SILENT PUSH

2024
YEAR IN REVIEW

TRENDS, INSIGHTS, AND LESSONS LEARNED

TABLE OF CONTENTS

A YEAR IN SUMMARY

2024 marked a transformative year in cyber threat intelligence. Rapidly evolving adversary tactics, increasingly novel malware proliferation techniques, and the widespread availability of artificial intelligence (AI) enabled malicious infrastructure scaling methods have made the jobs of security teams exponentially more challenging worldwide.

Dealing with these threats thus requires a transformative approach. Reactive defense measures are no longer effective, and Indicators of Compromise (IOCs) are stale at best. The industry is turning toward Indicators of Future Attack (IOFAs) to gain actionable threat intelligence that can stop attacks *before* they are weaponized.

In pursuit of that goal, the preemptive cybersecurity intelligence company Silent Push spent 2024 tracking millions of hidden malicious domains and IP addresses, fingerprinting attacker infrastructure—both at scale and as it was built—mapping the impact of critical vulnerabilities spread across the web and working closely with partners to disrupt global threat actor operations.

We delivered world-first, in-depth technical reporting to our customers and produced IOFA feeds setting the gold standard for preemptive threat intelligence. We continue to perfect our rigorously curated, first-party dataset and intuitive threat-hunting platform. At Silent Push, when we say, “We Know First,” – we mean it.

1 INTRODUCTION

From C-suite leaders to hands-on keyboard analysts, Silent Push strives to ensure that the information we provide benefits all our readers. This "Year in Review" white paper contains a mix of technical information and analysis alongside high-level overviews and key trends regarding cyber attackers who have swiftly embraced the rise of AI to scale their operations and become more sophisticated by the minute.

We report the threat landscape as we see and experience it. Delving into some of the technical details behind Advanced Persistent Threats (APTs) pursuing nation-state objectives and major crimeware families focused purely on extracting financial gain, we objectively explore some of the latest emerging threats the security industry is facing. Examining the various malware and malicious infrastructure trends we have observed, we cover our own improvements and contributions in the fight against these threats and provide strategic recommendations for cyber-conscious organizations alongside our predictions for 2025.

The insights powering this paper are built on our proprietary dataset, which represents the most comprehensive view of the internet available anywhere in the world, to map attacker tactics, techniques, and procedures (TTPs) and infrastructure in real time. Our technology enables the tracking and analysis of adversaries' network changes as they occur, stopping them at the gates – before they can get in.

Note: *Operational security requirements prevent us from revealing certain technical details in this and the rest of our public-facing publications. For in-depth analysis of the threats listed herein (as well as many others), access to our industry-defining data, IOFA feeds, and more, please contact our Sales team to see about becoming an enterprise customer.*

2 THE EVER-EVOLVING THREAT LANDSCAPE

SILENT PUSH KEY STATISTICS

We enable organizations to stay one step ahead of emerging threats:

- Hundreds of thousands of Indicators of Future Attack (IOFAs) provided on a constantly recurring basis to organizations worldwide alongside a similar number of indicators in our Bulk Data Feeds.
- Published dozens of blogs and technical reports detailing analysis and mitigation needed to stop activities of multiple APTs and major crimeware groups.
- Collaborated with worldwide partners in law enforcement and the security industry, leading to the disruption and/or takedown of numerous networks and the blocking of countless cyber attacks.
- Continuously expanded our data collection, processing, and fingerprinting capabilities.

TOP THREAT TRENDS

The cybersecurity environment in 2024 experienced rapid escalation in both volume and complexity of cyber threats. Silent Push analysts noted considerable increases in activity driven by both state-sponsored APTs and financially-motivated cybercriminal groups, including a dramatic increase in the sophistication of phishing kits – with new iterations appearing faster than ever before to shift targeting across industry verticals (financial, retail, technology, and energy).

Another trend, one of the most significant in 2024, was the proliferation of AI-powered infrastructure scaling. Threat actors harnessed AI to enhance their spear-phishing campaigns, automate malware development, and obfuscate their infrastructure. The use of generative AI tools has made it easier for adversaries to scale operations and create convincing lures, complicating traditional detection and response efforts.

"Infrastructure Laundering" is a term we coined to describe the growing criminal practice our analysts observed of threat actors intentionally hiding their infrastructure behind large, mainstream providers hosting many otherwise legitimate subscribers. We see it as an increasingly pressing issue.

Our research into Triad Nexus (some of which we covered publicly and will discuss later), combined with insights driven by our unparalleled DNS data, has revealed troubling associations between cybercrime and real-world criminal gangs, most notably Chinese Triad groups.

Threat actors increasingly exploited Cloudflare's proxying services to obscure their infrastructure, effectively concealing the true IP addresses behind their malicious campaigns. This tactic allowed adversaries to add a layer of anonymity and resilience to their operations, complicating efforts to identify and disrupt their hosting environments. Silent Push's research utilized advanced unmasking techniques to reveal the real IPs behind proxied domains, enabling organizations to uncover hidden infrastructures and preemptively defend against these sophisticated threats.

Exemplified by actors like Raspberry Robin, that facilitated human-operated ransomware campaigns by providing compromised infrastructure to other threat groups, "Access-as-a-Service" models have continued to grow in prominence. These services streamlined the ability of less sophisticated actors to execute high-profile attacks, further diversifying the threat landscape. They also have worrisome ties to Russian threats that the industry should keep in mind when defending against them.

RASPBERRY ROBIN

Raspberry Robin evolved from its initial discovery in September 2021 as a highly prevalent worm with little post-compromise activities to a key player in Access-as-a-Service operations.

