

**FORTINET**

 FortiRecon

# THREAT INTELLIGENCE REPORT



FortiGuard Threat Research

## Cyber Threat Landscape Overview for the 2025 Holiday Season


Relevance:

INFORMATIONAL

Reliability Rating:

     A - Reliable  
     1 - Confirmed

TLP Level:

 CLEAR

### Detailed report

#### Threat Brief

#### Executive Summary

As the 2025 holiday season approaches, events like Thanksgiving, Black Friday, Cyber Monday, and Christmas will bring millions of shoppers online seeking deals and discounts. This surge in activity also attracts cybercriminals who exploit the increased traffic to target both consumers and businesses. The threats observed this year are varied and while this report highlights key examples, it represents just a portion of the broader activity seen across the threat landscape.

During this period, holiday themed and E-commerce related malicious domains are on the rise, many designed to trick users into sharing sensitive information or to redirect them to fraudulent storefronts. Stolen E-commerce account logs including passwords, cookies, session tokens, and autofill data are actively used in large-scale attacks. Combo lists and card dumps fuel brute-force and credential-stuffing campaigns, taking advantage of spikes in login traffic. Cybercriminals are also leveraging website cloning, sniffers, and other tools to compromise user accounts and E-commerce platforms. Services such as prebuilt SEO manipulation and guides for cashing out e-wallets are increasingly used to amplify attacks or monetize stolen data. While the report focuses on notable trends and examples, the threat ecosystem is extensive and evolving.

By understanding these attack patterns and implementing proactive security measures, both consumers and merchants can reduce exposure to financial loss and data breaches during the holiday shopping season. The insights presented in this report provide actionable guidance and a high-level view of current threats, serving as a window into a much larger landscape of activity that continues to develop as the season progresses.

#### Content

- Key Findings
- Understanding the Threat Surface
- Reconnaissance and Information Gathering
  - Data Capture & Enrichment
    - Deceptive Domains

- Reconnaissance and Information Gathering
  - Data Capture & Enrichment
    - Deceptive Domains
    - Credential and Credit Card Dumps
    - Holiday-Season Surge in Stealer Logs
  - E-commerce Platform Vulnerabilities
    - Known Exploited Vulnerabilities
    - Notable Vulnerabilities
    - Security Weakness
- Attack Preparation
  - Tools
    - Illicit Login Checker
    - AI Tool for Brute Force
    - Tutorial to cash-out E-wallets
  - Services
    - Hosting Provider
    - Proxy Provider
    - SEO Poisoning
    - SIP Service Offering
    - Smishing Platform
    - Website Cloning
    - Stolen Gift Card
    - Gift Card Scam
    - Mass Phishing Mailer via AI
    - E-commerce Sniffers
- Monetization
  - Sale & Trade
    - E-commerce Stealer Logs Dump
    - E-commerce Website Databases
    - Admin Access to E-commerce Website
- Conclusion
- Recommendations

---

## Key Observations

---

- Surge in Holiday-Themed & Retail Deceptive Domains and Stolen Account Data
  - 18k+ Newly Registered holiday-themed domains registered (within past 3 months); 750+ (4%) are classified as malicious domains and 17K+ (96%) are classified as non-malicious domains.
    - The top 3 keywords in the newly registered holiday-themed domains are 'Christmas' (14K), 'Black Friday' (2.3K), and 'Flashsale' (750+).
  - 19k+ Newly Registered Popular E-commerce domains registered (within past 3 months); 2.9K+ (15%) are classified as malicious and 16K+ (85%) are classified as non-malicious domains.
  - Over 1.57M+ stealer log dumps collected over the past three months, primarily involving major E-commerce platforms.
  - Threat actors are seen offering Black Friday deals on credit card data and CVVs provoking other threat actors to buy the stolen data.

- Notable Vulnerabilities targeting E-commerce Platforms/Tools
  - Known exploited vulnerabilities like CVE-2025-54236 (Adobe/Magento) and CVE-2025-61882 (Oracle EBS) are actively used to target E-commerce platforms.
  - Notable vulnerabilities present in WooCommerce Ultimate Giftcard plugin, Bagisto, Welcart, and EasyCommerce plugins can be exploited for RCE, privilege escalation, and data theft, particularly during holiday peaks.
  - Magecart-style JavaScript skimmers continue to be major security weakness across Magento, WooCommerce, Shopify.
- Tools & Services Supporting Attacks During Holiday Season
  - AI-driven brute-force tools and credential validation checkers are promoted in underground forums
  - Threat actors are procuring pre-configured hosting, proxy, and VPN services to rapidly deploy phishing, C2, and scam infrastructure with anonymity.
  - Bulk SMS and SIP-spoofing panels are enabling large-scale smishing and vishing campaigns targeting holiday shoppers.
  - Threat actors are even advertising “Black Friday-style” discounts on their SEO-manipulation services to boost the visibility of malicious sites.
  - Underground forums show increased advertising of AI-driven phishing tools and gift-card fraud services ahead of the holiday season.
  - Attackers offer sniffer deployment services targeting CMS-based E-commerce stores.
  - Attackers sell E-commerce website cloning services on dark web to manipulate content on high traffic
- Monetization: Full Exploitation of Compromised Data During Holiday Peak
  - Multiple actors monetizing E-commerce breaches by selling large customer databases, including millions of records from platforms like WooCommerce and Yellowshop.es.
  - High-value administrative and FTP access to major U.S. retail E-commerce corporations is being sold, offering full control over compromised systems.

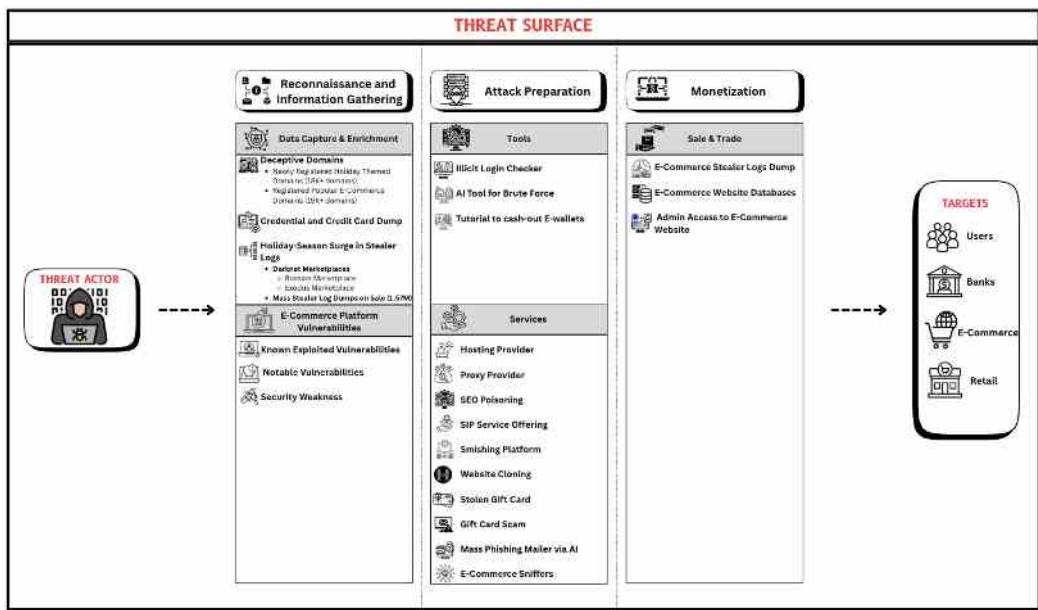
---

## Understanding the Threat Surface

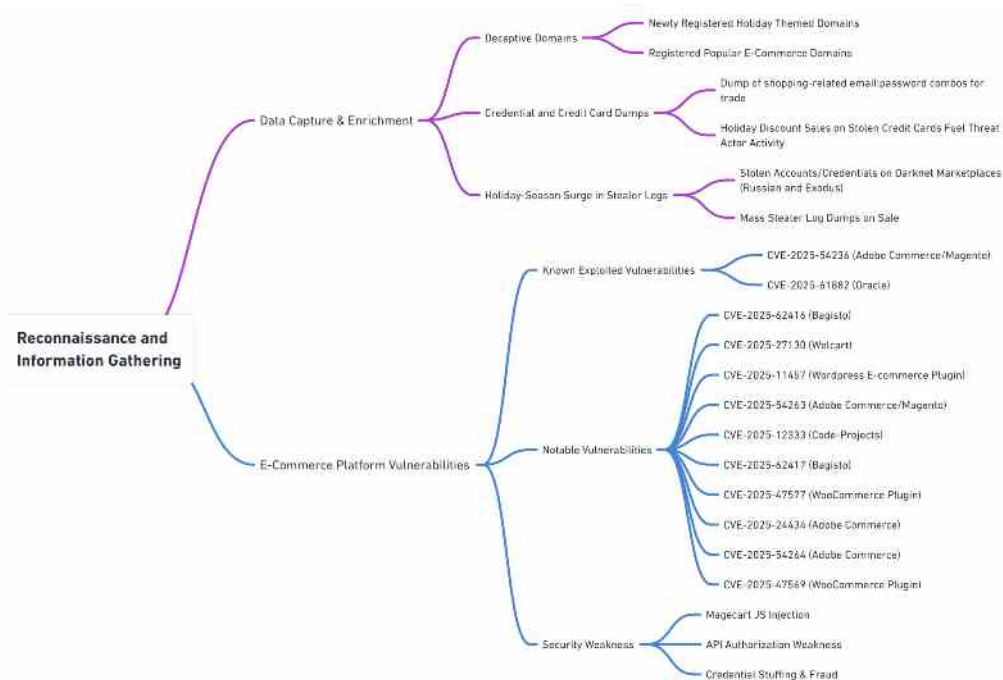
---

During the holiday season, the overall threat surface expands as threat actors take advantage of increased online activity, seasonal themes, and high transaction volumes. Deceptive holiday-themed domains, credential and credit-card dumps, stealer logs, and known E-commerce vulnerabilities contribute to a richer pool of data and opportunities within the ecosystem. At the same time, a range of tools and services such as illicit login checkers, brute-force utilities, proxy and hosting providers, SEO poisoning, phishing and smishing platforms, website-cloning services, SIP offerings, gift-card fraud schemes, and E-commerce sniffers remain readily accessible and can

