



Webwurm

A Vast Network of Deception by
Impersonating Thousands of Brands



Category

Adversary Intelligence

Region

Global

White papers and reports can be downloaded from CloudSEK website by visiting <https://cloudsek.com/whitepapers-reports> or by mailing to info@cloudsek.com.

 **Table of Contents**

1	Introduction & Overview of the Scam	4
2	Victim Complaints and Monetary Losses	5
3	Modus Operandi	6
4	Campaign Enablers	8
5	Insights & Observations	11
6	Impersonated Organizations by Region	13
7	Communication Channels (WhatsApp and Telegram)	15
8	Tracing Scammer Infrastructure: Historical Insights	17
9	Attribution	20
10	Takeaways	21
11	Appendix	23
12	References	28

Schedule a CloudSEK Demo

At CloudSEK, we predict cyber threats.

Our research into Webwurm (pronounced 'web-worm') was powered by CloudSEK XVigil's Fake Domain Monitor and Underground Discussions modules. CloudSEK XVigil combines the power of Cyber Intelligence, Brand Monitoring, Attack Surface monitoring, Infrastructure Monitoring, and Supply chain to give visibility and context to our customer's Initial Attack Vectors.

Interested to find out more about CloudSEK platform capabilities? Let us know by clicking the link below.

[Request a Demo](#)

Introduction & Overview of the Scam

A global scale scam nicknamed 'Webwyrms' (pronounced 'web-worm') that has been targeting more than 100,000 victims across over 50 countries globally by impersonating over 1000 companies across 10 industries for a combo task scheme akin to the 'Blue Whale Challenge' (from a few years ago that caused a massive global impact) is causing collective personal losses of possibly over a 100 million dollars. The scale of the scams and the TTPs (Targets, Techniques, and Procedures) employed show a highly skilled and persistent Threat Actor (TA) group who have been using effective OpSec (Operational Security) like consistent shifting of infrastructure and creating tight silos to prevent infiltration into the group.

CloudSEK has shared the details of the investigation with **Global Law Enforcement Agencies** to help implement remedial actions, including dismantling the scammer infrastructure and reporting to the impersonated organizations.

Webwyrms, likely active since late 2022, has grown multifold since early 2023 with the TA group employing various deceptive tactics. The following statistics unearthed by CloudSEK researchers show the scale at which the group is operating the scam.



Victim Complaints and Monetary Losses

Drawing from a trove of victim complaints and reported monetary losses, the reported losses from the impersonation of a single company exceed USD 200,000. As the scope of our investigation broadens, we unveil a network of approximately 1000 organizations that have been impersonated as part of Webwyrn, encompassing around 6000 fraudulent domains spread across 12 distinct Autonomous Systems, beyond these figures lies the pivotal question: **what might be the collective impact of these individual losses?**

The path to a comprehensive understanding requires us to employ a data-driven extrapolation. By averaging the monetary loss attributed to impersonating a single company – approximately USD 100,000 – we arrive at an astonishing conclusion. The potential collective impact on victims, taking into account the multitude of impersonated companies and an average loss of USD 100,000 per company, based on reported financial losses, potentially exceeds USD 100 million, impacting more than 100,000 individuals.

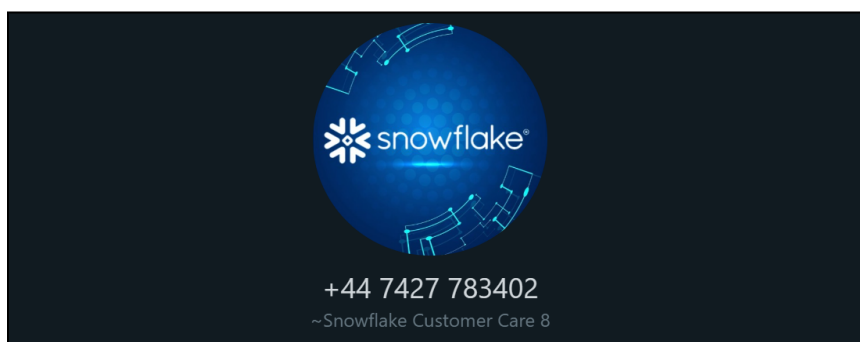
This forecasted figure is a stark reminder of the genuine threat this scam poses to individuals, businesses, and the broader ecosystem. Our intention in unveiling this projection is to underscore the urgency of awareness and action. This report, intended for a diverse readership encompassing the general public, authorities, and impersonated organizations, stands as a testament to the power of knowledge in combating such sinister activities.

This financial upheaval caused by Webwyrn not only devastates individual victims but also tarnishes the image of the impersonated companies. As the lure of thousands of dollars under their names traps countless individuals, brand trust takes a nosedive. This becomes evident as **victims in plight are inadvertently attributing legitimate companies to the orchestrators of these scams.**

In the [appendix](#) section, we have provided a selection of victim complaints—testaments.

Modus Operandi

- Scammers trap victims inside Webwyrn by predominantly engaging through social media platforms, with WhatsApp being a primary channel. While their approach may involve contacting random numbers, certain complaints highlight scammers specifically referring to Job Search and Recruitment Portals as the source of victim contacts. This suggests a potential focus on job seekers, with scammers possibly leveraging data from recruitment portals to tailor their schemes.



WhatsApp Profile of scammers impersonating a legit US-based Organization

- The text contains a job offer of a weekly salary (avg. \$1200-\$1500).
- A reference person is assigned who is the main point of contact via WhatsApp.
- The following are some of the points from the Job Description that the reference person provides which plays a key role in convincing the victims of how they can make large sums of money:
 - Total revenue is based on the base salary and commissions.
 - The more tasks one does, the more he/she earns.
 - Commissions are the main income, while base salary depends on whether the task is being done every day.
 - The daily job is to complete 2-3 packets (also referred to as resets) per day with 40 tasks in each packet. At least 2 packets of tasks should be completed in a day.
 - Once the task is performed, the platform will take the money out of the victim's account and put it back in along with the commission.
- The money has to be deposited into specific cryptocurrency exchange platforms like KUCOIN or SHAKEPAY.
- Scammers claim that converting the deposited cryptocurrency into USDT (a stablecoin pegged to the US dollar) will offer better security or higher returns.

USDT stands for "Tether," which is a type of cryptocurrency known as a stablecoin. The main purpose of stablecoins like USDT is to provide a digital asset with a stable value, minimizing the price volatility associated with other cryptocurrencies like Bitcoin and Ethereum.

- Now once the victim accepts the offer, the training begins.
- They are **directed to create an account on the website related to the organization the scammers are impersonating**. There are thousands of such websites spread across different ASNs.
- ~100 USDT are deposited to the victim's account after their training to begin with.
- During training, victims are also informed of a task called a "**combo task**" These have 2 major characteristics:
 - Earn a huge sum of money instantly apart from the usual tasks. A recharge of balance is required to perform every single task. Every new combo task requires 2x the amount invested last time.
 - All the combo tasks are to be performed in a streak and until all of them are completed, the victims can't withdraw their money, unlike the standard tasks.
- Victims encounter 1-2 combo task streaks in the first few days and they earn handsome amounts of money but the catch comes after a few days. On a random day, they get stuck in a recurring loop of Webworm. The streak never gets complete and in an attempt to complete all tasks to withdraw their money, victims end up draining their bank accounts.
- On contacting the referral person or the platform developers, they start intimidating them by asking them to finish the assigned tasks of the day or the account would be frozen.
- There's an option to get a 24-hour extension for arranging more money.
- Eventually, the victims cannot log into the website as their accounts get frozen.
- They are further added to a group chat where people would post profits they have made from the platform to give victims additional social proof that they were doing nothing wrong and that there's no way this could be a scam.

Campaign Enablers

This section reveals Campaign Dynamics: Factors Driving the Extensive Reach of Webworm and Noteworthy Aspects.

