

# Threat Intelligence Report

■	■	■	■	■	■	■	■	■	■	■
■	■	■	■	■	■	■	■	■	■	■
■	■	■	■	■	■	■	■	■	■	■
■	■	■	■	■	■	■	■	■	■	■
■	■	■	■	■	■	■	■	■	■	■



FortiGuard®  
Threat Research



# Understanding Threat Actor Readiness for the Upcoming Holiday Season

Nov 15, 2024

| Medium

TLP

## Executive Summary:

As we approach the end of 2024, the upcoming holiday season and events like Thanksgiving, Black Friday, Cyber Monday, and Christmas bring millions of shoppers online with attractive discounts and limited-time offers. They also create ideal conditions for cybercriminals to exploit users and shoppers.

This report delves into the evolving threat surface of e-commerce, highlighting how cybercriminals leverage Remote Code Execution (RCE) exploits, Man-in-the-Middle (MITM) phishing kits, sniffers, and website cloning services to manipulate online transactions and gain access to steal sensitive data. It uncovers the dangers posed by the proliferation of holiday-themed deceptive domains and compromised e-commerce sites, emphasizing the critical risks to both shoppers and businesses during high-traffic shopping during the holiday season.

This report also offers recommendations for shoppers to protect themselves and for businesses to improve their defenses against these malicious activities. By understanding the tactics employed by threat actors and implementing proactive measures, both consumers and merchants can mitigate the risks associated with this critical time of year.

## Content:

- Understanding the Threat Surface
- Datasets Available on Darknet
- Darknet Services Empowering Threat Actors
- Deceptive Domains
- Targeting of E-commerce Platforms
- Conclusion
- Recommendations

## Key Observations

### Available Resources on the Darknet:

- **Datasets:** Gift cards, credit/debit card information, POS/payment gateway database, user credentials, and database/admin access to e-commerce sites are widely available for sale, particularly during the holiday season
- **Phishing and Spam Services:** Inbox spam services, phishing kits, and SMS spam tools are used to deceive shoppers with fake offers and promotions.
- **Website Cloning:** The creation of malicious replicas of trusted websites enables threat actors to steal sensitive user information.
- **Trafficker Services:** Threat actors leverage these services to drive traffic to fake or malicious websites.
- **Drop Services:** Sniffing tools are deployed on compromised sites to intercept and steal sensitive customer information like credit card details, login credentials, and transaction data. Threat actors have also developed brute-forcing tools designed to target e-commerce platforms.
- **Tools:** Sniffing tools developed are deployed on compromised sites to intercept and steal sensitive customer information like credit card details, login credentials, and transaction data. Also, Threat Actors have developed Bruteforcing tools that are designed to target E-commerce platforms.
- **Prompt Engineering:** Threat actors leverage AI models and prompt engineering to craft highly convincing phishing emails. These emails mimic the tone, branding, and writing style of legitimate organizations, such as banks or retailers, making them almost indistinguishable from genuine communications.

### Deceptive Domains:

- Thousands of holiday-themed domains have been registered, mimicking well-known brands (Amazon, BestBuy, Walmart) and domains related to events such as Black Friday, Thanksgiving, Cyber Monday, and Christmas.

- These domains often use keywords like "offer," "deals," and "discount" to lure unsuspecting shoppers.

Threats to E-commerce platforms:

- Sniffers, brute-forcing tools, and malware target popular e-commerce platforms like Adobe Commerce (Magento), WooCommerce, Shopify, and OpenCart.
- Threat actors exploit weak configurations, outdated plugins, and unpatched software to gain unauthorized admin access to platforms.

Understanding the Threat Surface

The Darknet provides threat actors with a wide range of opportunities, enabling them to carry out various types of attacks. The image below highlights the threat surface for the upcoming holiday season. It provides insights into what datasets are available to threat actors on the Darknet that are being traded or leveraged for malicious purposes. Threat actors with limited knowledge or skills can also leverage services designed to deceive users and steal sensitive information. The threat surface also includes deceptive domains registered in the past three months and e-commerce platforms that could be at a high risk of targeting since the holiday season is the right time to monetize attacks and maximize gains.



Figure 1: Holiday season threat surface overview

Datasets Available on the Darknet

This section explores datasets commonly available on the Darknet that could be used during the holiday season. It highlights how threat actors weaponize these to exploit increased online activity and shopping during the holidays.

Stolen Gift Cards of E-commerce Sites

During the holiday season, gift cards are very attractive—making them prime targets for cybercriminals. Stolen gift cards are often obtained through brute-force attacks on poorly secured accounts on e-commerce sites or by purchasing these gift cards using stolen credit cards. These gift cards are then circulated on Darknet markets at cut-rate prices. Threat actors capitalize on holiday demand by reselling these stolen gift cards, which are attractive to buyers due to their anonymity and flexibility. For consumers, using stolen gift cards may seem like a quick discount, but they often become victims when the cards get canceled or reported as stolen, leaving them with a useless purchase.

Below is an example of stolen gift cards available for sale on Darknet marketplaces. This type of advertisement presents both a financial and reputational challenge for retailers, as they face the dual impact of loss and decreased customer trust.

