Regional Threat Report: Europe

August 2025

Stephanie Schneider
Cyber Threat Intelligence Analyst

Michael Kosak
Senior Principal Intelligence Analyst

Regional snapshot

Europe has continued to experience a moderate threat level compared to other regions. According to IBM's X-Force 2025 Threat Intelligence Index, Europe is the third most targeted region after the Asia-Pacific and North America. Europe's strong economies, high internet penetration rate, involvement in the ongoing Russia-Ukraine and Israel-Gaza conflicts, and digital ecosystem vulnerabilities make it a particularly attractive target for hackers. Recent cyber threats in Europe included ransomware, malware targeting a wide range of industries, information operations, and data exfiltration for financial and espionage purposes. Additionally, hacktivist activity has remained elevated but stable.

EUROPE

23%

of incidents

Europe came in third place in terms of incidents investigated in 2024. They followed behind the Asia-Pacific region (34%) and nearly tied with North America (24%).[1] In Q2 2025, Europe experienced the highest year-over-year (YoY) growth in regional attack volume (22%).[2]

UNITED KINGDOM

25%

of incidents in Europe

The United Kingdom was the most targeted country in Europe in 2024, followed by Germany (18%) and Austria (14%).[1]

RANSOMWARE

2nd

most targeted region

Europe accounted for 25% of reported ransomware incidents, coming in second place after North America at 53% in Q2 2025.[2]

TOP SECTOR

38%

Professional, Biz & Consumer

Attackers primarily went after the Professional, Business, and Consumer Services sector. Attackers also targeted Finance and Insurance (18%), Manufacturing (18%), and others.[1]

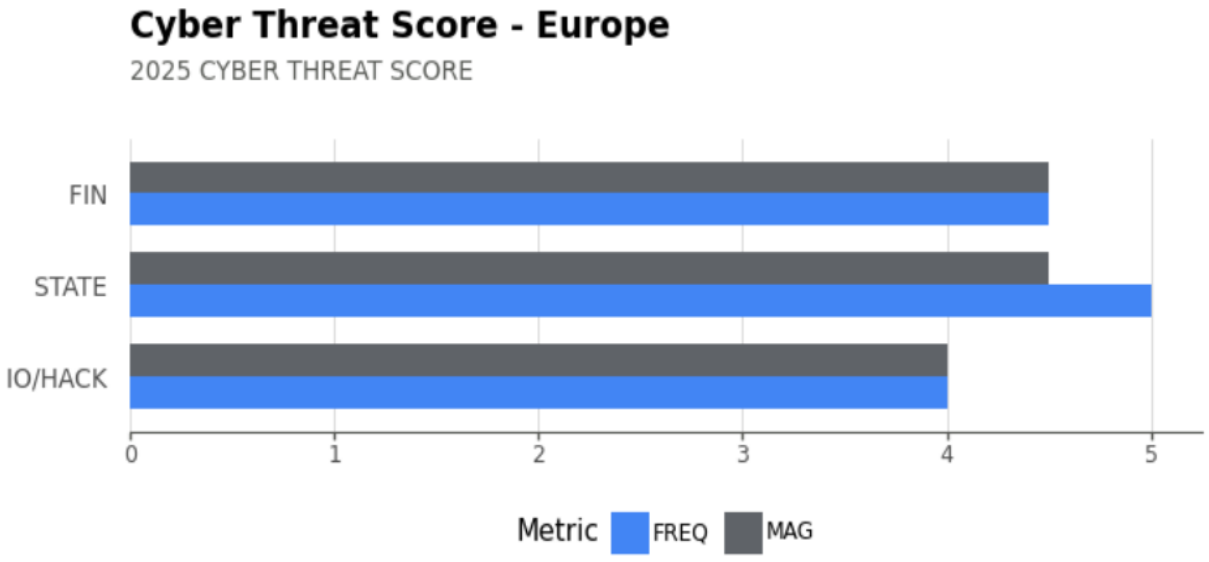
WEEEKLY ATTACKS

1,669

Average # of weekly attacks

The number of average weekly attacks per organization increased from 1,368 in 2024 to 1,669 in 2025.[2]

