.
- DDoS attacks or defacement accompanied by claims or incompetence or concealment.
- Uptake by credible domestic actors, mainstream media, regulators, or politicians.
- Conflicting public statements from different parts of the targeted organisation.

> *"States increasingly outsource activity to proxy media, contractors, influencers and commercial amplification networks"*

High online volume alone should not be treated as evidence of reputational impact. The strongest warning of significant harm is from coordinated or covert channels into authentic public debate, stakeholder decision-making, or exposes inconsistencies in the organisation's response.

European Digital Sovereignty

One of the consequences still playing out from the breakdown of the transatlantic relationship is a growing drive among European and Western states to reduce supply chain dependencies on the US over concerns that service will be arbitrarily and suddenly disrupted as a result of political decisions. For example, following the US imposition of sanctions on the International Criminal Court in February 2025, in May 2025, access to the chief prosecutor's Microsoft email account was suspended. For observers in Europe, the ICC case was a warning shot. Across Europe, governments are making moves away from US software and technology providers like Microsoft and instead seeking homegrown solutions in pursuit of 'digital sovereignty'.

For example, the European Commission is currently calling for tenders for a sovereign cloud alternative to Microsoft services and has just proposed a European Technological Sovereignty Package to strengthen continental capacity across AI, semiconductors, cloud and open-source technologies. Member states are reviewing existing contracts and pushing for open source or homegrown options. Alongside service disruption, extensive US data access laws, such as the 2018 Cloud Act, may also be driving digital sovereignty policies across Europe: in July 2026, aerospace manufacturer Airbus announced migration of critical applications from AWS to French cloud provider Safeway, citing a need to retain sensitive data under European control.

Pursuit of digital sovereignty can bring positive developments: reducing strategic dependencies and single points of failure can help insulate countries and organisations against geopolitical shocks and potential supply chain disruptions. However, it also risks creating more issues than it fixes. External and internal political pressure may drive rushed, improper implementation of sovereign solutions without appropriate due diligence and consideration of security risks. This pursuit of digital sovereignty can, therefore, conversely introduce more technical (as opposed to political) supply chain risk, rendering an entity ultimately more insecure.

> *"One of the consequences still playing out from the breakdown of the transatlantic relationship is a growing drive among European and Western states to reduce supply chain dependencies on the US"*

Implementing new solutions that lack the 'tried-and-tested' value from legacy/historic vendors like Microsoft or Google may also reduce security posture. For cybersecurity solutions, this could take the form of reduced visibility: a smaller-scale national provider is unlikely to have the telemetry and access to the sheer amount of global IoCs and intelligence feeds as a tech behemoth like Google, for example. Smaller solutions may also lack established capabilities and functionality, further impacting detection and response.

This issue is particularly acute when considering advanced technologies such as AI models: as it currently stands, US models are the market leaders and homegrown options are unlikely to be viable alternatives in the near future. While use of US AI models can realistically bolster security (e.g., in terms of vulnerability detections), more entrenched dependence on US technology renders entities vulnerable to geopolitical shocks that could impact service provision. US-based AI models also raise additional issues for data security and confidentiality.

Digital sovereignty may also manifest as different organisations ultimately using different products and services. This lack of cohesion could negatively impact interoperability across various entities – for example, in intragovernmental or public-private coordination—reducing ability to cooperate, share intelligence and identify and respond to cyber security threats and incidents. There is also a learning curve and adaptation process required in adopting new products and ways of working that can hamper and frustrate personnel and potentially exacerbate misconfiguration issues and accidental insider risk as users adapt to new processes.

THE TRADE-OFF

Independence: *reducing strategic dependencies and single points of failure can help insulate against geopolitical shocks and potential supply chain disruption.*

Technical risk: *the pursuit of digital sovereignty can introduce more technical supply chain risk, rendering an entity ultimately more insecure.*

Reduced visibility: *smaller national providers are unlikely to match the telemetry, global IoCs and intelligence feeds of the largest vendors, and may lack established capabilities and functionality.*

Fragmentation: *organisations could end up on different products, reducing the ability to cooperate, share intelligence and respond to incidents.*

Rising exposure: *homegrown vendors become more attractive targets as adoption grows, and smaller and newer vendors may lack the resources to cope.*

As more entities adopt solutions from homegrown vendors, those vendors themselves become more attractive targets for threat actors, ranging from targeted nation-state operations to opportunistic, financially motivated groups. This raises the supply chain risk associated with these providers. Smaller and newer vendors may also lack the resources and capability to deal with these escalating threats, further compounding the risk.

