Cyberint
A Check Point Company

Europe Threat Landscape 2024-2025

Trends, Risks, and Strategic Recommendations

October 2024

Table of Contents

Executive Summary

The **Cyberint Europe Threat Landscape 2024-2025** report sheds light on the increasingly complex and evolving cyber threat environment affecting organizations across Europe and the UK. Leveraging data from **Cyberint**—which monitors threats like phishing, malware, and supply chain vulnerabilities—the report highlights a surge in malicious activities driven by global conflicts, technological shifts, and the growing use of generative AI in cybercrime.

Key trends in 2024 include a **notable increase in ransomware attacks,** which have become more aggressive, often involving multiple extortion methods. **Malware infections,** fueled by the rise of **Malware-as-a-Service** (MaaS), have targeted industries across the board, while **phishing** campaigns, increasingly powered by AI, have become more convincing and harder to detect. Additionally, **DDoS attacks** have intensified, likely influenced by nation-state conflicts, disrupting industries from finance to transportation.

Cyberint Attack Surface Management through Argos has identified significant increases in **exploitable network ports and misconfigured email security,** exacerbated by the complexity of hybrid work environments and cloud-based infrastructures. **Data leakage** remains a growing concern, with compromised credentials and payment cards leading the charge, while **fraud schemes** like coupon fraud and mule operations continue to adapt and target retail and financial sectors.

Looking ahead to 2025, organizations will face a heightened risk landscape, driven by the following emerging trends:

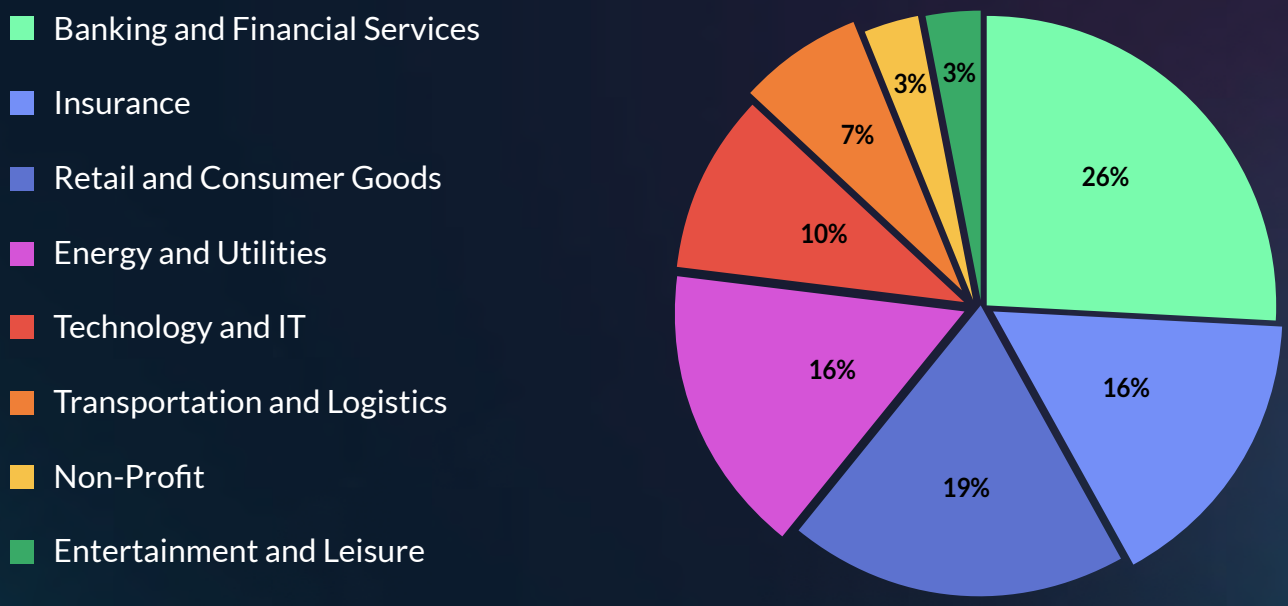
- AI-enhanced phishing and social engineering. Expect phishing attacks to become more sophisticated, leveraging AI to generate highly personalized, automated campaigns.
- Supply chain vulnerabilities. Attackers will increasingly exploit third-party vendor weaknesses, leading to a rise in supply chain attacks.
- Evolving ransomware tactics. Ransomware will continue to grow in complexity, with AI-empowered malware evading detection and new extortion techniques being developed.
- Risks associated with remote and hybrid work models. Unsecured personal devices and home networks will be targeted, emphasizing the need for more robust endpoint security.
- Threats from uncontrolled mobile apps. The unregulated distribution of mobile apps will heighten the risk of SDK- and API-based attacks, causing data breaches and exposing sensitive information.
- Geopolitical-driven cyber warfare. The escalation of nation-state cyberattacks will impact critical infrastructure and government entities, further intensifying the cybersecurity challenge.

Organizations must strengthen their cybersecurity postures, focusing on multi-layered defenses, real-time threat detection, and rigorous employee training to mitigate these growing risks. The integration of AI in both defensive and offensive capabilities will be key to staying ahead of the evolving threat landscape in 2025.

Methodology

Cyberint's Europe Threat Landscape Report 2024-2025 is built on a multi-faceted intelligence approach that integrates both proprietary and public data sources. We sourced intelligence derived from our own Cyberint solution, which monitors a wide range of threat vectors through modules such as Attack Surface Management, Darkweb Threat Intelligence, Supply Chain Intelligence, Malware Intelligence, Phishing Detection, Social Media Monitoring and more.

Cyberint provides critical alerts and indicators that inform our analysis, allowing us to offer an intelligence-focused overview of the cybersecurity threat landscape of Europe and the United Kingdom. Cyberint-sourced information in this report is from a sample of approximately 140,000 intelligence alerts, from October 1, 2021 to October 1, 2024, from 40 companies in Europe and the UK, in the following industries:



We also leverage open-source intelligence (OSINT), including threat feeds, news articles, and research publications from cybersecurity experts and regulatory bodies. Additionally, we give credit to the following agencies, whose threat landscape and state of security analyses supplemented our 2024 Threat Landscape Overview (see citations):

1. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. September 2024. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

2. Cloudflare. Shielding the Future: Europe's Cyber Threat Landscape. March 2024. Available at: https://www.cloudflare.com/shielding-the-future.

3. Splunk. State of Security 2024: The Race to Harness AI. 2024. Available at: https://www.splunk.com/state-of-security-2024.

We then apply advanced analytics and threat modeling to identify patterns and predict emerging cyber trends for 2025, particularly key threats and vulnerabilities that European organizations should prepare for.

This report does not go deep into ransomware--Cyberint's Research Team produces quarterly and annual ransomware reports separately.

2024 Threat Landscape Overview

Top Industry Topics This Year

Ransomware

Ransomware continues to be one of the most significant threats, evolving with more sophisticated tactics such as double and triple extortion, where data is encrypted, stolen, and threatened to be released unless a ransom is paid. This has been highlighted in the ENISA Threat Landscape report, where ransomware consistently ranks as a top threat.[1] In Europe, ransomware attacks continue to cause substantial financial damage, with many organizations experiencing repeated attacks.[2] Additionally, the increasing use of AI to create more complex ransomware variants adds to the challenge.[3]

Malware

Malware remains a broad threat category that includes everything from trojans and viruses to spyware and worms. ENISA reports a rise in Malware-as-a-Service (MaaS), allowing less-skilled attackers to deploy sophisticated malware.[1] This threat is prevalent across industries, particularly in technology and financial services.[2] Splunk's State of Security report emphasizes that AI is enhancing malware's adaptability, making detection and response even more challenging.[3]

Social Engineering

Phishing, spear-phishing, and business email compromise (BEC) continue to be highly effective attack vectors. ENISA highlights social engineering techniques as a major means for attackers to gain unauthorized access.[1] Phishing remains the most common form of attack, particularly in sectors like IT, education, and healthcare.[2] With the advent of AI-generated phishing scams, these attacks are becoming more convincing and harder to detect.[3]

DDoS

DDoS attacks, which aim to overwhelm systems and disrupt services, remain a key threat. ENISA notes the increasing availability of DDoS-for-hire services, making it easier for attackers to launch large-scale attacks.[1] Cyberint observes its prevalence may highly likely be due to the ongoing conflicts, where nation-states are leveraging cyber warfare as part of their strategy, such as in the Russia-Ukraine conflict, and the Israel-Hamas conflict. DDoS attacks frequently target high-traffic industries such as transport, IT, and finance,[2] and their complexity has been increasing, making mitigation more difficult.[3]

Supply Chain Attacks

Supply chain attacks target vulnerabilities in third-party software, vendors, or partners, which can lead to widespread compromise. ENISA highlights the growing concern around supply chain risks, noting that these attacks are difficult to detect and have far-reaching consequences.[1] Many organizations remain unprepared for supply chain risks, with incidents affecting sectors like energy, healthcare, and finance.[2] The increased reliance on cloud services and complex supply chains heightens the vulnerability.[3]

Generative AI Risks

The rapid adoption of generative AI brings new risks, as threat actors leverage AI to enhance their attacks. ENISA and other reports have observed that AI can be used to create more convincing phishing attacks, automate vulnerability discovery, and even generate malicious code.[12] Splunk's State of Security report stresses that both defenders and attackers are racing to harness AI, with 45% of security professionals fearing that AI will benefit attackers more.[3] As organizations increasingly rely on AI, the potential for AI-powered attacks to outpace defenses is a growing concern.

