

Unmasking Task Scams to Prevent Financial Fallout From Fraud

Appendix

Microsoft Office User

This appendix supplements the Unmasking Task Scams to Prevent Financial Fallout From Fraud report that exposes the life cycle and tactics of task scams by presenting real-world cases as well as strategies to help identify and avoid these threats.

Table of contents

- I. The investigated task scam's infrastructure**
 - a. Task scam website
 - b. Domain registrar abused for scams and fraudulent websites
 - i. Domain registrar reputation
- II. The criminal market for scams**
 - a. Actors
 - i. Crime groups
 - ii. Organized crime networks
 - b. Platforms for the proliferation of scams
 - i. Scam services offerings on social media
 - ii. Legitimate messaging and chat applications abused for scams
 - iii. Underground market offerings
- III. The impact of a task scam**
- IV. References**

The investigated task scam's infrastructure

In this section of the appendix, we look more closely at the elements of the scam that we investigated in the main report where we posed as a potential victim. This section provides more information on the website that the scam handler, "Betty," provided. It also discusses the role that domain registrar's play in the proliferation of these fraudulent websites.

Task website

Our research revealed that a fake and malicious Cloverstone website that "Betty" linked to the potential victim was registered on July 5, 2024 using the domain registrar *GNAME.com Pte. Ltd.* We found that the site owners are using WHOIS privacy and the CloudFlare content development network to mask their identity. CloudFlare is a legitimate provider of DDoS (Distributed Denial of Service) security, used in this case to help obfuscate the true server being used to host the scam sites.

There are clear indications that the people behind the malicious site are attempting to impersonate a legitimate company. The design of the site matches that of the legitimate company, Cloverstone Digital LLC. Pivoting on this domain using a fuzzy domain search revealed similarly named domains; while the base domains resolved to CloudFlare DNS, two sub-domains were found to resolve to IP addresses in Hong Kong.

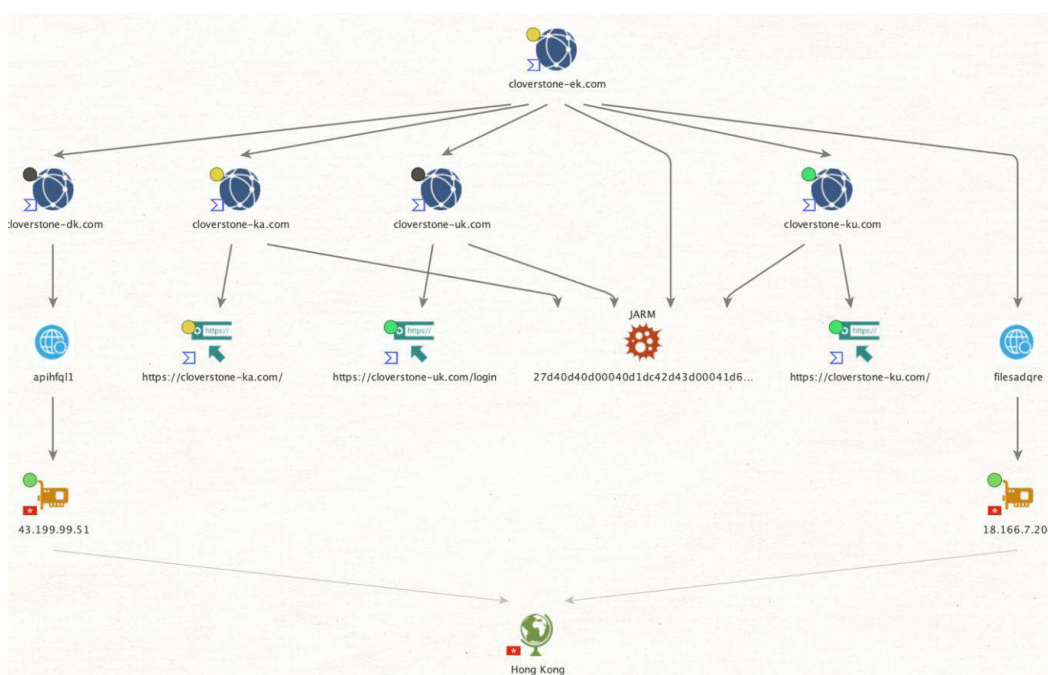


Figure 1. Pivoting to related parts of the scam infrastructure

Pivoting on the IP addresses that didn't belong to the CloudFlare network, it was possible to identify further domains that are possibly previous iterations of the scam and related to the same group. All the domains we have found are also registered with *GNAME.com Pte. Ltd.*, have a similar domain name structure, and impersonate small eCommerce or digital marketing companies. We believe this is likely for believability, but that these organizations are usually without large security teams that monitor for brand impersonation could also be a factor as to why the scammers chose to impersonate them. Table 1 lists the domains we found in our investigation.

IP address	Domain name
43.199.99.51	absolute-pk[.]com
	absolute-ux[.]com
	absolute-th[.]com
	exasol-ck[.]com
	adwordvigilante-ek[.]com
	adwordvigilante-uk[.]com
	adwordvigilante-ck[.]com
18.166.7.204	commer-ci[.]com
	arct-rx[.]com
	ambaum-pk[.]com

Table 1. A list of the domains we found that are related with Gname.com Pte. Ltd.



Figure 2. A screenshot of the fake website impersonating the legitimate company Absolute Digital Media (left) and the scam login (right)



Figure 3. A screenshot of the fake website impersonating the legitimate company Olivine (left) and the scam login (right)

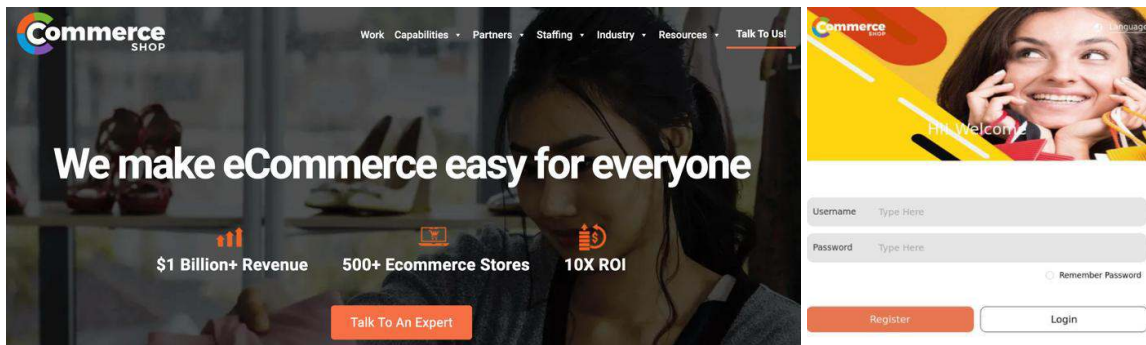


Figure 4. A screenshot of the fake website impersonating the legitimate company Commerce Shop (left) and scam login (right)

We also found a subdomain, *admin.cloverstone-dk[.]com*, which revealed a different login screen. This login panel translates to "Cloverstone management backend system."



Figure 5. A screenshot of the Cloverstone Management Backend System login page. Other campaigns likely have similar sites with the impersonated company used as the scam campaign name.

We found lines in the JavaScript of the scam site that were written in simplified Chinese. Many of these task scam pages contain simplified Chinese in the source code as comments; this suggests the origin of at least a part of the cybercriminal group behind the task scam.

```

window.onload = function () {
  // 阻止双击放大
  var lastTouchEnd = 0
  document.addEventListener("touchstart", function (event) {
    if (event.touches.length > 1) {
      event.preventDefault()
    }
  })
  document.addEventListener(
    "touchend",
    function (event) {
      var now = new Date().getTime()
      if (now - lastTouchEnd <= 300) {
        event.preventDefault()
      }
      lastTouchEnd = now
    },
    false
  )
  // 阻止双指放大
  document.addEventListener("gesturestart", function (event) {
    event.preventDefault()
  })
}

```

Figure 6. Comments showing simplified Chinese

Domain registrars abused for scams and fraudulent sites

It should be noted that domain registrars are not inherently malicious actors, but they can inadvertently attract cybercriminals that seek to carry out phishing attacks, spread malware, and commit fraud. Criminals typically seek out the path of least resistance, and a relaxed posture by registrars when dealing with abuse complaints can be appealing to attackers, which then results in a higher rate of criminality associated with that registrar.

In our research over the past year, we've noticed a surge in gamified job scams, often called, and in this research referred to as task scams, originating from the registrar GNAME. While GNAME is not the sole culprit, it has consistently appeared in our findings. Fraudulent sites registered via GNAME include the numerous domains from the scam campaign impersonating Cloverstone Digital and the other domains that impersonate legitimate companies. We also found that *mac.suoosee[.]com*, the site mentioned in a November 2024 report where a victim said they lost US\$800,000 to a scam as mentioned in the main research is also registered via GNAME. There are also domains associated with the scam group called The Smishing Triad that are registered via GNAME.



Figure 7. A report from Trustpilot of a victim losing US\$800,000 to a task scam

cloverstone-ek.com

Updated 1 second ago

Domain Information

Domain:

cloverstone-ek.com

Registered On:

2024-07-05

Expires On:

2025-07-05

Updated On:

2024-11-12

Status:

client transfer prohibited

Name Servers:

kareem.ns.cloudflare.com
mia.ns.cloudflare.com

Registrar Information

Registrar:

Gname.com Pte. Ltd.

IANA ID:

1923

Abuse Email:

complaint@gname.com

Abuse Phone:

+65.65189986

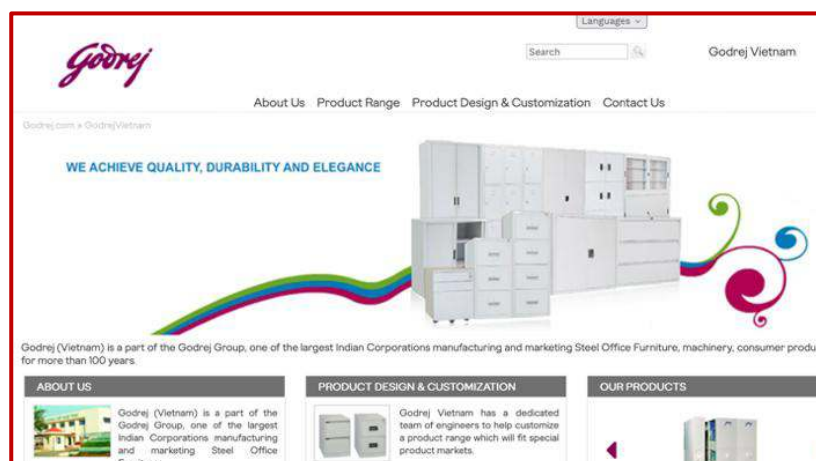
Figure 8. Cloverstone-ek[.]com domain information that shows GNAME as its domain registrar

During our investigation we also uncovered domains registered via GNAME that impersonate legitimate businesses and known trademarks such as Target, Walmart, Meta, Amazon, and other small but known enterprises to deceive victims into sharing personal information and financial data. Some of these fake sites were found in reports from Trustpilot, and in Reddit reviews, as well as in arbitration.

Similar to the scam impersonating Cloverstone Digital, these fake sites sometimes use the real logos of the websites they are impersonating. To make the fake websites more attractive, they post items on sale or at a discount. Our research found one fake supply store selling suits at US\$100, half the price that the legitimate seller being impersonated was selling them. Previous research have mentioned similar fraudulent shops in campaigns dubbed “BogusBazaar” and “Phish ‘n’ Ships,” which also appeared to have China as its main operating hub. Phish ‘n’ Ships dates to at least 2019, with threat actors using simplified Chinese in their internal tools.

We found hundreds of fraudulent websites operating as fake online shops. These sites not only sell counterfeit items but have also been observed to be frequently used to deploy phishing campaigns. The domain names are deliberately chosen to be confusingly like the established trademarks. Many of these fraud shops are built using the WooCommerce plugin for WordPress and use simplified Chinese in the code, which again suggests the origin of the actors behind the scams. However, we also found sites using multiple languages, such as English, German, French, Spanish, and Italian, that offer discounted items.

FAKE



LEGITIMATE

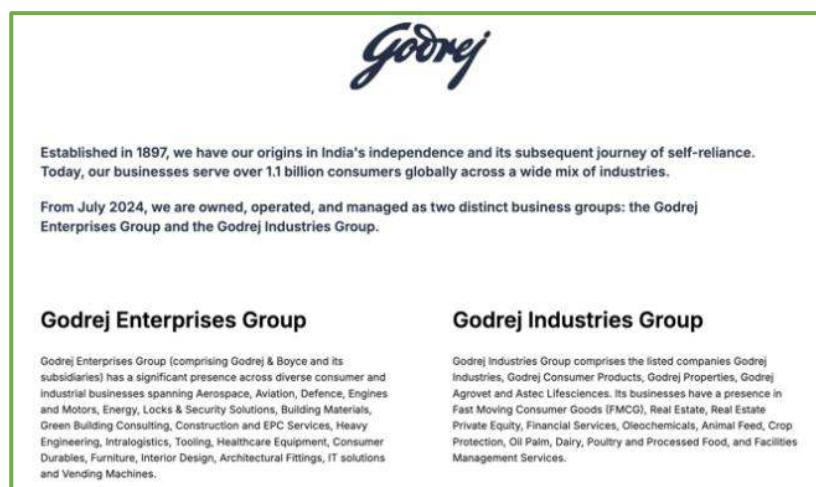


Figure 9. The fake site godrejvietnam[.]com (in red) impersonating the legitimate sitegodrej[.]com (green)

The legitimate business called Godrej is based in Vietnam and has been around since 2005. Godrej specializes in engineering, manufacturing, and dealing with consumer and industrial products/services. The company also filed for a domain dispute using World Intellectual Property Organization (WIPO) against these fraud shops.

FAKE



LEGITIMATE

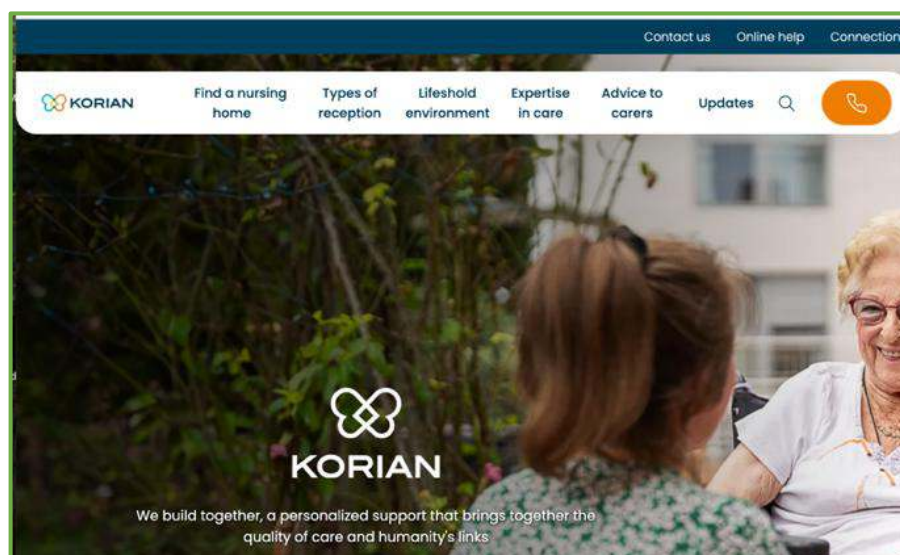
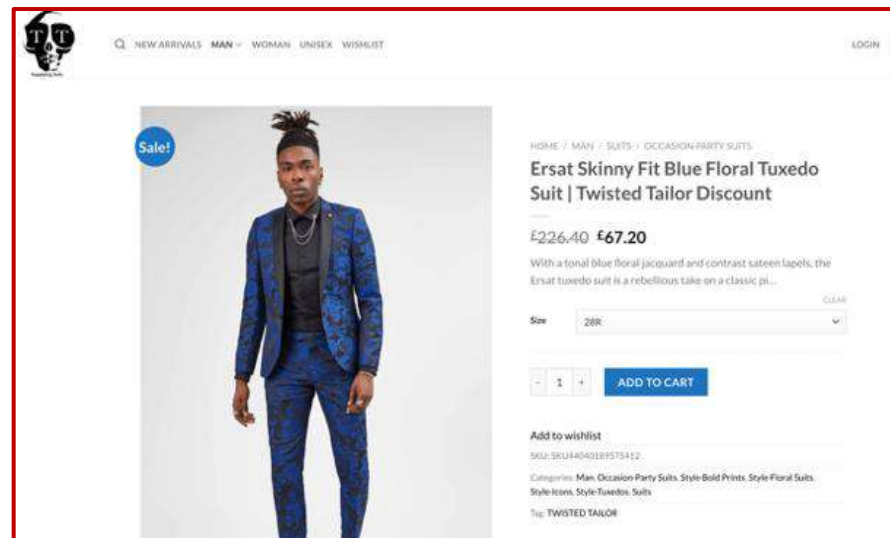


Figure 10. The fake site koriansa[.]com (in red) versus the legitimate site korian[.]fr (green)

Meanwhile, Korian is a French company specializing in nursing home care for the elderly, founded in 2003. The fake scam site currently forwards to a gambling site, but it was previously masquerading as the legitimate Korian brand. In April 2024, several fraudulent phone calls and emails purporting to be from Korian's managers or its staff members were sent inviting private individuals to invest in fake savings or investment products. Some of the domain names used in the fraudulent emails were *korian-sa[.]fr*, *korian-sa[.]com* and *koriansa[.]com*.¹

FAKE



LEGITIMATE

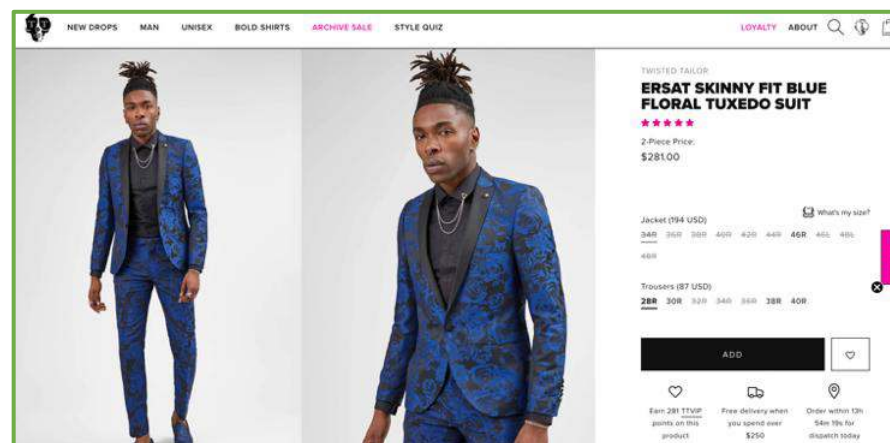


Figure 11. The fake site supplying suits [.]com (in red) versus the legitimate site twistedtailor [.]com (in green)

Twisted Tailor is another legitimate company that scammers have impersonated. It is a textiles company based in the UK and founded in 2016 that designs and manufactures a broad range of apparel and accessories for men and women. The fake website version, under the name Supplying Suits, added this fake name to the bottom of the legitimate company's logo. Prices in the fake site are significantly lower than those on the real site. The shipping page on Supplying Suits "sample page" at the top, along with the description of items that are eligible for a return, mentions CD, DVD, and VHS. The incomplete pages and inaccurate information and text shows sloppy work on the end of the cybercriminal group's website designer. A phishing campaign around December 2024 was deployed with Supplying Suits used as the domain.

Domain registrar reputation

GNAME's involvement in hosting domains used for phishing attacks and task scams, along with its slow response to complaints about scam sites, raises concerns about its role in attracting criminal activity. GNAME is a Singapore-based international domain name registrar. The primary accreditation was originally Chinese, in the name of Beijing Huaqi Weiye Technology Co. and doing business at *iwanshang [.]cn*, before it moved to a Singaporean company called GNAME. As of May 2025, GNAME had 501 ICANN registrar accreditations.

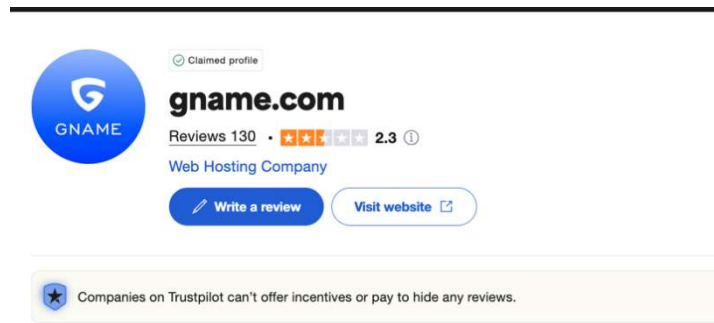


Figure 12. Trustpilot reviews for GNAME

As of May 2025, GNAME was rated at 2.3 out of 5 with 130 reviews on Trustpilot. 79% of the reviews are one-star ratings with many of the complaints being about fraudulent sites and brand impersonation.

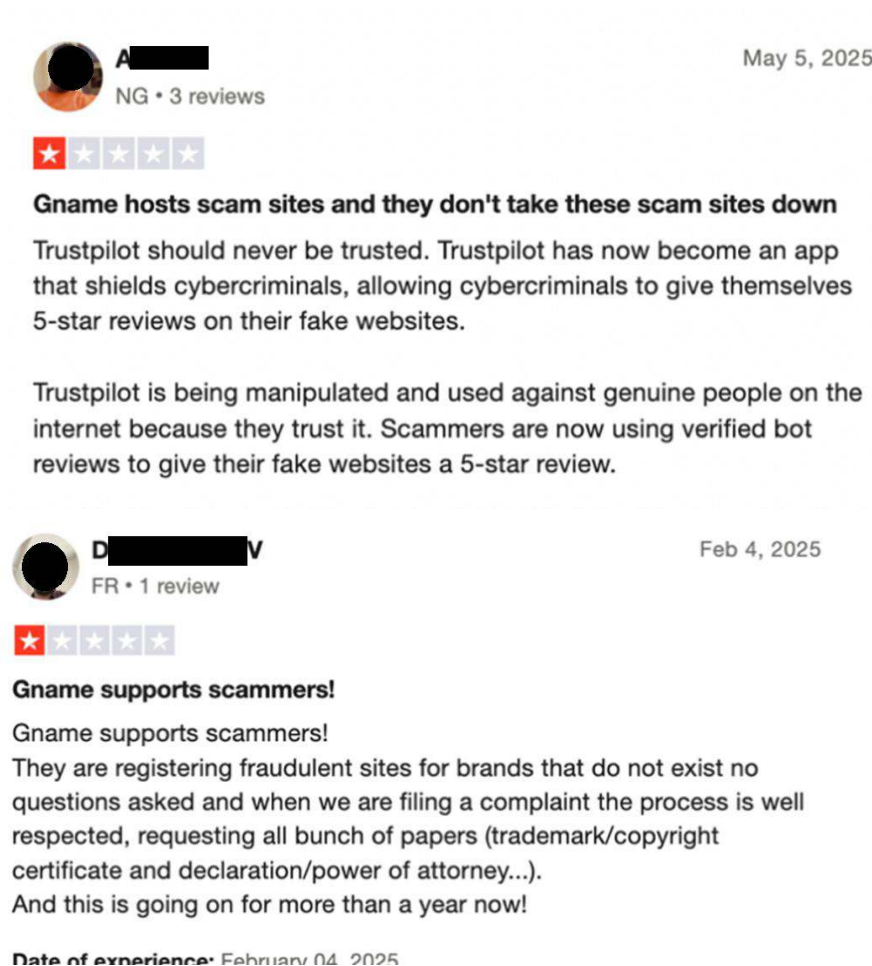




Figure 13. Screenshots of a few of the Trustpilot reviews on GNAME²

While GNAME is not ranked the lowest in Trustpilot for registrars, it is among the bottom ten. Table 2 shows the Trustpilot ranking of other registrar companies. The color code is based on a combination of the registrar's score and the number of reviews.

Registrar	Score	Reviews
Tucows Domains Inc	1.3	68
ENom, LLC	1.5	82
Dominet (HK) Limited (Alibaba)	1.7	80
PDR Ltd. D/b/a PublicDomainRegistry.com	1.9	30
GNAME.com Pte, Ltd	2.4	135
GMO Interne Group, Inc d/b/a Onamae.com	2.4	8
Key-Systems, LLC	2.5	5
Sav.com, LLC	2.6	965
Hosting Concepts B.V	3.7	1
NameCheap, Inc	4.3	18k
Dynadot Inc	4.5	2.4k
Spaceship, Inc	4.5	2.9k
Name.com, Inc	4.5	2.3k
GoDaddy.com, LLC	4.6	120k
NameSilo, LLC	4.6	2k
Porkbun LLC	4.8	17k

Table 2. Trustpilot ranking for registrar companies, sourced on May 8, 2025)

Figure 14 shows the domain name registrars with the highest number of reported phishing domains as reported to the *Cybercrime Information Center*; GNAME is listed at number five.

Ranking of Domain Registrars by Phishing Domains (November to January 2025)

Registrars with a minimum of 30,000 domains and 25 phishing domains

Rank	Registrar	Registrar IANA_ID	gTLD Domains under Management	Phishing Domains ▼	Phishing Domain Score
1	NameSilo, LLC	1479	4,500,512	46,167	102.6
2	NICENIC INTERNATIONAL GROUP CO., LIMITED	3765	133,987	39,896	2,977.6
3	Key-Systems, LLC	1345	1,154,412	34,382	297.8
4	GMO Internet Group, Inc. d/b/a Onamae.com	49	5,620,341	33,648	59.9
5	Gname.com Pte. Ltd.	1923	4,986,740	26,734	53.6
6	Web Commerce Communications Limited dba WebNic.cc	460	790,066	25,871	327.5
7	Dominet (HK) Limited	3775	647,283	25,352	391.7
8	NameCheap, Inc.	1068	18,281,060	25,041	13.7
9	GoDaddy.com, LLC	146	64,987,396	21,181	3.3
10	PDR Ltd. d/b/a PublicDomainRegistry.com	303	4,014,135	17,082	42.6
11	Dynadot Inc	472	4,773,467	9,532	20.0
12	HOSTINGER operations, UAB	1636	3,880,007	8,303	21.4
13	OwnRegistrar, Inc.	1250	274,549	7,704	280.6
14	Tucows Domains Inc.	69	10,159,586	7,361	7.3
15	eNom, LLC	48	3,589,335	6,275	17.5
16	Sav.com, LLC	609	1,040,041	5,796	55.7
17	Registrar of Domain Names REG.RU LLC	1606	805,624	5,546	68.8
18	Hosting Concepts B.V. d/b/a Registrar.eu	1647	1,226,302	5,023	41.0
19	Chengdu West Dimension Digital Technology Co., Ltd.	1556	1,194,385	4,318	36.2
20	Aceville Pte. Ltd.	3858	59,956	4,108	685.2

Figure 14. The number of reported phishing domains per domain registrar from November 2024 to January 2025³

The criminal market for scams

This section discusses the criminal market for scams where this type of cybercrime originates, and the platforms that the actors responsible for them occupy.

Scams can originate from various sources including cybercriminals, crime groups, and organized crime networks. Our investigations also found that there is a market for scam services found on social media sites and underground criminal hacking forums.

Scam actors

Crime groups

The Smishing Triad is a known cybercriminal group with a modus operandi involves conducting SMS phishing campaigns, also known as smishing. Initially identified in 2023 as a Chinese eCrime group,⁴ it has been observed to target organizations across at least 121 countries and various industries, including postal services, logistics, telecommunications, transportation, finance, retail, and public sectors.

Over the years, these Chinese-speaking fraudsters have developed and operated what is believed to be the world's most extensive smishing operation, sending millions of text messages and likely raking up millions of dollars in successful scams.

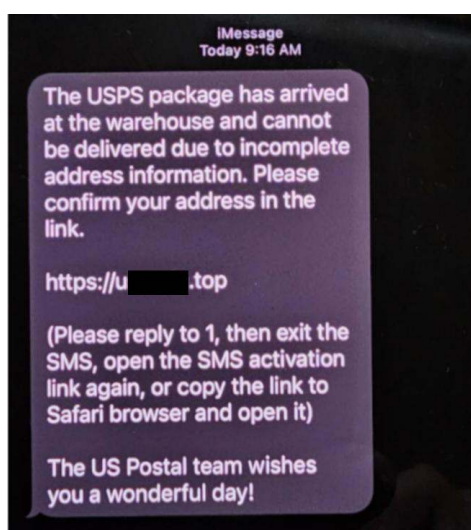


Figure 15. A sample smishing message posing as the United States Postal Service (USPS) in what is believed to be a smishing campaign by the Smishing Triad⁵

In 2023, a notable instance of this group's activity was observed where 5,405 phishing attacks impersonating the United States Postal Service (USPS) was detected.⁶ Another campaign sent fraudulent text messages claiming unpaid toll bills or payment requests related to toll services like FasTrak, E-ZPass, and I-Pass. This campaign utilized over 60,000 domain names, which made it difficult for platforms like Apple and Android to block fraudulent activity effectively.⁷ The Smishing Triad also participates in the sale of smishing kits within Telegram channels.

Organized crime networks

As the phenomenon of scams has become a significant concern worldwide with billions of dollars lost annually, it is essential to recognize that some of the actors involved in these cybercrimes can themselves also be victims. There are those known to have been lured into jobs, only to find themselves trapped in compounds and subjected to violent exploitation, while others are deceived by individuals within their social circles, friends, or relatives. Trend Micro previously researched⁸ how criminals are using scams and deceptive tactics for financial gain.

During the pandemic, out-of-work gangsters turned to kidnapping people for scam operations as a means of survival. Furthermore, fake job listings have been used to recruit adults and children from numerous countries,⁹ including the following:

- Bangladesh
- Brazil
- Burundi
- Cambodia
- Eritrea
- Ethiopia
- Hong Kong
- India
- Indonesia
- Japan
- Kazakhstan
- Kenya.
- Laos
- Malawi
- Malaysia
- Mongolia
- Nigeria
- Pakistan
- People's Republic of China
- Philippines
- Russia
- Senegal
- Singapore
- South Africa
- Sri Lanka
- Taiwan
- Tajikistan
- Thailand
- Türkiye
- Uganda
- United Kingdom
- United States
- Uzbekistan
- Vietnam

Several reports tell of operations led by Thai, Chinese, and Myanmar authorities that revealed thousands of people have been forced to work in “scamming centers,” sometimes tied to Chinese criminal syndicate groups.¹⁰ In February 2025, 7,000 people were released from locked compounds in Myanmar where they were forced to scam Americans and other victims of their life savings.¹¹ According to Reuters there may be over 100,000 victims still trapped working in these scamming centers in the Thai-Myanmar border.

Meanwhile, “Hustle Academies” have reportedly emerged in West Africa, where individuals – often young people – are taught how to commit fraud and sextortion scams online. These academies provide training on various techniques, including phishing emails, romance scams, and extortion schemes. Similar setups existed in the 1980s and 1990s under the name “business centers.” Back then, their task was to target victims worldwide via postal letters, telephone calls, and faxes.¹²

Platforms for the proliferation of scams

Scam services offerings on social media

Social media and messaging or chat apps also serve as a platform for task scams: cybercriminals sell and advertise services on these sites, making the barrier for entry virtually nonexistent. These advertisements on social media enable criminals even if they do not have a complex arsenal at hand. There are Facebook and Instagram advertisements for bulk SMS services. We have also found 50 Facebook groups dedicated to these types of services, which include Voice over Internet Protocol (VoIP), set up solutions, and even AI bulk SMS campaigns. During our research, we found that pricing is not always included in these postings.

The image is a collage of several social media advertisements for VoIP and bulk SMS services. The top section features a profile for a "Bulk Sms Service Provider" with a list of services: "Get Reliable & Scalable VoIP Solutions", "I provide solutions for:", "✓ DID Numbers", "✓ SIP Trunking", "✓ Autodialers", "✓ Spoofing Calls", "✓ IVR Setup", and "Available Platforms: Twilio | Telnyx | VoIP | Pivo | Vonage | SignalWire | Asterisk | 3CX". It also includes a Telegram contact: "Contact me on Telegram: @Davidpetert" and a list of hashtags: "#VoIP #SIPTrunking #DIDNumbers #Twilio #CloudTelecom #IVR #Autodialer #VoIPsolutions #CallSpoofing #BusinessCommunication #TelecomSolutions". Below this, there are several smaller ads. One says "I have good voip route, bulk sms, call center, DID number for any country" and "IVR". Another says "Good and Viable Twilio account, Voip route, Bulk sms, Call center, DIDww, Voice cloning, 3cx, IVR Setup, Autodialer setup for any Country". A third says "Are you looking to launch or upgrade your call center or communication system with cutting-edge VoIP technology?". A fourth says "services offered: Twilio, Telnyx, Pivo, Vonage, Voip, Bulk sms, 3CX, DID Number". The bottom right corner has a section titled "TWILIO TELNYX PLIVO" with a list of services: "My Service: Bulk sms sending, App integration, Sms forwarding, Call forwarding, Account Upgrading".

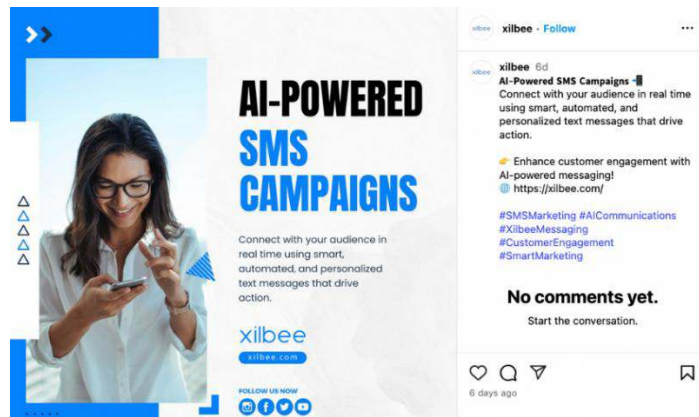


Figure 16. A Facebook group post¹³ that advertises VoIP, bulk SMS, and other mass calling related services, and an ad for an AI-powered SMS campaign on Instagram

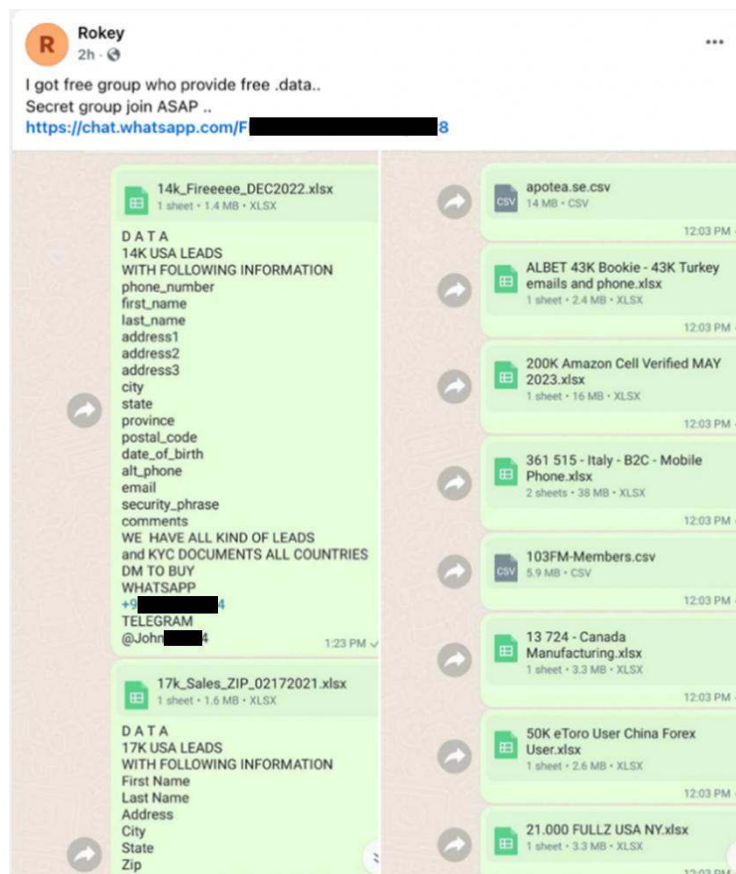


Figure 17. Another Facebook post offering a group to share spreadsheets of email and phone numbers for download¹⁴

There are also some Facebook groups that provide links to secret WhatsApp groups where people share free Microsoft Excel documents with information such as names, addresses, emails, dates of birth, and phone numbers. Based on the descriptions, some of these could have come from compromised databases from breaches.

Legitimate messaging and chat applications abused for scams

Telegram and WhatsApp are two messaging and chat applications that are widely used for employment task scams. Between the two, Telegram offers more functionality that task scammers can utilize to their advantage: Telegram has channels that can be used to promote the scam, which makes for better efficiency versus having to contact victims individually. While Telegram also has a search functionality, which can mean that users can find the channel being used for the scam, the platform's channels can be set up with relative ease and if the criminals are careful, they can maintain their anonymity.

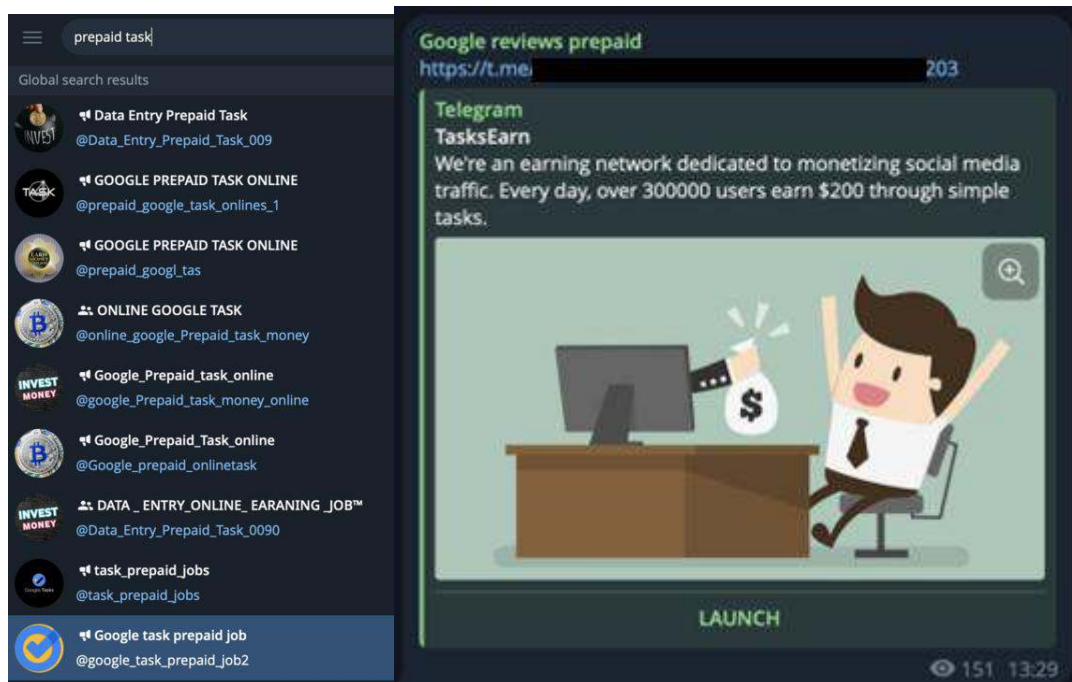


Figure 18. A screenshot showing Telegram groups for task scams

Telegram also has other features, such as bulk SMS, that can be abused to facilitate these scams. Figure 5 shows how tasks can be sent via Telegram in batches, with compulsory tasks being strategically placed in every second batch. This is to provide the bait payout and then require money to be paid to continue after the subsequent batch. Similar to the scam we encountered in the main paper, the amounts often increase incrementally so that the lure of a big payout at the end keeps victims hooked.

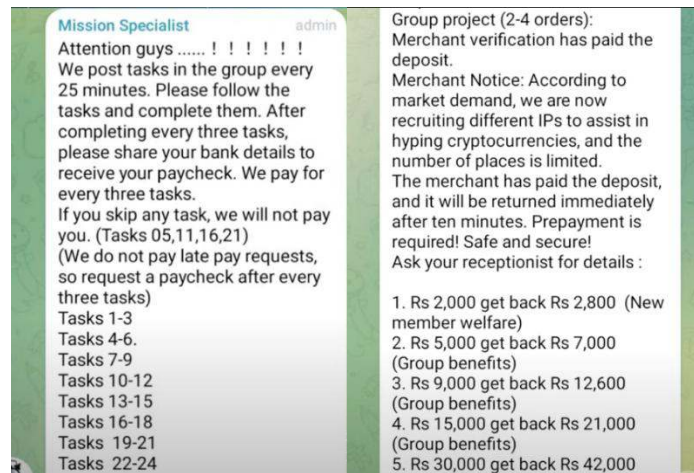



Figure 19. Task Scams advertised on YouTube; these scams use the Indian rupee for currency, suggesting that the scam takes place in India¹⁵

WhatsApp is another messaging platform that provides the architects of these scams with a simple delivery mechanism. The cost for phones, particularly prepaid phones, means that the overhead is not prohibitive: these phones can be used solely for the purpose of messaging victims and can be easily replaced if they are blocked.

Underground market offerings

Underground bulk SMS services also enable cybercriminals to scale their operations, targeting millions of users simultaneously. These services allow attackers to efficiently send thousands or even millions of fraudulent instant messaging (IM) messages, targeting individual users or groups of users based on specific demographics across various regions. Such underground vendors provide the infrastructure to send millions of malicious IM messages at scale. These messages often include links to fraudulent websites mimicking legitimate entities such as banks, payment systems, and other online services. Setup prices start at US\$2,000 and up.

Some cybercriminals in the underground also look to recruit spammers for their call center as illustrated in Figure 8. Countries may vary, and prices are usually discussed privately via Telegram.




Patolus
CD-disk
User
Registration: 30.09.2024
Messages: 17
Reactions: 1
Guarantor of the transaction: 1

11/14/2024

Price: Starting at 0.02 EUR/SMS
Contacts: @LimitlessTXT

Post your UID below and receive **5 EUR** balance on LimitlessTXT.com
Free SMS for XSS users!



Get started sending SMS both singles and bulk via our web-app - everything is automatic including sending, testing and deposits. We allow the BULK SMS Spoofing of SMS and Singles SMS spoofing, if the country supports spoofing. Exceptional prices around the globe - **where everything is automatic** - Automatic deposits without KYC, **Auto test routes** , **Auto select routes** !

English:
Everything happens automatically for your convenience, no human contact is needed to get started. Test 200 routes, select 200+ routes and top up your account online.
It's free to create an account and check prices.
Find your UID for free for 5 EUR when you create an account.
Offers SMS hooks and phone number verification for companies like Binance, Amazon, Facebook, WhatsApp and more. Full list below.
Welcome!

Spanish:
Todo es automático para su facilidad, no se necesita human contacto para empezar. Pruebe 200 rutas, seleccione más de 200 rutas y deposite todo en línea.
Crear una cuenta y consultar precios es gratis.
Encuentra tu UID gratis 5 EUR al crear una cuenta.
Ofreciendo pistas SMS y Phone Number Checker contra empresas como Binance, Amazon, Facebook, WhatsApp y más. Lista completa a continuación.
Bienvenido.

Thread design for LimitlessTXT
Hiding it because it's big. Infographics in the spoiler.

List of current services for scanning (Only phone numbers):

BINANCE
WhatsApp (Active, Days, Age, Gender)
IOS (+ iMessage)
RCS
Amazon
Telegram

Other less popular services:
Zalo
Line (Active, Age) (+ Line TW)
Facebook
Viber
Moniepoint
Coupant
Band
Signal
Skype
Botim
Momo
TikTok
VK
Ins
Twitter
LinkedIn

Terms: Minimum 10k scanning per order
TO ORDER: Create an account on [\[redacted\].com/](#) and go to "Leads"
(It's free to create an account)

Terms of service: No matter what - NO
REFUNDS !
Leave your password, NO DELIVERY! Whatever you say - NO REFUND !

Figure 20. An example of SMS services offered on the XSS cybercrime forum

callcenter3cx
byte
•

3CX

Paid registration
0 1
4 posts
Joined
04/18/25 (ID: 195989)
Activity
хостинг / hosting
Deposit
0.000185 B
Autogarant
0

Posted Friday at 06:08 AM (edited)

📞 Struggling to set up a proper call center?
Many people run into issues when trying to build a professional call center — that's why we offer fully customized 3CX solutions, tailored exactly to your needs.

✅ What we offer:

- ✓ Custom IVR menus
- ✓ Smart call queues & routing
- ✓ Fully tailored call flows
- ✓ 24/7 support – we've got your back
- ✓ Reliable & experienced – you can count on us

💰 Investment: \$2,000 for the full setup
We also want 20% of the revenue generated through our call center – because we build systems that actually work and deliver long-term results.

📄 A test/demo is possible, but don't message us unless you're serious.
We're only investing our time in people ready to move fast and build something real.

🔒 Payments are done securely via escrow – so both sides are protected and everything stays professional.

Extra:
For serious clients, we also provide:

- 🔗 Crypto exchange checkers (Coinbase, KuCoin, Binance).
- 📊 Custom data generation to the boost results even more.

📧 Interested? Send me a message.
⚠️ Serious inquiries only – no time for empty talk.

Contact: @callcenter3cx

Edited Friday at 06:21 AM by callcenter3cx

Figure 21. An offer for startup services posted on the Exploit cybercrime forum

B Need Crypto Spammers & Traffic Now

By BigPanda, 8 hours ago in [Spam] - mailings, databases, responses, mail-dumps, software

BigPanda
byte
•

B

Paid registration
0
6 posts
Joined
04/03/21 (ID: 115575)
Activity
кардинг / carding
Autogarant
0

Posted 8 hours ago

I'm looking for quality traffic to Coinbase and Binance from the following countries:
Germany, Australia, Austria, Canada, Hong Kong, Japan, Netherlands, Norway, Poland, Singapore, Spain, Switzerland, Turkey, and the UK.
I run a large call center with a full team of closers ready. Leads are in place—we just need solid traffic that hits (no spam folder, no SMS filtering).
Email, web, or other working routes welcome.
Open to percentage or upfront, whatever works best for you.
If you've got real traffic, let's talk and lock this in.

You can contact me on telegram- @HQthe1

+ Quote

Figure 22. Another post on Exploit looking for spammers for a cryptocurrency scam

The impact of a task scam

This section gives perspective on the financial and psychological impact of task scams on victims, which we first touch on in the section of the main report titled, “Real victims losing real money to fake job opportunities.”

As shown in our investigation where we posed as a potential victim and engaged with a task scammer, these bad actors get more hands-on after the initial contact via SMS message when they transfer the point of contact onto WhatsApp. During our research, we found that sometimes the scammer also sends friendly messages to gain the potential victim’s trust and get them to respond. Other examples of friendly texts share updates about weekend plans and about the scammer’s fictional family, likely to establish some form of connection and intimacy with the potential victim.

We have observed that scammers can keep up this friendly façade from weeks up to several months, but many of the images they send to establish this front can easily be found on reverse image searches. This shows that the impact of task scams, when they are successful, goes beyond the financial fallout and can also affect the victim’s psychological well-being.



Figure 23. A screenshot of a scammer’s message sharing a seemingly innocent update with a conversation starter sent to the potential victim. The picture attached in the scammer’s message can be reverse-searched and was found on at least two Instagram and one TikTok account.



Figure 24. Another message from the scammer with a stolen picture of a woman and a child that originally belongs to a wellness and fitness influencer-based South Carolina.

We also investigated the financial impact of the task scam we encountered in our research. In the following paragraphs, we mention six different cryptocurrency wallets, the addresses for each have been redacted.

The scammer used cryptocurrency wallets to add funds to the potential victim's training account: *USDT TRC20*: T[crypto wallet 1]x and *USDT/USDC Polygon*: 0x1A7Bc[crypto wallet 2]e.

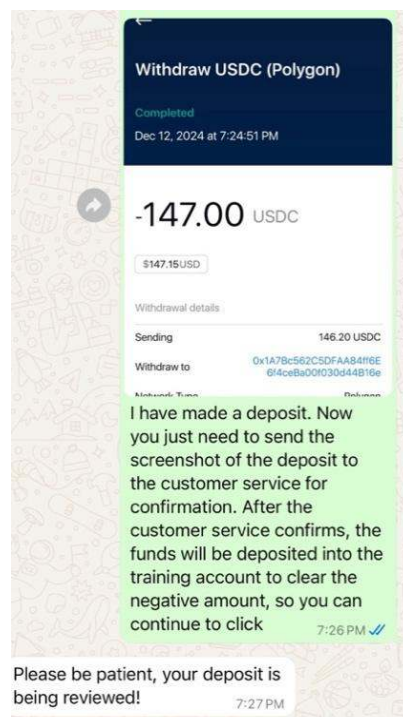


Figure 25. The crypto wallet receiving funds during the scam

The Polygon wallet 0x1A7Bc[crypto wallet 2]e had 184 transfers with 162 transactions from December 1, 2024, to January 22, 2025. It had 34 days of active transactions before going

quiet, with the highest transfer amounting to US\$23,161.76. Throughout its period of activity, this account received approximately US\$187,392. The current value is under US\$1, as the funds likely have been moved elsewhere.

Following an investigation of the Polygon wallet, one of the recipient's wallets was also linked to a task scam. The Polygon wallet *0xf[crypto wallet 3]9* was provided to a victim by the operators of a review submission scam using the *lavisualhot[.]com* and *lavisualapt[.]com* domains.¹⁶ Both of these domains are also registered with GNAME. The domains are impersonating a Los Angeles visual brand that offers marketing and branding services. This falls under the same tactics used by the operators of the scam impersonating Cloverstone.

Meanwhile, the Tron wallet *T[crypto wallet 1]x* had 95 transfers with 59 transactions from December 5, 2024, to February 18, 2025. The highest transfer was US\$28,000, but its current value is also under US\$1.

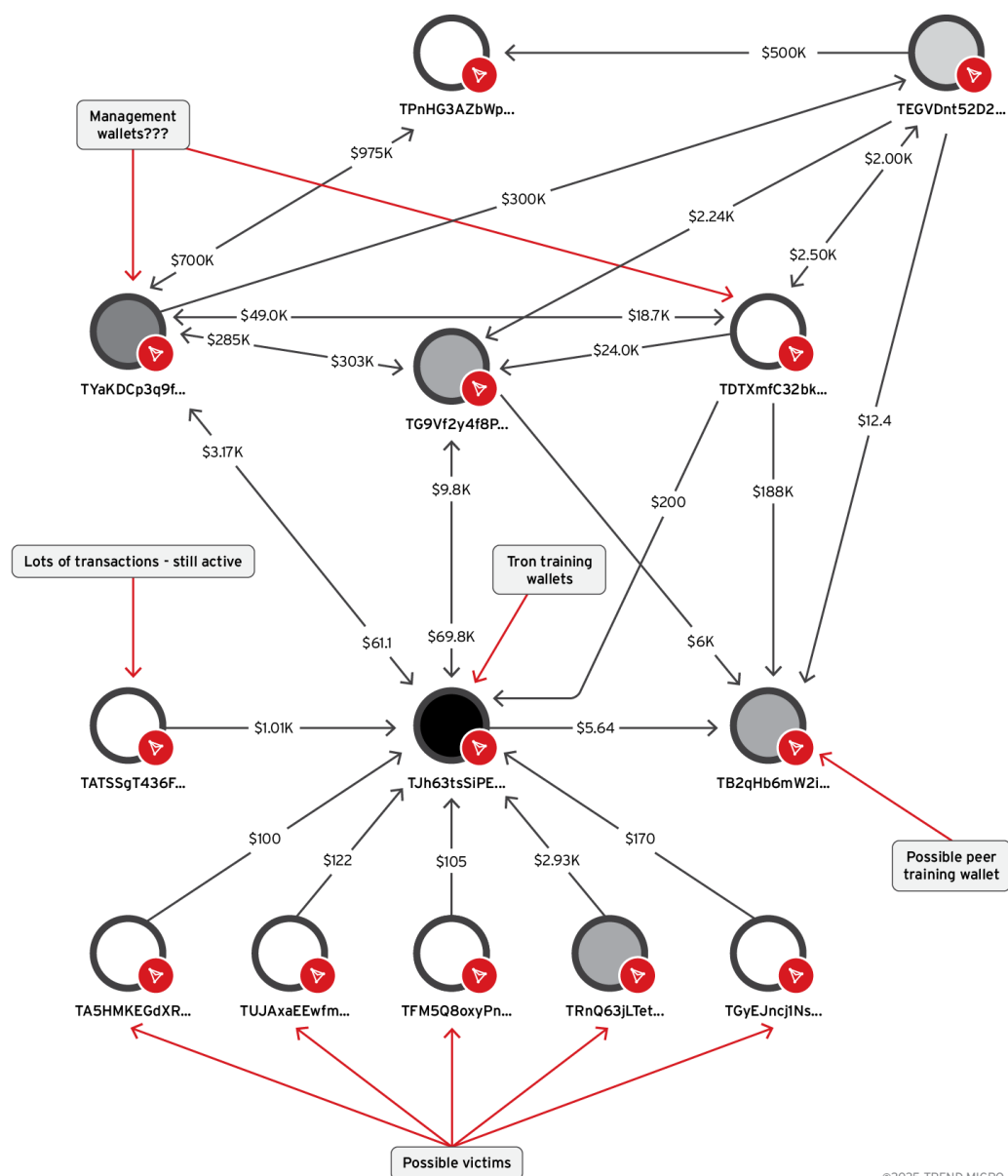


Figure 26. A recreation of the multi-level network of scammers connected to the Tron account

We further investigated the Tron account 7[crypto wallet 1]x and uncovered a network of scammers connected to the account. Figure 25 illustrates this network with the Tron account shown as the black circle in the middle. While most transactions are not visible here, this diagram illustrates that the scammers likely have a tiered system not unlike a multi-level marketing business. There are inbound transactions that are likely from other victims starting at least approximately at US\$100. Further levels of transactions increase in amount, ranging from tens of thousands to six figure-amounts.

We have also identified another BTC (bitcoin) wallet, 3[crypto wallet 4]3, as being associated with the malicious and fraudulent Cloverstone website *cloverstone-ek[.]com*. In a 3-month period approximately US\$1.2 million went in and out of the wallet through 1,439 transfers. The current value is US\$11.14 as of June 1, 2025. This wallet was used to pay almost US\$75,000 to another wallet 3[crypto wallet 5]d. This former wallet also received US\$242,000 from another wallet 3[crypto wallet 6]C. When multiple users of a crypto trading platform were observed making payments to this wallet, a subsequent investigation found that the victims believed they were working for a legitimate marketing and advertising company.

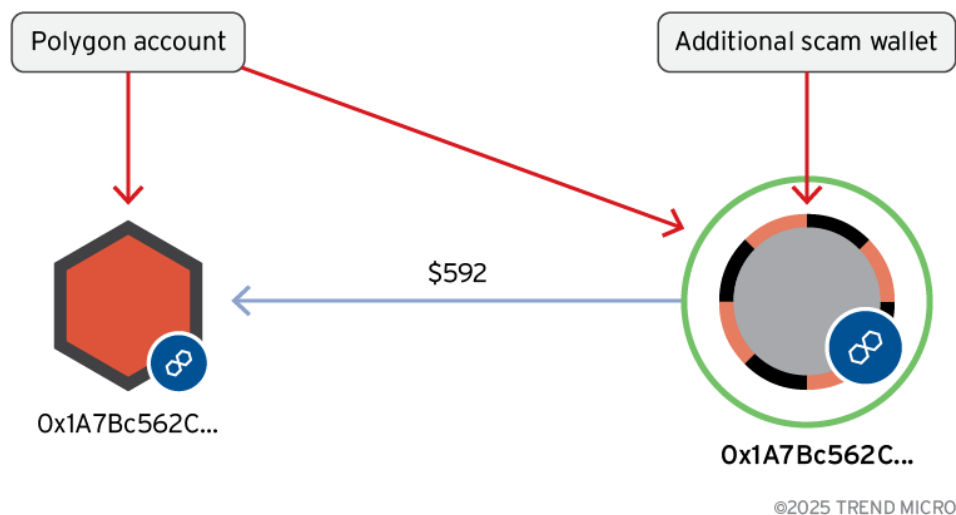


Figure 27. The exact values made by the cybercriminals vary from scam campaign to scam campaign but frequently amount to hundreds of thousands, or millions of dollars - showing the scale of this very major cybercrime problem today.

The large amounts of money that course through the few cryptocurrency wallets we investigated barely scratches the surface of how the immense financial impact of task scams are. This emphasizes the need for coordinated efforts between individuals, businesses, technology providers, and law enforcement to reduce the impact of these increasingly sophisticated criminal operations.

By understanding how these scams operate and the warning signs to watch for, individuals can better protect themselves from becoming victims to what has become one of the fastest-growing types of fraud in the digital economy.

References

- ¹ Clariane Group. (April 30, 2024). "Clariane". "Fraud Alert: Fraudsters purporting to be Clariane attempting to sell fake". Accessed on July 30, 2025, at [link](#)
- ² Trustpilot Users. (Date unavailable). "Trustpilot". "Gname.com Reviews". Accessed on July 30, 2025, at [link](#)
- ³ Cybercrime Info Center. (Date unavailable). "Cybercrime Info Center". "Phishing Activity in Registrars November-January 2025". Accessed on July 30, 2025, at [link](#)
- ⁴ Reddit. (June 27, 2024). "Reddit". "US Task Scammers using Business Names to Lure in Victims". "Accessed on July 30, 2025, at [link](#)
- ⁵ Resecurity. (August 30, 2023). "Resecurity". "Smishing Triad Targeted USPS and US Citizens for Data Theft". Accessed on July 30, 2025, at [link](#)
- ⁶ APWG. (February 27, 2024). "APWG (Anti-Phishing Working Group)". "Phishing Ended 2023 with a Bang". Accessed on July 30, 2025, at [link](#)
- ⁷ Resecurity. (April 8, 2025). "Resecurity". "Smishing Triad is Now Targeting Toll Payment Services in a Massive Fraud Campaign Expansion". Accessed on July 30, 2025, at [link](#)
- ⁸ Trend Research. (May 2, 2024). "Trend Micro". "Unmasking Pig Butchering Scams and Protecting Your Financial Future". Accessed on July 30, 2025, at [link](#)
- ⁹ U.S. Department of State. (June 2023). "U.S. Department of State". "Human TraWcking and Cyber Scam Operations". Accessed on July 30, 2025, at [link](#)
- ¹⁰ CSJS. (December 12, 2024). "Center for Strategic and International Studies (CSJS)". "Cyber Scamming Goes Global: Unveiling Southeast Asia's High-Tech Fraud Factories". Accessed on July 30, 2025, at [link](#)
- ¹¹ Huizhong Wu, Jintamas Saksornchai, Martha Mendoza (March 10, 2025). "PBS". "Inside the Scam Centers and TraWcking Rings of Myanmar". Accessed on July 30, 2025, at [link](#)
- ¹² BBC. (Date unavailable). "BBC". "School for scammers: Inside Nigeria's hustle kingdoms". Accessed on July 30, 2025, at [link](#)
- ¹³ Facebook Group Administrator. (Date unavailable). "Facebook". "Facebook Group: 1035145263591388". Accessed on July 30, 2025, at [link](#)
- ¹⁴ Facebook Group Administrator. (Date unavailable). "Facebook". "Facebook Group: 295241984934366". Accessed on July 30, 2025, at [link](#)
- ¹⁵ Ajey Talks. (February 24, 2023). "YouTube". "1 Hotel Review = ₹50 | Give Hotel Reviews on Google Maps and Earn Rs.5000 Daily | Telegram Task Scam ". Accessed on July 30, 2025, at [link](#)
- ¹⁶ Reddit. (December 2024). "Reddit". "LA Visual Review Submission Scam". Accessed on July 30, 2025, at [link](#)



**Proactive Security
Starts Here**

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints.

With 7,000 employees across 56 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to simplify and secure their connected world.

TrendMicro.com