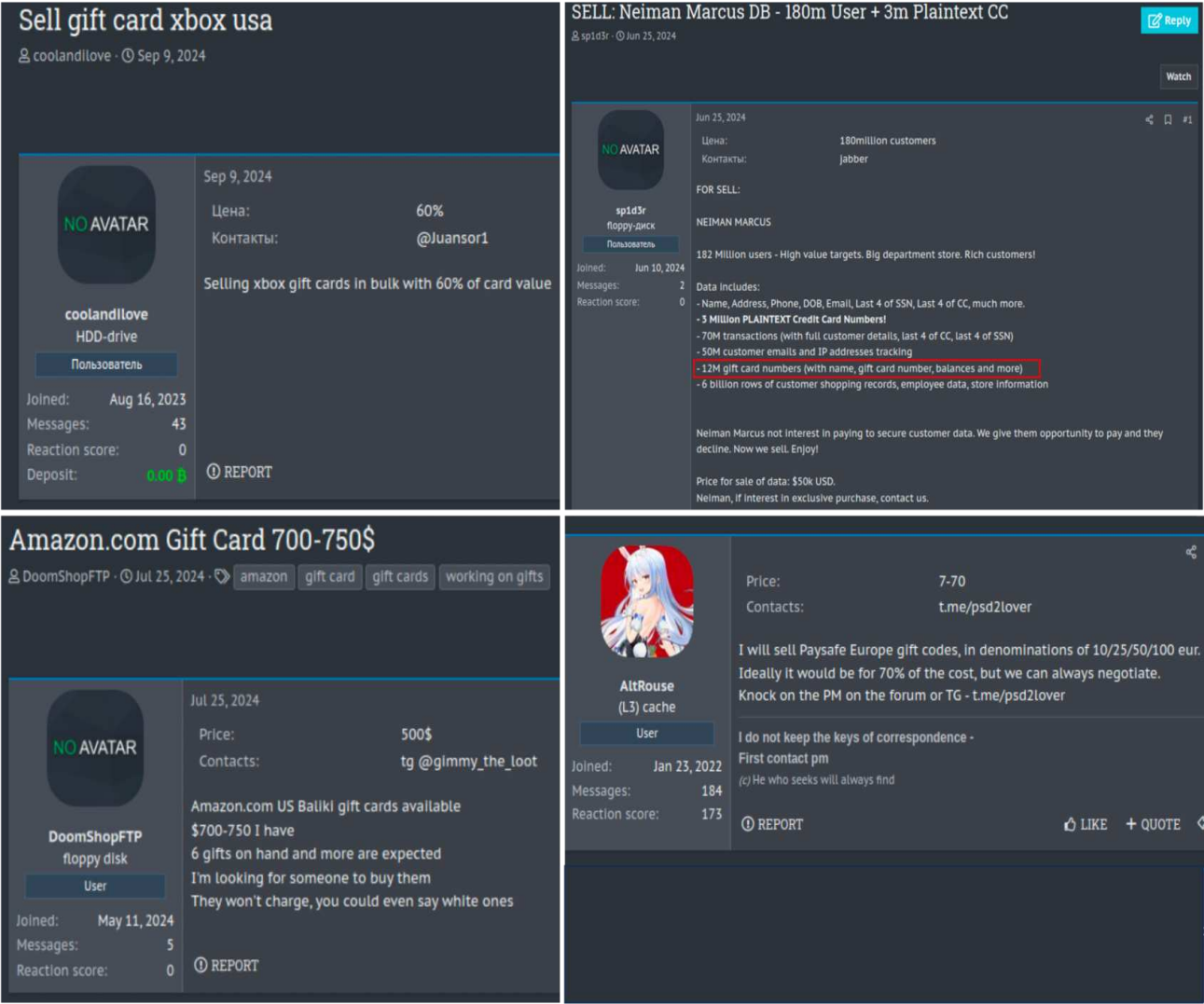



Figure 2. Gift card advertisements

POS/Payment Gateway Databases

Point-of-sale (POS) and payment gateway databases are critical components of modern commerce, facilitating seamless transactions between merchants and customers. These databases store sensitive information such as payment card details, transaction logs, API keys, and merchant account credentials. However, as highlighted in the following screenshot, cybercriminals use these valuable resources as prime targets on Darknet forums

- The LoyLap breach illustrates how compromised payment systems can expose sensitive payment and loyalty program data. This type of data is often sold or leaked on Darknet forums, enabling unauthorized transactions and customer data theft.
- Stolen POS data allows attackers to create fake merchant accounts, conduct unauthorized transactions, or manipulate payment systems to redirect funds.

CyberNiggers] LoyLap Data Breach - Leaked, Download!  
 by 888 · Friday October 25, 2024 at 02:23 PM



**#88**

Kingpin

---

**GOD**

A S

Posts: 180  
Threads: 85  
Joined: Aug 2023  
Reputation: 2,362

10-25-2024, 02:23 PM (This post was last modified: 10-25-2024, 03:19 PM by 888.)

Hello BreachForums Community,

Today I have uploaded LoyLap Data Breach for you to download, thanks for reading and enjoy!

# LoyLap

LoyLap is a software company that provides customizable closed loop payment systems including Gift Card, Loyalty, Online Ordering, Self Checkout and Cashless systems. It is currently used by 3300 businesses.

Stolen Credit/Debit Card Information

Combo Lists Containing User Credentials

Combo lists are massive compilations of leaked usernames and passwords, often assembled from previous data breaches. As more people shop online during the holiday rush, these lists become especially valuable for threat actors. Criminals use these lists for credential stuffing attacks, attempting to log in to various e-commerce sites using stolen credentials. If successful, they gain access to a victim's shopping accounts, potentially leading to unauthorized purchases or further exploitation. With so many accounts compromised, both consumers and retailers face significant risk, as attackers often leave a trail of financial and personal damage.

Below are some sample advertisements for combo lists on Darknet forums. These ads offer spamming and cracking tools along with 'HQ combos'—lists of stolen credentials, including emails and passwords. Such resources pose a major threat during the holiday shopping season as threat actors can exploit these credentials to access accounts on popular shopping platforms, make fraudulent purchases, or deplete gift card balances. Even more concerning is the potential for threat actors to carry out large-scale phishing campaigns, tricking consumers with fake Black Friday, Thanksgiving, or Christmas deals.

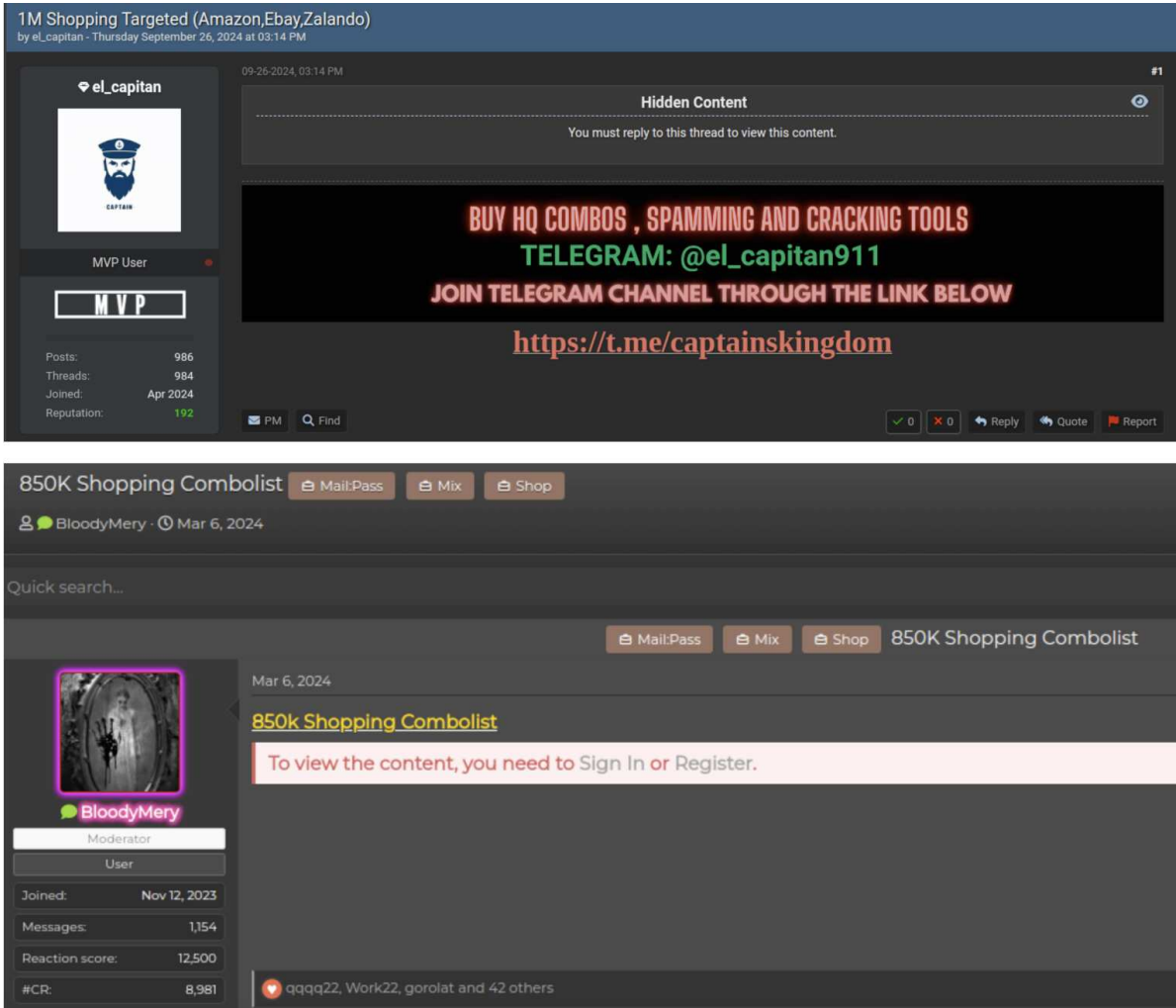


Figure 5. Darknet combolist advertisements

Compromised E-commerce Sites Database

Compromised databases of e-commerce websites are another high-value target on the Darknet. These databases typically contain sensitive customer PII data, including names, addresses, email IDs, and purchase histories. During the holiday season, threat actors target e-commerce sites with poor security, exploiting vulnerabilities to gain access to their databases. Once acquired, the data is sold to other criminals who use it for various malicious activities, from targeted phishing attacks to synthetic identity fraud. For companies, a database breach can be devastating, leading to regulatory fines, loss of business, and brand damage as customers question the security of their personal information.