Cyberint Intelligence Insights for Europe & the UK

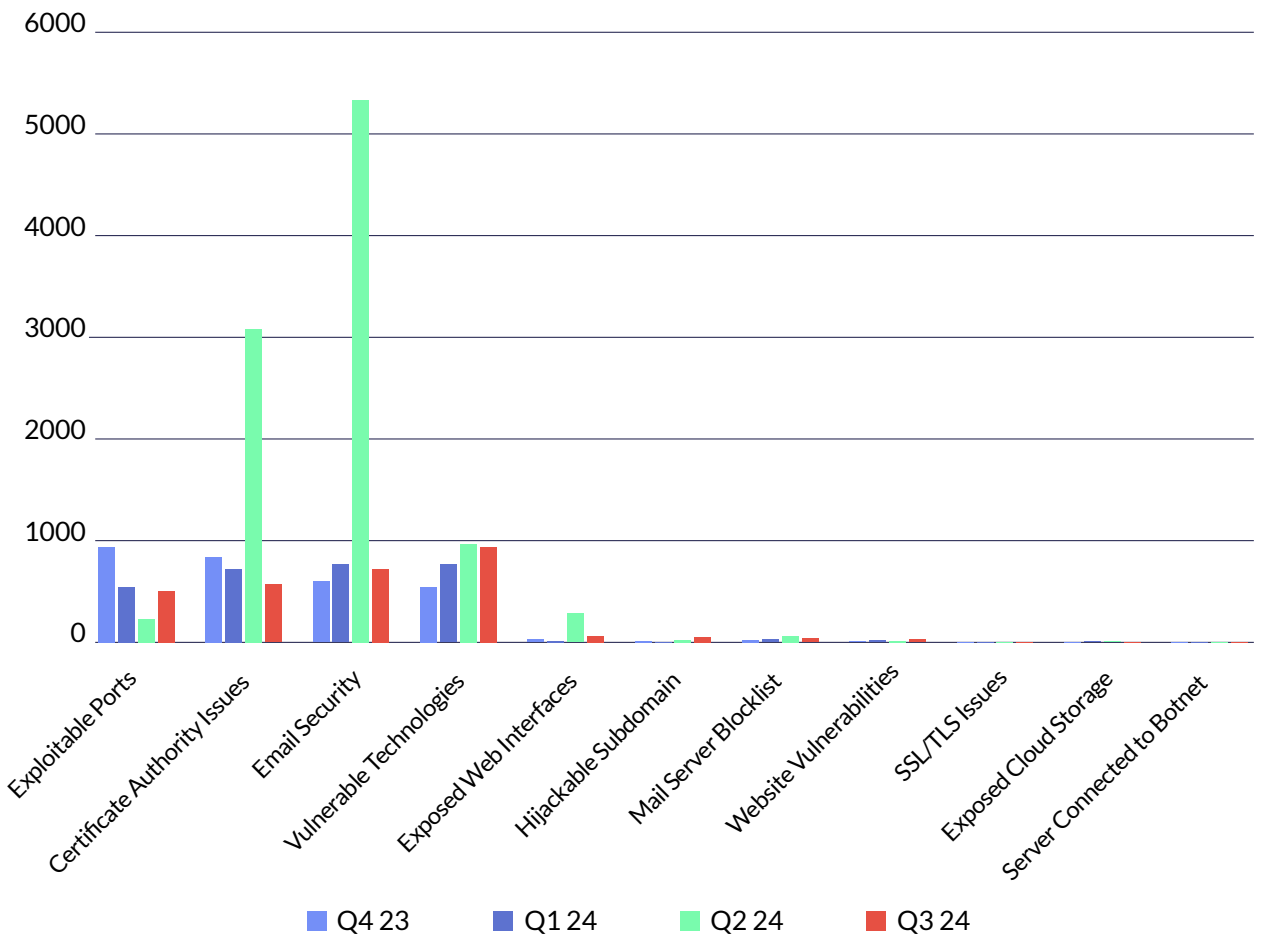
Throughout the past year, Cyberint has provided a comprehensive view of the cyber threat landscape across various sectors in Europe, capturing key insights through its threat intelligence modules.

Our alert data highlights distinct trends across multiple threat categories, from malware and phishing to more sophisticated attacks such as supply chain compromises.

While the raw numbers reveal an uptick in threat activity, it is important to contextualize this growth. The expansion of our client base throughout the year has contributed to an overall increase in the number of detected instances. This upward trend reflects not only the rising volume of threats but also the broader reach of our intelligence capabilities as we onboarded more organizations across different industries. Each data point represents more than just a figure; it offers critical insights into the evolving tactics of adversaries and the shifting nature of cyber risks that businesses must address.

Vulnerabilities

Vulnerability Alert Statistics for Cyberint's Client in Europe and the UK



Cyberint Attack Surface Management

Cyberint Attack Surface Monitoring & Management provides automatic and full visibility into your digital presence – uncovering security issues and vulnerabilities that can be exploited by potential adversaries.

- ***Exploitable Ports.*** *Argos monitors open network entry points that, if exploited, can lead to significant security breaches, allowing threat actors to install malware, exfiltrate sensitive data, or disrupt business operations.*

- ***Certificate Authority Issues.*** *Misconfigured or compromised certificate authorities can lead to man-in-the-middle attacks, severely undermining the company's ability to ensure secure communications.*

- ***Email Security.*** *Missing or misconfigured SPF and DMARC records, among others, expose companies to email spoofing and phishing attacks.*

- ***Vulnerable Technologies:*** *Outdated software with known vulnerabilities (e.g., old versions of NGINX or JavaScript) can be easily exploited, putting sensitive systems and data at risk.*

- ***Exposed Web Interfaces.*** *Public-facing login pages or interfaces that should be internal can give attackers direct access to sensitive systems, increasing the risk of breaches.*

- ***Hijackable Subdomains.*** *Subdomains that can be hijacked allow attackers to impersonate trusted parts of a company's website, facilitating phishing attacks or malware distribution.*

- ***Mail Servers in Blocklist.*** *Blocklisted mail servers cause email delivery issues, disrupting communication with clients and partners and damaging the company's reputation.*

- ***Website Vulnerabilities.*** *Cross-site scripting (XSS) and similar vulnerabilities allow attackers to inject malicious scripts, leading to data theft or user compromise.*

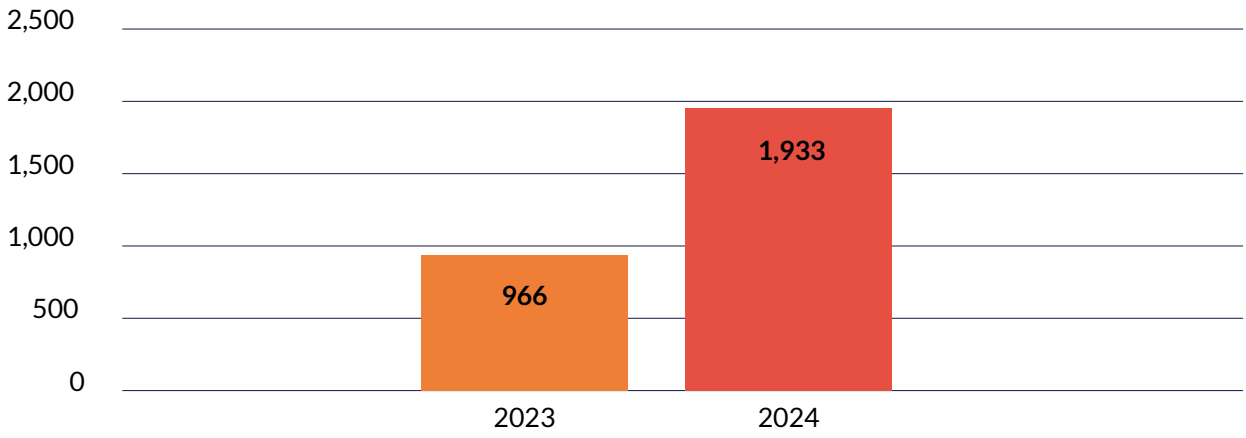
- ***SSL/TLS Issues.*** *Weak or outdated SSL/TLS configurations can expose encrypted communications, allowing attackers to intercept sensitive data or compromise user privacy.*

- ***Exposed Cloud Storage.*** *Publicly accessible cloud storage buckets can lead to unauthorized data access, putting confidential company or client information at risk.*

- ***Server Connected to Botnet.*** *Servers infected with botnet malware can be used for malicious purposes, leading to reputational harm, data loss, and potential legal liabilities.*

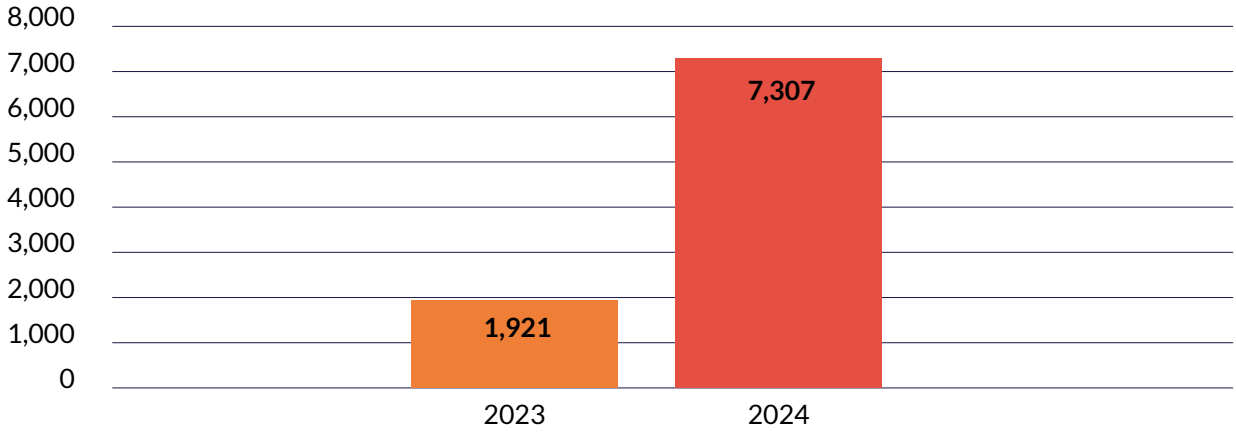
Key Insights

Exploitable Ports



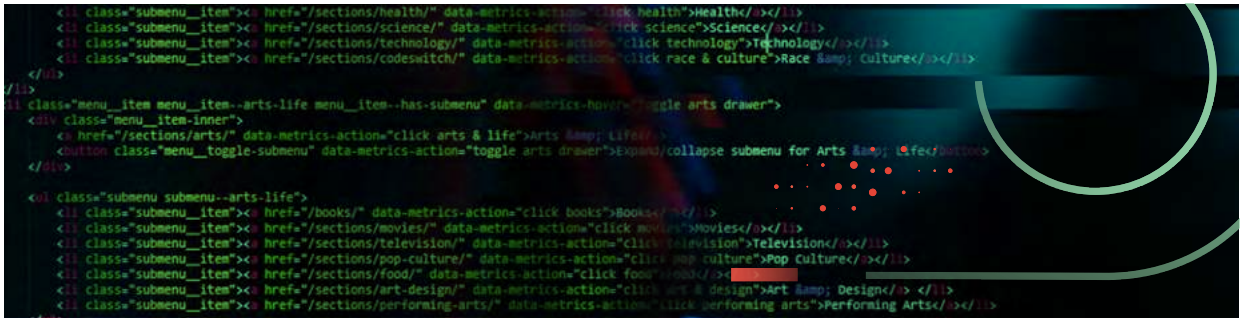
- The number of exploitable ports in 2024 saw a two-fold increase compared to 2023.
  - Companies continue to scale their operations and adopt new technology, and as cloud services, hybrid infrastructures, and IoT devices become more widely adopted, IT environments increase in complexity.
  - The continued shift to remote and hybrid working models increases reliance on remote access services, which, if not properly secured, expose additional ports.
  - Exploitable ports are particularly common in large companies with vast infrastructures and a broad attack surface, making them attractive targets for cybercriminals.
  - Mitigating these vulnerabilities can be challenging due to the complexity of managing numerous devices and services, but with proper network monitoring, regular port scanning, and strict firewall configurations, it is a manageable task. Proactive measures like automated vulnerability detection and regular audits are essential to minimizing the risk.

