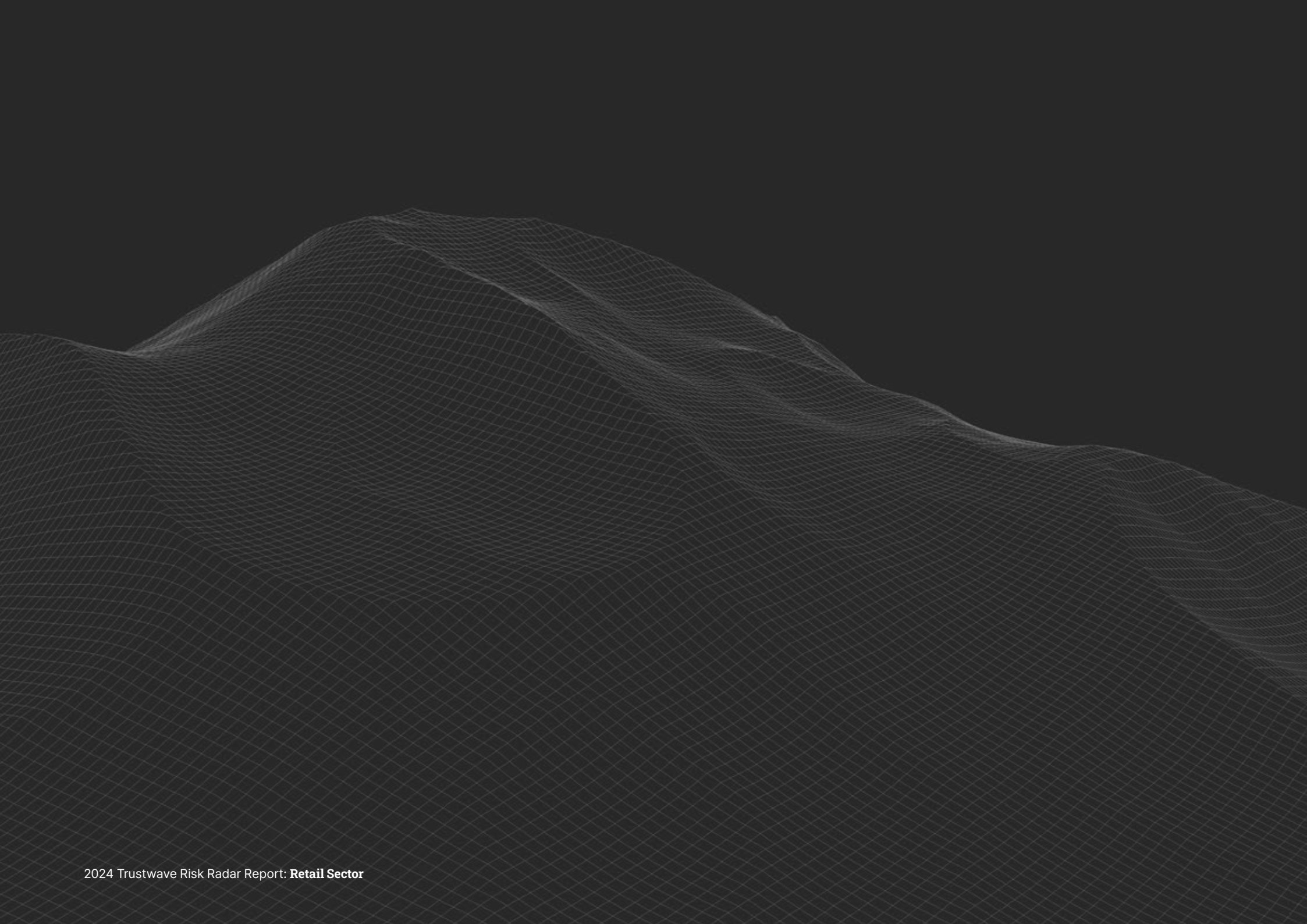
Trustwave SpiderLabs

2024 Trustwave Risk Radar Report

Retail Sector

Trustwave®



2024 Trustwave Risk Radar Report: **Retail Sector**

Contents

In 2023, Trustwave released its Retail Sector Threat Intelligence Briefing that analyzed the attack flow specific to retailers, offering insight on specific threat actors, actionable intelligence, and recommended mitigations for each stage.

Building on that foundation, our 2024 report delves deeper into the unique factors influencing the retail sector today. The Trustwave SpiderLabs team highlights significant trends currently reshaping the industry, such as the rise of e-commerce vulnerabilities and evolving consumer behaviors. We offer a comprehensive overview of threat actor techniques categorized by attack stage, equipping retailers with the knowledge needed to fortify their defenses.

