Cyberint
A Check Point Company

Europe Retail Threat Landscape - 2024 Overview

January 2025

TABLE OF CONTENTS

INTRODUCTION

As one of the world's largest and most advanced economic regions, the European region consists of 37 countries including the 27 European Union (EU) countries. With some of the most important economies in the world, Europe remains a prime target for cyber adversaries and state actors. The retail industry faces a constantly evolving array of threats among its major sectors. The rise of e-commerce and the increasing volume of digitally collected and stored customer data have made retailers particularly vulnerable to cyber attacks.

This report examines the current threat landscape in the retail sector, identifying the most pressing threats, such as data breaches, ransomware, and supply chain attacks. We will also aim to provide strategies to mitigate these risks.

WHY EUROPE?

The EU represents one of the most important economic regions of the world with a GDP of $18.3 billion USD[1], and it is one of the leading trade entities worldwide representing 14.8% of the world's exports share, and 14.2% of the world imports share.

Europe, and particularly the retail industry is still an attractive region for cyber criminals mainly due to the following reasons:

Strict Data Protection. Put in effect on 2018, The General Data Protections Regulation (GDPR) is a comprehensive and very strict privacy law that imposes obligations onto organizations in the EU and everywhere in the world if they collect data related to people in the EU. This law penalizes the transgressors with harsh fines, in some recent cases those fines reached the outstanding amount of €1.2 billion[2]. This makes it extremely persuasive for threat actors when negotiating with companies whose data has been breached and are facing potential fines of such caliber; creating leverage for the attackers and making enterprises more likely to comply with ransomware demands to avoid legal, and financial repercussions.

Highly Integrated Market. The EU's spirit of an integrated market that facilitates the free movement of goods and services brings many benefits for businesses. It also makes it a central hub for global supply chains where many retailers can source and distribute their products internationally. However, this key benefit can also be exploited by malicious entities, meaning that a successful attack on one retailer or a vendor that is part of the organization's supply chain can quickly create a domino effect across borders amplifying the attack's impact by targeting and impacting multiple organizations simultaneously, using the EU's interconnected market and its position as a global trade point.

---

[1] EU GDP for 2023, https://www.macrotrends.net/global-metrics/countries/EUU/european-union/gdp-gross-domestic-product#:~:text=European%20Union%20gdp%20for%202022,a%201.99%25%20decline%20from%202019.

[2] https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

Diverse Cultural Landscape. European Retailers often operate in cultural and linguistically diverse regions, that requires them to adapt their systems and platforms to local markets in various languages and law requirements. This level of complexity creates a scenario where cyber security measures can be mistakenly overriden or forgotten, making it easier for threat actors to exploit weaker points in their digital infrastructure.

Broad use of digital payments systems. The EU has a high adoption rate of digital payments systems and contactless technologies [3]. Even though every time these systems are more robust and secure, there is an immense attack surface that creates opportunities for cyber criminals to exploit it via POS Malware, phishing campaigns, fraud targeting digital wallets and payment platforms.

Increased Attack Surface and Exposure. The technological ecosystem required to support retail operations is big and complex, for example, just the amount of Point of Sales terminals (POS) has risen to around 20.6 million in 2023 [4]. E-commerce is also challenging in terms of the number of customers that can be reached through phishing attacks, with the increase of E-commerce in the region.

[3] https://www.statista.com/outlook/fmo/digital-payments/europe

[4] https://www.statista.com/statistics/444944/number-of-pos-terminals-the-european-union/

RANSOMWARE & RETAILERS IN EUROPE

Based on data collected by Cyberint, in 2024 the most targeted industries in Europe were Business Services, Retail and Manufacturing with over 800 incidents reported. Even though Business Services is still the most attacked industry, the biggest surge in incidents was on Retail, where we detected an increase of 22% in the same period.

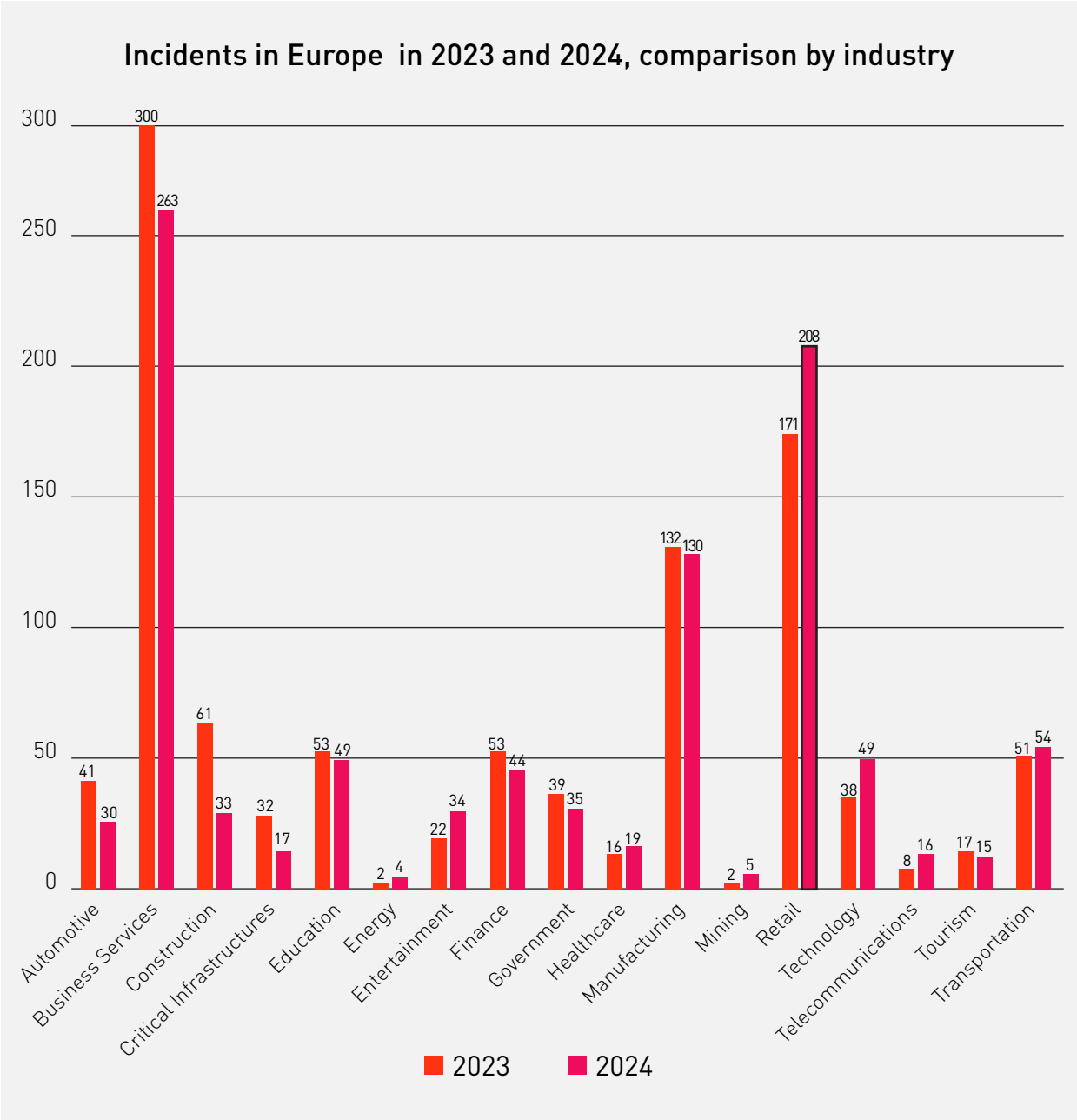


Figure 1: Incidents in Europe in 2023 and 2024, comparison by industry

An in-depth analysis on ransomware incidents reveals that the most targeted countries in Europe during 2024 in the retail industry are the same as in 2023, France, Germany, Italy, Spain, and UK counting over 67% of the total incidents in those five countries alone. However, the biggest increase this year has been in Spain and the UK with a significant spike of 100% and 20% (UK) in incidents reported in that span of time.