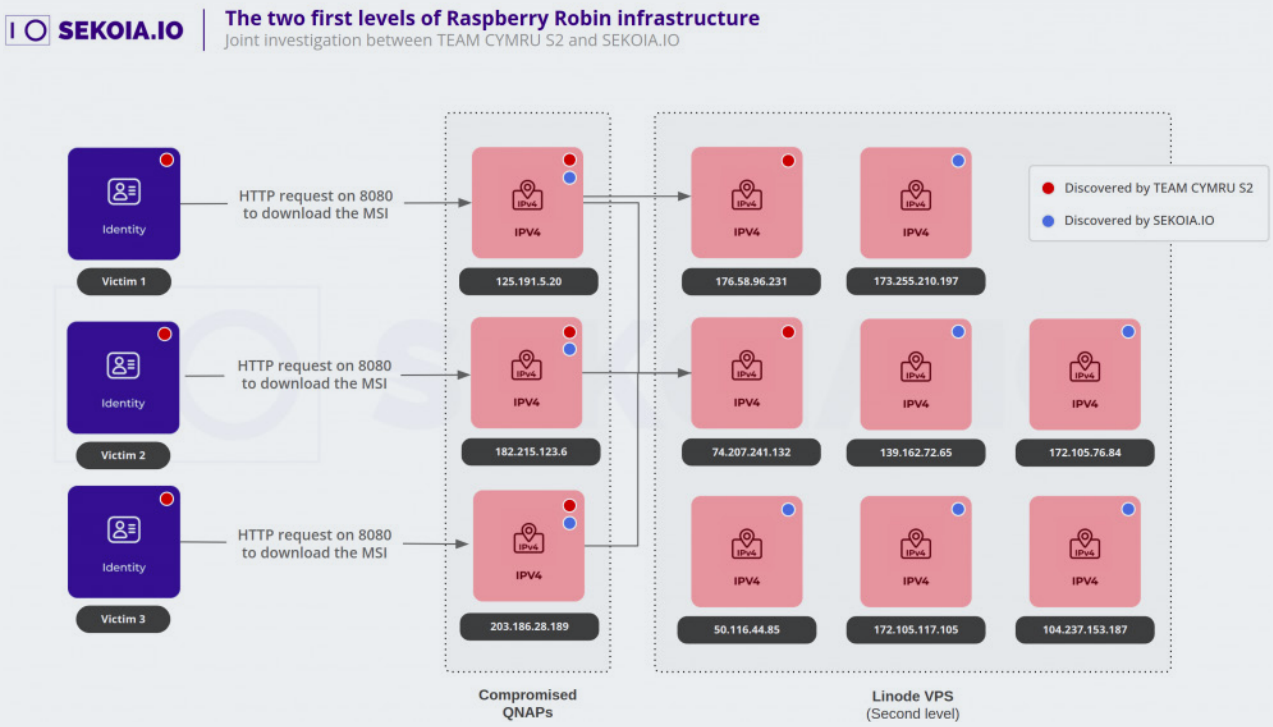
Originally spread via USB drives, the worm's payloads evolved to more traditional methods that utilize file-sharing websites and various victim-targeted lures. Once infected, victim devices connect to compromised QNAP NAS devices whose IP addresses are mapped via DNS A Records to short, two- and three-letter domains on niche domain suffixes, that act as command and control (C2) servers. Raspberry Robin is one of the most significant initial access brokers (IABs) operating today.

Silent Push researchers uncovered Raspberry Robin domains by identifying key nameservers, naming conventions, and a combination of IP and autonomous system number (ASN) diversity patterns. This led to the discovery of more than 180 unique Raspberry Robin C2 domains and allowed us to continue to track their infrastructure through 2024.

In 2023, there was a partial disruption of Raspberry Robin due to approximately 30% of their domains being registered via Namecheap. In 2024, Silent Push analysts uncovered data showing that new Raspberry Robin domains were registered with more unique registrars, many in Asia and thus likely not so receptive to takedown requests. Their top 8 registrars through 2024 were:

1. Sarek Oy
2. NETIM
3. Epag[.]de
4. CentralNic Ltd
5. eName Technology Co., LTD.
6. TLD Registrar Solutions LTD
7. Hefei Juming Network Technology Co.
8. Sarek

In 2023, Sekoia analysts worked with Team Cymru to map the NetFlow of Raspberry Robin infrastructure. They found a diversity of second-level panels being used to communicate with the compromised QNAP devices:



NetFlow map of Raspberry Robin infrastructure

In 2024, Silent Push analysts worked with Team Cymru on a similar analysis using our new data. We were able to confirm the Raspberry Robin threat actors have a new setup that relies on a singular data panel/relay to connect to the compromised QNAP devices. They are still heavily using Tor Relays, but this new NetFlow data pointed to a potential singular point of failure and a collection opportunity for law enforcement. For those reasons, we redacted the IP address but can share a chart of the current architecture:

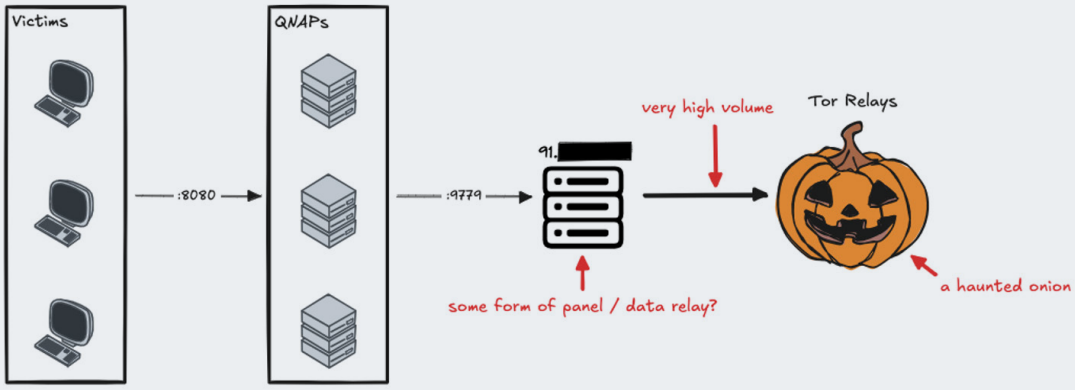


Chart of current Raspberry Robin architecture

In September 2024, CISA released the "Russian Military Cyber Actors Target US and Global Critical Infrastructure" report that highlighted the Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) has been using Raspberry Robin as an IAB.

This alarming fact about Raspberry Robin being used by Russian government threat actors aligns with their history of working with other serious threat actors, many with connections to Russia, including LockBit, Dridex, SocGholish, DEV-0206, Evil Corp (DEV-0243), Fauppod, FIN11, Clop Gang, and Lace Tempest (TA505).

