

Retail Sector **Deep Dive**

Fraud Targeting Retailers

Contents

Overview	5	Gift Card Fraud on the Dark Web	21
Malware Targeting Retail	6	Refund Fraud	25
Ducktail	6	Cost of Illicit Retail Goods	
DarkGate	8	on the Dark Web	29
Phishing Attacks	9	Gift Cards	29
Common Lures Used on the Retail Sector .	9	Personally Identifiable Information (PII) .	30
Phishing Links	9	Credit Card (CC) Numbers:	31
Noteworthy Campaigns	11	Bank Account Access:	33
Phishing via Attachments	13	Conclusion	34
Gift Card Scams	18	Mitigations	35
Fake Online Stores	20		

Overview


There are many ways that retail businesses are targeted by criminal actors. In our other report on [e-commerce threats](#), we discussed how e-commerce retailers are targeted by threat actors directly. In this report, we will discuss other methods criminals use to target retailers and their customers alike.

Malware Targeting Retail

Ducktail

Overview

Ducktail is a malware family originating from Vietnam, targeting platforms including Facebook and LinkedIn and file-hosting sites such as Dropbox and Mega, to distribute malware. It spreads primarily through phishing and social engineering tactics on social media, where users are tricked into downloading malicious content. The malware is often disguised as legitimate files, such as PDFs, delivered via shortcut files that deceive victims into initiating the download.



Project Title:	Digital Marketing Manager	Project Category:	Marketing
Department/Group:	Marketing	Project Code/Req#:	88767
Location:	Everywhere	Travel Required:	No
Lever/Salary Range:		Position Type:	Contract
HR Contact:	support@	Date Posted:	07/06/2023
Will Train Applicant(s):		Posting Expires:	30 days
External Posting URL:			
Internal Posting URL:			
Applications Accepted By:			
EMAIL:	Everywhere. 154 Krog Street, 100, Atlanta, Georgia 30307, US		
support@ Subject Line: Digital Marketing Manager			
Project Description: We are looking for an experienced Digital Marketing Manager to join our dynamic team. This position is responsible for creating, managing, leading the team and optimizing our Facebook ad campaigns from start to finish. The successful candidate will have a deep understanding of how to leverage Facebook's advertising platform to achieve business objectives and deliver measurable results.			

Figure 1. A decoy document dropped by Ducktail used to divert the user’s attention from the malicious activities going on in the background.

The malware uses PowerShell to download and execute a batch file that installs the main payload, compiled as a .NET binary. This payload extracts and executes malicious code hidden within the resource section of the file. The malware performs anti-emulation and anti-debugging checks to avoid detection in virtual environments or sandboxed systems. Once active, it gathers system information via Windows Management Instrumentation (WMI) and queries and targets popular browsers (Chrome, Edge, Brave, Firefox) to extract stored cookies, including authenticated session cookies. It further hijacks Facebook sessions, stealing user information, two-factor authentication (2FA) codes, and gains unauthorized access to Facebook Business accounts. The stolen data is compressed and exfiltrated to a Telegram command-and-control (C2) server, enabling the attacker to hijack Facebook Business accounts by adding their email to the compromised accounts and receiving recovery emails from Facebook.

Impact on the Retail Sector

This malware poses a threat especially to businesses relying on social media for marketing and customer engagement. The malware's ability to hijack Facebook Business accounts can result in attackers gaining control over critical company assets, including customer data, marketing campaigns, and financial information. Unauthorized access could allow attackers to manipulate or shut down social media accounts, disrupt online business operations, and damage a company's reputation. Additionally, the theft of cookies and sensitive session data compromises consumer trust, leading to financial losses and potential legal ramifications for failing to protect customer data adequately.

DarkGate

Overview

Recently, we observed the DarkGate malware being spread through social engineering attacks on Microsoft Teams, where a compromised Teams account was used to send ZIP files containing company-related lures, such as HR-themed content. These ZIP files contain LNK files masquerading as PDF documents, which, when clicked, execute a VBScript that begins the infection chain. The VBScript downloads additional batch commands and Autolt scripts that eventually lead to the execution of the DarkGate malware loader.

Teams -> ZIP -> LNK -> VBScript -> AutoIt -> Darkgate

[illegible]

Figure 2. The decompiled Autolt code revealed the DarkGate binary hidden in the Base64-encoded strings.

Once deployed, DarkGate can perform multiple tasks:

- Gather system information
- Communicate with a remote C2 server
- Steal sensitive data
- Perform keylogging
- Perform cryptomining

The malware incorporates multiple evasion techniques, such as antivirus detection and persistence mechanisms that allow it to stay hidden on the infected system.

Impact on the Retail Sector

The impact of DarkGate malware on the retail sector can be significant, especially given its method of delivery through Microsoft Teams, a messaging tool frequently used for internal and external communications in various organizations. The use of Teams as a phishing vector exploits employees who might be unaware and less familiar with the platform's risks compared to email-based attacks. Retail companies targeted by this malware risk having sensitive employee and customer data stolen, including system credentials, financial records, and proprietary business information.

Phishing Attacks

In our accompanying [Retail Risk Radar](#) report, Trustwave SpiderLabs found that 58% of initial access techniques used in attack were related to phishing.

Common Lures Used on the Retail Sector

To blend into the usual emails received by customers in the retail sector, threat actors pose as potential buyers in their phishing emails. Another tactic is imitating email notifications of services or applications potentially used by sector customers such as QuickBooks, Meta for Business, or Microsoft apps including Planner and Word.

Phishing Links

Below are characteristics of phishing links targeting the retail sector as observed in malicious messages:

- Phishing links often utilize open redirects to trick users into thinking that the link leads to a legitimate site and mask the actual malicious destination.
- Phishing pages are often hosted on various cloud platforms that offer free plans.
- Once targets click on a malicious link from an email, they will reach the phishing page after a series of redirections that often employ legitimate services.
- The target's email address is often incorporated in the phishing link. This tactic is used in personalizing websites and prefilling web form fields.

Across the board, we have observed an increase in phishing links concealed in attachments. This is primarily driven by [phishing-as-a-service \(PaaS\) platforms](#) such as Tycoon, Greatness, and W3LL, to name a few.

- HTML email attachments that are usually observed as standalone phishing pages or redirectors.
- PDF files and Office Documents. These contain links or QR images leading to the phishing page or a redirector, or a contact number controlled by threat actors (used in [callback phishing](#)).

In the retail sector's phishing email samples, we found the following common attachment themes:

- Invoice
- Purchase orders
- Shipping documents
- HR documents that require e-signatures

Noteworthy Campaigns

The email examples shown in this section were received by customers in the retail sector.

Fake Invitations from Prospective Clients

Cybercriminals are presenting themselves as potential clients. Under the guise of establishing communication with a retailer for a purchase order, threat actors craft emails that mimic invitation notification emails from professional networking platforms such as Zoom and LinkedIn. To be more credible, they claim that they belong to the upper management of a company.

LinkedIn Invitation from Fake Buyer

The scammer created a fake LinkedIn email to “connect” to its target retailer. The sender disguises himself as the Chief Executive Office of a well-known company and stresses that he is a genuine buyer to lure the target into accepting the supposed LinkedIn connection request. Clicking the View profile or Accept buttons lead to a credential harvesting page. Note the link in the email that contains the target’s email address after the hash sign (#).