- **Understanding Victim Susceptibility Factors:** The susceptibility of victims to these campaigns is largely influenced by the inherent trust within the context. The trust stems from victims' prior engagement with job and recruitment portals, where they have applied for positions. Scammers exploit this reference and capitalize on impersonating legitimate entities. The combination of these factors creates a potent environment for entrapping victims.
- **Initial Gains and Trust-Building Withdrawal:** Victims are enticed with an initial deposit of USDT 100-150 in their account. The scheme offers withdrawals of USDT 2000-4000 weekly, reinforcing perceived legitimacy. This strategic approach capitalizes on victims' trust and encourages further investments, perpetuating the scam's cycle of deception.
- **Eluding Detection through Infrastructure Rotation:** Scammers exploit the transient nature of their scheme, hosting fake domains on an IP address or Autonomous System Number (ASN) for an average of 2-4 months. When abuse reports arise, scammers swiftly transition to new infrastructure, preserving the integrity of their operation. This adaptive tactic ensures sustained anonymity and operational continuity while evading detection.
- **Precise Regional Targeting:** Analyzing the impersonated domains, we found notable instances of country codes combined with impersonated organization names. The country codes for the UK, Canada, Singapore, Australia, Hong Kong, Indonesia, and India are being used in significant fake domains, reflecting the scammers' strategic approach to engaging victims within specific locales and also paving the path for the enablement of the following point.

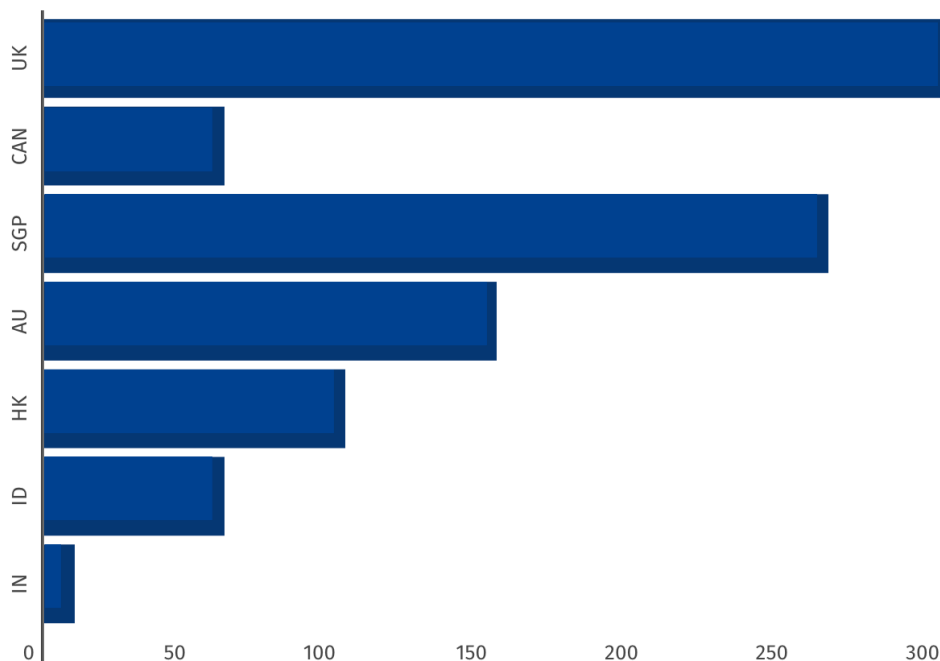


Chart depicting the country codes being used by scammers in fake domains along with their count

- Strategic Victim Engagement:** Dedicated SPOC utilize platforms such as WhatsApp to establish communication with victims. By addressing queries and fostering trust, scammers create an illusion of legitimacy, presenting the fraudulent operation as a genuine organization offering daily tasks.

These spokes can potentially be forced to indulge in such campaigns as disclosed here: [Cyber slavery starts up in Southeast Asia, Inside the 'pig-butcher' scams seeing thousands trafficked into cyber slavery.](#)

- Mobile-Centric Design and Cryptocurrency Transactions:** In a shrewd move, the majority of victim-facing websites are meticulously optimized for mobile-based browsers. This deliberate design choice allows victims to seamlessly navigate the platforms while conducting cryptocurrency transactions and recharging their balances. This accessibility ensures that victims can engage with the scams conveniently, contributing to Webwurm's widespread success.

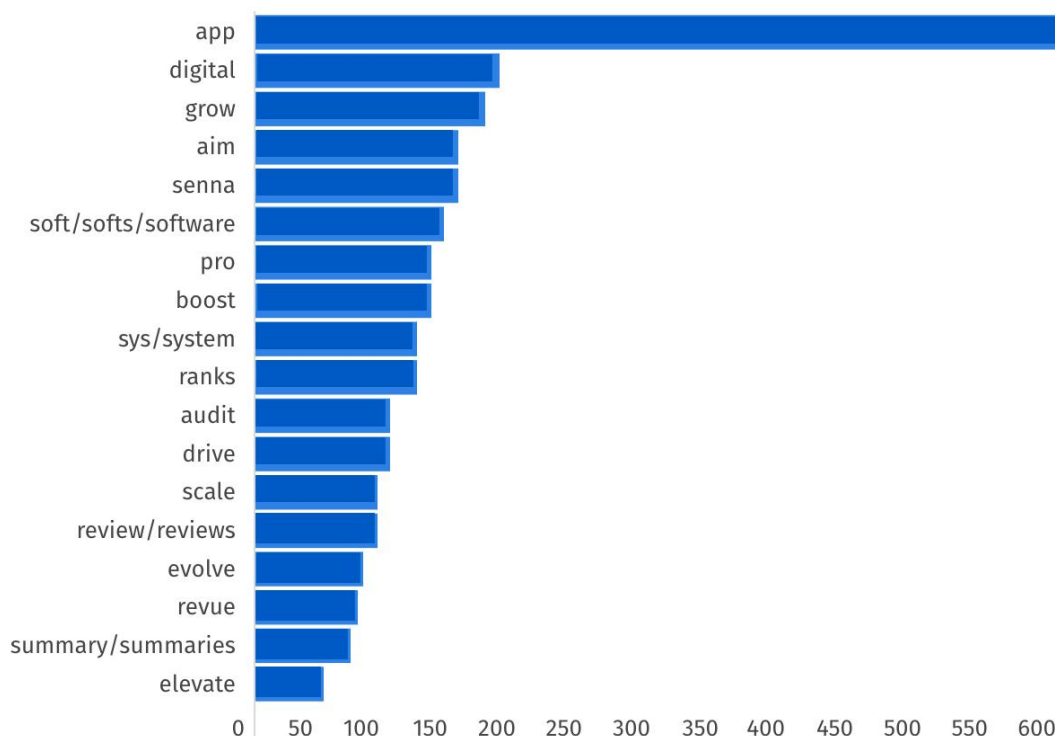
Furthermore, the utilization of cryptocurrency wallets such as KuCoin and Shakepay adds another layer of complexity to the fraud. These wallets offer a level of anonymity that hampers authorities' ability to investigate fraudulent transactions, shielding the scammers behind the shroud of cryptocurrency's decentralized nature. This strategic combination of mobile-centric design and cryptocurrency transactions serves as a potent enabler for the far-reaching impact of Webwurm.

- Keyword Selection:** The deliberate selection and use of these appended strings in fake domain names is done by mimicking legitimate keywords, descriptive terms, action-oriented language, and technical terminology in order to enhance the credibility and trustworthiness of their fake websites.

A list of 34 such keywords along with their approximate count in fake domains has been provided in the [appendix](#) section.

24kdesign-advance.com	anymind-home.com	cognitive-boots.com
24kdesign-analyse.com	anymind-mini.com	cognitive-examines.com
24kdesign-analytic.com	anymind-pro.com	cognitive-program.com
24kdesign-analyze.com	anymind-ranks.com	cognitive-reviews.com
24kdesign-app.com	anymind-senna.com	cognitive-revue.com
24kdesign-audit.com	anymind-software.com	cognitive-senna.com
24kdesign-boost.com	anymind-sys.com	cognitive-survey.com
24kdesign-drive.com	apadmi-aka.com	cognitive-top.com
24kdesign-elevate.com	apadmi-premium.com	cognitive-up.com

Snapshot of a few Fake Domains with appended strings



A bar chart depicting the count of Fake Domains for each appended string

Insights & Observations

Distinct Victim and Threat-actor facing domains:

The following inferences were drawn by analyzing ~6000 domains:

- Majority of the live domains can be categorized into 2 formats:
 - example.com &
 - admin.example.net (~800 of the total domains are in this format)
- All the domains in the format example.com are victim facing domains that are hosting a registration/login page to login into the platform where tasks are to be performed by the victims.
- While all the domains in the format admin.example.net have a login panel built using ThinkAdmin, an open-source background management system developed and maintained in China. These domains are suspected to be threat-actor-facing due to the following reasons.
- Through proxy softwares it was observed that the data being submitted at victim-facing domains is systematically redirecting all user information to threat actor-facing counterparts.