3 ADVANCED PERSISTENT THREATS (APTS)

STATE-SPONSORED APT GROUPS

The primary point of concern for governments, organizations, and critical infrastructure managers is state-sponsored APT groups that continue to pose a significant challenge to global cybersecurity. APTs remain a driving force behind the evolution and innovation of cyber threats. Their actions often pave the way for less sophisticated threats to imitate.

Collaboration across organizations, governments, and security providers is essential to mitigate APT groups' impact. Silent Push's focus on mapping adversary infrastructure before weaponization and sharing actionable intelligence underscores the critical need for preemptive threat intelligence in combating these persistent, sophisticated actors.

This section covers a few groups we tracked in 2024, namely APT 28 (Fancy Bear), APT 43 (Kimsuky), and Sapphire Sleet, that have operated with surgical precision throughout the year, targeting individuals and organizations involved in finance, technology, and government across multiple regions.

Note: *For the same operational security concerns mentioned before, which are only enhanced for high-profile threats backed with significant state resource pools, technical details and analysis of our reach into most APT groups are restricted to reports only available to our enterprise customers. Contact our Sales team for more information on how to access this crucial intelligence.*

APT28 (FANCY BEAR)

APT28 (also known as Forest Blizzard, Fancy Bear, and many other names) is a long-running APT group linked to Russia's military intelligence agency GRU. The group continues to be active, with public reporting discussing campaigns targeting countries in Europe and Central Asia using the HATVIBE HTML loader and CHERRYSPY custom python backdoor.

Silent Push was able to pivot on and generate fingerprints from publicly-mentioned CHERRYSPY domains within our platform. This enabled us to find more C2 domains than those currently being reported, and we are actively tracking new IOFA domains from this threat as they are registered.

KIMSUKY (APT43)

Kimsuky (also known as APT43, Black Banshee, Emerald Sleet, TA427, THALLIUM, and Velvet Chollima) is an APT group originating from North Korea that has been active for more than a decade. They are known for cyber espionage and targeting victims in countries including Japan, South Korea, and the U.S.

Considerable effort and persistent analysis led Silent Push Threat Researchers to find hundreds of Kimsuky domains that aligned closely with those involved in previous attacks.

Note: *Due to operational security concerns, the IOFA feeds containing those domains and IPs, others we fingerprinted to pre-emptively track Kimsuky infrastructure before it could be weaponized, and the accompanying technical report on their methods of operation, are currently only available to our enterprise customers.*

SAPPHIRE SLEET

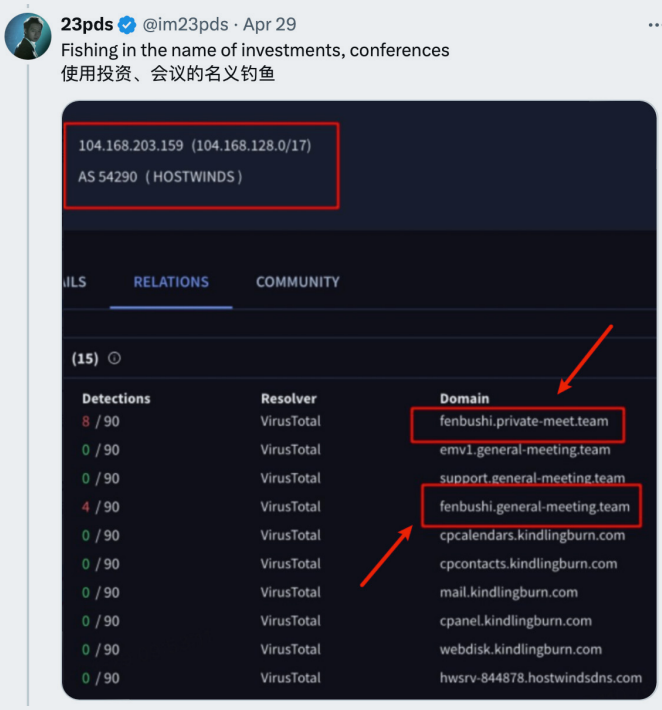
Sapphire Sleet is a sub-group of the North Korean-affiliated and state-sponsored Lazarus group, active since the first quarter of 2020. Specializing in financial heists and cyber espionage, Sapphire Sleet primarily targets individuals and organizations operating in cryptocurrency exchanges, venture capital, blockchain, and other next-generation technology sectors.

The cluster is known for heavily relying on spear-phishing and social engineering as their initial attack vector, posing as employees of legitimate organizations on LinkedIn and using job openings and collaboration opportunities as lures.

During 2024, the attackers launched numerous campaigns impersonating EU, U.S., and East Asian-based organizations on Linkedin in an attempt to fool victims into following a virtual meeting invite. The meeting URL redirected unsuspecting victims to an attacker-controlled, password-protected website serving malware designed to steal their cryptocurrency and intellectual property related to cryptocurrency technology.

2:57 AM · Apr 29, 2024 · **12.8K** Views

Screenshot warning of Sapphire Sleet fake Fenbushi Capital post on LinkedIn



Second screenshot alerting of the scam

EVASION TECHNIQUES

Silent Push researchers analyzed several Sapphire Sleet attacks that occurred in 2024 and identified evasion techniques enforced by the group that were previously unreported:

- Registered domains with generic names, usually including the meeting-related keywords
- Bulk-registered domains with similar names but with different top-level domains (TLDs)
- Apex domains pointed to the shared IP address of a reputable service, usually on Namecheap
- Infrastructure that was aged for many months before use
- Right before the attack, the threat actor:
  - Created wildcard DNS records pointing to low-density attacker-controlled IP addresses, usually on U.S.-based hosting provider Hostwinds (AS54290)
  - Created wildcard SSL certificates
  - Sent subdomains to victims, usually with the targeted/impersonated organization's name

These findings led to the discovery of hundreds of high-confidence domains, as well as the identification of organizations targeted by Sapphire Sleet.

