FEBRUARY 2026

REGIONAL THREAT REPORT

EUROPE

STEPHANIE SCHNEIDER

CYBER THREAT
INTELLIGENCE ANALYST

MICHAEL KOSAK

DIRECTOR OF THREAT
INTELLIGENCE

The Regional Threat Report delivers strategic insights from the LastPass Threat Intelligence, Mitigation & Escalation (TIME) Team into the evolving cyber threat landscape across key global markets. Each edition provides a concise, intelligence driven overview of the most significant threats affecting organizations within a specific region, including Europe, Asia-Pacific, and North America.

For more cybersecurity insights, visit the LastPass Threat Intel blog or listen to The Phish Bowl podcast featuring the LastPass TIME team.

UK AND WESTERN CYBER AGENCIES WARN ABOUT THREATS TO INDUSTRIAL OPERATIONAL TECHNOLOGY.

Britain's National Cyber Secure Centre (NCSC) and international partners warned of growing digital threats facing operational technology (OT), the systems that run industrial equipment in critical infrastructure. The alert explained how organizations should securely connect industrial control systems, sensors and other critical services. U.S. agencies, the Dutch and German cybersecurity agencies, and fellow Five Eyes cyber partners from Australia, Canada and New Zealand co-authored the guidance. The guidance coincided with a Cisco Talos report detailing a Chinese-backed campaign targeting several North American critical infrastructure organizations over the last year using stolen credentials and vulnerable servers.

Many industrial technologies were not originally built with modern security needs in mind, leaving more openings for attackers. Threat groups targeting these environments now include ransomware gangs, state-backed hackers, and hacktivists. Due to intelligence gathering efforts and potential disruption in the event of an active conflict, Chinese-backed hackers remain an ongoing threat to Western critical infrastructure. In January 2026, the European Union proposed updates to the 2029 Cybersecurity Act to strengthen critical infrastructure by reducing reliance on high-risk foreign suppliers in communication and technology supply chains and tightening ICT security standards.