Conclusion: This orchestrated scheme allows the threat actors to **manage access to the data of countless victims** associated with a single victim-facing website through the corresponding threat-actor-facing website. This intrusive practice results in a comprehensive repository of statistics and financial details for each victim, including critical information such as investment amounts, task completion records, and other pertinent monetary data.

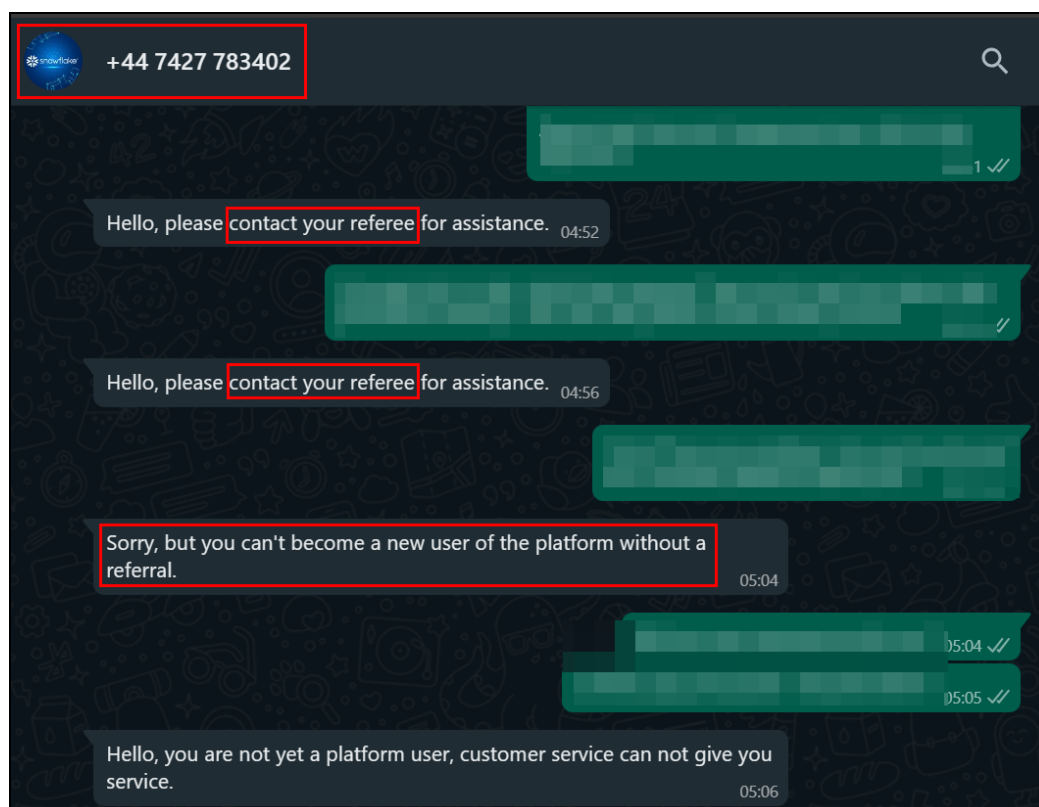
Restricted Access and Referral Codes

Intriguingly, the labyrinthine web of these scam websites is not accessible to all, but rather selectively targets victims who have been contacted via WhatsApp.

This referral system operating as a gatekeeper ensures that only those who have received a referral code from a contact within the scam network can gain entry.

The deployment of referral codes via WhatsApp both limits entry to the intended victims and highlights the intricate nature of this deception, ultimately underscoring the calculated strategy employed by the scammers.

The following screenshot is evidence of the same:



A snapshot of a chat where scammers confirm platform registrations are prohibited without a referral

Scammer Strategy: Identifying Impersonation Targets

Amidst the multitude of impersonated companies, a pertinent question arises: how are scammers meticulously selecting their targets? This enigma prompted us to delve deeper into our investigation. Our analysis yielded a revealing insight as we discovered that scammers had impersonated clutch.co and digitalagencynetwork.com into their web of deceit.

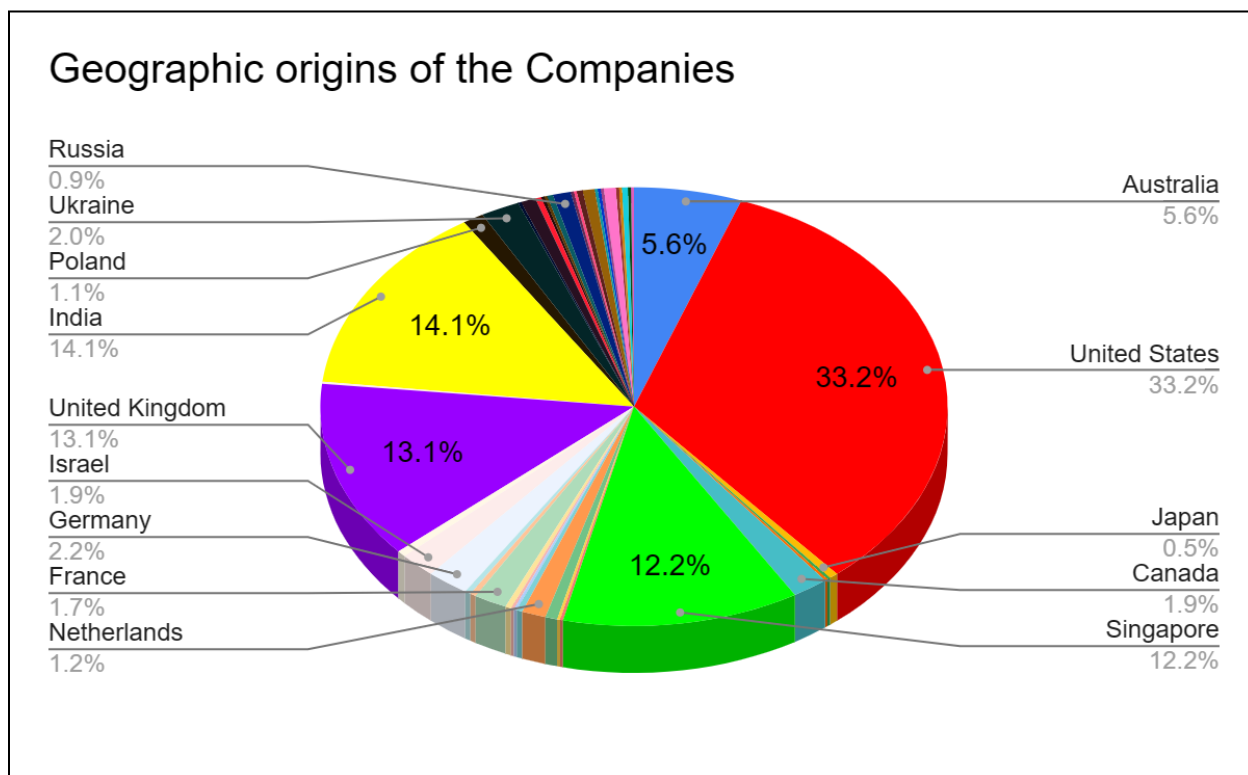
Clutch.co and Digital Agency Network are B2B ratings and reviews platforms bridging businesses with service providers. While Clutch.co emphasizes IT, marketing, and business services, Digital Agency Network focuses on digital marketing and advertising services. Intriguingly, these are the *most affected sectors as part of Webwurm*. **Scammers could be leveraging these platforms to strategically identify and target other companies**, employing a gamut of filters ranging from geographical location to revenue thresholds.

Here are some of the companies featured on clutch.co that are getting impersonated as part of Webwurm: [pixated](#), [neetclick-pte](#), [bluelabel](#), [izeno](#), [izea](#), [itomic](#), [wishbone-digital-group-pte](#), [wdi](#), [hyperlink-infosystem](#), [topanda](#), [moburst](#).

Impersonated Organizations by Region

Within our comprehensive investigation encompassing approximately 6,000 domains, we have unraveled noteworthy insights related to impersonated organizations that shed light on the breadth of Webwurm.

1. **Country of Origin Analysis:** Through meticulous analysis, we have discerned the geographic origins of the companies falling prey to impersonation. This discernment not only underscores the global scale of Webwurm but also highlights the diversity of regions affected by the malicious endeavor.