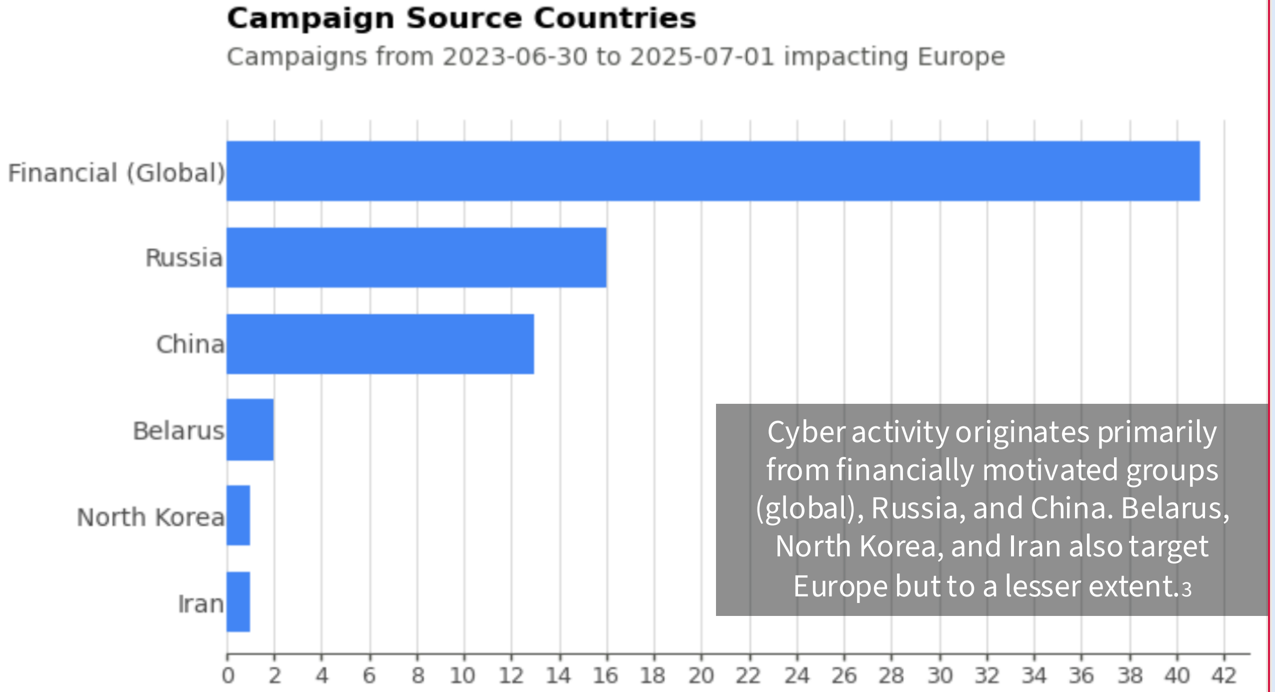
Threat landscape: Drivers of regional cyber threat activity



Cyber Threat Score - Europe

2025 CYBER THREAT SCORE

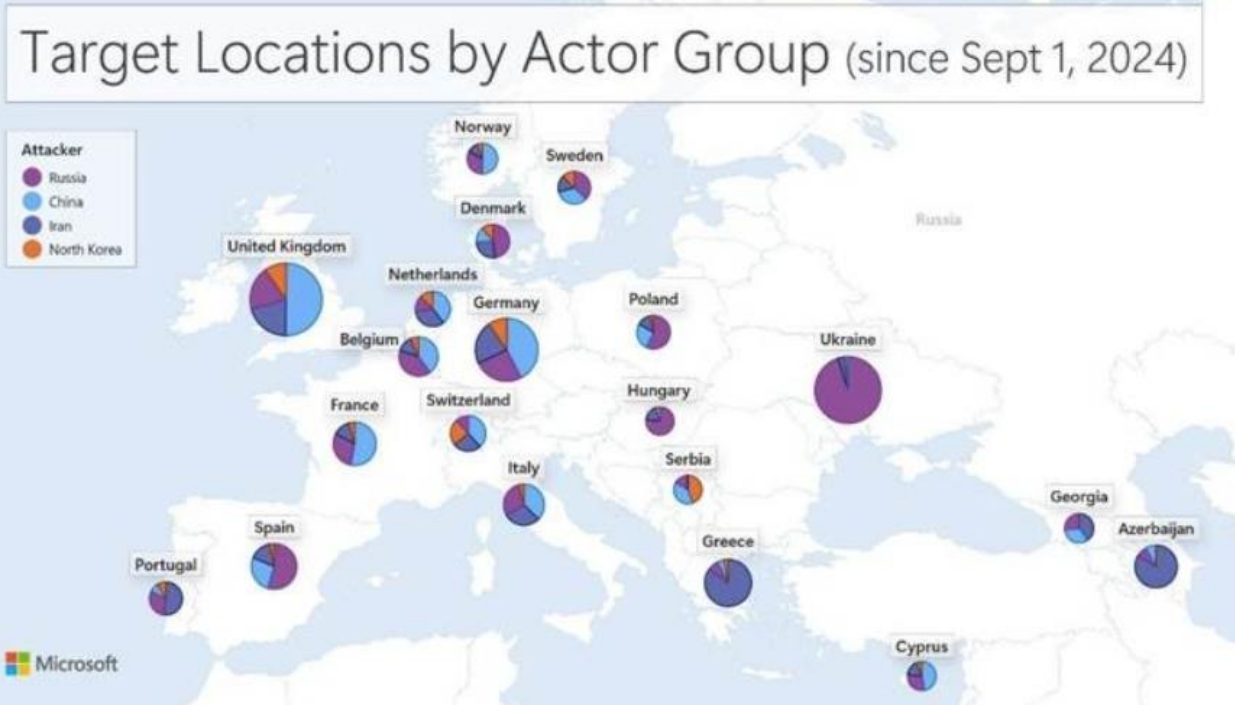
Europe Region Cyber Threat Score: 8.1 [3]