Figure 2: Most targeted countries within the retail industry, 2023 and 2024

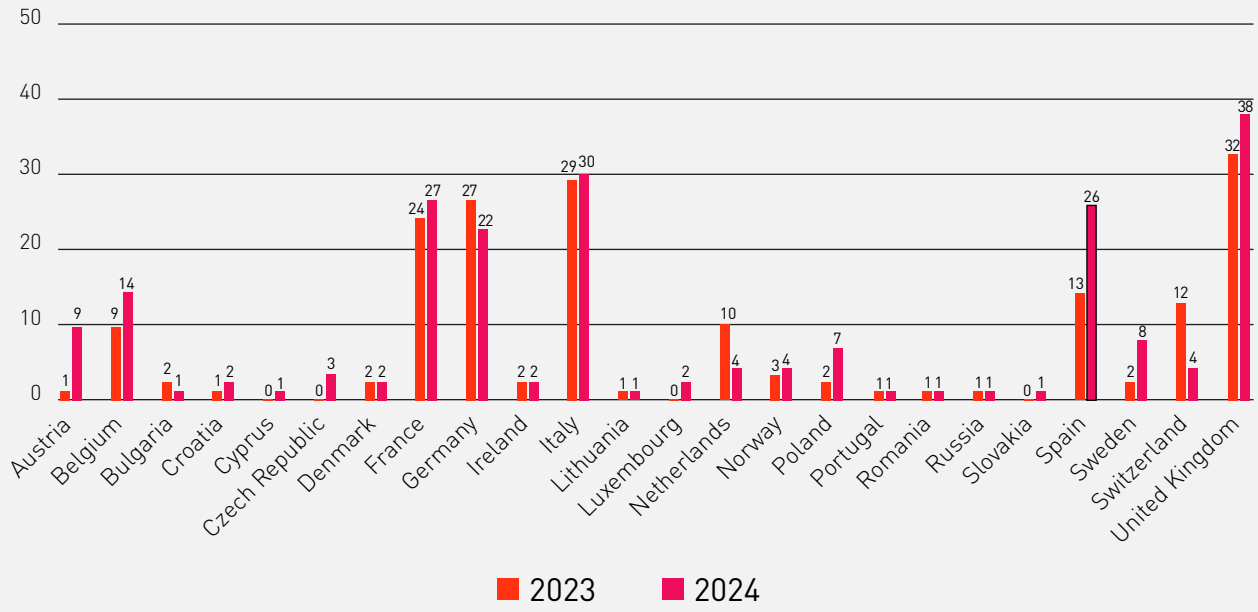


Figure 2: Most targeted countries within the retail industry, 2023 and 2024

RANSOMWARE GROUPS LANDSCAPE

Regarding Threat Actors, our research shows an increase of 23% in the number of malicious groups attacking European companies, for example "Ransomhub" and "Hunters", which are attempting to enhance their reputation and stand out among other ransomware groups. It's worth noting that prominent ransomware groups' activities from 2023 are dropping and, this is attributed to law enforcement activity against major players such as Lockbit[5] and AlphV/Black Cat[6] during 2023-2024.

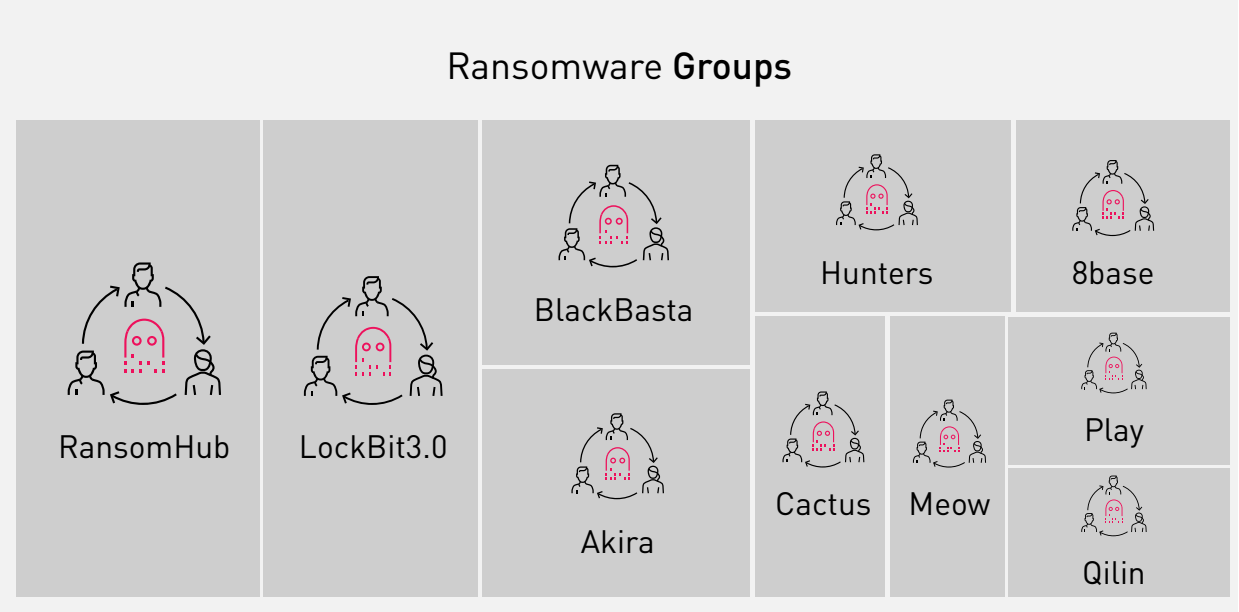


Figure 3. Top 10 ransomware groups targeting European countries 2024

CLOP RANSOMWARE GROUP RETURNS

The Clop Ransomware group, also known as Cl0p, first appeared in February 2019 and has since targeted a wide range of industries globally, including retail, manufacturing, energy, healthcare and financial services among others. In recent months, this ransomware group has resumed operations, once again listing victims on its site.

In 2023, they accounted for 384 successful breaches. However, in 2024, the group has only posted 27 victims on the site. In December 2024, Clop intensified its campaign, publishing more than 60 companies allegedly affected by their most recent attack and giving them a 48 hour deadline to meet their ransom demands.

[5] EU.S Department of Justice. Office of Public Affairs | U.S. and U.K. Disrupt LockBit Ransomware Variant | United States Department of Justice

[6] U.S. Department of Justice. Office of Public Affairs | Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant | United States Department of Justice

RANSOM PAYMENTS

Ransomware continues to be one of the most destructive cyber threats worldwide, impacting virtually every industry and region. However, in the first quarter of 2024, a notable shift was observed in the landscape of ransomware attacks. The amount of ransom paid to cybercriminals dropped significantly, with the proportion of victims who paid falling to an all-time low of 28%. This trend, while encouraging, reflects a complex shift in the dynamics between attackers and organizations. Several key factors are likely contributing to this decline in ransom payments:

1

Improved cyber-resilience:

Organizations are becoming increasingly better at enduring ransomware attacks, thanks in large part to advancements in their cyber resilience strategies. Many businesses now employ robust disaster recovery plans (DRPs) that include frequent and secure data backups stored in isolated environments. These backup systems, which are often automated and tested regularly, provide organizations with a way to recover from an attack without capitulating to ransom demands.

Additionally, many organizations have established incident response teams that can act quickly to contain an attack and minimize damage, further reducing the pressure to pay a ransom. This shift towards proactive defense mechanisms reflects a growing recognition that the cost of recovery can often be less than the ransom itself, especially as cyber criminals continue to evolve their tactics. Still, the risk of a reputational hit is something most companies need to address when calculating the financial implications of paying a ransomware attack, even with a strengthened cyber security infrastructure; businesses must also consider the long-term damage to their brand image and customer trust.