A Pie chart depicting the Geographic origins of the companies getting impersonated

2. **Targeted Industries:** Our analysis further unveils the industries that have borne the brunt of these fraudulent activities. The data underscores the concerted efforts by scammers to focus their attention on certain sectors, making these industries their prime targets.



A tag cloud depicting various services provided by companies that are getting impersonated

3. **Comprehensive Impersonation List:** We have painstakingly compiled an extensive roster of thousands of companies that have fallen victim to impersonation, drawing from a curated selection of domains. This list serves as a testament to the far-reaching implications of Webwyrms and offers a glimpse into the scale of the deception.

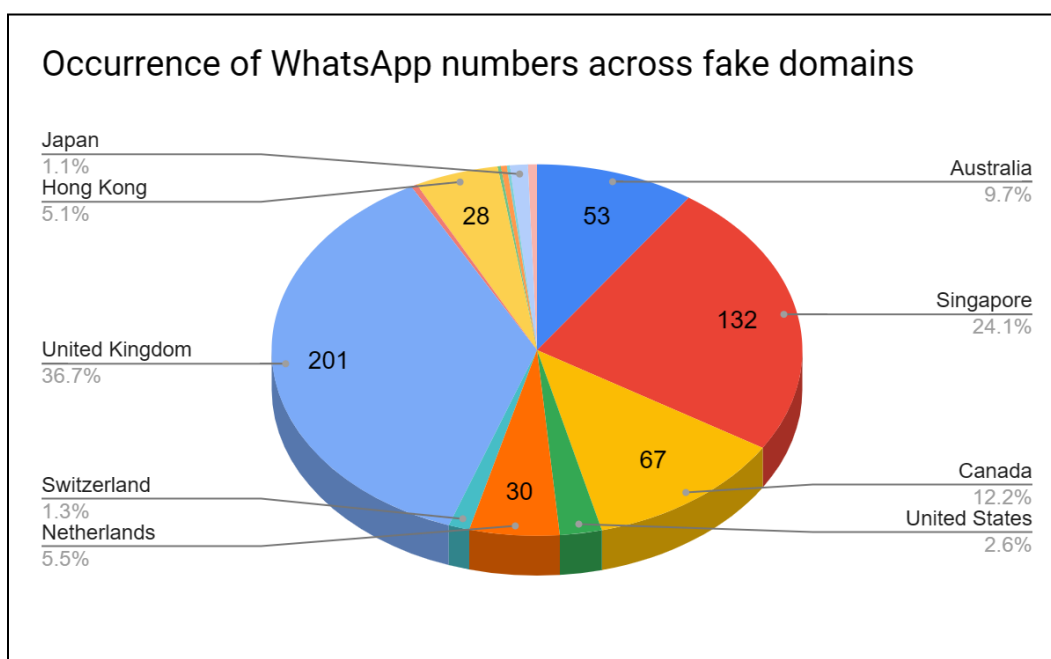
The following screenshot shows a few companies getting impersonated across 4 regions:

United States	Australia	India	United Kingdom
Airbnb	WeClan	Flipkart	Farfetch
Best Buy	Dick Smith	Shopclues	BrainLabs
BigCommerce	Appetiser	PhonePe	Depop
Amazon	Applogics	Tata Consultancy Services	Boohoo
Gartner	Smile	NetScape	Wordbank

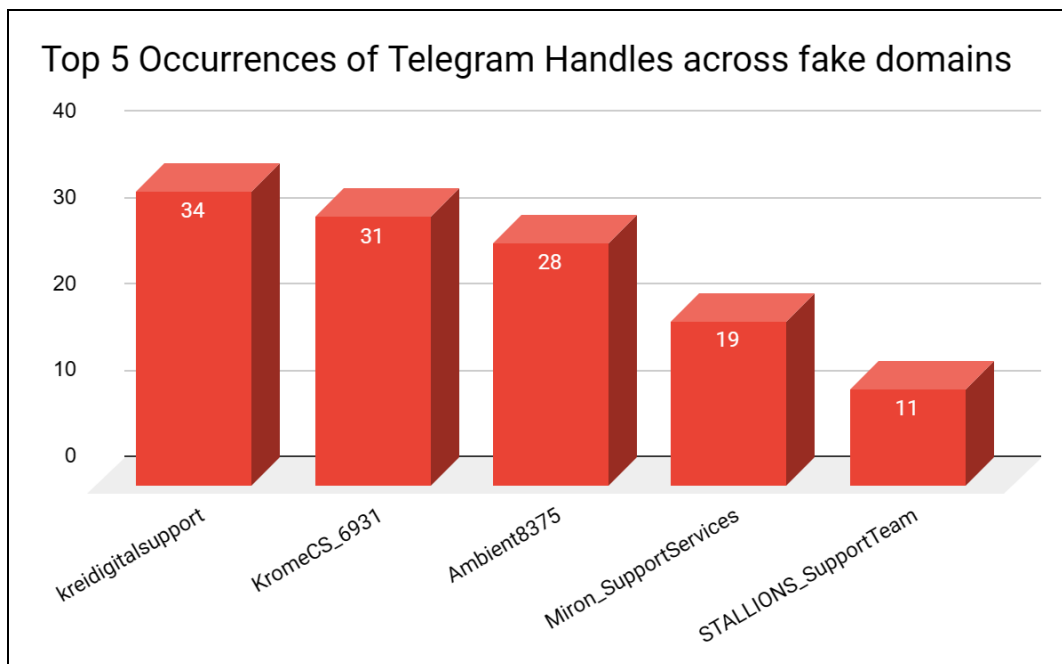
Communication Channels (WhatsApp and Telegram)

In our investigation, we have identified a significant trend in the use of communication platforms by scammers to interact with victims. Thousands of impersonating websites have adopted WhatsApp and Telegram as primary channels to reach out to victims and also for customer service, offering victims dedicated spokes to address their inquiries. This engagement only remains active till the point victims get trapped in a combo task scam loop.

Through extensive efforts, we have compiled a comprehensive list of these contact numbers and Telegram handles, providing insights into the mechanisms employed by scammers to maintain a façade of legitimacy.



A pie chart depicting the region to which WhatsApp numbers belong and their occurrence across impersonating domains



A Column chart depicting the top 5 used Telegram handles across fake websites

Over 600 websites sharing **nearly 200 unique WhatsApp numbers** and **230 Telegram handles** have been discovered.

The following screenshot shows sample data of the same:

Victim-Facing URL	WhatsApp Number	Country	Attacker-Facing URL
https://generateleadsplatforms.com	46767299015	Sweden	https://admin.generateleadsplatforms.com
https://www.generateleadssenna.com	46767299015	Sweden	https://admin.generateleadsplatforms.com
https://ciklum-network.com	61414754986	Australia	https://admin.ciklum-analysis.net
https://au-rootstrap.com	61424240271	Australia	https://admin.rootstrapau-app.net
https://rootstrapau-app.com	61424240271	Australia	https://admin.rootstrapau-app.net
https://www.au-rootstrap.com	61424240271	Australia	https://admin.rootstrapau-app.net
https://www.rootstrapau-app.com	61424240271	Australia	https://admin.rootstrapau-app.net
https://abs-steelkiwi.com	61434024952	Australia	https://admin.steelkiwi-analysis.net
https://aussteelkiwi-grow.com	61434024952	Australia	https://admin.steelkiwi-analysis.net
https://steelkiwi-analysis.com	61434024952	Australia	https://admin.steelkiwi-analysis.net
https://www.abs-steelkiwi.com	61434024952	Australia	https://admin.steelkiwi-analysis.net
https://www.aussteelkiwi-grow.com	61434024952	Australia	https://admin.steelkiwi-analysis.net
https://abs-steelkiwi.com	61434068516	Australia	https://admin.steelkiwi-analysis.net
https://aussteelkiwi-grow.com	61434068516	Australia	https://admin.steelkiwi-analysis.net