enable various malicious activities. These dynamics support downstream monetization, including the sale or trade of E-commerce stealer log dumps, website databases, and admin-level access. Taken together, these factors illustrate a broadened tactical and strategic threat environment affecting users, banks, E-commerce platforms, and retail organizations during the high-traffic holiday period.



## Reconnaissance and Information Gathering



As the holiday season approaches, cyber threat actors intensify reconnaissance and information-gathering efforts to exploit the surge in online shopping and digital transactions. During reconnaissance, adversaries actively purchase or trade combolists, leaked credentials, credit card details and other stolen data on the dark web. They also register deceptive domains which are used in social engineering attacks. At the same time, attackers are also on the lookout for E-commerce related vulnerabilities to gain footholds in exposed systems or services.

## Data Capture and Enrichment

Within the data capture and enrichment, threat actors prioritize harvesting user credentials and exfiltrating sensitive payment information. They often augment these datasets with compromised credentials sourced from illicit underground marketplaces to facilitate credential-based attacks and subsequent account takeover operations.

- Deceptive Domains
  - Newly Registered Holiday-Themed Domains (18K+ domains)
  - Registered Popular E-commerce Domains (19K+ domains)
- Credential and Credit Card Dumps
  - Dump of shopping-related email:password combos for trade
  - Actors selling stolen payment data(CVV, Card dumps)
- Stealer Log Database
  - Darknet Marketplaces (Russian and Exodus)
  - Stealer Log Dumps

### Deceptive Domains

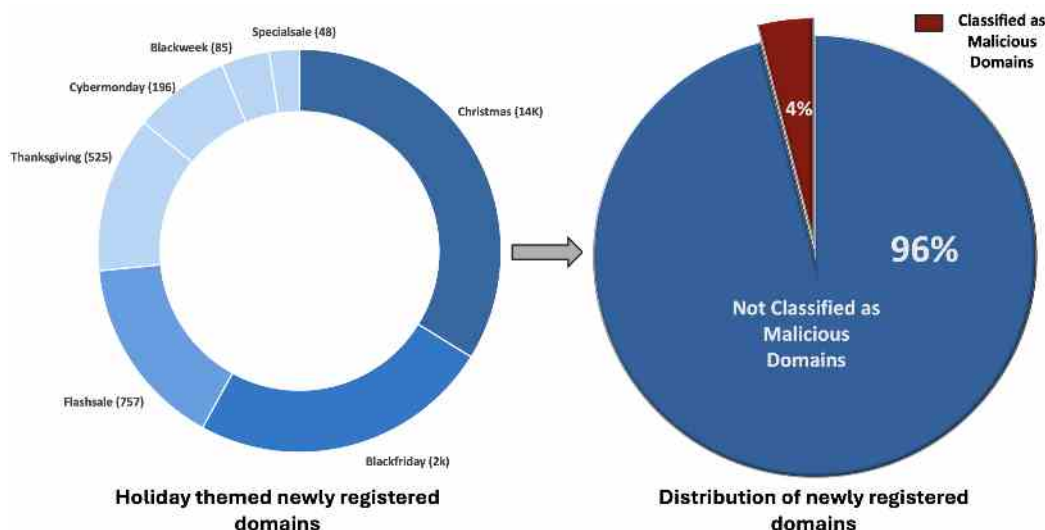
Most threat actors begin setting up deceptive domains designed to mimic popular E-commerce websites, shopping websites, gift card promotion sites etc., aiming to deceive users via social engineering and harvest sensitive credentials or fraudulent payments. Common keywords found in such domains include "Black Friday," "Thanksgiving," "Cyber Monday," "Christmas", "festivesale" etc. This rise in holiday-themed deceptive domain registrations presents potential risks to online shoppers. These domains are often leveraged in phishing campaigns or used to host malicious content by imitating legitimate retail websites during the festive season.

#### Newly Registered Holiday-Themed Domains:

In the past 3 months, FortiGuard Threat Research analysis found that there was a surge in holiday-themed domain registrations with a total of 18K+ domains registered. Within these newly registered domains, a 750+ (4%) were flagged malicious.

Below chart represents the percentage distribution of malicious domains and highlights the most commonly used keywords, providing insights into domain naming patterns exploited by threat actors.

The entire list of newly registered holiday-themed domains can be found [HERE](#).

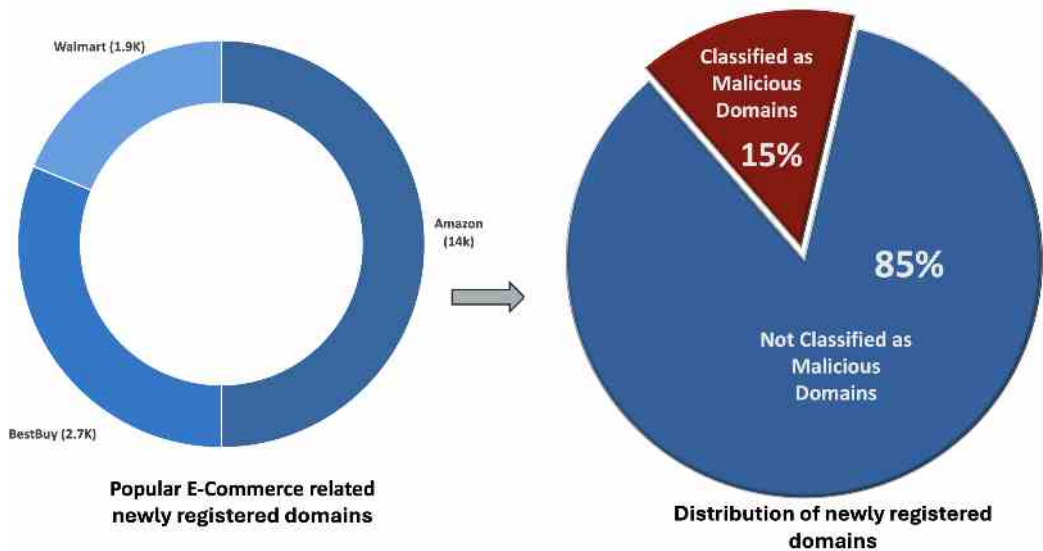


#### Registered Popular E-commerce Domains:

Besides, the holiday-related domains there was also a surge in registration of domains related to E-commerce websites with a total of 19K+ domains registered. Our analysis determined that 2.9K+ (15%) of these E-commerce related domains were classified as malicious.

This trend highlights a growing pattern of domain abuse by threat actors who exploit seasonal and E-commerce related themes to deceive users and facilitate phishing, fraud and other cyberattacks.

Below chart represents the percentage distribution of malicious domains for a few of the most common retail websites. The entire list of newly registered popular E-commerce domains can be found [HERE](#).

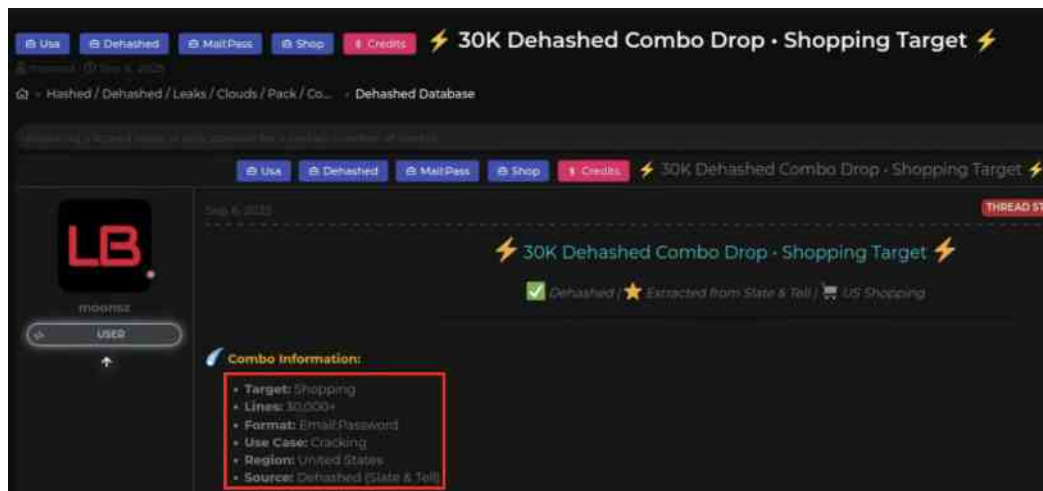


Credential and Credit Card Dumps:

Threat actors also hunt to obtain credentials and credit card details via combolists and card dumps that are being sold on the Darknet. These extensive databases of email-password combos assist the threat actors in credential stuffing attacks, focusing on account takeovers during critical seasonal shopping spikes.