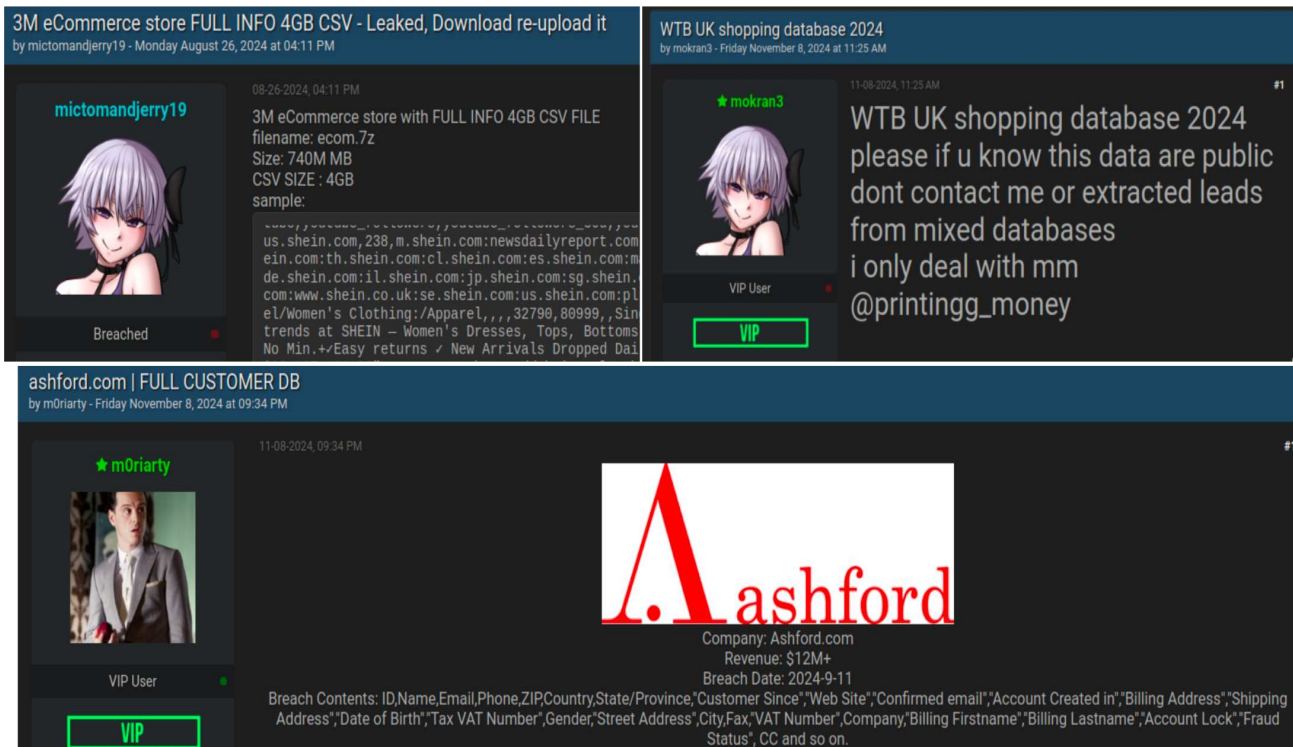


Figure 6. Compromised e-commerce site databases

### Stealer Logs (URLs, Email IDs, Passwords, Cookies)

Stealer logs are digital footprints collected by malicious software that captures information like browsing history, email credentials, passwords, and cookies. This data is sold on Darknet marketplaces, giving threat actors access to a wide range of user accounts. In the shopping season frenzy, people often log into numerous e-commerce accounts, increasing their vulnerability. Threat actors use this information for account takeover or to sell to other criminals who then exploit it for financial gain. Businesses also feel the impact, as compromised accounts can lead to loss of sales and challenges with fraud detection.

Stealer: 

All

System: 

All

Country: 

United States (115814)

Links: 

x amazon.com
x bestbuy.com
x walmart.com

ONLY WITH COOKIES: ☐

State: 

All

City: 

All

Zip:

ISP: 

ADSL Maroc telecom

Outlook: 

@domain.com

Per page: 

10

Vendor: 

All

Price: 

0 \$

10 \$

Search

Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
lumma	Pennsylvania ISP: Datacamp Limited	the-hive.be   nzbforu.com   cs.rin.ru   account.proton.me   moddb.com   account.proton.me   ibuypower.com   gmail.com   nb.fidelity.com   gmail.com   Show more...	-	-	archive.zip	2024.11.08 0.02Mb	Nu####ez (Diamond)	\$ 10.00	Buy
lumma	California ISP: Charter Communications Inc	amazon.com   facebook.com   amazon.com   boyfriendv.com   mrdeepfakes.com   subscribestar.adult   accounts.google.com   poshmark.com   login.live.com   login.aliexpress.com   Show more...	-	-	archive.zip	2024.11.08 0.10Mb	Nu####ez (Diamond)	\$ 10.00	Buy
lumma	Tennessee ISP: AT&T Services, Inc.	cltexam.com   login.yahoo.com   cltexam.com   login.yahoo.com   accounts.google.com   academicrecords.net   legacyhc.org   amazon.com   cbaccount.collegeboard.org   account.collegeboard.org   Show more...	-	-	archive.zip	2024.11.09 0.55Mb	Nu####ez (Diamond)	\$ 10.00	Buy
lumma	Virginia ISP: Comcast Cable Communications	account.live.com   discord.com   app.bold.org   us05web.zoom.us   discord.com   logon.mcafee.com   webportalapp.com   app.sp2.org   advanceauto.wd5.myworkdayjobs.com   discord.com   Show more...	-	-	archive.zip	2024.11.09 0.49Mb	Nu####ez (Diamond)	\$ 10.00	Buy
lumma	Florida ISP: Comcast Cable Communications, LLC	platinmods.com   auth.amersc.com   amazon.com   netflix.com   accounts.google.com   restream.io   disneyplus.com   thetechgame.com   bigbadtoystore.com   broward.onelogin.com   Show more...	-	-	archive.zip	2024.11.09 0.40Mb	Nu####ez (Diamond)	\$ 10.00	Buy
lumma	Illinois ISP: Comcast Cable Communications	app.hubspot.com   app.hubspot.com   clover.com   clover.com   clover.com   clover.com   app.hubspot.com   app.hubspot.com   clover.com   clover.com   Show more...	-	-	archive.zip	2024.11.09 0.26Mb	Nu####ez (Diamond)	\$ 10.00	Buy
lumma	West Virginia ISP: Comcast Cable Communications	accounts.google.com   amazon.com   authenticate.riotgames.com   khanacademy.org   users.nexusmods.com   signin.rockstargames.com	-	-	archive.zip	2024.11.09 0.04Mb	Nu####ez (Diamond)	\$ 10.00	Buy
lumma	Pennsylvania ISP: Verizon Business	amazon.com   facebook.com   sharemania.us   amazon.com   secure.dol.state.nj.us   audiomack.com   secure1.peco.com	-	-	archive.zip	2024.11.09 0.78Mb	Nu####ez (Diamond)	\$ 10.00	Buy
lumma	Alabama ISP: Charter Communications	zoro.vc   vrchat.com   amazon.com   roblox.com   duelingnexus.com   9animetv.to   paypal.com   anilist.co   vrchat.com   accounts.google.com   Show more...	-	-	archive.zip	2024.11.09 0.48Mb	Nu####ez (Diamond)	\$ 10.00	Buy
lumma	Ohio ISP: Charter Communications	mobile.twitter.com   minecraft.net   apply.commonapp.org   android.snapchat.com   greatoaks.payschools.com   facebook.com   android.khanacademy.org   clubhousevr.com   login.live.com   gamestop.com   Show more...	-	-	archive.zip	2024.11.09 0.10Mb	Nu####ez (Diamond)	\$ 10.00	Buy

1
2
3
4
5
6
7

Buy all logs from this page

Figure 7. Logs available on a stealer marketplace

## Admin Access to E-commerce Sites

Access to e-commerce platform admin panels is among the most coveted items on the Darknet. With admin access, attackers can manipulate products, alter pricing, and, more importantly, access customer databases directly. During Black Friday and Cyber Monday, attackers ramp up their efforts to gain admin access, using techniques like phishing, credential stuffing, or exploiting unpatched vulnerabilities. A compromised e-commerce site has far-reaching effects: customer trust is eroded, revenue is impacted, and the company faces possible regulatory scrutiny.