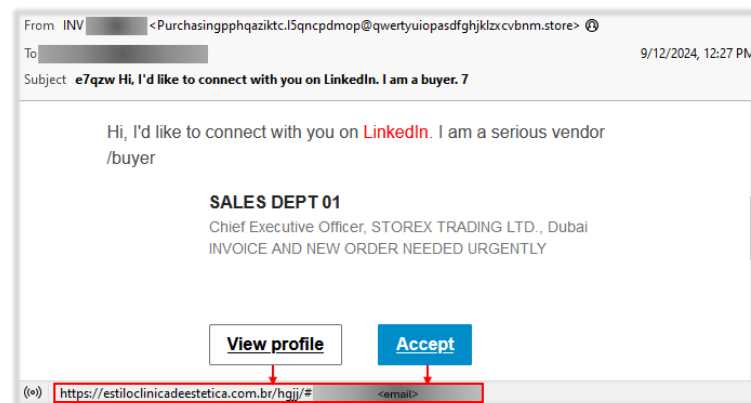


Figure 3. Fake LinkedIn phishing email.

Fake Zoom Meeting Invite

Below is a dummy Zoom meeting invitation. The sender, who claims to be a company director, wants to discuss an order via Zoom. Clicking the “Join/accept meeting” button leads the user to a phishing page hosted on Cloudflare Pages pages[.]dev. This is a web hosting service that offers free usage, hence its popularity among phishers. Last July 2023, Trustwave SpiderLabs [blogged](#) about the increasing abuse of Cloudflare services in phishing emails.

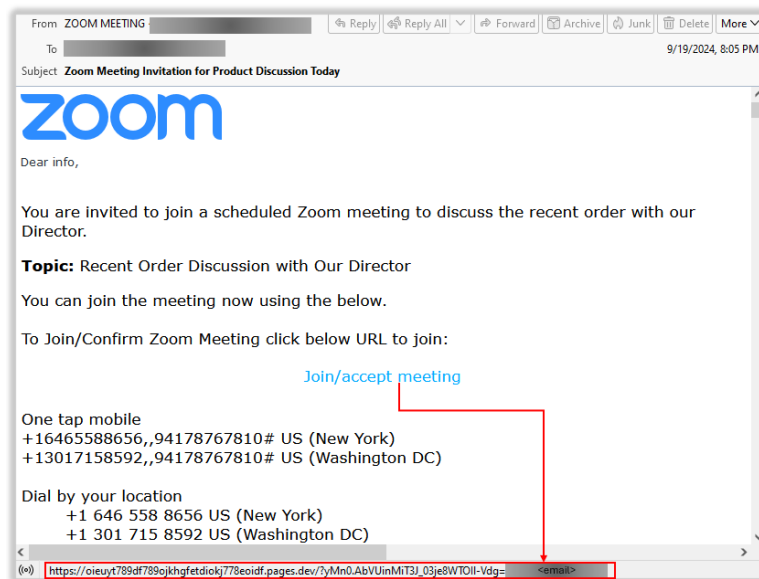


Figure 4. Fake Zoom meeting invite.

Users are redirected to a fake Zoom site after clicking on the phishing link and will be prompted to input their Zoom password when the “Join” button is clicked. The email field on the page is prefilled using the user’s email address as this data is grabbed from the phishing link (after the equal sign or = in the link). Apart from the user’s credentials, the network information of the user, through the Geoapify service, can be exfiltrated as well with this phishing attack. Stolen data is then sent to the attacker’s email, btex[.]emirates[.]net[.]ae@zohomail.eu.

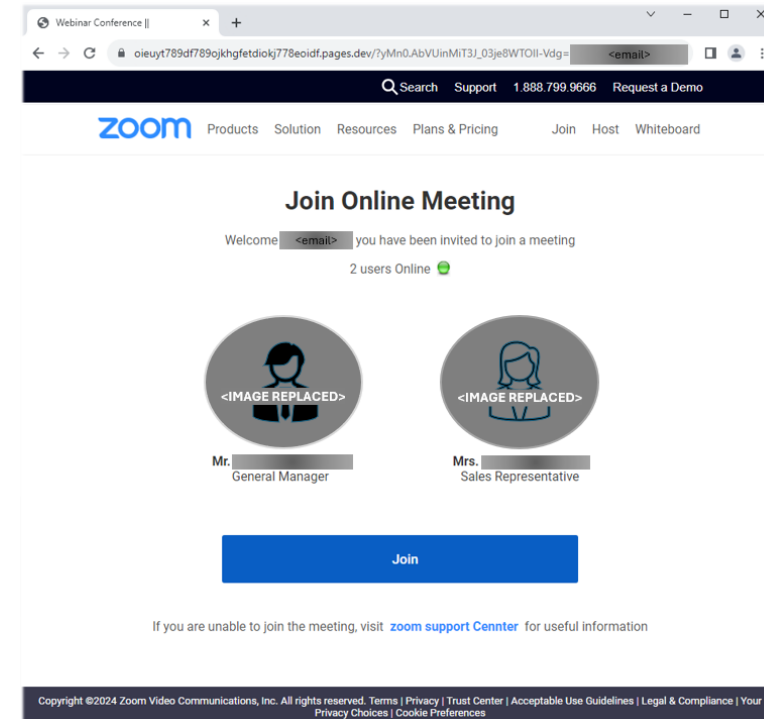


Figure 5. Fake Zoom meeting page hosted on Cloudflare's pages.dev.

Phishing via Attachments

HTML Phishing Page as Purchase Order

The email sample below has an HTML attachment disguised as a purchase order. It is noted on the message body that the sender, a General Manager, initially attempted to call the recipient but failed. This scheme is set to prepare the recipient for what they will see when the attachment is opened.

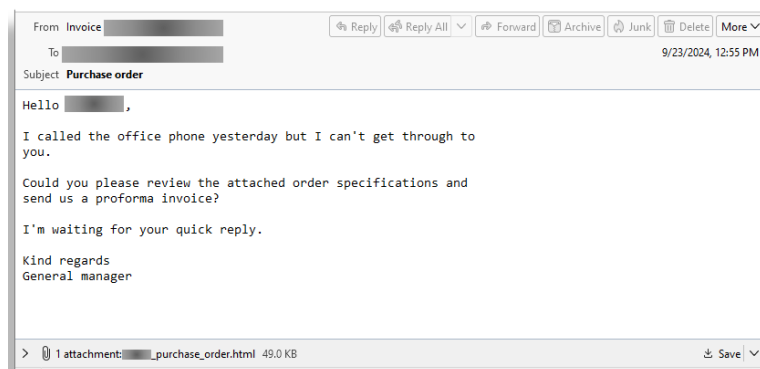


Figure 6. Invoice-themed email with HTML phishing attachment.