In addition, Trustwave SpiderLabs has created two complementary deep-dive analyses that explore critical areas of concern: e-commerce threats and fraud targeting retailers. These write-ups feature extensive research and analysis, providing retailers with a clearer understanding of the landscape and effective strategies to mitigate risks.

Cybersecurity in the retail sector is particularly challenging due to the increasing complexity of IT environments, which often encompass in-store systems, online platforms, and supply chain networks. Retailers face a diverse range of threats, from point-of-sale (POS) malware that targets payment systems to phishing attacks aimed at employees. The shift to digital and contactless payment methods has opened new avenues for cybercriminals, making it essential for retailers to implement robust security measures.

While the average cost of a data breach in the retail sector is $3.5 million—lower than the overall industry average of $4.8 million—the reputational damage can be far more significant. The extensive public awareness surrounding major retail brands, combined with their loyal customer bases, can amplify the consequences of any breach. A single incident can undermine customer trust and lead to long-term financial impacts, making robust cybersecurity measures not just a necessity, but a critical component of sustainable business practices in today's retail landscape.

Key Report Findings for the Retail Sector

58%
of attacks originated from phishing

47%
of stolen user sessions leverage Amazon domains

92%
of credential access techniques were brute-force attempts

15%
of ransomware attacks were conducted by Play & LockBit

62%
of ransomware attacks were in the US

16%
of ransomware attacks targeted Food & Beverage retailers

Retailers' Unique Threat Landscape

Seasonal Fluctuations

- The retail industry experiences significant seasonal fluctuations, particularly during peak shopping periods such as the holiday season, Black Friday, and back-to-school sales. During these times, retailers face a surge in customer traffic and transaction volume, which can strain existing cybersecurity measures. Cybercriminals often exploit these busy periods, launching attacks when systems are more vulnerable due to increased loads.
- The heightened activity not only raises the risk of data breaches but can also overwhelm IT staff, making it difficult to monitor and respond to potential threats effectively. Retailers must therefore enhance their security protocols in anticipation of these busy seasons, ensuring they have adequate resources to manage both customer demands and cybersecurity risks.

Third-Party Dependencies

- In the retail landscape, third-party dependencies are prevalent and can significantly amplify cybersecurity risks. Retailers often collaborate with vendors for payment processing, logistics, marketing, and other essential services. Each of these partnerships introduces potential vulnerabilities; a breach at a third-party vendor can compromise the retailer's own systems.
- For example, if a payment processor is compromised, customer payment information may be exposed, leading to reputational damage and financial loss. Retailers must therefore establish rigorous vetting processes for third-party vendors, implement robust contracts that address cybersecurity standards, and continuously monitor the security practices of their partners to mitigate risks associated with these dependencies.

Owner of Vans and Supreme, VF Corporation, Says Hackers Stole 35 Million Customers' Personal Data

January 2024, **TechCrunch**

Physical Security Risks

- Retailers are not only susceptible to cyber threats but also face physical security risks that can impact their cybersecurity posture. Physical breaches—such as the installation of skimming devices on point-of-sale terminals or unauthorized access to store locations—can lead to significant data theft.
- In addition, retail environments often have high employee turnover, making it challenging to maintain consistent security protocols. A former employee might retain access to sensitive systems, posing an insider threat. To combat these risks, retailers must integrate physical and cybersecurity strategies, such as installing surveillance systems, conducting regular audits, and implementing strict access controls to safeguard both physical and digital assets.

Franchise Model

- The franchise model introduces unique cybersecurity challenges within the retail sector. Franchisees often operate semi-autonomously, which can lead to inconsistencies in security practices across different locations. While franchisors can establish overarching cybersecurity policies, individual franchisees may lack the resources or knowledge to implement these effectively, creating vulnerabilities in the system.
- Additionally, breaches at one franchise location can affect the entire brand's reputation and customer trust. To address these challenges, franchisors must provide comprehensive training and support to franchisees, ensuring they understand and adhere to established cybersecurity protocols. Regular assessments and communication can also help maintain a strong security posture across the franchise network.

Diverse Payment Systems

- The retail industry utilizes a wide range of payment systems, including credit cards, mobile payments, and digital wallets, each of which presents its own set of security challenges. As retailers embrace omnichannel strategies—integrating online and offline sales experiences—they must secure multiple platforms, from e-commerce sites to in-store point-of-sale systems. This diversity increases the potential for vulnerabilities, as cybercriminals may target any weak link in the chain.
- Furthermore, the rapid adoption of new payment technologies, such as contactless payments and buy-now-pay-later options, requires retailers to continually assess and update their security measures. To effectively safeguard customer data, retailers must implement end-to-end encryption, tokenization, and robust authentication processes across all payment channels, ensuring a secure and seamless shopping experience for customers.

