NOVEMBER 2025

REGIONAL THREAT REPORT
EUROPE

STEPHANIE SCHNEIDER

CYBER THREAT INTELLIGENCE ANALYST

MICHAEL KOSAK

SENIOR PRINCIPAL INTELLIGENCE ANALYST

REGIONAL SNAPSHOT

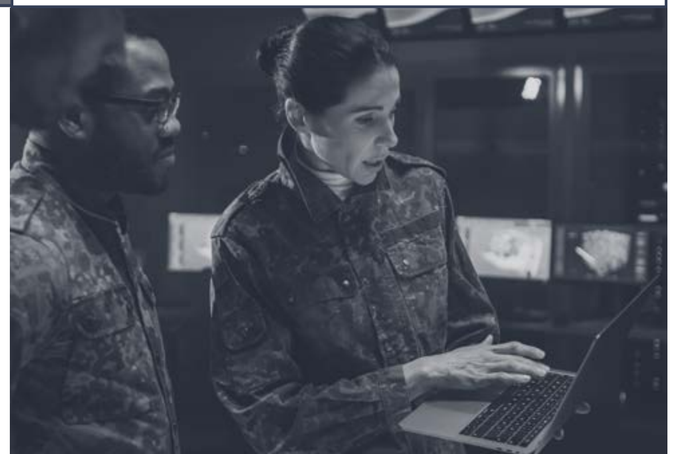
The overall trend in cybersecurity indicates a continuously challenging environment for European entities. Over the last quarter, Europe has faced aggressive cyber espionage, financially motivated ransomware, cryptominers, and infostealers, impacting governments, aerospace, industrial, critical infrastructure sectors, and more. Additionally, the United Kingdom (UK) saw a significant spike in nationally significant cyber attacks, with ransomware being a significant threat.

Europe faces an elevated level of supply chain attacks, including software supply chain attacks. The primary drivers for the recent surge in these attacks include the growing targeting of vulnerabilities, Software-as-a-Service (SaaS), and IT service providers, as well as cloud security and AI-based phishing campaigns. The Jaguar Land Rover (JLR) cyber attack illustrates how hackers can leverage vulnerabilities in supply chains with severe consequences. Additionally, the attack highlights Manufacturing as the most targeted sector by ransomware. Read on to identify ways to reduce your risk of supply chain compromise.

REGIONAL SNAPSHOT

Ransomware continues to be a core threat to entities in the region, with Europe becoming the second largest global target for ransomware and extortion. Big Game Hunting, or large-scale ransomware attacks, heavily targeted the UK, Germany, Italy, France, and Spain. Qilin has been the most active ransomware group in Europe this year to date. The most targeted sectors include Manufacturing, Legal & Professional Services, Construction & Engineering, Retail, and Technology.

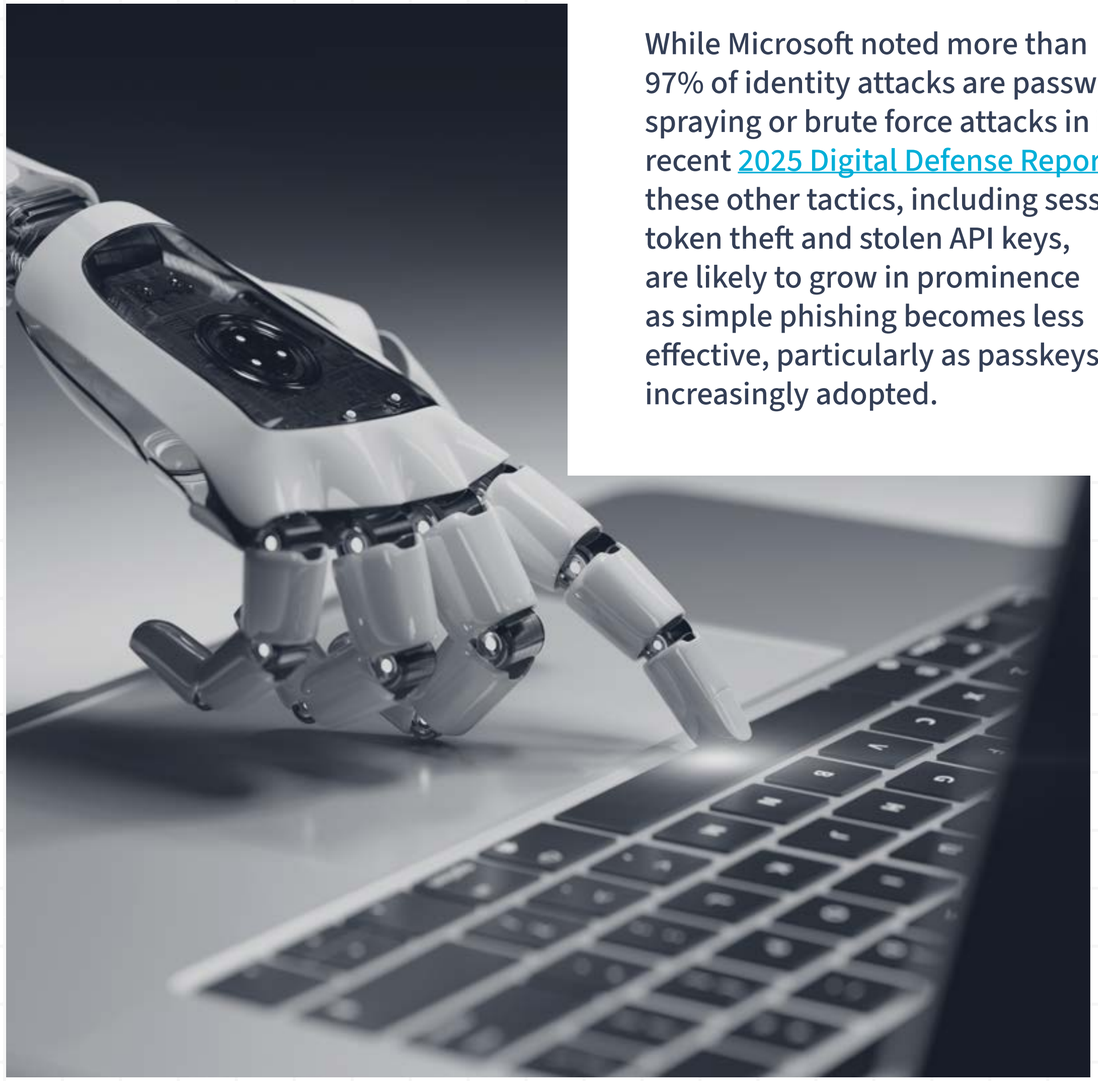
Nation-state groups have continued targeting Europe, and Russian-backed groups intensifying cyber espionage and destructive campaigns against Ukrainian targets but also across European government, military, energy, and telecommunications sectors. Hacktivism targeting the region continues to be fueled by kinetic conflicts, especially the ongoing war in Ukraine. Critical infrastructure remains a key focus for cybercriminals, nation-state hackers, and hacktivists.