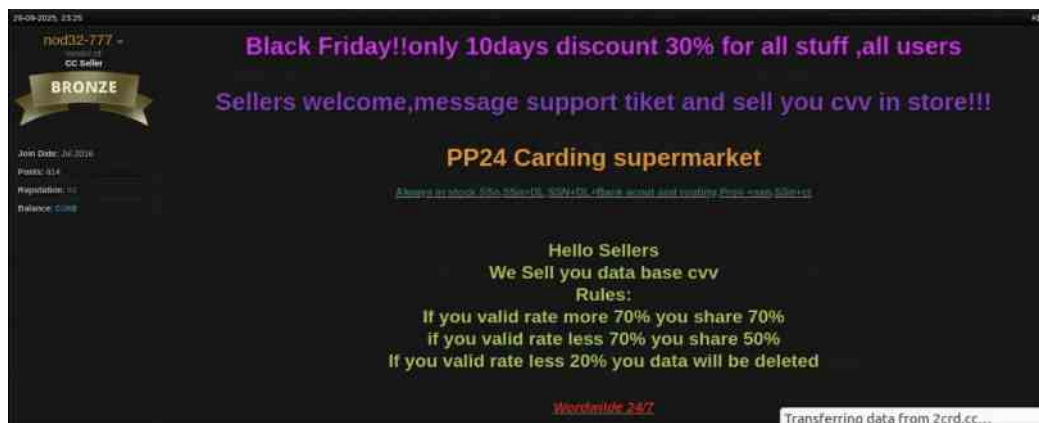
Dump of shopping-related email:password combos for trade

The below post lists compromised credentials related to shopping websites which contains customer email and passwords, particularly targeting U.S.-based online retailers. This data is can be used in mass credential-stuffing attacks.





During holiday season, threat actors seek to purchase credit card details such as CVV numbers, sold on darkweb that helps them in fraudulent purchases. The post below is from darkweb that is offering to sell credit card details to interested buyers. Threat actors often offer these compromised card datasets at discounted prices during major shopping events like Black Friday, using seasonal promotions to attract more buyers. These limited-time “holiday deals” not only increase sales but also provoke other threat actors to stock up on card data, further amplifying fraud activity during this period.



## Holiday-Season Surge in Stealer Logs

Stealer logs are datasets generated by infostealer malware that captures sensitive information from compromised endpoints, including browser-stored credentials, session cookies, autofill data, email logins, crypto-wallet details, and system fingerprints. During the busy holiday shopping season, users often log into multiple E-commerce platforms, increasing their exposure to threats. Cybercriminals leverage this data to take over accounts or sell it to other malicious actors for financial exploitation.

## Stolen Accounts/Credentials on Darknet Marketplaces (Russian and Exodus)

After exfiltration of credentials, threat actors aggregate and sell these logs on Darknet marketplaces such as Russian Marketplace and Exodus Marketplace. On these platforms, the stealer logs are indexed by domain, sector, geography, or account type. These marketplaces operate with commercial-style features (reputation systems, filters, automated delivery), lowering the skill barrier for actors seeking ready-made access to compromised accounts.

The availability of stealer logs on these marketplaces directly enables threat actors to perform successful cyberattacks such as account takeover (ATO), fraud, credential-stuffing, and session hijacking, particularly when active cookies are included. Monitoring these marketplaces provides defenders with visibility into exposure levels, emerging malware families, and targeting trends, with retail and E-commerce credentials remaining a frequent component of circulated datasets.

## Mass Stealer Log Dumps on Sale

Across Darknet marketplaces, numerous threat actors continue to share large volumes of stealer log dumps. These logs are parsed and categorized by threat actors based on specific targets, in this case, retail and E-commerce platforms.

Our research, based on the data obtained from the past three months primarily involving major E-commerce platforms reveals availability of a total of 1.57M stolen account credentials.



E-commerce Platform Vulnerabilities

Threat actors plan to exploit critical 2025 vulnerabilities affecting E-commerce platforms. They often approach to leverage weaknesses in input validation, authentication bypass, and API exposures to gain initial access, escalate privileges, and maintain persistent control of targeted E-commerce environments.

For example, the widely exploited [CVE-2025-54236](#) ("SessionReaper") in Adobe Commerce/Magento uses crafted requests against improperly validated REST API endpoints. Exploiters uses the backdoors to execute arbitrary commands, extract data, manipulate orders, and maintain persistence on compromised stores.

Similarly, for the Clop ransomware exploited [CVE-2025-61882](#) in Oracle E-Business Suite (EBS), threat actors exploit authentication and input validation weaknesses to perform unauthenticated remote code execution. This enables attackers to steal sensitive order, customer, and inventory data and deploy ransomware, massively disrupting E-commerce backend ERP systems.

Across platforms, attackers also target API authorization weaknesses and third-party supply chain integrations, injecting malicious JavaScript (Magecart-style attacks) to skim payment data or performing credential stuffing attacks to hijack user accounts. Combined with cross-site scripting (XSS) vulnerabilities, adversaries gain credentials and execute unauthorised actions, further compromising ecommerce business operations and user data integrity.

An overview of exploited and critical vulnerabilities in E-commerce platforms throughout 2025 is shown in the following table:

Known Exploited Vulnerabilities				
<a href="#">CVE-2025-54236</a>	Adobe Commerce (Magento)	Improper input validation leading to session takeover and RCE via webshell uploads	9.1 (Critical)	<a href="#">Over 250 Magento stores compromised, persistent backdoors and data theft, low exploit complexity</a>
<a href="#">CVE-2025-61882</a>	Oracle E-Business Suite (EBS)	Unauthenticated RCE, data theft, and ransomware extortion	9.8 (Critical)	<a href="#">Clop ransomware is exploiting Oracle EBS zero day, severely disrupting ecommerce ERP backend</a>
Notable Vulnerabilities				
<a href="#">CVE-2025-62416</a>	Bagisto	Server-Side Template Injection (SSTI), potential RCE	6.8 (Medium)	Potential for remote code execution through crafted template input
<a href="#">CVE-2025-27130</a>	Welcart	Untrusted PHP object deserialization leading to RCE	8.8 (High)	Vulnerability to remote code execution via unserialized data

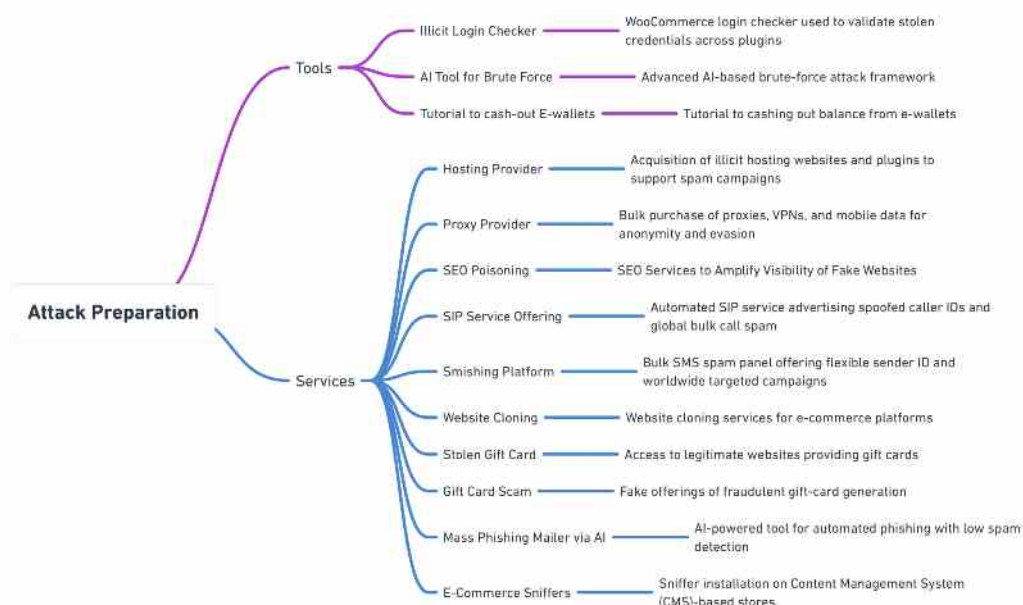
<a href="#">CVE-2025-11457</a>	EasyCommerce WordPress plugin	Privilege escalation via REST API abuse	9.8 (Critical)	Plugin currently closed for review, no active exploitation observed
<a href="#">CVE-2025-47569</a>	Woo Commerce Ultimate Giftcard plugin	Exploitation could allow attackers to manipulate or exfiltrate sensitive database information	4.3 (Medium)	Significant security risk to WooCommerce-based online stores.
<a href="#">CVE-2025-54263</a>	Adobe Commerce (Magento OSS)	Improper access control, privilege escalation	8.1 (High)	Low privileged users may bypass restrictions
<a href="#">CVE-2025-12333</a>	Code-projects E-commerce Website	Cross-Site Scripting (XSS) in supplier input fields	6.1 (Medium)	No patch available; risk of session theft and data manipulation
<a href="#">CVE-2025-62417</a>	Bagisto	Spreadsheet formula input leading to logic flaws/injection	7.8 (High)	Potential injection or privilege escalation risk
<a href="#">CVE-2025-47577</a>	TI WooCommerce Wishlist plugin	Impacting the TI WooCommerce Wishlist plugin for WordPress	10 (Critical)	Unrestricted Upload of File with Dangerous Type vulnerability in TemplateInvaders TI WooCommerce Wishlist allows Upload a Web Shell to a Web Server
<a href="#">CVE-2025-24434</a>	Adobe Commerce	Incorrect Authorization vulnerability that could result in Privilege escalation	9.1 (Critical)	An attacker could leverage this vulnerability to bypass security measures and gain unauthorized access
<a href="#">CVE-2025-54264</a>	Adobe Commerce	Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields	8.1 (High)	Attacker can abuse this to achieve session takeover, increasing the confidentiality, and integrity impact to high