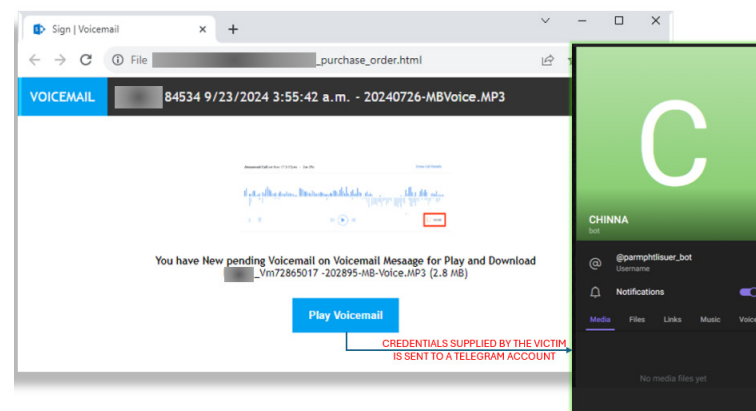


Figure 7. Opened HTML phishing attachment with a voicemail theme.

Quishing via Word Document

Quishing is a phishing attack where the phishing URL is hidden in a QR code. The rise of phishing campaigns employing this technique [were](#) observed by Trustwave in 2023, and this attack remains a persistent threat.

Figure 8 is a message received by a customer in the retail sector and is an example of an HR-themed phishing email purporting to be a notification email from the Microsoft Word application. The message includes a Word document file attachment that contains a QR code. The URL in the QR code is associated with the [Tycoon Group phishing-as-a-service \(PaaS\)](#).

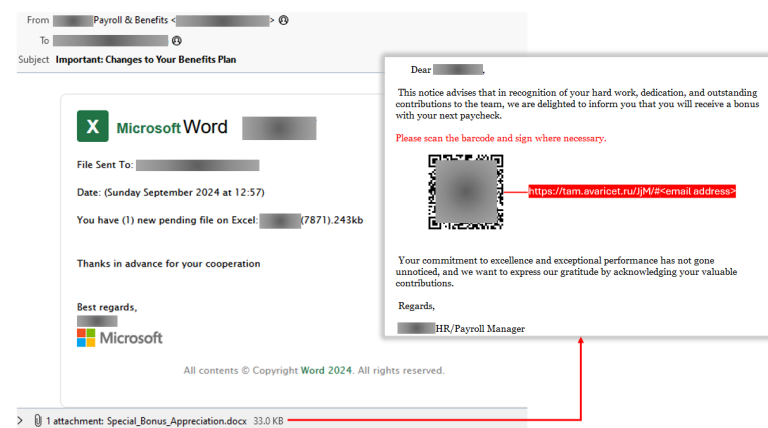


Figure 8. A phishing email containing a Word document with a malicious QR code.

QuickBooks Callback

Below are two examples of phishing emails pretending to be from QuickBooks, an accounting software from Intuit that is commonly used by small- to medium-sized businesses in tracking their financial activities. Both emails are fake subscription cancellation email notifications.

The first sample is a [callback phishing email](#). Also known as BazarCall, this type of phishing attack disguises an attacker-controlled contact number as a legitimate business support number. In Figure 9, the attacker's contact number is cloaked as QuickBooks'. If the target decided to call the number, this could lead to a voice phishing (vishing) attack.

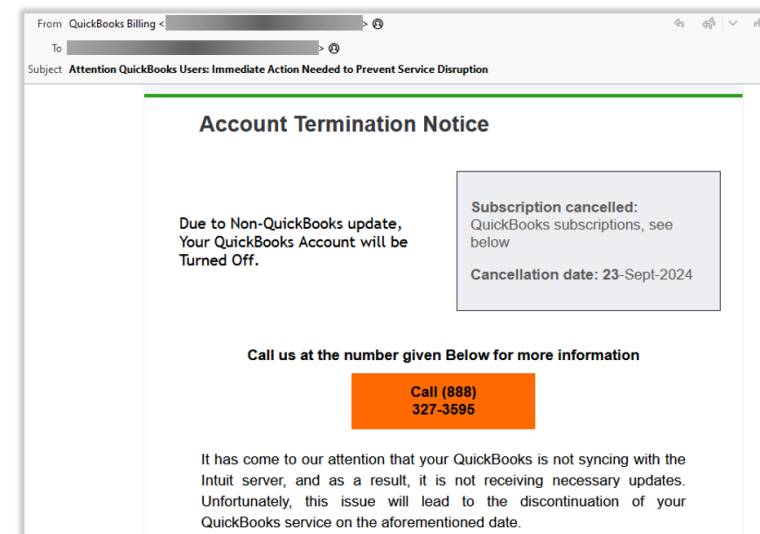


Figure 9. A callback phishing email with a fake QuickBooks support number.

The second sample leads to a credential harvesting phishing site. The email has a PDF attachment cloaked as an Intuit subscription document. The PDF file contains the initial phishing link.

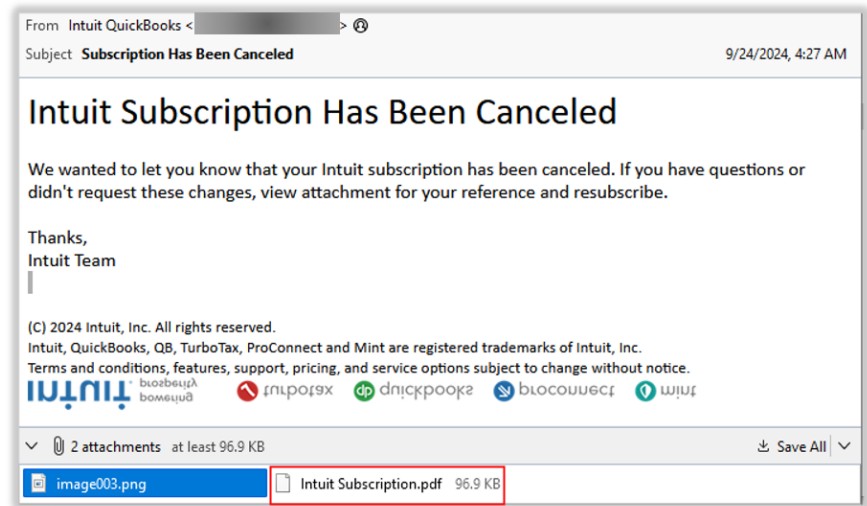


Figure 10. A phishing email with a malicious PDF file attachment.

As seen on Figure 11, the initial link found in the malicious PDF attachment, `hxxps://s[.]id/tD5Dx`, is from a URL shortening service. This is anchored to the “Resubscribe” string. When clicked, the short URL will redirect to an Intuit phishing page which is hosted on a newly registered domain `qbintmerchantonline[.]com`.

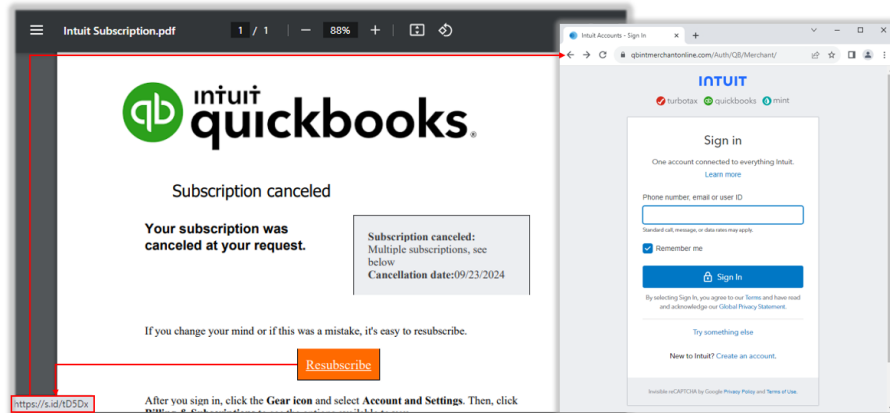


Figure 11. The “Resubscribe” button in the malicious PDF attachment leads to a phishing page.