IDENTITY THREATS ARE GROWING IN SCOPE AND SCALE

Identity threats have moved beyond simple phishing emails and credential theft as defenses have gotten more advanced and threat actors have grown more sophisticated, meaning that it's more important than ever for organizations and individuals to protect their identities. In addition to the well-established threats of phishing and infostealers, identity attacks also include session token theft, which allows for threat actors to bypass authentication, and one-time code (OTC) interception, in which a victim is tricked into sharing their OTC with a threat actor who can then leverage previously stolen credentials along with the OTC to login to an account.

Importantly, identities go beyond simply the human identities typically associated with access management (i.e., a specific human user and their corresponding credentials and MFA) to include non-human identities as well. These non-human entities include applications and services that access critical accounts and resources and are vulnerable to many of the same authentication attacks people are. These entities are the target of attacks seeking to steal passwords, API keys, and tokens and are of high value to attackers because they frequently have escalated privileges within connected environments.



While Microsoft noted more than 97% of identity attacks are password spraying or brute force attacks in its recent 2025 Digital Defense Report, these other tactics, including session token theft and stolen API keys, are likely to grow in prominence as simple phishing becomes less effective, particularly as passkeys are increasingly adopted.

SUPPLY CHAIN ATTACKS ON THE RISE

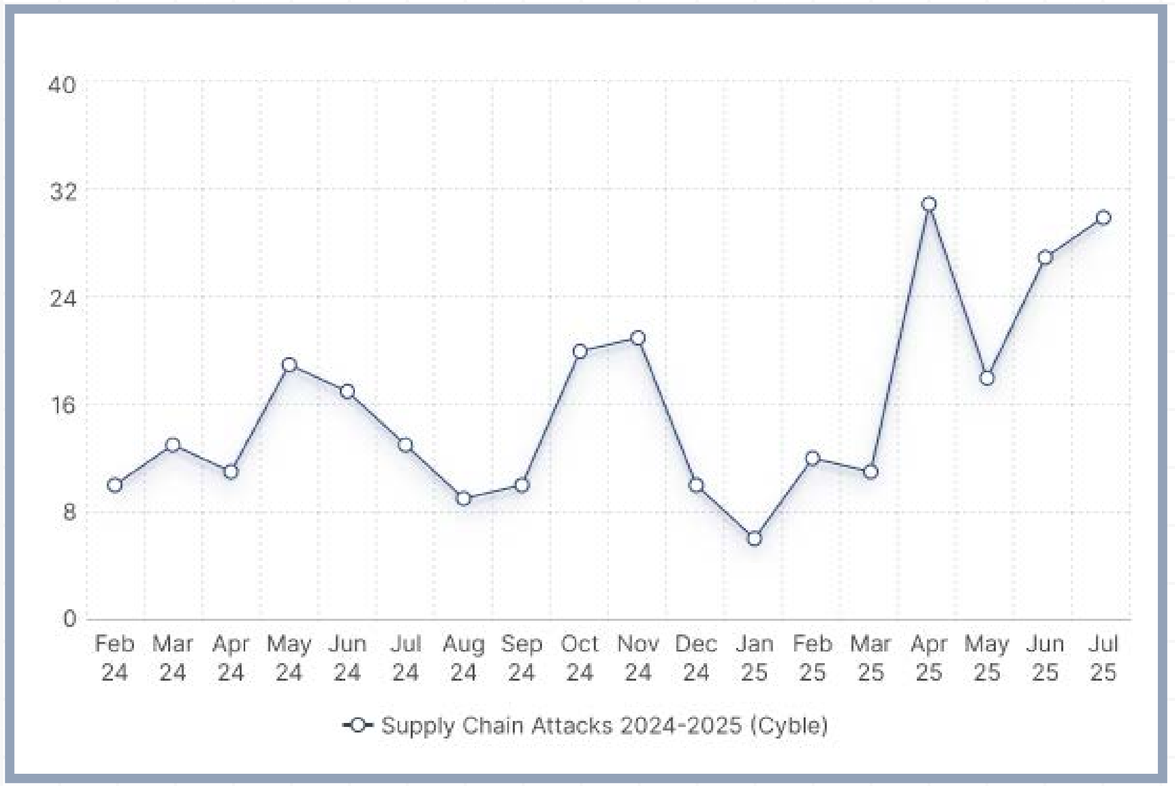
Supply chain attacks targeting the region are elevated, aligning with the global trend of increasing incidents. The EU Agency for Cybersecurity (ENISA) released its 2025 Threat Landscape report in October that found supply chain risks made up nearly 11% of cyber activities between July 2024 and June 2025. A combination of critical and zero-day IT vulnerabilities and threat actors targeting Software-as-a-Service (SaaS) and IT service providers are the primary drivers for the recent surge in supply chain attacks, as well as cloud security and AI-based phishing campaigns. The prevalence of ransomware as the most impactful threat in the EU further amplifies the risk posed by software supply chain vulnerabilities, as these often serve as initial access vectors for such attacks.

While digital infrastructure and services faced a high volume of data breaches, the manufacturing sector was consistently identified as the most targeted by supply chain attacks and ransomware in Europe throughout 2025, with significant interdependencies impacting related industries like automotive. In one case, Germany expressed heightened concerns regarding its critical material supply chain dependencies, particularly due to Beijing's implementation of export control measures, which posed risks to its automotive and military equipment industries.

Software supply chain attacks specifically are rising globally, reaching a new record globally in October 2025, and remaining an elevated threat to European entities. In the first five months of 2025, 27 incidents were recorded in European countries, with France experiencing the highest number at 10 attacks.

SPOTLIGHT ON SAAS-SPECIFIC VULNERABILITIES AND ATTACK VECTORS

The convergence of SaaS adoption and supply chain attacks present a complex challenge for global and European cybersecurity. SaaS applications have become a widespread, critical component of business operations; however, their widespread adoption has also introduced a significant and expanding attack surface for hackers to exploit. Hackers commonly exploit weaknesses in SaaS apps themselves as well as interconnected SaaS ecosystems to gain unauthorized access, steal data, compromise downstream customers, and deploy malware, including ransomware.