Security  
Weakness

<b>Magecart JS Injection</b>	Multiple platforms (Magento, WooCommerce, Shopify, etc.)	Payment skimming via malicious JavaScript injection	8.0 (High)	Ongoing widespread attacks stealing credit card information via checkout page compromises
<b>API Authorization Weakness</b>	Multiple platforms (Magento, WooCommerce, Shopify, etc.)	Account/data breaches, fraudulent order manipulation	8.0 (High)	Exploitation of API misconfigurations in omnichannel commerce environments
<b>Credential Stuffing &amp; Fraud</b>	Multiple platforms (Magento, WooCommerce, Shopify, etc.)	Account takeovers and financial fraud	8.0 (High)	Widespread automated attacks targeting user credentials and BNPL abuse refer to large-scale bot-driven attempts to steal login details and exploit "Buy Now, Pay Later" services for fraudulent purchases.

## Attack Preparation

Attack Preparation is the pre-attack phase where adversaries assemble everything needed to turn intent into action. It includes sourcing credentials and accounts, acquiring hosting/proxy/illicit resources, building or buying tooling, and setting up distribution channels (phishing kits, smishing/SMS platforms, etc.). Actors also prepare distribution channels such as phishing mailers, bulk SMS/spoofed-call platforms, skimmer services, and establish a marketplace presence to buy or sell tools, stolen data enabling rapid and large-scale holiday-season scams.



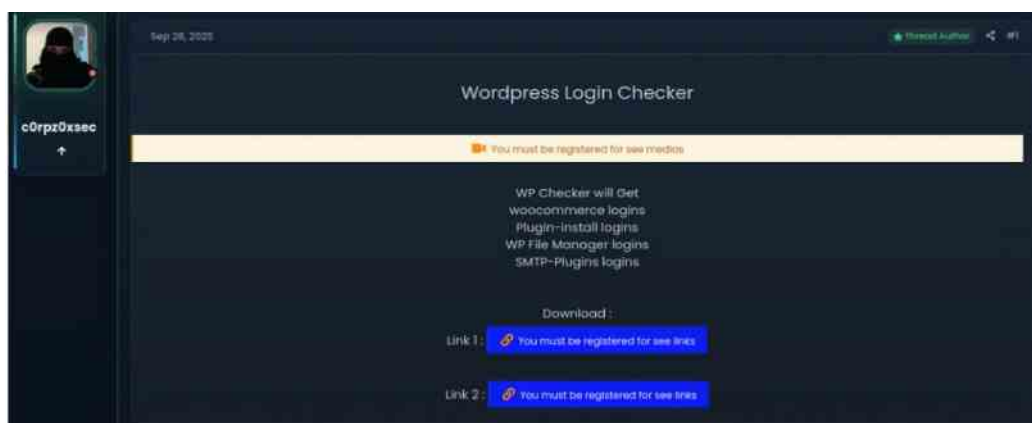
## Available Tools leveraged by Threat Actors during Holiday Season

During the holiday season, threat actors rely on a range of technical enablers that help them automate and scale their campaigns. These include credential checkers used to validate stolen accounts, AI-driven brute-force and fraud tutorials that outline cash-out methods. During the holiday rush, these tools let actors scale attacks quickly and efficiently, taking advantage of increased online activity and hurried shoppers.

- WooCommerce login checker used to validate stolen credentials across plugins
- AI-powered login brute-force tool framework for large-scale account compromise
- Tutorial to cashing out balance from E-wallets.

### WooCommerce login checker used to validate stolen credentials across plugins

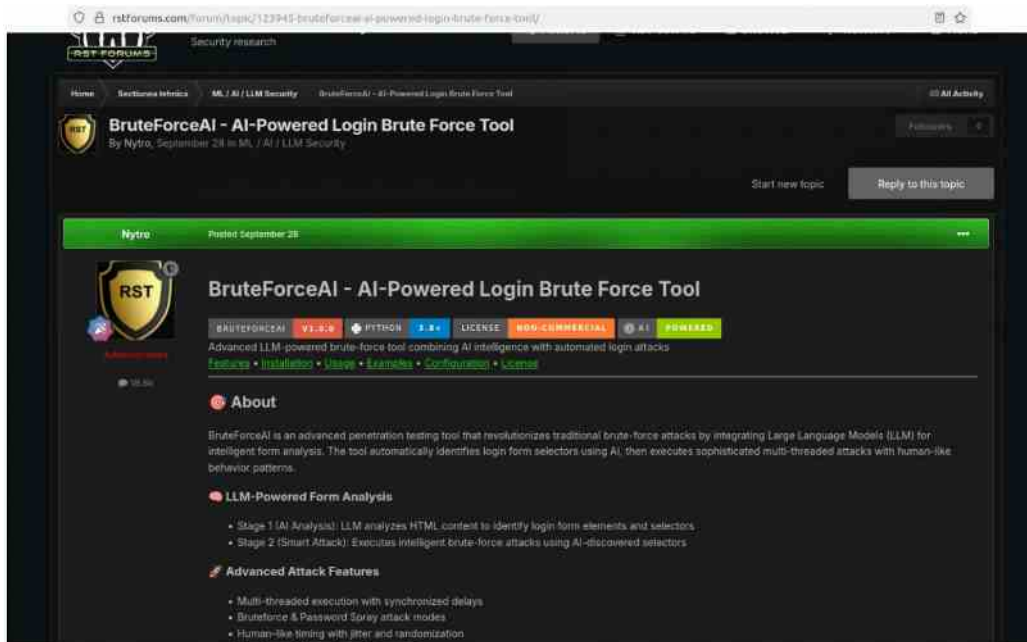
Attackers run such checkers on breached credential lists to extract high-value, actionable logins for site takeover, malware deployment, or payment-fraud routes. These tools automate the testing of stolen usernames and passwords across platforms to find working accounts. Below is the post shared on a cyber criminal forum for a credential-validation tool that automates login attempts against WordPress/WooCommerce and common plugins (FTP/SMTP/File Manager) to identify working credentials.



### Advanced AI-based brute-force attack framework

AI-driven tools automate brute-force attacks on login forms, mimicking human behavior to evade detection. A post advertised Brute ForceAI, letting attackers rapidly compromise accounts when online shopping activity peaks.

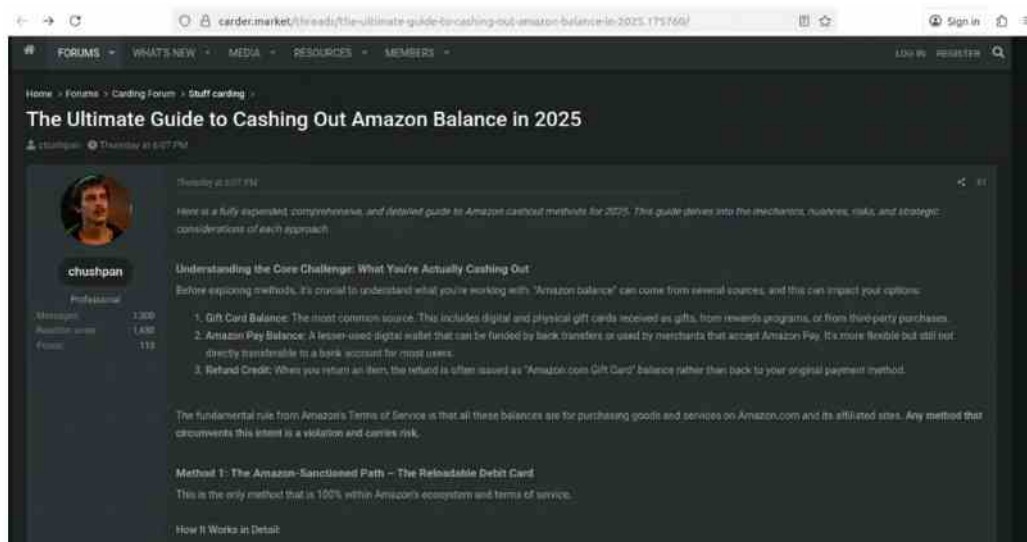
This AI-powered tool automates brute-force attacks on login forms. It leverages Large Language Models (LLMs) to analyze web pages and identify form elements automatically. The tool then executes multi-threaded brute-force and password spray attacks with human-like behavior, including random delays and timing variations to avoid detection.