Campaign Source Countries

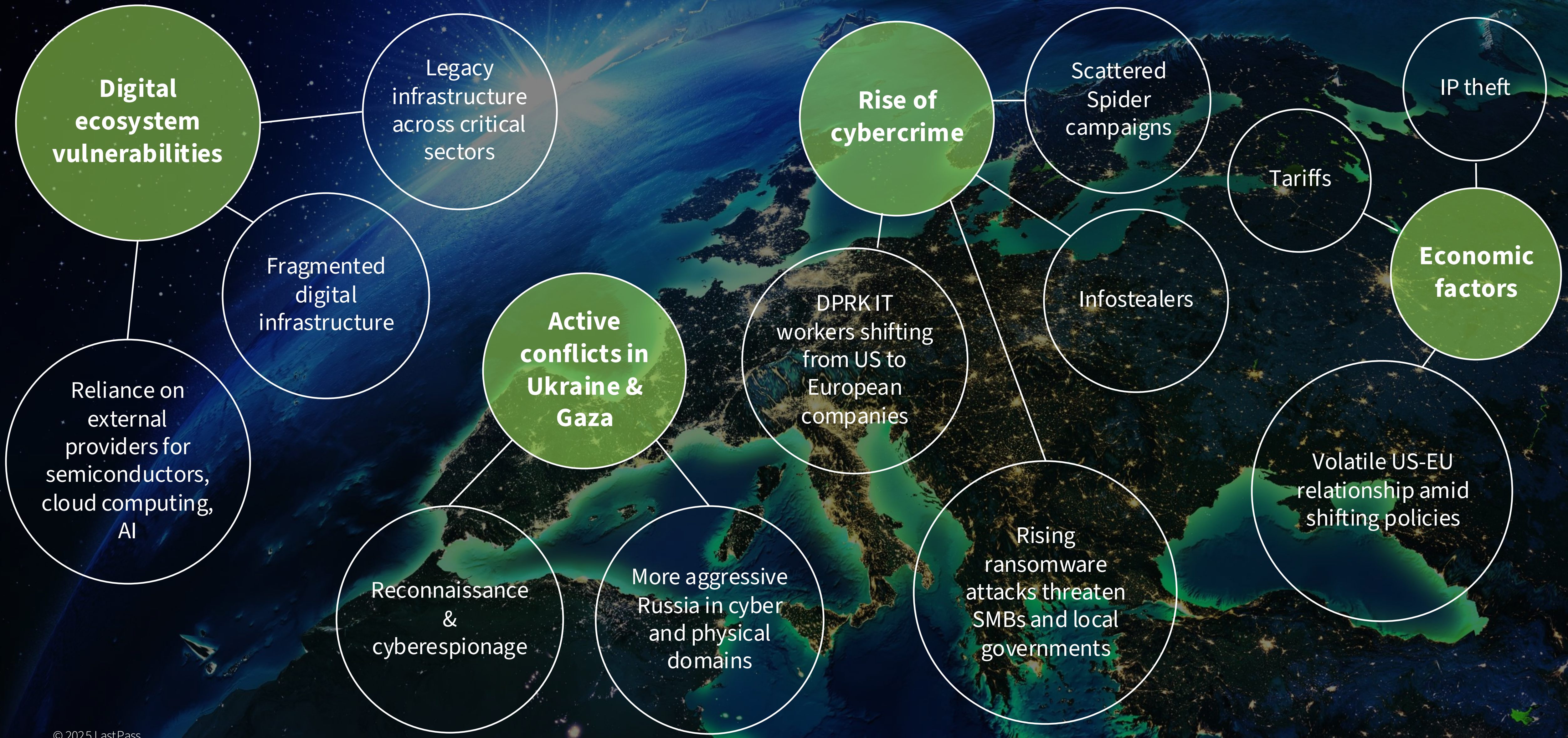
Campaigns from 2023-06-30 to 2025-07-01 impacting Europe

Cyber activity originates primarily from financially motivated groups (global), Russia, and China. Belarus, North Korea, and Iran also target Europe but to a lesser extent.[3]



Target Locations by Actor Group (since Sept 1, 2024)

Trends driving a heightened threat landscape



Digital ecosystem vulnerabilities

- Legacy infrastructure across critical sectors
- Fragmented digital infrastructure
- Reliance on external providers for semiconductors, cloud computing, AI

Active conflicts in Ukraine & Gaza

- Reconnaissance & cyberespionage
- More aggressive Russia in cyber and physical domains

Rise of cybercrime

- Scattered Spider campaigns
- DPRK IT workers shifting from US to European companies
- Infostealers
- Rising ransomware attacks threaten SMBs and local governments