Recent incidents demonstrate the significant impacts supply chain attacks can have.

- **Transportation vendor:** A September cyber attack on Collins Aerospace, a third-party provider of check-in and boarding systems, impacted several European airports, including Brussels, Berlin, and Heathrow.

- **Salesforce third-party breach:** A widespread supply chain attack campaign in August, attributed to Scattered Lapsus$ Hunters impacted over 700 organizations, including French companies like Air France and subsidiaries of LVMH. Hackers exploited compromised OAuth tokens from Salesloft Drift to access Salesforce customer instances that had enabled the Drift-Salesloft integration in their Salesforce instances. Hackers exfiltrated data for extortion and searched for sensitive credentials such as AWS access keys, passwords, and Snowflake-related tokens.

- **Swedish IT services provider breach:** Milijodata, an IT services provider in Sweden suffered a data breach in late August. This ransomware attack exposed approximately 1.5 million individuals' personal data from multiple municipalities, regional authorities, and prominent companies, including Volvo, SAS, and GKN Aerospace.

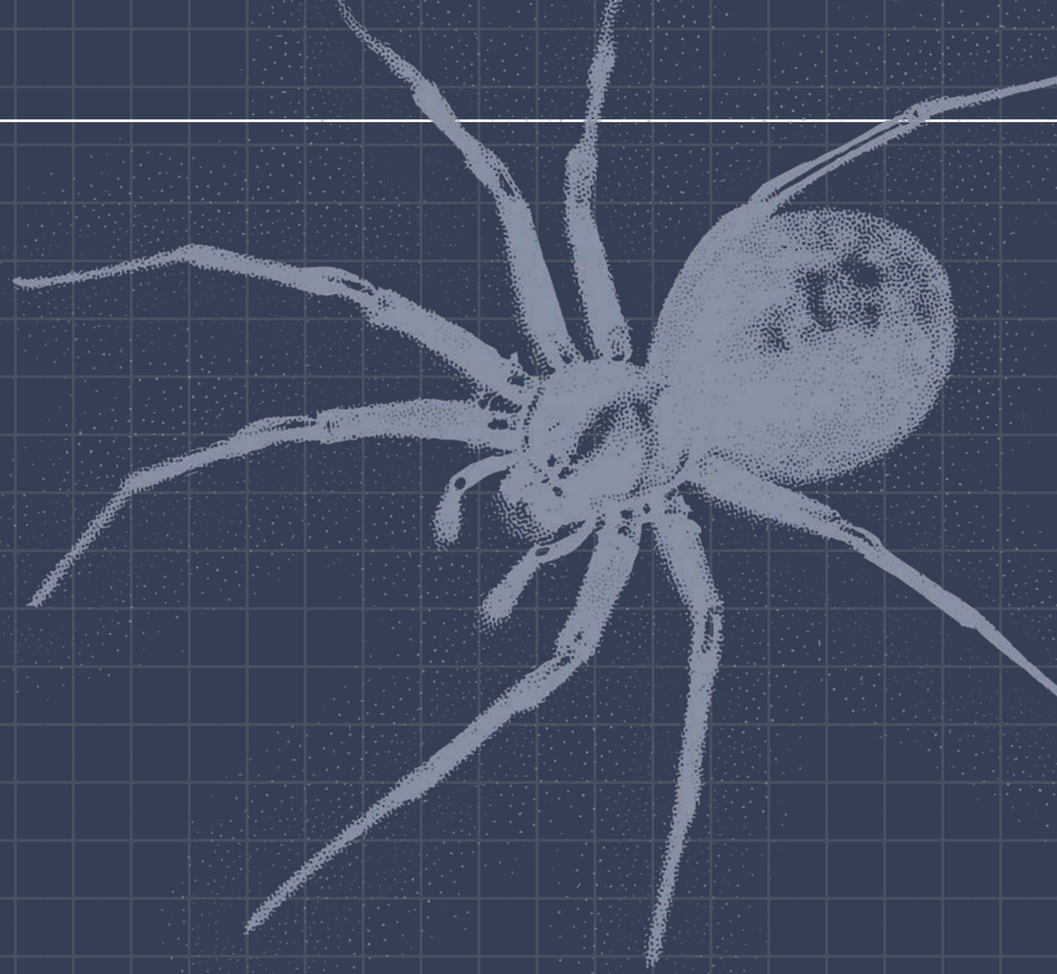
- **Nation-state hacker:** A suspected nation-state threat actor, tracked as CL-STA-1009, is distributing a new malware called "Airstalk" via the AirWatch mobile device management (MDM) application programming interface (API) in a likely supply chain attack. The malware can capture screenshots and exfiltrate browser cookies, history, and bookmarks from Google Chrome, Microsoft Edge, and the Island enterprise browser. Hackers' use of MDM APIs and targeting of enterprise browsers suggest a focus on the business process outsourcing (BPO) sector, where stolen session cookies could provide access to numerous clients.

SUSPECTED SCATTERED SPIDER MEMBERS ARRESTED IN UK

Two teenagers, Thalha Jubair and Owen Flowers, were arrested in the UK in August for their connection with the 2024 ransomware attack on Transport for London (TfL). Flowers has also been linked to cyber attacks on US healthcare companies, while Jubair was the focus of a US Department of Justice complaint that was unsealed at the time of the arrest charging him with conspiracy to commit computer fraud, wire fraud, and money laundering in connection to at least 120 network intrusions from May 2022 to September 2025.

Scattered Spider and similar groups (e.g., Shiny Hunters and Lapsus$) continue to pose a serious threat across sectors and industries. The constant evolution and proliferation of their tactics across a large community of cybercriminals ensures this activity will continue despite arrests.

SOURCE



PRO-RUSSIAN HACKTIVIST GROUP NONAME057(16) TARGETS GERMAN ORGANIZATIONS WITH DDOS ATTACKS

The pro-Russian hacktivist group NoName057(16) has been conducting a series of distributed denial of service (DDoS) attacks against defense and critical infrastructure entities in Germany, including German banks and municipal government websites. The group is conducting the attacks in protest to European support for Ukraine.

Russia has frequently leveraged support from hacktivist and cybercriminal groups to conduct cyber attacks in support of its foreign operations and policies.