## Tutorial to cashing out balance from E-wallets

Threat actors were seen posting a detailed guide on cashing out Amazon balances, showing ways to convert gift card balances, Amazon Pay balances, and refund credits into usable funds outside Amazon. It explains the types of balances and how each affects cashout options, while highlighting risks, rules, and strategies some of which may violate Amazon's terms of service.

While it references legitimate options like Amazon reloadable debit cards, the broader purpose of such posts is often to teach scammers how to bypass normal purchasing restrictions, enabling unauthorized resale, laundering, or monetization of stolen Amazon balances.



## Available Services supporting Attacks during Holiday Season

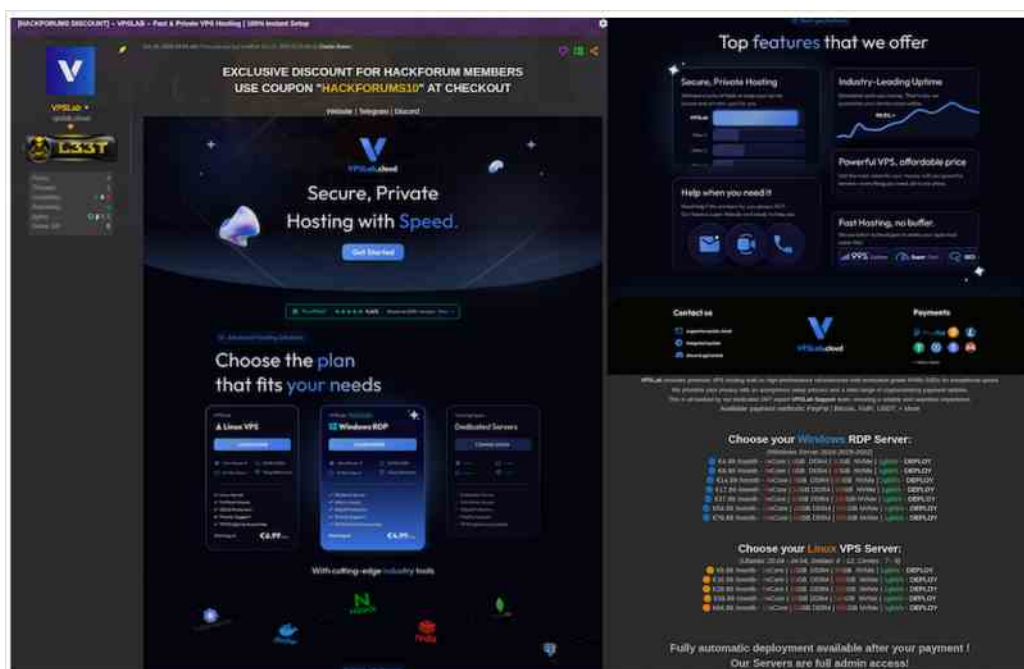
Threat actors depend on a broad set of outsourced services that provide the infrastructure required to run and monetize their operations. These services include anonymous hosting, proxy and VPN providers, SIP-spoofed telephony, smishing and bulk-SMS platforms, SEO manipulation for malicious sites, website cloning offerings, E-commerce sniffer installation, and marketplaces sell stolen gift cards. These services allow threat actors to distribute phishing content, hide their identity, host fake storefronts, intercept payment data, and monetize stolen assets.

During the holiday period, such services enable rapid, large-scale fraud with minimal technical skill.

- Acquisition of illicit hosting websites and plugins to support spam campaigns
- Bulk purchase of proxies, VPNs, and mobile data for anonymity and evasion
- SEO Services to Amplify Visibility of Fake Websites
- Automated SIP service advertising spoofed caller IDs and global bulk call spam
- Bulk SMS spam panel offering flexible sender ID and worldwide targeted campaigns
- Website cloning services for E-commerce platforms
- Access to legitimate websites providing gift cards
- Fake offerings of fraudulent gift-card generation
- AI-powered tool for automated phishing with low spam detection
- Sniffer installation on Content Management System (CMS)-based stores

## Acquisition of illicit hosting websites and plugins to support spam campaigns

On cybercriminal forums, threat actors usually offer pre-configured hosting websites for phishing, malware, or C2 servers. The post below advertises instant-setup VPS and Windows RDP with full root/admin access, DDoS protection, crypto payment options and claims of privacy, positioned to appeal to threat actors. Such offerings are used to host phishing pages, store payloads, run credential-checkers, or act as C2 servers, anonymous payment and instant deployment.



## Bulk purchase of proxies, VPNs, and mobile data for anonymity and evasion

Threat actors openly advertise bulk resources like 4G/LTE proxies, VPNs, mobile SIMs, and pre-configured domains, hosting, and plugins on marketplaces. These ready-made infrastructure let attackers automate campaigns, evade detection, and scale operations without technical setup. These deals and pre-staged tools suggest preparation for sustained or repeated attacks.




## SEO Services to Amplify Visibility of Fake Websites

During the holiday period, SEO manipulation and marketing assets help malicious pages to increase visibility in search results. Attackers use these services to drive traffic to phishing sites and fake storefronts targeting holiday shoppers.

In the post below, a digital-marketing/SEO provider boosts high rankings for keywords and shows search-engine-results-page (SERP) snapshots, services that can be abused to surface malicious landing pages, phishing sites, or fake storefronts via search-engine manipulation (SEO poisoning).






DX-GENERATION  
Elite Member  
2 Yr  
Apr 14, 2018  
1,840  
884

Jul 8, 2025 Threat Hunter

**The Unstoppable Superman Soaring High with Amazing Results**

We are one of the leading Digital Marketing Company on Internet.

As of 8th July 2025, we are currently ranking in the Top 10 on Google Search for the keywords 'SEO Services' and 'SEO Service'.



**Blackfriday Sales are on for DX SEO Services**

**Google master 2 becomes 10x Times stronger Compare to any other service on Blackhatworld**  
We have added 100 more High DA fast indexing sites (Frontiers, Studiopress, Qualtrics, Armor Games, Intense Debate and Slashdot ) that have been added to our database!

**Breaking News:- We have added more High-Quality websites likes of Wordpress (do-follow link) (DA-95) - Service update 8th July 2025**

(Why do we rank better than any other provider? becoz we make high quality and handmade links compare to automated backlinks of other providers).

**High-Quality Service = High-Quality Reviews!** 🌟

**Catch Amazing Discounts upto 70% OFF on SUPERMAN SPEED PACKAGE.**

Our List of SEO Services with Excellent deals please check our deals page: <https://oxygenites.com/deals/>

Automated SIP service advertising spoofed caller IDs and global bulk call spam

SIP panels allow attackers to spoof caller IDs and make mass voice calls globally, supporting large-scale social engineering or fraud campaigns. Threat actors were observed advertising Limitless SIP highlighted coverage in 190+ countries, enabling attackers to run holiday-season vishing campaigns with minimal setup and high operational reliability.

**SIP Service - Spoofed Caller ID & Bulk Call Spam [Automated SIP panel Online] + Spoofer**

Patolus • 2 Oct 2025

Forums • Marketplace • **Sellers Section**

**If you want to secure your transaction, you can always use our Escrow service**

Tuesday at 11:28 AM

**LimitlessSIP - Your Ultimate SIP Solution**

Looking for a reliable and cost-effective SIP service? LimitlessSIP has you covered with global reach and top-tier performance. Here's why you should choose us:

**Key Features:**

- Fully Automated - No manual work, everything is fully automated and working after payment.
- Spoofed Caller-ID - Spoof and choose your Caller ID by yourself.
- 190+ Countries - Global coverage, no matter where you are.
- 99.99% Uptime - No downtime, always connected.
- 3 NOCs (Redundant Routes) - Ensuring maximum stability and performance.
- High-Quality Voice - Clear and reliable communication.
- Best Pricing - Competitive rates for businesses of all sizes. Check our pricing


Easy-to-Use Dashboard - Manage your account with ease and automation. Visit the dashboard

**Why LimitlessSIP?**

- Scalable Solutions for businesses of all sizes.
- Advanced Security to protect your data.
- Fast Support whenever you need it.
- Get started today at LimitlessSIP Dashboard!