Email Security



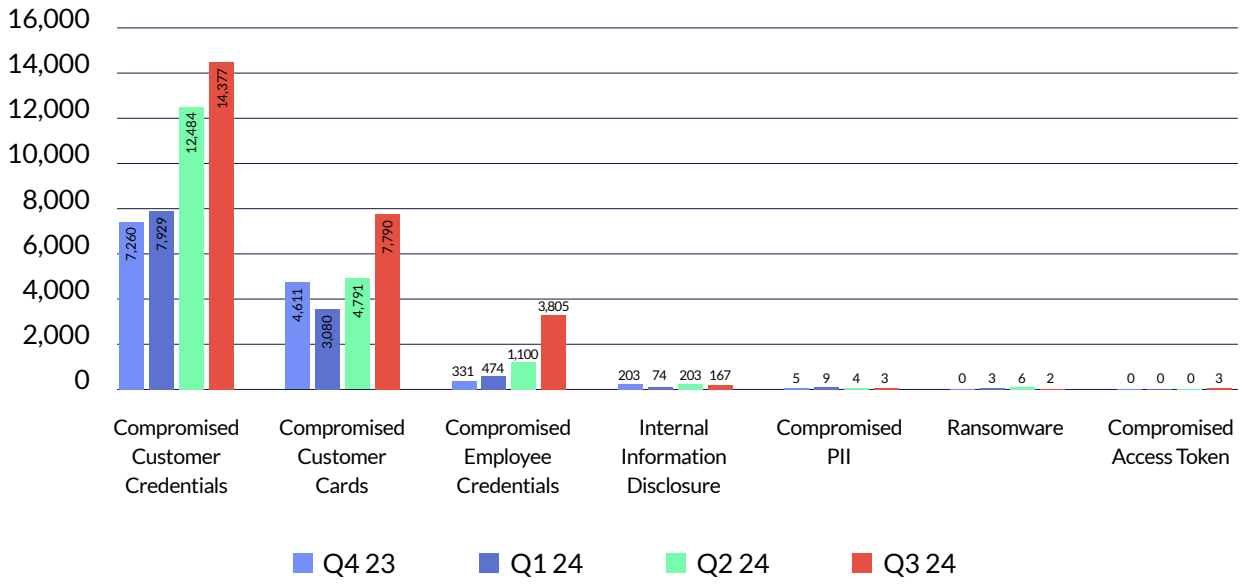
- Using multiple domains for sending emails increased email security issues in 2024.
  - Companies may use different domains or subdomains for different brands, subsidiaries, or regions. They also often use third-party platforms for email marketing and customer service.
  - It is crucial to configure SPF, DKIM, and DMARC for each sending domain to prevent misuse, such as phishing and spoofing.

- 2024 saw a decrease in cloud security issues for Cyberint clients.
  - Cloud security was a major issue post-COVID, and was still significant in 2023-2024, albeit to a lesser extent. According to ENISA, 82% of data breaches involved data stored in public and private clouds. However, data breaches are often the result of exploiting human factors, such as social engineering, phishing, or user error.
  - Cyberint detected zero cases of unsecured cloud storage for the past two years, which could be attributed to increased awareness and training, and the improvement of cloud security design by cloud providers.



Data Leakage

Data Leakage Alert Statistics for Cyberint's Clients in Europe and the UK



Cyberint Darkweb Intelligence

Cyberint helps access top-tier sources in the dark web. We collect and analyze data from elusive web sources that most other companies cannot penetrate, and enrich our automated collection with a human approach, through research and analysis of our expert team. Data risks we cover include:

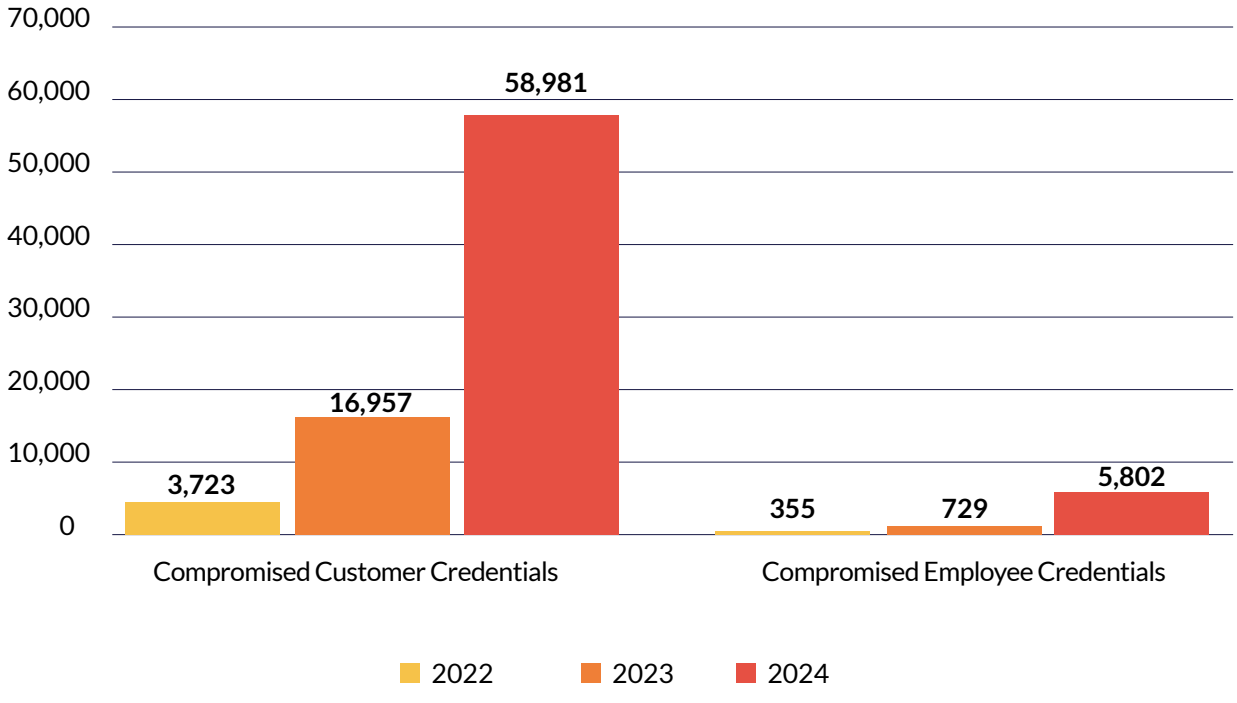
- *Compromised employee or customer credentials, and/or personally identifiable information (PII).*
- *Compromised payment cards, for banking clients.*
- *Exposed private access tokens, source codes, sensitive internal email correspondences, and confidential files.*
- *Breached data, including those disclosed by malicious insiders.*
- *Outputs of vulnerability scanners targeting organizations.*

Key Insights

Most Prevalent Data Leakage Cases Across Cyberint's Clients in Europe and the UK for 2024

	2022	2023	2024
Compromised Customer Credentials	3,273	16,957	58,981
Compromised Employee Credentials	355	729	5,802
Compromised Payment Cards	1,485	11,919	20,311
Internal Information Disclosure	71	171	648

An Annual Comparison of Compromised Customer and Employee Credentials



- Cyberint data shows a dramatic increase in customer credential exposure in the past three years, with an average percentage increase of 333% per year. This is likely driven by factors such as increased phishing attacks, credential stuffing, and data breaches. This also reflects the increasing sophistication of threat actors, and the growing use of automation in attacks. We expect this to continuously increase amid the emergence of generative AI.

- Compromised employee credentials alerts increased nearly eightfold from 355 in 2022 to 5,802 in 2024. The sharp rise in compromised employee credentials, largely sourced from malware logs, highlights the growing risk of employee exposure to malware. This can be attributed to the widespread use of personal devices, remote and home networks, coworking spaces, and unsecured public Wi-Fi. As employees access sensitive company resources from less secure environments, the potential for malware infections that harvest credentials increases significantly.

    - Companies should enforce strong security policies, including multi-factor authentication (MFA), endpoint protection, and VPN usage, along with regular employee training on avoiding risky online behaviors and securing their devices.

- The sharp rise in compromised payment card alerts can be attributed to threat actors increasingly targeting vulnerable point-of-sale (PoS) systems, exploiting weaknesses in banking infrastructure, and using phishing campaigns to steal customer payment information. Additionally, **BIN stuffing** (where attackers guess valid payment card details using the first six digits of a card) and the use of **BIN checkers** (tools to verify the validity of card details) have become prevalent techniques to compromise payment card data. Malware-infected devices, whether used by customers or within the company's infrastructure, also play a significant role in harvesting sensitive payment card data.

    - Companies should secure PoS systems with up-to-date software, employ strong anti-malware solutions, and use advanced fraud detection systems to identify suspicious activity. Additionally, implementing measures to detect and block BIN stuffing attempts, as well as educating customers on avoiding phishing schemes and ensuring device security, can help mitigate these risks.

Fraud

Cyberint Virtual Humint Operations

Gain a valuable human element when it comes to research, investigation, and threat intelligence operations. Deepen your understanding of the vectors behind the threat itself, including the threat actor's motivation, the tools, tactics and procedures (TTPs) in use, third-party vendors involved, and other crucial factors.

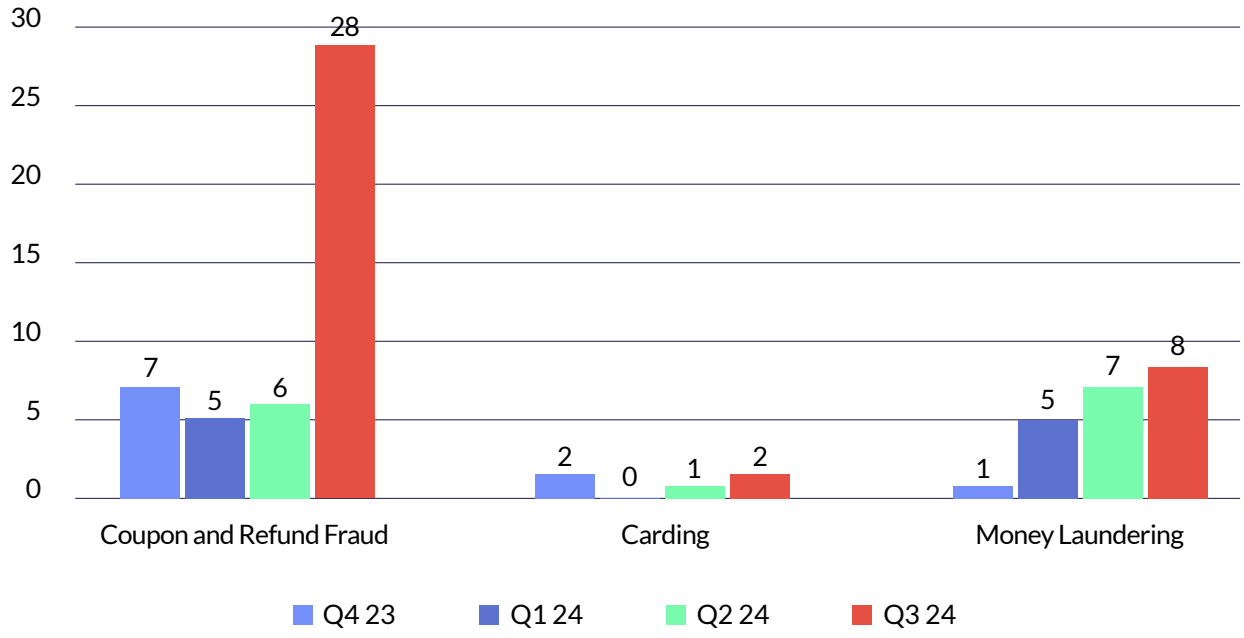
- ***Coupon and Refund Fraud.*** *Refund fraud involves exploiting return policies or using stolen payment information to obtain money or goods without returning legitimate items. Coupon fraud occurs when counterfeit or stolen coupons are used to acquire goods or claim refunds. Fraudsters often combine both methods, leading to significant financial losses for retailers.*