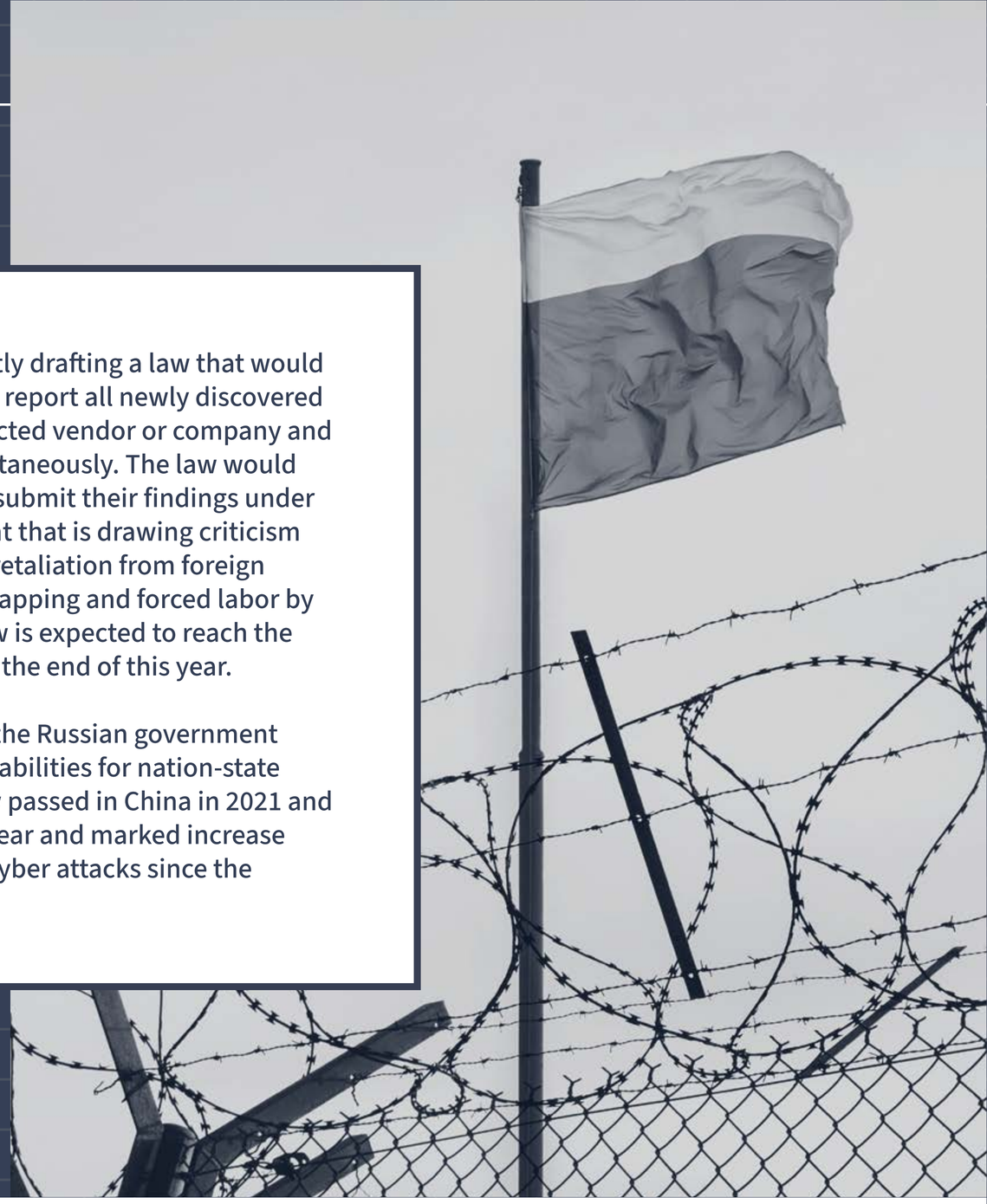
SOURCE

RUSSIA DRAFTING LAW THAT WOULD DIRECT VULNERABILITY REPORTING TO THE GOVERNMENT

Russian lawmakers are currently drafting a law that would require security researchers to report all newly discovered vulnerabilities to both the affected vendor or company and the Russian government simultaneously. The law would also require all researchers to submit their findings under their real names, a requirement that is drawing criticism for fear of potential arrests or retaliation from foreign governments or potential kidnapping and forced labor by criminal organizations. The law is expected to reach the Duma, Russia's parliament, by the end of this year.

The law would raise concerns the Russian government would weaponize these vulnerabilities for nation-state cyber operations. A similar law passed in China in 2021 and data since then has shown a clear and marked increase in China's use of zero-days in cyber attacks since the legislation went into effect.

SOURCE



RANSOMWARE ATTACK ON AEROSPACE COMPANY DISRUPTS EUROPEAN AIRPORTS

A ransomware attack on Collins Aerospace caused major disruptions at airports across Europe in September. Impacted airports included those in Berlin, Brussels, London, and Dublin, as the company is behind a widely used software that allows airlines to share check-in desks and boarding gates. The disruptions forced airlines to revert to paper records and disrupted the travel of thousands of passengers.