Economic factors

- IP theft
- Tariffs
- Volatile US-EU relationship amid shifting policies

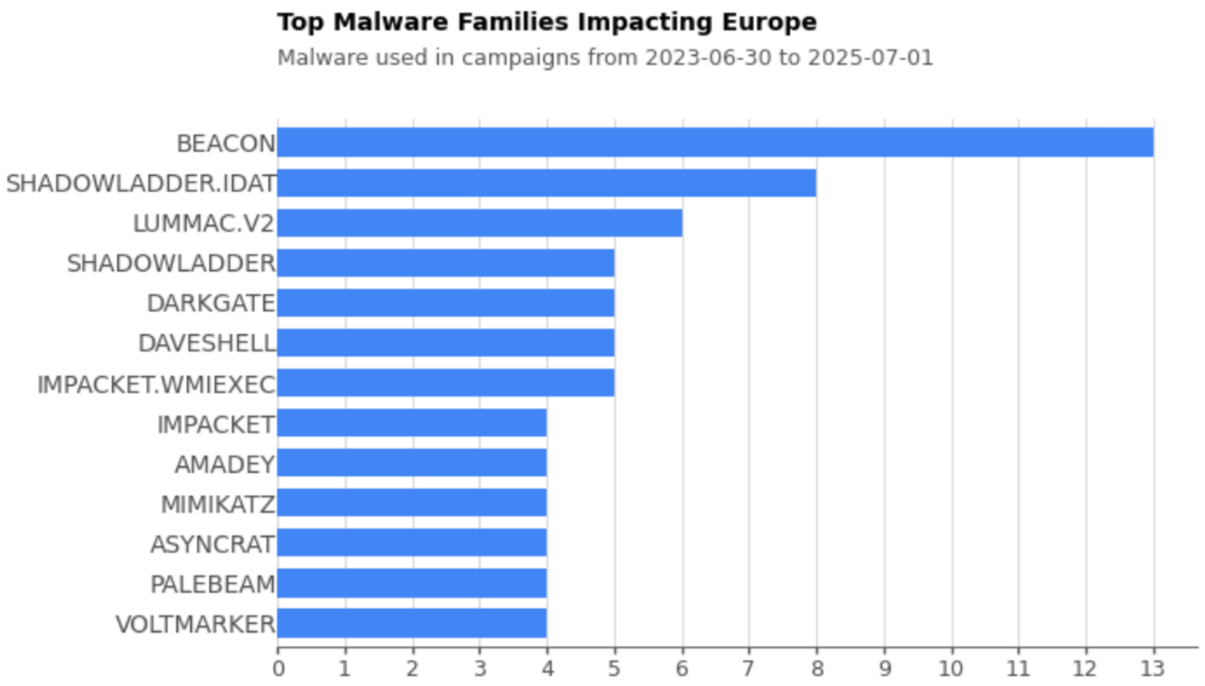
Top malware families targeting Europe

TRENDS & INSIGHTS

Malware campaigns target a wide range of sectors and are frequently delivered via phishing emails, cloud storage abuse like GitHub, mobile malware via social platforms, and more. Observed malware most frequently targeting Europe included Beacon (backdoor), Shadowladder.IDAT and Shadowladder (downloaders), Lummac.v2 (credential stealer), DarkGate (Malware-as-a-Service), Mimikatz (credential dumping tool), and various others. Malware used in campaigns targeting Europe commonly focused on credential theft and identity persistence.

- Many of the top malwares either directly steal credentials or facilitate delivery of tools that do. Mimikatz and Lummac.v2 target authentication data, while Beacon and DarkGate use session hijacking and keylogging.
- Shadowladder exemplifies the rise of stealthy loaders that deliver payloads like AsyncRAT.
- AsyncRAT and DarkGate combine remote control with credential harvesting. These tools are commonly used in ransomware staging or espionage operations.

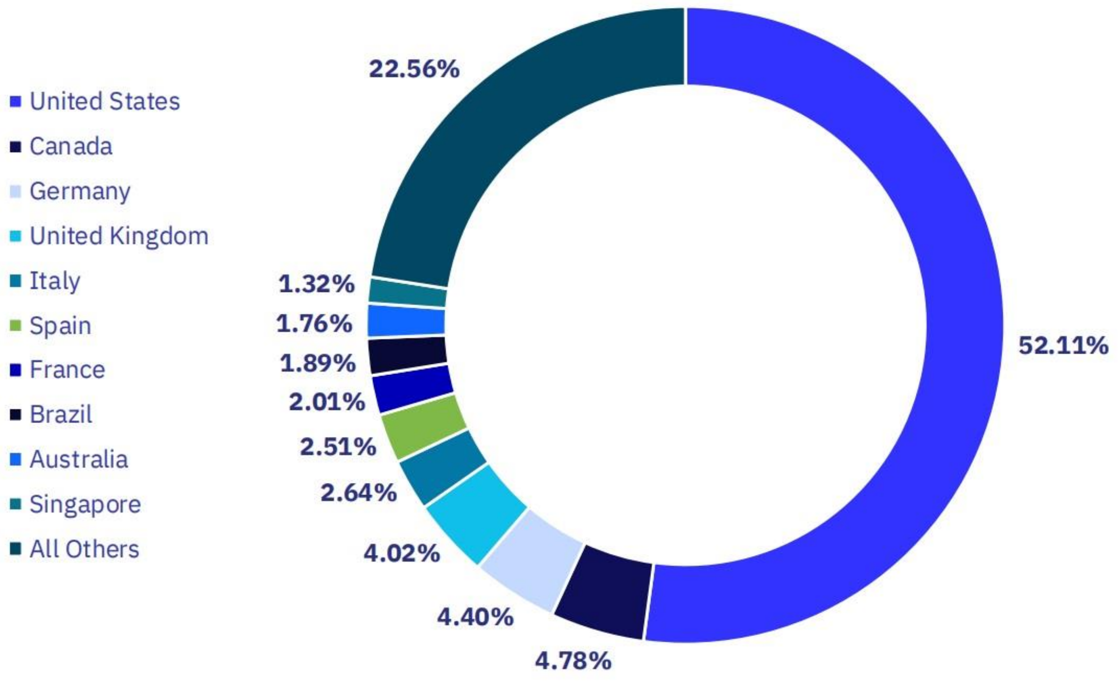
Top malware families
targeting Europe



Top Malware Families Impacting Europe

Malware used in campaigns from 2023-06-30 to 2025-07-01

(Source: Google Threat Intelligence)



