



Retail Sector **Deep Dive**

Rise of E-Commerce Threats

Contents

Overview	4
Gaining Access	6
Log Stealer Results for Sale	6
Web Shells and E-Commerce	11
Credential Stuffing	13
Vulnerability Exploitation and E-Commerce Malware	14
Magento Flaws Used for Magecart: CVE-2024-20720 (2024)	14
Magecart Attack Targets Cisco Merch Customers: CVE-2024-3410	15
SQL Injection Risks in E-Commerce (Hs): CVE-2024-36680 (2024)	15
Supply Chain Attacks	16
Ransomware Attacks	16
Mitigations	18

Overview

E-commerce, the purchasing and selling of goods via an internet-powered infrastructure, has become universal for its accessibility, convenience, and profitability. Having a virtual storefront increases a business's reach, improves its ability to provide excellent customer service, and boosts sales. It also allows businesses to stay afloat and even thrive in challenging times, such as what businesses with online stores experienced during the height of the **global pandemic**.

Because of its many business benefits, e-commerce sites have propagated rapidly and will continue to grow in the years to come. In 2023, an estimated [26.2 million](#) e-commerce sites were operating globally. By 2025, the global e-commerce market is expected to reach a staggering [\\$4.8 trillion](#).

With e-commerce's wide reach and lucrativeness, it's not just businesses and consumers who are drawn to its appeal — malicious actors who want to make illicit financial gains are also targeting e-commerce sites to steal sensitive data, exploit vulnerabilities and weaknesses, and launch malware attacks.

In this report, the Trustwave SpiderLabs team dives into the threats and risks surrounding e-commerce platforms and provides guidance on how to mitigate them, empowering organizations to keep e-commerce environments and customer data safe.

This supplemental report is part of the "[2024 Trustwave Risk Radar Report: Retail Sector](#)," a broader and more comprehensive report that analyzes the threats and trends surrounding the retail sector.



**By 2025,
the global
e-commerce
market is
expected
to reach
\$4.8 trillion**

Gaining Access

To wreak havoc and compromise an e-commerce business, a threat actor must first obtain access to it. The goal of cybercriminals targeting e-commerce systems is simple: to gain a foothold into targeted systems and surreptitiously siphon off important data and financial information. Popular initial access methods threat actors use include phishing, abusing valid accounts, and exploiting vulnerabilities, as discussed in our [Retail Risk Radar Report](#).

In this section, we tackle how malicious actors are gaining access to e-commerce platforms based on what Trustwave SpiderLabs researchers are observing in the cybercriminal underground and in recent attacks against e-commerce businesses around the world.

Log Stealer Results for Sale

In the world of cybercrime, user logs obtained through credential stealers and other forms of malware represent one of the most valuable resources for malicious actors. These logs often contain sensitive data such as login credentials, payment details, and personal information, which can be exploited to infiltrate systems, commit fraud, or resell on dark web marketplaces. For retailers and e-commerce companies, the theft of user credentials is a major cause for concern, as it can lead to account takeovers, unauthorized transactions, and significant financial losses.

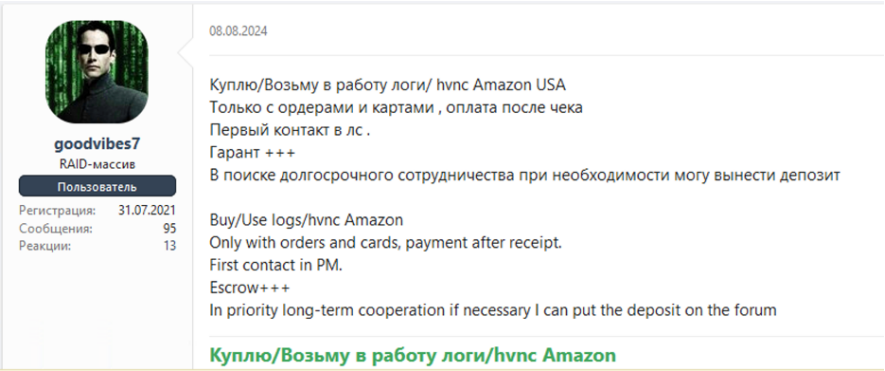


Figure 1. An actor on a Dark Web forum is looking for retailer logs.