Trustwave SpiderLabs

With more than 250 cybersecurity experts across the globe, the Trustwave SpiderLabs team puts its resources to task researching the top threats in today's landscape. We are uniquely positioned to do so, as we perform over 200,000 hours of penetration tests and uncover tens of thousands of vulnerabilities annually. We also have a dedicated email security team analyzing millions of phishing URLs validated daily, including 10k per day that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Advanced Continuous Threat Hunting, Digital Forensics and Incident Response, Malware Reversal, and Database Security, give us insight into identifying how these breaches occur, as well as mitigations and controls that your organization can put in place to prevent these compromises.

This report examines the myriads of threats facing the retail industry. In addition to supplemental reports focused on e-commerce threats and fraud targeting retailers, Trustwave SpiderLabs will offer recommendations to help retailers mitigate risks and safeguard their customers and data.

Notable and Prominent Trends in Retail

Continued Rise of E-Commerce

The Threat

We explore e-commerce threats in depth in our accompanying report. At a high level, here are some key points to consider:

E-commerce platforms are increasingly targeted by malicious actors due to their wide reach and profitability. The primary goal of these attackers is to gain access to sensitive data and financial information. Common methods used to gain access include phishing, abusing valid accounts, and exploiting vulnerabilities.

Once access is obtained, attackers can steal user credentials, payment details, and personal information, which are often sold on Dark Web marketplaces. Other attack methods include installing web shells to gain remote control over compromised servers, and using credential stuffing attacks to exploit stolen login credentials. Additionally, vulnerabilities in e-commerce software, such as those in Magento, are frequently exploited to inject malicious code and steal transaction data.

What Trustwave Is Seeing

Trustwave SpiderLabs found that the Russian Market, a popular dark web marketplace, had over 3.3 million stolen user sessions for sale, highlighting the widespread nature of credential theft. This marketplace specializes in the sale of stolen credentials, user sessions, and personal information, making it a significant threat to e-commerce platforms.

Larger, globally recognized companies like Amazon, Apple, and eBay are frequent targets due to their massive user bases. The deep-dive report shows a clear correlation between the global reach, popularity, and digital presence of these companies and the number of times they appeared in credential stealer logs.

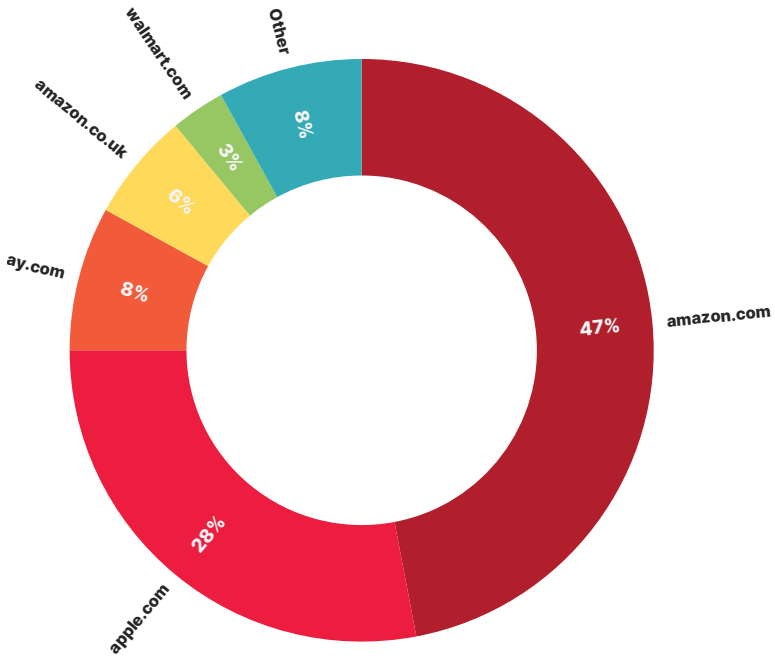


Figure 1. The distribution of the number of stolen user sessions by company domains offered on the Russian Market

Regional leaders such as Zalando.de, Thomann.de, and Tesco.com also show significant appearances in the logs, suggesting that localized platforms with strong regional footprints are heavily targeted. This indicates that cybercriminals exploit both large and small platforms.

Smaller or more niche retailers like Chefkoch.de and Myer.com.au still appear in the logs, indicating that cybercriminals are also exploiting smaller platforms, albeit less frequently.