2

Increased law enforcement and governmental action:

Another significant factor contributing to the decline in ransom payments is the heightened activity of law enforcement agencies and governments taking down ransomware groups. Efforts such as the European Union's coordinated law enforcement operations, the FBI's ransomware task force, and major operations such as the takedown of LockBit during Operation Cronos,[7] have had a noticeable impact on the ability of cyber criminals to operate with impunity. The arrests of key figures within ransomware gangs, coupled with the seizure of their infrastructure, has made it riskier for cyber criminals to launch successful attacks.

This heightened legal pressure may also deter victims from paying ransoms, as they recognize that law enforcement may be more likely to pursue avenues for recovery and apprehension of the perpetrators.

[7] Law enforcement disrupt world's biggest ransomware operation | Europol

3

Fragmentation of the ransomware ecosystem:

The ransomware landscape has also seen a shift towards more fragmented and less organized ransomware groups. In the past, high-profile cyber crime syndicates like REvil or DarkSide were the primary actors behind many of the largest ransomware attacks. However, in 2024, there has been a rise in smaller, less trusted ransomware groups operating in a more decentralized and opportunistic manner.

These groups often lack the sophistication, resources, or follow-through on promises to provide decryption keys after payment. The growing perception of these groups as less reliable or trustworthy may discourage victims from negotiating or paying ransom, as they face the risk of being scammed or reinfected. This decentralization has led to a decrease in overall payments, as companies may be more inclined to reject ransom demands.

4

Increased awareness of the risks and consequences of paying ransoms:

As the cybersecurity landscape has evolved, there has been a growing awareness among organizations about the long-term consequences of paying ransoms. These risks include data reinfection (where cybercriminals attack again after payment), the funding of further criminal activities, and the potential for reputation damage.

High-profile cases where victims paid ransoms only to face additional attacks or where ransoms were linked to financing other illicit activities have further highlighted the dangers. Moreover, after successfully conducting Operation Cronos, law enforcement agencies find out that the seized infrastructure of Lockbit contained copies of data stolen from victims who had paid the demanded ransom, even though the LockBit perpetrators had falsely promised those victims that they would delete the victims' stolen data after the ransom was paid.[8]

Many businesses are now turning to alternative recovery methods, such as cyber insurance or decryption toolkits provided by law enforcement or cybersecurity firms, to avoid engaging with cybercriminals.[9, 10]

---

[8] US Department of Justice: https://www.justice.gov/opa/media/1381806/dl

[9] Home | The No More Ransom Project

[10] #StopRansomware Guide | CISA

Despite the overall decline in ransom payments, 2024 witnessed the largest known ransom payment in history. Cencora Inc., a major drug distributor, paid $75 million USD to the Dark Angels ransomware group, nearly doubling the previous record ransom payment. This case serves as a reminder that while many organizations are becoming more resilient and reluctant to pay ransoms, certain industries or high-value targets may still be susceptible to paying large sums to secure their data. The vast sums involved in such payments underscore the massive financial risks companies face when they lack effective prevention and mitigation strategies. This high-profile case could set a precedent for other attackers, possibly leading to larger and more aggressive ransom demands in the future. Cyber criminal groups are likely to focus on fewer, but more lucrative targets, potentially shifting from widespread attacks to focused, high-stakes extortion schemes. This is particularly true as larger organizations with sensitive data and operations become prime targets for cyber criminals looking to extract significant sums. Ransomware-as-a-Service (RaaS) platforms may further enable this trend by allowing less skilled attackers to execute highly targeted attacks with sophisticated tools and infrastructure.

[11] Forbes: Record-Breaking $75 Million Ransom Paid To Dark Angels Gang

[12] Cencora pays $75 million in Bitcoin in the largest known case of ransomware attack

[13] Largest Ransom Ever Paid: Fortune 50 Co pays Unprecedented $75 Million

SUPPLY-CHAIN THREATS

In 2023 and 2024, the topic surrounding supply chain threats almost became synonymous with discussions surrounding ransomware, as many high-profile data leaks in the past two years were due to supply chain vulnerabilities that ultimately led to ransomware. This trend is also shown in OpenText's 2024 Cyber security survey[14] which found that 62% of respondents experienced a ransomware attack originating from a supply chain partner.

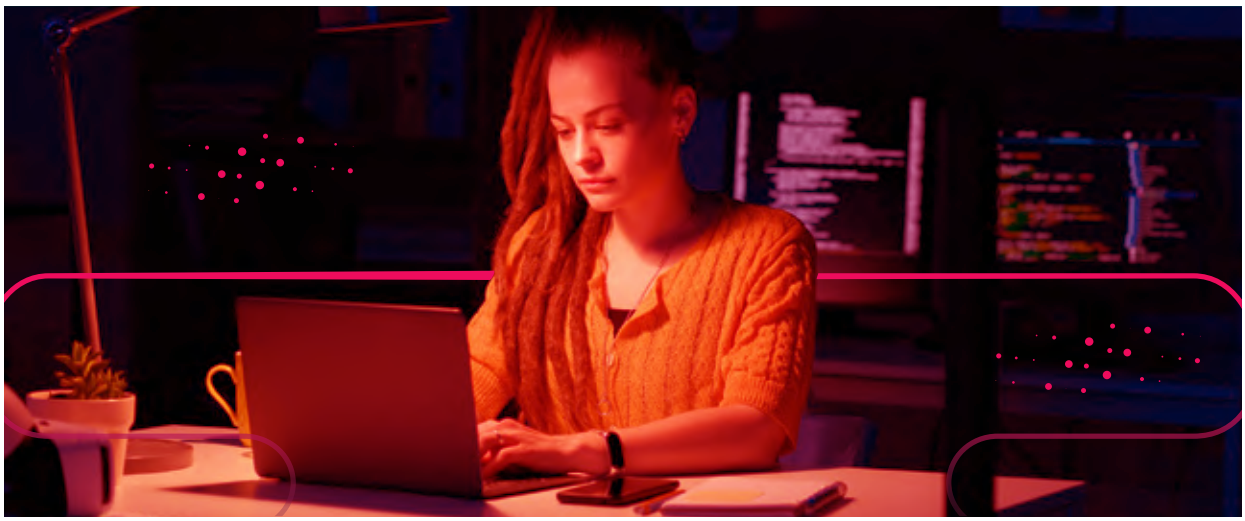
One such example of the effect of Ransomware on the retail sector is the attack on Blue Yonder in November 2024. Blue Yonder (formerly JDA Software Group) is an American supply chain management company operating as an independent subsidiary of Panasonic. On the 21st of November it disclosed that it suffered a Ransomware attack that at the time no Ransomware group took credit for. The company has more than 6,000 employees and over 3,000 customers across 76 countries and serves a variety of industries, including retail, manufacturing, and distribution. Its list of over 3,000 customers includes other high-profile companies like Microsoft, Renault, Bayer, Tesco, Lenovo, DHL, 3M, Ace Hardware, Procter & Gamble, Carlsberg, Dole, Wallgreens, Western Digital, and 7-Eleven.

[14] https://www.opentext.com/about/press-releases/opentext-cybersecurity-2024-ransomware-survey-supply-chain-attacks-surge-ransom-payments-persist

One of the immediate effects of the attack on Blue Yonder was on the retail sector. This incident has led to a wave of outages affecting customers using the company's software, including the U.S. coffeehouse chain Starbucks and the Morrisons and Sainsbury's supermarket chains in the United Kingdom. Due to disruptions affecting Blue Yonder's managed services hosted environment, Starbucks said it was forced to pay baristas manually as the software tracking work schedules across over 10,000 stores was affected.

French pen manufacturer BIC was also hit by shipping delays, while Morrisons revealed that the incident impacted its warehouse management systems for fresh foods. Morrisons, uses Blue Yonder's demand forecasting and replenishment solution software primarily for fresh produce and chilled foods, and has reverted to a manual back-up system. Morrisons suppliers have also reported being unable to deliver stock to depots.