## Selling private WooCommerce WorldWide (USA+UK+Europe) 140 orders daily

& Dementorfraud · Feb 28, 2024

**ESCROW AVAILABLE IN THIS THREAD!**

New deal

---



**Dementorfraud**  
 Premium  
 Premium

Joined: Jan 17, 2024 Messages: 109 Reaction score: 15 Escrow deals: 11	Feb 28, 2024  Цена: 16000 Контакты: 41F772EB5FD57D6114FF5094F592D198CDE02049682CF6CC7ABE30B9E4AC228739400F980BF
---	--

Selling private WooCommerce WorldWide (USA+UK+Europe) 140 orders daily  
 Payment available only with card  
 Native payment form - 80-85% orders, rest of orders - PayPal redirect (most of them from Asians)  
 Private access from stealer, no neighbors  
 Selling to one hand only  
 Price 16000\$, negotiable in some cases  
 Escrow +  
 After last bid 12 hrs

Buying BrainFree Keys from all your shops

# Looking for hacker to breach custom target (woocommerce, bigcommerce)

Kool E · 🕒 Apr 16, 2024

NO AVATAR

Kool E

CD-диск

Пользователь

Joined: Feb 23, 2024

Messages: 10

Reaction score: 1

Apr 16, 2024

Цена: ?

Контакты: tox CC33F7FBE140D6A009B9B4CA6D3E1D6144E46564562FD95DCA4F6BFC55DC6A6471B9ACAB2CEF

I am looking for a hacker to breach a custom target.

One target is woocommerce website, other is bigcommerce website. Both from small companies in USA. Later I will have more targets.

Customer and order database is required.

I want silent work, no public announcement, no ransom, nothing that could make target feel insecure.

Escrow will be used of course. Please let me know your tox or session ID.

2000\$

🕒 REPORT

Figure 8. Admin panels access for sale


## Darknet Services Empowering Threat Actors

This section analyzes Darknet services, showcasing how these services empower threat actors with limited technical knowledge to exploit vulnerabilities and deceive shoppers during the holiday season.

## Website Cloning Service

A website cloning service enables individuals with little to no technical expertise to create a copy of legitimate e-commerce or other trusted websites. These replicas mimic the original site's design, layout, branding, and functionality. Cloned websites are designed to deceive users into believing they are interacting with a genuine website, tricking them into providing sensitive information such as login credentials, payment details, or personal data.

The actor "w3t0n1337," shown below, was advertising a website cloning service and demonstrated its functionality by mirroring a trusted e-commerce site. As per the claim in the following thread, this cloning service can even clone sophisticated websites like Amazon.



**w3tts0n1337**  
(L3) cache

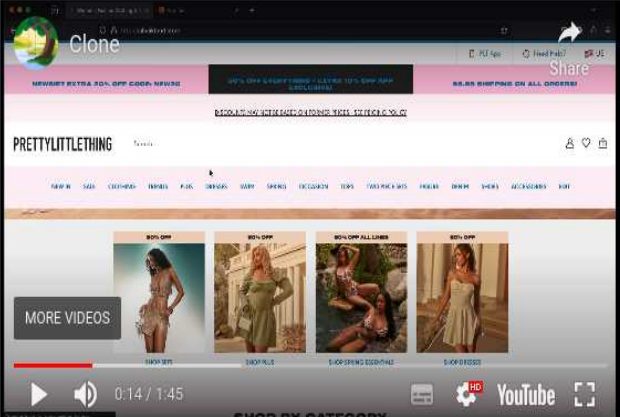
Пользователь

Joined: Feb 3, 2024  
Messages: 216  
Reaction score: 7  
Escrow deals: 10

Apr 21, 2024

Цена: 799

Контакты: tg: @w3tts0n1337 / tox : A798B7AE8F563D32007B0D80094693ADD141000D81460420AA7FD4ABC92D9A016DE3769057E3



With this script you will be able to mirror any website you want and change all its content with Javascript.

**What do you get?**

- Full source code
- Help with Installation on hosting
- Help with cloning any website you want.


**Accept escrow!**

REPORT

Figure 9. Website cloning service)

## Develop Custom Phishing Sites

Cybercriminals offer custom phishing site development to create tailor-made websites that mimic specific targets, such as banks, e-commerce platforms, or social media sites. These custom sites are highly realistic, replicating legitimate websites' branding, design, and functionality to deceive users into entering sensitive information like login credentials, payment details, or personal data. Unlike generic phishing kits, custom phishing sites are tailored to the attacker's needs, often including specific features, multi-language support, or integration with other malicious tools to maximize their effectiveness and bypass security measures.



**I develop fake store fake shop Clone ecommerce website Products scrapper Lifetime updates**

By codeinventory, Monday at 01:20 PM in [Job] - search, execution of work

Follow 1

Start new topic Reply to this topic

codeinventory

Posted Monday at 01:20 PM

Dear clients, today I am here presenting to share with you one of the most complete and complex platform called fake store, i have taken many details into account when programming to meet your specific needs and objectives and it is time to share with a limited number of people.

Here are few features listed, but custom development also available.

**Service for scrapping products from other websites also available.**

- ✓ ANTIBOTS
- ✓ +550 PRODUCTS READY
- ✓ FAKE REVIEWS
- ✓ READY FOR SPAM
- ✓ GUEST CHECKOUT
- ✓ AUTO DETECT ADDRESS
- ✓ SMTP SYSTEM
- ✓ CLOAKER V9
- ✓ LIVE CHAT SYSTEM
- ✓ STAFF SYSTEM
- ✓ TICKET LIVE SYSTEM
- ✓ CHECKOUT SYSTEM
- ✓ PRODUCT PAGE
- ✓ STRIPE AND +10 GATEWAY
- ✓ API PAYMENT MANAGE
- ✓ SYSTEM FOR CC + OTP
- ✓ ADD ANY FUNCTION
- ✓ ADD ANY GATEWAY
- ✓ Pack+500 products 500\$
- PRICE: 2000USD

---

### Crafting Email Lures using AI Models

Threat actors use AI models, like ChatGPT or other advanced language models, to create convincing phishing emails. AI-generated emails can replicate the tone, branding, and writing style of major retailers, banks, or courier companies, making them nearly indistinguishable from legitimate communications. With prompt engineering, attackers can also quickly generate large volumes of unique phishing emails, reducing the chance of detection by spam filters.

In the following forum post, the threat actor mentioned multiple prompts for generating phishing emails using AI models for numerous occasions, including New Year.

 Reply

◀ Prev 1 2 3 Next ▶



Joined:	Dec 19, 2018
Messages:	2,673
Solutions:	10
Reaction score:	3,572
Deposit:	0.0001B

### Prompt #1

Hey [name],

```
kind regards,  
[name]
```

Hey [Name],

Kind regards,  
[Name]

Hey [name],

[name]

Hey [Name],

Here's to a wonderful year ahead and the creation of cherished memories. May we find comfort and joy in the little moments and embrace the adventures that lie ahead.

Wishing you all the best,  
[Name]

P.S. Feel free to share your own New Year's wishes and resolutions with me! It's always wonderful to hear how others plan to embrace the year ahead.

Trafficker services refer to malicious platforms or tools that drive traffic to fake or malicious websites, often to enhance the credibility of phishing campaigns, spread malware, or steal sensitive data. The traffickers' role in driving massive traffic to fraudulent websites ensures that more shoppers are lured into making purchases and risk having their credit card details, personal information, and payments stolen. The organized structure of the operation, which includes profit-sharing incentives and proof of high earnings, suggests a well-coordinated effort to exploit consumer trust and urgency during the holiday rush.