Credential stealers are a significant threat to e-commerce platforms because they capture sensitive information from a victim's device, such as login credentials, browser session cookies, payment card details, autofill data, and other personal or system information. Credential stealers allow attackers to bypass normal authentication mechanisms and gain instant access to personal accounts. With access to session cookies and login details, attackers can impersonate victims online, bypassing passwords and two-factor authentication (2FA).

Mitigations to Reduce Risk

- **Implement MFA:** MFA significantly reduces the risk of unauthorized access, even if login credentials are compromised. It is recommended to use MFA for both customer and administrative accounts to enhance security.
- **Regularly Update and Patch E-Commerce Software:** It is essential to have a robust patch management process in place to ensure that all software components are updated promptly.
- **Conduct Thorough Security Audits and Continuous Monitoring:** Implementing intrusion detection systems (IDS) and security information and event management (SIEM) solutions can enhance the ability to monitor and respond to security incidents.
- **Educate Employees and Customers About Phishing and Social Engineering Attacks:** Phishing and social engineering attacks are common methods used by cybercriminals to gain access to sensitive information. Educating employees and customers about these threats and how to recognize and respond to them can significantly reduce the risk of credential theft. Regular training sessions and awareness campaigns can help reinforce this knowledge.
- **Limit Access to Sensitive Information:** Implementing the principle of least privilege (PoLP) ensures that users and systems have only the minimum access necessary to perform their functions.

Ace Hardware Client Data Affected by Cyberattack

April 2024, **CyberNews**

Fraud Targeting Retailers

The Threat

We cover fraud targeting retailers in our accompanying report. At a high level, here are some key points to consider:

Retailers are increasingly becoming targets of sophisticated fraud schemes that exploit various vulnerabilities in their systems. These schemes not only result in significant financial losses but also damage the reputation and trust that retailers have built with their customers.

More than a third (35%) of UK retailers fell victim to fraudulent activity, cyber-attacks, or data leaks over the past 12 months, according to new research by Ayden and the Centre for Economic Business and Research (CEBR). This represents a 37% increase on the proportion of retail businesses affected by such incidents in 2022. In total, the UK retail industry lost £11.3bn ($14.30bn) to fraud last year.

According to a survey done by PYMNTS Intelligence, 41% of retail respondents said they were already modernizing their anti-fraud toolkits, and 54% say they plan to in the months to come. PYMNTS Intelligence also found those merchants that primarily sell physical items were being more proactive — 45% are currently in the process of upgrading their anti-fraud capabilities, while only 37% of digital service providers were taking similar steps.

What Trustwave Is Seeing

Malware attacks, such as Ducktail and DarkGate, are particularly concerning. Ducktail, originating from Vietnam, targets social media platforms and uses PowerShell to download and execute malicious payloads. It hijacks Facebook Business accounts, stealing user information and two-factor authentication codes. DarkGate spreads through Microsoft Teams, using social engineering to send ZIP files containing malicious LNK files. It can perform tasks like keylogging, cryptomining, and stealing sensitive data.

Phishing campaigns are another major threat. These attacks often use lures such as fake LinkedIn invitations and Zoom meeting invites to steal credentials. Phishing links frequently utilize open redirects and are hosted on cloud platforms offering free plans. Phishing-as-a-service platforms like Tycoon and Greatness are driving an increase in phishing links concealed in attachments. Fake LinkedIn emails and Zoom meeting invites are common tactics used to lure victims into credential harvesting pages.

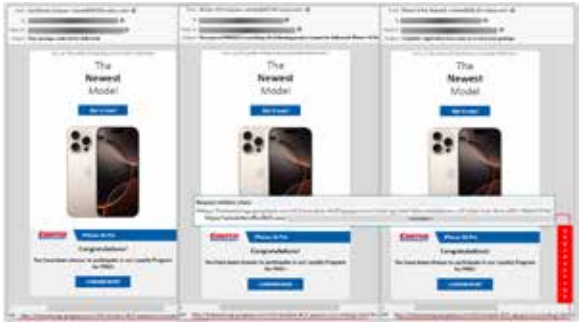


Figure 2: Abuse of Legitimate Invoicing Platforms

Additionally, gift card scams are rampant on the Dark Web, where cards are sold at a fraction of their value. Fraudsters use automated tools to brute force gift card numbers and exploit vulnerabilities in retailer systems to generate or manipulate gift card values. A notable scam involves the Morocco-based cybercriminal group Atlas Lion or Storm-0539, which breaches large retailers' systems to fraudulently issue gift card codes to themselves.

Figure 3: Dark Web marketplace gift card sale advertisement

Fake online stores, like the BogusBazaar network, have scammed hundreds of thousands of shoppers. Operated primarily from China, this network has processed over one million orders since 2021, stealing victims' card details and cash.