Ransomware and Extortion in Europe

Despite a reduction in average ransom profits and increased joint law enforcement takedowns, the rate of extortion attack attempts is rising. Reporting indicates that in H1 2026, there were 104 active ransomware groups, 28 of which were newly emerged or rebranded.

Our scraping of victim listings on publicly available data leak sites shows that in H1 2026, 4,828 organisations were claimed as targets, an 18% increase from the previous year. European entities accounted for 24% of the total listed victims. Germany and the UK were the most-listed geographies, followed by France, Italy and Spain, which collectively accounted for 68% of the total European listings. The top targeted sectors were manufacturing, professional services, engineering, and retail, a pattern similar to that observed in previous reporting periods. Qilin and the Gentlemen dominated as key actors targeting the region, followed by Akira, Dragon Force and LockBit5. More generally, the list of top ten active ransomware groups has largely remained unchanged from 2025.

"Most visible CI/CD activity is financially motivated. However, politically motivated state-nexus threat actors have also begun exploiting these opportunities"

While the landscape remains a chaotic cluster of established actors alongside many new groups, differentiating key threats and their behaviours is vital to remaining defensively focused. As it stands, the actors operating within the ransomware landscape can be split into three tiers:

- **Top tier:** The prolific ransomware groups with established operations that utilise high technical proficiency, a pool of resources, and custom malware to conduct and offer affiliates access to traditional ransomware attack capabilities. Key groups in this category include Qilin, Akira, LockBit5 and Safepay, with new groups like The Gentlemen.

- **Secondary tier:** Divided between traditional ransomware groups with lesser skills than tier one, skilled extortion actors who leverage partial encryption techniques, and highly capable extortion-only groups that focus on large-scale data theft operations. These groups either leverage leaked malware variants as bases for their own, rely on Initial Access Brokers (IABs) and/or open-source tooling (e.g. AI) to boost capabilities and scale their attacks. Key groups at this tier include ShinyHunters, Scattered LAPSUS% Hunters, TeamPCP, KillSec, and Chaos.

- **Lower Tier:** Made up of actors/groups with the least capability, few available resources, who heavily rely on AI and pressure tactics to conduct their attacks which are beset by frequent operational security failures. This tier includes 0APT, APT73, CMD Organisation, and Exfilsquad.

The defining characteristic of the top and lower-tier groups is a preference for pure data-leak extortion tactics over double extortion (encryption combined with threats to publish exfiltrated information). Research indicates that 22% of ransomware incidents in 2026 involved no data encryption. Despite being in part due to a surge of new or rebranded ransomware/extortion groups, actors are also dropping encryption to prioritise attack speed, reduce operational expenditure, and lower the risk of EDR detection. Reporting also indicates that extortion-only attacks are enabling actors to counteract the general collapse in ransom payment rates, which recent reporting puts at 28% (i.e., barely a quarter of victims pay). Looking ahead, its likely more ransomware groups will adopt the practice of prioritising partial encryption or removing it from their playbooks completely.

In H1 2026, AI was leveraged in the ransomware landscape to create polymorphic malware, automate reconnaissance and execution, and accelerate data exfiltration by a factor of 100. In H2 2026, AI will continue to play a notable part in the upskilling of threat actors and scaling up of their attacks. Ransomware groups across all tiers of capability will leverage AI for various purposes across almost all stages of the attack lifecycle, notably increasing their attack sophistication and reducing dwell times.

NEW CHALLENGES

Managing the ransomware threat will increasingly mean monitoring a growing pool of actors and ransomware strains, while maintaining focus on the groups that remain the most credible threat to the organisation.

The defender's role will increasingly include deducing which breach claims are authentic and which are fabricated, as less capable actors seeking notoriety attempt to extort high-profile organisations without credible breach evidence.