As a result, Morrisons warned its wholesale and convenience customers that availability on some lines may drop as low as 60%. Sainsbury's is also understood to be impacted. It's just completed in 2024 the rollout of a comprehensive new 'Supply Chain Transformation Programme' to implement its demand forecasting, store ordering and fulfillment solutions across its fresh, frozen and ambient categories, which was impacted directly by the Blue Yonder attack.[15]



In addition to the usual threats via privileged access through unsecured supply chain vectors, social engineering attacks that abuse the relationship between the third-party vendor and the client are also noteworthy. Therefore, remaining vigilant against social engineering attacks following a data leak or significant outage is important. Additionally, supply chain breaches provide threat actors with opportunities to gather intelligence on the company, including knowledge of specific contracts and agreements and potential email correspondence history, which could be leveraged in their social engineering campaigns as it would make them seem more trustworthy.

Threat actors will persist in exploiting any vector that gives them an advantage in social engineering tactics to breach an organization.

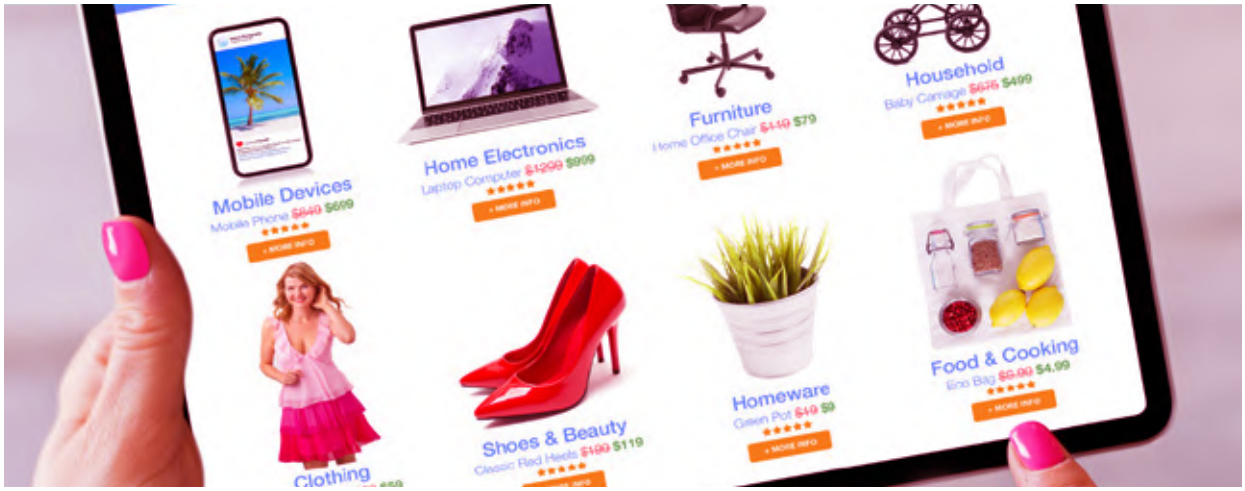
---

[15] Blue Yonder software hack impacting supermarket supply chains | The Grocer

Key Policy Recommendation and Considerations:

It is imperative to conduct risk analyses of supply chain vendors and stay vigilant for social engineering attacks following a third-party breach, especially those that have business relations with the organization. Consider the following:

- Temporarily blocking communications to a third-party vendor after a breach (depending on its severity and access).
- Attach an automated warning temporarily to any emails received from an affected vendor to warn employees of the breach, and its implications.



ECOMMERCE PLATFORMS

It is no coincidence that the top targeted countries of 2023 are the same as in 2024, hence 86% of all online spending in Europe is concentrated in five countries, France, Germany, Italy, Spain and the UK. Their contributed revenue alone is €598.1 Billion.[16]

1. **The United Kingdom:** The UK, with a population of 67.9 million, is expected to have around 62.1 million E-commerce users by 2025. The country generates over €254 billion in E-commerce revenue, with €129.5 billion coming from consumers.[17] Despite its relatively small size, the UK is the top spender in online purchases in Europe, allocating 10.26% of its GDP to E-commerce. The most popular marketplaces in the United Kingdom are: Amazon, eBay, Etsy, Argos.

2. **France:** In 2023, France had over 51 million E-commerce users, with more than 5% of its GDP directed towards E-commerce spending. Marketplaces and other platforms revenue is expected to reach €60.91 billion in 2024 and shows an annual growth rate of 7.93% (2024-2029), resulting in a projected market volume of €89.20 billion by 2029[18]. The most popular marketplaces in the France are: Amazon, Aliexpress, Cdiscount, eBay.

---

[16] Channel Engine: The top 14 European marketplaces in 2024

[17] Statista: eCommerce - United Kingdom | Statista Market Forecas

[18] Statista: eCommerce - France | Statista Market Forecast

3. **Germany:** With over 67.9 million online customers, Germany's E-commerce revenue is estimated at €90.22 billion in 2024, with an increase of 8.8% and expected number of users to 51.8 million by 2029[19]. The most popular marketplaces in Germany are: Amazon, eBay, Otto, and Temu.

4. **Spain:** In a country of 46 million people, Spain has 33.8 million E-commerce users, with a projected revenue in 2024 of €32.58 billion, with an expected spending of €45.9 billion by 2029[20]. The most popular marketplaces in Spain are: Amazon, El Corte Ingles, Aliexpress, and Temu.

5. **Italy:** With a projected revenue of €58.90 billion in 2024 that represents an increase of 13% with the previous year, the current 31.7 million E-commerce users are expected to increase up to generate a annual growth rate of 9.77% and a €93.88 billion projected market volume by 2029. The most popular marketplaces in Italy are: Amazon, Temu, Aliexpress, and Etsy.

Figure 4: Most Impersonated domains for leading E-commerce websites 2022

[19] Statista: eCommerce - Germany | Statista Market Forecast

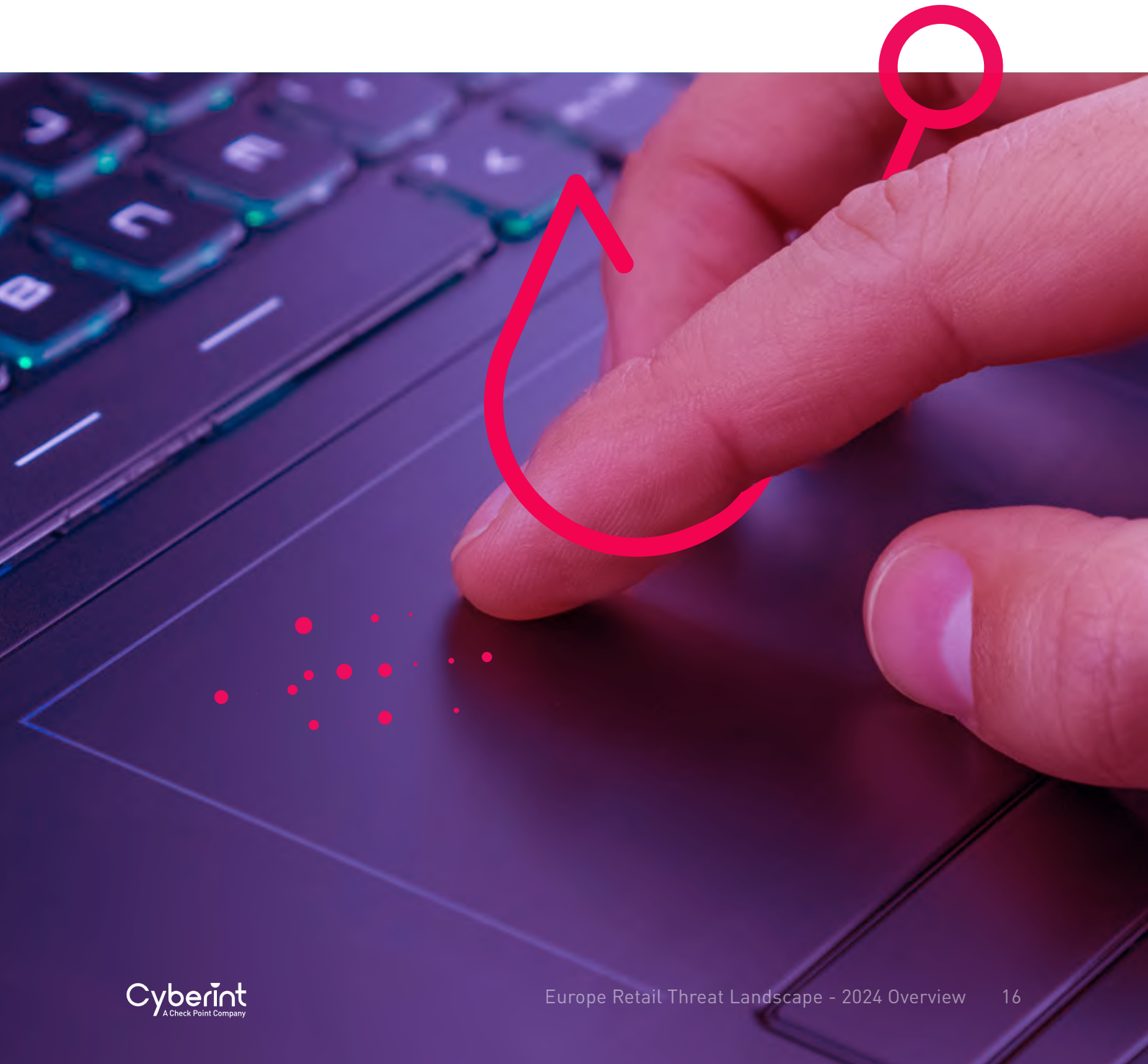
[20] Statista: eCommerce - Spain | Statista Market Forecast