- ***Mule Account and Cashout Operations.*** *Mule accounts are bank accounts used by criminals to transfer stolen funds, often through unsuspecting or complicit individuals, called "mules," to hide the origin of illegal gains. In cashout operations, cybercriminals use mule accounts to convert stolen assets, such as compromised payment card data, into real money through fraudulent transactions or withdrawals, making it harder to trace the funds.*

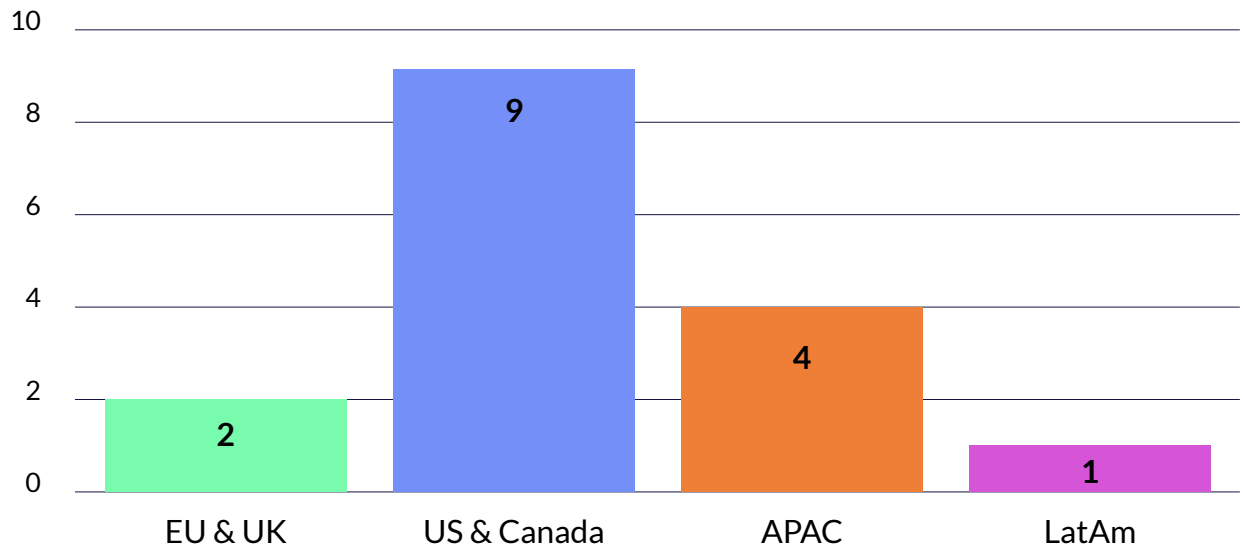
- *Argos is also capable of monitoring extortion schemes, as well as* ***victim reports*** *across the open, deep and dark web, and social media.*

Top Fraud Cases Among Cyberint's Clients in Europe and the UK.

The Surge in Q3 2024 in Coupon and Refund Fraud is Attributed to the Onboarding of Major Retail Clients in That Period.



Carding Cases Per Region Among Cyberint's Clients in 2024



Key Insights

- Carding is less prevalent in Europe compared to other regions. This may be due to the following:
  - Stronger Regulations. Europe enforces strict security standards, such as the Payment Services Directive 2 (PSD2), which mandates Strong Customer Authentication (SCA)for online transactions. This reduces the likelihood of fraudulent transactions by requiring multi-factor authentication.
  - Chip-and-PIN. Europe has widely adopted EMV chip-and-PIN technology, which is more secure than magnetic stripe cards. This makes it harder for fraudsters to clone cards or use stolen card data for in-person transactions.
  - Consumer Awareness. European consumers are often more aware of cybersecurity risks due to public education campaigns and stricter privacy regulations like GDPR, making them less susceptible to phishing and other carding-related schemes

- Continuous increase of money laundering cases have affected both Cyberint's finance and retail clients, as cybercriminals use stolen funds from fraudulent transactions to fuel illicit activities.
  - The rise in global conflicts has further exacerbated this issue, increasing the demand for money laundering services. International sanctions on conflict zones drive the need to move money through illegal channels to bypass financial restrictions. Additionally, the heightened trade of illicit goods, such as arms and contraband, creates a need to launder large sums of money. The influx of refugees and undocumented individuals also contributes, as they may require access to financial services, making them vulnerable targets for exploitation by criminal networks.

Phishing

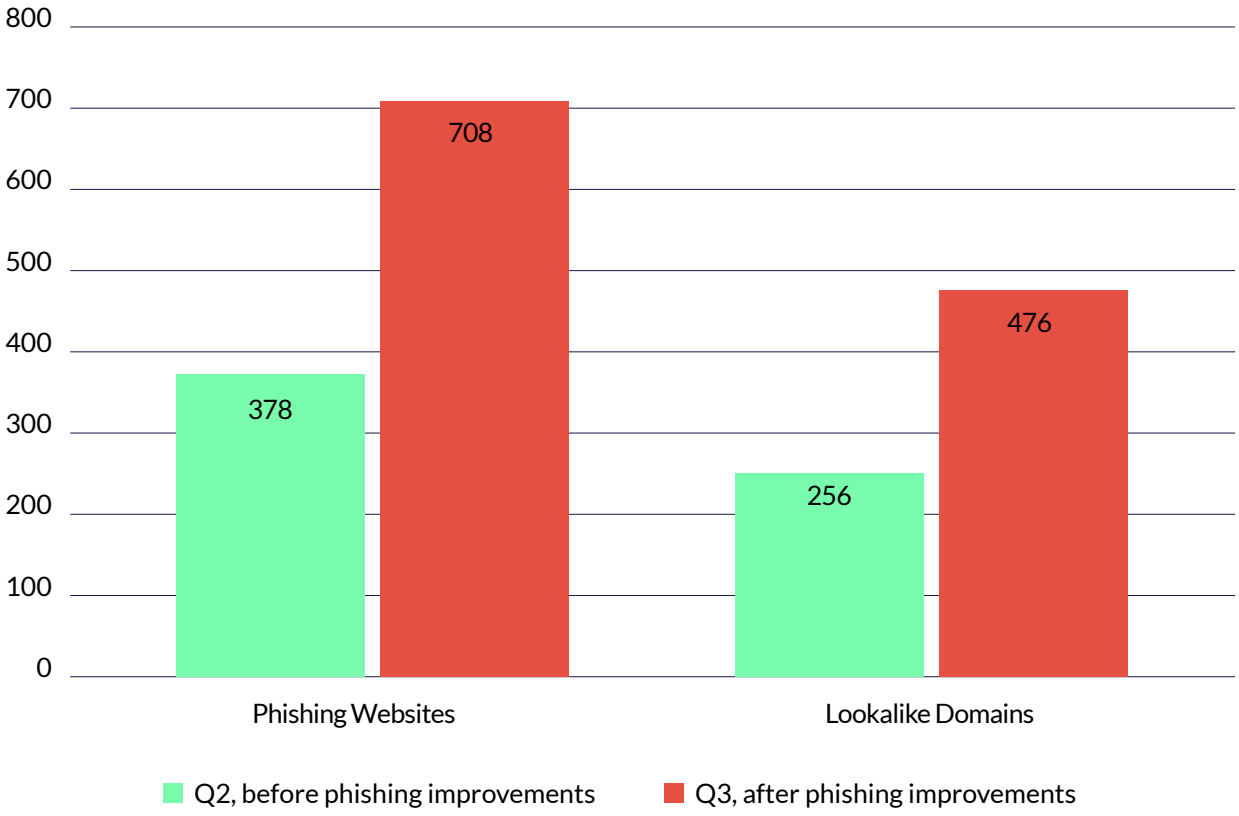
Cyberint Phishing Detection and Takedown

Cyberint uses various methods to identify potential phishing attacks and ensure end-to-end coverage, detection and protection from phishing attempts.

- *Identifying typosquatting domains.*
- *Phishing URL feed analysis.*
- *Chatter monitoring.*
- *Phishing beacon.*
- *Threat Intelligence.*
- *Mitigation and takedowns.*

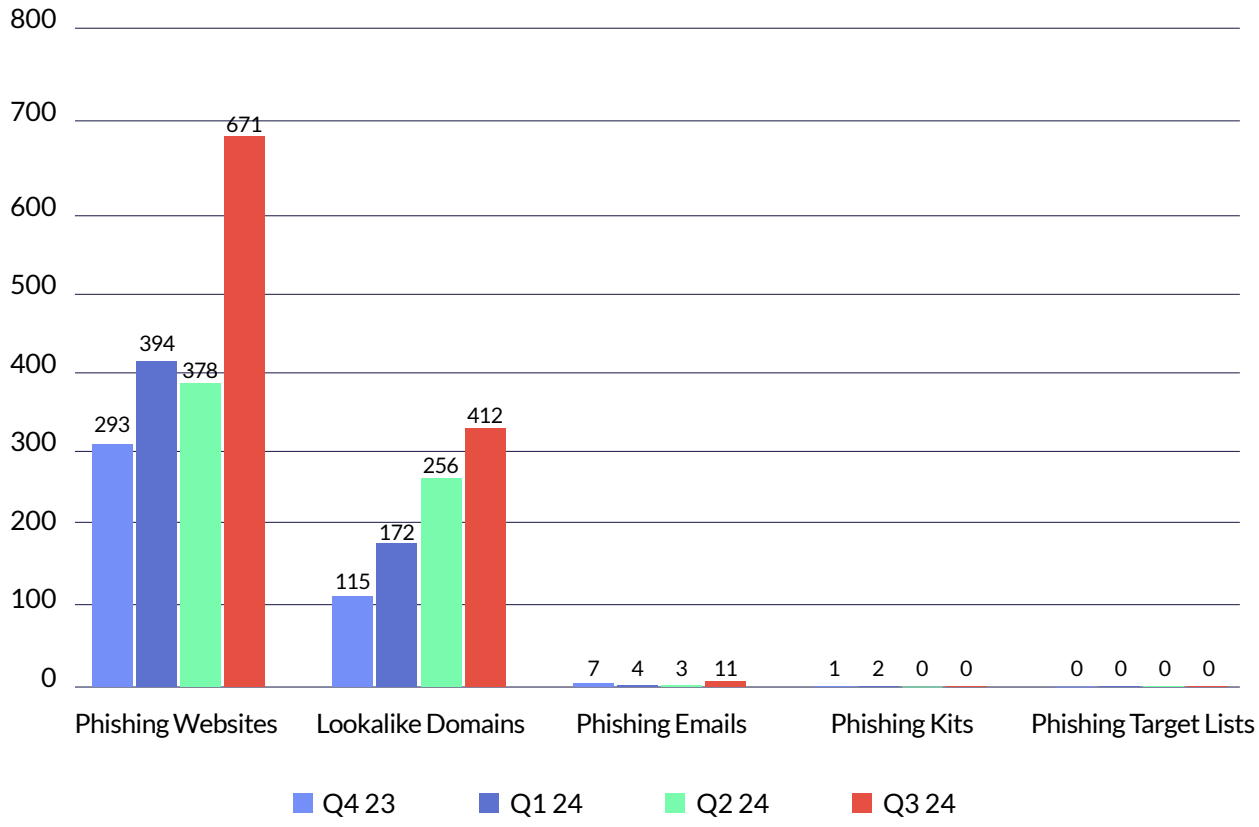
2024 Developments in Argos Phishing Detection