The threat actor "masterref" posted the following recruitment ad that poses a serious phishing and financial fraud threat to shoppers during high-spending seasons like Black Friday, Cyber Monday, and Christmas. The ad reveals a scheme involving fake online shops mimicking legitimate retailers and offering irresistible discounts on popular items such as electronics and jewelry. These fraudulent sites are strategically promoted through legitimate advertising platforms like Facebook, Instagram, Google, and Bing, enhancing their visibility and making them appear more credible to unsuspecting shoppers.

M

gigabyte

139 posts

Joined 11/14/23 (ID: 156152)

Activity carding

Masterref

Posted October 31 (edited)

Hello colleagues.

In view of the upcoming holidays and sales: Black Friday, Cyber Monday, Christmas, we are recruiting traffickers for our fake shops (jewelry, electronics, household appliances, etc...)

Country - US, interesting - FB, Instagram, Google, Bing.

We will show proof of past profits (500k+), we are ready to deposit money into the guarantor.

We don't pay in advance, unless you have decent reviews and proof.

Those who are testing, interested or just want to chat, please pass by!

Work only on a percentage of profit, everything is transparent and clear (cashing, accounting, etc.)

According to the rules from \$1

Please do not write hello, leave your contact information, but provide a short CV.

Edited October 31 by masterref

Quote

Follow 2

Start new topic


Reply to this topic

Figure 12. Traffickers for the upcoming festive season

Drop Services

On October 21, 2024, the threat actor "primum\_leo" on the dark web forum WWH Club posted an advertisement for their "drop service." A drop service offers temporary addresses or accounts to receive and forward goods or money obtained through fraud, often used in schemes like credit card fraud, reshipping stolen goods, or money laundering. The post suggests that the drop accounts or addresses are based in the United States, which may be desirable for reshipping goods or committing fraud that targets US merchants.

TC



primum\_leo

Verified

Project participant

Registration: 22 Mar 2015

Messages: 329

Reactions: 261

Total sales: \$0

General purchases: \$14,431

Donated: \$0

GUARANTEE: 2

31 Oct 2024

New

#623

A new set of drops for Black Friday has started, we add new addresses to the admin panel daily! We are working!

The best USA Drops! High-quality shipping of any packs \$40 + Buy list with the highest percentages on the market! CARDERS BROTHERHOOD

<https://www-club.link/index.php?threads/luchshie-usa-dropy-kachestvennyj-pereysl-ljubyx-pakov-40-skup-list-s-maksimalnymi-procentami-na-rynke-carders-brotherhood.120906/>

Figure 13. Drop services


Sniffing Service

Sniffing services involve deploying a "sniffer" on online shop websites to intercept sensitive customer information such as credit card details, login credentials, and other transaction-related data. The service is advertised as compatible with various platforms, including Adobe Commerce (Magento), OpenCart, WordPress, and PrestaShop, and can target both self-written and widely-used content management systems (CMS).



# Partnership. I'll put sniff on shops

Ineversober111 · Sep 10, 2024 · cc sniffer partnership shop sniffer



**Ineversober111**  
RAID array  
User

Joined: Oct 28, 2022  
Messages: 80  
Reaction score: 9  
Deposit: 0.08 £

Sep 10, 2024

Price: 100  
Contacts: tg: @sou1catcher

I put a sniffer on shops

Conditions:

Form on the site: from 3 orders per day  
IFrame/Redirect: from 30 orders per day

Any CMS is suitable, including self-written ones: Magento, OpenCart, WordPress, Prestashop, etc.

Type of access: Shell, hosting, Admin panel

For partners:

Dedicated panel with statistics on cards, you will have access to it  
Up to 24 hours for installation  
Your reward is 70%

REPORT

Figure 14. Intercepting customer information using sniffing services on well-known e-commerce platforms

## Inbox Spam Service

Spam services are designed to send mass unsolicited emails to large groups of recipients. Using advanced methods to bypass spam filters, these emails often land directly in the recipient's inbox. Leveraging holiday season themes like "Black Friday Deals," they aim to lure users into acting quickly without verifying the email's legitimacy. These services are commonly advertised on dark web forums and hacker marketplaces, enabling cybercriminals to distribute:

- **Phishing Links:** Redirect victims to fake websites to steal sensitive information, such as passwords or payment details.
- **Malware:** Spread harmful attachments or links that compromise devices with viruses or spyware.
- **Scams:** These involve promoting fraudulent offers, fake gift cards, or bogus holiday deals to deceive users into handing over money
- **Counterfeit Promotions:** Advertise fake or malicious products disguised as genuine discounts.

Going by the alias "InboxInvasion," the threat actor in the following image posted an advertisement for an "Inbox Spam" tool that can directly impact the Black Friday shopping season. It enables the spamming of inboxes with fake deals, phishing links, and fraudulent offers, tricking consumers into revealing sensitive information like passwords and payment details. Many are also directed to fake shopping sites that mimic genuine retailers, making the scams even more convincing.

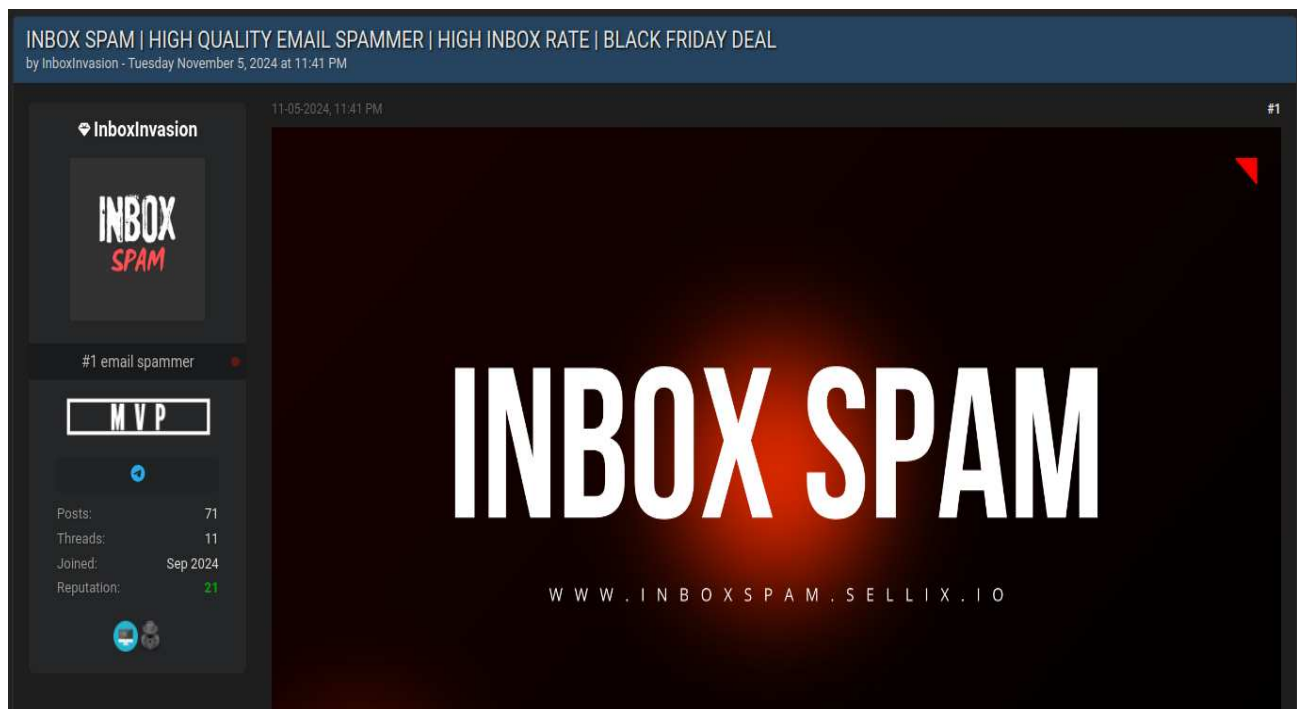




Figure 15. Inbox spam service for sending phishing emails

Similar spamming services are also available for SMS, enabling cybercriminals to target mobile users by sending bulk text messages for malicious purposes. These services are designed to mimic legitimate communications, making it difficult for users to distinguish between genuine and fraudulent messages. A threat actor using the alias "SagaSMS" advertised a bulk SMS spam service with features such as bulk SMS sending and sender ID spoofing, allowing messages to appear as if they are coming from trusted sources like banks or retailers. Additionally, the service claims to support message delivery to over 100 countries, enabling attackers to target victims globally. In terms of affordability, the service offers approximately 31 messages for USD 1.