4 FINANCIALLY-MOTIVATED THREAT ACTORS

For the majority of organizations, financially-motivated threat actors (also known as major crimeware groups) dominated the cyber threat landscape during 2024. Employing increasingly complex tactics against their targets, groups including FIN7, Scattered Spider, CryptoChameleon, and others exemplified the evolution of crimeware, showing a significant willingness to pivot and innovate while combining traditional methods such as phishing and malware delivery with advanced infrastructure management methods.

FIN7, for instance, utilized AI-driven social engineering campaigns and deepfake lures. Scattered Spider leveraged Evilginx proxies and rapidly deployed phishing kits to breach high-value targets. CryptoChameleon constantly shifted its campaigns to thwart the publications of threat researchers tracking them. Silent Push research highlights these actors' reliance on diverse infrastructure, including the use of bulletproof hosting (BPH), suspect registrars, and other techniques.

Remaining one of the most persistent and damaging adversaries to organizations worldwide, financially-motivated threat actors and their ability to quickly scale operations and exploit vulnerabilities have led to widespread ransomware attacks, credential theft, and fraud. Collaborative efforts between organizations and threat intelligence providers, such as Silent Push's work in mapping malicious infrastructure and disrupting criminal networks, have proven essential in mitigating the financial and reputational damage caused by these groups. The need for preemptive intelligence and rapid-response capabilities has never been greater since these adversaries continue to adapt and innovate at an alarming pace.

Note: *For the same operational security concerns mentioned before, which are only enhanced when discussing threats backed with their own ill-gotten gains, the technical details and analysis of our reach into most APT groups are restricted to reports only available to our enterprise customers. Contact our Sales team for more information on how to access this crucial intelligence.*

FIN7

In 2024, Silent Push analysts received a valuable lead from one of our partners about FIN7 using shell websites to age domains.

Since our initial FIN7 public report, we tracked over 5,000 domains and focused considerable efforts on finding new campaigns being launched through these websites.

Some of the findings from the original report include:

- FIN7-related attacks resurfaced a year after the DOJ claimed victory
- Prominent global brands targeted, including Reuters, Meta, and Microsoft
- "Requires Browser Extension" malware reappeared in the wild
- From a single origin point, Silent Push Threat Analysts uncovered an extensive series of FIN7 campaigns, including several hundred active phishing, spoofing, shell, and malware delivery domains and IPs targeting the following organizations: Louvre Museum, Meta, Reuters (and WestLaw), Microsoft 365, Wall Street Journal, Midjourney, CNN, Quickbooks, Alliant, Grammarly, Airtable, Webex, Lexis Nexis, Bloomberg, Quicken, Cisco (Webex), Zoom, Investing[.]com, SAP Concur, Google, Android Developer, Asana, Workable, SAP (Ariba), Microsoft (Sharepoint), RedFin, Manulife Insurance, Regions Bank Onepass, American Express, Twitter, Costco, DropBox, Netflix, Paycor, Harvard, Affinity Energy, RuPay, Goto[.]com, Bitwarden, and Trezor.
- Software being targeted includes 7-zip, PuTTY, ProtectedPDFViewer, AIMP, Notepad++, Advanced IP Scanner, AnyDesk, pgAdmin, AutoDesk, Bitwarden, Rest Proxy, Python, Sublime Text, and Node[.]js.
- Silent Push Threat Analysts also identified an active cybersecurity shell company – cybercloudsec[.]com – that is being used to facilitate FIN7 activity in line with previous attack vectors.

FIN7 SHELL DOMAINS MORPHING INTO PHISHING WEBSITES

A common FIN7 TTP is to take shell domains and morph them into conventional spoofing websites (via redirects or on-page content), targeting users of well-known brands with phishing and malware delivery.

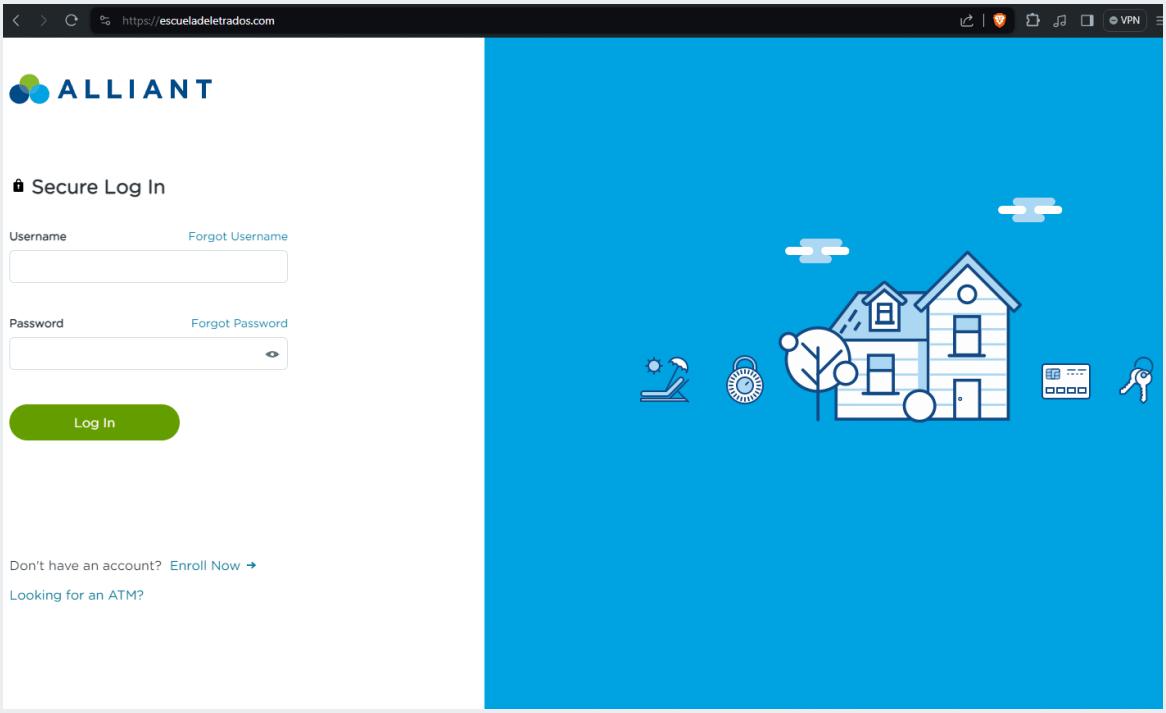
From our analysis, content is served based on a range of user-specific parameters. Domains may populate based on geographic region, IP address, local time, type of connection, or browser settings (such as JavaScript being enabled).

