Silent Push Unwraps the AIZ—Aggressive Inventory Zombies—Retail & Crypto Phishing Network Campaign

By Peggy Kelly

Published: 2024-12-11 · Archived: 2026-04-05 14:25:20 UTC

- Key Findings
- Executive Summary
- Sign up for a free Silent Push Community account
- Background on AIZ Retail Targeting
- Initial Intelligence Gathering
- Expanding Beyond “Etsy” Sites into Other Brands
- Targeting Multiple Retailers
- Searching 1,300 Brand Names
- Amateur Monetization Efforts Across the “Aggressive Inventory Zombies” Network – Phishing Chats with Out-of-Office Sellers
- “AML Check” Cryptocurrency Phishing from AIZ Threat Actor
- “Input Pass Code” Phishing Sites
- “MBN” Crypto Phishing Sites
- Pantera Exchange Crypto Phishing Campaign
- “Exness” Crypto Phishing
- “Moomoo Financial” Phishing Campaign
- Aliexpress Targeting Pivots into Larger Retail Phishing
- Bitcoin Targeting Pivots into Larger Crypto Phishing Campaign
- Continuing to Track the AIZ Retail and Crypto Phishing Campaigns
- Additional information
- Mitigation
- Register for Community Edition
- Indicators of Future Attacks (IOFAs)

Key Findings

Silent Push Threat Analysts have been tracking the activity of a threat actor we’ve dubbed “Aggressive Inventory Zombies” (AIZ) throughout 2024, which has been noticeably ramping up over the past few months.

Our observations of a few suspicious domains impersonating Etsy led to the discovery of a large-scale phishing and pig-butchering network targeting retail brands and a crypto phishing campaign.

- The retail phishing campaign extends beyond Etsy – taking aim at major retailers and marketplaces, including but not limited to Amazon, BestBuy, eBay, Wayfair, and more.
- The threat actor has been building phishing websites using a popular website template and integrating chat services for its phishing activities.
- The threat actor behind this retail campaign is also targeting crypto audiences, and the scale of the sites in this network proves it is a substantial effort.
- Silent Push Threat Analysts received a substantial source of pivots for this network by collaborating on takedown efforts of some related campaign infrastructure with Stark Industries. They shared several dozen other IPs with us that the threat actor had been using, which helped us flesh out the full extent of these malicious campaigns.
- Our research can confirm the threat actor has some financial ties to India.

Executive Summary

Silent Push Threat Analysts recently observed a few suspicious domains appearing to impersonate the e-commerce company Etsy—something we initially thought was timely for the 2024 holiday season. Further investigation, however, led us to uncover a large-scale phishing campaign and a crypto phishing network.

We found that the retail phishing campaign extends beyond Etsy and targets major retailers, including, but not limited to, Amazon, BestBuy, eBay, Rakuten, Wayfair, and more.

The threat actor has been using a popular website template to build phishing websites and appears to primarily conduct phishing activities over chat services integrated into the sites. Based on some sensitive details acquired when testing the phishing process on retail sites, our team can confirm that the threat actor has some financial ties to India.

It’s clear that the threat actor behind this AIZ retail campaign is also targeting crypto audiences, and the scale of the sites in this network proves this is a substantial effort.

This blog's research will begin with our understanding of the AIZ retail network and then provide additional context about the crypto sites and other infrastructure we found.

Silent Push Enterprise users have access to two dedicated IOFA Feeds containing all the true positive domains and IPs we gathered during our research.

For operational security reasons, we are unable to share the exact specifics of each query and pivot utilized. Silent Push Enterprise customers have access to a dedicated AIZ Retail & Crypto Phishing Network TLP: Amber report, which contains all the relevant data types and pivot points we used to track the infrastructure referenced in this blog.

Register for our free Community Edition to use all of the tools and queries mentioned in this blog.

Background on AIZ Retail Targeting

Silent Push Threat Analysts have been tracking a threat actor's activity throughout 2024 that has been noticeably ramping up over the past few months. Our discovery of its large-scale phishing campaign began with our researchers observing suspicious domains appearing to impersonate Etsy.

Extending beyond Etsy, the phishing campaign targets major retailers and marketplaces, including, but not limited to, Amazon, BestBuy, Costco, eBay, Rakuten, and Wayfair.

The threat actor has been using a popular website template with nearly 9,000 sales, available for purchase publicly on Envato, to build its retail phishing sites. These sites feature dozens to hundreds of products that appear to have been scraped from other sites. Searching the exact title of products in popular search engines exposed additional websites in the threat actor's network.

The threat actor appears to be primarily conducting its phishing activity over chat services integrated into the websites, with some sites not having working checkout systems. Based on some sensitive details acquired when testing the phishing process, our team can confirm this threat actor has financial ties to India.

As the Silent Push Threat Analyst Team dug deeper into the activities of the AIZ retail phishing network, we discovered the threat actor is also targeting crypto audiences. We researched reused metadata to find a huge pool of crypto phishing sites targeting Binance, Kraken, and a variety of other generic crypto brands.

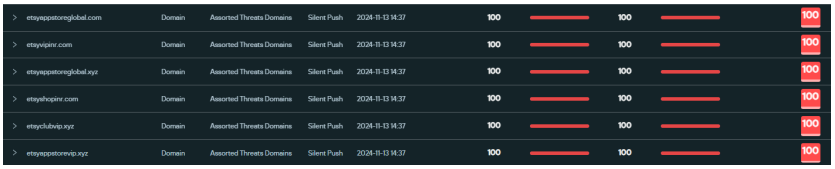
After completing our initial research and starting the process of alerting impacted organizations, we requested a takedown of some domains hosted on Stark Industries (AS44477). Within half an hour, Stark had not only taken down the offending host but was also able to connect the account that had registered that IP to 34 other IPs, some of which hosted similar retail phishing websites but also several new groupings of crypto phishing websites. This Stark lead also allowed us to pivot into even more of their infrastructure.

Targeted brands include:

- Etsy
- Allegro
- AliExpress
- Amazon
- ASOS
- BestBuy
- eBay
- Costco
- Flipkart
- Rakuten
- Shopee
- Temu
- TikTok
- Wayfair
- Wish

Initial Intelligence Gathering

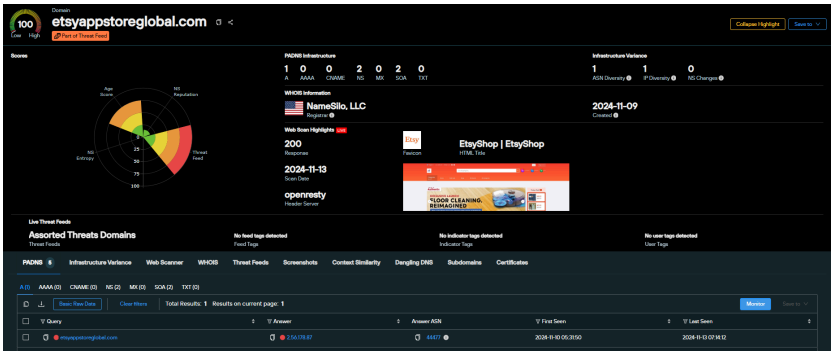
While reviewing recently registered domains, Silent Push Threat Analysts found a few appearing to impersonate the official Etsy store, a popular e-commerce company that specializes in the sale of handmade/vintage goods and craft supplies.



Etsy impersonations registered in early November 2024

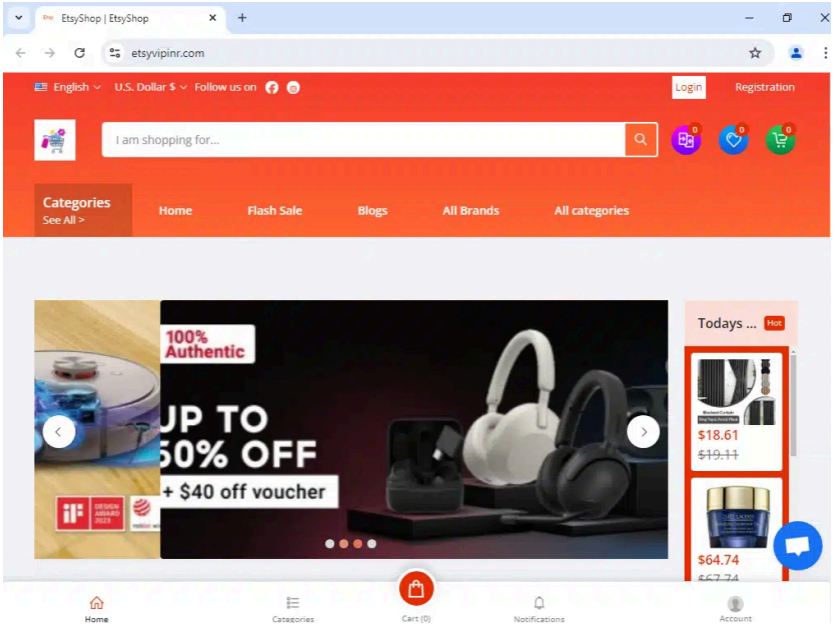
We found a short list of six domains, all targeting Etsy:

- etsyappstoreglobal[.].com (live page – 13Nov)
- etsyappstoreglobal[.]xyz (live page – 13Nov)
- etsyshopinr[.]com (live page – 13Nov)
- etsyvipinr[.]com (live page – 13Nov)
- etsyclubvip[.]xyz
- etsyappstorevip[.]xyz

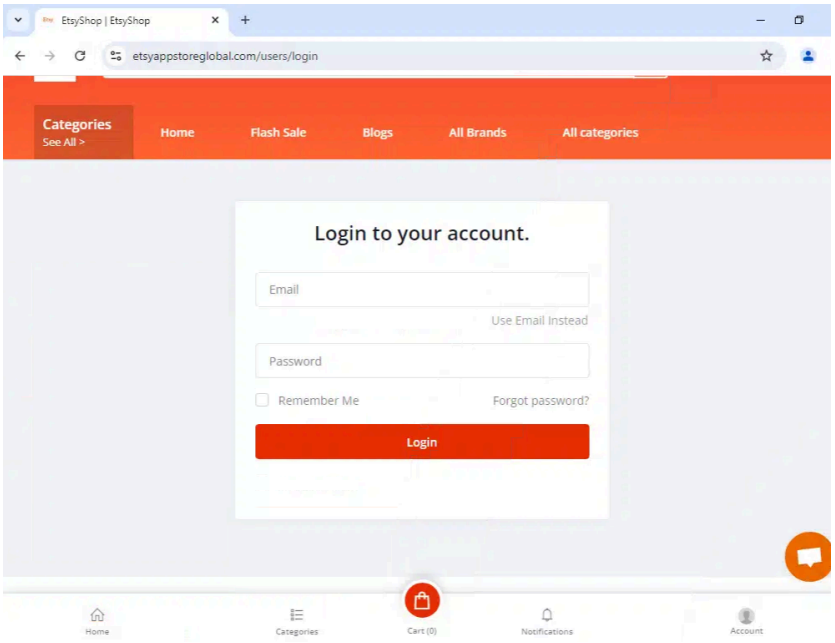


The Silent Push app found a live site, etsyappstoreglobal[.]com, targeting Etsy

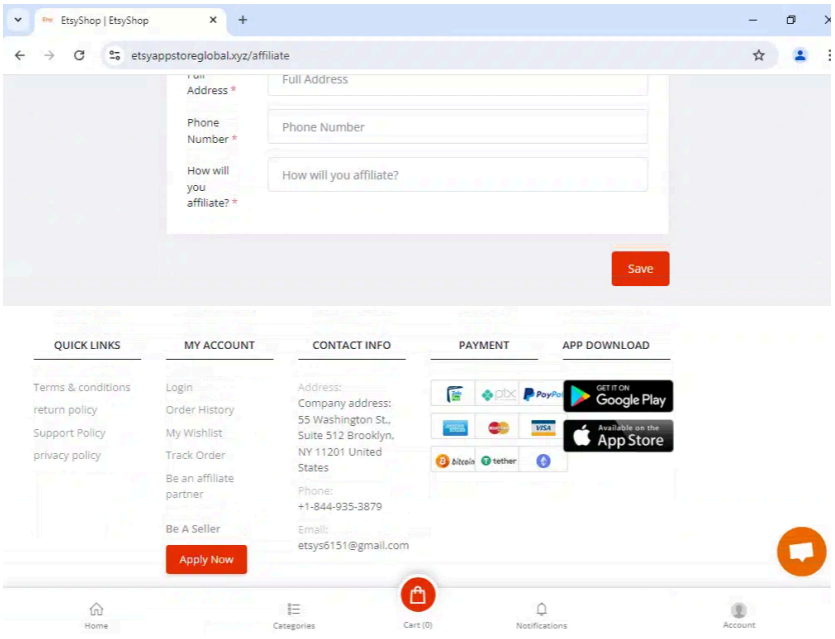
The six domains appearing to target Etsy were mapped to 2.56.178[.]87 – and four live sites all utilize the same theme:



Live site: etsyvipinr[.]com, targeting Etsy



Live site: etsyappstoreglobal[.]com, targeting Etsy



Live site: etsyappstoreglobal[.]xyz, targeting Etsy

Expanding Beyond “Etsy” Sites into Other Brands

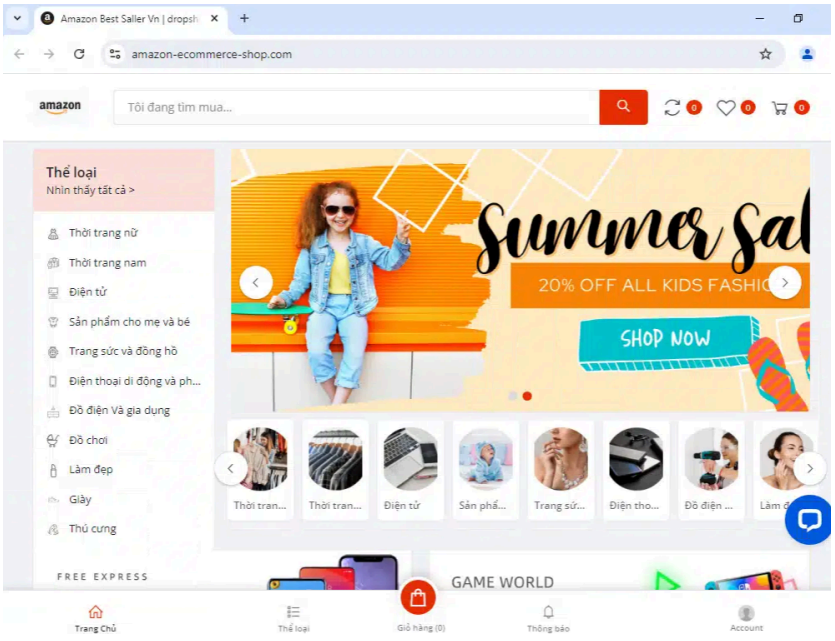
While doing the initial investigation, Silent Push Threat Analysts realized the Etsy-targeted sites all shared a website theme and some common code. We began to look for potential pivots.

Targeting Multiple Retailers

We experimented with our research by performing Silent Push Web Scanner queries on Amazon, BestBuy, and eBay in the following examples:

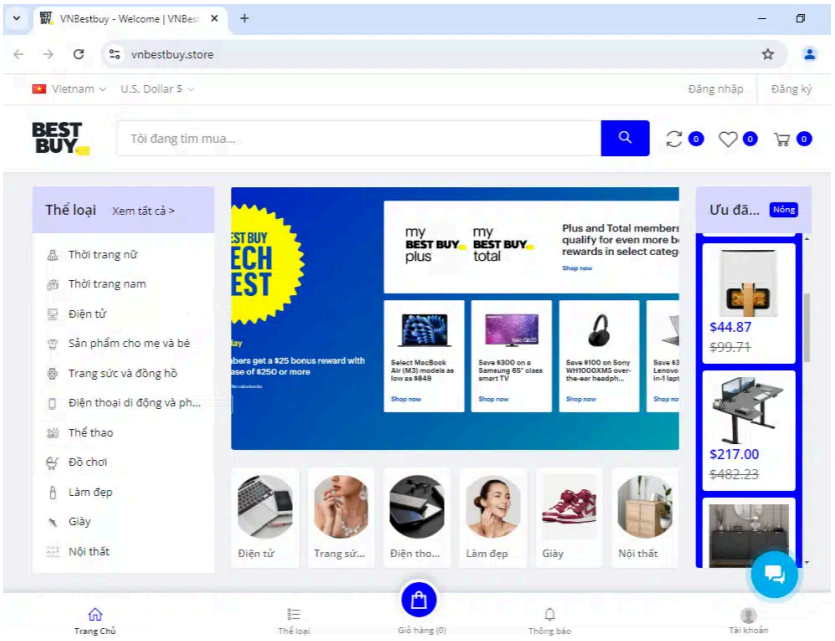
Amazon:

amazon-ecommerce-shop[.]com



amazon-ecommerce-shop[.]com

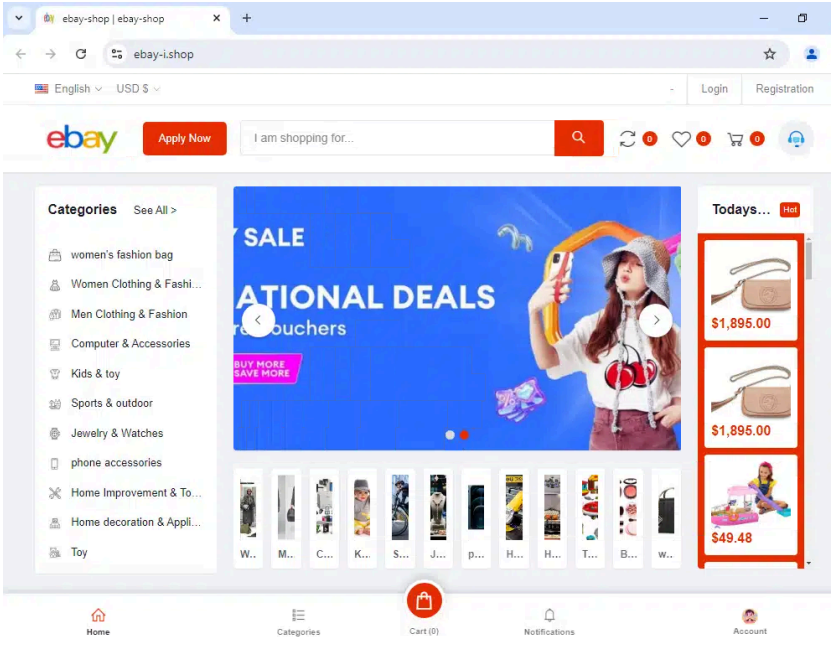
BestBuy:



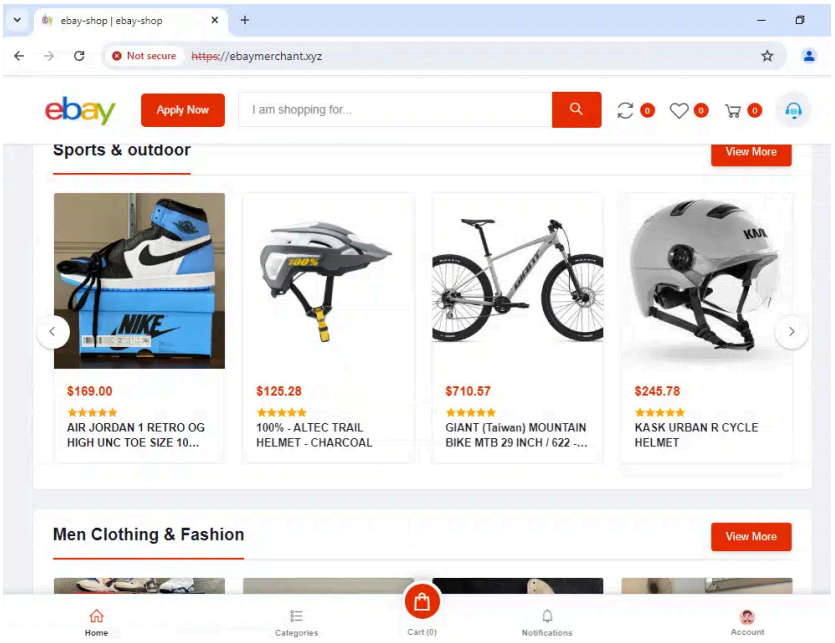
vnbestbuy[.]store

---

eBay:



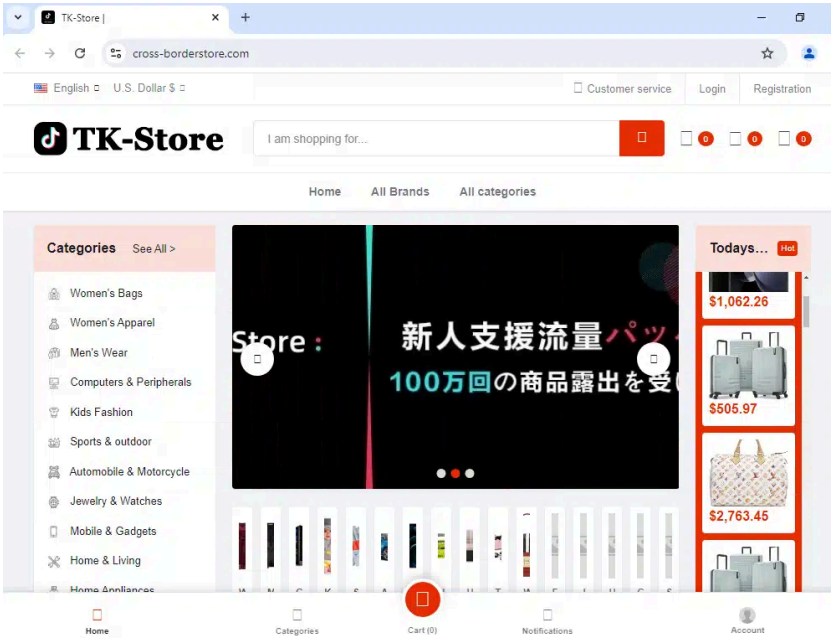
ebay-i[.]shop



ebaymerchant[.]xyz

Searching 1,300 Brand Names

After spot-checking approximately 1,300 brands, starting with Etsy and then searching Amazon, BestBuy, eBay, and many more, we gathered a list of true positive hits in this phishing network, including but not limited to Etsy, Allegro, AliExpress, Amazon, ASOS, BestBuy, eBay, Costco, Flipkart, Rakuten, Shopee, Temu, TikTok, Wayfair, and Wish.

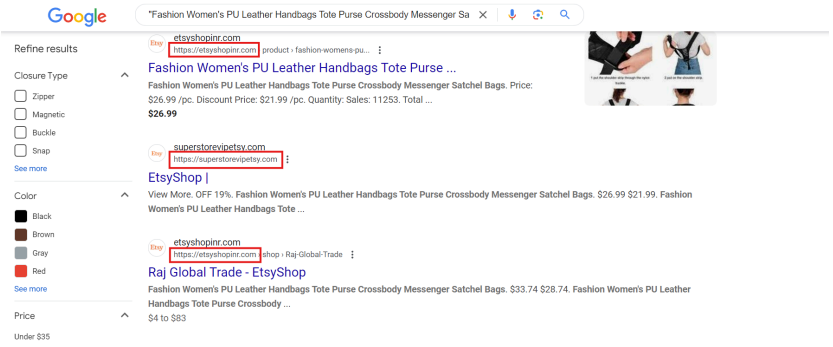


cross-borderstore[.]com – TK-Store (TikTok store)

Amateur Monetization Efforts Across the "Aggressive Inventory Zombies" Network – Phishing Chats with Out-of-Office Sellers

The threat actor's malicious websites feature products that appear to have been scraped from other sites. Searching for the exact title of products in popular search engines exposes more websites in the network. These websites feature dozens (to hundreds) of products that could show up on specific search results.

One example is a Google shopping search for the term "Fashion Women's PU Leather Handbags Tote Purse Crossbody Messenger Satchel Bags" that results in:



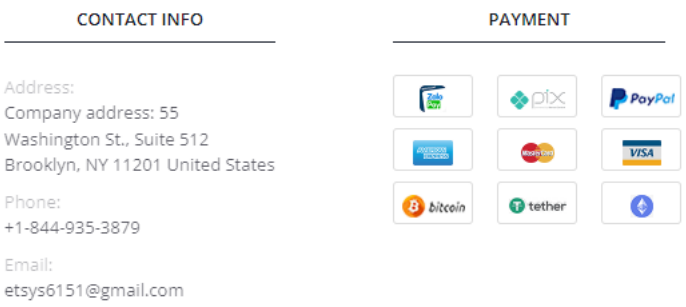
Search for "Fashion Women's PU Leather Handbags Tote Purse Crossbody Messenger Satchel Bags"

The "Contact Info" on the Etsy sites includes a real Etsy phone number but a fake email address such as "etsys6151@gmail[.]com."

Additional emails used by this network include:

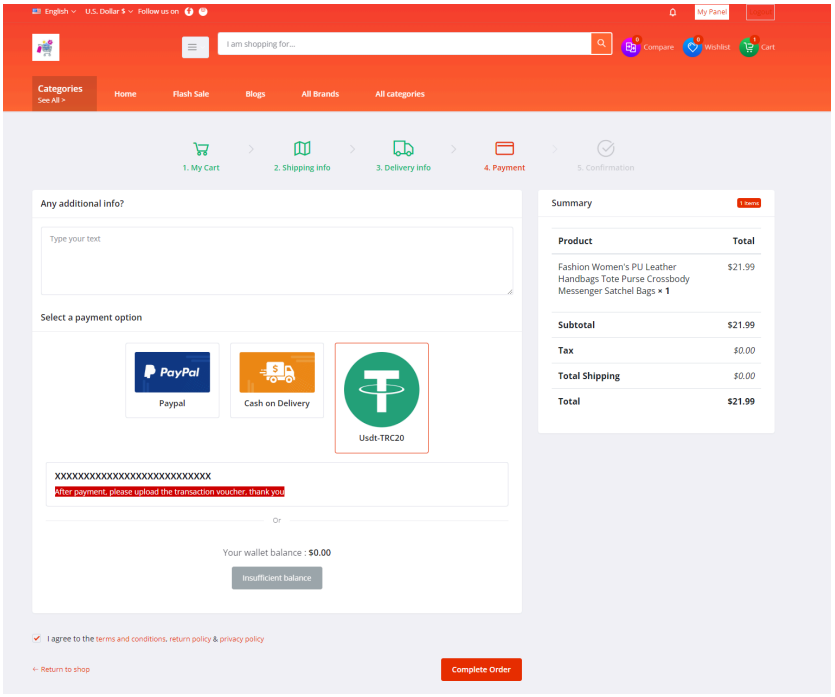
- cskhEbay8686@gmail[.]com
- miravia88888@gmail[.]com
- aisellemall@gmail[.]com

Payment methods on the sites include crypto and methods of payment not accepted at Etsy:



Methods of payment are not those actually accepted by Etsy

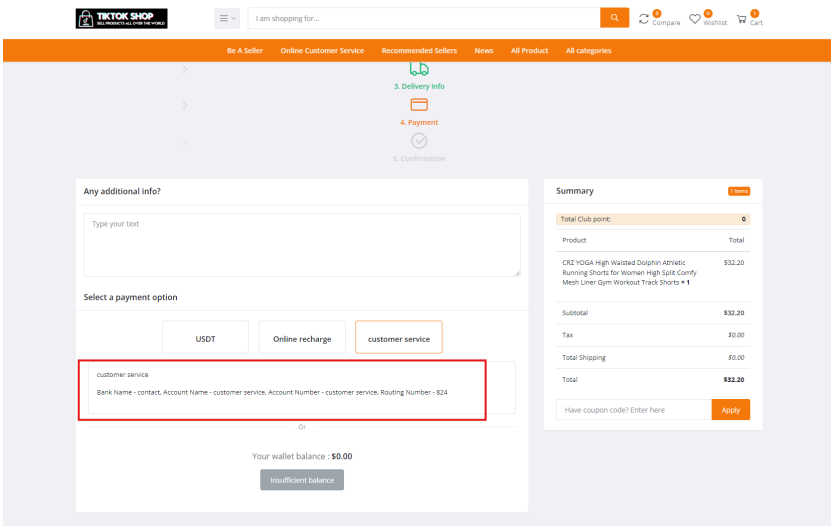
On some sites in the network, navigating to a product and then adding it to the cart starts the purchase process, which leads to a checkout page with three payment options: PayPal, "Cash on Delivery," or Tether/(USDT) cryptocurrency:



Purchase checkout flow on etsyappstoreglobal[.]com

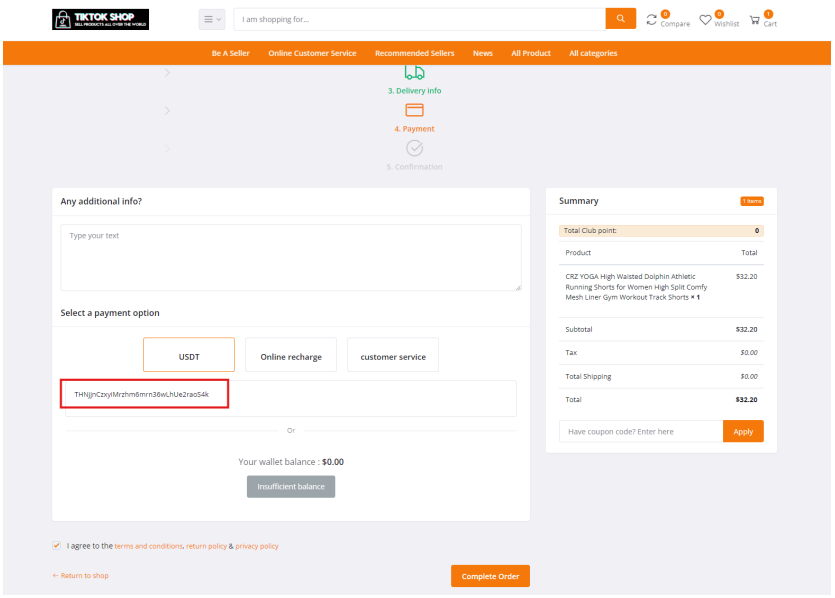
When attempting to test this purchase flow on **etsyappstoreglobal[.]com**, the PayPal option wasn't available, the "Cash on Delivery" option provided no details, and the Tether option didn't have a wallet ID to send the money. The website was using a chat widget from crisp[.]chat, a French company founded in 2015.

When we reviewed another store in the network, **ai-tiktok[.]top**, we uncovered different purchase options. The "Customer Service" option includes what appears to be an effort to obtain a bank account number and routing details—essentially a checking account phishing effort.



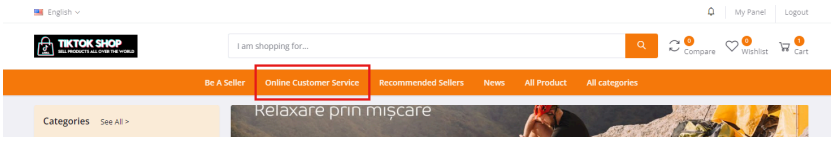
ai-tiktok[.]top checkout page with a checking account phishing effort

The same site, **ai-tiktok[.]top**, has an option for "USDT" (Tether) that appears to have a wallet address of "THNjjnCzxyiMrzhm6mrn36wLhUe2raoS4k" which appears to be a wallet containing only about $30. It's unclear if this is the real threat actor's wallet or if a generic one was embedded here.



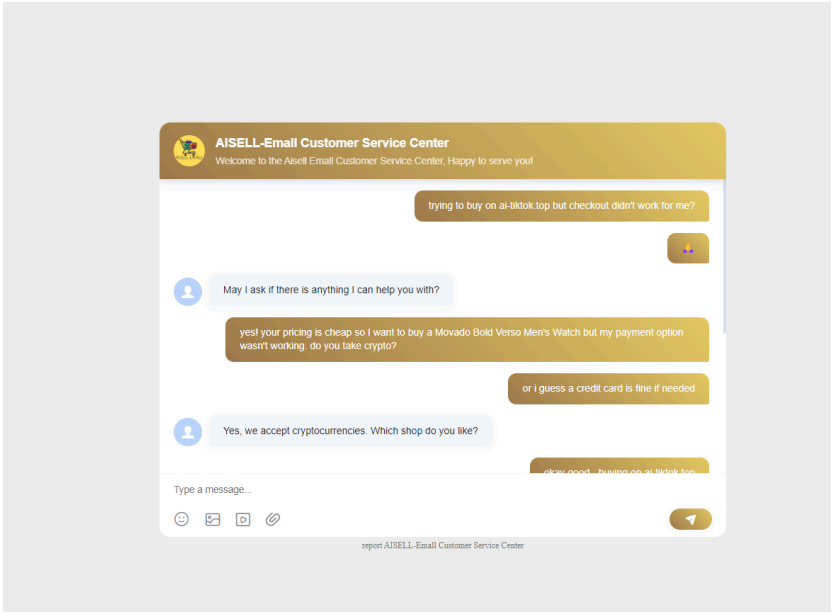
ai-tiktok[.]top checkout page

The menu bar on this **ai-tiktok[.]top** TikTok site features a prominent “Online Customer Service” link that redirects to **chat.ssrchat[.]com/service** and a unique chat session ID.

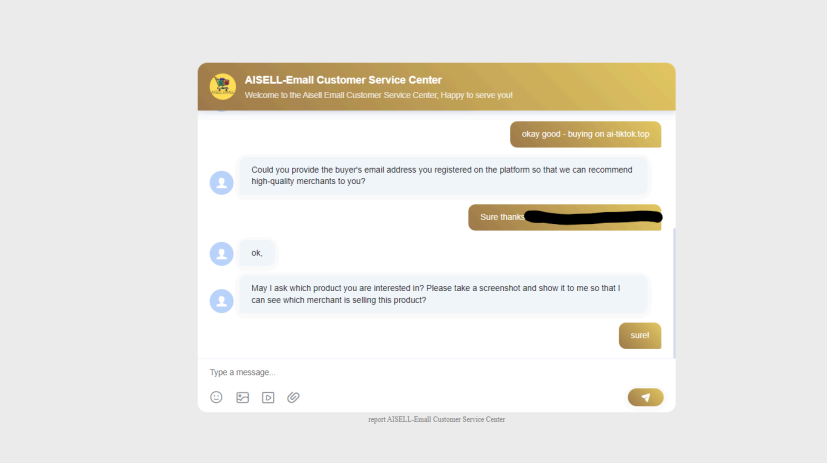


Online Customer Service tab highlighted on ai-tiktok[.]top

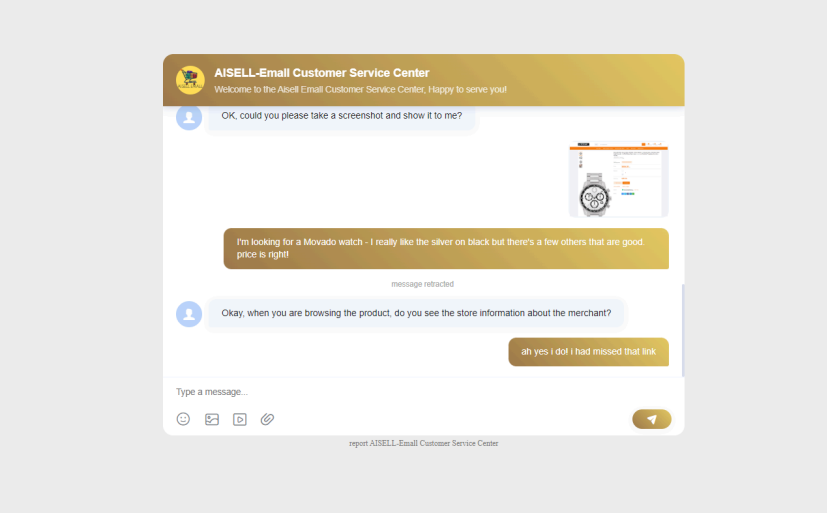
On the TikTok Shop **ai-tiktok[.]top**, the site’s “Online Customer Service” redirected our researchers to **chat.ssrchat[.]com/service**, and this is where customer support finally chimed in:



Chat via chat.ssrchat[.]com

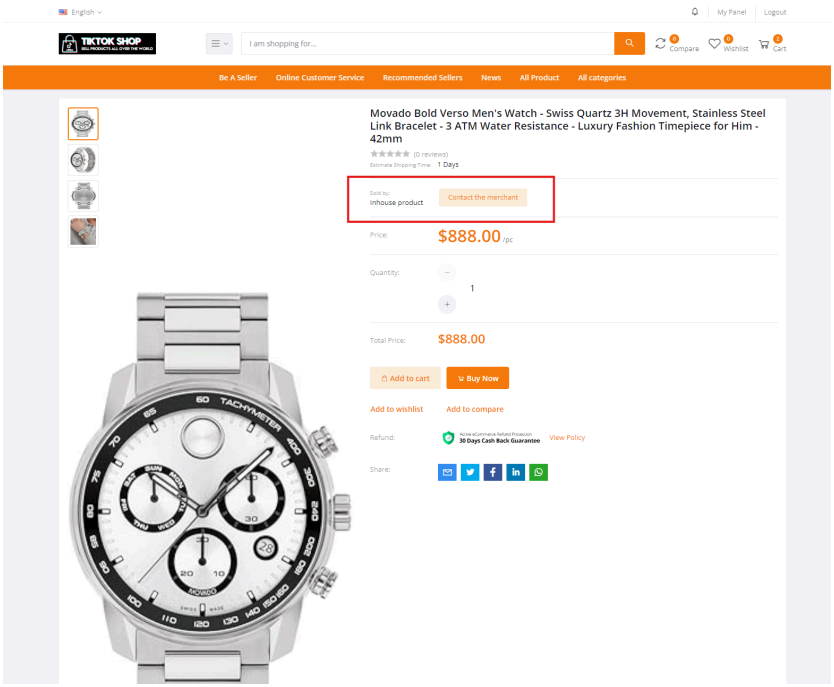


Chat via chat.ssrchat[.]com (continued)



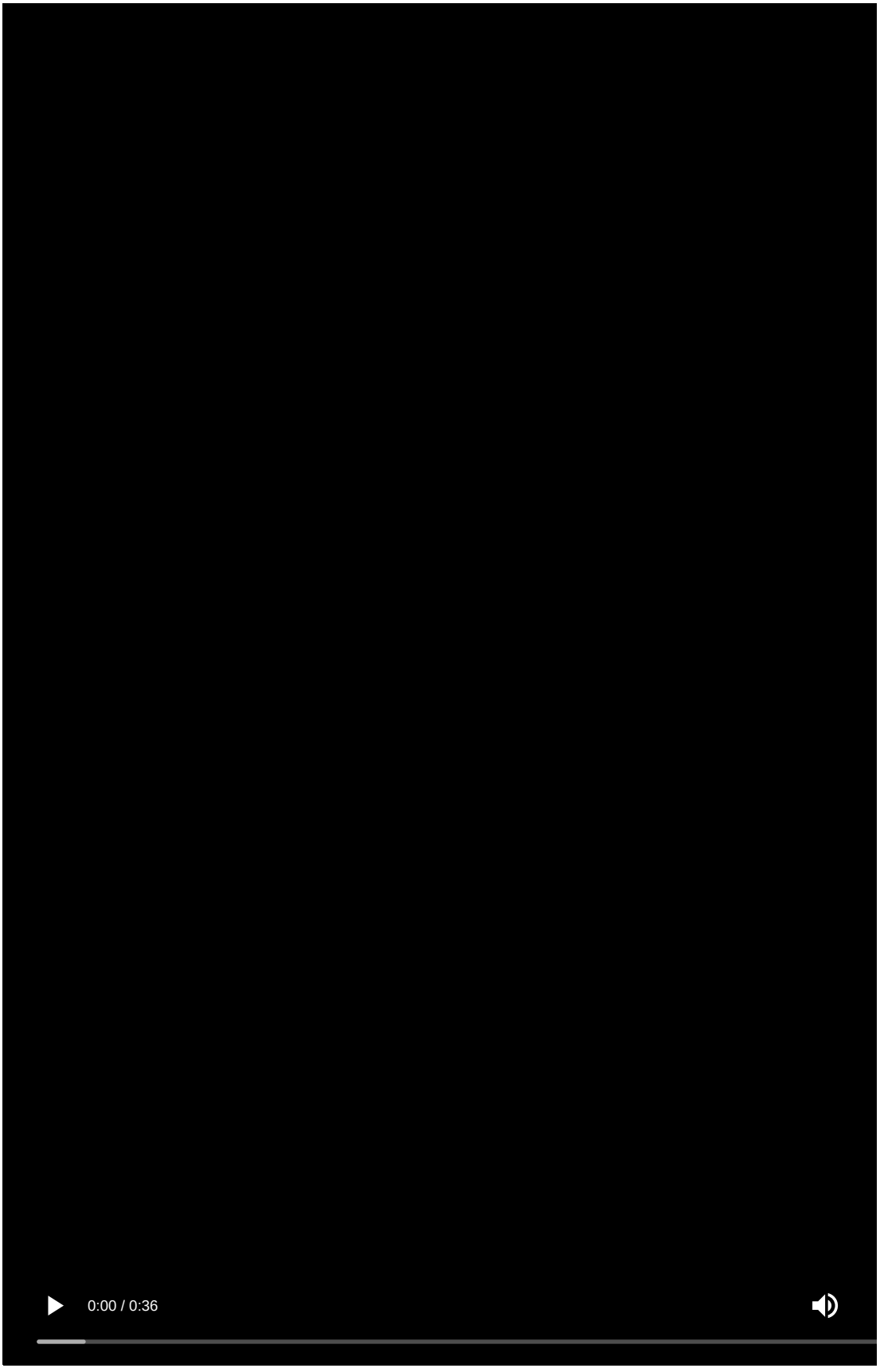
Chat via chat.ssrchat[.]com (continued)

The support staff asked us, “When you are browsing the product, do you see the store information about the merchant?” This was alluding to a subtle “Contact the Merchant” link that can be easily overlooked:



“Contact Merchant” link on ai-tiktok[.]top

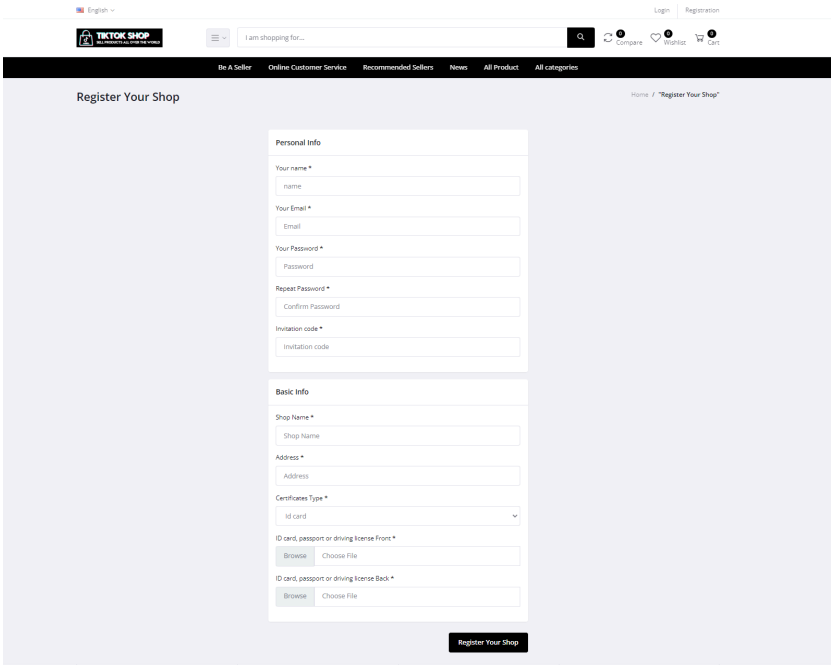
Clicking the "**Contact the merchant**" button opens a chat widget to communicate with the "seller account" – as seen in this short video (*click the "Play" icon in the lower left corner to view*):



ai-tiktok[.]top features a video on how to "Contact the Merchant"

While hosting a seemingly inefficient phishing process on at least some of the websites, this network seems to operate like a common e-commerce phishing network.

On this same TikTok site, the option to "**Register Your Shop**" includes a request for the front/back of an ID card, which could be part of an effort to acquire credentials:



"Register Your Shop" option on ai-tiktok[.]top

Customer Support on Malicious TikTok Shop via Chinese Chat Tool

The menu bar on the **ai-tiktok[.]top** TikTok site features a prominent "Online Customer Service" link that redirects to **chat.ssrchat[.]com/service** and a unique chat session ID.

In this support portal, the threat actors communicated with website visitors, directing them on how to continue (in the scam).

Whenever Silent Push Analysts find a service like this, we always work to confirm whether the threat actors have built a customer support tool or if they are using a third-party resource.

After a brief investigation, our analysts confirmed **ssrchat[.]com** is a Chinese customer support tool called "SaleSmartly."

ssrchat[.]com is a Chinese customer support tool called "SaleSmartly"

The **ssrchat[.]com** website lists numerous Chinese companies using the platform, which appears to be a popular choice for certain Chinese organizations. In the footer of the website is a Chinese ID known as an "ICP license"—this "Internet Content Provider license" is required for most Chinese businesses on the mainland that send data through the Great Firewall.

The ICP license number for ssrchat[.]com is listed in their footer as "**20046039**":

ssrchat[.]com ICP license

To learn about vendors this network is using, we used the Silent Push Web Scanner to find other organizations with the same ICP license number.

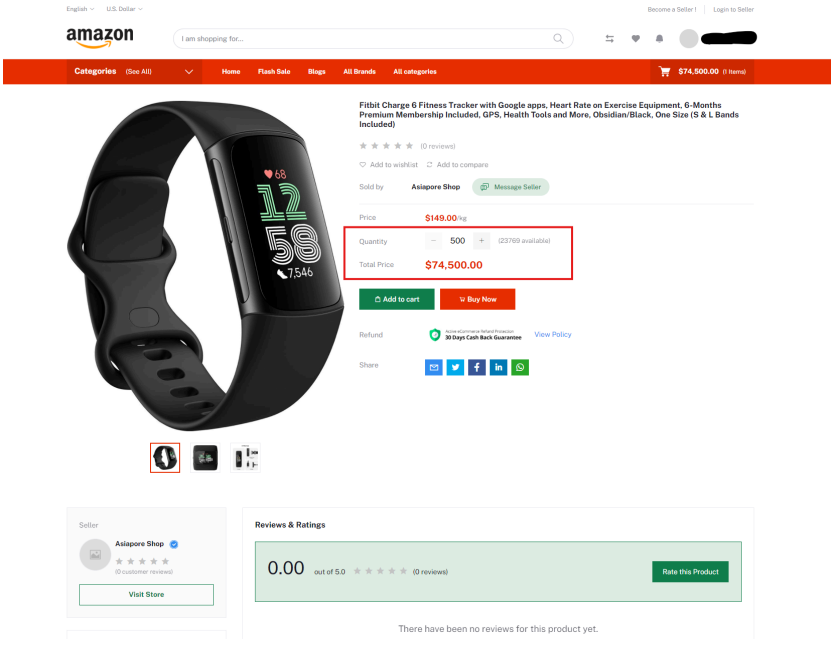
We found 21 unique hosts with matching data. The results include one domain standard-software[.]cn, that claims to own SaleSmartly and several other products, including adspower[.]net.

It appears the threat actor creating countless e-commerce phishing sites is using a Chinese “chat widget” product from a company with a product called AdsPower, which is a browser for ban evasion and managing multiple social media accounts.

We could spend time requesting takedowns of these likely phishing accounts abusing the ssrchat[.]com service, but knowing more about the parent company and confirming they don’t have any clear way to report abuse helps us save time. We changed our focus from takedown efforts to hosts, registrars, and third-party products being used that are more likely to support takedowns.

Bulk Pricing on Product Phishing Sites – Potential Business Targeting

Across this network, there are some sites spoofing Amazon, such as **amazonprime[.]id**, designed to offer products only via bulk purchase with a minimum of 500 units, so the minimum purchase price is nearly $75,000 – this could be a mistake and potential way to find more of their sites:



Example of bulk product purchase requirements on amazonprime[.]id

AIZ Websites Heavily Featuring “Live Chat” Widgets for Phishing

While analyzing the initial pools of domains, along with additional domains found via the pivots below, it’s clear this network heavily uses “Live Chat” widgets. Most of the sites appear to use “Message Seller” and “Contact the Merchant”

links on product pages, and many of them also have additional chat widgets from third-party companies embedded into the pages.

Outside of the sites using the Chinese chat widget from SaleSmartly, many appear to be using “Crisp” chat from **crisp[.]chat**.

Another grouping of sites from this network, like **wayfairmy[.]cc**, which targets Wayfair, uses **livechat[.]com**.

Our team reached out to Crisp Chat and Live Chat to share details and encourage them to investigate and potentially ban these clients.

Within hours of our report, Crisp Chat significantly escalated the research, banned the client, and took additional steps to look for any other sites where the threat actors were using their service. Our team at Silent Push thanks the Crisp Chat team for their prompt and serious response.

We are still waiting for feedback from Live Chat and will update the report if/when it arrives.

Stark Industries / PQ Hosting Takedown Uncovers More Infrastructure from this Threat Actor

As part of the Silent Push commitment to collaborating with hosts, our team sent an initial lead to Stark Industries (stark-industries[.]solutions) about one of the IPs in this network hosting these domains, which was registered through the Stark Industries service.

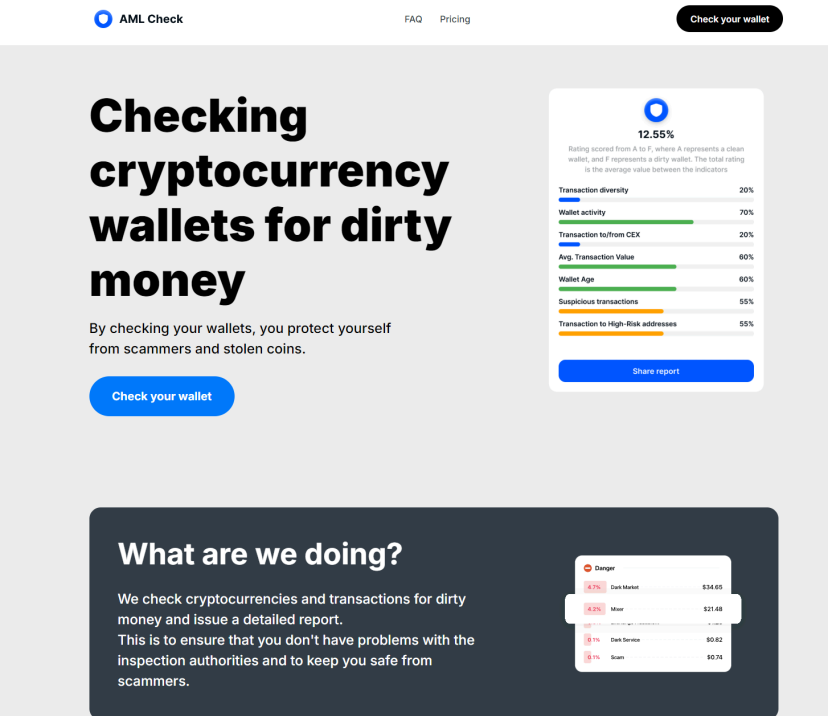
Our initial IP shared with Stark Industries was taken down in less than half an hour, and they were able to conduct an investigation and take down even more infrastructure associated with this same account and threat actor – sending us a total of 34 new IPs, which provided deeper insight into the AIZ threat actor infrastructure.

“AML Check” Cryptocurrency Phishing from AIZ Threat Actor

Through our reporting process to web host Stark Industries, we were given an IP used by this threat actor, **45.144.30[.]184,** to which the domain mapped to **aml-check-wallet[.]com**.

Performing a Web Scanner query confirmed that this domain used consistent metadata, which allowed us to pivot into several dozen other domains/hosts with the same content as the original source.

The cryptocurrency phishing sites in this network look like the example below:



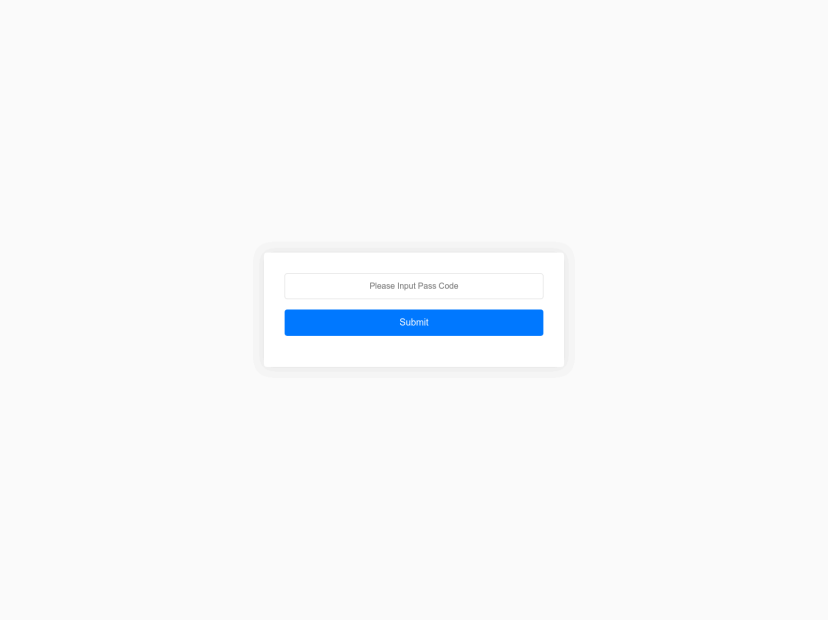
Example of cryptocurrency phishing sites in this network: amlguards[.]com

---

“Input Pass Code” Phishing Sites

One of the IP ranges shared by Stark Industries included **45.144.31[.]235** which has an odd grouping of sites hosted on it – several have the classic “shopping” structure like vipmydealshopgo[.]xyz, but others such as store-joo[.]org, group-joo[.]org,

and global-joom[.]org have hosted pages that may have led to unique phishing or pig-butchering experiences. One site had a "Please Input Pass Code" message, which raises questions about the purpose of these sites:

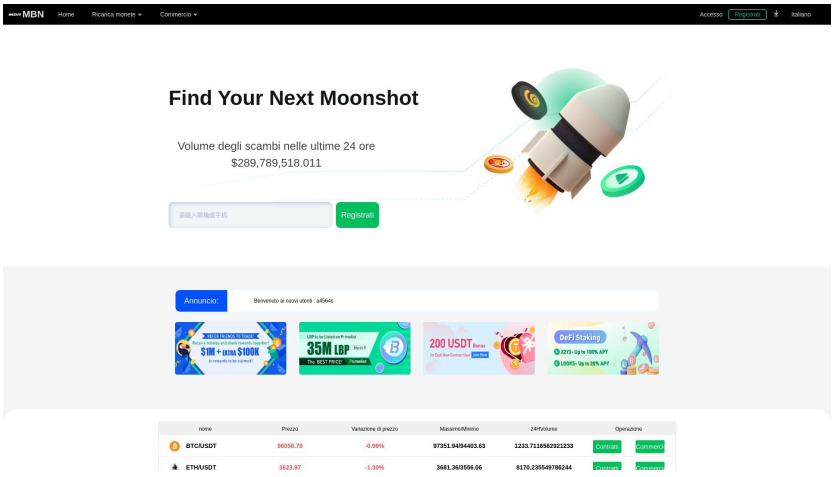


One site, group-joo[.]org displayed a "Please Input Pass Code" message

"MBN" Crypto Phishing Sites

One of the IPs shared by Stark Industries that this threat actor was using briefly hosted a site, "haiwaidemosite[.]com," with the HTML title "MBN" in October 2024.

A huge pool of these crypto phishing sites can be found via reused metadata on the sites – targeting Binance, Kraken, and a variety of other generic crypto brands.

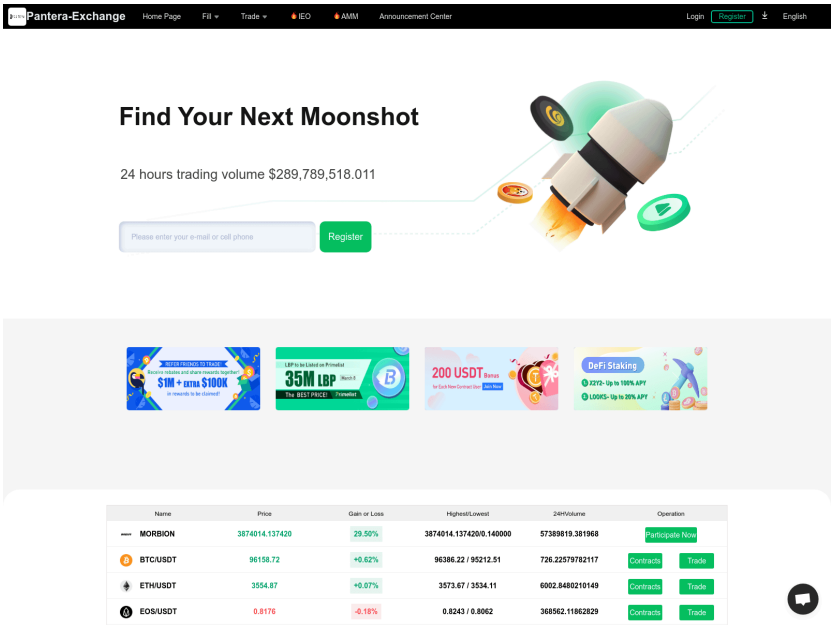


Example site in the network: exchangeaaa[.]xyz

Pantera Exchange Crypto Phishing Campaign

On an IP shared with us by Stark Industries, there are domains such as "**pantera-exchange[.]com**" with the HTML title "**Pantera-Exchange**."

These sites look nearly identical to the "MBN" phishing sites, and there are hundreds of unique results with the same metadata targeting crypto audiences:



Another example of a nearly-identical site in the phishing network: pammvip[.]com

---

“Exness” Crypto Phishing

From another IP shared by Stark Industries, we can pivot into a small grouping of domains, such as **klo-ok[.]cc**.

This website had similar metadata to other new sites in the network, and by creating a proprietary query, we can pivot into about a dozen unique hosts. The results include an IP that has a live “crypto investment” website in Mandarin, albeit with somewhat broken functionality.

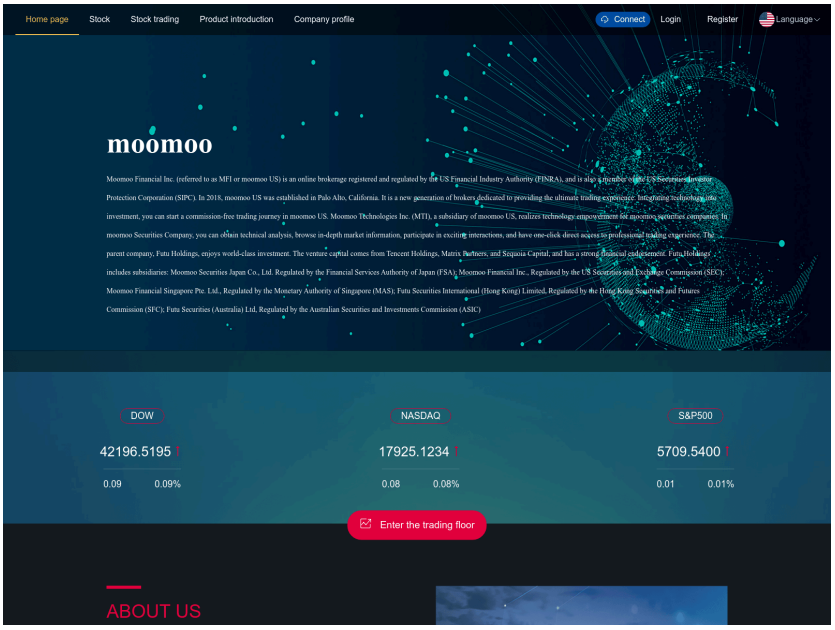
This IP has a live “crypto investment” website in Mandarin

“Moomoo Financial” Phishing Campaign

Another IP shared by Stark Industries used by this threat actor is connected to a grouping of websites that look similar, including:

- m2stock[.]net
- mioiocapitald[.]com
- moomoccapital[.]com

While these sites now all appear to be down, at one point, they looked like this example:



The sites looked similar to msostock[.]net in the phishing network

---

Aliexpress Targeting Pivots into Larger Retail Phishing

Another IP taken down by Stark used by this threat actor is connected to domains like **spsailexpsess[.]com**, which appear to be targeting Aliexpress.

This site has unique indicators, resulting in hundreds of additional retail phishing sites being discovered.

Bitcoin Targeting Pivots into Larger Crypto Phishing Campaign

One IP taken down and shared by Stark connects to a pool of websites targeting Bitcoin and other crypto tokens – likely for a phishing or pig-butchering scam.

These sites include:

- bitcoin-contract[.]vip
- coinworld-online-exchange[.]cc

Like many of this threat actor's websites and campaigns, the site templates are unique and are being reused across the sites. As a result, we can find hundreds of crypto phishing efforts targeting major brands and what appears to be made up of crypto brands via this template.

Continuing to Track the AIZ Retail and Crypto Phishing Campaigns

Silent Push threat researchers will continue to observe and monitor changes to this actor's infrastructure. New discoveries and TTP changes will be immediately reflected in our feeds.

We will also continue to share our research on threats like this with law enforcement. If you have any tips about this threat actor or other kinds of retail and crypto phishing scams, please consider sharing those details with our team.

Additional information

We're continuing to track the **AIZ Retail & Crypto Phishing Network's** activity and will report our findings to the security community in a series of follow-up reports.

We've also published a **TLP: Amber report** for Enterprise users that contains links to the specific queries we've used to identify and traverse the **AIZ Retail & Crypto Phishing Network**—including proprietary queries that we've omitted from this blog for operational security reasons.

Mitigation

Silent Push believes all **AIZ Retail & Crypto Phishing Network** domains offer some level of risk.

Our analysts have constructed a Silent Push IOFA Feed that provides a partial list of **AIZ Retail & Crypto Phishing Networks** Indicators of Future Attack domains focused on their scams, along with an IOFA Feed containing suspect **AIZ Retail & Crypto Phishing Network** IPs.

Silent Push IOFA Feeds are available as part of an Enterprise subscription. Enterprise users can ingest IOFA Feed data into their security stack to inform their detection protocols or use it to pivot across attacker infrastructure using the Silent Push Console and Feed Analytics screen.

Silent Push Community Edition is a free threat-hunting and cyber defense platform featuring a range of advanced offensive and defensive lookups, web content queries, and enriched data types.

Click **here** to sign up for a free account.

Indicators of Future Attacks (IOFAs)

Here is a sample list of **AIZ Retail & Crypto Phishing Network** IOFAs – our full list is available for enterprise users. Silent Push Enterprise clients have access to a domain and IP feed containing the AIZ Retail & Crypto Phishing Networks' infrastructure:

- adspower[.]net
- ai-tiktok[.]top
- amazon-ecommerce-shop[.]com
- amazonprime[.]id
- aml-check-wallet[.]com
- amlguards[.]com
- appstoreetsy[.]vip
- bitcoin-contract[.]vip
- chillivipstore[.]com
- coinworld-online-exchange[.]cc
- crisp[.]chat
- cross-borderstore[.]com
- ebay-i[.]shop
- ebaymerchant[.]xyz
- e-box[.]vip
- etsy[.]one
- etsyappstoreglobal[.]com
- etsystore[.]org
- etsyme[.]com
- etsyoou[.]icu
- etsyvipclub[.]xyz
- exchangeaaa[.]xyz
- global-joom[.]org
- group-joo[.]org
- haiwaidemosite[.]com
- haiwaisite666[.]com
- inretsyvipclubapp[.]com
- jd-shopvnvip[.]top
- jngfhjiu56u7[.]top
- klo-ok[.]cc
- livechat[.]com
- luxury-collection[.]cc
- m2stock[.]net
- mgciscoin[.]co
- midjornieyskilload[.]com
- miravia88888@gmail[.]com
- mkgmailgo[.]com
- moomoccapital[.]com
- msostock[.]net
- officialjunglee[.]com
- ozatchenum[.]com
- pammvip[.]com
- pantera-exchange[.]com
- snaspshopping[.]com
- spsailexpsess[.]com
- ssrchat[.]com

- standard-software[.]cn
- store-joo[.]org
- tik-tokvnshop[.]net
- vipetsyappshop[.]cc
- vnbestbuy[.]store
- wayfairmy[.]cc
- xbtce-exchange[.]xyz