(Source: Guidepoint Security)

Top malware families targeting Europe

RANSOMWARE

Europe was the second most targeted region globally in Q2 2025.2 Germany and the UK, in addition to Canada, are among second tier ransomware targets compared to the US (52%). Several other European countries are also significantly targeted by ransomware to a lesser extent. Recent notable ransomware activity targeting the region includes the following:

- BERT ransomware group emerged in April 2025 and targeted healthcare, technology, and event services in Europe, Asia, and the US. Their activity has expanded as they are actively developing and tweaking the software, such as upgrading encryption methods.[6]
- A ransomware attack on a European railway network in early 2025 halted operations for four days and led to economic losses exceeding €200 million.[7]
- The ToolShell SharePoint exploit chain has emerged as one of the most disruptive ransomware vectors targeting European businesses and government entities in 2025 to date. Western European governments, multinational corporations, and telecom firms in Europe were among the 148+ organizations compromised by Chinese-backed and cybercriminal hackers who exfiltrated data, stole cryptographic keys, and encrypted systems using the 4L4MD4R ransomware variant.[8]

Top threat actors targeting Europe

APT29

- APT29 is attributed to Russia's Foreign Intelligence Service (SVR). Their primary objective is espionage.
- APT29 frequently targets European and NATO members' government entities, research institutions, think tanks, and critical infrastructure. They have targeted commercial sectors in Europe, including financial, manufacturing, energy, and telecommunications entities.
- They use phishing campaigns to gain initial access and deploy custom malware loaders and backdoors to harvest data and establish persistent access.

Turla

- Turla is a stealthy espionage group attributed to Russia's Federal Security Service (FSB) targeting a wide range of victims, from government to military, education, and pharmaceutical companies.
- Known for conducting watering hole and spearphishing campaigns and using custom tools and malware, Turla can stay undetected for years in some cases.
- Turla was recently discovered intercepting Moscow-based foreign embassies' internet traffic through its control of domestic internet service providers (ISPs).[9]

Salt Typhoon & Flax Typhoon

- Both Chinese-backed groups prioritize stealth and persistence, making them difficult to detect and remove.
- Flax Typhoon focuses on long-term compromise to computer networks globally, with a focus on Taiwan. They focus on remote access and credential abuse.
- Salt Typhoon specializes in strategic espionage. They have breached telecoms providers, including those in Europe, to conduct espionage and potentially disrupt services.

Scattered Spider

- Active since 2022, Scattered Spider consists of a group of young operators in the UK, US, and Canada. They are known for their effective social engineering techniques to compromise a wide range of victims.
- Scattered Spider shares similar TTPs with other groups including Lapsus$, ShinyHunters, and The Com.
- In addition to targeted social engineering techniques, they've also attempted to bypass endpoint security tools and deployed ransomware for extortion.

Qilin

- This Ransomware-as-a-Service (RaaS) operation was the most active group in Q2 2025. Data leak disclosures doubled from February to April 2025.[10]
- Qilin uses double extortion tactics and offers tools and services to increase pressure on victims. Qilin introduced a distributed denial-of-service (DDoS) capability in April 2025.
- Qilin targeted healthcare and telecom sectors in the UK and Netherlands in H1 2025. Victims included hospitals and tech firms.

Key regional incidents

Arrest and disruption of XSS Forum.[15]

Ukrainian authorities arrested the suspected administrator of the Russian-speaking hacking forum XSS.is in July 2025. Active since 2013, the XSS forum was used to sell malware, access to compromised systems, advertise ransomware-as-a-service (RaaS) platforms, and discuss illegal activities. Law enforcement intercepted messages on the platform related to cybercrime and ransomware indicating they had generated at least $7 million dollars in profit.

Stolen data marketplaces drive a range of cybercrime. While this takedown will not disrupt the cybercriminal marketplace in the long term, it sends a strong warning. This takedown also follows recent law enforcement takedowns of other forums and cybercriminal infrastructure.

ShinyHunters leveraging voice phishing attacks to steal data from Salesforce customers.[11,12]

ShinyHunters conducted several data breaches against companies in Europe and globally, including a French multinational company and a German athletic apparel and footwear corporation. Hackers impersonated IT support staff over the phone to trick them into granting access to cloud-based Salesforce databases. This allowed data exfiltration from Salesforce and lateral movement to other systems (Okta, Microsoft 365, etc.). ShinyHunters also launched a data leak site, escalating their extortion tactics by applying added pressure to victims to pay ransoms.

Customer-facing frontline support personnel are attractive targets because these individuals possess the access and knowledge threat actors can exploit.