To truly grasp the seriousness of the issue, in September our research uncovered 3,393,740 stolen user sessions for sale on just one popular dark web marketplace — the Russian Market. These sessions were related to prominent retailers and e-commerce platforms in the US, UK, Germany, and Australia, highlighting the scale at which cybercriminals target and potentially harm these businesses. The sheer volume of stolen sessions demonstrates how widespread credential theft and session hijacking has become, posing a significant risk to businesses and consumers alike.

The Russian Market is a well-known dark web marketplace that specializes in the sale of stolen credentials, user sessions, and personal information. It has gained a strong reputation among cybercriminals for offering a wide variety of illicit data, including login details, credit card information, and even accounts with multi-factor authentication (MFA) bypass methods. Cybercriminals are drawn to the Russian Market due to its anonymity, user-friendly interface, and consistent availability of freshly stolen data. It is especially popular for bulk purchases of compromised credentials from retailers and e-commerce platforms.

On the Russian Market, buyers can find login credentials, full user sessions that bypass standard login steps, credit card details, and personal identification information (PII) such as Social Security numbers.

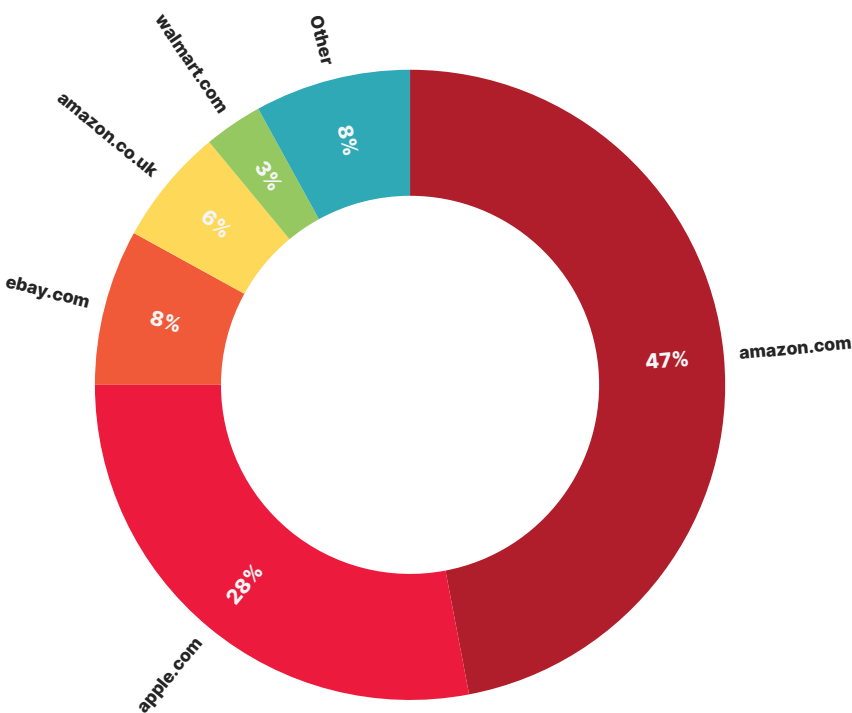


Figure 2. The distribution of the number of stolen user sessions by company domains offered in the dark web marketplace Russian Market.

Table 1 shows the detailed distribution of e-commerce and retail companies along with the number of times they were found in the credential stealing logs we analyzed in our research.