The most common marketplaces are also the most popular targets for phishing or smishing attempts due to their widespread use and popularity among the public. However, other types of services related to E-commerce are also commonly featured in phishing kits, especially logistics and delivery services. There are several reasons why this type of services are so effective for phishing campaigns:

- **Timing and Urgency:** Many people are expecting a package, so an email or message about a missed delivery or shipping delay creates a sense of urgency and compels the recipient to act quickly without carefully verifying the message.

- **Emotional Manipulation:** When a scam is framed around something people are excited or anxious about, such as receiving a package, it significantly increases the chances of a successful phishing attempt.

- **Impersonation of trusted brands and marketplaces:** Pairing a well-known logistics company with a popular E-commerce brand or marketplace enhances the credibility of a phishing attempt, making the victim more likely to trust it.



For retail companies with a presence on E-commerce platforms, preventing fraud is a significant challenge. Businesses face various types of fraudulent activities, which can impact both their revenue and customer trust. Some of the most common types of fraud attacks that online retailers encounter include:

- **Account Takeover Fraud:** This happens when an unauthorized party gains access to a customer's account, often through phishing or brute force attacks. Once in control, the fraudster can make unauthorized purchases or change account details to redirect shipments or funds.

- **Card Testing Fraud:** Cyber criminals attempt to validate a stolen credit card by making small, low-value transactions. The objective is to verify if the card is still active and functional, which can later lead to bigger purchases.

- **Friendly Fraud:** This occurs when legitimate customers make online purchases and then dispute the transaction with their bank, claiming that they never made the purchase or that the product was never received. This type of fraud can be particularly difficult to detect, as the fraudster is typically the genuine cardholder.

- **Interception Fraud:** Cyber criminals monitor and hijack a legitimate transaction, usually by intercepting the delivery address during the checkout process. This allows them to redirect the purchased goods to an address under their control

- **Refund Fraud:** In this case, criminals purchase goods online and then claim that the products are defective or not as described, seeking a refund or chargeback. This can be a major issue for retailers, especially if the fraudster manages to return counterfeit or stolen goods.

- **Triangulation Fraud:** In this fraud scheme the criminal sets up a fake online store, attracts customers with low prices, and then uses stolen credit card information to fulfill orders. Once the customer's order is completed, the fraudster uses the stolen card data to make the purchase from a legitimate retailer and pockets the difference between the inflated price on the fake site and the actual cost of the product from the legitimate merchant. The consumer receives the item but is unaware of the fraudulent scheme, while the legitimate merchant may suffer chargebacks or financial losses.

MALWARE INFECTION VECTORS

Retailers manage large amounts of customer data, including personal information, payment details, and purchase history, making them prime targets for cyber criminals. A malware attack can disrupt operations, steal sensitive data, and cause severe financial and reputational damage. In recent years, as the retail industry increasingly embraces digital transformation and omnichannel strategies, the attack surface for malware has grown exponentially. Retailers are now heavily reliant on online platforms, mobile apps, and E-commerce solutions, all of which can be vulnerable to malware targeting these digital environments. Failing to recognize and secure these potential vectors exposes retailers to other serious risks, including ransomware attacks and data breaches.

In 2024, Cyberint observed various methods employed by threat actors to compromise potential victims. These strategies were identified through darknet communications, instructional guides, tutorials, and use cases shared by clients and cyber security practitioners.

UTILIZATION OF TRUSTED PLATFORMS

In 2024 Cyberint, now a Check Point company, observed the abuse of trusted platforms for malware distribution. For instance, malware payloads were distributed via GitHub comments, where the download links or payloads evaded endpoint system detection. Additionally, encrypted emails and platforms such as Dropbox were utilized to distribute malware, successfully bypassing firewalls in some cases.

These observations indicate that threat actors have identified that exploiting platforms trusted by endpoint systems and firewalls increases their chances of evading initial detection, thereby providing more opportunities to infect victims.

```
https://github[.]com/microsoft/vcpkg/files/14125503/Cheat.Lab.2.7.2.zip
https://github[.]com/microsoft/STL/files/14432565/Cheater.Pro.1.6.0.zip
```

Figure 5: GitHub Comments Distributing Malware Hosted on Microsoft's Official GitHub Repository

INFO STEALER MALWARE

Information stealers or stealer malware are a type of malware designed to steal sensitive data such as financial information, credentials, and sensitive personal data. Moreover, Info stealers do not only steal credentials, but also cookies that may enable them to bypass multi-factor authentication.

Information stealers can spread through phishing emails, malicious software downloads, and other means, making it important for retailers to have robust security measures in place to protect their customers' and employees' sensitive information.

Stealer malware will continue to be a prominent risk among all industries due to its successful implementation of the Malware-As-A-Service nefarious strategy.

Top Affected Countries in Info Stealer Malware

The top 10 affected countries in Europe remain the same as in 2023, still the most affected country in 2024 was Spain, with Germany on a very close 2nd place. One of the most common vectors for info stealer infection are through downloading pirated software which are more prominent among the European countries.

Figure 6: Top 10 Affected European Countries in Info Stealers 2024

Info Stealer Malware Families Distribution

Currently, the information stealers industry is distributed among various malware families. While Redline remains the leading player, accounting for 35% of stealer cases in the Europe (42% worldwide), it is no longer the sole dominant force. Lumma is linked to 34% of cases, followed by other significant players such as Stealc and Aurora.