Mitigations to Reduce Risk

- **Enhance Fraud Detection Measures:** Implement stronger fraud detection systems and secure gift card processes to prevent unauthorized access and manipulation.
- **Employee Training:** Educate employees about the risks associated with phishing attacks, especially those delivered through platforms like Microsoft Teams.
- **Customer Awareness: Inform customers about common fraud tactics, such as** fake online stores and phishing emails, to help them recognize and avoid scams.
- **Regular Audits:** Conduct regular audits of return and refund policies to identify and address potential vulnerabilities that could be exploited by fraudsters.

Recent Changes in PCI Compliance

The Threat

While not a threat, recent changes to the Payment Card Industry (PCI) Data Security Standard (DSS) may significantly change the industry. These updates will go into effect starting on March 31, 2025.

PCI DSS 4.0 introduces stricter requirements for password management, multi-factor authentication (MFA), and data encryption. This enhanced security is designed to protect against unauthorized access and data breaches. The standard now adopts a more pragmatic, risk-based approach, allowing organizations flexibility in demonstrating compliance. However, the bar for maturity is set very high, and many organizations may find that achieving compliance is more challenging than initially thought.

Additionally, the standard places greater emphasis on identifying and mitigating risks, such as phishing attacks and other cyber threats. Third-party service providers have more specific requirements for providing information about their PCI compliance status, ensuring that organizations can assess the security of their vendors. Enhanced obligations for monitoring third-party security are also expected.

What Trustwave Is Seeing

One of the most significant changes in PCI DSS 4.0 is the introduction of the Targeted Risk Analysis (TRA). This new approach allows organizations the flexibility to perform a risk assessment appropriate for their unique environment. The TRA focuses on identifying specific risks and vulnerabilities within an organization's PCI environment, including operations, infrastructure, and compliance requirements. If an organization has the right controls and maturity in place, they don't necessarily need to follow the standard to the letter. However, organizations must prove that they have thoroughly considered their risk posture.

Organizations are encouraged to review and update their TRA regularly, at least annually. This review should align with change management activities; whenever there is a change in the environment, the TRA should be reassessed and updated as necessary. Moreover, the TRA helps organizations determine and justify the frequency of "periodic" control activities, but this customized approach requires careful thought. Many may see it as an easy workaround, yet failing to adequately assess and document these choices can lead to significant compliance challenges.

Organizations must also understand the implications of their chosen compliance path. For instance, adopting password-less authentication methods like magic links to email may seem simpler, but it requires thorough risk analyses, including penetration testing, to justify this approach. The burden of maintaining compensating controls can be more significant than expected, and organizations should carefully consider whether to take on a larger upfront challenge or manage a more continuous compliance process.

Key updates from PCI DSS 4.0 come into effect from March 31, 2025, and entities will need to comply with these requirements during their next certification event. Major changes include:

- Clearly defined roles and responsibilities for meeting requirements.
- Malware scan frequency based on documented risk analysis.
- A specific requirement to detect and protect staff from phishing attacks.
- MFA mandated for any access to the CDE.
- All vulnerability scanning must now be conducted on an authenticated basis.
- Any PCI requirement that allows flexibility in control applicability must undergo a targeted risk analysis.

Organizations must balance the initial effort of implementing these controls with the ongoing compliance burden they are committing to. Understanding the long-term implications of their decisions is crucial for successful compliance with PCI DSS 4.0.

Mitigations to Reduce Risk

Organizations should take a proactive approach to ensure they meet the requirements of PCI DSS 4.0. Here are some key steps:

- **Conduct a Thorough Assessment:** Identify sensitive data, assess current security measures, and identify gaps.
- **Implement Strong Security Controls:** Enforce password management, data encryption, access control, vulnerability management, and security awareness training. For example, MFA is now mandated for any access to the Cardholder Data Environment (CDE).
- **Document Security Policies and Procedures:** Create comprehensive policies and procedures and maintain documentation.
- **Monitor and Test Security Systems:** Conduct regular testing and continuous monitoring. All vulnerability scanning must now be conducted on an authenticated basis, reinforcing the need for rigorous monitoring.
- **Establish a Compliance Program:** Assign responsibilities, conduct regular reviews, and consider third-party assessments. Clearly defining roles and responsibilities per requirement is now essential.