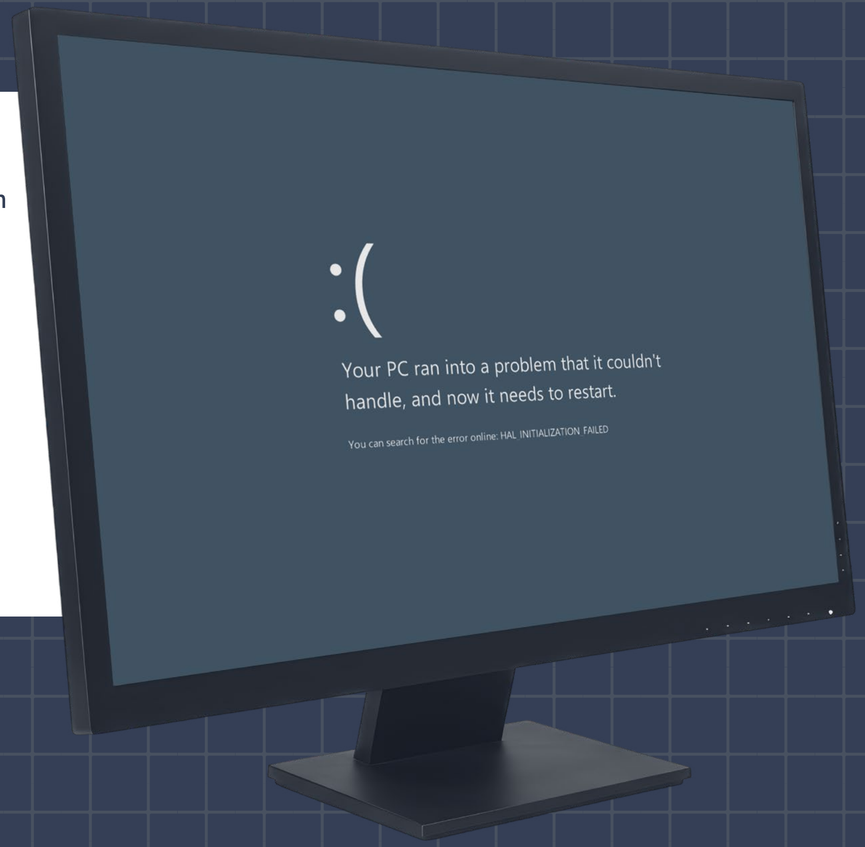
SOURCE | SOURCE

CLICKFIX ATTACKS TARGET EUROPEAN HOSPITALITY INDUSTRY WITH ‘BLUE SCREEN OF DEATH’ MALWARE.

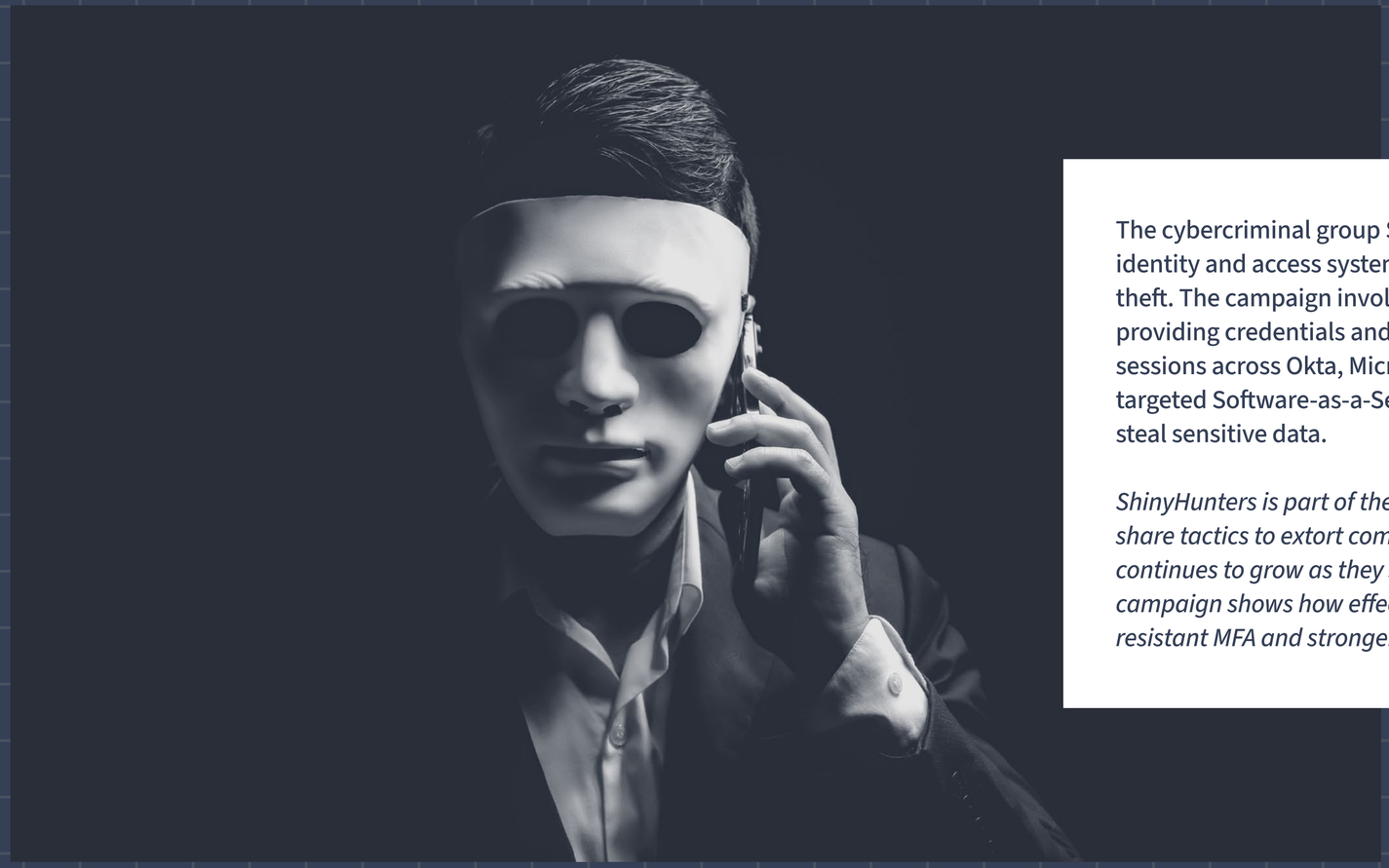
Securonix identified the PHALT#BLYX malware campaign tied to unnamed Russian-based attackers and targeting European hospitality organizations. The campaign sends a fake reservation cancellation message impersonating a popular travel booking site, eventually displaying an error message and “Blue Screen of Death” page. To exit the page, victims are asked to take a series of actions that prompt the download of DCRat malware, giving attackers control of infected systems and the ability to drop secondary payloads. As a decoy, a real booking page is opened while the malware works in the background.