**Website (Panel):** <https://dashboard.limitlessip.com/>  
**Support:** [https://t.me/LimitlessSIP\\_bot](https://t.me/LimitlessSIP_bot)  
**Telegram:** <https://t.me/LimitlessSIP>

**Supported Countrys (190+):**

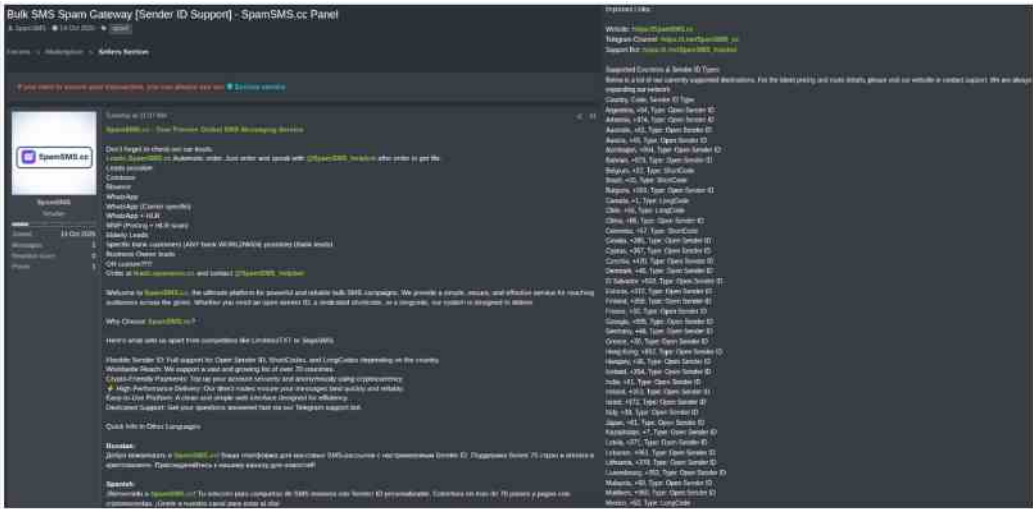


Patolus  
Member

Joined: 11 Apr 2025  
 Messages: 2  
 Reaction score: 1  
 Points: 3

Bulk SMS spam panel offering flexible sender ID and worldwide targeted campaigns

Platforms offering bulk SMS with flexible sender IDs and automated dashboards enable large-scale smishing campaigns. During the holiday period, a SpamSMS.cc listing provide bulk SMS services with flexible sender IDs, worldwide reach (70+ countries), and crypto payments.



Website cloning services for E-commerce platforms

Website cloning involves creating an exact replica of a legitimate site including its design, content, and functionality often hosted on a malicious domain. Threat actors are selling 'Free Review Copy' and 'website cloning' services access to insert backdoors or manipulate content on high-traffic E-commerce sites. While marketed as a legitimate service, attackers can exploit this to gain admin-level access to websites, enabling backdoor insertion, content manipulation, or unauthorized control over client sites.

\$99

WORDPRESS

- Upto 5 pages
- Upto 3 Products
- Functional Website
- Responsive Design
- Content Upload
- Social Media Icons
- Plugins Installation
- Opt-In Form
- Delivered within 4 days

BUY NOW

\$98

SHOPIFY

- Professional theme enhancements
- Upto 5 products
- Mobile-friendly
- Integration of apps
- Full setup for shipping, and
- payment systems
- Social media links added
- Blog creation included
- Delivered within 5 days

BUY NOW

\$90

CUSTOM WEBSITE

- Professional Website Design
- Number of page 3
- Fully Responsive Design
- User friendly Content Upload
- Speed optimization
- Contact forms
- Delivered within 4 days

BUY NOW

\$19 /PAGE

CLONE/REDESIGN

- Professional Website Design
- Number of page 1
- Fully Responsive Design
- Speed optimization
- Contact forms
- Contact forms
- Delivered within 2 days

BUY NOW

**NOTE: CLONE/REDESIGN IS FIGMA/XD/PSD TO WORDPRESS/SHOPIFY/CUSTOM CODE SERVICE.**

FREE REVIEW COPY Wordpress Website!

backman\_02 Jun 30, 2025 affiliate agency websites blog clone website custom code gmc premium ecommerce redesign website shopify development wordpress development

backman\_02

Power Member

> WP

Dec 11, 2024

744

80

Jun 30, 2025

We offer Review copy for our Wordpress website service

My BST Thread:

Starting from \$19!Premium Ecommerce GMC Blog Affiliate Agency Websites WordPress & Shopify Development Custom Code Clone/Red

What's Included in the Free Review Copy:

1 Page design of any type of Wordpress Website except adult niche.

Requirements:

1. Wordpress dashboard login

2. Images/logo/banners which you want us to add.

3. Text Details

Comment Interested Will contact!

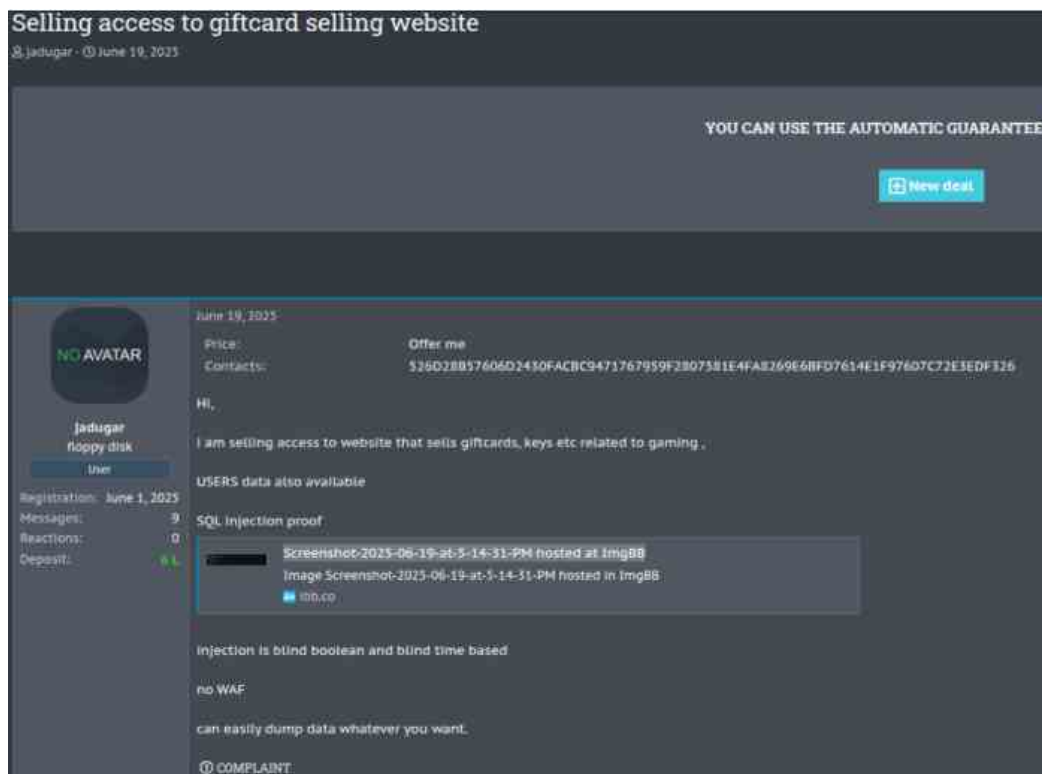
Please note: A detailed review is required within 24-48 hours after delivery.

Thanks in advance

solav288 NoFoundU and Muzkut

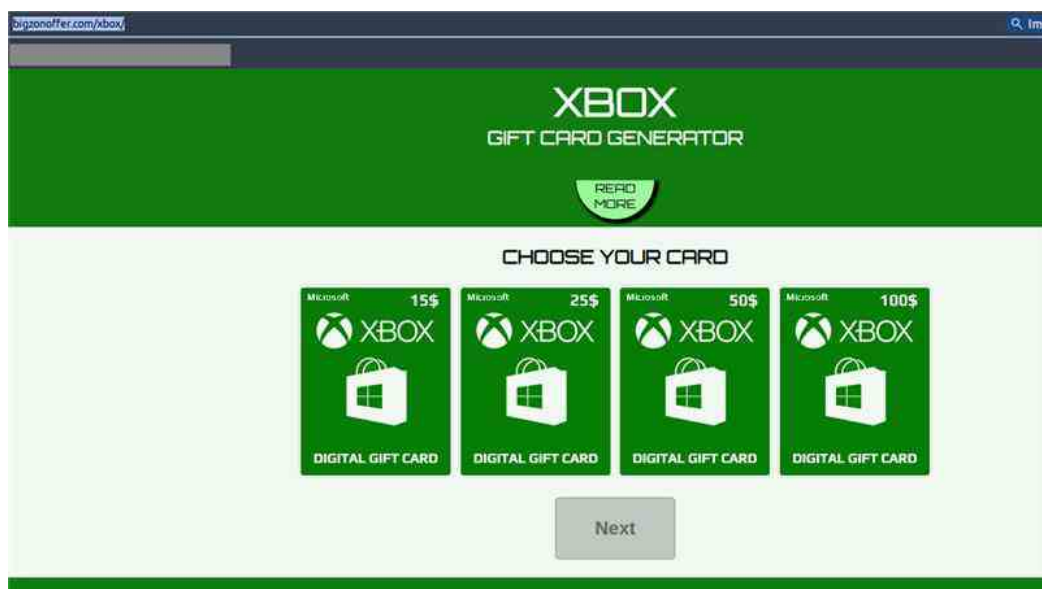
Access to legitimate websites providing gift cards