## PHISHING SMS BULK SMS SPAM GATEWAY - Send SMS VIA InstantSMS web-app.

By SagaSMS, September 3 in [Mobile communication] - receiving calls, sms, info lookups, detailing



**SagaSMS**  
byte

Paid registration  
1  
8 posts  
Joined  
08/30/24 (ID: 176072)  
Activity  
cnam / spam  
Deposit  
0.000138 \$

Posted September 3

### Welcome to InstantSMS.eu

Your ultimate platform for online SMS spam, bulk messaging, and spoofing services.

Your ultimate platform for online **SMS spam, bulk messaging, and spoofing services.**

With InstantSMS.eu, you can:

- Easily send bulk SMS, spam, and spoofed messages.
- Customize your Sender ID to suit your needs.
- Enjoy fast, reliable, and secure online performance.
- Start for as low as ~0.03 EUR per message—one of the most affordable options available.
- Reach a global audience, supporting over 100 countries.
- Pay securely with cryptocurrency (Only crypto accepted).
- Auto top-up balance

**Website: InstantSMS.eu/**

**SMS Panel ONLINE: InstantSMS.systems/**

**Private SMS Panel: Contact me**

Join our thousands of satisfied users today by starting on our Telegram Channel at <https://t.me/InstantSMSeu>

Figure 16. Bulk SMS spam service

## Phishing Kits

Phishing kits allow attackers to set up advanced phishing operations that intercept and manipulate user data during real-time interactions. For instance, they can replicate login processes and steal credentials, cookies, and session tokens from victims accessing legitimate websites. Such kits usually come with the following features:

- High customization options, such as creating fake pages for platforms like Facebook, Binance, or Dropbox.
- Services are sold at varying price points (\$100–\$1,000) based on complexity and customizations.
- Support for cloning login pages and bypassing multi-factor authentication (MFA) by intercepting session cookies.

The threat actor "MertyeDushi" advertised the following Man-in-the-Middle (MITM) phishing kit. MITM phishing kits are more advanced than standard phishing kits because they operate in real-time, acting as a proxy between the victim and the legitimate website. Unlike static phishing kits that only clone websites to steal credentials, MITM kits can intercept live communications, capture session tokens, cookies, and OTPs, and even bypass multi-factor authentication (MFA). This makes them highly effective for account takeovers, stealing financial details, and maintaining access without repeated logins.

**[SELL] MITM PHISHING KITS**  
By MertyeDushi, May 12 in [Software] - malware, exploits, bundles, crypts

Follow 3

Start new topic Reply to this topic

MertyeDushi  
byte  
MD  
Paid registration  
15 posts  
Joined  
03/14/22 (ID: 127094)  
Activity  
безопасность / security

Posted May 12

Hello! I'm back.

My name is MertyeDushi and I specialize in software development in the area of Man-in-the-Middle (MITM) phishing.

Over the past few years, I have successfully collaborated with various developers, provided my services through resellers, completed custom jobs, and, together with colleagues, launched a successful PhaaS.

Currently, I am creating settings for various sites, but I am not interested in using them for spam mailings. Perhaps you can help me with this. Here is the current list of services and conditions:

### Pricing

1. **\*\*High quality MITM setup:\*\***  
Price: about \$1000 per site. Includes customization with custom additions or additional features.  
Examples: settings for the Office page (supports all types of authorization), Facebook (grab the balance of an advertising account), Binance (grab the total account balance).
2. **\*\*Setting up AiTM (authorization data + cookies):\*\***  
Price: about \$300-500 per site.  
Examples: Dropbox, Amazon, Yahoo, Twitter, QQ.
3. **\*\*Simple pages and consultations:\*\***  
Price: \$100-\$300.  
Includes creating a clone of a page in PHP, assistance in solving problems, site research, expert opinions.  
Fixes/updates for existing configs/sites. Minor tasks.

### Reliability

If an offer seems too good to be true, I suggest using the Guarantor service. I will provide a working demo site for verification and other necessary information upon request.

Figure 17. Sale of advanced phishing kits

## Bruteforcing Tools

The following dark web advertisement for a CMS Brute/Checker tool is designed to exploit vulnerabilities in a wide range of content management systems (CMS) used by e-commerce platforms and websites. The tool supports 48 CMS platforms, including popular ones like WordPress, OpenCart, Magento, and others. The seller highlights an updated software version (Version 2.2.1) with enhanced capabilities, such as support for 31 new CMS platforms, improved methods for successful brute-force authorization, reduced false positives, and smoother scanning processes.

glower  
gigabyte  
G  
Seller  
160 posts  
Joined  
02/19/18 (ID: 85669)  
Activity

Posted February 27

A new update has been released

Version 2.2.1:

- Added brute 31 new cms : AbanteCart, WHMCS, ClicShopping AI, CE Phoenix, osCommerce, Zen Cart, Loaded Commerce, LiteCart, thirty bees, Invoice Ninja, CubeCart, Open Source Point of Sale, QuickCart, CS-Cart Store Builder Free, Blesta, InvoicePlane, Arastta, Shopware, AlegroCart, Open eShop, SeoToaster, Thelia 2, Zeuscart, ClientExec, Logic Invoice, Bagisto, WhatACart, QloApps, PEEL SHOPPING, Maian Cart, NetCat
- Improved methods for determining successful authorization, now there are even fewer false positives
- Minor improvements such as more accurate statistics, smoother scanning stops and more

Price: ~~2999\$~~ 1000\$

A discount is possible if you take the software with only some modules (for example, only WordPress)

Figure 18. The brute-force tool is designed for CMS platforms like cPanel, WordPress, OpenCart, Magento, etc.

The recent surge in the registration of holiday-themed deceptive domains poses potential risks to shoppers, as such domains are often used in phishing campaigns or to host malicious content by mimicking legitimate websites during the holiday season. The most frequently used keywords in these domains include "offer," "shop," "deals," "2024," "discount," and "sale." While the majority of these domains have not been flagged as malicious by security vendors, their sheer volume highlights the importance of vigilance. It's crucial to note that these are currently just registered domains, and there is no concrete evidence yet to suggest they are being actively used for malicious purposes. However, their potential to be weaponized remains a significant concern for cybersecurity.

Holiday-Themed Domains	Counts	Detection (by five security vendors)
Thanksgiving	450+	Unknown
Blackfriday	2500+	28
Cybermonday	100+	Unknown
Christmas	31000+	153
Amazon	24000+	924
BestBuy	1400+	12
Walmart	700+	34

Our research identified a counterfeit version of the legitimate site jcrew[.]com, registered under the domain name jcrewblackfriday[.]com. This site was likely created to exploit the Black Friday shopping event.

Google

"JCrew" AND jcrewblackfriday.com

X

J.

jcrewblackfriday.com

https://www.jcrewblackfriday.com › products › mens-jc...

J.Crew Mens Classic black wash Black Rinse Wash

Our designers are obsessed with denim - and it shows. · 100% cotton · Traditional 5-pocket styling · Zip fly · Machine wash · Import · Select stores · Item BC232.

\$83.88

J.