This opportunistic phishing campaign during the busy holiday travel season uses a version of the “ClickFix” technique. Hackers socially engineer victims by prompting them to fix issues by copying, pasting and launching commands that result in downloading malware.

SOURCE



SHINYHUNTER'S SOCIAL ENGINEERING CAMPAIGNS TARGET SAAS PLATFORMS.



The cybercriminal group ShinyHunters is using social engineering tactics to compromise identity and access systems using vishing, company-branded phishing sites, and credential theft. The campaign involves hackers impersonating IT support to trick employees into providing credentials and MFA codes and using sophisticated phishing kits to hijack SSO sessions across Okta, Microsoft, and other cloud identity providers. Once inside, the group targeted Software-as-a-Service (SaaS) applications, like Salesforce and VPN providers, to steal sensitive data.

ShinyHunters is part of the larger Scattered Lapsus$ Hunters community, whose affiliates share tactics to extort companies for financial gain. The group's focus on cloud platforms continues to grow as they search for higher-value data to increase extortion payouts. This campaign shows how effective social engineering is and highlights the need for phishing-resistant MFA and stronger identity controls within enterprises.

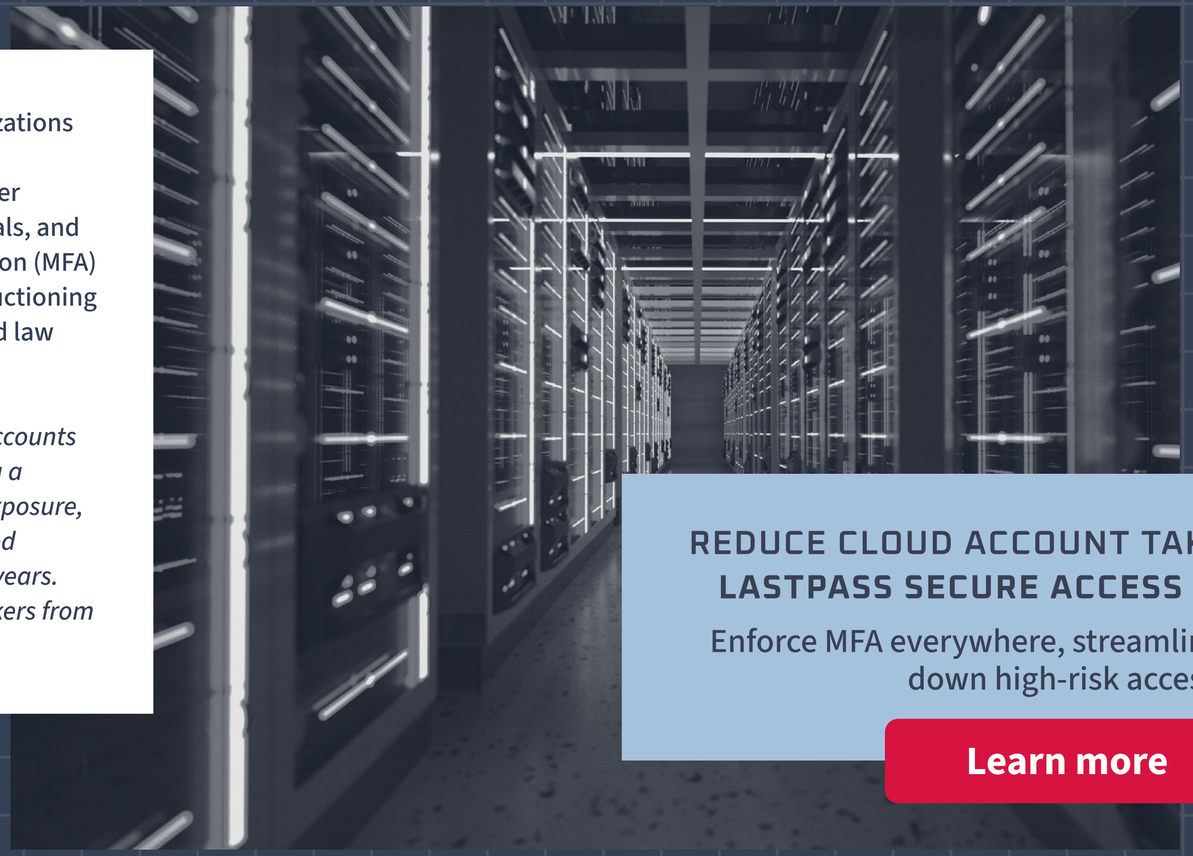
SOURCE

DOZENS OF GLOBAL COMPANIES BREACHED VIA STOLEN THIRD-PARTY CLOUD CREDENTIALS.

Hudson Rock researchers reported that multiple organizations had their self-hosted file sharing platforms breached in credential theft attacks. The hacker likely used infostealer malware to infect employees' devices, capture credentials, and access cloud accounts without multi-factor authentication (MFA) enabled. In December 2025, threat actor Zestix began auctioning data allegedly stolen from about 50 large companies and law firms, including Iberia, Spain's national airline.

Infostealers are a common and effective way to breach accounts and leak confidential data to pressure victims into paying a ransom. Hudson Rock warned of broad potential cloud exposure, noting that thousands of organizations have compromised credentials circulating in infostealer logs, sometimes for years. MFA adds an additional layer of security to prevent attackers from logging in with stolen credentials.

SOURCE



HACKERS BREACH INTERNAL SERVERS OF TECH PROVIDER FOR BRITAIN'S HEALTH SERVICE.

In December 2025, UK NHS tech provider DXS International suffered a breach of its internal servers. The ransomware group DevMan claimed responsibility for stealing an alleged 300 GB of data. Devman likely gained access via compromised credentials or vulnerability exploitation.

The incident adds to growing concerns over attacks on UK health technology suppliers and the operational risks tied to third-party systems. In November 2025, the UK government introduced the Cyber Security and Resilience Bill, which would impose large fines for companies that fail to protect themselves and could extend oversight to managed IT providers serving critical sectors, including healthcare.