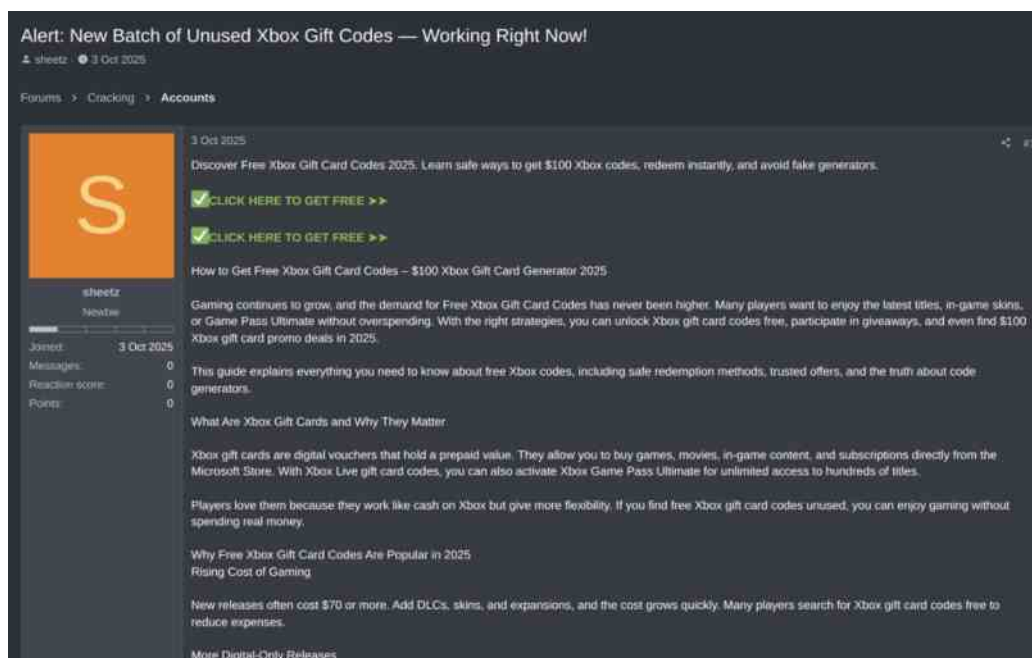
Threat actors sell access to legitimate websites that provide gift cards. Such access can be exploited to obtain gift cards for unauthorized use or resale, enabling fraudulent purchases and financial abuse.



## Fake offerings of fraudulent gift-card generation

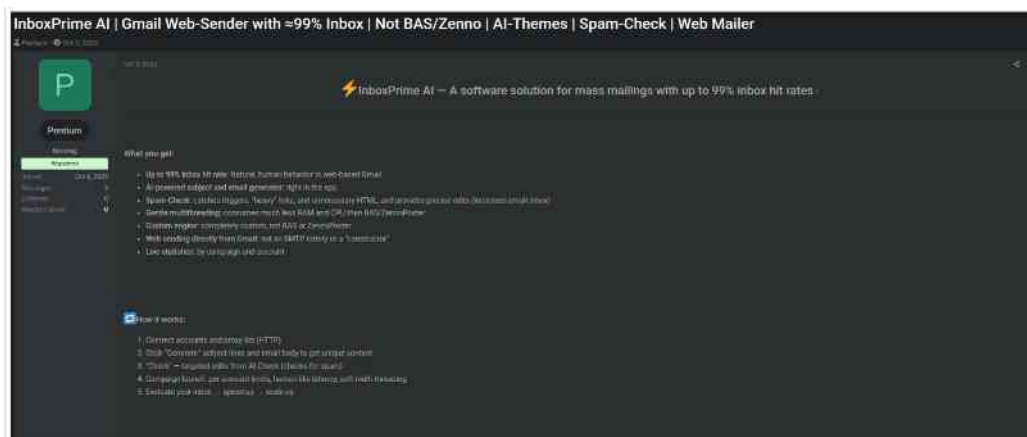
During the holiday season, gift card scams become prevalent as attackers exploit the surge in online shopping and digital gifting. Threat actors on underground forums sell access to Xbox gift card generators, and fresh batches of unused Xbox gift codes. These resources allow scammers to quickly defraud victims, either by reselling the cards, laundering funds, or using them to make unauthorized purchases.






AI-powered tool for automated phishing with low spam detection

AI-driven phishing tools automate targeted email campaigns, mimicking legitimate patterns to evade detection. A forum post promoted such a mailer for holiday campaigns, enabling attackers to efficiently harvest credentials from shoppers rushing to buy seasonal deals. The post promotes an AI-powered phishing mailer designed to automate the delivery of phishing and spam emails with minimal risk of detection.



Sniffer installation on Content Management System (CMS)-based stores

E-commerce Sniffers are used by attackers to inject malware (skimmers) into online stores. This is a post observed on cybercrime forums which advertises a skimmer installation service for CMS-based online stores, highlighting an affiliate program, guaranteed installation within 12 hours, dashboards for tracking stolen data, and ongoing backdoor access. It supports popular platforms such as Magento, WordPress, OpenCart, and PrestaShop, and offers flexible payment options for threat actors.



Cadiz

RAID array

Seller

Registration: October 2...

Messages: 79



Reactions: 9


Deposit: 0.9178

Today at 01:40


Price: 9999

Contacts: 144DC94B1B5B783B82C76579AA6D9F95F045B06E897CCEC28B1FB1CCA9A14A72065F5A47EEAD

 Hello, we'd love to partner with you on installing a sniffer on your access points! 

 Our affiliate program guarantees:
 

- Optimal price (we can adjust the percentage in your favor, subject to pilot cooperation).
- A unique code for each shop.
- A convenient dashboard for tracking materials and access.
- Timely control of access and the appearance of neighbors (we'll keep them there as long as possible using backdoors).
- We'll help you gracefully remove neighbors from your resource.
- RU/English support guaranteed to respond within 2-3 hours.
- We guarantee installation within 12 hours
- Payments within the agreed-upon timeframe with materials or money.


 We work with any CMS: Magento, OpenCart, WordPress, Prestashop, etc.
 

- We will consider any payment options
- form on the website from 5 per day / iframe; redirect 30 days

- Deposits are available on all neighboring boards

I buy merchant keys, paying up to \$10,000

<https://xss.pro/threads/112462/>

 COMPLAINT

New deal

## Monetization

The holiday season's surge in digital commerce brings a parallel rise in cybercriminal monetization activities, where threat actors seek to convert compromised data and access into financial gain. This phase is characterized by the resale of stolen credentials, cookies, and administrative access to E-commerce platforms, along with the distribution of breached databases within underground markets. Attackers exploit the seasonal influx of shoppers and merchants to maximize profits, leveraging large-scale data compromises and targeted access listings to enable fraud, account takeovers, and secondary exploitation. In parallel, specialized networks emerge to recruit individuals for cash-out operations, facilitating the laundering of funds obtained through these cyber-enabled schemes.



## Sale & Trade

Dark web activity targeting E-commerce platforms has increased ahead of the holiday season, with threat actors selling stolen browser session data, customer records, and even administrative access to retail systems. These listings enable unauthorized account access and potential exploitation of payment and customer information, creating elevated risks of fraud and disruption during peak shopping periods.

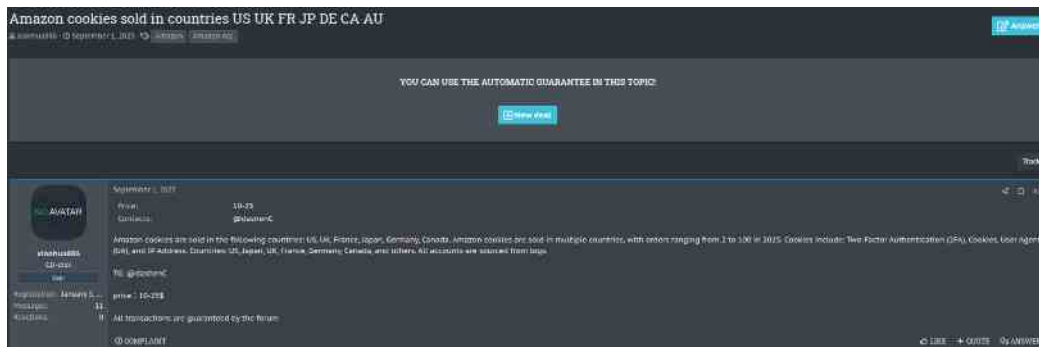
- Stolen E-commerce Website Login Data Marketed from Stealer Logs
- Selling of E-commerce database



- Large-scale data breaches fueling seasonal fraud ecosystems
- Sale of compromised shopper and merchant data from E-commerce sites
- Selling of admin access of E-commerce website
- Recruitment for Cash-Out Services