Ransomware Groups Continue to Target Retailers

The Threat

Retailers handle vast amounts of sensitive customer data, including payment information and personal details, making them prime targets for cybercriminals looking to disrupt operations and extract hefty ransoms. The impact of a ransomware attack on a retail business can be catastrophic, leading to operational paralysis, substantial financial losses, and severe damage to brand reputation. Attackers often use sophisticated encryption methods to lock access to critical systems, demanding ransoms in cryptocurrency, which complicates recovery efforts and legal responses.

The retail sector is particularly vulnerable due to its interconnected nature and reliance on complex IT infrastructures. Retailers operate intricate networks of point-of-sale systems, inventory management, and online platforms that, if compromised, can create ripple effects across the supply chain and customer experiences. Downtime caused by ransomware attacks can halt sales, disrupt inventory management, and negatively impact customer service, affecting everything from in-store transactions to e-commerce operations.

In addition to direct financial costs and operational disruptions, ransomware attacks on retailers can lead to a loss of customer trust and increased scrutiny from regulatory bodies. Customers expect high levels of security and reliability from their retailers, and any breach can erode confidence, driving them to seek safer alternatives. Furthermore, regulatory bodies may impose fines and require enhanced security measures, placing additional strain on the resources of affected retailers.

What Trustwave Is Seeing

Trustwave SpiderLabs analyzed ransomware incidents targeting the retail sector and identified Play and LockBit 2.0 as the predominant groups operating in this space. Last year, Play accounted for 9% of attacks, but this year their share has increased to 15%. Last year, LockBit was the predominant group at 34%, but this year has dropped to 15%.

Top Ransomware Groups

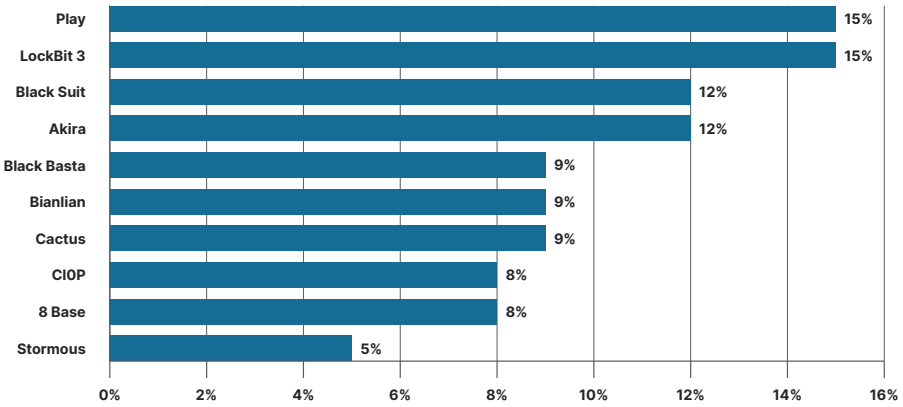


Figure 4: Top ransomware groups targeting retailers

Staples Hit by Cyberattack During Critical Cyber Week Sales Push

December 2023,
Cybersecurity Dive

Though threat actors target companies worldwide, the majority of reported breaches involve organizations from the US, with the UK and Canada coming in second and third, respectively. The proportion of breaches affecting US companies has slightly increased from 57% last year to 62% this year.

Top Countries Impacted

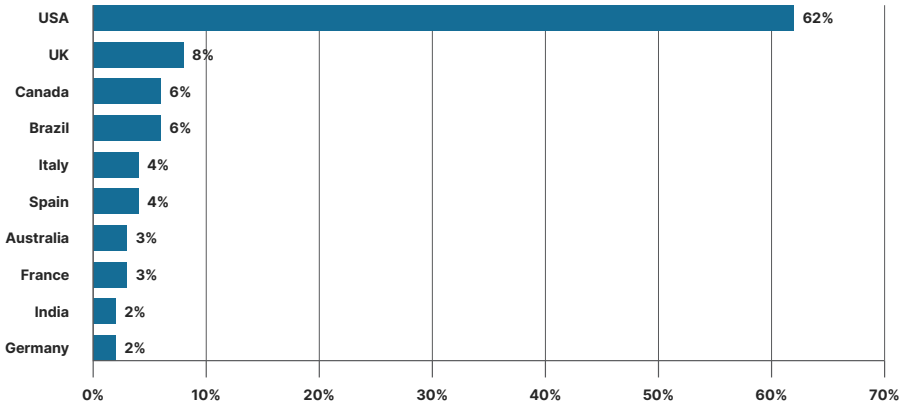


Figure 5: Retail organizations affected by ransomware by country

Food and beverage retailers are the top target for ransomware attacks, accounting for 16% of incidents, followed closely by apparel and home improvement, both accounting for 15%. It's important to note that no subsector is immune from these attacks. This distribution underscores the need for robust cybersecurity measures across all retailers. From big-box stores to mom-and-pop shops.