Aeroflot systems succumb to hacktivist cyberattack.[13]

Russian airline Aeroflot suffered a cyberattack in July 2025 claimed by Ukrainian and Belarusian hacktivist collectives Silent Crow and Cyberpartisans BY. The hackers claimed to have had access to Aeroflot's IT infrastructure for over a year and "destroyed" valuable resources. The attack resulted in 60 flights being delayed and additional flights were severely delayed.

Cyberattacks targeting the various Russian industries have continued as part of the ongoing Russia-Ukraine conflict.

Russia targeting foreign embassies via adversary-in-the-middle attacks.[9]

Russia-backed Turla (aka Venomous Bear, Secret Blizzard) is targeting Moscow-based embassies with their custom ApolloShadow malware in an ongoing cyberespionage campaign since at least 2024. Turla is using their adversary-in-the-middle position at the ISP/telecommunications level to lawfully intercept devices. The campaign includes fake cybersecurity certificates that effectively unencrypt the target's browsing, including the delivery of certain tokens and credentials.

This demonstrates how Russia can use its controlled information environment, like its domestic intercept systems (System for Operative Investigative Activities (SORM), to collect intelligence.

France's Naval Group suffers 1TB data leak.[14]

French defense contractor Naval Group was extorted for 1 TB of data, including what appears to be classified information for military vessels, technical documents, and more. The data was published after failing to reach a negotiation agreement. At the time of reporting, Naval Group denied the breach, and investigations are ongoing to determine if this leaked data is new or recycled from a previous breach.

Defense contractors are frequently targeted by cyberespionage and financially motivated operations. They can be easier targets than government entities to gain access to sensitive information.

Deep dive of the month

Scattered Spider targets UK retailers prior to arrest

Summary

Scattered Spider has been actively targeting organizations in Europe, especially the UK. In April 2025, Scattered Spider conducted social engineering attacks to deploy DragonForce ransomware against several major British retail companies, which reportedly cost an estimated £440 million.[16] They pivoted to US retailers next, and then the insurance and aviation industries. Scattered Spider frequently uses social engineering techniques to obtain credentials, install remote access tools, and/or bypass multi-factor authentication (MFA). They know how to circumvent modern security tools and opportunistically target a wide range of sectors. Four individuals in the UK—aged between 17 and 20—were arrested in July 2025 in connection with the attacks.

How did it happen?

- Scattered Spider commonly gains initial network access through interactive social engineering of IT help desk employees leading to ransomware deployment and/or data theft extortion. They're known for using a range of techniques in their attacks, including phishing, push bombing, SIM swapping, ransomware, adversary-in-the-middle attacks, and abusing text messaging services.
- Scattered Spider continues to adapt their techniques. Recent incidents attributed to the group have revealed the use of more sophisticated social engineering and the deployment of new malware families, such as the DragonForce ransomware.[17]
- They gained access to M&S systems by using the login credentials of two employees from its third-party IT vendor and business partner, Tata Consultancy Services, which is also Co-op's contracted IT vendor.[18]

How can you protect yourself?

- Effective defense tactics to counter threats like Scattered Spider should consider both technical systems and human behavior. Humans are the weakest link, which social engineering attacks seek to exploit, so educating employees to recognize and detect social engineering attempts is crucial. Traditional controls like patching and segmentation are fundamental, plus good identity access controls, like phishing-resistant MFA across all user accounts.
- TIME analysts highly recommend reading the Scattered Spider joint advisory, as well as UK's National Cyber Security Centre's (NCSC) blog post with recommendations.[17, 19]
- These sources provide a list of Scattered Spider tactics, techniques, and procedures (TTPs), recent developments in their activity, mitigation recommendations, and threat hunting guidance.

Trends on tap

Critical Infrastructure (CI)

A combination of heightened geopolitical tensions and rampant ransomware activity have contributed to an elevated level of cyberattacks targeting European CI. In August 2025, the UK's NCSC warned that the risk posed by hackers to the country's critical infrastructure is escalating especially against energy, healthcare, and transport, and published an updated version of its Cyber Assessment Framework.[20]

Nation-state groups, sometimes collaborating with hacktivists, have conducted cyber operations against CI as a direct extension of the ongoing Russia-Ukraine conflict. Recent Russian-backed operations have focused on disruption and espionage against European governments and CI entities, especially NATO member countries. Chinese-backed hackers are increasingly targeting European CI, including the finance and manufacturing sectors. Chinese hackers have shifted from commercial espionage to gain a competitive economic edge to deep infrastructure infiltration such as telecommunication networks.

Ransomware poses a threat to European CI entities, in particular Germany and the UK, likely due to their relatively strong economies and roles as commercial hubs. Ransomware attacks combined with data theft extortion have recently targeted European entities in the UK, Germany, Italy, France, and Spain in particular. Top targeted industries include CI and primarily include manufacturing, finance and insurance; professional, business, and consumer services; and healthcare.