MORPHED DOMAIN (ALLIANT)

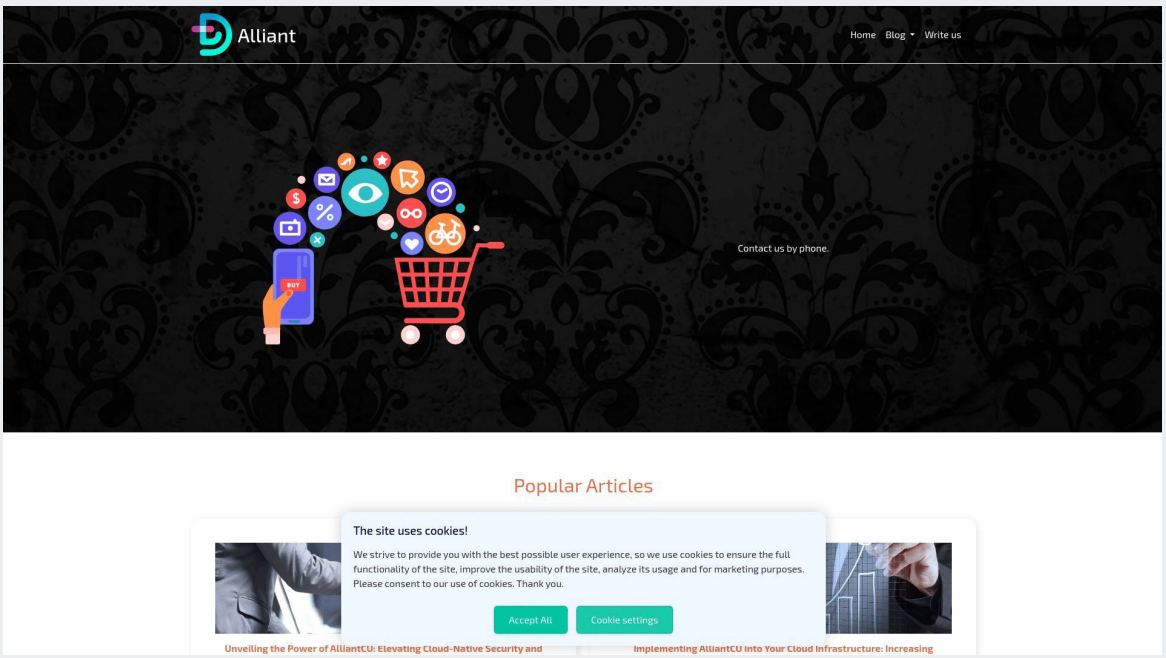
The domain **escueladeletrados[.]com** was accessed on June 9, 2024, via a browser session behind a VPN.

At one point, the domain presented as a **shell website**, however when accessed live with a different set of user parameters, it returned a **phishing page** targeting Alliant Credit Union.

Here are the two different versions of the same domain:



escueladeletrados[.]com as an Alliant phishing page on June 9, 2024

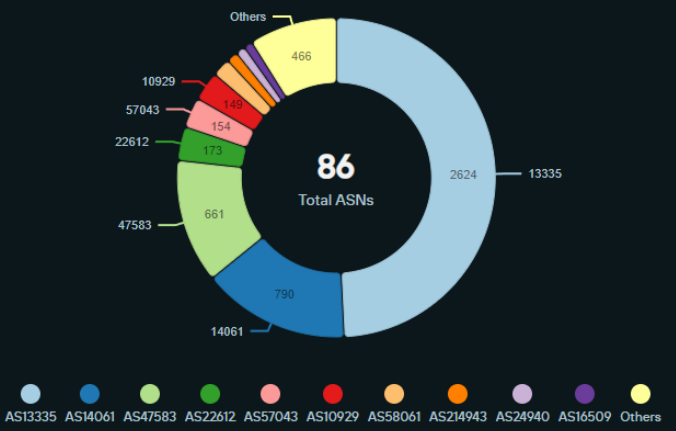


escueladeletrados[.]com as a shell domain on June 9, 2024

Analysis of the domains used in this campaign indicates a high level of diversity with domain structure, hosting locations, and registrars.

Top ASNs

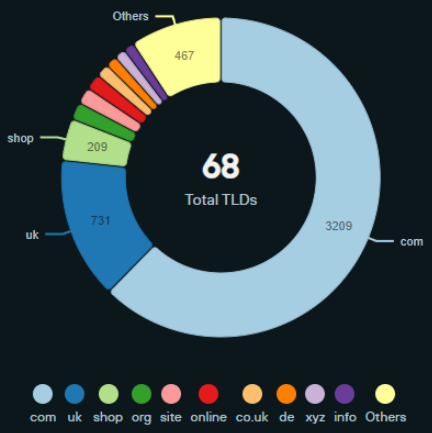
Top 10 ASNs with the highest number of indicators