In H2 2026, we may also see attackers mirroring the targeting patterns of successful operations from ShinyHunters and Scattered LAPSUS$ Hunters, for example the targeting of CI/CD and cloud supply pipelines. These groups could encourage a broader shift in targeting focus away from highly protected endpoints and towards valid accounts from Software-as-a-Solution external partners, open-source software and cloud-based services. As seen with the attacks by ShinyHunters, these could trigger broad impacts, affecting the data of tens to hundreds of organisations from a single compromise.

Lastly, it is likely that the expansion of players within the ransomware landscape will also include an expansion of the initial access brokers ecosystem, driven by an increased demand for prior compromise and AI-assisted access capabilities. However, a saturation of sellers operating in the cybercriminal market will likely drive down the average price of initial access to remain competitive. While credible sellers will lower their prices to encourage purchases, less capable actors, primarily seeking notoriety, will attempt to extort high-profile organisations without credible breach evidence. The role of the defender will increasingly include deducing which breach claims are authentic and which are fabricated.

In H2 2026, managing the ransomware threat will become increasingly about monitoring an increasing pool of actors and ransomware strains while maintaining focus on the groups that remain the most credible threat to their organisation. As seen in many areas of the threat landscape, AI will continue to facilitate attacks, increasing the baseline capabilities of many actors, and reducing barrier to entry for aspiring cyber criminals.

European Supply Chain Targeting

Increased threat actor activity against continuous integration and continuous development infrastructure (CI/CD) was a significant development in the threat landscape for H1 2026. Emergent campaigns in late 2025 preceded an intensive tempo of supply-chain compromise with widespread impact. Widely used software integrations for SAP, Axios, Bitwarden, and Trivy, were compromised during the reporting period, alongside less widely used packages such as Jscrambler. This heightened threat level is highly likely to persist in H2 2026.

Two main factors drive threat actors' recent focus on CI/CD infrastructure. First, organisations' implicit trust of external software enables a single successful supply chain compromise to impact multiple entities, which may include large or influential organisations. The March 2026 compromise of the Trivy vulnerability scanner is estimated to have compromised at least 1000 organisations. These organisations included the European Commission, which experienced a data breach as a result. Second, automated testing and deployment processes accelerate attacker operations and reduce opportunities for network defenders to prevent compromise.

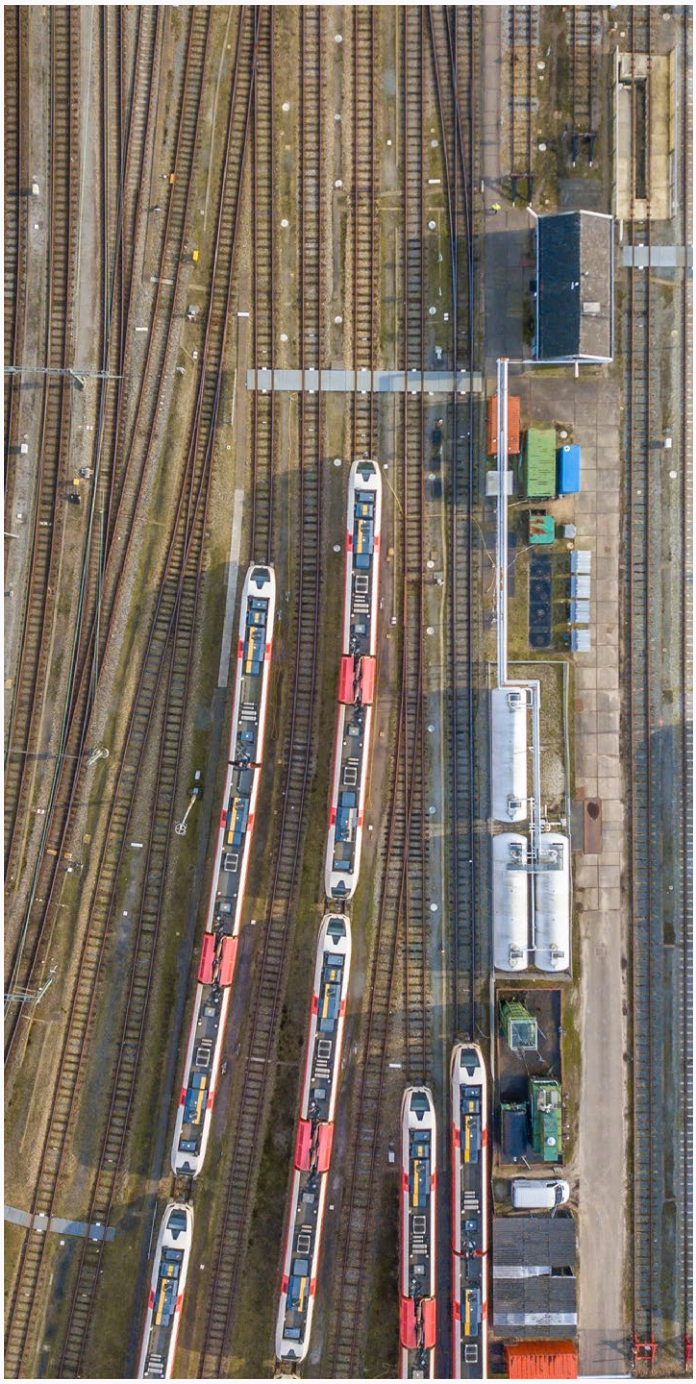
Most visible CI/CD activity is financially motivated. However, politically motivated state-nexus threat actors have also begun exploiting these opportunities. These operations are less typically more stealthy than financially motivated attacks which likely impacts detection and public reporting; however, this is expected to increase over the immediate to short term.