SOURCE

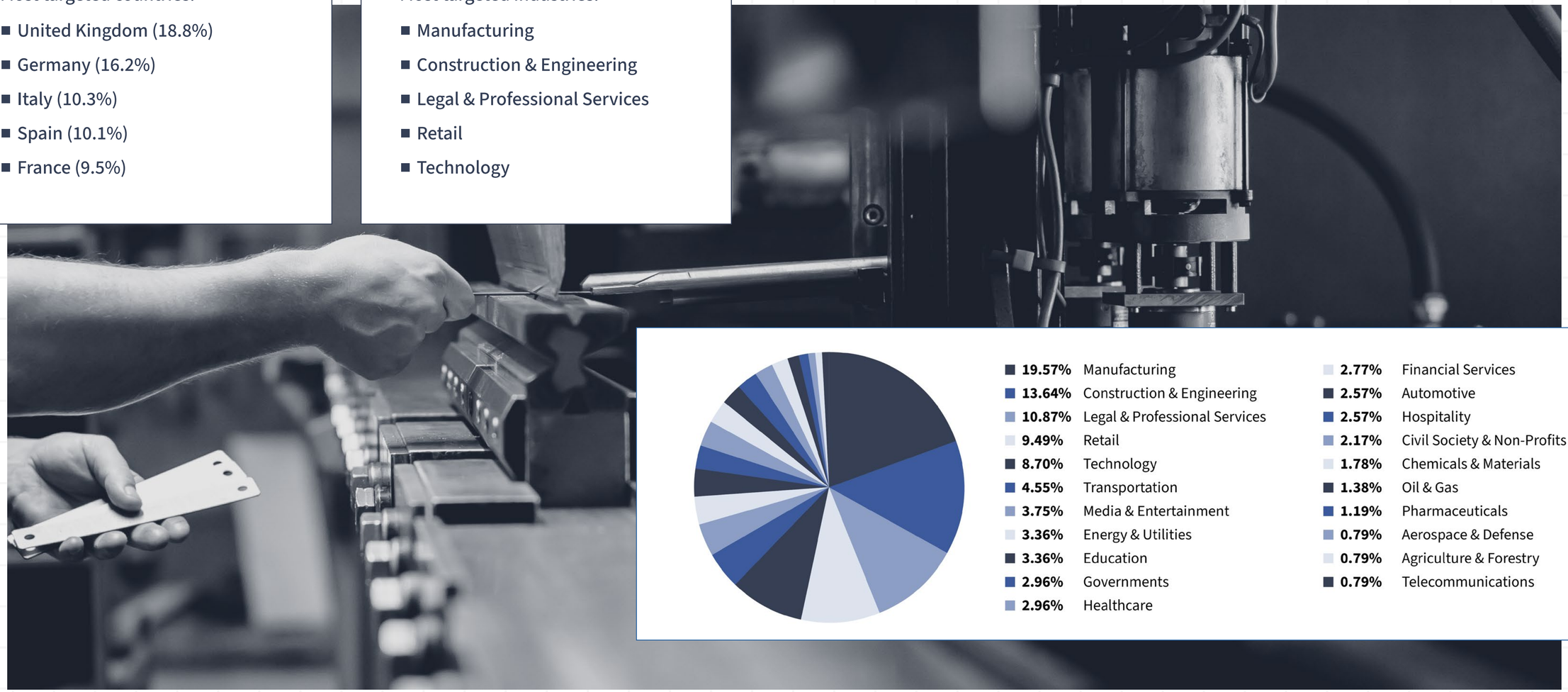
RANSOMWARE BY LANDSCAPE

Most targeted countries:

- United Kingdom (18.8%)
- Germany (16.2%)
- Italy (10.3%)
- Spain (10.1%)
- France (9.5%)

Most targeted industries:

- Manufacturing
- Construction & Engineering
- Legal & Professional Services
- Retail
- Technology