Tracing Scammer Infrastructure: Historical Insights

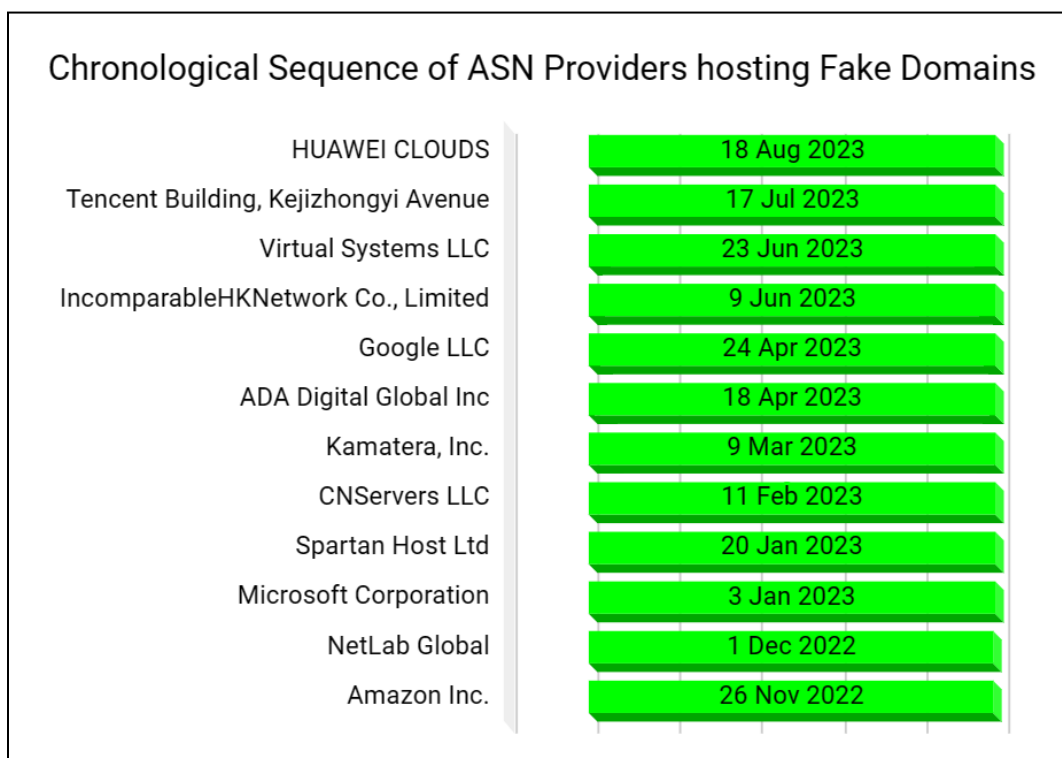
The network and infrastructure of Webwyrms deployed by the scammers are extensive, making comprehensive tracing a labor-intensive task.

For this report's scope, our research halted at **12 ASNs** where we could identify **119 IP Addresses** hosting malicious domains. Had we continued, more ASNs and IP addresses might have emerged, potentially hosting additional fake domains.

Currently, around 6000 fake domains are hosted on these IP addresses. However, this number could potentially be higher.

Points to keep in mind before reviewing the following table:

- Analysis of numerous domains and IP addresses revealed their first appearance dates, forming a chronological sequence for ASNs.
- Not all domains were transferred between ASNs; various patterns emerged for domains hosted on different ASNs/IPs.
- These patterns included shuffling, addition, shifting, and subsequent return to specific ASNs within the timelines mentioned in the table.



A Bar chart depicting the chronological sequence of ASN Providers hosting fake domains

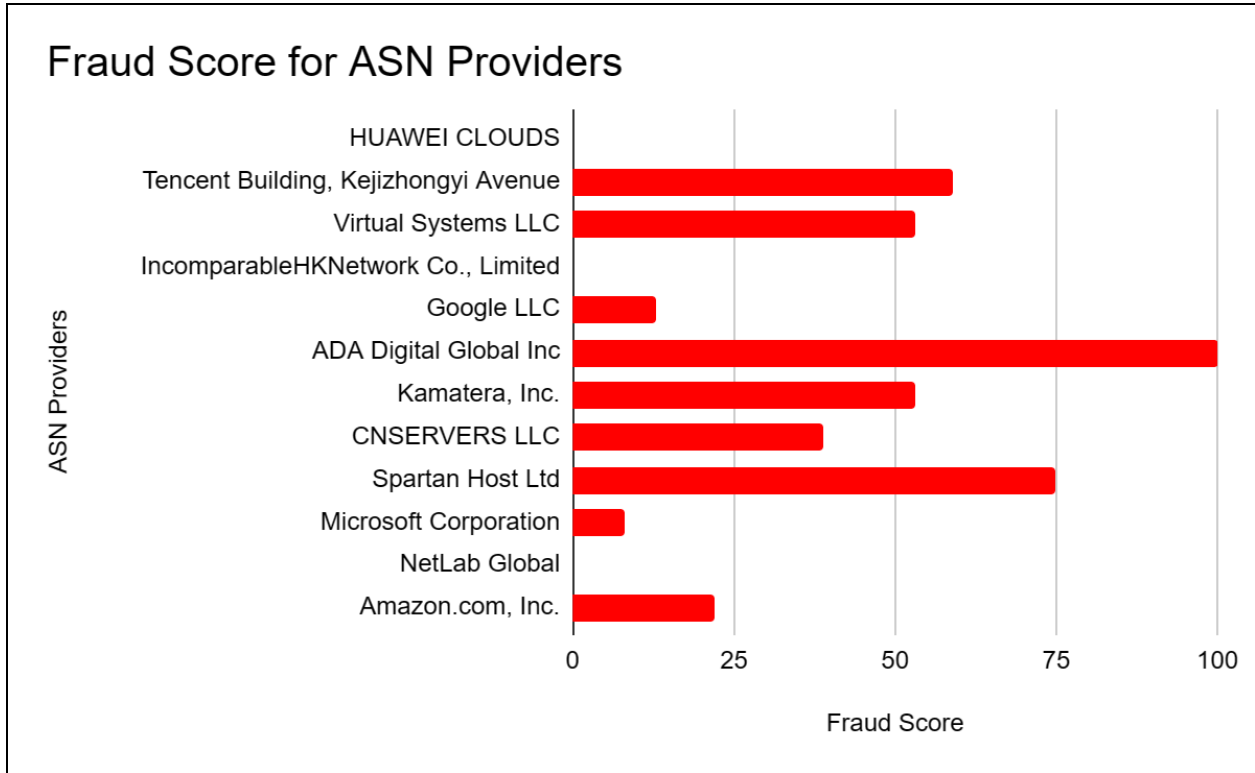
The chronological sequence for 12 ASNs based on IPs that were first detected along with

- ASN
- ASN Organization
- IPs hosting Fake Domains
- IPs First Detected
- Timelines for First Seen IPs

has been compiled together during our analysis.

The following screenshot contains the sample data on the same:

ASN	ASN Organization	IPs hosting Fake Domains
AS201106	Spartan Host Ltd	172.83.153.67 172.83.153.68 172.83.153.69 172.83.153.70 172.83.153.82 172.83.153.83 172.83.153.84 172.83.153.85 172.83.153.86 172.83.153.87 172.83.153.88 172.83.153.89
AS40065	CNSERVERS LLC	23.224.160.106 23.224.160.107 23.224.160.108 23.224.160.109 23.224.160.110 23.225.157.203 23.225.157.204 23.225.157.205 23.225.157.206 172.247.14.88 172.247.14.94
AS36007	Kamatera, Inc.	103.89.14.105