J.Crew

https://www.jcrew.com › women › belts

Women's Belts

Shop Women's belts at J.Crew. Find the best belts ... Free shipping on jcrew.com, points on every purchase and so much more! ... J.Crew Factory. © 2024 J.Crew.

Fake website

Original website

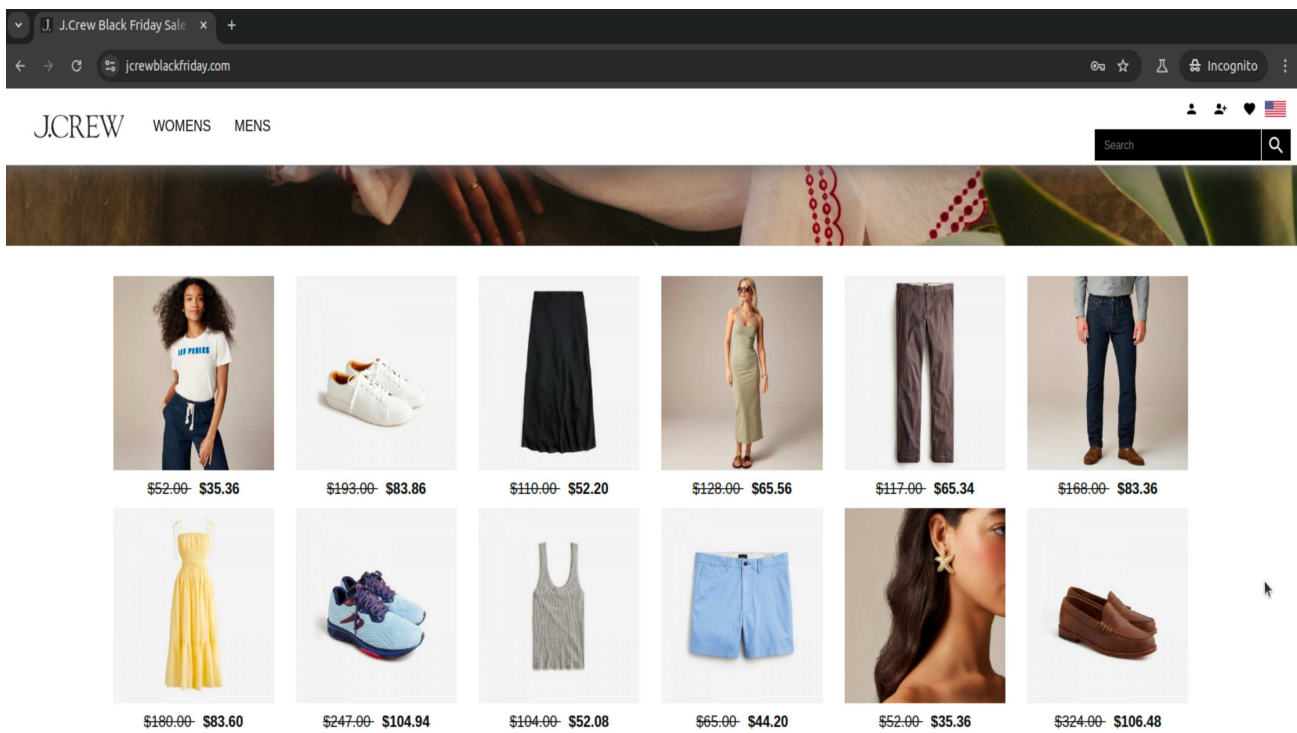


Figure 19. Counterfeit website mimicking jcrew[.]com

#### Domain Information:

Domain Name	jcrewblackfriday[.]com
Domain Registration	10th July 2024
Registrar:	Dynadot Inc
IP Address	165.231[.]67.4 (Cloudflare)

### Targeting of E-commerce Platforms

E-commerce platforms, such as Adobe Commerce (Magento), Shopify, WooCommerce, and OpenCart, are used to build and manage online stores. They provide merchants with tools to design storefronts, manage products, process payments, and handle customer interactions. While these platforms empower businesses with robust features, they are also prime targets for threat actors on the dark web.

Threat actors exploit these platforms by targeting vulnerabilities in their code, plugins, or configurations. Common attacks include deploying malware, installing card skimmers, or using admin panel brute-forcing tools to gain unauthorized access. Once inside, attackers can steal customer data and payment details or even manipulate store transactions. Additionally, unpatched software and weak credentials make these platforms even more vulnerable. During peak shopping seasons, like Black Friday or Christmas, e-commerce stores face heightened risks as attackers aim to exploit the surge in transactions to maximize their gains.



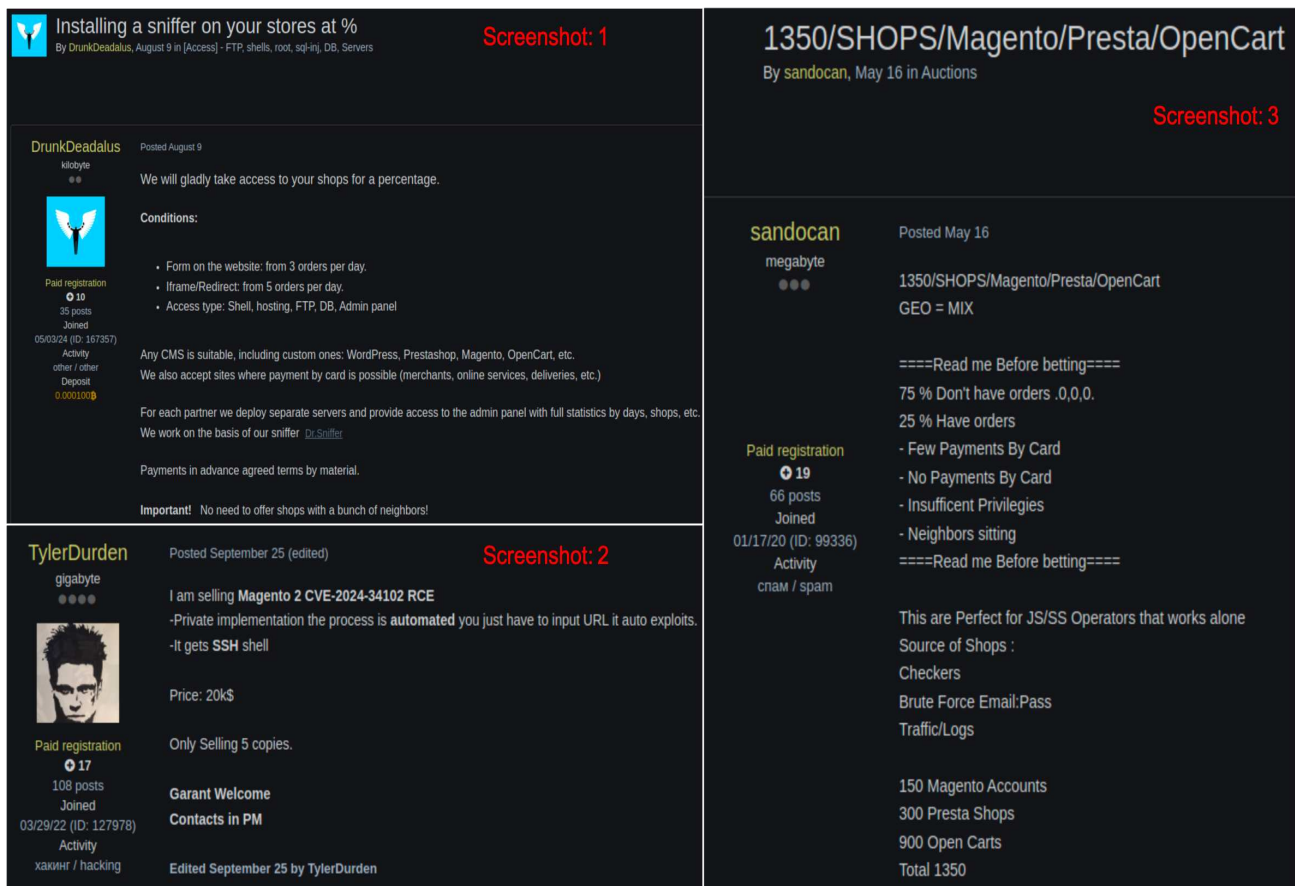


Figure 20. Compilation of threats to shopping websites

#### Sniffer Installation Scripts on E-commerce Websites (Screenshot 1):

- Threat actors offer to install sniffers on eCommerce websites, enabling them to intercept sensitive customer data such as credit card information, login credentials, and personal details.
- The service supports various CMS platforms like WordPress, PrestaShop, Adobe Commerce (Magento), and OpenCart, making it versatile and scalable.
- Attackers even provide access to admin panels with detailed statistics, allowing partners to analyze stolen data and revenue performance.