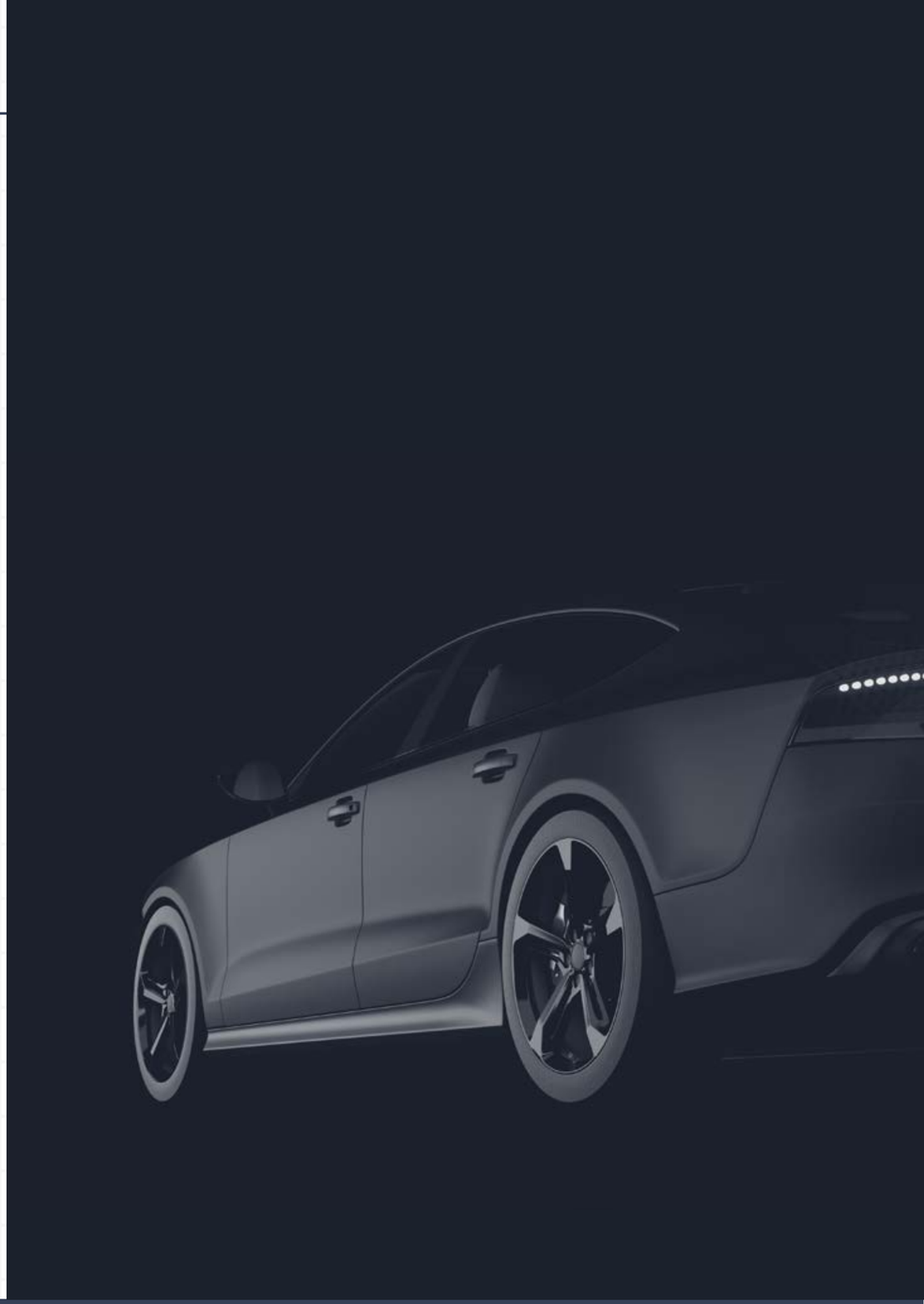
The impact of the ransomware attack underscores the vulnerability of the aviation and transportation sectors, both of which are part of critical infrastructure, to supply chain and ransomware attacks.

SOURCE

DEEP DIVE OF THE MONTH

JAGUAR

The cyber attack against Jaguar Land Rover (JLR) in late August was one of the most impactful supply chain attacks this year. This attack reportedly relied on the theft and exploitation of credentials, facilitated by infostealer malware and compounded by vulnerabilities related to legacy credentials and third-party access. The attack forced JLR to stop its global manufacturing operations into October and led to disruptions to the company's supply chain, affecting around 5,000 UK businesses, particularly small, owner-managed firms that faced cancelled or delayed orders and significant cash flow problems.



HOW THEY DID IT

01

Scattered Lapsus$ Hunters claimed credit for the attack and reportedly gained access via a social engineering campaign targeting a third-party IT helpdesk.

02

While details about the August attack on JLR remain limited at the time of reporting, credentials previously stolen by Hellcat infostealer were reportedly subsequently used, underscoring the enduring danger of exposed legacy credentials if left unaddressed.

03

The hackers used several techniques to bypass multi-factor authentication (MFA) and used “living off the land” (LotL) techniques to avoid detection, while establishing channels for persistence.

04

The hackers deployed credential extraction tools to harvest additional authentication credentials.

IMPACT

The attack is estimated to have cost the UK economy approximately £1.9 billion ($2.55 billion) and is reportedly the most economically damaging cyber event to hit the UK. Most of the impact comes from lost manufacturing output, causing an estimated 27% drop in UK car manufacturing in September 2025. Full recovery isn’t expected until 2026.

ADDITIONAL CONTEXT

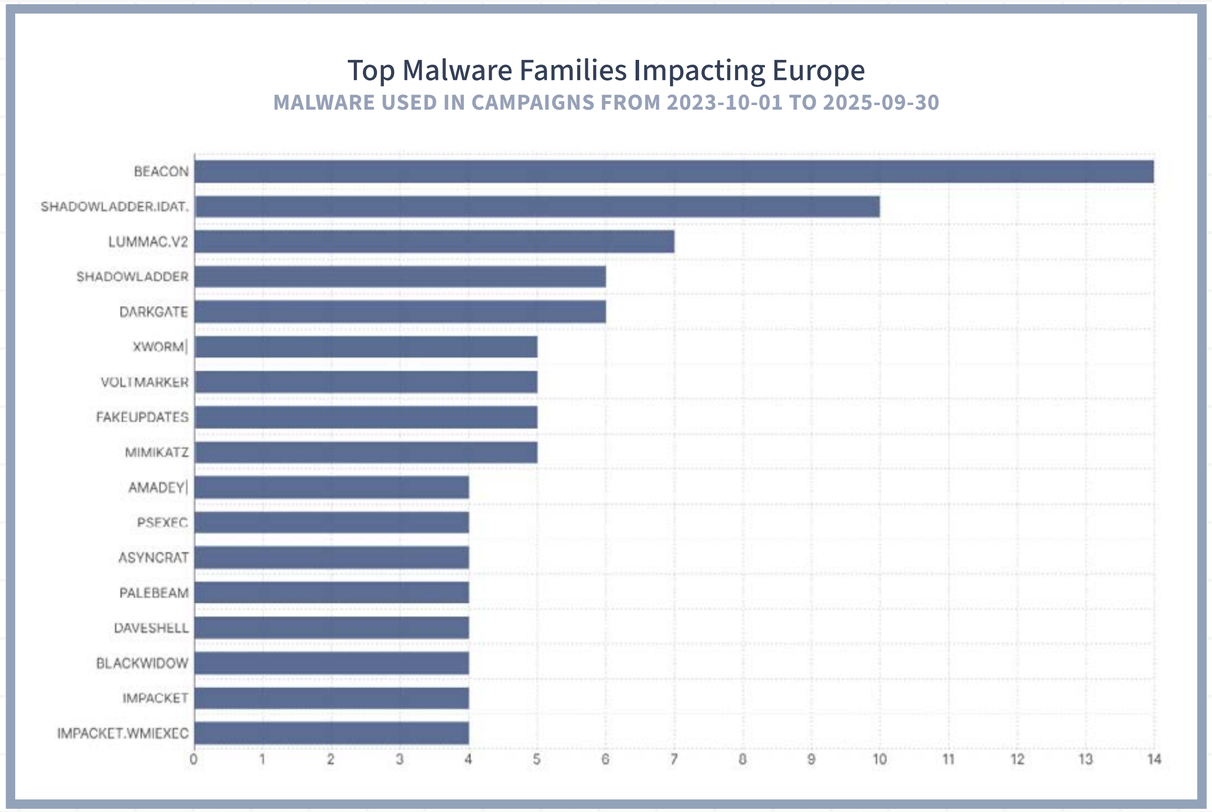
This was the second recent cyber incident for JLR in 2025. In March 2025, the Hellcat ransomware group claimed to have stolen hundreds of gigabytes of sensitive data from the carmaker by compromising Atlassian Jira project management software using infostealer-harvested Jira credentials. The compromised credentials reportedly belonged to an LG Electronics employee infected by an infostealer who had third party credentials to JLR’s Jira server. Another threat actor claimed to have exploited infostealer credentials that dated back to 2021, also belonging to an LG Electronic employee to exfiltrate additional data from JLR’s systems. These breaches show how the credentials infostealers harvest can remain valid for years, especially if companies fail to implement monitoring, MFA, or timely credential rotation.