Increase in Phishing Detections After July 2024 Developments



In July 2024, Cyberint launched a significant new tool in our arsenal to combat phishing misdetections and campaigns. The new capability relies on the way threat actors both copy customer websites and reuse phishing kits. It allows us to mark specific page resources, like images and text files, as protected page resources, and to tag any suspicious page from any of our feeds as phishing if it uses them. Pages with the configured resources will trigger a high confidence phishing alert which will be published automatically, preventing any human errors or delays in reviewing candidates. This, along with our continuous commitment to improving our machine learning capabilities for detecting lookalike domain permutations, reaped great rewards in our phishing detection: **We saw an 87.3% increase in the detection of phishing sites, and an 85.94% increase in the detection of lookalike domains, after the improvements were deployed.**

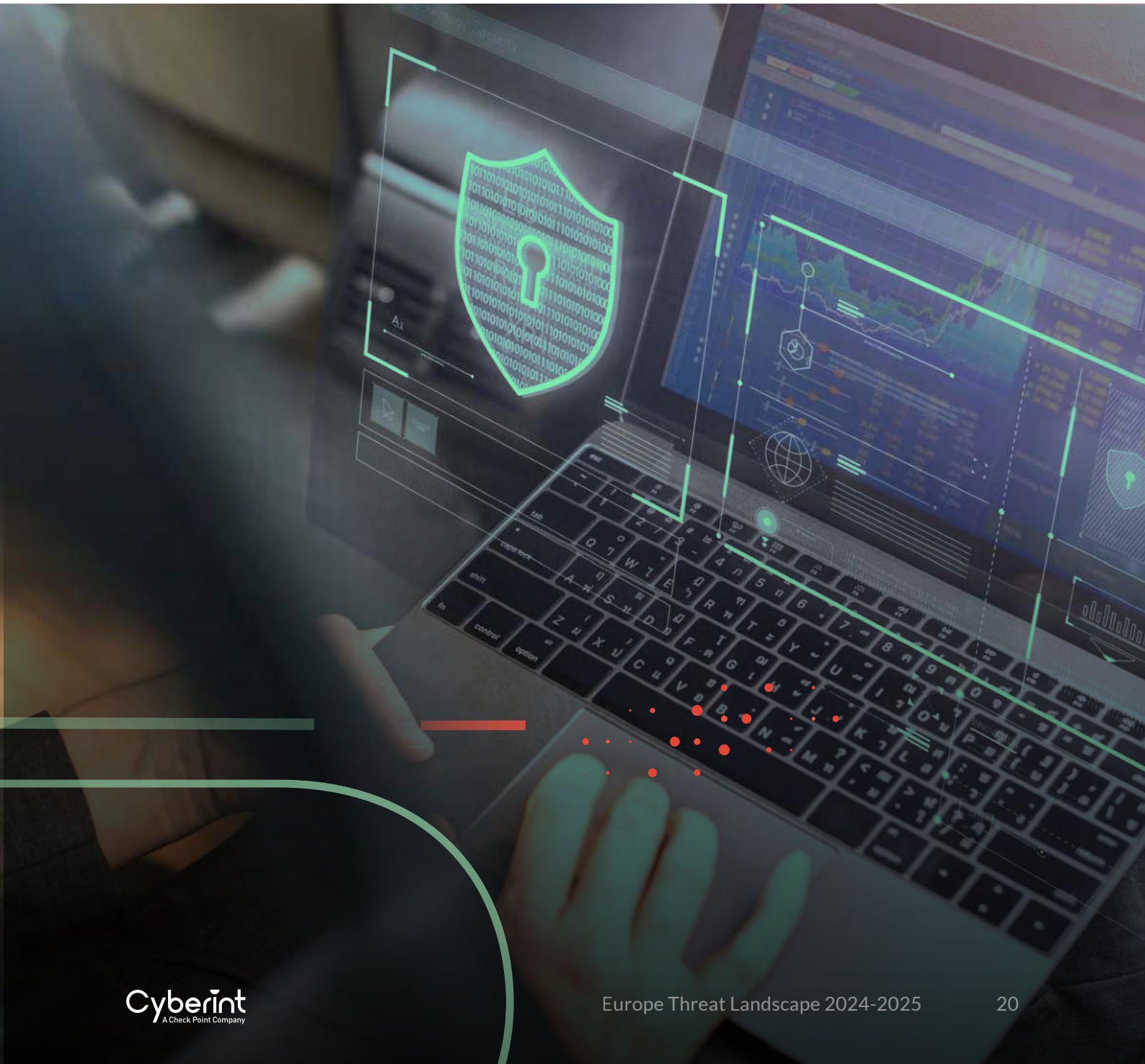
Phishing Cases in 2024 Across Cyberint's Clients in Europe and UK



Key Insights

- **Increase in dynamic phishing sites.** Cyberint observed more cases of dynamic phishing sites in 2024. Unlike traditional static phishing sites, which can be quickly identified and blacklisted, dynamic phishing sites change their content, or appearance frequently; in most cases, they only appear to specific devices and user agents, making it harder for security systems and users to recognize them as malicious. This adaptability allows attackers to target users more effectively by presenting seemingly authentic environments and avoiding blacklists.

- **Generative AI** significantly enhances the sophistication of phishing attacks by enabling attackers to craft highly convincing and personalized messages at scale. Threat actors can quickly generate emails, text messages, or social media posts that mimic the tone, language, and style of legitimate organizations, making phishing attempts harder to detect. AI also allows for dynamic adaptation, tailoring phishing content based on publicly available information about the target, such as their role, interests, or recent online activity. This level of personalization increases the likelihood of successful social engineering, as victims are more likely to trust and engage with communications that appear authentic. Additionally, AI can automate the creation of phishing websites that adapt to different user behaviors, making it more challenging for traditional detection systems to keep up. As generative AI tools become more accessible, the potential for widespread, sophisticated phishing campaigns grows.



Brand

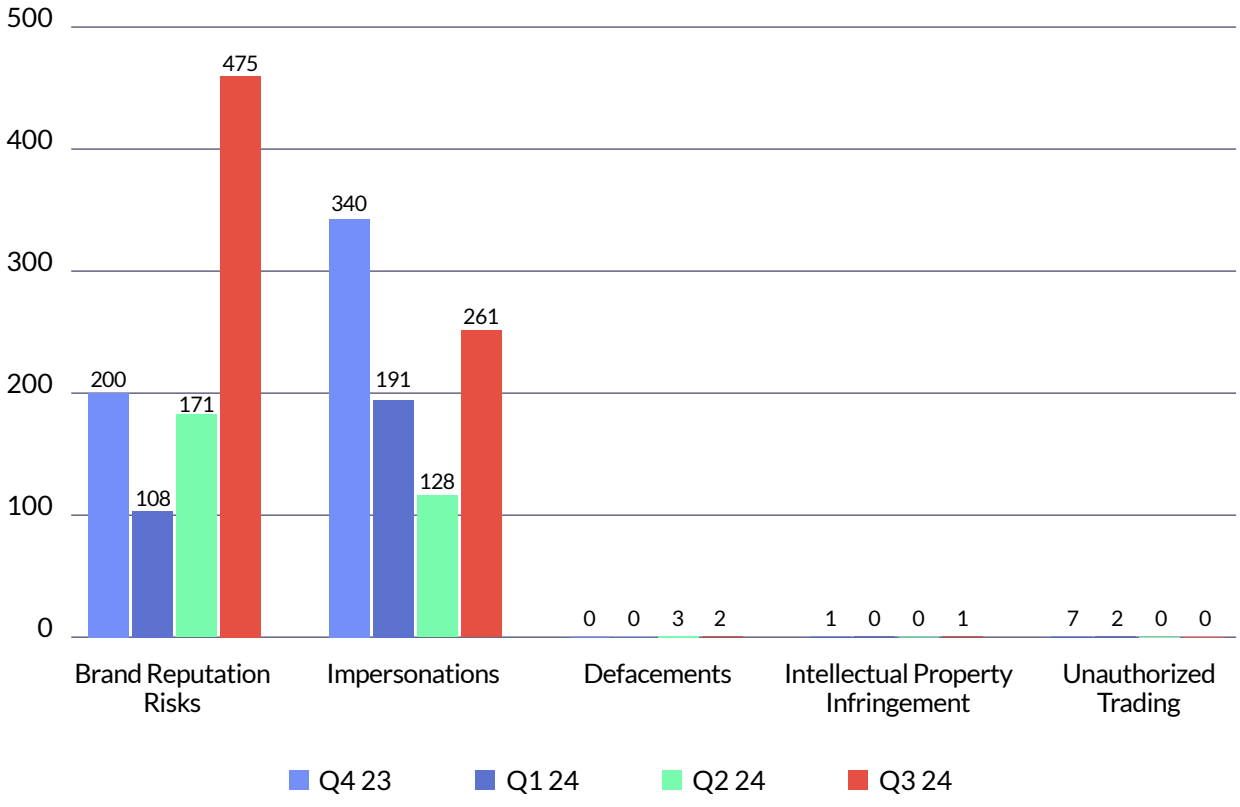
Cyberint Digital Brand Protection

Monitor for malicious brand impersonation across the open, deep, and dark web, identify suspicious behaviors, such as mentions of your brands and products in threat actor forums, and outsource takedowns to Cyberint to remove any illegal posting of proprietary information.