Costco Reward Scam

A reward scam is a common type of scam where fraudsters impersonate well-known retail brands and promise rewards after completing a fake task, such as participating in the brand's loyalty program or survey. To entice victims, reward scams typically offer a gift card or the latest product to entice victims. This kind of attack often leads to a credential phishing page mimicking the brand's account sign-in page.

Figure 12 shows Costco reward scam email samples. The reward being advertised is an iPhone 16 Pro, a recently released Apple product. When users click on the "CONFIRM NOW!" button, they will be redirected to a page hosted on Google's Firebase storage. As of writing, the next stage URL `newsletteroffer2025[.]com` is already down.

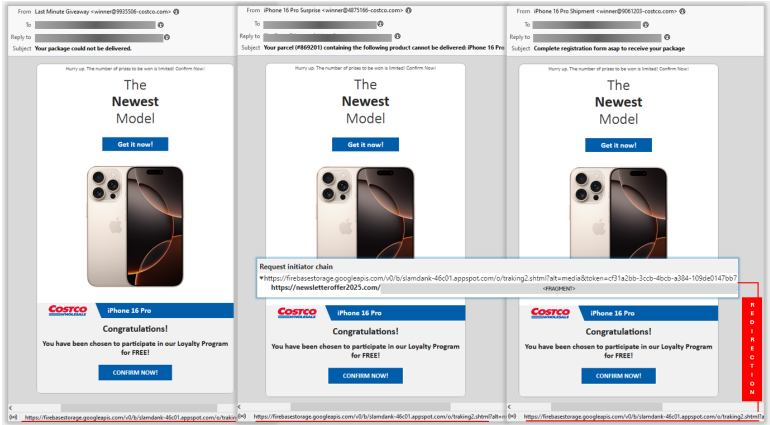


Figure 12. Costco reward scam email samples.

Abuse of Legitimate Invoicing Platforms

We have seen the use of legitimate payment services and invoicing platforms to deliver phishing links and host content. In the case below, the accounting platform Xero is used to both send a phishing email and host a PDF file, which is another example of callback phishing. With Xero, users can send an invoice with a link and/or document attachment containing transaction details.

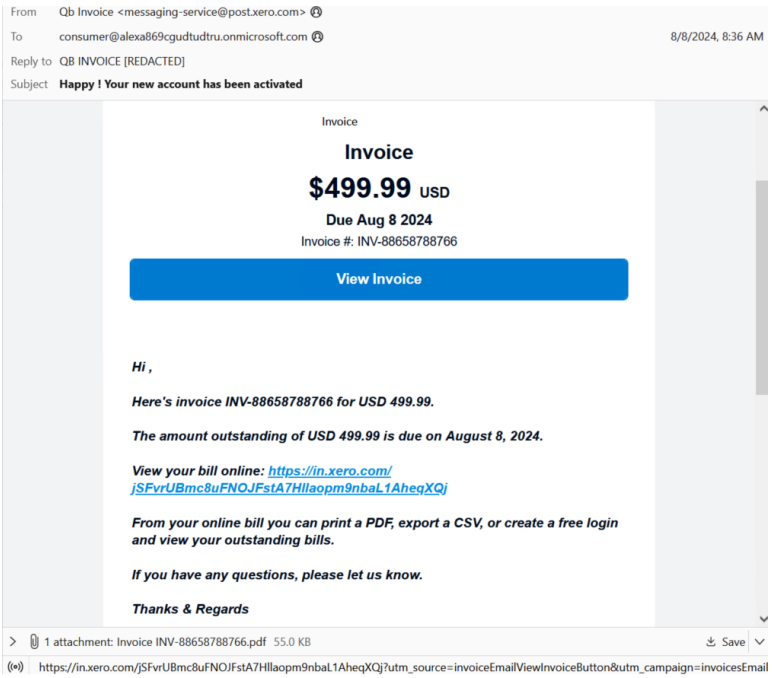


Figure 13. Callback phishing email sent using Xero, a legitimate accounting platform.

This email is a legitimate notification sent through the Xero platform. This was sent on behalf of “QB Invoice.” Viewing the full invoice, either by clicking the link or opening the PDF attachment, will reveal a convincing and proper-looking document.

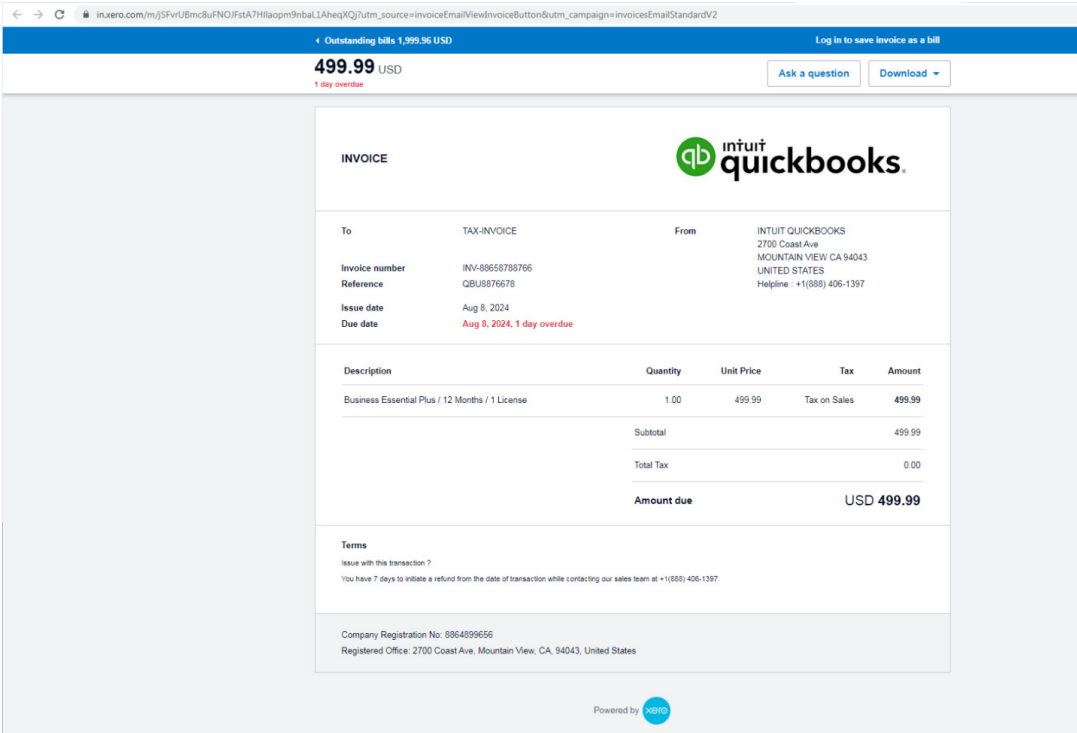


Figure 14. A bogus QuickBooks invoice hosted on Xero.