Domain name	Number of appearances
amazon.com	1,497,077
apple.com	893,162
ebay.com	236,494
amazon.co.uk	184,751
walmart.com	106,278
amazon.de	85,857
Amazon.com.au	21,093
zalando.de	20,669
target.com	14,730
asos.com	10,836
macys.com	10,190
thomann.de	9,185
tesco.com	8,768
otto.de	8,321
argos.co.uk	6,034
samsclub.com	4,801
mediamarkt.de	4,737
lowes.com	3,769
kroger.com	3,549
sainsburys.co.uk	2,997
rewe.de	2,599

Domain name	Number of appearances
amazon.com	1,497,077
apple.com	893,162
ebay.com	236,494
amazon.co.uk	184,751
walmart.com	106,278
amazon.de	85,857
Amazon.com.au	21,093
zalando.de	20,669
target.com	14,730
asos.com	10,836
macys.com	10,190
thomann.de	9,185
tesco.com	8,768
otto.de	8,321
argos.co.uk	6,034
samsclub.com	4,801
mediamarkt.de	4,737
lowes.com	3,769
kroger.com	3,549
sainsburys.co.uk	2,997
rewe.de	2,599

Table 1. The number of e-commerce website appearances we found in credential stealing logs.

The data shows a clear correlation between the global reach, popularity, and digital presence of e-commerce and retail companies and the number of times they appeared in credential stealer logs. Larger, globally recognized companies including Amazon, Apple, and eBay appear most frequently, reflecting their massive userbases and the appeal of these platforms to cybercriminals.

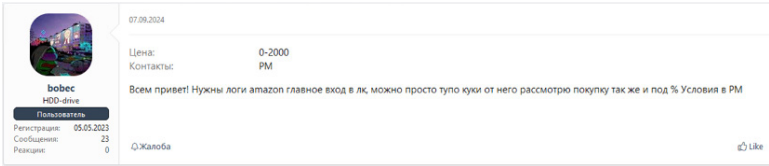


Figure 3. An actor is looking for retailer logs that have personal account access.


Translation:

Hello everyone! Need logs amazon main login in lk, you can just stupid cookies from him consider buying as well and under the % Terms in the PM Conditions in the RM

Regional leaders such as Zalando.de, Thomann.de, and Tesco.com show significant appearances in the logs, suggesting that localized platforms with strong regional footprints are also heavily targeted. Companies with a strong digital presence, particularly those in consumer goods and electronics including Walmart and Target, are frequent targets due to their large customer bases and the amount of stored payment data associated with their accounts. Meanwhile, 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.

A stealer log session refers to data captured by malware known as credential stealers or information stealers. These logs contain sensitive information stolen from a victim's device, such as login credentials, browser session cookies, payment card details, autofill data, and other personal or system information.

Stealer logs pose significant risks for end users because they provide attackers with the ability to impersonate victims online. With access to session cookies and login details, attackers can bypass normal authentication mechanisms, including passwords and two-factor authentication (2FA), and gain instant access to personal accounts such as email, social media, and even banking or e-commerce platforms.



спакilla
floppy-диск

Пользователь

Регистрация: 21.03.2024
Сообщения: 7
Реакции: 1

14.08.2024

Цена: 10-20\$
Контакты: XSS

в наличии логи Амазона с историей покупок, вход по Кукам, в основном почта невалид

10-20\$ за акк
гарант+

🔗 Жалоба

Figure 4. An actor on a dark web forum is offering retailer logs with cookie log-in abilities.

Translation:
*available amazon logs with purchase history, Cookie login, mostly mail invalid
10-20\$ per acc
warrant+*

Web Shells and E-Commerce

When malicious actors are able to successfully install a web shell or gain access to a retail or e-commerce website, the consequences can be severe. A web shell provides attackers with remote control over a compromised server, allowing them to steal sensitive data, manipulate website content, and launch further attacks. One of the most immediate risks is a data breach, where attackers can access customer information such as payment details and login credentials, potentially leading to identity theft and financial fraud.