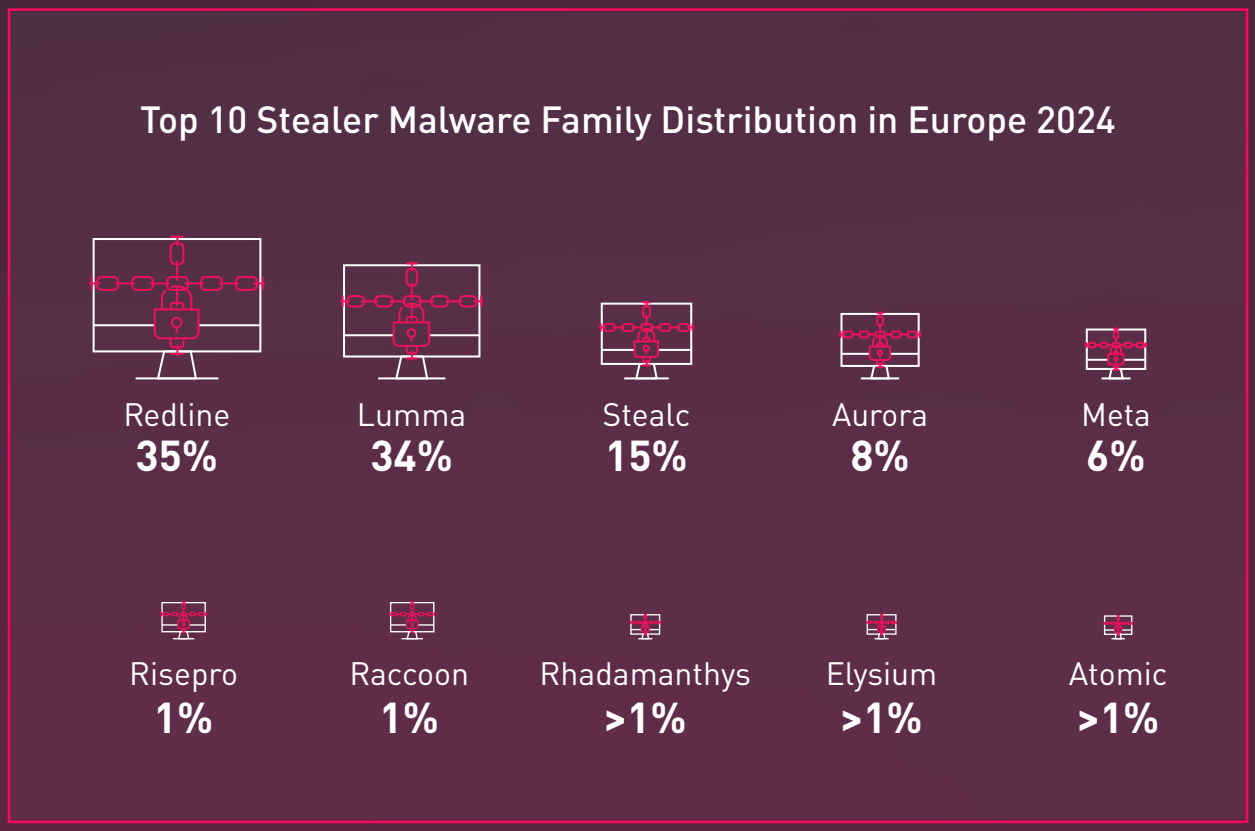


Figure 7: Info Stealer Malware Distribution in Europe

Key Policy Recommendation and Considerations:

Employee Awareness: Employees should be reminded to practice good credential hygiene, such as not reusing credentials, and to give due consideration to the security of any stored credentials, such as within applications.

Behavioral Analysis: Monitoring for behavior that deviates from a baseline, such as unusual login times and unauthorized access of resources could assist in preventing access to a Threat Actor in cases of a compromise.

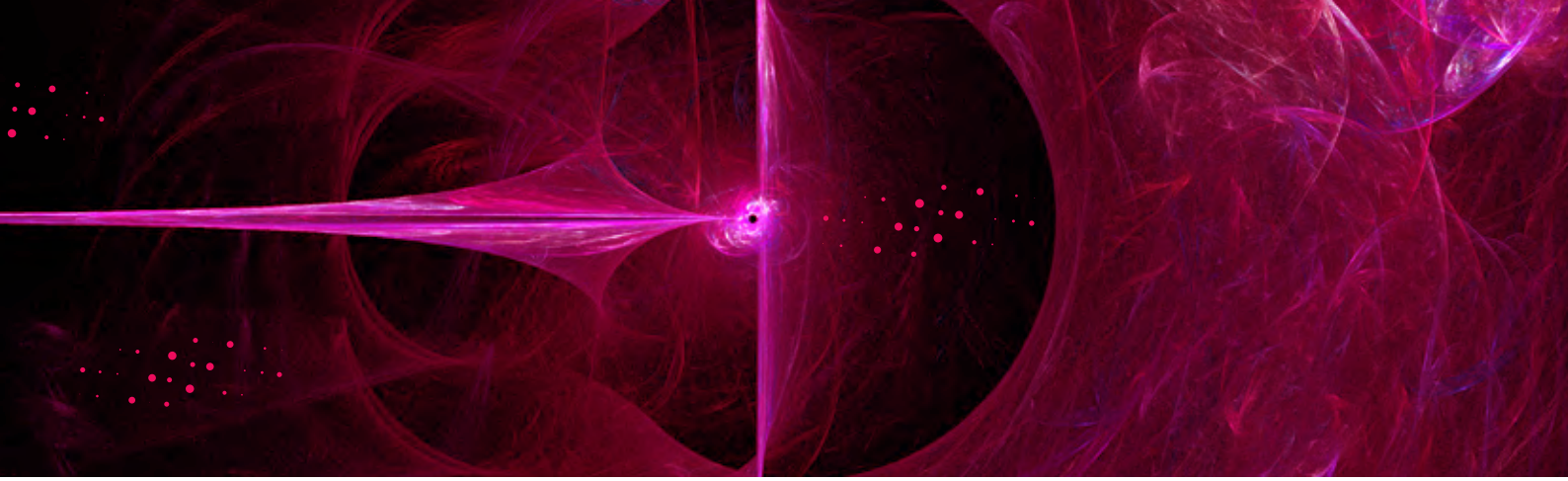
Practice Least Privilege – Conditional Access: In cases where employees or vendors that have internal access are compromised, implementing conditional access best practices can help mitigate the risk. By allowing only compliant devices from specific locations to access company resources, the potential vectors through which threat actors could infiltrate company systems are significantly limited.

NOTABLE PHISHING THREATS

Phishing attacks continue to pose a significant threat to retailers, targeting both organizations and customers with the intent to steal sensitive information, financial data, or access credentials. As E-commerce platforms becomes more integrated in the everyday life, threat actors are increasingly exploiting vulnerabilities in online shopping platforms to deceive users. These attacks can be very sophisticated, with cyber criminals using E-mail, text messages, social media, and fake websites to impersonate trusted brands. Retailers face the dual challenge of protecting their internal systems from these threats, while also safeguarding their customers from falling victim to scams that could harm their reputation and customer trust.

In 2024, Cyberint, now a Check Point company, discovered and analyzed many different phishing campaigns, with several more sophisticated and distributed than others. The most notable are the campaigns that attempted to bypass email firewalls with malicious QR codes, phishing websites that tried to circumvent and steal 2FA codes, and the continuing trend of malicious ads.

Additionally, certain events, such as benefit enrollment periods, Defcon and Blackhat, or other industry-specific conferences, are potential opportunities for Threat Actors to utilize in their phishing campaigns.



MALICIOUS QR CODES THAT REDIRECT TO PHISHING INTERFACES

Cyberint, now a Check Point company, have observed an increasing trend of malicious QR codes being used to bypass email firewalls. Typically, these emails do not contain any other links or executable malicious content. Most security solutions do not actively scan QR codes to verify if they link to malicious content, making QR codes an additional vector that threat actors can exploit to circumvent email firewalls.

If the email content is convincing and not blocked due to the sender's IP address or a potentially spoofed domain, recipients who scan the QR code may be directed to a phishing link if they do not exercise due diligence. Furthermore, malicious QR codes can indirectly bypass corporate endpoint security and firewalls, as recipients are likely to use their private devices, which are usually not under organizational scrutiny. Consequently, uninformed victims are more likely to visit phishing sites or download malware.