In this example, the bill is said to be one day overdue, which raises a sense of urgency to victims. The term of the invoice declares that the victim has seven days to call the bogus phone number to dispute the transaction.

Gift Card Scams

Gift card scams are some of the most pervasive and effective scams today, racking up [\\$217 million](#) in total money lost in 2023 according to the Federal Trade Commission. There are different [kinds of gift card scams](#), ranging from threat actors pretending to be family members in an emergency situation needing gift cards to cybercriminals [impersonating tech support professionals](#) and deceiving victims into paying them using gift cards.

With the holidays fast approaching, malicious actors are bound to launch gift card attacks. The following are some of the most recent gift card scams we're seeing in the wild.

Card Draining Scam (2023)

In December 2023, police officers in California apprehended a man named Ningning Sun who was found to be tampering with gift cards being sold in a Target store in Sacramento. Based on reports, detectives observed Sun taking gift cards on a rack inside his jacket. He then proceeded to replace the

gift cards he stole with seemingly identical ones. Before he had the opportunity to leave the store with the stolen goods, police officers confronted him. The police found more than 5,000 Apple and Target gift cards in Sun's possession.

With the holidays coming up, police are sending out warnings to consumers to be wary of gift cards that have signs of tampering, including scuff marks or scratches, especially those near the card's bar code. [Card draining](#) happens when malicious actors steal a gift card's card number and security code that's typically hidden by a thin silver layer, illicitly get the gift card balance, and reseal the card to make it look uncompromised.

[Gift card draining](#) can also happen when scammers remove gift cards from their respective envelopes, physically cut up the part of the card that contains the code, and put the rest of the card back to the envelope.

Atlas Lion or Storm-0539 (2024)

According to Microsoft, Atlas Lion (aka Storm-0539), has been targeting retail organizations, breaching their systems, and illicitly issuing gift cards with amounts reaching up to \$100,000 per day to themselves.

The Morocco-based group conducts a [sophisticated gift card scam](#) that involves the following steps:

- Conducting reconnaissance on retailers' gift card issuance processes, and employee access.
- Pretending to be legitimate non-profit organizations by creating fake, but convincing, websites to obtain resources from cloud providers.
- Launching phishing and smishing attacks to get login information and registering their own devices into a victim's network to bypass MFA and establish persistence within the environment.
- Creating new gift cards for cashing out or selling to other cybercriminals on the Dark Web.

Fake Online Stores

Cybercriminals are taking advantage of consumers' penchant for making purchases online by creating realistic-looking fake online stores to steal victims' credit card information, credentials, and personal information.

Security Research (SR) Labs observed that the China-based [BogusBazaar group](#) has been actively creating and managing a network of fake e-commerce sites. Collectively, these fraudulent websites have processed over a million orders since 2021, victimized approximately 850,000 mostly US and Western European consumers, and stolen over \$50 billion from fraudulent orders.

The researchers noted that although not all orders made through the fraudulent websites are successfully processed, the BogusBazaar group has access to victims' financial and personal information.

Gift Card Fraud on the Dark Web

Gift card fraud has emerged as a significant issue for retailers and e-commerce platforms, particularly with cybercriminals exploiting various weaknesses in the system. Fraudsters commonly purchase gift cards using stolen credit card details. Once the card is acquired, they quickly redeem or sell it before the fraudulent transaction can be flagged and reversed. In many cases, this leaves the retailer to absorb the financial loss, as the transaction is often unrecoverable.

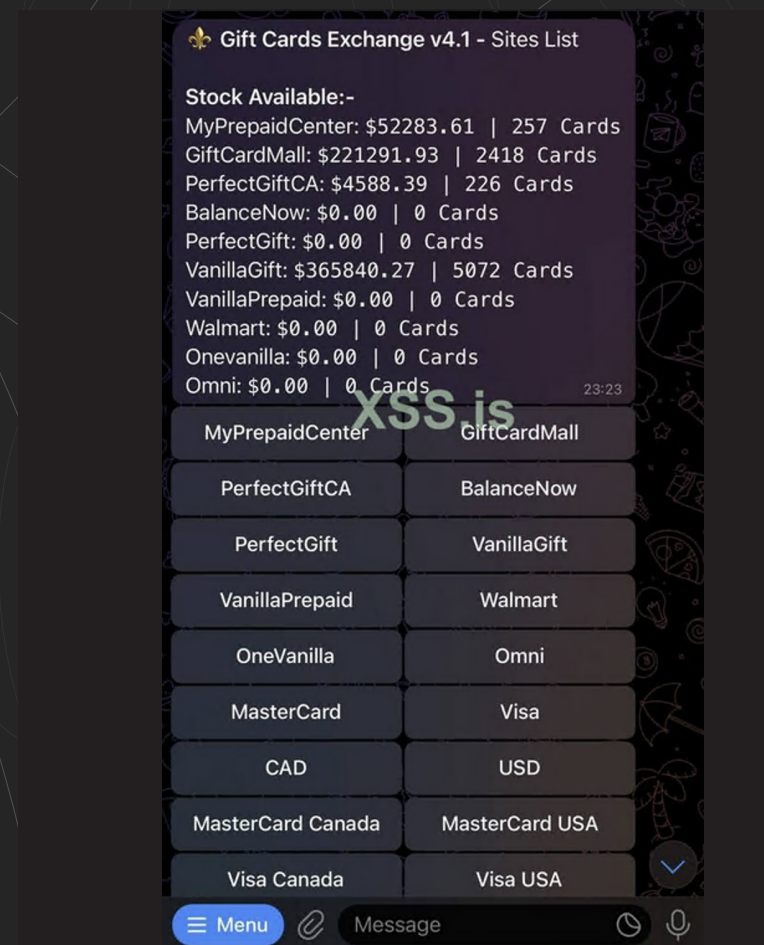


Figure 15. Dark Web forum XSS, an actor's illustration of a Telegram channel for selling gift cards.

Hackers also employ phishing attacks and account takeovers to access customer accounts and steal their gift card balances. In addition, some attackers find vulnerabilities in retailers' systems that allow them to generate or manipulate gift card values without legitimate transactions. Another common scam involves refund fraud, where criminals return purchased items and receive a refund in the form of a new gift card, which is then resold.














Ordering form			
	Gold CC/Fullz balance: 7000\$	299\$	Quantity: <input type="text"/>
	Platinum CC/Fullz balance: 15000\$	499\$	Quantity: <input type="text"/>
	AliExpress Gift Card balance: 500\$	249\$	Quantity: <input type="text"/>
	AliExpress Gift Card balance: 1000\$	449\$	Quantity: <input type="text"/>
	Amazon Gift Card balance: 300\$	69\$	Quantity: <input type="text"/>
	BestBuy Gift Card balance: 300\$	69\$	Quantity: <input type="text"/>
	Ebay Gift Card balance: 300\$	69\$	Quantity: <input type="text"/>
	iTunes Gift Card balance: 200\$	119\$	Quantity: <input type="text"/>
	Steam Gift Card balance: 300\$	69\$	Quantity: <input type="text"/>
	Target Gift Card balance: 300\$	69\$	Quantity: <input type="text"/>
	Visa Gift Card balance: 500\$	149\$	Quantity: <input type="text"/>
	Visa Gift Card balance: 1000\$	449\$	Quantity: <input type="text"/>
	PayPal account balance: 5000\$	349\$	Quantity: <input type="text"/>
	PayPal account balance: 10000\$	449\$	Quantity: <input type="text"/>

Figure 16. An advertisement for a Dark Web marketplace that sells gift cards.