The threat to CI/CD infrastructure will almost certainly remain high into the medium and long term due to its role in AI development and deployment. Frameworks for AI and machine learning tools are frequently distributed through modular packages and trusted with broad access to developer's filesystems and networks. These tools therefore provide high-value targets for threat actors attempting supply chain compromise.

> ***"The threat to CI/CD infrastructure will almost certainly remain high into the medium and long term due to its role in AI development and deployment"***

It is assessed as likely that over the next reporting period, threat actors will refine their targeting in two ways, as follows.

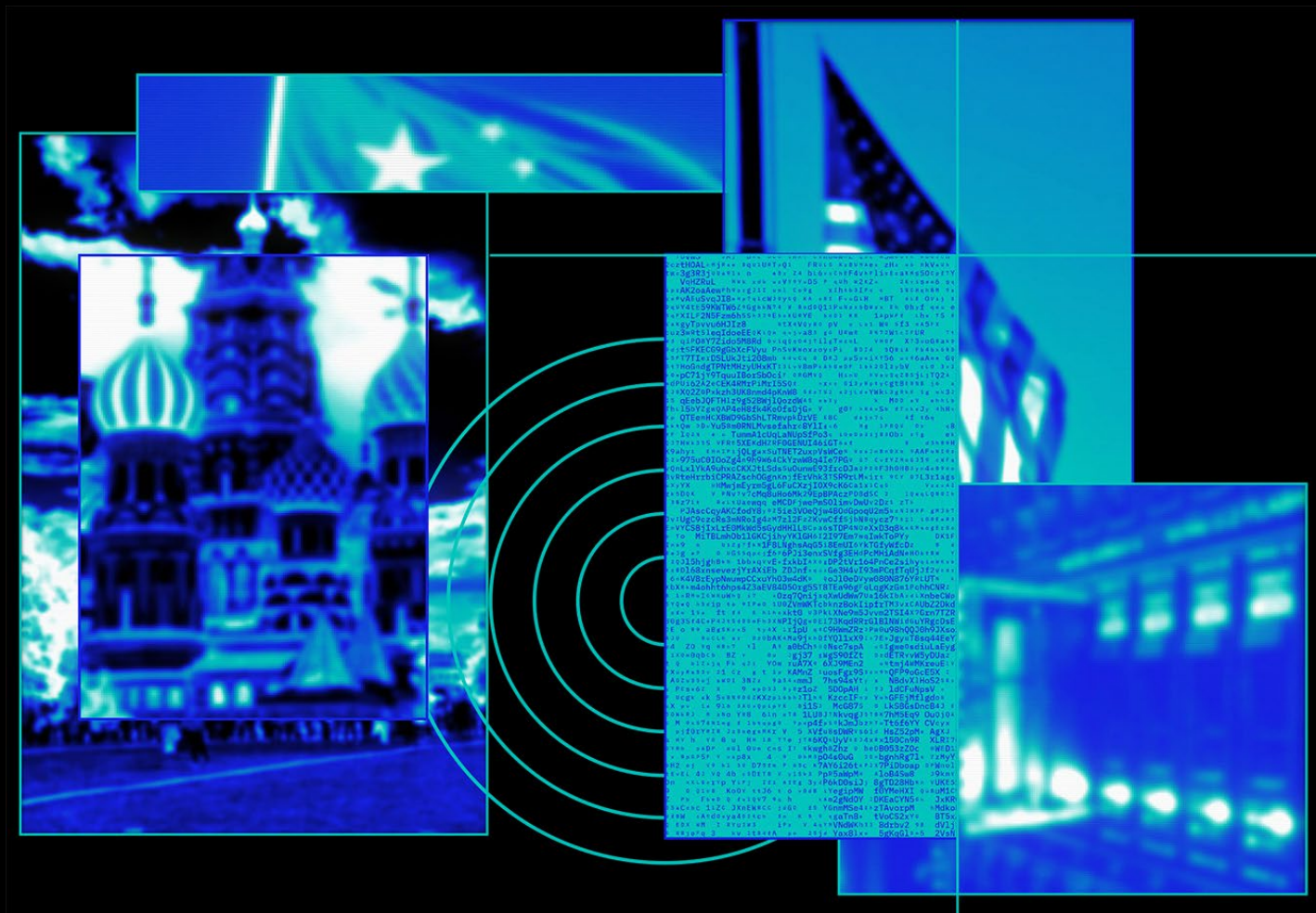
- Focussing their activity on a smaller number of high-value package, with the intent of preventing detection.
- Shifting their focus towards compromising the developers and maintainers of the CI/CD infrastructure, rather than exploiting vulnerabilities in repositories and package management infrastructure, as the security of this infrastructure is improved.