Top Industries Impacted

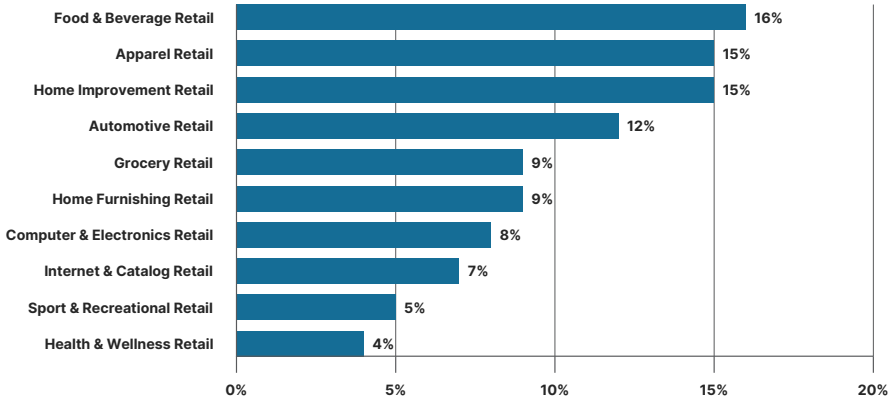


Figure 6: Ransomware attacks by retailer type

Mitigations to Reduce Risk

- **Deploy Endpoint Detection and Response (EDR) Tools:** Implement EDR solutions on individual endpoints to monitor, detect, and respond to potential threats in real-time. EDR tools provide advanced visibility and can analyze behavioral patterns to identify suspicious activities. However, it's important to remember that while EDRs are more robust than traditional antivirus solutions, they may still face challenges from sophisticated threats, so combining them with other security measures is essential.
- **Enable and Audit System Logs:** Activate logging on valuable systems and workstations. Implement network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels. These logs are crucial for identifying potential compromises.
- **Active Monitoring of Logs:** Regularly monitor logs to detect abnormal behavior or traffic. Establish a baseline of normal activity to make deviations more noticeable, as merely enabling logs without active monitoring diminishes their effectiveness.
- **Establish a Formal Incident Response Process:** Develop and routinely practice a formal incident response plan to ensure a swift and coordinated reaction to ransomware attacks.
- **Ongoing Underground and Dark Web Monitoring:** Continuously monitor the underground and dark web for information leakage that might have been overlooked. This can provide early warnings about potential threats or data exposure.

Home Depot Confirms Third-Party Data Breach Exposed Employee Info

April 2024, **Bleeping Computer**

Threat Actor Techniques by Attack Stage

Data breaches and compromises come in many forms, but they often follow a similar pattern. Attackers gain access, escalate privileges, establish a foothold, steal, or destroy data, and then vanish. Trustwave SpiderLabs analyzed data from its Fusion platform to understand the path that threat actors take within the retail industry and the techniques they deploy at each stage.

Initial Access Techniques

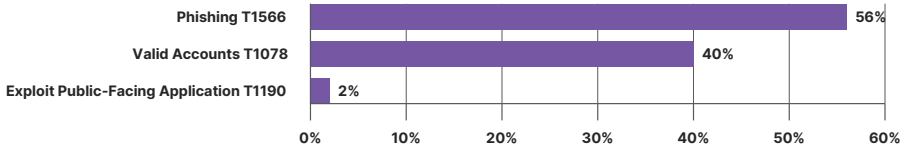


Figure 7: Initial access techniques used by attackers of retailers

More than half of all initial access techniques used by threat actors to gain entry to retail entities were phishing (58%). Following that, threat actors exploited valid accounts (40%) and public-facing applications (2%), including CVE-2021-44228, Apache Log4J.

Execution Techniques

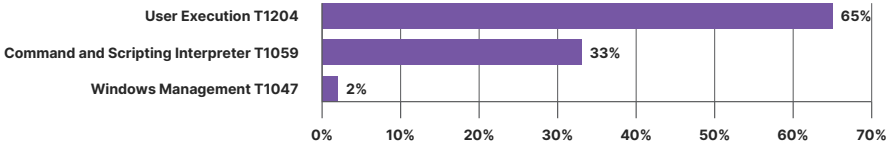


Figure 8: Execution techniques used by attackers of retail

In retail security incidents, execution techniques pre-dominately involve user execution of malicious files and links (65%). Adversaries often rely upon social engineering to convince users into executing malicious files and links. Attackers also used command and scripting interpreter techniques (33%), which involved execution of PowerShell and JavaScript files. PowerShell is often used to run commands and scripts on compromised systems and download malicious payloads.