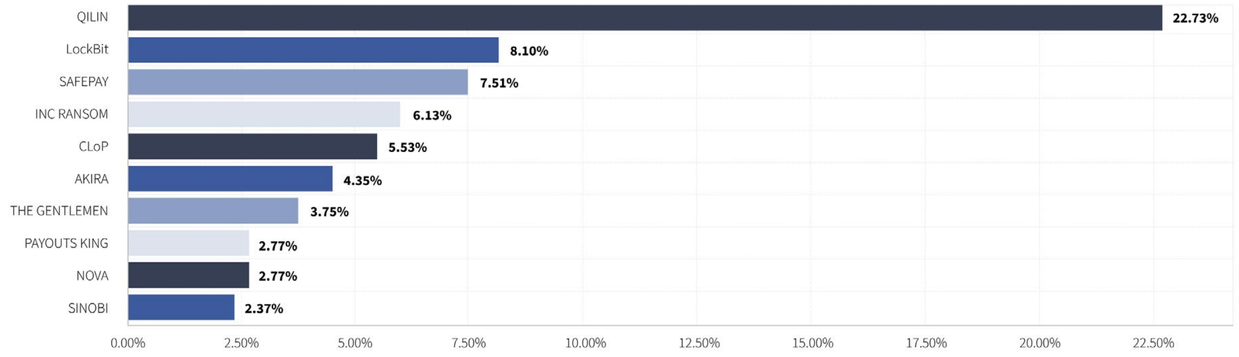


19.57%	Manufacturing	**2.77%**	Financial Services
13.64%	Construction & Engineering	**2.57%**	Automotive
10.87%	Legal & Professional Services	**2.57%**	Hospitality
9.49%	Retail	**2.17%**	Civil Society & Non-Profits
8.70%	Technology	**1.78%**	Chemicals & Materials
4.55%	Transportation	**1.38%**	Oil & Gas
3.75%	Media & Entertainment	**1.19%**	Pharmaceuticals
3.36%	Energy & Utilities	**0.79%**	Aerospace & Defense
3.36%	Education	**0.79%**	Agriculture & Forestry
2.96%	Governments	**0.79%**	Telecommunications
2.96%	Healthcare		