Aerial shot of train tracks.

FORECASTS

Forecasts	69
Artificial Intelligence	69
Digital Sovereignty	70
Cybercrime	70
Russia	71
China	71
United States	72

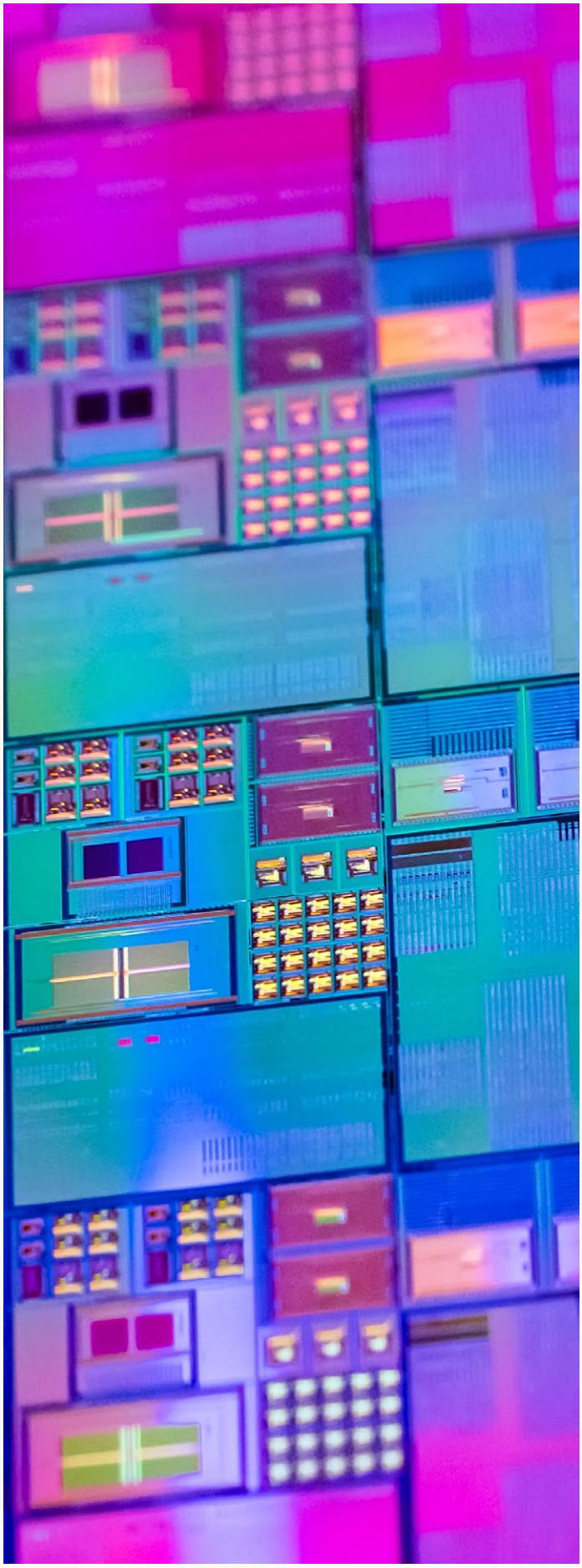


Forecasts

The abbreviation VUCA (Volatility, Uncertainty, Complexity and Ambiguity), gained currency in the post-cold war environment of the early 1990s to describe the emerging strategic environment. This abbreviation was largely replaced by BANI "Brittle, Anxious, Non-Linear and Incomprehensible" around the time of the coronavirus pandemic. More recently RUPT (Rapid, Unpredictable, Paradoxical, Tangled) and TUNA (Turbulent, Uncertain, Novel, Ambiguous) are gaining currency. Even if we choose to dismiss these terms as business buzz-words, a theme is apparent: we live in an increasingly unstable geopolitical environment, which significantly reduces our ability to make confident, long-term forecasts. The only entirely reliable prediction that we can make is that some of the forecasts outlined below will be wrong. However the following forecasts, based on the information in this report, represent our view of sensible planning assumptions.

Artificial Intelligence

- Patch volumes are almost certain to remain consistently high in the immediate term, and likely to remain high in the short term.
- The cost of effective exploits is likely to reduce significantly in the short term, increasing availability.
- The US is highly likely to mandate federal assessment and approval of proprietary frontier models and almost certain to implement federal control over overseas access to advanced proprietary models. China is also likely to take similar steps in relation to advanced open-weight models.