Credential Access Techniques

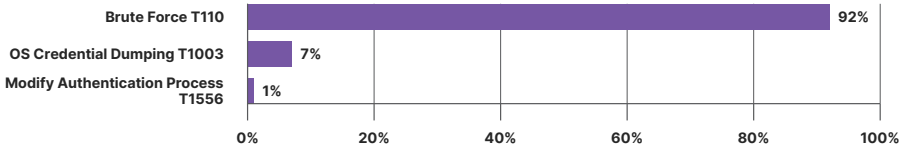


Figure 9: Credential access techniques used by attackers of retail

Credential access techniques observed in attacks against retailers predominantly relied on password brute-force attempts (92%), but also OS credential dumping (7%) from LSASS memory and use of CSync technique.

Lateral Movement Techniques

Figure 10: Lateral movement techniques used by attackers of retail

To move laterally within retail organizations, attackers relied on Remote Desktop Protocol (RDP) (56%) and use or alternate authentication material (40%), also known as pass the ticket attempts.

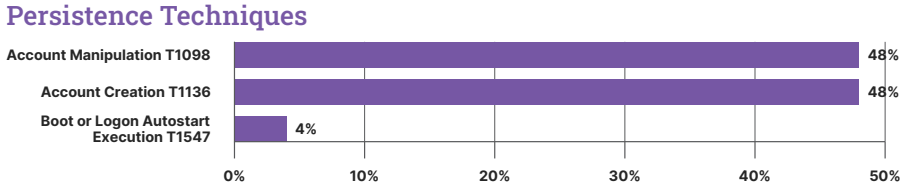


Figure 11: Persistence techniques used by attackers of retail

Lastly, the persistence techniques observed were account manipulation (48%) and account creation (48%). Account manipulation involves modifying existing accounts to either maintain access or escalate privileges. For example, an attacker might change account permissions or add their own credentials to an existing user account to retain access. Account creation refers to the creation of new user accounts by attackers. These new accounts are often used to maintain access or to disguise their activities as legitimate users.

London Drugs Pharmacy Closes All Stores to Respond to Cyber Incident

April 2024, **SC Magazine**

Conclusion & Key Takeaways

The retail sector continues to face a dynamic and evolving threat landscape, with cybercriminals constantly adapting their tactics to exploit vulnerabilities. The rise of e-commerce, the complexity of IT environments, and the integration of diverse payment systems have all contributed to the increased risk.

Retailers must remain vigilant and proactive in their cybersecurity efforts to protect their customers and maintain trust. The insights and recommendations provided in this report aim to equip retailers with the knowledge and strategies needed to mitigate these risks effectively.

The Iconic Pledges to Refund Customers Charged for Bogus Orders After Hack

January 2024, **The Guardian**

Key Takeaways

1. **E-commerce Vulnerabilities:** The increasing popularity of e-commerce platforms has made them prime targets for cyberattacks. Retailers must prioritize securing their online platforms to protect customer data and financial information.
2. **Seasonal Fluctuations:** Peak shopping periods, such as the holiday season, present heightened risks due to increased customer traffic and transaction volumes. Retailers need to enhance their security protocols during these times to manage both customer demands and cybersecurity risks effectively.
3. **Third-Party Dependencies:** Collaborations with third-party vendors introduce potential vulnerabilities. Retailers must establish rigorous vetting processes and continuously monitor the security practices of their partners to mitigate risks.
4. **Physical Security Risks:** Retailers face both cyber and physical security threats. Integrating physical and cybersecurity strategies is essential to safeguard both physical and digital assets.
5. **Diverse Payment Systems:** The use of various payment systems, including credit cards, mobile payments, and digital wallets, requires retailers to implement end-to-end encryption, tokenization, and robust authentication processes across all payment channels.
6. **Ransomware Threats:** Ransomware attacks continue to pose significant risks to retailers, leading to operational disruptions and financial losses. Implementing endpoint detection and response tools, active monitoring, and a formal incident response process are critical measures to mitigate these threats.
7. **Fraud Targeting Retailers:** Sophisticated fraud schemes are increasingly targeting retailers, resulting in financial losses and reputational damage. Enhancing fraud detection measures, educating employees and customers, and conducting regular audits are essential steps to combat these schemes.

By addressing these key areas, retailers can better protect their operations and customer data, ensuring a secure and trustworthy shopping experience.

Hacker Dumps Data of 2.8 Million Giant Tiger Customers

April 2024, **CSO Online**

Yacht Retailer MarineMax Discloses Data Breach After Cyberattack

April 2024, **Bleeping Computer**


Trustwave®