TOP MALWARE FAMILIES TARGETING EUROPE

Over Q3 2025, malware campaigns in Europe continued to heavily focus on credential theft and identity persistence, as well as ransomware.

- The most common stealer variants impacting the region are Beacon, ShadowLadder.IDAT, Lumma, ShadowLadder, and DarkGate.
  - The publicly available Beacon backdoor allows attackers to maintain access and control over a compromised system.
  - ShaddowLadder/IDAT/HijackLoader and SmokeLoader are modular loaders that deliver payloads and evade detection.
  - Lumma was the most common infostealer malware family targeting Europe overall, indicating a concentration of malware campaigns targeting credential theft. Although Lumma's infrastructure was disrupted in May, variants persist.
  - Darkgate is a prominent malware family offered as a Malware-as-a-Service (MaaS). Darkgate was particularly active in Europe during August 2025, primarily used in credential theft campaigns and establishing persistence on compromised systems. Distribution methods for DarkGate have included platforms such as Microsoft Teams.

TOP MALWARE FAMILIES TARGETING EUROPE



Europe has become the second most targeted region for ransomware and extortion, making up approximately 22% of victims worldwide.

Additionally, ransomware was identified as the most impactful threat in the EU by ENISA's Threat Landscape Report 2025. Ransomware attacks across Europe were projected to exceed 1,746 by the end of 2025. So far, this number seems on track as ransomware attacks reached record levels across the region in Q3 2025 and surged 25% on a global level in October.

Big game hunting ransomware remains widespread, hitting high-value sectors across the U.K., Germany, Italy, France, and Spain. Qilin accounted for 15% of the total Q3 attack count, with 234 victims globally.

The increasing adoption of AI-enhanced phishing and social engineering, designed to facilitate ransomware deployment and other malicious activities, poses a significant threat.

Unsurprisingly, as some of the strongest economies in the region, the most targeted European countries by ransomware were Germany, UK, France, Italy, and Spain. These countries also have high internet usage rates, allowing ample opportunities for attacks.

GERMANY

Germany was consistently ranked among the European countries experiencing a high frequency of cyber attacks throughout the first half of 2025, a trend that has continued into the second half of the year so far. This sustained threat environment underscores the persistent vulnerability of German organizations to ransomware. Recent ransomware attacks in Germany significantly impacted critical infrastructure and government entities.

UNITED KINGDOM

According to the latest Annual Review by the UK's National Cyber Security Centre (NCSC), cyber threats facing the UK continue to escalate. The UK was a prime target for ransomware attacks, ranking second place in the region. These operations frequently involved data leaks, cryptomining software, and various backdoors. The NCSC dealt with 204 'nationally significant' cyber attacks against the UK in the 12 months to August 2025 (vs. 89 in the previous year). In Q3, Safepay and INC Ransom were the most active in the UK, followed closely by Qilin, according to Check Point. The most heavily targeted sectors were Legal & Professional Services (20%), Manufacturing (14%), Construction & Engineering (12%), and Financial Services (10%). However, no sector or organization is exempt from this threat.

FRANCE

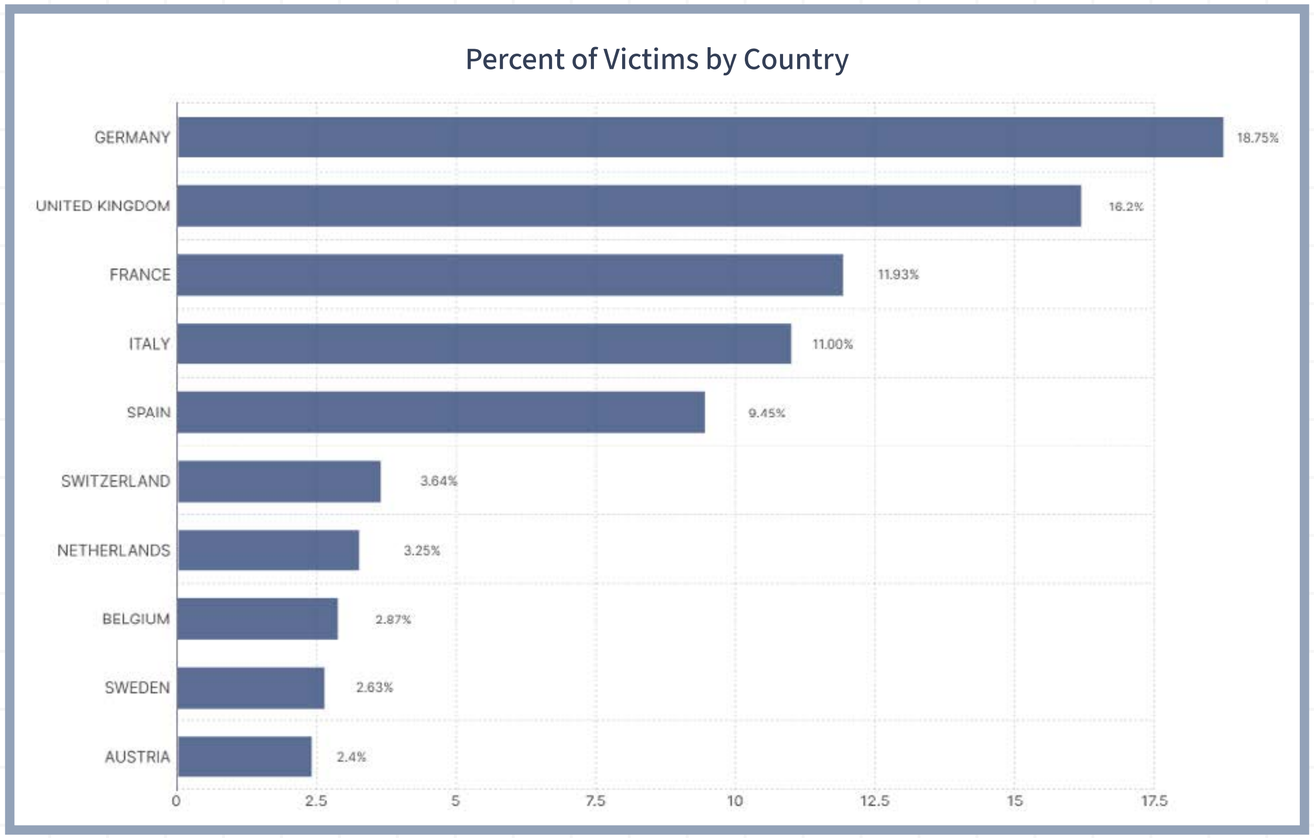
Ransomware remains a frequent, serious threat to French organizations. Qilin was by far the most active ransomware group targeting France and launched numerous attacks across various sectors. In October 2025, the Qilin ransomware group claimed responsibility for an attack and the theft of approximately 150 GB of data, including personal information of vehicle owners and internal documents. Qilin launched another significant on the Hauts-de-France region's high schools, impacting 80% of the region's high schools and stealing 1.1 TB of data.