On the Dark Web, gift cards are frequently bought and sold at a fraction of their original value, as they are often obtained through hacked accounts or stolen credit cards. Fraudsters also use automated tools to brute force gift card numbers, searching for active cards with a balance. Once found, they quickly use or sell these cards, leaving legitimate customers with depleted funds.



Cytron
Премимум

Регистрация: 18.04.2023
Сообщения: 14
Реакции: 2
Гарант сделки: 1
Депозит: 30 ₺

07.08.2024

👤 Список товара и проценты 🔄 Update

- Bitnovo | CoinBase | Binance — 95%
- Steam USD | EUR | GBP — 82%
- Razer Gold — 80% (Hold) | Instant — 75%
- iTunes USA — 75% на номиналы 10-15-25-50-100
- Amazon Physical Card + чек paid by cash — 75%
- iTunes EU — 70% | UK — 65%
- Google Play USA | EUR — 70% | UK — 65%
- PlayStation USA | EUR — 70% | UK — 65%
- Xbox EURO | USA — 70% | UK — 65%
- Nintendo EURO | USA — 70% | UK — 65%
- Blizzard EURO | USA — 70% | UK — 65%
- Ebay — 70%
- Netflix EURO | USA | UK — 65%
- Roblox EURO | USA | UK — 65%
- League of Legends Gift Card — 65%
- Uber, Uber Eats — 65%
- Airbnb gift cards — 65%
- Adidas gift cards — 65%
- Twitch Gift Card — 65%
- Zalando — 60%
- Spotify — 60%
- Starbucks — 60%
- IKEA gift cards — 60%
- Bigo Live — 60%
- Hulu — 45%
- Meta Quest — 45%

Figure 17. Another Dark Web forum XSS, an advertisement for selling gift cards.

Gift card prices on Dark Web marketplaces are influenced by several factors. First is the gift card balance; cards containing higher amounts generally command higher prices, though they are sold at a significant discount compared to their face value. For example, a \$100 gift card might be sold for \$30 to \$60, depending on additional factors. The popularity of the retailer also plays a major role; cards from major stores such as Amazon, Walmart, or other popular chains are typically more valuable because they offer greater flexibility for purchases, making them easier to resell or use.

Amazon.com Gift Card 700-750\$

DoomShopFTP · 25.07.2024 ·

amazon

gift card

гифт карты

отработка на гифты

В ЭТОЙ ТЕМЕ МОЖНО И

NO AVATAR

DoomShopFTP
фору-диск
Пользователь

25.07.2024

Цена:

700\$

Контакты:

tg @gimmy_the_loot

В наличии гифт карты Amazon.com US

Балики 700-750\$

На руках 6 гифтов и ожидаются еще

Ишу кто купит

Не чарджнут, можно сказать даже белые

Жалоба

Figure 18. A Dark Web advertisement for Amazon gift cards.

Translation:

Amazon.com US gift cards available

Nominal value \$700-750

I have 6 gifts on hand and more are expected

I'm looking for someone to buy them

They won't charge, you could say even white ones

The level of risk associated with the gift card's origin also affects pricing. Cards obtained through high-risk methods, such as those purchased with stolen credit cards, tend to sell at deeper discounts since there's a higher chance they could be flagged or canceled by retailers. Conversely, cards that are seen as "clean" or low risk, such as those taken from compromised customer accounts or through insider manipulation, may command higher prices. Lastly, market demand plays a role — when certain retailers are more in demand or seasonal factors make certain types of cards more desirable, prices may rise accordingly.

The consequences for retailers are severe, including direct financial losses from the fraudulent use of gift cards, increased operational costs to prevent fraud, and potential reputational damage. Companies are forced to invest in stronger fraud detection systems and more secure gift card processes, but despite these efforts, gift card fraud remains a persistent threat in the retail industry.

Refund Fraud

Refund fraud is a growing problem in the e-commerce and retail industry, with large retailers being frequent targets. The scam involves fraudsters exploiting the lenient return and refund policies of these companies to obtain refunds without returning the purchased items. This type of fraud is increasingly being advertised on the dark web, where groups offer to carry out the scam on behalf of customers in exchange for a fee or a portion of the refund.

The image shows a screenshot of a forum post on a dark web platform. The forum interface includes a user profile on the left for 'cocoluman' (Advanced Member, joined Mar 08, 2024) and a main post area. The post is titled 'COCO'S REFUNDING SERVICE' and is dated 'Posted 08 June 2024 - 06:30 PM'. The service claims a success rate of up to 99.99% and offers expedited refunds. It outlines a three-step procedure: STEP 1: PLACE THE ORDER, STEP 2: RECEIVE THE ORDER, and STEP 3: CONTACT ME FOR THE REFUND. The post also includes a list of targeted retailers: AMAZON, INSTACART, TARGET, BESTBUY, WALMART, NIKE, WAYFAIR, and SEPHORA.

Coco's Refunding Service [5% FEE] [100% SR] [AMAZON] [INSTACART] [TARGET] [BESTBUY] [WALMART] [NIKE] [WAYFAIR] [SEPHORA] [ETC]

Posted 08 June 2024 - 06:30 PM

E96eemKE96eemKE96eemK

COCO'S REFUNDING SERVICE

WHY CHOOSE US?

We offer expedited refunds with a success rate of up to 99.99%. Our team responds promptly and completes your requests efficiently.

PROCEDURE

STEP 1	STEP 2	STEP 3
PLACE THE ORDER	RECEIVE THE ORDER	CONTACT ME FOR THE REFUND

Figure 19. A refund fraud scheme advertisement on a Dark Web forum that illustrates how the scam is carried out.

The process typically begins with fraudsters purchasing high-value items, such as electronics or luxury goods, from retailers. After receiving the item, they initiate a refund request, falsely claiming that the item was not delivered, damaged upon arrival, or missing from the box. Retailers with automated or customer-friendly refund processes may issue a refund without investigating the claim thoroughly. The fraudster then keeps the item and resells it for profit, leaving the retailer to absorb the financial loss.



Figure 20. A partial refund fraud advertisement on a dark web forum that shows retailers and e-commerce providers that the advertiser can sell information for.

In response to the increasing threat of refund fraud, many retailers are tightening their return and refund policies and leveraging technology to detect fraudulent activity. While these efforts can mitigate the impact, refund fraud remains a persistent problem that continues to evolve in the world of e-commerce.

New aces up malicious actors’ sleeves have recently been making the rounds on the cybercriminal underground — malicious insiders. These insider threats work for targeted organizations and are headhunted or hired by malicious actors. Malicious insiders within retail companies can significantly undermine refund procedures by exploiting their access to internal systems and knowledge of company policies. These insiders may collaborate with external fraudsters or act independently to manipulate refund processes for personal gain.