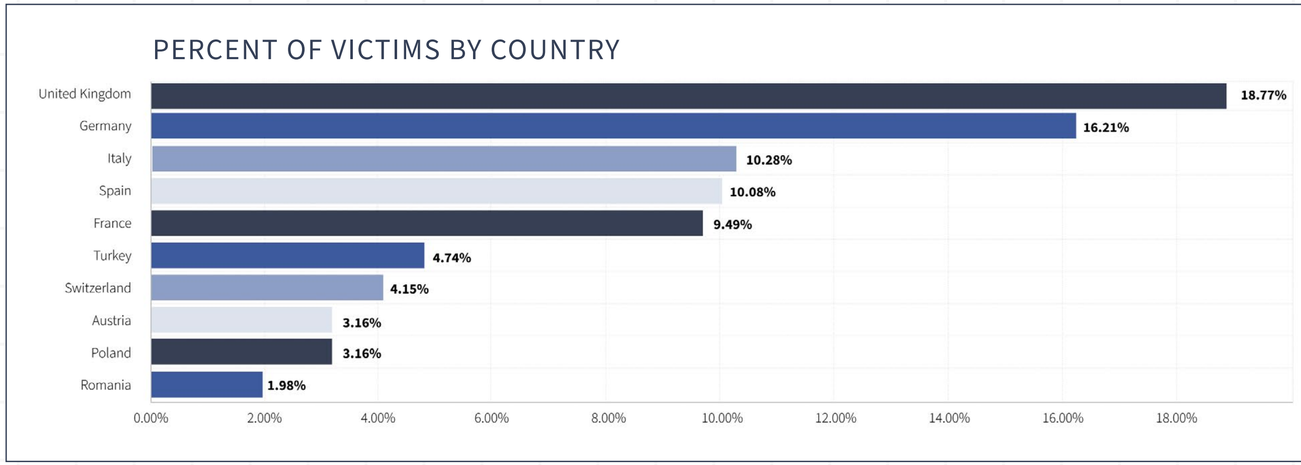
MOST ACTIVE RANSOMWARE GROUP: **QILIN**

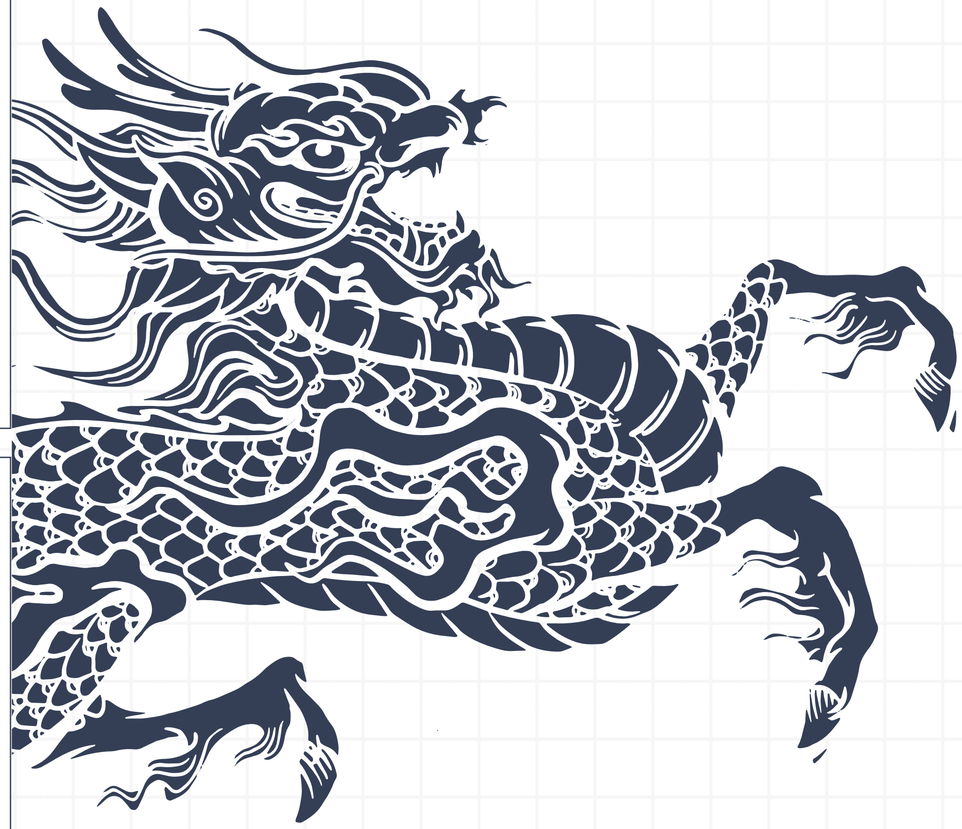
Target Profile: Small and medium-sized businesses (SMBs) remain the most frequently targeted companies in Europe. Companies of this size are generally attractive to attackers because they offer a balance of valuable data, ransom-paying capability, and perceived weaker defenses compared to larger enterprises.