- A real-world, adaptive, LLM-driven computer worm spreading in a widespread attack is assessed as likely in the short-medium term.
- A multi-million dollar lawsuit resulting from an accidental LLM-driven intrusion is likely in the short term.
- Despite a rising probability over time, a global market correction due to overinflated technology stocks is assessed as unlikely in the immediate term.



Close-up of microchips after photolithography.

Digital Sovereignty

- Europe is almost certain to continue developing independent intelligence and security cooperation structures. These structures are almost certain to be a priority target for many hostile nation state intelligence services.

- New trade, defence and diplomatic initiatives between the EU and other nation-states or trading blocks are almost certain to be an increasing focus of foreign cyber-enabled espionage operations.

- There is an increasing likelihood that EU owned and controlled digital infrastructure (sovereign cloud, sovereign AI) will be subject to attacks on confidentiality to facilitate espionage operations. Attacks on integrity and availability are also increasingly likely, intended to highlight security issues and erode confidence in such solutions.

- European regulators will increase pressure on all economically significant entities to adopt 'sovereign solutions'. Defence and CNI related entities will be the initial focus, but technology companies, financial services providers and healthcare firms will also face pressure.

- The absence of an abundance of sovereign providers will almost certainly make mechanisms for ensuring 'operational sovereignty' whilst still making use of extra-jurisdictional suppliers a key priority, and a key regulatory concern.