ITALY

Italy is a significant target for cyber attacks, which have seen a substantial increase in 2025. Akira and Qilin were the most active groups targeting Italy, so far this year to October 31. Manufacturing (31%) and Legal & Professional Services (19%) were by far the most targeted industries in Italy. In early November, the Everest ransomware gang threatened to leak an alleged 159GB of stolen data from Italy's SIAD Group, a leading industrial gas company. Separately, the RansomHouse ransomware group claimed to have breached major Italian yarn manufacturer Fulgar S.p.A., which supplies major companies like Adidas, H&M, and Wolford.

SPAIN

Most of the top recently targeted companies in Spain were small to mid-sized, local businesses, or public institutions. Qilin and Akira were the top ransomware groups, while Manufacturing (21%), Legal & Professional Services (14%), and Retail (11%) were the most targeted industries, reflecting regional trends.

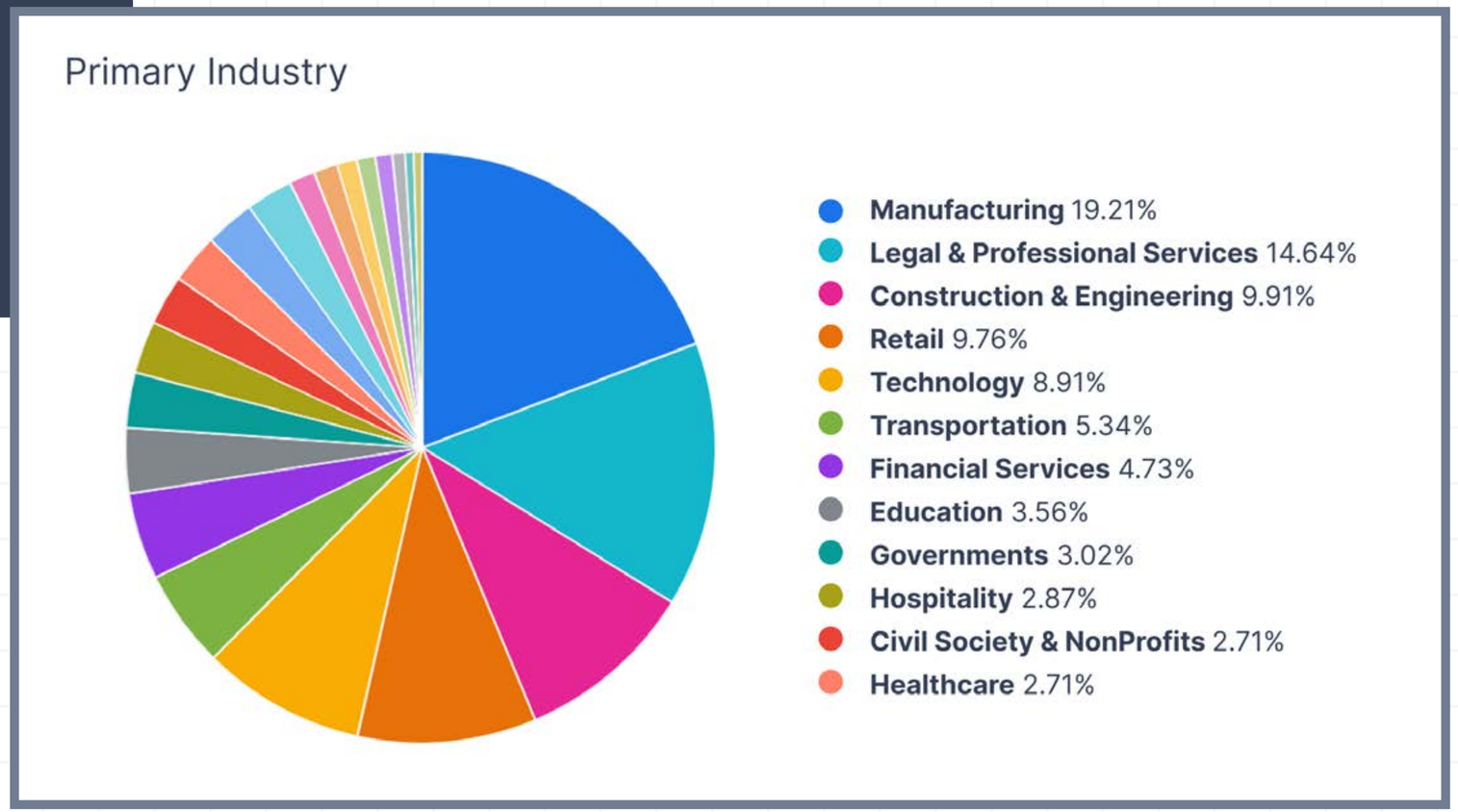


Top ransomware groups targeting Europe:

- Operating as a sophisticated Ransomware-as-a-Service (RaaS), Qilin accounted for a significant portion of ransomware attacks in Europe. Qilin was especially dominant throughout Q3 2025. Qilin continued its broad targeting of organizations across the region. One recent notable incident involved the compromise of the third-party service provider Collins Aerospace, which led to widespread disruption of airport systems across multiple European countries.
- **Akira** was the second most active ransomware group in the region, targeting various business and industrial sectors. The group deploys ransomware payloads compatible with both Windows and Linux operating systems, enabling them to impact a broad collection of enterprise environments and critical systems.
- **Safepay** showed a significant surge in activity in Q3 2025, employing double extortion tactics. Safepay focused on targeting critical, high-value sectors in Europe, including manufacturing, healthcare, IT services, and Operational Technology (OT) environments, including industrial control systems and programmable logic controllers within critical infrastructure. Safepay maintained a strong focus on Germany and the UK, with each accounting for approximately 10% of its total victims in Q3.

THE FIVE MOST TARGETED INDUSTRIES IN EUROPE WERE:

- Manufacturing (19%)
- Legal & Professional Services (15%)
- Construction & Engineering (10%)
- Retail (10%)
- Technology (9%)



The ransomware data analyzed in this report includes the following date range: Jan 1, 2025-Oct 31, 2025

Ransomware attacks against the manufacturing sector surged by 61% in 2025, making it the most targeted industry globally with some of the steepest growth compared to other industries. Manufacturing as the top targeted industry in Europe reflects this global trend. The attack against JLR that disrupted its global manufacturing operations was one of the most disruptive attacks this year to date.

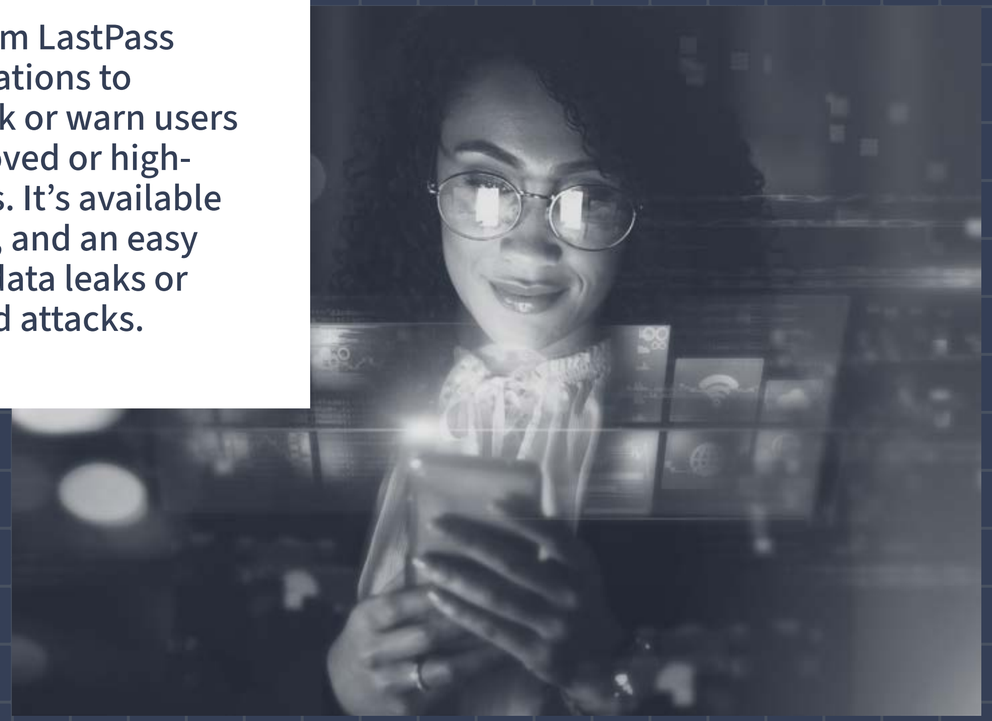
Cyberattacks targeting Retail exploit entities' volume of sensitive data, constant transactions of online purchases, and the high-stakes nature of retail operations where even brief disruptions can result in significant revenue losses and reputational damage. Looking at notable cyber attacks targeting the Retail sector in Europe, the UK retail sector suffered a series of sophisticated cyber attacks attributed to Scattered Spider starting in April before the group moved on to other sectors and regions.

REDUCE YOUR RISK OF SUPPLY CHAIN ATTACKS

Defending against software supply chain attacks can be challenging due to the relationship with partners and suppliers built on trust. Improving third-party security and reducing your risk of supply chain attacks requires a multi-prong approach.

- **Third party risk assessment:** Carefully vet partners and products in the initial acquisition phase and implement continuous monitoring on a recurring basis. Vendor assessments evaluate security risks, regulatory compliance, operational risks, financial stability, and business continuity. This process helps identify risks like data breaches, regulatory non-compliance, and operational standards.
- **Strong user identity and authentication:** Implement strong user identity and authentication by enforcing multi-factor authentication (MFA), requiring strong passwords, and using Identity and Access Management (IAM) solutions to manage user identities and enforce strict policies, for example.
- **SaaS monitoring and policy enforcement:** To protect against SaaS sprawl and Shadow IT (essentially unsanctioned technology), organizations need to know what users are accessing so they know what to protect.

SaaS Protect from LastPass enables organizations to proactively block or warn users against unapproved or high-risk applications. It's available in Business Max, and an easy way to present data leaks or credential-based attacks.



- **Zero trust framework:** A zero-trust approach to create specific security perimeters around individual applications and users. This limits the bast radius of an attack and prevents lateral movement across systems. For instance, if malware gets into one section, it's trapped and can't move to other parts. Zero-trust security also allows organizations to enforce the principle of least privilege for third-party vendors, granting them access to only the specific systems they need, no more and no less.
- **Proper configuration of API and cloud service connections:** This significantly enhances protection against supply chain attacks by establishing secure communication channels and controlling access to sensitive information.
- **Backups as a fall back:** Ensure your organization maintains ransomware-resistant backups that are unchangeable and isolated as much as possible.

WANT MORE?

Hooked on cybersecurity? Dive into The Phish Bowl podcast, where the LastPass TIME team's Stephanie Schneider and Mike Kosak cast a wide net on the latest on cyber threats, trends, and tales from the digital deep.

Bookmark the LastPass Labs blog for news on real-time threats, commentary on cybersecurity trends, and best practices to stay safe in the digital world.