Cyberint can monitor the following:

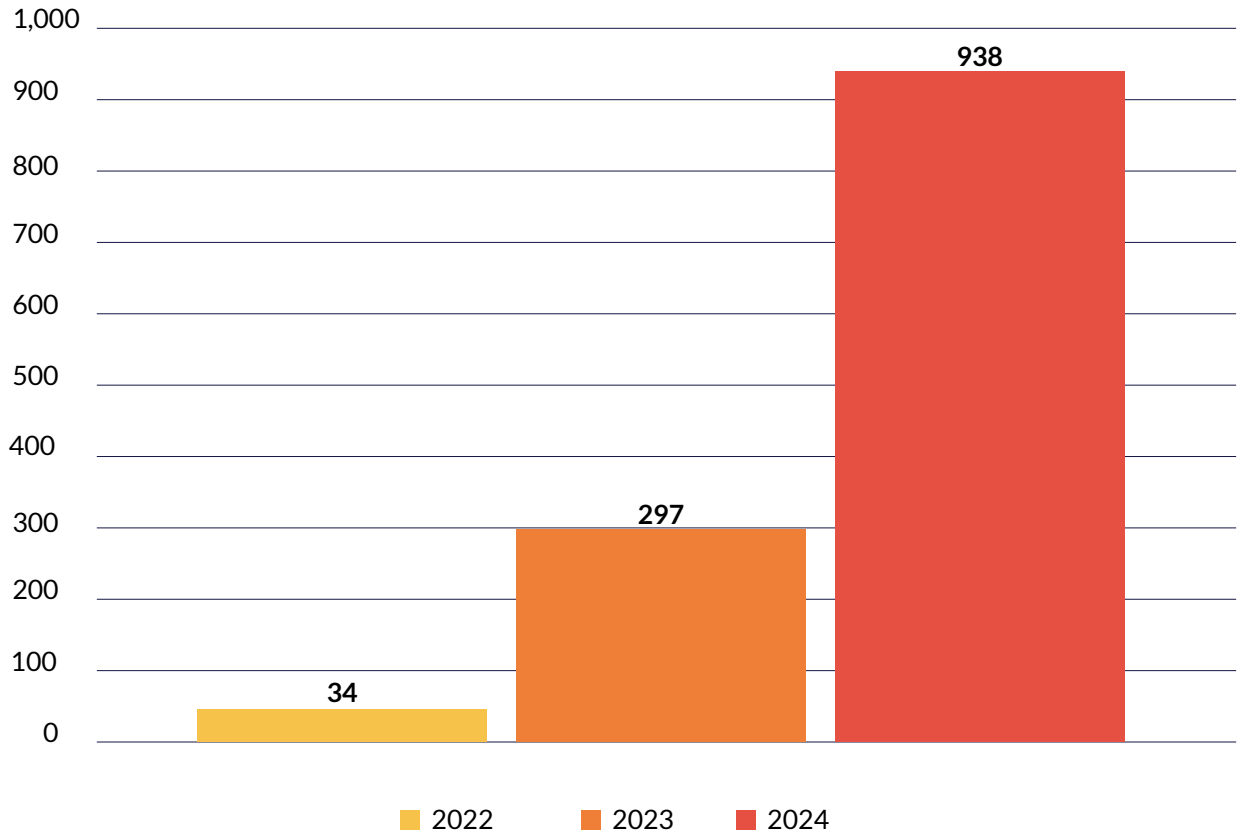
- *Brand reputation risks: Negative sentiments, unofficial distribution of mobile apps.*
- *Impersonations: websites and social media accounts impersonating companies and executives.*
- *Defacements.*
- *Unauthorized trading.*
- *Fake job postings.*
- *Intellectual property infringement.*

Top Brand Risks in 2024 Across Cyberint's Clients in Europe and the UK



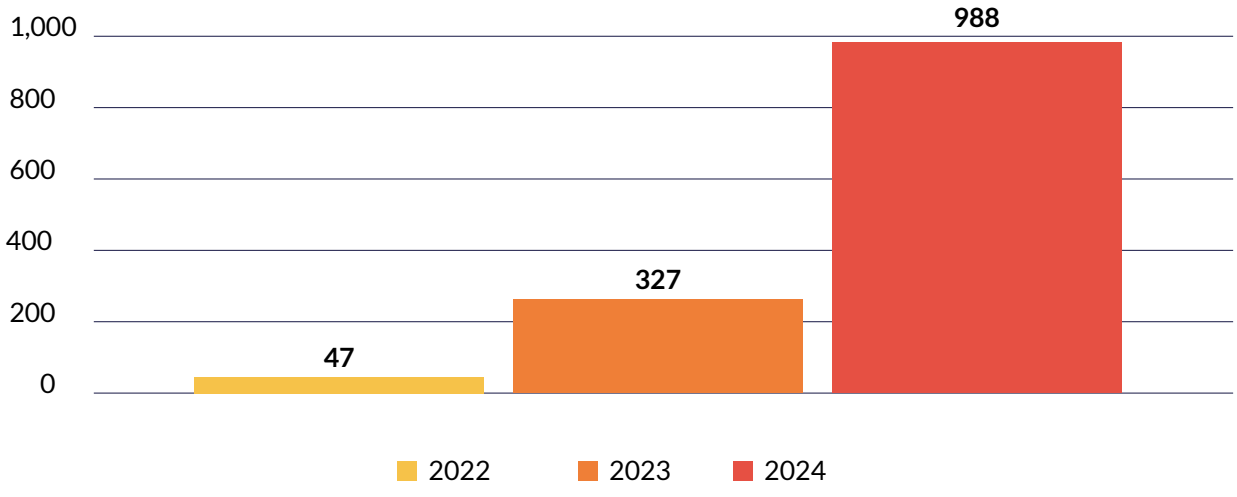
Key Insights

Impersonations

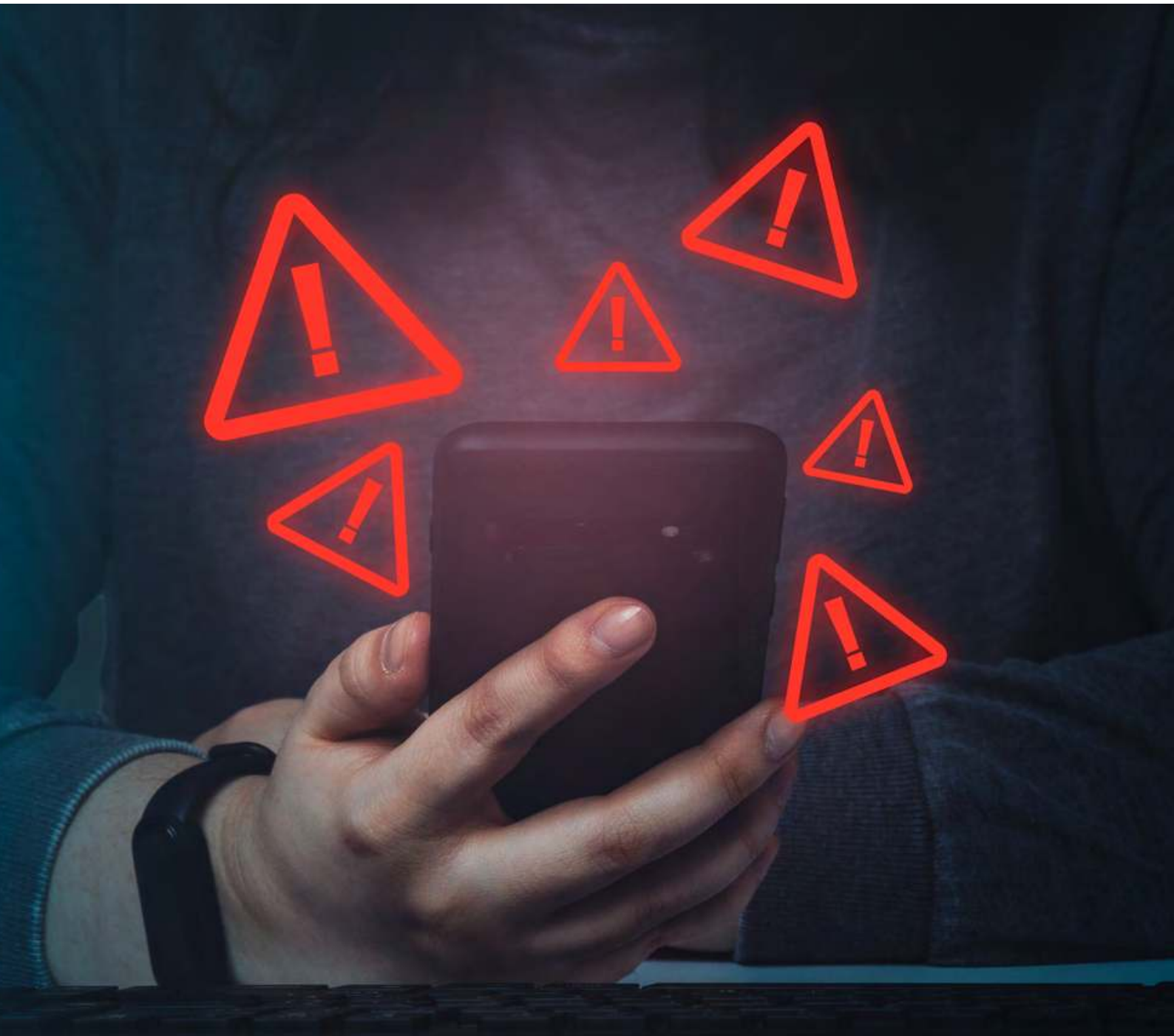


- Social media pages impersonating companies have become a prevalent tool for phishing and social engineering operations. Cybercriminals create fake profiles that closely mimic legitimate company pages, often using the same logos, branding, and tone of communication to deceive users into believing they are interacting with the official organization. These fraudulent pages are then used to spread phishing links, lure victims into providing sensitive information, or conduct scams, such as fake customer service interactions or investment schemes.

Unofficial Mobile Apps



- The distribution of unofficial mobile apps significantly increases the risk of **SDK (Software Development Kit) and API attacks,** which can lead to severe data leaks.
  - Unofficial apps often bypass the security checks imposed by official app stores, making them more likely to contain malicious or compromised SDKs. Threat actors exploit these apps by embedding harmful SDKs that can access sensitive information such as user credentials, financial data, or personal identifiers. Once installed, these SDKs can covertly collect and transmit data to unauthorized third parties without the user's knowledge.
  - They may also interact with legitimate APIs without proper security protocols, opening the door for threat actors to intercept API requests and responses, leading to man-in-the-middle (MITM) attacks; as well as leak API keys and expose API endpoints.