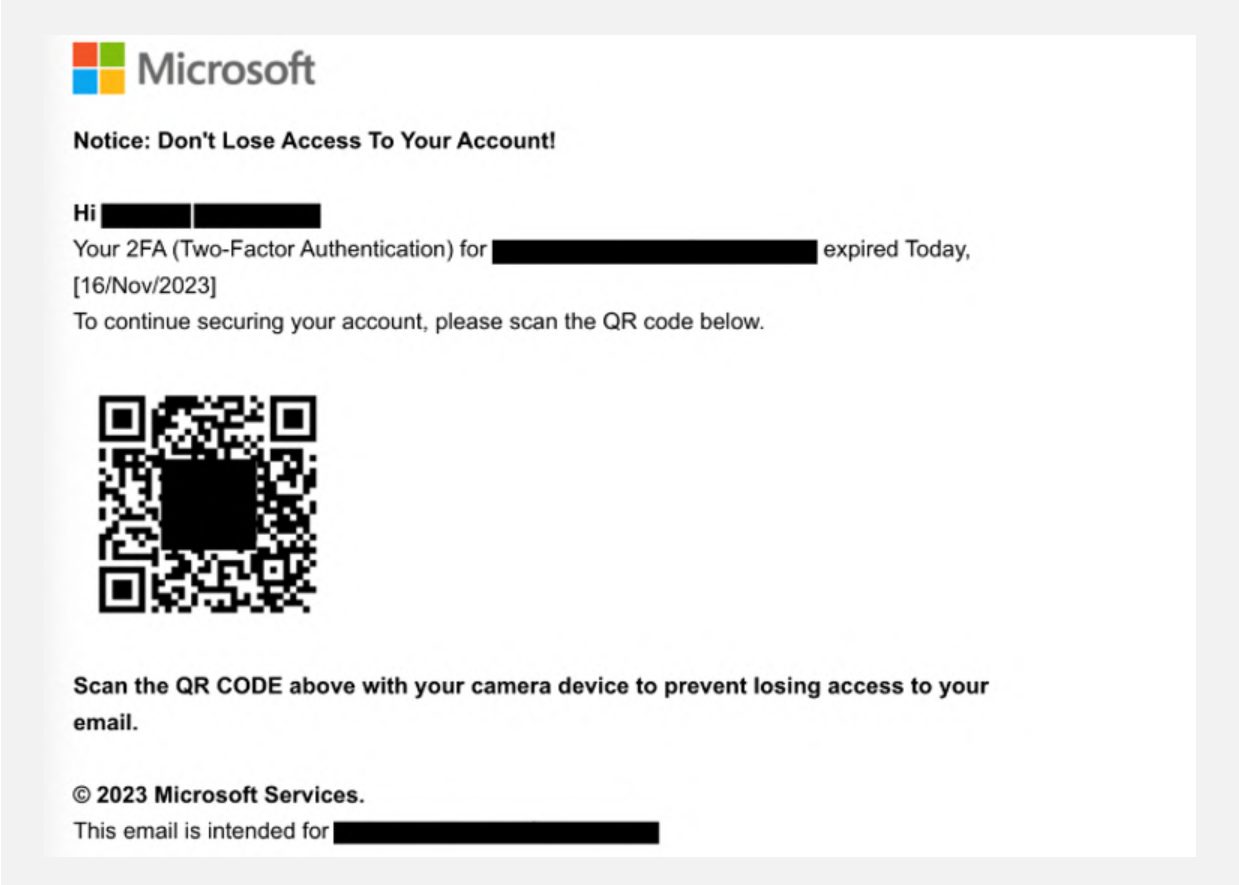


Figure 8: Malicious QR Code Utilized for Phishing

AI TOOLS EMPOWERING PHISHING CAMPAIGNS

Generative AI tools have been observed aiding social engineering methods by impersonating human users in live chats. These tools often pose as support staff or interact with victims in real-time on social media platforms, SMS, and other communication channels. Essentially functioning as chatbots, these AI tools possess greater autonomy due to their generative capabilities, making them highly convincing and increasing the likelihood of victims falling for these attacks.

Compared to a pre-determined set of instructions in static phishing kit code, this enables threat actors to act during real time during their phishing campaigns.

HR IMPERSONATION – ABUSING KNOWN PROCEEDINGS

During the first half of 2024, several clients were targeted by email phishing campaigns impersonating HR personnel during the expected benefits enrollment period. These campaigns primarily targeted newly employed individuals, indicating that threat actors are actively monitoring new hires within various companies. New employees are perceived as particularly vulnerable and more susceptible to social engineering attacks due to their limited familiarity with the company's email correspondence, procedures, and protocols.

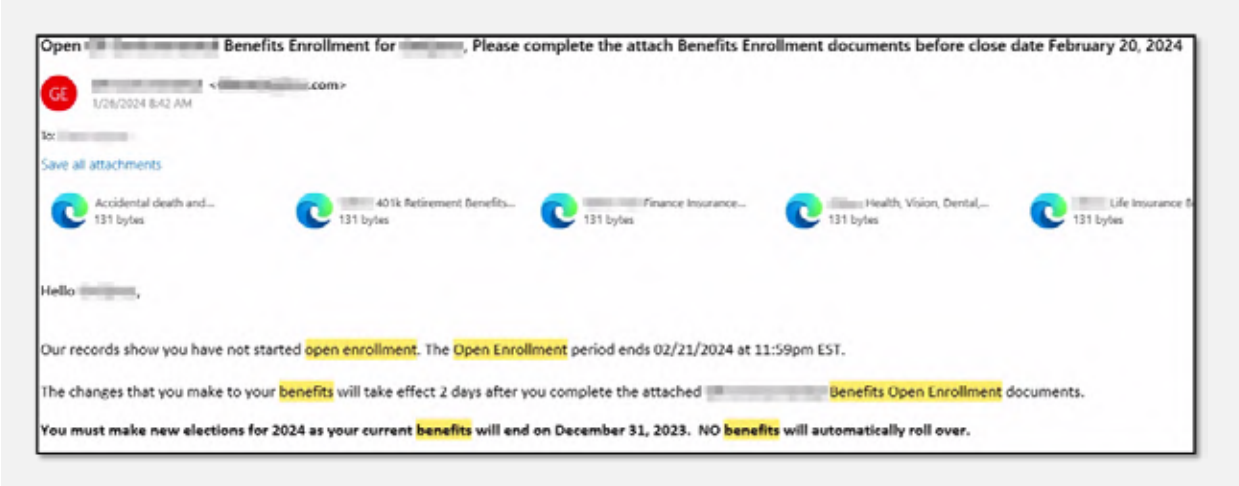


Figure 9: HR Impersonation – Fake Benefits Enrollment

Key Policy Recommendations and Considerations:

Organizations should implement and add these additional tactics (malicious QR codes, HR impersonations around known events, chatbots powered by generative AI) to their repository of phishing exercises. Organizations should consider:

- Implementing additional security solutions that can detect and block any of the newer threats.
- Consider sharing regular updates and reminders during known periods when phishing campaigns are rampant. Such periods include, but are not limited to, tax filing season, elections, world events (such as the Olympics, World Cup, NFL season), etc.

GLOBAL EVENTS INFLUENCING CYBER ACTIVISM

Global events significantly influence cyber activism, often serving as catalysts for increased online activity and coordinated efforts by hacktivist groups.