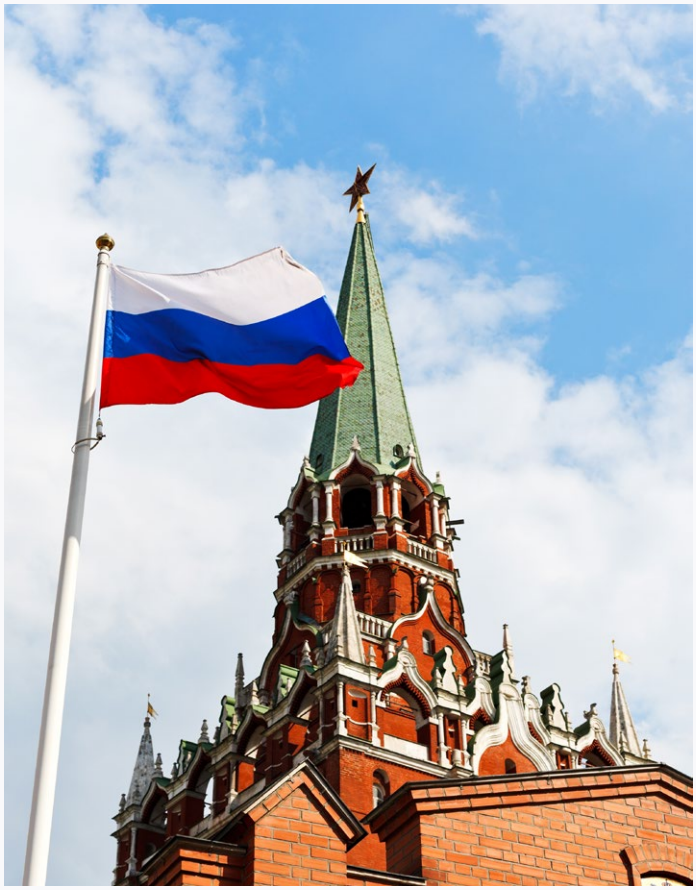
EU flag waving in the sky.

Cybercrime

- Phishing is expected to remain a primary collection mechanism, with continued reliance on trusted brands, cloud-hosted infrastructure, and lures designed to capture more than passwords alone. Attackers are likely to continue targeting session cookies, browser-stored secrets, MFA-related workflows, and account recovery paths. As a result, a growing share of compromises may resemble legitimate user activity, complicating detection and response.

- Infostealers and stolen credentials are expected to remain major drivers of enterprise intrusion. As stolen access data continues to circulate rapidly across criminal ecosystems, the time between initial theft and follow-on intrusion is likely to narrow further. Organisations should therefore anticipate faster progression from credential theft to remote access, post-exploitation activity, and broader business disruption.

- Ransomware is expected to remain concentrated in large economies and operationally significant sectors, particularly where identity compromise can be converted into wider enterprise access. While the actor mix may shift, the underlying operating model is unlikely to change materially. Stolen access, persistence, and lateral movement are expected to remain the most reliable path to high-impact outcomes.



Russian flag in front of a building.

Russia

- The threat of Russian grey-zone operations in Europe is likely to continue to increase in the short term, including cyber-enabled sabotage operations on CNI.

- The likelihood that the Putin regime will be deposed within the short term is increasing, but remains highly unlikely (10-20%). It the event that this occurs, is almost certain that Russian state sponsored offensive cyber operations, and Russian cyber-criminal operations targeting European nations, would continue unabated.

- The likelihood of a Russian battlefield collapse or 'rout' is increasing as a result of highly effective Ukrainian targeting of Russian supply lines, however such an outcome is assessed to be highly unlikely (10-20%) within the next two years. In such an event is highly likely that Western Europe would experience a significant increase in Russian offensive cyber activity, with widespread attempts at cyber-enabled sabotage, as well as other 'grey-zone' activities, including the targeting of CNI, potentially including sub-sea communications cables.

China

- Trade relations between the EU And China are highly likely to deteriorate in he short term, resulting in an increased cyber threat to European trade, foreign & finance ministries. The threat of Chinese cyber enabled sabotage operations is assessed to be a remote chance in the short term, however pre-placement activity to support future operations is highly likely.

- Chinese IP theft operations are almost certain to focus on advanced chip manufacturing processes, developments in AI, robotics, biotechnology and 'green technologies' in the short-medium term. IP concerning the practical methodologies underpinning high-end chip manufacturing are almost certain to be China's primary strategic intelligence requirement in relation to industrial espionage.

- A Chinese military invasion, or naval blockade of Taiwan is assessed as a remote chance in the short term.



China flag in front of Shanghai.



America flag behind barbed wire.