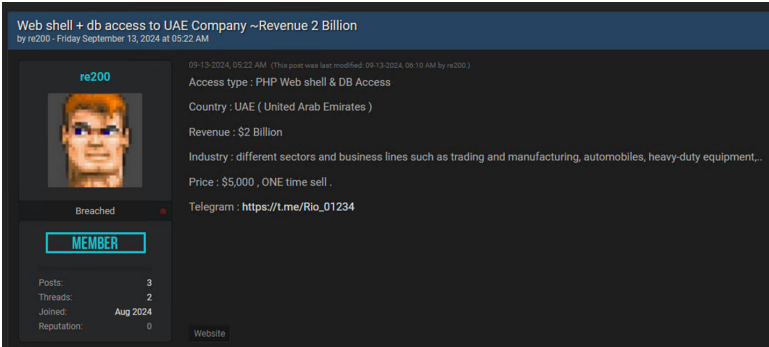


Figure 5. An actor on a dark web forum offers web shell and database access to a company in the UAE.

In addition to data theft, financial losses can occur as attackers exploit the website to conduct fraudulent transactions or divert sales. Threat actors can also engage in website defacement or cause downtime, both of which can disrupt operations and harm customer satisfaction. For e-commerce platforms, even a short period of downtime can result in significant revenue loss.

Attackers can inject malware into the website, which can lead to SEO and ranking issues, as search engines may blacklist the site, further diminishing online visibility and sales.

NO AVATAR

zerro0pluse

florru-диск

Пользователь

Регистрация: 25.05.2024

Сообщения: 5

Реакции: 1

07.09.2024

Новое

Цена: 1

Контакты: лс

Продам или готов к партнерству по доступу.

zoominfo

Цитата

Industry: Other Rental Stores (Furniture, A/V, Construction & Industrial Equipment), Retail

Revenue: ~ \$15B

Компания торгуется на NYSE, market cap ~ 50млрд, ebitda ~ 7млрд.

Вид доступа - веб шелл.

Пишите в ЛС предложения и токс для связи.

Устроит разом выкуп либо партнерство (опять же пишите - что предлагаете), линк на контору покажу если предложение заинтересует.

Жалоба

Like

+ Цитата

Ответ

Figure 6. An actor on a dark web forum offers a web shell to a retail company.

Translation:

For sale or ready for access partnership.

The company is traded on NYSE, market cap ~ 50bn, ebitda ~ 7bn.

Type of access is web shell.

Write in PM offers and tox to contact.

Will arrange a one-time buyout or partnership (again, write - what you offer), link to the office will show if the proposal is interested.

The installation of a web shell allows attackers to maintain persistent access, posing ongoing security concerns. Even after the initial attack is mitigated, companies will need to conduct thorough audits and reinforce security to prevent further exploitation. These potential consequences highlight the critical importance of robust website security and continuous monitoring in the retail and e-commerce sectors.

Credential Stuffing

When threat actors get their hands on a database of stolen login credentials, they can use an automated software to quickly run thousands of stolen credentials into a targeted website or application to gain access to it. This attack is called [credential stuffing](#), and it's a simple, swift, and effective technique cybercriminals employ to compromise systems using valid yet stolen login credentials.

In January 2024, customers of Australian fashion and sports retailer [The Iconic](#) took to the retailer's official Facebook page to complain about fraudulent orders — with some amounting to \$1,000 — made using their accounts without their knowledge. According to the [company](#), the affected customers' accounts were accessed via a credential stuffing attack using login credentials obtained via past data breaches on other compromised websites.

American fast-fashion retail chain [Hot Topic](#) disclosed in March 2024 that its website and mobile app were hit with two waves of credential stuffing attacks that exposed customers' personal information, including names, order histories, phone numbers, and months and days of birth. Customers' partial payment data was also exposed via customers' breached Rewards accounts. The attacks reportedly happened in November 2023.

Meanwhile, in the same month, pet specialty retailer [PetSmart](#) warned their customers about credential stuffing attacks that targeted their website. Because PetSmart couldn't determine which among the logged in accounts were being used by legitimate customers as opposed to hackers, the retailer automatically logged out and deactivated the passwords of the accounts that were logged in when password-guessing attacks were ongoing.