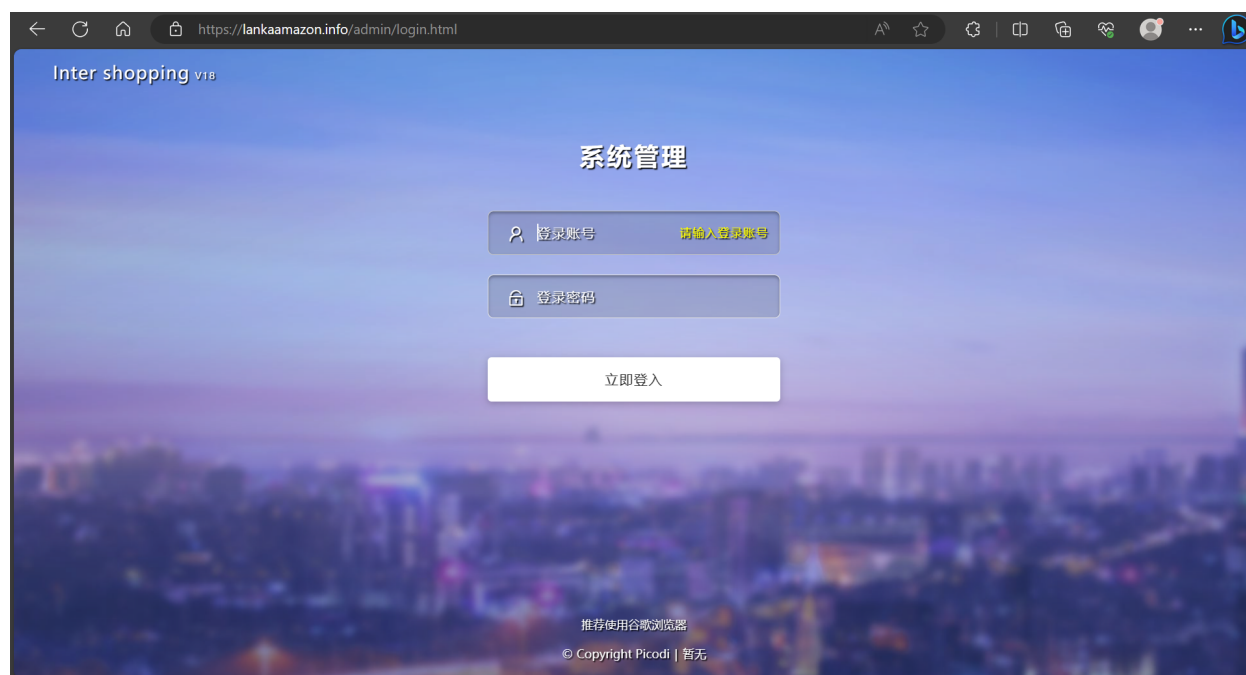


A Bar chart depicting the fraud score of ASN Providers

Attribution

Although Webwyrms targets victims globally, as evidenced by previous sections and the extensive infrastructure spans across various countries, making direct attribution complex but there are still some indicators suggesting that the campaign can potentially have a Chinese Connection:

- Approximately 800 threat-actor facing domains, dedicated to accessing victim investment data by scammers themselves, were constructed using ThinkAdmin. This backend framework originates from China. The page content for all these domains by default is in Chinese.



Threat actor facing domain targeting Amazon is in Chinese

- Chinese language or references are present in the source code of both victim and threat actor facing domains.
- CNServers (CloudRadium) Link: An important pointer is the use of the CNServers (CloudRadium)'s ASN, hosting the fake domains for the most significant amount of time. CNServers LLC is a hosting company based in China. Notably, it has a history of hosting phishing domains related to other cryptocurrency scams in the past.
- **CloudRadium** is connected to major Chinese ISPs and is CN2 (China Telecom Next Generation Carrier Network) optimized networking - use of a dedicated network of servers that are located in China.

The combination of these indicators points towards a potential connection to China in the operation of the scam.

Takeaways

Given the involvement of three distinct parties— General Audience (Potential Victims), Impersonation Targets, and Authorities—our takeaways are divided into three sections, each tailored to provide specific insights for these groups

General Audience: Potential Victims

- Be cautious of job offers received through WhatsApp, as genuine companies seldom use this platform for recruitment; such offers are likely scams.
- The scam's initial appeal often hinges on the promise of quick profits and early withdrawals to build trust—be wary of such tactics.
- Even if the scam's methods evolve in the future, this report contains valuable information to help you avoid falling victim:
 - Scrutinize domain names closely; we've highlighted two common tactics used by scammers to mimic legitimate domains:
 - Appending country codes (e.g., uk, au, sgp); refer to the [Pie Chart](#).
 - Appending generic strings; consult the [table](#) for details.
 - We've compiled a list of WhatsApp numbers and Telegram handles used by scammers; consider blocking these if you receive messages from them.

These takeaways aim to provide the general audience with practical insights to help them recognize and avoid falling for similar scams in the future.

Companies and Impersonation Targets

The immense impact of this scam potentially leading to the loss of millions of dollars in the name of your brand is huge. Innocent victims placing their trust in the brand's reputation makes it imperative to takedown all the domains impersonating your organization:

- **Domain Discovery and Action:** Identify all domains impersonating your organization within this campaign. Swiftly take down each one to dismantle task completion platforms that ensnare victims. Prompt action can mitigate further harm.
- **Proactive Solutions:** Develop a robust system to swiftly detect and counter new fake domains as they arise. A proactive approach to discovering and combating such threats is essential. Notably, CloudSEK's Digital Risk Protection Platform XVigil offers an effective solution through its brand monitoring module.

By adopting these measures, organizations like CloudSEK can not only safeguard your brand reputation but also contribute to thwarting these fraudulent schemes.

Authorities and Countermeasures

- **Tracing Scammer Origins through Job Portals:** Given that the chain could originate from extracting victim information from job portals, it's imperative for authorities to give utmost attention to probing job search and recruitment platforms, such as <https://bestpersonnel.ca/explore-our-jobs>, which victims have cited. Revealing these origins is crucial to proactively counter their efforts and protect potential victims.
- **Collaborative Action:** Recognize the widespread and intricate nature of this scam campaign involving 12 Autonomous System Numbers (ASNs) and 119 associated IP addresses that are present in the report. Collaborate across jurisdictions to formulate a unified approach against these threat actors.
- **Rapid Response Teams:** Establish specialized teams equipped to swiftly investigate and counter such multi-layered scams. Given the scale of this operation, responsive teams can significantly impede the scam's growth and protect victims.
- **Domain Blacklisting:** Enforce domain blacklisting measures to prevent the operation of fraudulent websites. By identifying and blocking domains associated with the campaign, authorities can curb scammers' ability to deceive victims.
- **Seize Assets:** Investigate and seize assets associated with the scam, such as cryptocurrency wallets and financial accounts. Disrupting the financial gains of threat actors can diminish their motivation to continue such fraudulent activities.
- **Educational Campaigns:** Launch awareness campaigns to educate the public about the tactics employed by scammers. Empower potential victims with knowledge to recognize and report fraudulent activities promptly.

Check your Organization's Exposure to the Webworm Campaign

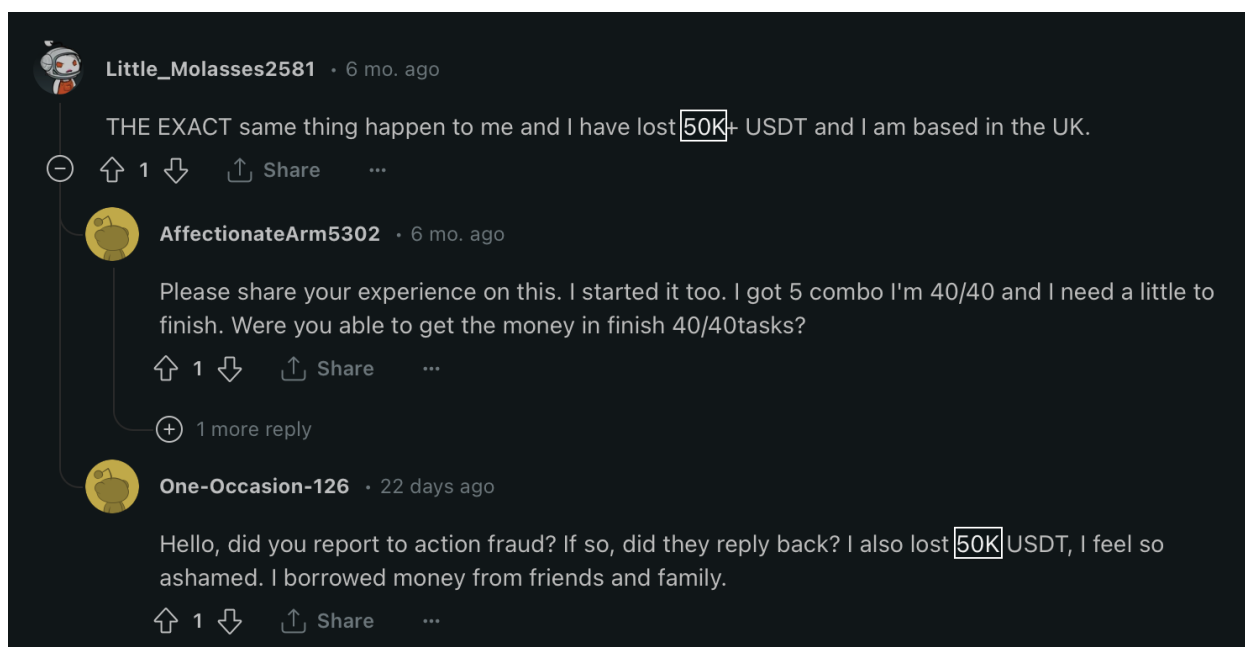
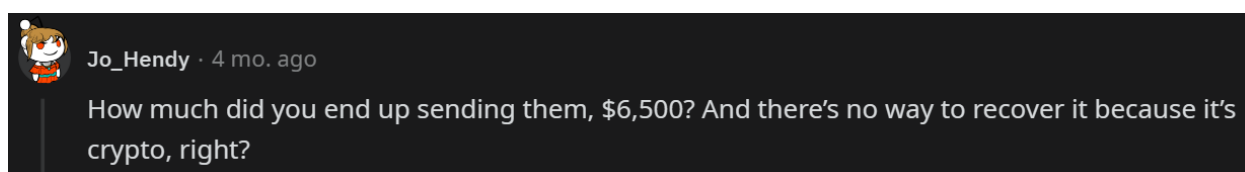
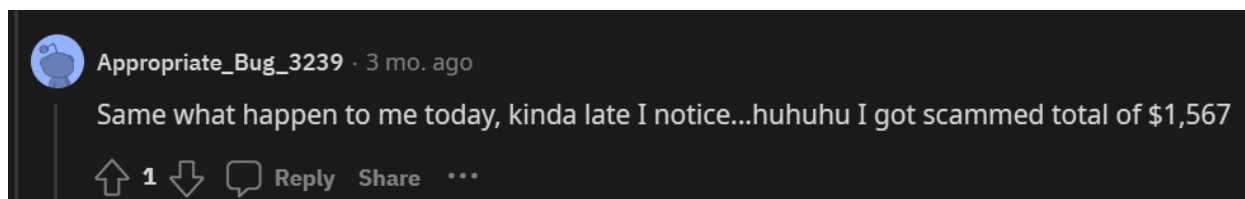
This report, powered by CloudSEK's Fake Domain & Underground Discussions modules, highlights our investigation of the fraudulent Webworm campaign carried out by the Threat Actor group globally (potentially with Chinese origins with a global network).