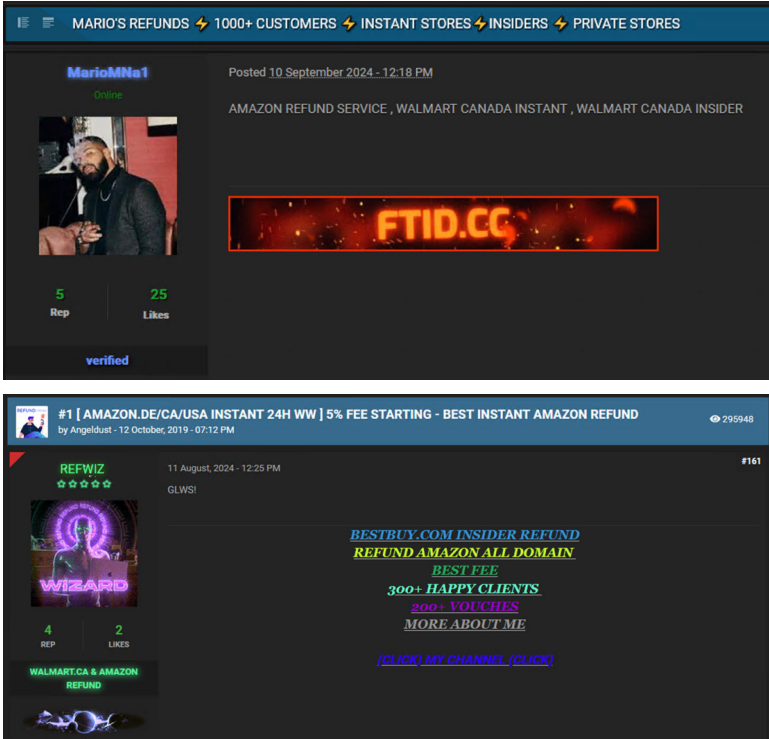


Figure 21. Dark Web forum advertisements that mention refund fraud via malicious insiders.

With their understanding of the company's refund mechanisms, they can bypass certain security checks, approve fraudulent claims, or falsify return records, allowing refunds to be issued without actual product returns. They can also manipulate customer accounts, create fake transactions, or inflate the value of returns, all while avoiding detection through their insider privileges. This can lead to substantial financial losses for the retailer, as fraudulent refunds are processed seamlessly without raising red flags.

For retailers, refund fraud results in significant financial losses as they not only lose the value of the item but also incur the cost of processing the fraudulent refund. Over time, these schemes can lead to stricter return policies, making it harder for legitimate customers to return items. Retailers may also suffer reputational damage, as frequent fraud can diminish customer trust. Combatting this type of fraud often requires investing in advanced AI-driven fraud detection systems, training customer service staff to identify suspicious claims, and working with law enforcement to pursue criminal charges against perpetrators.

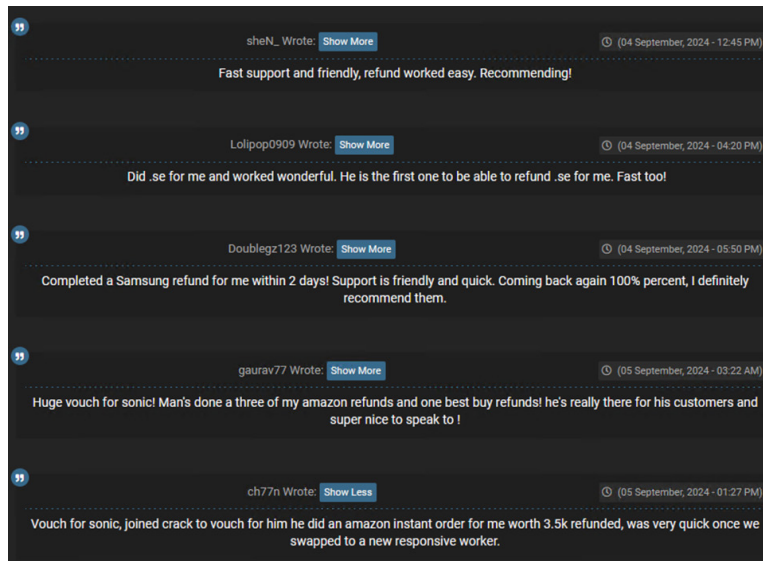


Figure 22. Users of a return fraud service give their positive feedback on a Dark Web forum.

Cost of Illicit Retail Goods on the Dark Web

Prices on the Dark Web are influenced by several key factors. For example, the rarity of data or items, freshness (how recent the stolen data is), validity (whether the credentials are still working), and quality (what kind of access or benefits the information provides) all play a role. Additionally, demand in certain sectors or geographical locations impacts prices. For instance, credit card numbers with high credit limits or bank accounts from affluent individuals can fetch higher prices, while simple usernames and passwords without much-associated value are typically lower priced.

In 2024, the prices of various illicit goods on the Dark Web are shaped by demand, item rarity, and the level of risk associated with the stolen data. Here's a more detailed breakdown:

Gift Cards

Value: \$20–\$1000+

On a Dark Web forum, sellers are offering gift cards from well-known retailers, pricing them based on a percentage of their face value. These cards come from popular stores like Amazon, Walmart, and others, with higher-value cards fetching premium prices. The pricing strategy depends on the balance, popularity of the vendor, and ease of cash-out for buyers. Such gift cards are highly sought after, often used for laundering money or acquiring goods anonymously, making them a key commodity in cybercriminal trade. They provide a low-risk method for converting digital profits into real-world assets.

Personally Identifiable Information (PII)



Figure 23. Fullz, which consists of complete sets of PII, for sale on the Dark Web.

Fullz, which consist of complete sets of PII, are highly valuable on the Dark Web because they enable identity theft and fraudulent activities. Criminals can use Fullz to open bank accounts, apply for loans, or conduct other forms of financial fraud. Medical records, in particular, are even more sought after since they contain not only PII but also sensitive health data, making them useful for insurance fraud. The detailed nature of medical records allows for more complex fraudulent schemes, increasing their price and demand.

- **Basic PII (name, address, email):**
\$5–\$15
- **Full identity profiles (fullz) (including SSN, DOB):**
\$20–\$100+
- **Medical records:**
Up to \$500+

Credit Card (CC) Numbers:

Prices for credit cards on the Dark Web can vary dramatically across different markets, influenced by multiple factors. Here’s an expanded breakdown:

- **US:** With a large supply of stolen credit cards and relatively lower barriers to purchase, US credit cards are cheaper, averaging \$10-\$40. The sheer volume of available data and more lenient regulations contribute to these lower prices.