#### Exploits of E-commerce Platforms (Screenshot 2):

- A private implementation of an Adobe Commerce (Magento) RCE vulnerability (CVE-2024-34102) is advertised for sale. It offers automated exploitation via SSH shell access.
- With such exploits, attackers can completely compromise an e-commerce platform, gaining unauthorized access to manipulate transactions, steal customer data, or install additional malicious tools.

#### Sale of Access to E-commerce Websites (Screenshot 3):

Posts like these pose significant risks to online merchants, especially during high-traffic periods like the holiday season, as they can be exploited to gain unauthorized access, steal sensitive data, and manipulate transactions.

- Threat actors list compromised shops (1350 accounts) from platforms like Adobe Commerce (Magento), Presta, and OpenCart for sale.
- Some shops are confirmed to have orders and accessible payment methods, making them lucrative targets for fraudsters.
- The listing is intended for cybercriminals skilled in JavaScript or credential-stuffing operations who want to exploit stolen data or target these shops further.

---

## Conclusion

---

While the holiday season is a time of celebration and increased online activity, it also represents a period of heightened risk in the digital landscape. Cybercriminals leverage this transaction surge to deploy sophisticated attacks, ranging from phishing campaigns and stolen data sales to exploiting e-commerce platform vulnerabilities. This report's findings highlight the depth and breadth of these threats, illustrating the advanced tactics employed by threat actors on the dark web to target shoppers, businesses, and financial institutions.

Key challenges include the proliferation of holiday-themed deceptive domains, compromised e-commerce databases, and the sale of tools like phishing kits and sniffers that enable large-scale fraud. These threats underscore the need for both consumers and businesses to remain vigilant and adopt robust security practices during this critical period. Awareness and caution are paramount for shoppers, while companies must prioritize proactive security measures such as regular vulnerability assessments, system updates, and educating customers about potential risks.

As the digital threat landscape continues to evolve, collaboration between security vendors, businesses, and consumers is essential to stay ahead of cybercriminals. By implementing the following recommendations, individuals and organizations can minimize their exposure to cyber threats and ensure a safer, more secure online environment. The holidays should be a time of joy and opportunity, not risk and vulnerability. With the proper precautions, this vision can be achieved.

---

## Recommendations

---

### Recommendations for Users:

- **Verify URLs:** Always double-check the website address before entering sensitive information. Look for typos or unusual domains.
- **Use Secure Payment Methods:** Avoid direct bank transfers. Use credit cards or trusted payment gateways with fraud protection.
- **Be Cautious with Offers:** Avoid clicking on suspicious links in emails or SMS, even if they appear to come from legitimate sources. To add an extra layer of security, enable multi-factor authentication (MFA) and use it on all accounts.
- **Monitor Financial Activity:** Regularly check your bank and credit card statements for unauthorized transactions.
- **Avoid Public Wi-Fi:** When shopping online, use secure and private networks to reduce the risk of session hijacking.

### Recommendations for Businesses:

- **Strengthen Security Posture:**
    - Keep all e-commerce platforms and plugins updated.
    - Regularly scan for vulnerabilities and apply patches promptly.
  - **Implement Advanced Fraud Detection:** Deploy tools that detect unusual login attempts, brute-force attempts, and fake traffic.
  - **Monitor Domain Registrations:** Keep track of deceptive domains impersonating your brand and report them to the relevant authorities.
  - **Educate Customers:** Inform shoppers about identifying phishing attempts and ensuring safe online shopping.
  - **Secure Admin Panels:**
    - Use strong passwords and limit access to critical systems.
    - Regularly monitor login attempts for suspicious activity.
-

## Appendix A : Reliability Rating Criterion

FortiGuard Threat Research's Reliability rating is based upon the Admiralty System which is internationally accepted method for evaluating collected items of intelligence. The system comprises a two-character notation assessing the reliability of the source and the assessed level of confidence on the information.

### Reliability of Source

A source is assessed for reliability based on a technical assessment of its capability, or in the case of Human Intelligence sources their history. Notation uses Alpha coding, A-F:

A	Reliable	No doubt about the source's authenticity, trustworthiness, or competency. History of complete reliability.
B	Usually reliable	Minor doubts. History of mostly valid information.
C	Fairly reliable	Doubts. Provided valid information in the past.
D	Not usually reliable	Significant doubts. Provided valid information in the past.
E	Unreliable	Lacks authenticity, trustworthiness, and competency. History of invalid information.
F	Cannot be judged	Insufficient information to evaluate reliability. May or may not be reliable.

### Reliability of Information

An item is assessed for credibility based on likelihood and levels of corroboration by other sources. Notation uses a numeric code, 1-6.

1	Reliable	Logical, consistent with other relevant information, confirmed by independent sources.
2	Usually reliable	Logical, consistent with other relevant information, not confirmed.
3	Fairly reliable	Reasonably logical, agrees with some relevant information, not confirmed.
4	Not usually reliable	Not logical but possible, no other information on the subject, not confirmed.
5	Unreliable	Not logical, contradicted by other relevant information.
6	Cannot be judged	The validity of the information cannot be determined.

## Appendix B : Relevance Rating Criterion

### High

The Intelligence Report could be flagged with "High" Relevance under below criteria,

- > Threat Actor leaked or selling data pertaining to the customer organization in Public/Private Forum.
- > Threat Actor mentioned about customer organization in a Public/Private Forum
- > Public reporting on Organization was targeted.
- > Customer technology/product involved in an attack or being targeted.
- > Potential reputation harm to customer brand.
- > Customer related domains Typo-squat Fraudulent domains registered.
- > Proprietary customer related data found on internet. (Ex: GitHub containing source code)
- > Customer related domain email addresses found to be part of a data breach.
- > Customer specific keywords match identified across FortiGuard Threat Research's produced Intelligence.

### Medium

The Intelligence Report could be flagged with "Medium" Relevance under below criteria,

- > Identification of Threat Actor targeting related Industry.
- > Vulnerability disclosed Potentially impacting Organization.
- > Public/Private breaches or incidents relating the organization's sector.
- > Public/Private Incident identified is Unique and Provides insights into new TTPs.





### Low

The Intelligence Report could be flagged with "Low" Relevance under below criteria,

- > Public/Private Incident identified targeting non Customer specific industry.
- > Public/Private Incident identified outside of Customer geography vertical.
- > Public/Private Incident gaining significant Media Attention.
- > Data breaches or exposed data potentially impacting customer organization.

## Appendix C : TLP Criterion

TLP provides a simple and intuitive schema for indicating when and how sensitive information can be shared.

TLP Level	How may it be shared ?
 <div><b>TLP : Red</b> Not for disclosure, restricted to FortiGuard Threat Research and its customers who need to know the information.</div>	Recipients may not share TLP:RED information with any parties outside of the organization. The information could only be shared within the organization and should be restricted to the ones who needs to know the information.
 <div><b>TLP : Amber</b> Limited disclosure, restricted to FortiGuard Threat Research's customer organization</div>	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
 <div><b>TLP : Green</b> Limited disclosure, restricted to the community.</div>	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community.
 <div><b>TLP : White</b> Disclosure is not limited.</div>	TLP:WHITE information may be distributed without restriction