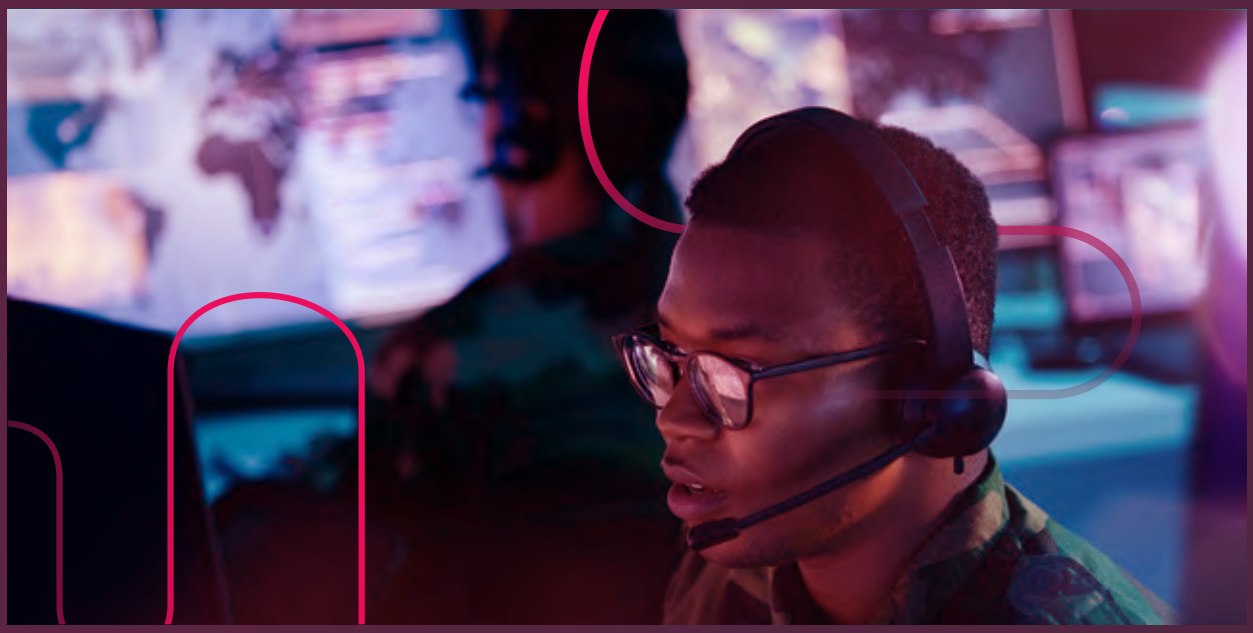
Political upheavals, social justice movements, and international conflicts can drive cyber activists to target entities they perceive as responsible for injustices or to support causes they believe in. For instance, geopolitical tensions may lead to cyber-attacks on government institutions, while social movements might inspire campaigns against corporations or organizations seen as opposing the activists' goals. Additionally, global events such as pandemics or economic crises can exacerbate vulnerabilities, providing opportunities for cyber activists to exploit these situations to further their agendas.

One of the examples of this is Russia-Ukraine war. Following Russia's invasion of Ukraine on 24 February 2022, Russian threat actors conducted several disruptive and destructive computer network attacks against Ukrainian targets, including Distributed Denial of Service (DDoS) attacks and the deployment of malware against various sectors, including government, financial, and energy. 2023-2024 witnessed constant expansion of scope of those attacks against NATO countries and other European allied countries that showed support for Ukraine[21]. Since January 2022, Russian cyber actors have targeted government, academic, private sector, and critical infrastructure entities in Denmark, Latvia, Lithuania, Norway, Poland, Italy, the US, and Turkey, as well as entities in Finland and Sweden, both of whom applied for NATO membership following the Russian invasion of Ukraine in February.

The Russia-Ukraine war had a wide indirect effect on the retail sector with the issue of sanctions evasion. In response to Russia's invasion of Ukraine, Western governments have imposed severe sanctions on Russian individuals, companies, and the financial sector. These sanctions were accompanied by decisions by private companies to suspend their activities partially or completely in Russia.

This has led to the rapid growth of fraudulent activities with the goal of satisfying the Russian consumer and creating an illusion of an intact world in Russia. Since the major brand withdrawal and the first sanctions, Cyberint noticed a growing trend of brand abuse, unauthorized resale, carding, and mule fraud, conducted by Russian threat actors. Cyberint is also detecting growing markets in Russia of retail goods from Western retailers getting to Russia via "gray import" or "parallel import". Western companies may not be able to prevent parallel imports of their goods via friendly to Russia countries such as Kazahstan, Kyrgystan, Armenia and Georgia.

However, Western governments may warn countries and companies not to help Russia circumvent sanctions or even threaten secondary sanctions. Considering the EU's proposal to make sanction evasion a criminal offense and therefore to put the responsibility on the manufacturers, some of the retailers began recently to require their customers to prove they are physically not in Russia while placing an order.



[21] https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf

Another example of global events affecting cyber activism is the Israel-Hamas war. The invasion of Hamas into Israel in October 2023 was in coordination with a massive cyber-attack on Israel. Following this has it has seen the expansion of campaigns against allies of both sides with such groups as Anonymous Sudan and Ghosts of Palestine attacking allies of Israel, and groups such as Gonjeshke Darande — also known as Predatory Sparrow, attacking Israel's enemies such as Iran.

2024 also saw expansion of these campaigns into the retail sector. The Boycott, Divestment, Sanctions (BDS) movement works to end international support for Israel. In November 2024 the BDS has partnered with Boycat, a so called "ethical" shopping platform and application, in order to allow consumers to join consumer-focused BDS campaigns more effectively. Through the app users can check regularly updated BDS targets, learn about companies, build their "ethical" shopping profile, join local teams and directly support BDS priority campaigns, ensuring that the consumer purchasing decisions "contribute to a larger movement for justice". Most importantly, the new BDS app allows consumers to scan the items in stores, to determine if the product is connected to Israel or not, thus making the simple act of purchasing into an ethical issue.

Politization of the retail sector can be seen in another example in the last year. In November 2023, a global retail chain headquartered in Britain was widely criticized on social media due a perceived support of Israel. A Christmas ad for the retail giant has featured a burning fire. The image shows red, green and silver paper hats — traditionally worn at British Christmas dinners — burning in a fireplace. It's an outtake from a Christmas commercial filmed in August that was meant to "playfully" illustrate how people don't enjoy some Christmas traditions, including donning the hats. The picture drew criticism from social media users who claimed there was a similarity between the colors of the hats and the Palestinian flag.

The Advertising Standards Authority, which regulates advertising in the UK, says it has received 40 complaints about the Instagram post. On social media - "IT SHOWS THE PALESTINIAN FLAG BURNING IN A PROMO," reads one post on X, formerly Twitter. "Their hashtag makes it clear that they intended to burn the Palestinian flag."

The post had received approximately 5,900 likes and more than 4,900 shares. Even though the commercial was filmed before the start of the latest Israel-Hamas war, and there was no evidence of connection to the war, the retailer has ended up apologizing and pulling the ad[22].

[22] https://apnews.com/article/fact-check-marks-spencer-ad-palestinian-flag-227961080585

Global retail companies in general are trying to avoid getting entangled in the conflict between Israel and Hamas as the fighting has prompted a rise in religious hate crimes globally. McDonald's franchises in some Muslim countries distanced themselves from a move by the company's Israeli restaurants last month to give free meals to the Israeli military. The U.S. burger giant's franchises in Saudi Arabia, Oman, Kuwait, the United Arab Emirates, Jordan, and Turkey issued statements disassociating themselves from the Israeli franchise and in most cases pledging aid to Gaza[23].

Key Policy Recommendations and Considerations:

Organizations should monitor global events and conduct risk assessment analyses. This is particularly important if certain executives or individuals affiliated with the organization have outspoken controversial or political opinions, as they may become targets of interest for cyber activists.

[23] https://www.reuters.com/world/middle-east/free-meals-israeli-soldiers-divide-mcdonalds-franchises-over-israel-hamas-war-2023-10-17/

CONTACT US

ISRAEL

Tel: +972-73-226-4555
5 Shlomo Kaplan Street
Tel Aviv 6789159

USA

Tel: 1-800-429-4391
100 Oracle Parkway, Suite 800
Redwood City, CA 94065

SINGAPORE

Tel: +65-6435-1318
78 Shenton Way, #09-01 Tower 1,
Singapore 079120

PHILIPPINES

Tel: +63 2 8465 9200
Unit 2005, 20th Floor, Zuellig Building,
Makati Avenue, corner Paseo de Roxas
Makati City 1223, Metro Manila

UK AND IRELAND

Tel: +44 20 7628 4211
85 London Wall, 4th Floor,
London, EC2M 7AD

JAPAN

Tel: +81-3-6205-8340
Toranomon Kotohira Tower 25F,
1-2-8, Toranomon Minato-ku, Tokyo 105-0001

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