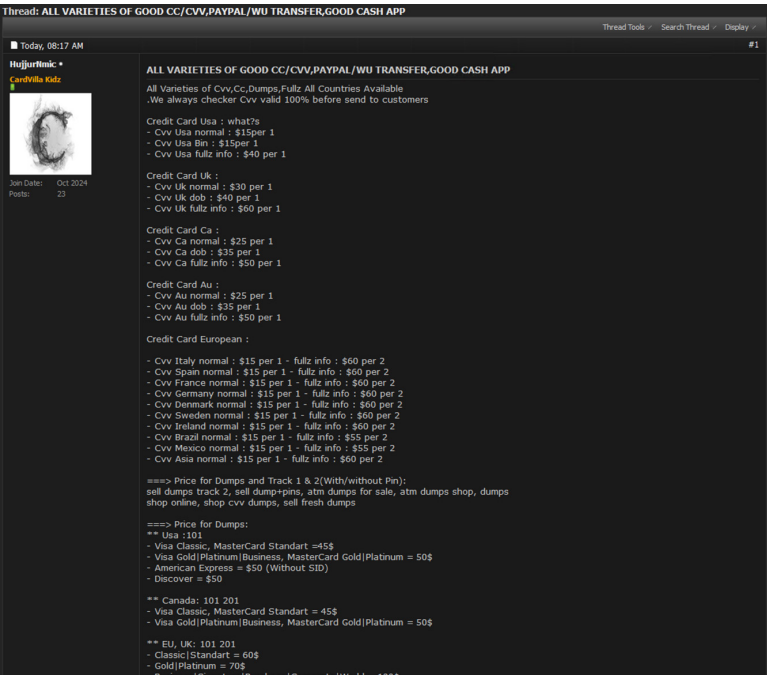


Figure 24: The Dark Web actor illustrates prices in its pricelist.

- **UK:** UK credit cards, priced between \$10-\$60, tend to be more expensive due to higher fraud detection rates and a smaller supply. Stricter bank regulations also push prices up.

Page: 1 2 >

Type	Number	Category	First Name	City	State	Zip	Country	SSN/CPF	DOB	Price	
	446053XXXXXX	VISA/MC	Julian	Melbourne	FL	32935	US	✗	✗	\$10.00 + \$0.10	<input type="checkbox"/>
	444796XXXXXX	VISA/MC	France	Melbourne	FL	32935	US	✗	✗	\$10.00 + \$0.10	<input type="checkbox"/>
	518725XXXXXX	VISA/MC	Kaley	Melbourne	FL	32935	US	✗	✗	\$10.00 + \$0.10	<input type="checkbox"/>
	521729XXXXXX	VISA/MC	Alfonzo	Melbourne	Victoria	3031	AU	✗	✗	\$15.00 + \$0.10	<input type="checkbox"/>
	521729XXXXXX	VISA/MC	Darrell	Melbourne	Victoria	3183	AU	✗	✗	\$15.00 + \$0.10	<input type="checkbox"/>
	521729XXXXXX	VISA/MC	Dakota	Melbourne	Victoria	3205	AU	✗	✗	\$15.00 + \$0.10	<input type="checkbox"/>
	521729XXXXXX	VISA/MC	Mrs.	Melbourne	Victoria	3183	AU	✗	✗	\$15.00 + \$0.10	<input type="checkbox"/>

Figure 25: Pricing from one of the Dark Web credit card shops shows differences in regional pricing.

- **Australia:** Credit cards from Australia, fetching around \$15-\$50, are priced higher due to lower availability and increased demand, as breaches in Australia are less common but highly targeted.
- **Germany:** German credit cards are among the most expensive, typically ranging from \$10-\$50. Strict European Union (EU) data protection regulations make these cards harder to obtain, hence the higher price.

Prices vary depending on the card's limit, the inclusion of the CVV number, and the reliability of the source. Cards from regions with less stringent fraud detection often command higher prices.

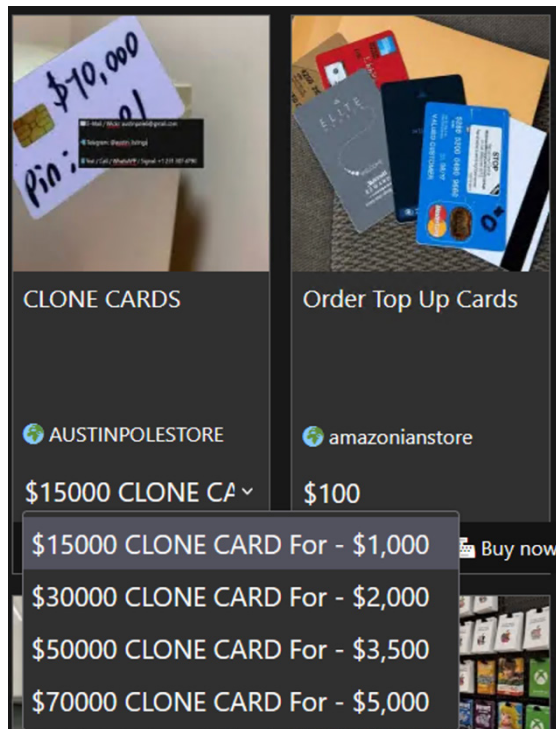


Figure 26: The Dark Web Credit Card shop offers cloned cards with different balances

Prices are influenced by the effectiveness of fraud detection systems and security measures in each country. In regions like the UK and Germany, where advanced anti-fraud protections exist, it's harder for criminals to exploit stolen cards, raising their value. Credit card prices also increase when more detailed information is provided, such as CVV, billing address, or account balance. In markets like the US, where credit is more accessible, cards may be cheaper but easier to misuse, while stricter systems in places like Germany make those cards more valuable for fraud.

Bank Account Access:

Bank account access is highly prized on the Dark Web due to its direct financial payoff. The price of an account varies depending on factors like the account balance, bank location, and whether the account comes with supplementary information such as security questions or transaction history. Higher balances command higher prices, as they offer a bigger payoff for attackers. Preferred banks are often those with weaker security measures or systems that allow quick transfers. Popular targets include US banks and international institutions with lenient fraud detection systems. Attackers also favor accounts from banks with high limits on transactions or withdrawals.

- **Low-balance accounts:**
\$200–\$500
- **High-balance accounts:**
\$1,000 or more
- **Bitcoin/crypto wallets:**
\$100–\$1,000+, depending on balance

Conclusion

Credential stealer logs remain highly dangerous because they provide direct access to victims' accounts across multiple platforms. Attackers who possess this information can carry out account takeovers, initiate fraud, or sell the data for further exploitation. Protecting against these threats requires constant monitoring, multi-factor authentication (MFA), and educating users about phishing attempts.

Mitigations

The most terrifying thing about retail scams is how common they are. Retail fraud is so prevalent, it can happen to anyone. Consumers can avoid falling for scams by adopting these security tips:

- **Think Before You Click:** Before downloading attachments or clicking on links, make sure that the email is from a trusted source. Use your cursor to hover over hyperlinks to check if the URL is from a legitimate company.
- **Use Email Security Services:** These can help effectively flag and block phishing emails and malware-laden attachments.
- **Carefully Check Gift Cards:** Don't purchase gift cards that appear to have been scratched, scuffed, or show signs of compromise.
- **Learn to Spot Phishing Emails:** Carefully check the content of the email for typographic errors, generic greetings, and requests for personal information.

Meanwhile, retail companies can remain protected against malware attacks and scams by following these security best practices:

- **Use Robust Email Security Solutions:** Use a multilayered, AI-powered email security solution that detects emerging and unknown email-based threats.
- **Conduct Security Training:** Regularly educate employees and run phishing simulations about time-tested and novel phishing tactics.
- **Implement Strong Password Policies:** Encourage employees to create strong and complex passwords and use MFA as an added layer of security.
- **Audit Financial-Related Processes:** Verify financial-related processes including refund and gift card processing to stop fraudulent requests and transactions.

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