86 ASNs were used across the current FIN7 infrastructure

Top TLDs

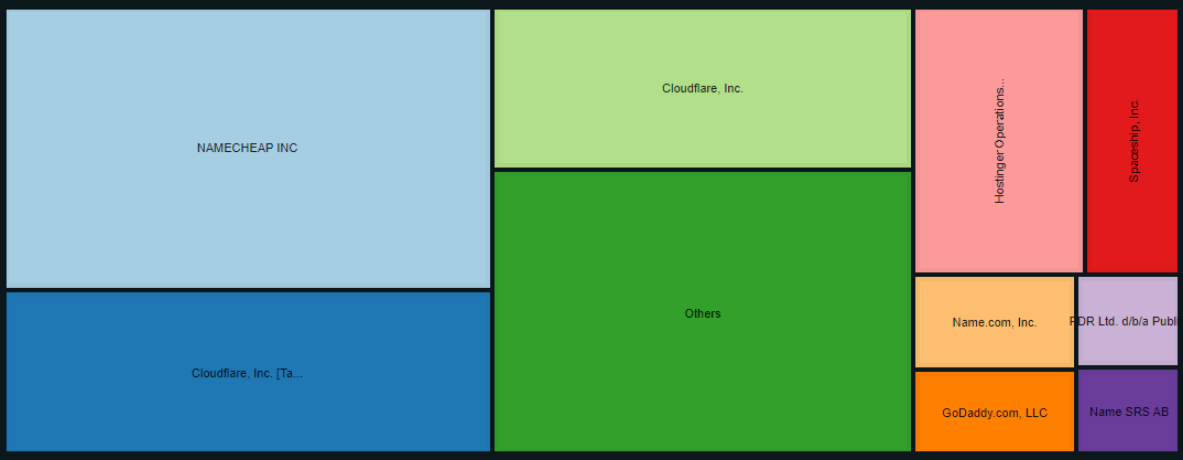
Top 10 TLDs with the highest number of indicators



68 TLDs were used with the majority on ".com" and the second most popular via ".uk"

Top Registrars

Top 10 Registrars with the highest number of indicators



10 Registrars were used by FIN7 across their shell websites for aging domains, with Namecheap being the most popular

STARK INDUSTRIES & SILENT PUSH TAKEDOWNS

During our FIN7 investigation, we reported some of the dedicated infrastructure to Stark Industries. Within hours, not only had the IPs been taken down, but we received a report with additional details about hosts that FIN7 controlled.

Throughout 2024, Silent Push has continued to look for opportunities to share leads with Stark Industries, as we've found them to be an extraordinary partner for taking down infrastructure and sharing leads back about other hosts controlled by the threat actor.

THE COMM - SCATTERED SPIDER & CRYPTOCHAMELEON

Scattered Spider and CryptoChameleon are both part of "The Comm" – a loosely organized group of threat actors, with many based in the West and the U.S., that includes many individuals in their early 20s with one member as young as 17. Over the past few years, both Scattered Spider and CryptoChameleon have been involved with numerous high-profile financial attacks, resulting in several of the members being arrested.

Throughout 2024, Silent Push analysts received private briefings and sensitive details from our research-sharing partners about The Comm, and we were excited to see EclecticIQ publicly publish an article in September 2024, "Ransomware in the Cloud: Scattered Spider Targeting Insurance and Financial Industries." This article was the first to publicly explain there is a "Developer-as-a-Service" (DaaS) group called "Telecom Enemies," aka "Telecom Clowns," that is building tools used by The Comm.

The tools being developed by Telecom Enemies include "Gorilla Call Bot," which is used for voice phishing campaigns and abuses Google Voice. The group has also developed a tool called "Suite's (all in one) AIO" used for creating phishing pages.

The AIO product includes phishing templates for Coinbase, Gemini, Kraken, Binance, Robinhood, OKX, Trezor, Ledger, Exodus, MetaMask, Trust Wallet, Bitwarden, LastPass, Yahoo!, AOL, Microsoft/MSN, Gmail, and iCloud. Both Scattered Spider and CryptoChameleon have targeted the companies listed.

Our team at Silent Push believes the AIO product is one of the strongest connections between Scattered Spider and CryptoChameleon. This further highlights that many members of The Comm are "script kiddies" who use the attack methods but often do not code directly themselves.

It appears Njalla and Virtuo have become preferred hosting providers for the group in combination with the registrar NiceNIC.

We decided to examine all domains hosted and registered on these services, looking for any names that included characteristic Scattered Spider keywords or typosquat domains featuring the companies mentioned above with new keywords.

DOMAINS SEARCH PARAMETERS:

- nsname = *.my-ndns.com
- asnum = 399486;39287
- first_seen_min = 2024-08-01

As we analyzed the results, we noticed that the response returned mainly:

- Additional **Scattered Spider** domains
- **CryptoChameleon** domains

Our team has continued to see patterns between Scattered Spider and CryptoChameleon infrastructure, and we believe our internal findings align with other external research. The Comm may have unique subgroups within it, but shared strategies, code, and attack targets extend across those groups.

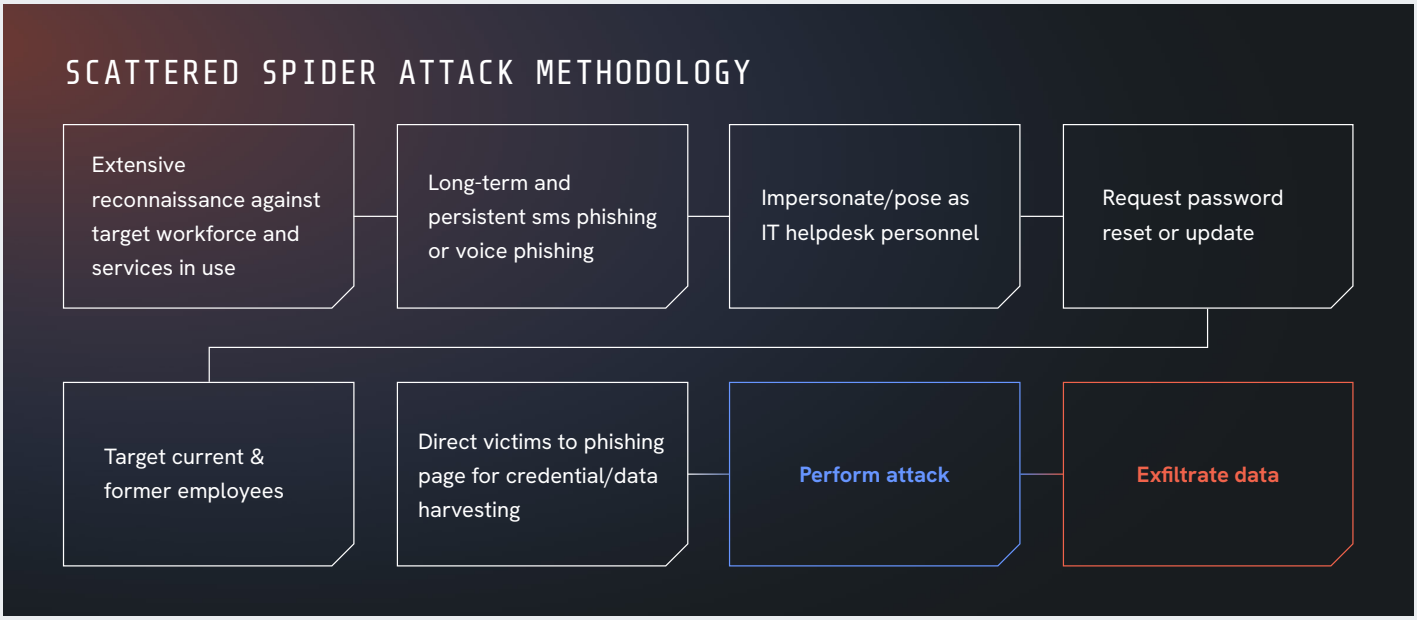
Examining Scattered Spider and CryptoChameleon's activity in greater detail:

SCATTERED SPIDER

Since the second quarter of 2022, Scattered Spider has been an active, financially-motivated hacker collective known for launching hundreds of sophisticated social engineering attacks.

The group's disruptive incidents, such as data exfiltration, extortion, and ransomware, affected organizations from a wide range of industries, including technology, telecom, BPO, financial, insurance, entertainment, retail, and gaming.

In 2024, Silent Push analysts discovered over 350+ new high-confidence indicators attributed to this threat actor, using new and more sophisticated techniques to target over 130 organizations, primarily located in the U.S. and Europe.



Scattered Spider's attack methodology

ATTACK METHODOLOGY

Scattered Spider operators have consistently impersonated help desk personnel, requesting that the targeted organization's employees update or reset their passwords as an initial attack vector.

Targeted employees are directed to a phishing page crafted to mimic their organization's legitimate page, usually hosted on an attacker-controlled domain with the company's name or a typo-squat, a specific keyword, and the TLD ".com" or ".net" including:

- hr
- api
- auth
- cdn
- corp
- corporate
- heip
- help
- helpdesk
- hub
- internal
- my
- okta
- plus
- secure
- servicenow
- sevicedesk
- socure
- sso
- support
- vpn
- workspace
- zendesk

The phishing pages were hosted on the domains 5 to 10 minutes after being registered but never for more than a couple of hours. The domains were usually abandoned after the attack, being parked or taken down by the registrars.

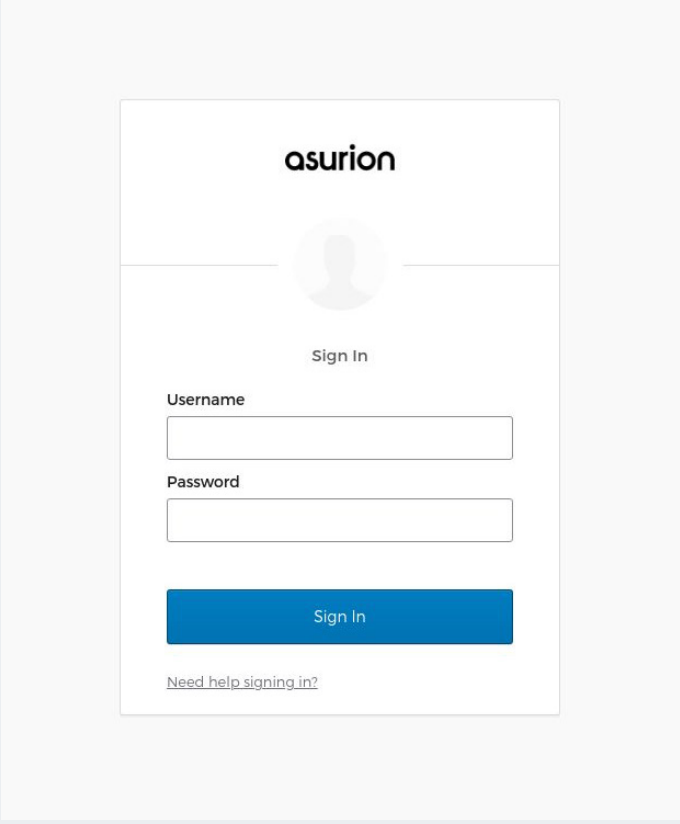
The threat actor tended to register multiple domains during the same day, targeting a particular organization or several organizations that operate in the same business sector.

PHISHING PAGES

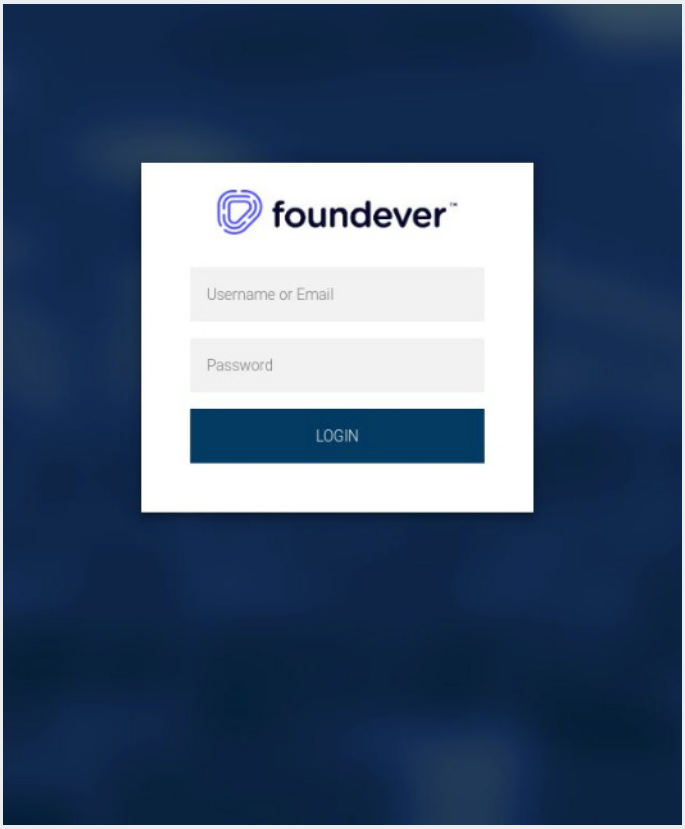
In 2024, Silent Push analysts identified hundreds of phishing pages attributed to Scattered Spider, which were crafted from a total of five phishing kits. The majority of them were first seen in 2024, and some phishing kits were used simultaneously. Despite visual similarities, the phishing pages from the different kits had distinct source codes and used different libraries.