Vulnerability Exploitation and E-Commerce Malware

Malicious actors are constantly looking for weaknesses and vulnerabilities to exploit, and e-commerce websites and platforms are popular targets. After all, the popularity of an e-commerce website is directly proportional to the number of customers it will attract, and subsequently, the number of sensitive data there is to steal.

[Magecart](#) is a kind of web-skimming or e-skimming attack that targets online businesses to steal financial information via vulnerability exploitation. We've previously covered Magecart attacks, providing an [analysis](#) of infected e-commerce sites running old Magento framework versions and how businesses can protect their e-commerce sites from Magecart attacks using [ModSecurity WAF rules](#).

Unfortunately, Magecart attacks are still being used to intercept and steal victims' payment data by leveraging vulnerabilities. In this section, we discuss some of the most recent and notable Magecart and SQL injection attacks targeting e-commerce businesses.

Magento Flaws Used for Magecart: CVE-2024-20720 (2024)

In April 2024, threat actors were found exploiting [CVE-2024-20720](#), an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability with a CVSS score of 9.1, to inject malicious code to e-commerce sites and execute arbitrary code. It's important to note that this attack was [reported](#) just two months after the vulnerability was discovered and published.

E-commerce security firm Sansec [disclosed](#) the attack and said that threat actors are using a layout template to maintain persistence on affected Magento servers. By combining the Magento layout parser with the beberlei/assert package, malicious actors can execute system commands. Sansec also shared that whenever the <store>/checkout/cart is requested, the sed command — which adds a backdoor to the CMS controller — is automatically executed. This is due to the layout block being tied to the checkout cart.

Magecart Attack Targets Cisco Merch Customers: CVE-2024-3410

In September 2024, The Register [reported](#) that Russia-based actors targeted a Cisco-branded online merchandise store by exploiting a critical bug in the Adobe Magento software, [CVE-2024-34102](#). This flaw allowed threat actors to launch XML external entity injection (XXE) and remote code execution (RCE) attacks on vulnerable systems and steal credit card information and other sensitive information from customers.

The Cisco merch site, which was reportedly hosted and managed by a third-party supplier, was running an unpatched Magento 2.4 (Enterprise) version. This vulnerable Magento version allowed malicious actors to inject malicious JavaScript code into the e-commerce site.

While Cisco addressed the security concern, the merch site was taken offline. The company also informed the limited number of affected customers of the issue. According to Cisco, customer credentials weren't compromised during the Magecart attack.

SQL Injection Risks in E-Commerce (Hs): CVE-2024-36680 (2024)

SQL injection (SQLi), a popular web hacking attack, occurs when a malicious SQL statement is inserted or injected into a query that an application makes to its database. [SQLi attacks](#) can result in malicious actors being able to view sensitive data accessible to the targeted application or belonging to other users, as well as modifying or deleting such data.

In June this year, threat actors exploited [CVE-2024-36680](#), a critical vulnerability in a premium Facebook module for PrestaShop, an open-source e-commerce platform. When successfully exploited, CVE-2024-36680 can allow malicious actors to trigger SQLi via HTTP requests.

The vulnerability was found in the pkfacebook add-on module created by Promokit, a company that develops Prestashop templates with custom-designed modules. The affected Promokit module enables website customers to log in, comment, and communicate with support agents using their Facebook account.

Supply Chain Attacks

E-commerce companies heavily rely on supply chains, which are intricate networks of third-party suppliers, to facilitate the efficient delivery of goods and services to customers. And because businesses provide access to supply chains to make their operations resilient and cost-efficient, they're great targets for compromise in the eyes of cybercriminals.

When malicious actors lock in on third-party tools, applications, and services with the goal of gaining unauthorized access to a targeted company's systems, a supply chain attack ensues.