## Stolen E-commerce Website Login Data Marketed from Stealer Logs

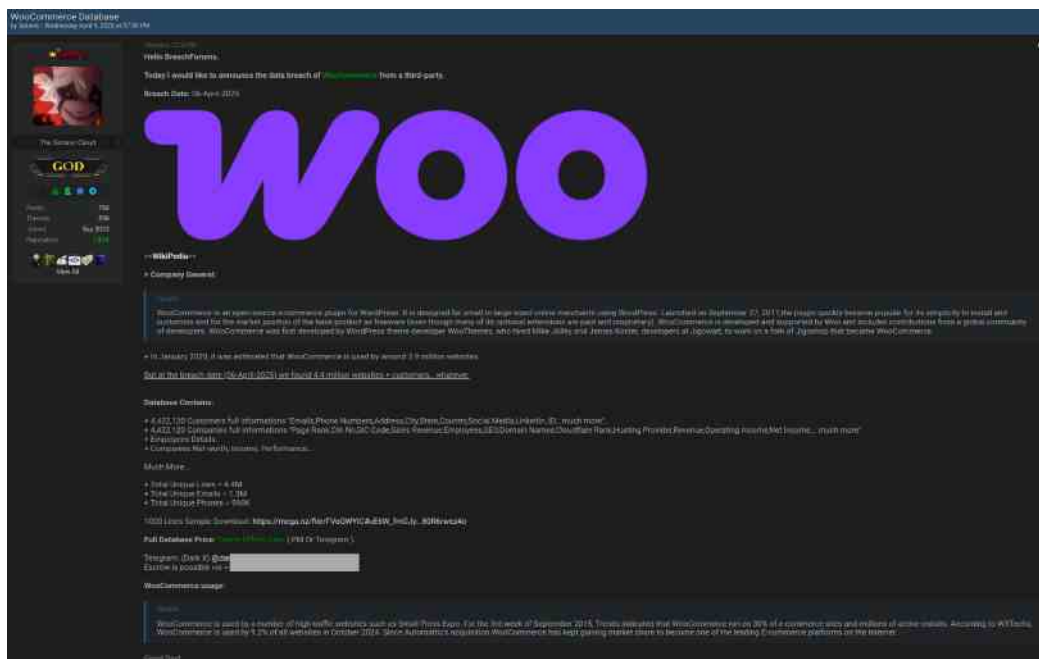
Threat actor sell stolen browser session data (cookies) harvested from stealer logs, enabling buyers to access E-commerce accounts without passwords or two-factor authentication (2FA). Below is an offering of Amazon account cookies inclusive of two-factor authentication details for account access. These accounts reportedly have active purchase histories with 2 to 100 orders placed in 2025. This method bypasses traditional login security, facilitating illicit account takeover and sales during the holiday shopping surge. This data is valuable for fraudulent transactions and further monetization.



## Selling of E-commerce Database

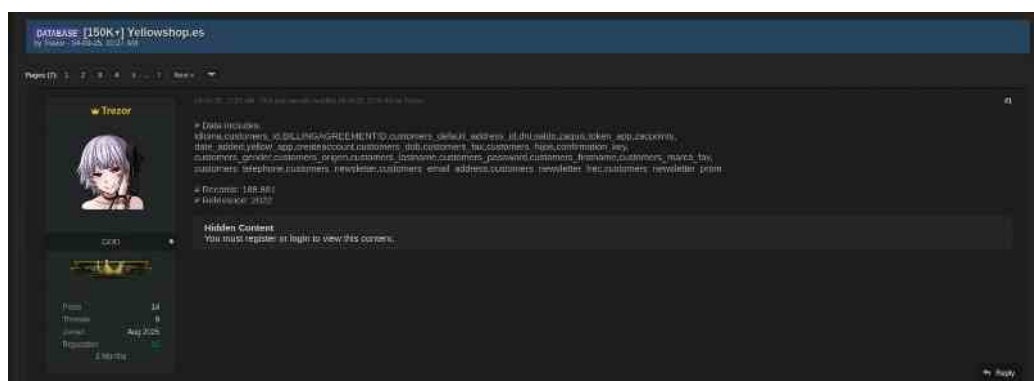
Large-scale data breaches fueling seasonal fraud ecosystems

Leaked customer and company data empowers attackers to scale credential fraud and impersonation at peak holiday activity. Below is an example of a listing advertising the breach of WooCommerce data affecting 4.4 million websites, leaking customer and business details for sale through private Telegram channels.



## Sale of compromised shopper and merchant data from E-commerce sites





## Selling of admin access to E-commerce website

Listings offering administrative or FTP access to high-revenue E-commerce companies reflect a shift toward direct exploitation and long-term monetization, as such access could enable large-scale data theft, payment skimming, or ransomware deployment to disrupt peak shopping traffic. A dark web offer advertised admin-level FTP access to a major U.S. sportswear retailer with \$6.5B in revenue, including payment and corporate server data.



## Conclusion

The holiday season brings a surge in online shopping, creating opportunities for cybercriminals to exploit increased traffic and transactions. Threat actors use phishing campaigns, stolen data sales, and vulnerabilities in E-commerce platforms to target both shoppers and businesses. This report highlights the significant risks posed by malicious holiday-themed domains, compromised E-commerce accounts, and the availability of tools such as phishing kits, sniffers, and card dumps that facilitate large-scale fraud.

These findings emphasize the need for vigilance from both consumers and organizations. Shoppers must exercise caution and adopt safe online practices, while businesses should implement proactive security measures, including regular system updates, vulnerability assessments, and customer education about potential threats.

As cyber threats continue to evolve, cooperation between security vendors, businesses, and users is critical to staying ahead of attackers. By following recommended security measures, both individuals and organizations can reduce exposure to online threats, ensuring a safer holiday shopping experience. With awareness, preparation, and the right precautions, the festive season can remain a time of enjoyment rather than risk.

---

## 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:**
  - **Enforce HTTPS Everywhere:** Make sure that HTTPS is used for all site traffic, including login and session pages, in order to encrypt cookies and guard against attacker interception.
  - **Keep ecommerce platforms, payment gateways, and software up to date** to reduce vulnerabilities.
  - **Keep all E-commerce platforms and plugins updated.**
- **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.
  - Encourage purchasing gift cards only from trusted sources and avoid sharing gift card details or codes.
- Secure Admin Panels:
  - Use strong passwords and limit access to critical systems.
  - Deploy multi-factor authentication, especially for administrative and user accounts to prevent account takeovers.
  - 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:

Rating	Label	Description
	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.otation uses a numeric code, 1-6.

Rating	Label	Description
	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.



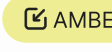


## Appendix B

### Relevance Rating Criterion

Rating	Description
High	<ul style="list-style-type: none"><li>• Threat Actor leaked or selling data pertaining to the customer organization in public/private forum.</li><li>• Threat Actor mentioned about customer organization in a Public/Private forum</li><li>• Public reporting on Organization was targeted.</li><li>• Customer technology/product involved in an attack or being targeted.</li><li>• Potential reputation harm to customer brand.</li><li>• Customer related domains Typo-squat Fraudulent domains registered.</li><li>• Proprietary customer related data found on internet. (ex: GitHub containing source code).</li><li>• Customer related domain email addresses found to be part of a data breach.</li><li>• Customer specific keywords match identified across FortiRecon's produced intelligence.</li><li>• Cyber Event impacting globally.</li></ul>
Medium	<ul style="list-style-type: none"><li>• Identification of Threat Actor targeting related Industry.</li><li>• Vulnerability disclosed Potentially impacting Organization.</li><li>• Public/Private breaches or incidents relating the organization's sector.</li><li>• Public/Private Incident identified is Unique and Provides insights into new TTPs.</li></ul>
Low	<ul style="list-style-type: none"><li>• Public/Private Incident identified targeting Customer geography vertical.</li></ul>
Informational	<ul style="list-style-type: none"><li>• Public/Private Incident identified outside of Customer geography vertical.</li><li>• Public/Private Incident gaining significant Media Attention.</li><li>• Data breaches or exposed data potentially impacting non Customer organizational.</li></ul>

# Appendix C

## TLP CRITERION

Rating	Description
<div> RED</div> <div>[Not for disclosure]</div>	<ul style="list-style-type: none"><li>Recipients may not share TLP:RED information with any parties outside of the specific organization, exchange, meeting, or conversation in which it was originally disclosed. Information could only be restricted to the ones who needs to know the information.</li></ul>
<div> AMBER+STRICT</div> <div>[Not for disclosure]</div>	<ul style="list-style-type: none"><li>Recipients may only share TLP:AMBER+STRICT information with members of their own organization.</li></ul>
<div> AMBER</div> <div>[Not for disclosure]</div>	<ul style="list-style-type: none"><li>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.</li></ul>
<div> GREEN</div> <div>[Not for disclosure]</div>	<ul style="list-style-type: none"><li>Recipients can spread the information with peers and partner organization within their community, but not via publicly accessible channels.</li></ul>
<div> CLEAR</div>	<ul style="list-style-type: none"><li>TLP:CLEAR Information May Be Shared Without Restriction. Recipients Can Spread This To The World, There Is No Limit On Disclosure.</li></ul>