PERCENT OF VICTIMS BY SHAMING SITE



PERCENT OF VICTIMS BY COUNTRY

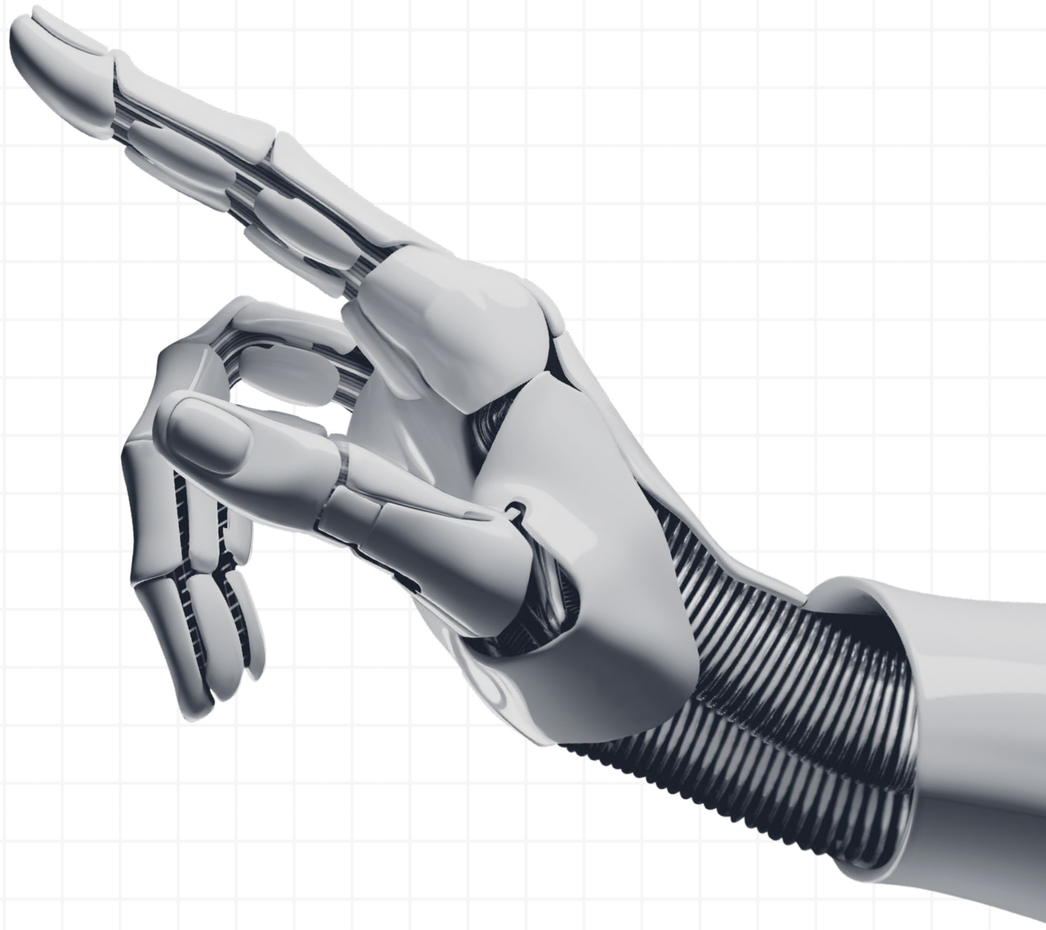




AI'S PROMISE, PERIL, AND THE OPENCLAW WARNING

- AI has reached a pivotal moment. Its ability to accelerate innovation is clear, but rapid development without adequate measures to protect users has outpaced security. Striking the right balance between incorporating AI capabilities into a company's technology stack while reducing risks this is an ongoing challenge for businesses. The pressure to rapidly adopt AI to maintain a competitive edge can expose organizations to data leakage, model poisoning, and agent hijacking.
- The viral AI personal assistant OpenClaw (aka Moltbot, ClawBot) illustrates the dangers of integrating AI without robust guardrails. OpenClaw's rapid rollout, misconfigurations, and lack of oversight enabled exploitation creating a new identity compromise vector. The use of unapproved AI tools is further amplifying the problem. Token Security found 22% of enterprises have employees running Moltbot without IT approval or basic protections like sandboxing and firewalls.

OpenClaw is an early warning that AI assistants can become significant identity-security risks. This technology reinforces the need for secure credential management, zero-trust access, and visibility into unsanctioned AI use. To ensure AI remains beneficial, organizations must embed responsible AI principles throughout development and deployment.



LastPass's TIME Team quickly identified and shut down a phishing campaign that started in January 2026 targeting LastPass customers. Attackers sent phishing emails disguised as LastPass maintenance alerts, asking users to back up their vaults in the next 24 hours. The emails included a link that allegedly takes users to a site designed to hijack accounts or steal vault master passwords.

Threat actors launched a second and third wave of phishing emails after LastPass disrupted their initial attack. The body of the email remained the same, but the links were changed. LastPass worked with third-party partners to quickly take down the malicious domain and shared Indicators of Compromise to boost awareness and collective defense.

Phishing is a common attack used to impersonate trusted brands. Remember that **LastPass will never ask for your master password.** Protect yourself by enabling MFA, checking sender details, and avoiding suspicious links or attachments. Use password managers, keep software updated, and verify urgent, unexpected requests. Immediately delete suspicious messages and report them to IT or via your email provider's phishing button.