Trends on tap

Credential theft enables a range of malicious activities

Credential harvesting has been observed in campaigns targeting European entities, mirroring a widespread trend. Hackers are targeting this data to enable follow-on activities, from monetizing stolen credentials on the dark web, to data breaches and more. Unauthorized access is harder to detect when hackers can simply log in as opposed to having to exploit vulnerabilities. Widely available tools like infostealer malware make this tactic even easier to succeed. Some recent examples include:

- The UK government linked Russia's GRU military intelligence agency-affiliated APT28 to the "Authentic Antics" cyber campaign, which used custom credential-stealing malware to target politicians, journalists, and public figures in the UK and beyond.[23]
- A suspected Russian espionage cluster, tracked as UNC6139, conducted a long-term credential harvesting campaign against European government and defense entities using NATO-themed lures.[3]
- Scania, a Swedish manufacturer of commercial vehicles, had their insurance claims portal breached in late May 2025 using stolen third-party credentials, resulting in the theft and the dark web sale of thousands of claim documents by an extortionist calling themselves “hensi.”[24]

Trends on tap

Ransomware shifts to data exfiltration focus

Ransomware remains a significant threat in Europe and globally, often involving double or triple extortion tactics to increase pressure on victims to pay. Ransomware actors have added coercive tactics to increase pressure on victims to pay ransoms, such as data exfiltration. This tactic significantly affects the EU’s General Data Protection Regulation (GDPR) compliance for entities operating in Europe. Beyond financial penalties (reaching up to €20 million or 4% of a company's global annual turnover) for failing to protect users’ data, entities can face reputational damage, operational disruptions, and potential legal action. Attackers may leverage the threat of public disclosure to extort higher ransom payments from victims seeking to avoid these fines. Some hacker groups explicitly warn victims that failure to pay the ransom will result in triggering GDPR penalties that could exceed the ransom demand. These actors often set ransom demands lower than the potential GDPR fines, making the payment seem like the cheaper option.

To curb ransomware payments that fuel cybercriminals’ business model, all 50 member countries of the International Counter Ransomware Initiative (including 48 countries, the EU, and Interpol) pledged to not pay ransomware demands; however, this is not a mandated ban.[21] Additionally, the UK government plans to ban ransomware payments for public sector bodies and critical national infrastructure.[22]

Trends on tap

ClickFix usage

Both financially motivated and state-backed groups have increasingly used ClickFix against organizations in various sectors across Europe and globally since 2024. ClickFix is a relatively new social engineering technique where users are tricked into executing seemingly harmless, everyday actions that are disguised as malicious commands. It’s an effective method to bypass phishing and other traditional defensive measures by exploiting social engineering and living-off-the-land binaries (LoLBins), making it harder to defend against. While threat actors are still experimenting with this technique, its adoption has increased by over 500% between H2 2024 and H1 2025.[25]

These attacks often use lures like fake CAPTCHA verification or software updates and instruct users to copy and paste malicious code into their system’s command prompt. They can ultimately lead to malware/ransomware deployment or credential theft to gain further access to systems. This attack method is being sold as a ready to use module in underground forums, expanding its use. The ClickFix technique will likely continue to gain traction among cybercriminals and nation-state hackers to conduct a wide range of threat activity.

What can you do?

With the constant threat from malicious cyber actors and a dynamic geopolitical environment, what steps can you and your organization take to protect yourself? Here's some advice, drawn largely from the UK's National Cyber Security Centre's (NCSC) Cyber Assessment Framework 4.0.[20] The framework addresses how to evaluate and strengthen organizations' governance, risk management, supply chains, identity and access control, data and system security, and more.

IDENTITY CENTRIC APPROACH

Comprehensively verify, authenticate, and authorize access to network and information systems. These three identity-centric controls establish trust, validate access, and limit exposure.