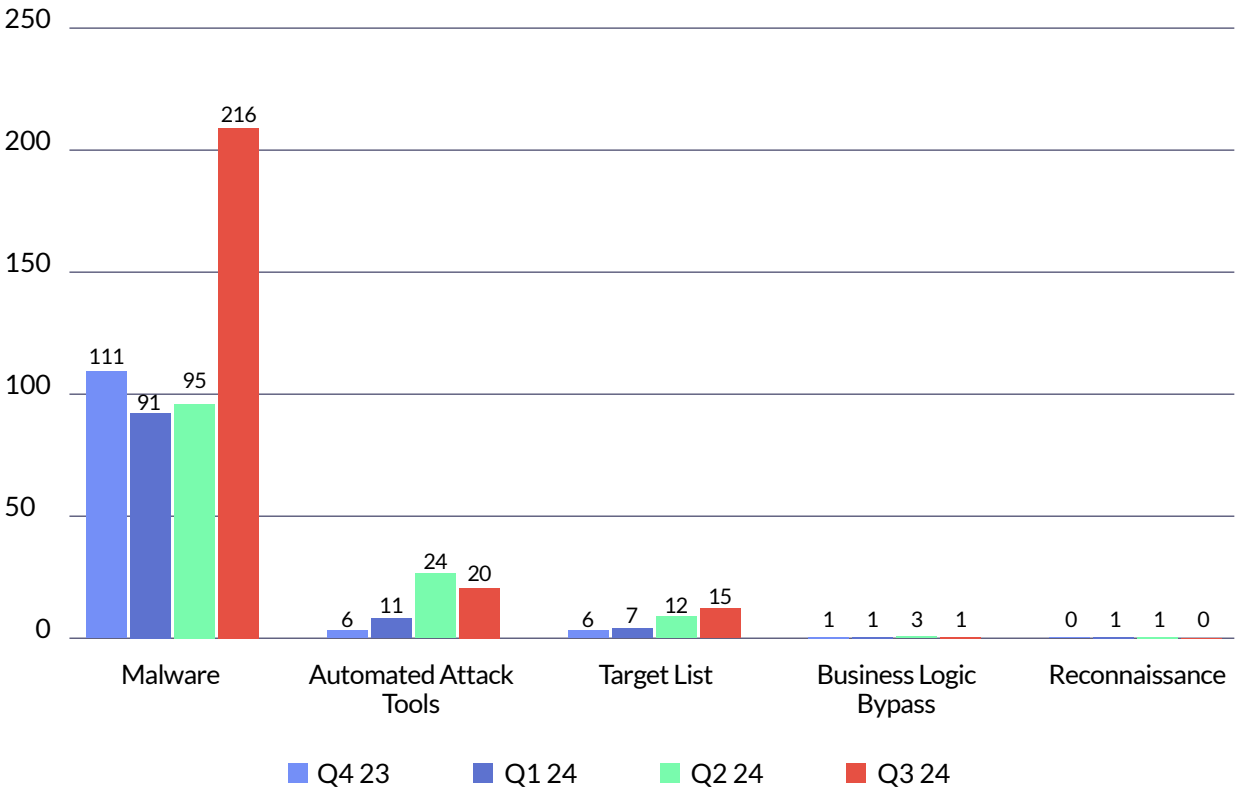


Attackware

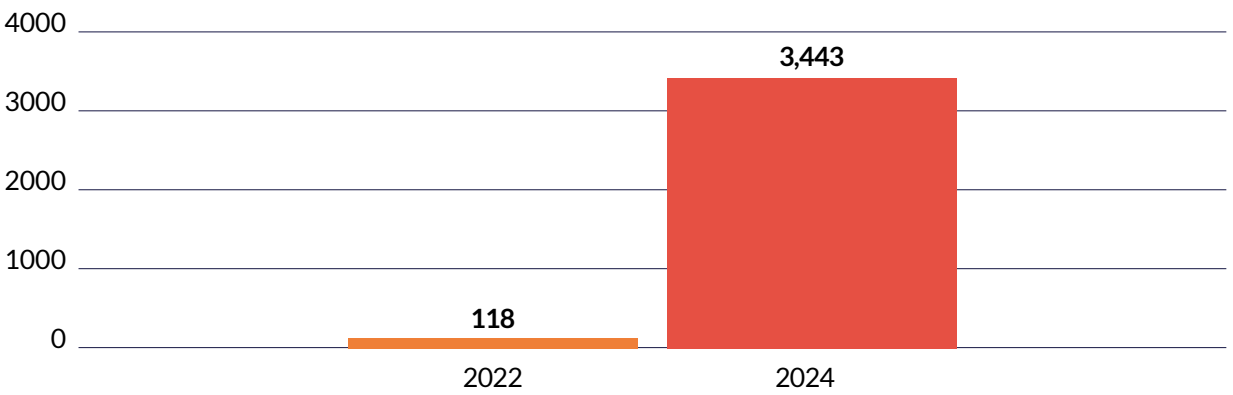
Cyberint Malware Intelligence

Cyberint continuously monitors forums, marketplaces and code repositories to detect and intercept various malware shared and sold by cyber criminals, help customers defend against these tools, and take them down in time. cyberint can identify the use of tools that systematically go through lists of credentials found in the dark web. Then, it automatically publishes alerts as these findings are detected.

Malware Risks in 2024 Across Cyberint's Clients in Europe and the UK



Malware risks surge within two years for Cyberint's clients in Europe and the UK



Infected Machines Lead to Data Breaches: European Air-Gapped Government Network Breached

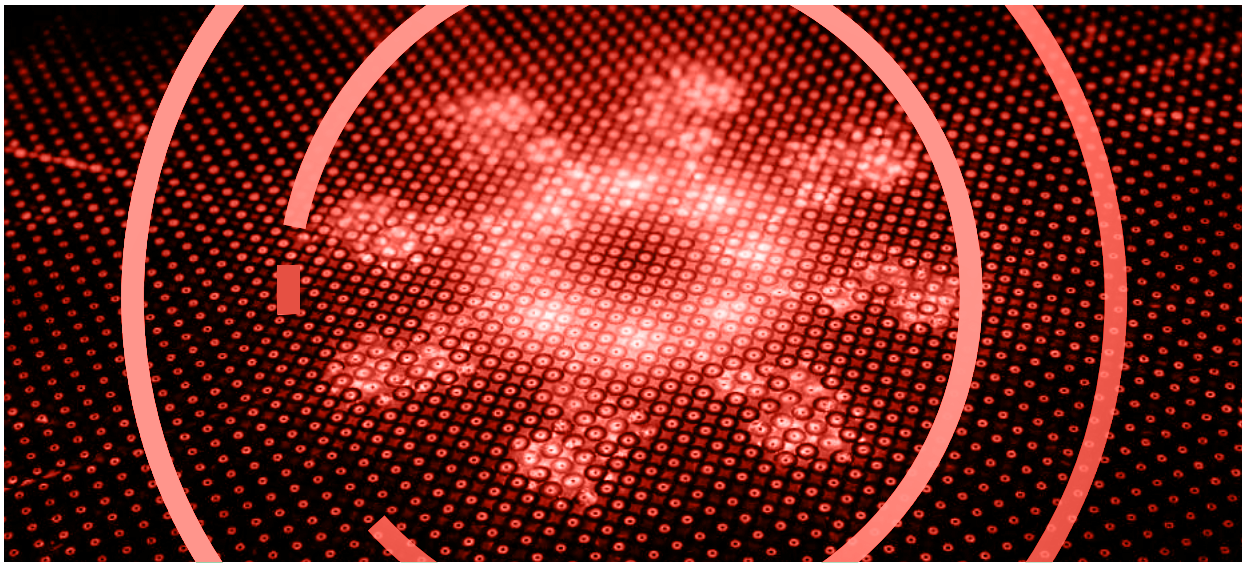
In October 2024, it was reported that APT group GoldenJackal was able to breach air-gapped government systems in Europe using two custom toolsets to steal sensitive data, such as emails, encryption keys, media files, and documents. the group executed these attacks on two separate occasions: one targeting a South Asian embassy in Belarus between 2019 and 2021, and another against a European government body from May 2022 to March 2024.

In May 2023, Kaspersky highlighted GoldenJackal's espionage-focused activities, which primarily target government and diplomatic entities. Although the group's use of custom USB-based tools, like "JackalWorm," was previously known, the successful compromise of air-gapped systems had not been confirmed until recently.

Air-gapped systems are typically isolated from networks to protect highly sensitive data, but GoldenJackal's attacks expose the vulnerabilities that still exist. The intrusion begins on internet-connected systems, where the GoldenDealer malware spreads through trojanized software or malicious documents. GoldenDealer automatically transfers itself to any inserted USB drives, which are then unknowingly used to infiltrate air-gapped systems.

When the compromised USB is plugged into the air-gapped machines, it installs GoldenHowl (a backdoor) and GoldenRobo (a data-stealing tool). GoldenRobo searches for sensitive data like encryption keys and confidential documents, storing them on the USB drive. Once the drive is reconnected to a networked machine, GoldenDealer sends the stolen data to the attackers' command and control server.

These breaches emphasize the **critical need to monitor malware trends, outputs, and manifestations in the dark web.** GoldenHowl, a versatile backdoor, enables persistence, vulnerability scanning, and communication with the attackers, highlighting the sophisticated methods used to compromise air-gapped systems.



Supply Chain

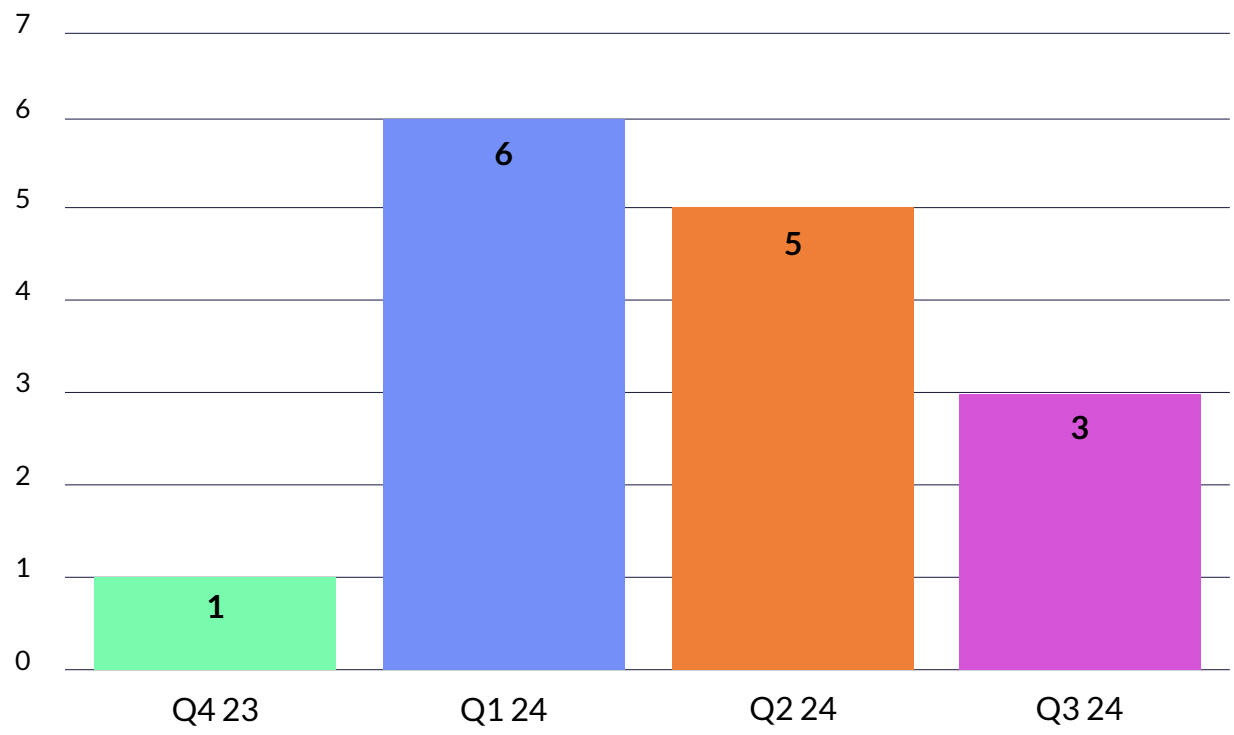
Cyberint Supply Chain Intelligence

Cyberint's Supply Chain Intelligence module automatically discovers the third-party technologies and vendors in your digital supply chain, continuously monitors these third parties, and assigns risk scores that leverage Cyberint's extensive open, deep and dark web intelligence. The module issues targeted alerts in real-time about the threats that may negatively affect your organization.