United States

- Any curtailment of security cooperation between the EU and the US is likely to remain confined to specific cases and thematic areas.
- Bilateral sharing on areas of convergent interest, such as transnational organised crime and state-nexus espionage activity, is almost certain to persist.
- The outcome of the November 2026 midterm elections is unlikely to significantly alter the direction of US foreign policy.

ASSESSMENT TERMINOLOGY

Time periods used in assessments of probability are almost always presented within the context of a time-frame. The precise meaning of the terminology used in this regard is provided in the table below:

Time Range	Definition
Immediate-term	<3 months
Short-term	3 months - 1 Year
Medium-term	1 year- 3 Years
Long-term	>3 years

The terminology used throughout the report when making an intelligence assessment is referred to as the 'Uncertainty Yardstick', a commonly used industry standard. Where this report contains terms of estimative probability, such as 'likely' or 'highly likely', the associated percentage probability is indicated in the table below:

Statement	Probability Range
Remote Chance	<5%
Highly Unlikely	10 - 20%
Improbable or Unlikely	25 - 35%
Realistic Possibility / Possible	40 - 50%
Probable or Likely	55-75%
Highly Probable / Likely	80-90%
Almost Certain	>95%

CSIS UPDATES

CSIS Security Group publishes its AI promise

Five principles now govern the application of AI across CSIS's cybersecurity work: human accountability, transparency, security, governance, and data residency. AI extends what analysts can do, but every output stays owned and verified by a person. Client data is stored and processed in Europe. Attackers are adopting AI quickly, and our AI Promise clearly sets out how CSIS uses the technology responsibly.

Pan-European incident response capability

CSIS is part of Allurity's pan-European incident response capability: a world-class team of case handlers, investigators and consultants that is able to take on the most sophisticated cases by leveraging a hybrid model that combines local presence and international talent. That's coverage no single national provider can build on its own.

Allurity OT Security Centre of Excellence

CSIS is now part of Allurity's operational technology (OT) Centre of Excellence. This group covers threat actor and attack intelligence for industrial systems, as well as strategy, design and implementation consultancy that addresses the requirements of companies that are looking to deliver a step-change in this critical domain.

Allurity: 830 people across 14 brands

Allurity now comprises 830 cybersecurity specialists, including 80+ in threat intelligence and 150+ in incident response, across 14 brands and 44 offices. That gives CSIS access to a larger network and additional capabilities, including offensive security, identity monitoring, OT security, and digital risk protection. Allurity is a European-owned group built to match the scale of the large global providers.

Copyright

This report is provided "as is" for informational purposes only. CSIS makes no representations or warranties, express or implied, regarding the accuracy, completeness, reliability, suitability, or availability of the information, products, services, or related graphics contained in this report for any purpose. All information in this report is subject to change without notice. CSIS reserves the right to make improvements and/or changes in the content of the report at any time without notice.

All third-party trademarks referenced by CSIS whether in logo form, name form or product form, or otherwise, remain the property of their respective holders, and use of these trademarks in no way indicates any relationship between CSIS and the holders of the trademarks.

Copyright 2026 © CSIS Security Group A/S.
All rights reserved.

www.csis.com

CSIS
REST ASSURED

ABOUT CSIS SECURITY GROUP

CSIS Security Group A/S is a leading European pure-play provider of tech-enabled cybersecurity and intelligence services. Operating 24/7, we deliver Managed Detection & Response, Incident Response, Security Consulting across all sectors, and provide a world-class threat intelligence capability through our SecAlliance brand. Accredited by organisations including CREST, we actively support global security initiatives to positively impact the cyber community.

CSIS IS IN THE ALLURITY FAMILY

Allurity is one of Europe's fastest-growing cybersecurity groups. Today, it is home to more than 800 cybersecurity specialists and some of the industry's most respected expertise across identity security, cyber defence, threat intelligence, offensive security and incident response.

Trusted by thousands of organisations, Allurity helps businesses and critical industries strengthen resilience, manage cyber risk and respond to an evolving threat landscape. With deep specialist capabilities and a strong European presence, Allurity is building the trusted cybersecurity partner for Europe.

CSIS Security Group A/S

info@csis.com
+45 88 13 60 30
www.csis.com

SecAlliance team

enquiries@secalliance.com
+44 (0) 20 7148 7475
www.secalliance.com