We had to remove some of the details we were able to obtain for the sake of brevity. These include IOCs - namely the 6000 fake domains, the 12 ASNs, 550 malicious IP addresses, WhatsApp numbers & Telegram Numbers. Should you require these IOCs to check your organization's exposure to the Webworm campaign, do reach out to us by clicking the link below.

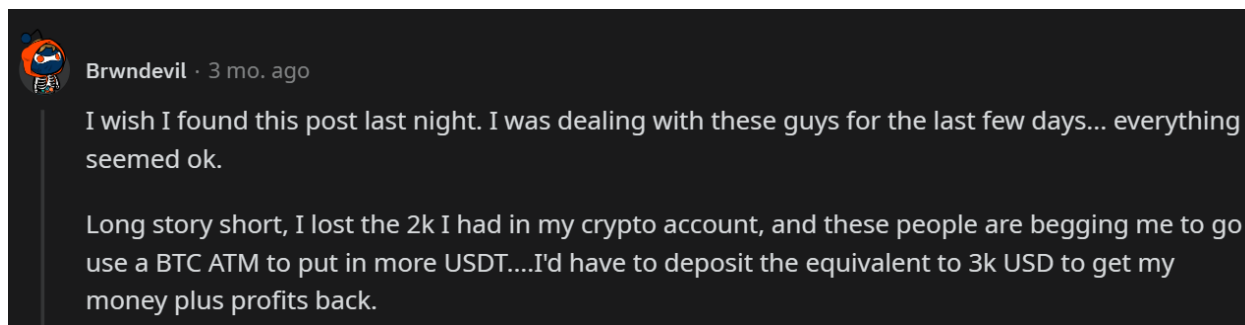
[Fill up a form](#)

Appendix 1 - Victim Grievances

The following screenshots have been sourced from open discussion platforms and comprise victim complaints, explicitly highlighting the total dollar value of the losses they have endured:



Two victims claim to have lost 50k USDT falling prey to the Webwyrms





Over-Set-2715 · 2 mo. ago

Nothing to be ashamed of, I went through the same thing and lost \$5k to them. The best thing you can do is to save others from losing their money.



No-Morning-9009 · 3 mo. ago

I lost 8000 with Cansnowflake

↑ 1 ↓ Reply Share ...



Over-Set-2715 · 2 mo. ago

Same here, I lost about \$5,000 to these guys. Had to borrow money from others thinking I'll get my money back but it's a painful experience. I'm sorry you had to go through that and I was also oblivious/forgot about the whole scam arena as well.



Expensive_Style_7289 · 2 mo. ago

This happened to me too, I lost \$4500 pls tell me what you did.



MotemaMotema · 1 mo. ago

it happened to me too, I lost 11200C\$ to snowflake. exactly how you described them is how they appeared to me, only if I saw this post ealier..... they are very evil people, they made me used all


task which required 7412 USDT to finish the day and withdraw my money. No money is allowed to be withdrawn until you finish all 40 tasks. I was completely out of money at this point, and transferring more was just not feasible.

I tried googling the company "AppTailors" seemed legit.


Today was day 3, started as normal and then I was getting "lucky" by getting 4 "combos" it worked fine, until I got this final "combo" that requested 5000. I am now down £2500. I borrowed money from my partner and family and have no money to feed myself or get to my main job for the month. I'm devastated right now, I don't know what to do. I'm ashamed.

TL;DR I got scammed £2500 by a company because I didn't trust my gut.


 Comment removed by moderator · 4 mo. ago

 Lund-pakora · 4 mo. ago
I have \$8000 usd stuck in there. Can anyone plz help me retrieve my money

 1   Reply  Share ...


 Simplestique · 3 mo. ago
damn, i got \$800 USD stuck in there


 1   Reply  Share ...

 Falcon9_Eyes · 3 mo. ago · edited 3 mo. ago
I have 4000usdt stuck as well in <https://www.cansnowflake.com>

It is scam website.

 1   Reply  Share ...

 Remarkable-End-2987 · 3 mo. ago
Shit man! I wish I had read your story before. It happened the same with me. The difference is that I couldn't go so far with depositing money. I don't have it. Thanks for the teaching. I lost around 2000 dollars.

 Rikanation · 3 mo. ago
This literally happened to me earlier today. I lost \$4100 CAD which is very close to £2500 but instead of AppTailors it was Can-Snowflake.

[Link to the Next Section](#)

Appendix 2 - Appended Strings inside Fake Domains

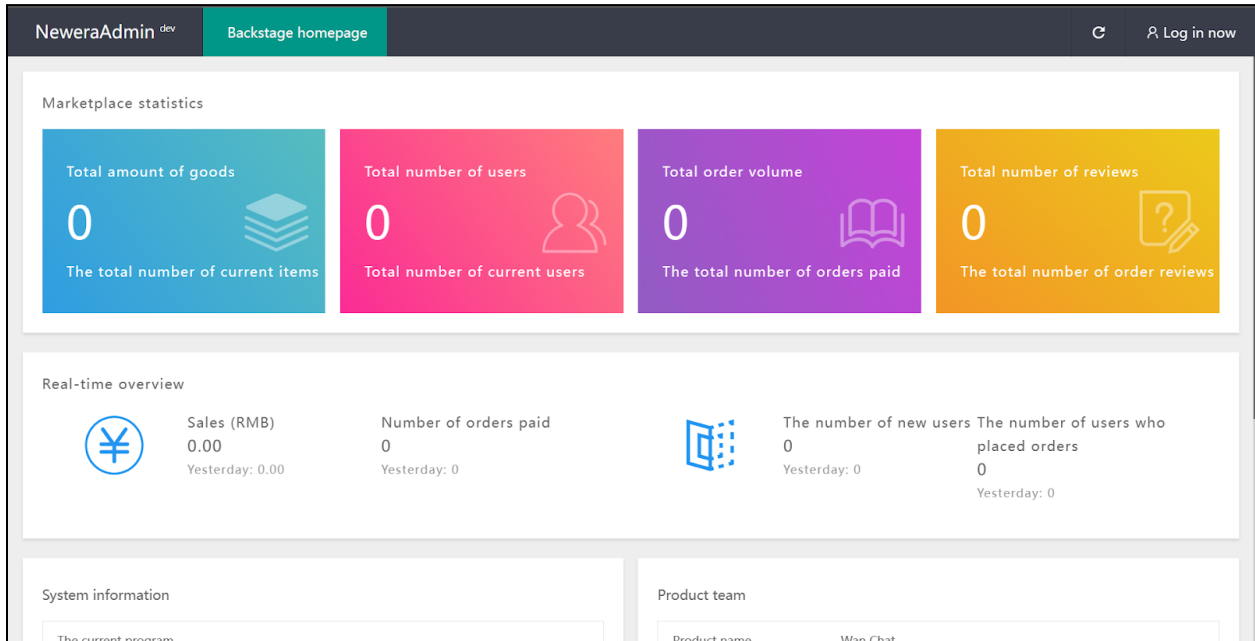
The following table contains 34 appended keywords inside fake domains along with their approximate count:

Appended Strings	Approx Count of Domains	Appended Strings	Approx Count of Domains
app	600	elevate	50
digital	180	enhance	50
grow	170	program	50
aim	150	advance	50
senna	150	network	50
soft/softs/software	140	assign	50
pro	130	overview	40
boost	130	analytic	40
sys/system	120	logical	40
ranks	120	advdrive	40
audit	100	boots	40
drive	100	analyse	30
scale	90	api	10
review/reviews	90	global	10
evolve	80	login	10
revue	75	official	10
summary/summaries	70	good	10

[Link to the Next Section](#)

Appendix 3 - Backend Admin Portal

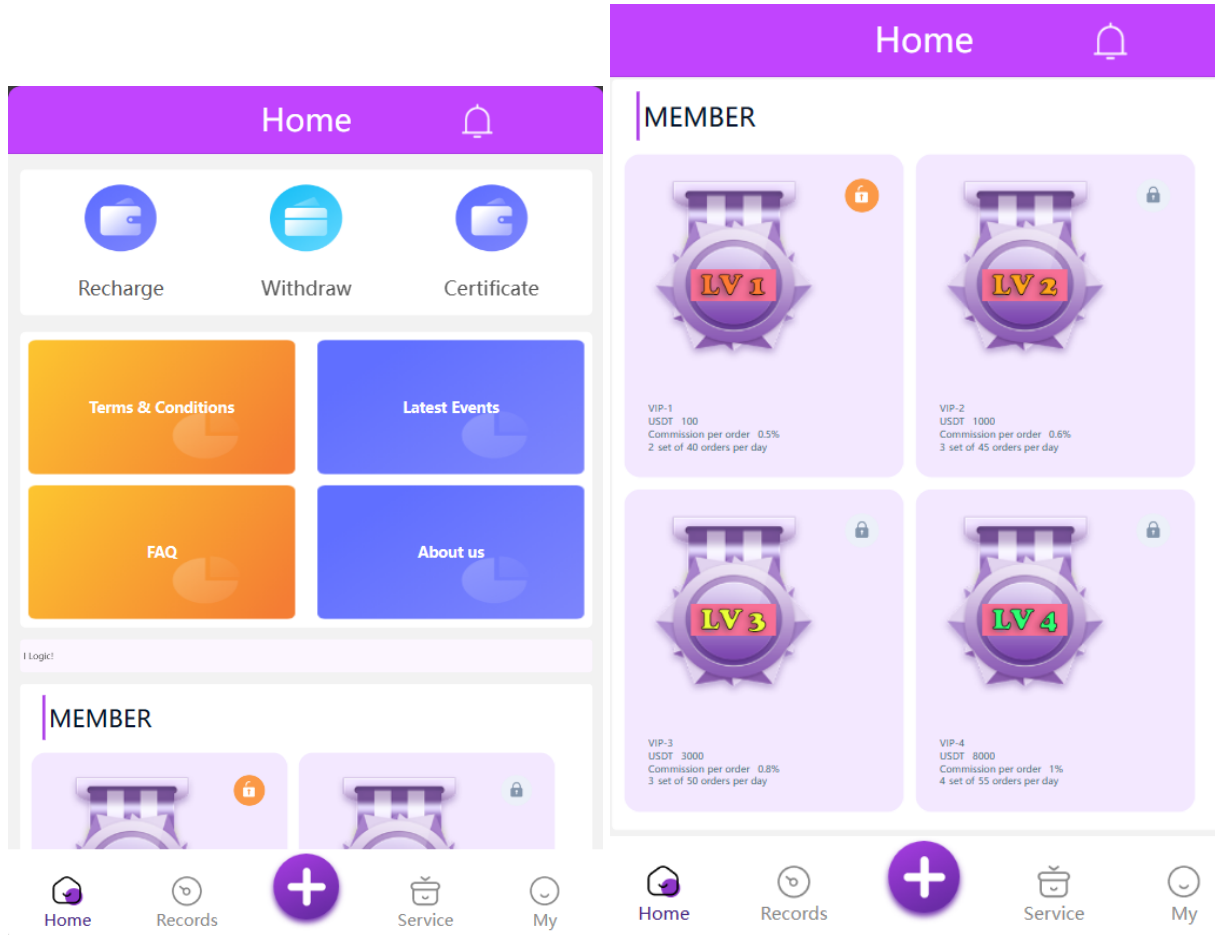
The following screenshot is from the backend Admin portal being used by threat actors to manage the users and their investments:



Snapshot of the backend Admin portal

Appendix 4 - Victim Facing Portal

The following screenshots are from the victim-facing domains where all the tasks are being and financial transactions are being performed:



Snapshot of the victim-facing portal


Records

All Pending Completed Frozen

Remaining available assets(\$)

70.80

Rush time 2023-10-09 15:39:40 success



Mango TV

\$ 22.00x 1

Total order amount	\$ 22.00
Order Commission	\$ 0.11
Expected return	\$ 22.11

Start

Balance

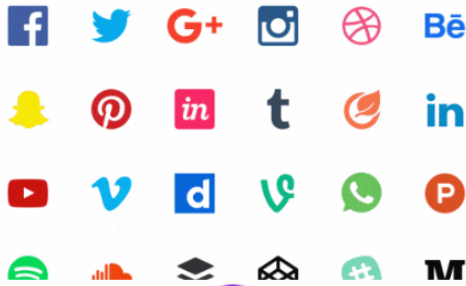
\$70.8


The profits from each application are added to the total assets.

Today's Profit

\$0

The system automatically updates profit data daily






Balance: **\$70.80**


Yesterday's commission	Accumulated Commission	Today's Commission
USDT 0	USDT 3.86	USDT 0

Recharge


Withdraw



Recharge record



Records



Withdraw Log

Snapshot of the victim-facing portal

References

- [Is https://www.can-snowflake.com/#/ part of the snowflake company? : snowflake \(reddit.com\)](https://www.can-snowflake.com/#/)
- [Has anyone run into this company claiming to be snowflake? : snowflake \(reddit.com\)](#)
- [Snowflake Task Scam : Scams \(reddit.com\)](#)
- [can-snowflake.com Review – 4 shocking facts about can-snowflake.com - ScamWatcher](#)
- [Fake Job Scam: App Reviewer - Cybertrace™](#)
- [Fake Job Scam: The App Growth Specialist - Cybertrace™](#)
- [TIFU By getting scammed : tifu \(reddit.com\)](#)
- [Explore Our Jobs - Best Personnel Employment Agency](#)
- [cansnowflake scam site:www.reddit.com - Google Search](#)
- [Cyber slavery starts up in Southeast Asia | East Asia Forum](#)
- [Inside the 'pig-butcher' scams seeing thousands trafficked into cyber slavery - ABC News](#)



We Predict Cyber Threats

Initial Attack Vector Protection Platform

Founded in
2015

200+
CloudSters

2 Offices
HQ in Singapore
and R&D in India

170+
Clients Globally

4
Products

We secure some of the Fortune 500 and Unicorns



... And we are backed by eminent investors



Accelerated by



CloudSEK is a **Customer First** Company

We are a **Gartner Peer Insights Customer First Vendor** for Security Threat Intelligence Products and services.



Gartner Rated 4.5+
peerinsights™



About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats.

At CloudSEK, we combine the power of Cyber Intelligence, Brand Monitoring, Attack Surface Monitoring, Infrastructure Monitoring and Supply Chain Intelligence to give context to our customers' digital risks.



www.cloudsek.com
info@cloudsek.com