Key Insights

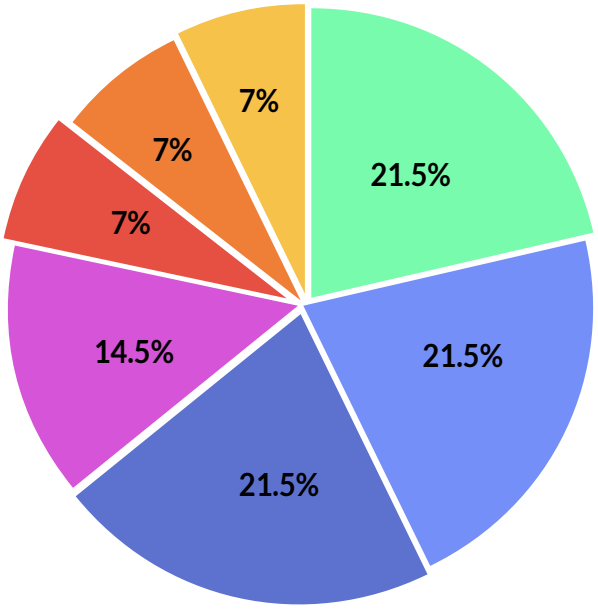
- The top three industries of compromised vendors in Europe and the UK are I.T./Technology, Insurance, and Financial Services.
- 84% of vendor incidents in 2024 were data breaches.

2024 Vendor Incidents



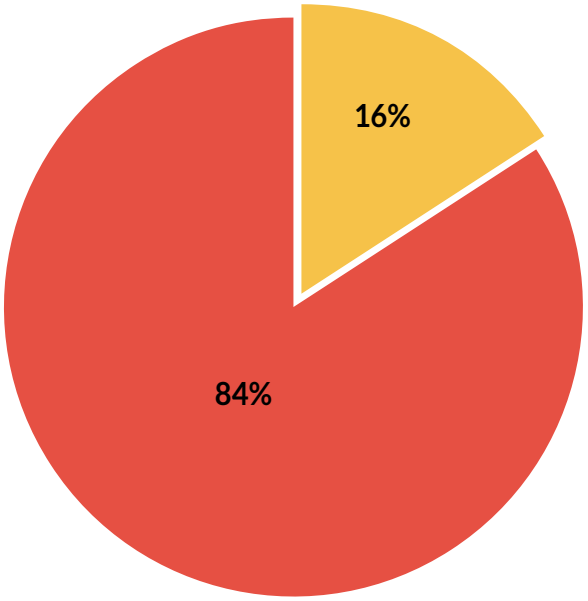
Industries of Compromised Vendors of Cyberint's Clients in Europe and the UK

- I.T.
- Insurance
- Financial Services
- Software
- Medical Technology
- Healthcare Services
- Cybersecurity



Incident Types That Affected Our Vendors

- Ransomware
- Breach



Compromised Vendors in Europe and the UK

Compromised Vendor	Industry	Date	Incident Type
ServiceNow	I.T. and Technology	October 2023	Breach
State Street	Financial Services	February 2024	Breach
Fiserv	Financial Services	February 2024	Breach
Prudential	Financial Services and Insurance	February 2024	Ransomware
Fujitsu	I.T. and Technology	February 2024	Breach
Microsoft	I.T. and Technology	April 2024	Breach
HOYA	Medical Technology	April 2024	Breach
Medibank	Health Insurance	May 2024	Ransomware
Synnovis	Healthcare Services	June 2024	Breach
Snowflake	I.T. and Technology	July 2024	Breach
Adobe	Software	July 2024	Breach
Crowdstrike	Cybersecurity	August 2024	Breach
TOTVS	Software	October 2024	Ransomware
Star Health Insurance	Health Insurance	October 2024	Breach

Looking Ahead: Emerging Threats and Priorities for 2025

Emerging Threats in 2025

As we look toward 2025, the cyber threat landscape will become increasingly complex, driven by rapid advancements in technology, shifts in work environments, and geopolitical tensions. Below are the key threats expected to dominate the cybersecurity space in 2025, which will require proactive planning and strategic response from organizations across industries.

AI-Enhanced Phishing and Social Engineering

Phishing attacks have long been a preferred tactic for cybercriminals, but with the integration of generative AI, these attacks will become far more sophisticated. Attackers will use AI to generate highly personalized phishing emails, texts, or social media messages, tailored to individual targets by analyzing publicly available data. These AI-powered phishing campaigns will be difficult to detect due to their human-like language, dynamic content generation, and ability to bypass traditional filters. Organizations will need to adopt advanced AI-based defense mechanisms that can identify subtle anomalies in communication patterns to combat this rising threat. Security awareness training will also need to evolve to equip employees to spot these highly convincing phishing attempts.

Supply Chain Vulnerabilities

Supply chain attacks—where attackers target vulnerabilities in third-party vendors or software suppliers—will continue to rise in 2025. As organizations increasingly rely on external vendors for critical operations, this interconnectedness presents a broader attack surface for cybercriminals. These attacks can disrupt entire supply chains, allowing adversaries to exploit weaknesses in software update mechanisms or third-party cloud infrastructure. We expect attackers to exploit these vulnerabilities to gain lateral access to corporate networks, steal sensitive data, or distribute malware. Continuous vendor security assessments, enhanced contractual requirements for cybersecurity standards, and real-time monitoring of supply chain activity will be essential for mitigating these risks.

Evolving Ransomware Tactics

Ransomware is expected to remain a dominant threat, evolving with even more sophisticated techniques. In 2025, we anticipate the use of AI-enhanced ransomware that can evade traditional detection methods by dynamically altering its behavior and encryption strategies. Attackers will continue to employ double and triple extortion schemes, not only encrypting data but also threatening to release sensitive information or target customers and partners unless a ransom is paid. This trend will also see the rise of Ransomware-as-a-Service (RaaS), where attackers lease out ransomware tools to lower-skilled threat actors. Organizations must implement zero-trust architectures, robust data encryption, and rapid incident response plans to minimize the damage of ransomware attacks and ensure quick recovery.

Exploitation of Hybrid Work Environments

The shift to remote and hybrid work models will continue to present significant security challenges in 2025. As employees access company resources from home networks, public Wi-Fi, and personal devices, attackers will exploit these often less-secure environments. Threat actors may use compromised home routers, infected personal devices, or poorly secured coworking spaces to gain access to corporate networks. The lack of centralized control over these environments leaves organizations vulnerable to a wide range of attacks, from malware infections to credential theft. To mitigate these risks, organizations will need to strengthen endpoint detection and response (EDR) systems, enforce virtual private networks (VPNs), and ensure that personal devices used for work meet strict security standards. Additionally, regular employee security training will be critical to reducing risky behaviors in remote work settings.

Threats from Uncontrolled Mobile/Web Apps and SDK Attacks

The unofficial distribution of mobile apps will increasingly lead to SDK-based attacks (attacks that exploit vulnerabilities within software development kits integrated into mobile applications). Attackers can distribute unofficial versions of legitimate apps that contain malicious SDKs capable of stealing user data, credentials, and other sensitive information. This poses a particular risk to both consumers and employees who may inadvertently download compromised apps outside of official app stores. Moreover, the growing use of mobile devices for work-related tasks increases the likelihood of corporate data being exposed via these apps. Organizations must enforce strict policies that limit the use of unofficial apps, implement mobile application management (MAM) tools to monitor app usage, and regularly audit mobile devices for compliance with security policies.

Geopolitical-Driven Cyber Warfare

As geopolitical tensions rise, nation-state-sponsored cyberattacks will become more frequent and sophisticated, targeting critical infrastructure, financial systems, and government organizations. These attacks will range from Distributed Denial of Service (DDoS) campaigns to cyber espionage and sabotage operations aimed at destabilizing national economies or critical industries. Cyber warfare could also involve targeting cloud services and operational technologies (OT), aiming to disrupt essential services like energy, healthcare, and transportation. For organizations, this will mean fortifying their defenses against nation-state attackers, including bolstering cyber resilience measures and working closely with governmental and cybersecurity agencies to share intelligence and mitigate threats.

Top 5 Priority Areas for CISOs

1

AI-Powered Phishing Defense. With generative AI driving the next wave of highly sophisticated phishing and social engineering attacks, CISOs must prioritize enhancing email and communication security. This includes deploying advanced AI-driven detection systems, automating threat identification, and training employees to recognize increasingly convincing phishing attempts.

2

Supply Chain Security. The rise in supply chain attacks targeting third-party vendors poses a significant threat to organizations. CISOs need to implement stringent vendor management protocols, conduct continuous security audits, and ensure that supply chain partners adhere to robust cybersecurity standards to reduce vulnerabilities from external sources.

3

Advanced Ransomware Resilience. As ransomware tactics evolve, including multi-layered extortion and AI-driven evasion techniques, building resilience against these attacks should be a top priority. CISOs should focus on multi-factor authentication (MFA), regular data backups, segmented network architectures, and real-time threat intelligence to mitigate the impact of ransomware incidents.

4

Securing Remote and Hybrid Work Environments. With hybrid work models becoming permanent, protecting employees' home networks, personal devices, and endpoints must be a core component of the cybersecurity strategy. Implementing robust endpoint detection and response (EDR) solutions, virtual private networks (VPNs), and security awareness training will help safeguard remote access to corporate resources.

5

Proactive Monitoring of App Ecosystems. The proliferation of unofficial mobile apps presents a growing risk of data breaches through SDK- and API-based attacks. CISOs must prioritize monitoring their app ecosystem, enforce strict policies around mobile and cloud app usage, and implement advanced cloud security frameworks to prevent unauthorized data exposure.

Contact Us

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972 3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
3rd Floor, Great Titchfield House
14-18 Great Titchfield Street,
London, W1W 8BD

USA – TX

Tel: +1-646-568-7813
7250 Dallas Pkwy STE 400
Plano, TX 75024-4931

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 02210

JAPAN

Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm