Inside Intelligence Center: Financially Motivated Chinese Threat Actor SilkSpecter Targeting Black Friday Shoppers

Archived: 2026-04-02 11:46:50 UTC

Executive Summary

In early October 2024, EclecticIQ analysts uncovered a phishing campaign that targets e-commerce shoppers in Europe and USA, looking for Black Friday discounts. Analysts assess with high confidence that it was very likely orchestrated by a Chinese financially motivated threat actor, analysts dubbed as SilkSpecter. The campaign leveraged the heightened online shopping activity in November, the peak season for Black Friday discounts. The threat actor used fake discounted products as phishing lures to deceive victims into providing their Cardholder Data (CHD) [1] and Sensitive Authentication Data (SAD) [2] and Personally Identifiable Information (PII).

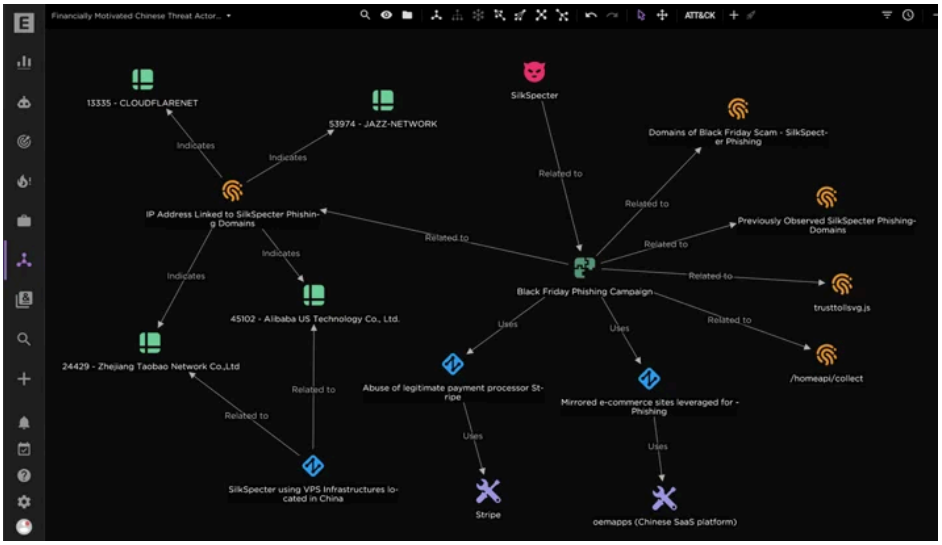

Figure 1 – Graph view for SilkSpecter activities in EclecticIQ's threat intelligence platform, Intelligence Center *(click on the image to enlarge).*

Threat actor SilkSpecter targeted victims' Cardholder Data (CHD) by leveraging the legitimate payment processor Stripe [3]. This tactic allowed genuine transactions to be completed while covertly exfiltrating sensitive CHD to a server controlled by the attackers. SilkSpecter enhanced the phishing site's credibility by using Google Translate to dynamically adjust the website's language based on each victim's IP location, making it appear more convincing to an international audience.

EclecticIQ analysts observed that prior to November 2024, SilkSpecter had launched similar phishing campaigns, all linked to a Chinese Software as a Service (SaaS) platform named oemapps [4]. Analysts assess with high confidence that oemapps very likely enables SilkSpecter to quickly create convincing fake e-commerce sites targeting unsuspecting users. These phishing domains predominantly use the .top, .shop, .store, and .vip top-level domains (TLDs), often typosquatting legitimate e-commerce organizations' domain names to deceive victims.

Tracking Black Friday Themed Phishing Domains with EclecticIQ Intelligence Center

Analysts used the EclecticIQ Intelligence Center to uncover a pattern among Black Friday-themed phishing domains that was very likely linked to the SilkSpecter threat actor.

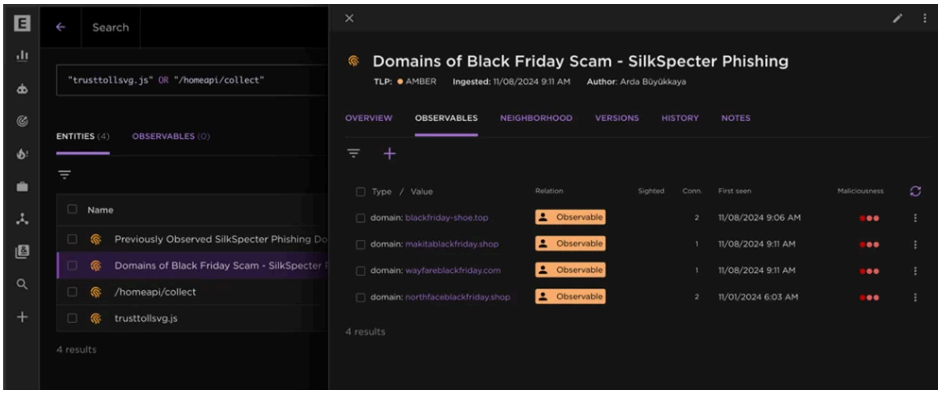

Figure 2 – Uncovering the pattern among Black Friday-themed phishing pages.

Each phishing page included "trusttollsvg," a deceptive icon designed to give the appearance of a trusted site, and a "/homeapi/collect" endpoint that informed attackers whenever a victim clicked or opened the URL - tracking the phishing campaign's success in real-time [5]. These distinct elements became crucial indicators, enabling analysts to identify additional discount-themed phishing domains associated with the SilkSpecter activity cluster.

Analyzing the SilkSpecter's Phishing Kit

SilkSpecter's phishing pages lured victims with a convincing Black Friday discount theme, often promoting an "80% off" offer to entice e-commerce shoppers into believing they were accessing exclusive deals. Once victims landed on the page, the phishing kit deployed several website trackers, including OpenReplay [6], TikTok Pixel [7], and Meta Pixel [8], to monitor the effectiveness of the attacks by collecting detailed activity logs from each visitor.

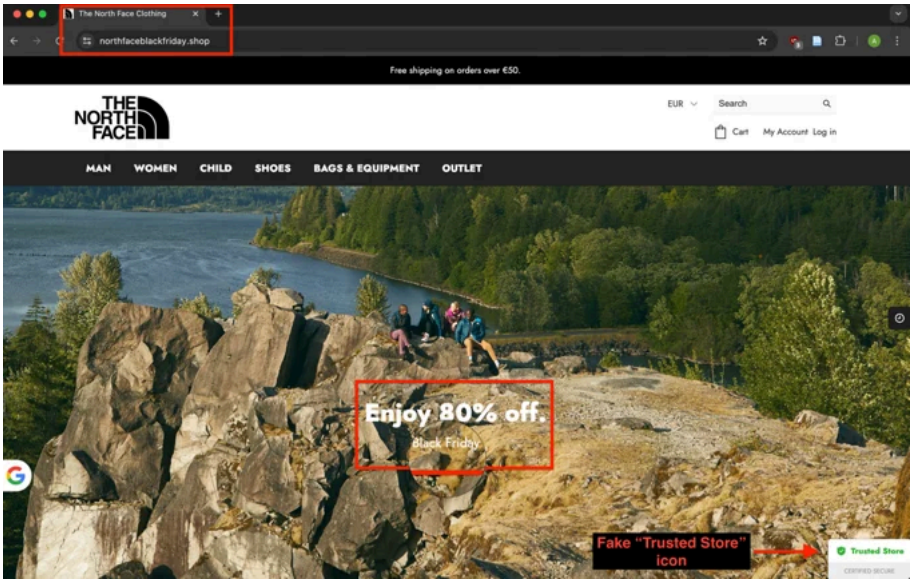

Figure 3 – Black Friday-themed phishing page with fake "Trusted Store" icon.

The phishing kit also captured key browser metadata, such as IP addresses, geolocation, browser type, and OS details. Using this information, the page is dynamically translated into the victim's language through Google Translate APIs, further increasing its authenticity.

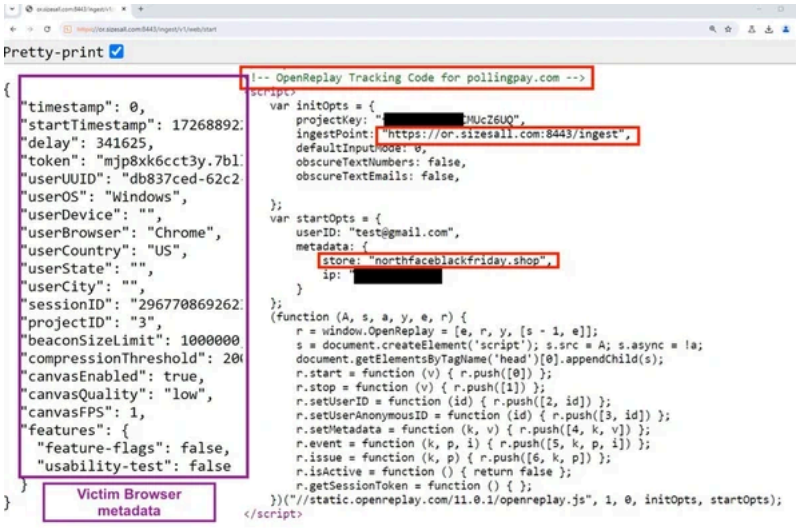

Figure 4 – Victim's browser metadata sent over another remote server likely managed by the attacker.

Victims entering their Personally Identifiable Information (PII) and banking details (CHD and SAD) for a fake discounted item submitted their information through Stripe, a legitimate payment service that SilkSpecter abused to process real transactions. After a payment was made, the phishing kit exfiltrated all entered details to an attacker-controlled server.

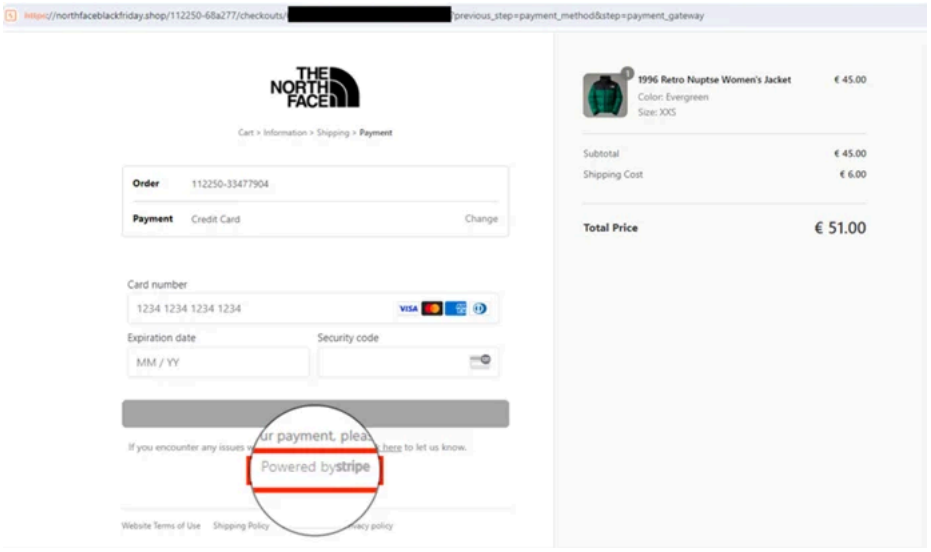

Figure 5 – Payment prompt screen on phishing page that uses Stripe.

Victims were also prompted to enter their phone numbers before completing their purchases. EclecticIQ analysts assess with medium confidence that this information could likely be leveraged in a second stage of the attack if SilkSpecter chooses to exploit the compromised credit or debit card details for financial fraud. The phone numbers could enable attackers to conduct vishing (voice phishing) or smishing (SMS phishing) attacks, deceiving victims into providing additional sensitive information, such as 2FA codes, personal identification details, or even account credentials.

By impersonating trusted entities, such as financial institutions or well-known e-commerce platforms, SilkSpecter could very likely circumvent security barriers, gain unauthorized access to victim's accounts, and initiate fraudulent transactions. After the victim initiates a payment request over Stripe´s APIs on the phishing website, the site covertly records the entire session and transmits the banking details to an external server hosted at longnr[.]com/payment/event-log[.]php. These additional requests, as seen in the intercepted traffic, indicate that the site is not only processing the payment through legitimate-looking means but is also capturing sensitive information, including card details, and relaying them to a separate server controlled by the attacker. This technique highlights how the phishing site is abusing legitimate APIs while simultaneously gathering and exfiltrating critical financial information.

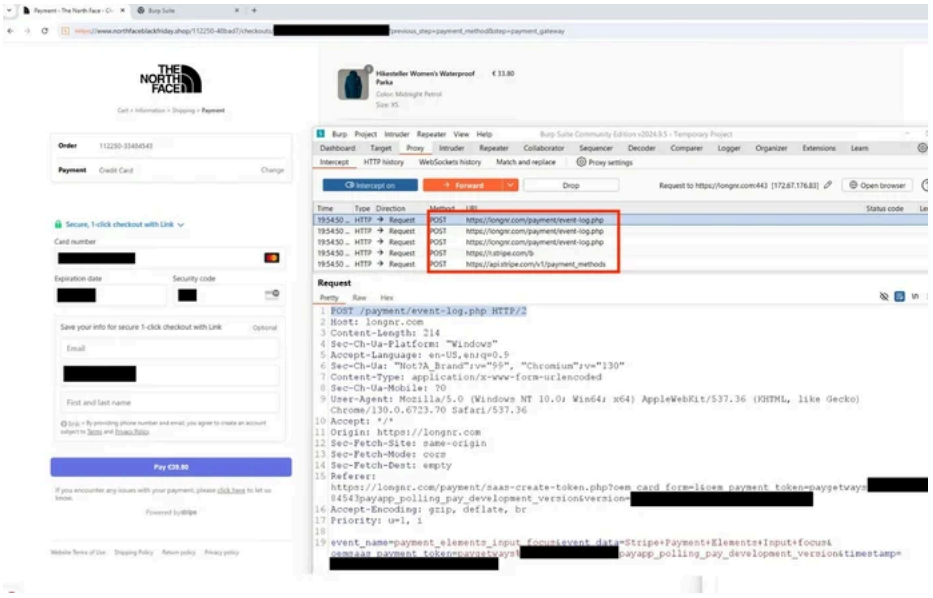

Figure 6 – Payment details exfiltrated over the attacker-controlled remote domain.

Analysts assess with medium confidence that SilkSpecter likely distributed these phishing URLs through social media accounts and search engine optimization (SEO) poisoning, leveraging a Black Friday discount theme as social engineering bait to deceive unsuspecting online shoppers.

Attribution to Chinese Threat Actor SilkSpecter

EclecticIQ analysts assess with high confidence that SilkSpecter is very likely a Chinese threat actor. This attribution is based on multiple indicators observed across several phishing campaigns:

Language Indicators:

- Each phishing page contained JavaScript code with Mandarin comments, suggesting the involvement of a Chinese-speaking developer.
- The "zh-CN" language tag in the HTML code strongly suggests that the phishing sites were developed by Chinese-speaking individuals.

```
const paramsStr = Object.keys(collectParams)
    .map((key) => `${key}=${collectParams[key]}`)
    .join("&");
const collectURL = "/homeapi/collect?" + paramsStr;
//页面卸载请求
if (requestType && requestType === "beforeunload") {
    console.log("发送页面卸载请求");
    try {
        navigator.sendBeacon ? navigator.sendBeacon(collectURL) : self.fireBeaconImg(collectURL);
    } catch (u) {}
}
try {
    fetch("/homeapi/collect", {
        method: "POST",
        headers: {
            "Content-Type": "application/json"
        },
        body: JSON.stringify(collectParams),
        keepalive:true
    });
} catch (u) {
    self.fireBeaconImg(collectURL);
}
};
```

Figure 7 – Mandarin Chinese language used in JavaScript comment.

Infrastructure Analysis

- SilkSpecter's infrastructure relied on Chinese-hosted Content Delivery Network (CDN) servers to serve images on Black Friday-themed phishing pages, indicating a preference for resources within China.

• Use of oemapps – a Chinese Software as a Service (SaaS) platform – enabled SilkSpecter to create and manage phishing e-commerce sites.
• Analysts linked SilkSpecter to over 89 IP addresses and more than 4,000 domain names associated with phishing activities.
• These domains were tied to specific Autonomous System Numbers (ASNs) and domain registrants connected to Chinese companies.

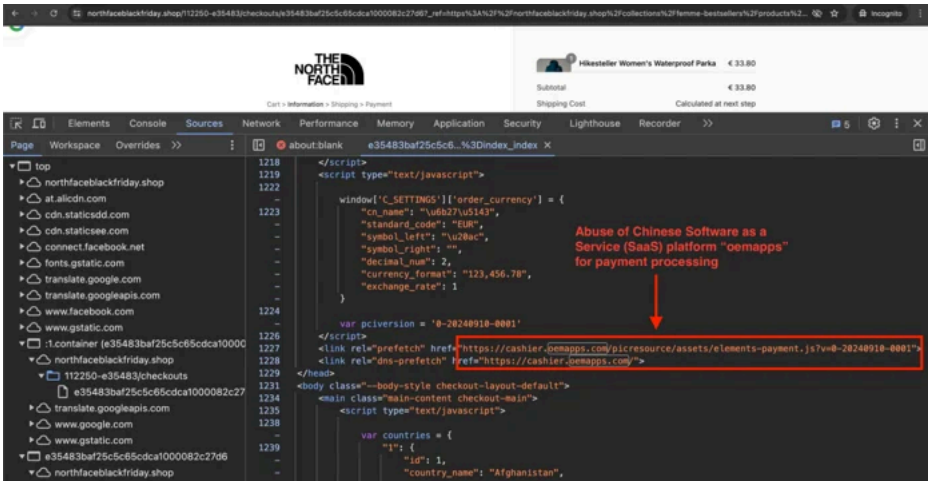

Figure 8 – Use of OEMAPPS library on phishing page.

Chinese Domain Registrars

- The most frequently used domain registrar in SilkSpecter's campaigns is West263 International Limited, a Chinese registrar.
- Other commonly used registrars include Hong Kong Kouming International Limited, Cloud Yuqu LLC, and Alibaba Cloud.
- Approximately 85% of the remaining IP addresses were routed through Cloudflare, allowing SilkSpecter to mask its true origin while benefiting from Cloudflare's scalable infrastructure.

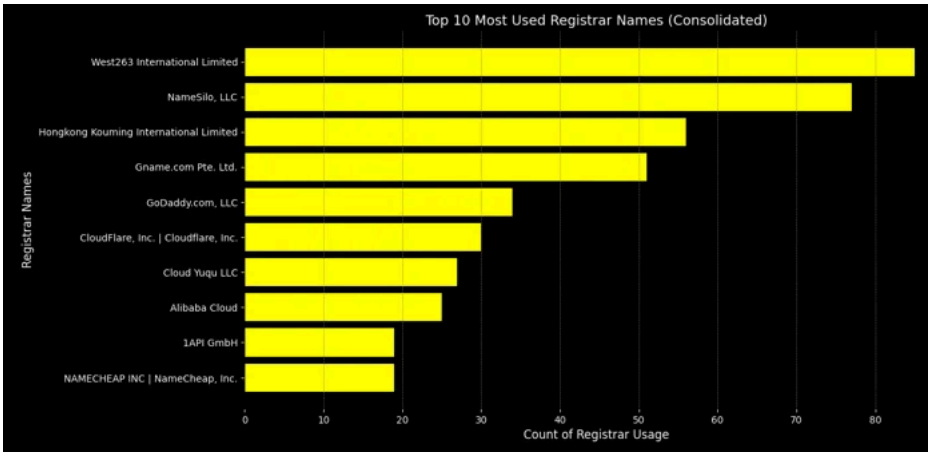

Figure 9 – Top 10 most used DNS registrar names by SilkSpecter.

nekodolar.top	XinNet Technology Corporation
mysteryboxonline.shop	Hong Kong Juming Network Technology Co. , Ltd | Hong Kong Juming Network Technology Co., Ltd.
qvcoutleteu.com	WEBCC | Web Commerce Communications Limited dba WebNic.cc
britaks.com	JIANGSU BANGNING SCIENCE & TECHNOLOGY CO. LTD | Jiangsu Bangning Science & technology Co. Ltd.
mereamazonwarehouse.site	West263 International Limited
horsewarestore.top	Hongkong Kouming International Limited
meforu.top	WEBCC | Web Commerce Communications Ltd
suicideboyshop.com	Hongkong Kouming International Limited
smaxiptv.com	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)
liverpoolmexi.com	West263 International Limited
llbeanclearance.com	Xiamen 35.com Information Co., Ltd.
betvplus.com	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)

Figure 10 – Other Chinese-originated registrar companies amongst phishing domains.

MITRE ATT&CK Analysis with EclecticIQ Intelligence Center

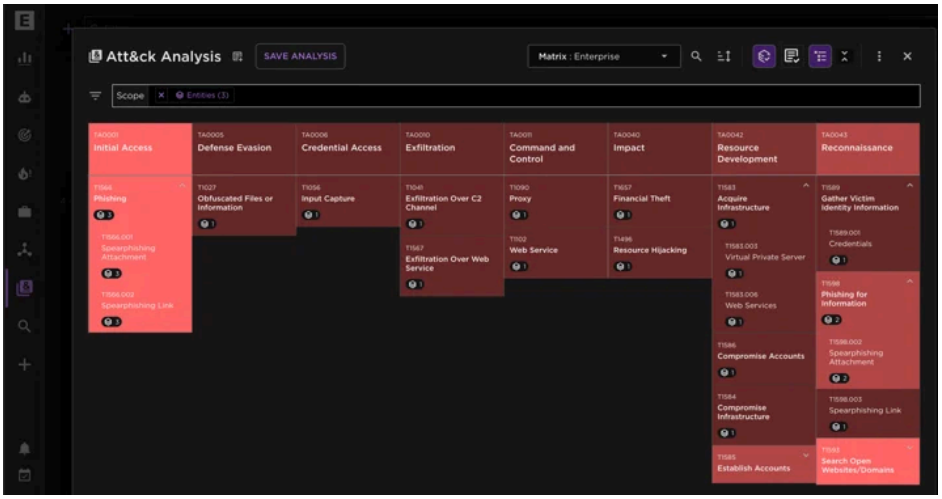

Figure 11 – MITRE ATT&CK Analysis tool and mapping of TTPs in EclecticIQ Intelligence Center.

Course of Action

Monitor for Indicators of Black Friday-Themed Phishing Campaigns

- **URL Patterns**: Monitor for URLs with themes like “discount,” “Black Friday,” or similar sales events. Additionally, look for the specific path “/homeapi/collect” and domains incorporating “trusttollsvg.”
- **Targeted IOC List**: Utilize IOC shared by EclecticIQ to identify and track SilkSpecter’s phishing domains with specific indicators (e.g., “/homeapi/collect” endpoint, Stripe API calls in unverified e-commerce URLs). Flag similar domains to alert for further investigation.

Monitor Network Traffic by Suspicious ASN Number Pattern

- **ASN Number Pattern Detection:** Set up monitoring rules or alerts for traffic communicating with specific ASNs linked to Chinese entities:
  - ASN 24429 - Zhejiang Taobao Network Co., Ltd.
  - ASN 140227 - Hong Kong Communications International Co., Limited
  - ASN 3824 - Cloud Yuqu LLC
  - ASN 139021 - West263 International Limited
  - ASN 45102 - Alibaba US Technology Co., Ltd.

Use these ASNs as a filter criterion in network traffic monitoring tools or SIEM (Security Information and Event Management) systems to detect suspicious connections to known Chinese infrastructure associated with SilkSpecter.

Minimizing the Attack Surface with Payment Safeguards

- **Use Virtual Cards for Safer Online Shopping:** Many banks offer virtual cards for online purchases, often with limited use or adjustable spending limits. A virtual card number is different from your main card and can be easily canceled if compromised.
- **Enable Spending Limits and Restrictions**: Contact your bank to set transaction limits, restrict international purchases, or require verification for online transactions. Many banks let you manage these settings through their mobile apps or online banking portal.

Indicator of Compromises (IOCs)

Hunting query for SilkSpecter phishing domains in Urlscan, looking for file hashes of reclusively used “trusttollsvg.js," and "/homeapi/collect.js":

hash:587b05cd8d59f9820d2cf168b07d46b1519d12ee7a2f7062a2490da0a99ccb50 AND
hash:9a049fe87fe472bd6e2a9f361b78a64576be9f827f9668af69bec03f5cbef0da

Black Friday Phishing Domains:

- northfaceblackfriday[.]shop
- lidl-blackfriday-eu[.]shop
- bbw-blackfriday[.]shop
- llbeanblackfridays[.]shop
- dopeblackfriday[.]shop
- wayfareblackfriday[.]com

- makitablackfriday[.]shop
- blackfriday-shoe[.]top
- eu-blochdance[.]shop
- ikea-euonline[.]com
- gardena-eu[.]com

References

[1] "Cardholder Data (CHD)," PCI Security Standards Council. Accessed: Nov. 10, 2024. [Online]. Available: https://www.pcisecuritystandards.org/glossary/cardholder-data/

[2] "Sensitive Authentication Data (SAD)," PCI Security Standards Council. Accessed: Nov. 10, 2024. [Online]. Available: https://www.pcisecuritystandards.org/glossary/sensitive-authentication-data/

[3] "Payments." Accessed: Nov. 10, 2024. [Online]. Available: https://docs.stripe.com/payments

[4] "首页-全国领先的跨境电商自建独立站SaaS建站系统." Accessed: Nov. 10, 2024. [Online]. Available: http://oemapps.com/

[5] "Search - urlscan.io." Accessed: Nov. 10, 2024. [Online]. Available: https://urlscan.io/search/#hash%3A587b05cd8d59f9820d2cf168b07d46b1519d12ee7a2f7062a2490da0a99ccb50%20AND%20hash%3A9a049fe87fe472b

[6] "OpenReplay: Open-Source Session Replay & Analytics." Accessed: Nov. 10, 2024. [Online]. Available: https://openreplay.com

[7] "About TikTok Pixel | TikTok Ads Manager." Accessed: Nov. 10, 2024. [Online]. Available: https://ads.tiktok.com/help/article/tiktok-pixel

[8] "Meta pixel: Measure, optimize and retarget ads on Facebook and Instagram," Meta for Business. Accessed: Nov. 10, 2024. [Online]. Available: https://en-gb.facebook.com/business/tools/meta-pixel

---