In June 2024, more than 100,000 e-commerce websites that used the [Polyfill.io service](#) were affected by a supply chain attack. Polyfill.io is a third-party library that delivers [polyfills](#) or pieces of code that enable older or outdated browser versions to support new programming languages or web features.

Earlier this year, a Chinese company called Funnul bought the domain and service for Polyfill.io. After the buyout, websites that embed [cdn.polyfill.io](#) were observed to inject malicious code on mobile devices to redirect victims to malicious sites.

Ransomware Attacks

For a threat that's been around for [35 years](#), [ransomware](#) is still prominent, nefarious, and ever-evolving. Ransomware attacks involve threat actors limiting a user's ability to access files in an infected system via data encryption until a ransom is paid. Not being able to access critical data, [having it exfiltrated and leaked online](#), and even [losing it permanently](#) are what malicious actors are banking on to coerce victims to pay large ransom amounts.

Businesses in the retail and e-commerce space are popular ransomware attack targets as they have access to large volumes of personal and financial information from customers.

Early this year, global apparel and footwear company VF Corporation, shared that a December 2023 ransomware attack caused the unintended exposure of company data and the personally identifiable information (PII) of [35.5 million customers](#). VF Corporation owns popular active-lifestyle brands such as Timberland, Smartwool, Vans, and The North Face.

After detecting "unauthorized occurrences" on a portion of its IT systems on December 13, 2023, the company rolled out its incident response plan. As investigations were ongoing,

some systems were forced to shut down, affecting company operations and customer experiences.

The extent of the attack, the kind of data stolen, and the attack vector exploited in the incident were not disclosed.

In April 2024, [Skanlog](#), a Swedish third-party logistics company, experienced a ransomware attack purportedly launched by North Korea-based actors (although it should be noted that the company did not clearly state how they came about this attribution). Skanlog provides services to Systembolaget, a government-owned chain of liquor stores in Sweden.

According to a Euro News [report](#), the ransomware attack affected Skanlog's financial and inventory systems. During the height of the cyberattack, Systembolaget was forced to offer a limited liquor selection and cancel orders that included items that were impacted by the supply disruption.

Overall, the ransomware attack affected 15% of Systembolaget's sales volume.

Mitigations

Unfortunately, cyberattacks aren't going anywhere — threat actors will continue to wage attacks against highly bankable targets such as those belonging to the retail and e-commerce industry. As e-commerce companies continue to embrace digital transformation and omnichannel strategies, cybercriminals will have more interconnected avenues to explore, find weaknesses on, and exploit.

To avoid falling prey to cyberattacks and the grave reputational and financial consequences they come with, e-commerce companies must fortify their cybersecurity defenses by adopting a multi-tiered security strategy and implementing robust and comprehensive security solutions that [detect and thwart](#) sophisticated threats.

E-commerce businesses can fight off threats and mitigate risks by adopting the following security strategies:

- **Access Controls:** Use Identity and Access Management (IAM) tools to manage access to critical resources such as [databases](#) that house sensitive data.
- **Security Training:** Conduct regular security awareness training to educate employees and suppliers about threats and risks, as well as create strategies and protocols that everyone should follow during security incidents.
- **Incident Response Plans:** Create and regularly update incident preparation and response plans to address common attacks against e-commerce companies, including credential stuffing, supply chain, and ransomware.
- **Zero-Trust Culture:** Apply policies that require continuous verification, authorization, and validation of all users before it gains access to IT resources.
- **Triage List of Suppliers:** Assess suppliers and vendors for business criticality, security maturity, regulatory adherence, and supply chain risk management.
- **Email Security:** Implement strong [email security solutions](#) to keep employees from falling for phishing attacks or unknowingly downloading email-distributed malware.
- **Vulnerability Scanning:** Use [Vulnerability Management](#) solutions to gain visibility over network vulnerabilities and prioritize mitigation strategies using a risk-based approach.

For all of Trustwave SpiderLabs' research on the Retail sector, [please see the full series here.](#)