DEVICE MANAGEMENT

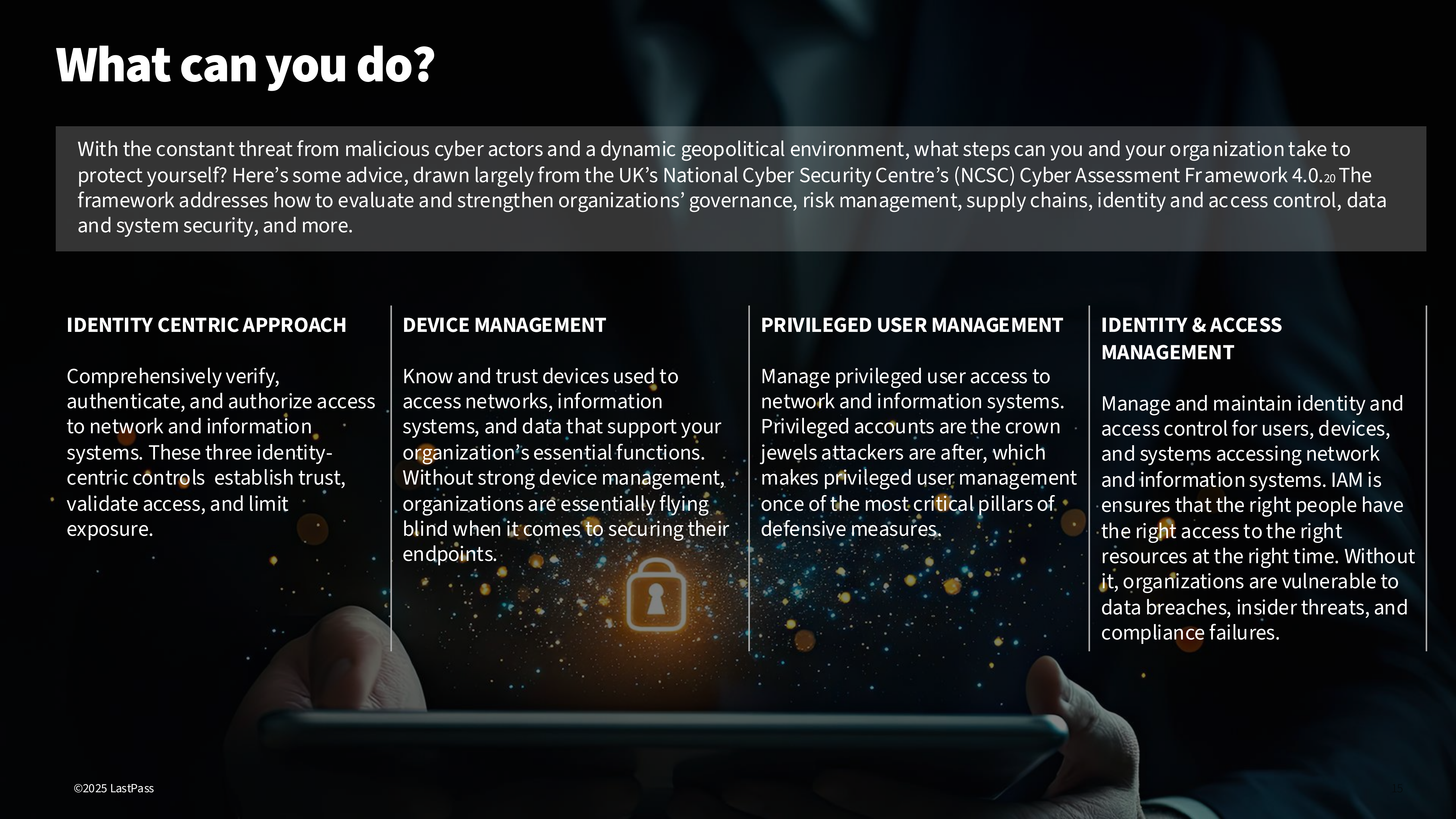
Know and trust devices used to access networks, information systems, and data that support your organization's essential functions. Without strong device management, organizations are essentially flying blind when it comes to securing their endpoints.

PRIVILEGED USER MANAGEMENT

Manage privileged user access to network and information systems. Privileged accounts are the crown jewels attackers are after, which makes privileged user management once of the most critical pillars of defensive measures.

IDENTITY & ACCESS MANAGEMENT

Manage and maintain identity and access control for users, devices, and systems accessing network and information systems. IAM is ensures that the right people have the right access to the right resources at the right time. Without it, organizations are vulnerable to data breaches, insider threats, and compliance failures.



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.

Follow **The Phish Bowl**

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.

Appendix – Sources & additional reading

1. IBM X-Force 2025 Threat Intelligence Index (IBM)
2. Global Cyber Attacks Surge 21% in Q2 2025 – Europe Experiences the Highest Increase of All Regions. (Check Point)
3. Google Threat Intelligence reporting.
4. Microsoft launches new European Security Program (Microsoft)
5. Q2 2025 Ransomware and Cyber Threat Insights (Guidepoint Security)
6. BERT Ransomware Group Targets Asia and Europe on Multiple Platforms (Trend Micro)
7. Malware Attacks and Infections 2025: Latest Statistics and Trends (Deep Strike)
8. Ransomware gangs join attacks targeting Microsoft SharePoint servers (Bleeping Computer)
9. Microsoft catches Russian hackers targeting foreign embassies (Ars Technica)
10. Ransomware debris: an analysis of the RansomHub operation (Group-IB)
11. ShinyHunters behind Salesforce data theft attacks at Qantas, Allianz Life, and LVMH (Bleeping Computer)
12. The Cost of a Call: From Voice Phishing to Data Extortion (Google Threat Intelligence Group)
13. Russian airline Aeroflot grounds dozens of flights after cyberattack (Bleeping Computer)
14. France's warship builder Naval Group investigates 1TB data breach (Bleeping Computer)
15. Ukraine arrests suspected admin of XSS Russian hacking forum (Bleeping Computer)
16. What we know about the cybercrime group Scattered Spider (Cybersecurity Dive)
17. Joint Cybersecurity Advisory: Scattered Spider (TLP: Clear) (CISA)
18. M&S says cyber hackers broke in through third-party contractor (Reuters)
19. Incidents impacting retailers – recommendations from the NCSC (UK's National Cyber Security Centre)
20. UK NCSC Cyber Assessment Framework 4.0 (UK National Cyber Security Centre)
21. Countries pledge to not pay ransoms, but experts question impact (Cybersecurity Dive)
22. UK plans to ban public sector bodies from paying ransom to cyber criminals (Reuters)
23. UK ties GRU to stealthy Microsoft 365 credential-stealing malware (Bleeping Computer)
24. Scania confirms insurance claim data breach in extortion attempt (Bleeping Computer)
25. ESET Threat Report H1 2025 (ESET)