The latest phishing kit deployed by the group, first detected in September 2024, featured phishing pages with HTML code that called to the **init.js** Javascript script.

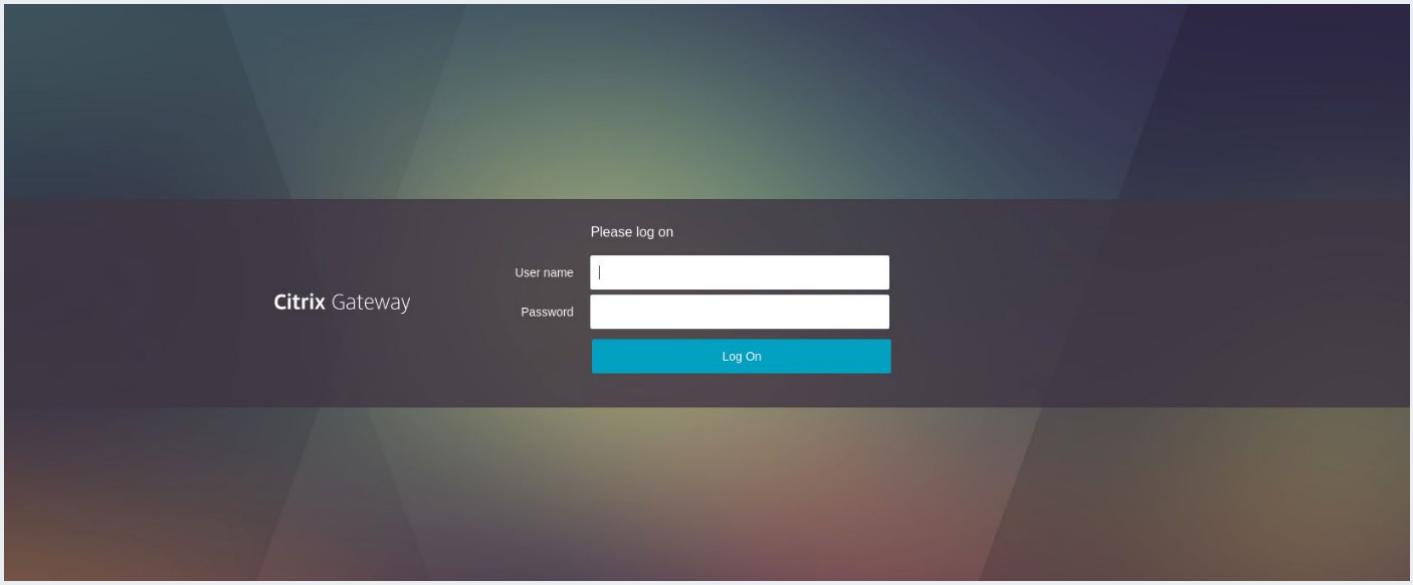
```
<!DOCTYPE html>
<html>
   <script src="/static/js/init.js"></script>
</html>
```



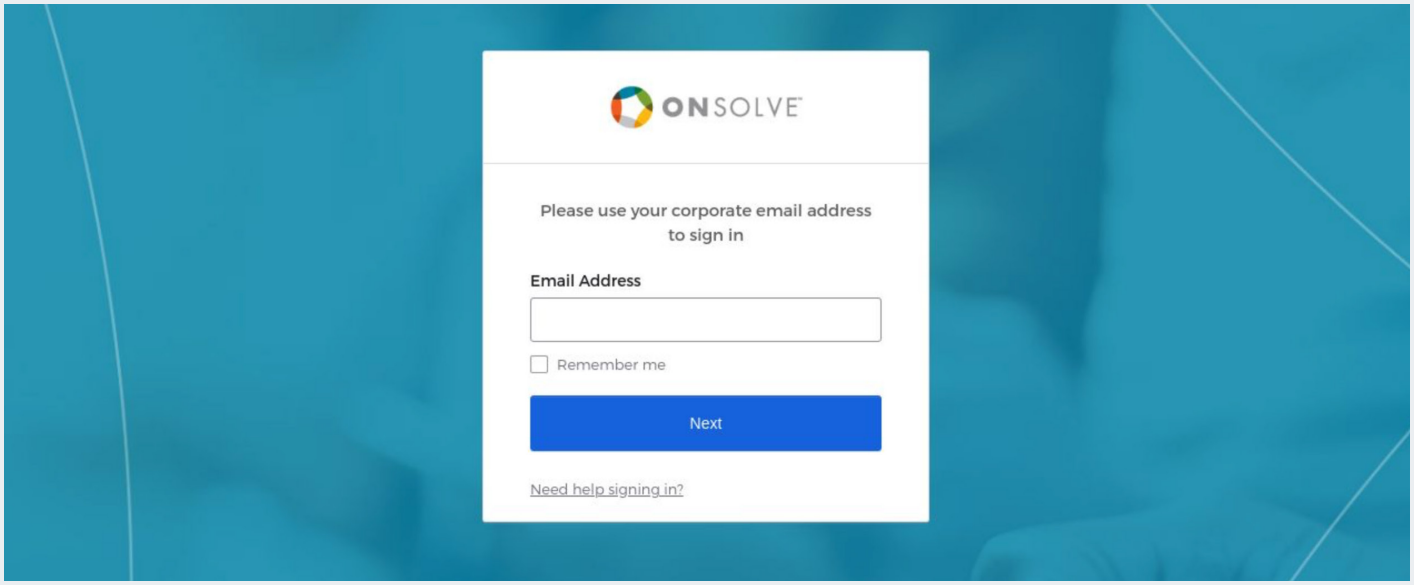
Phishing page 1



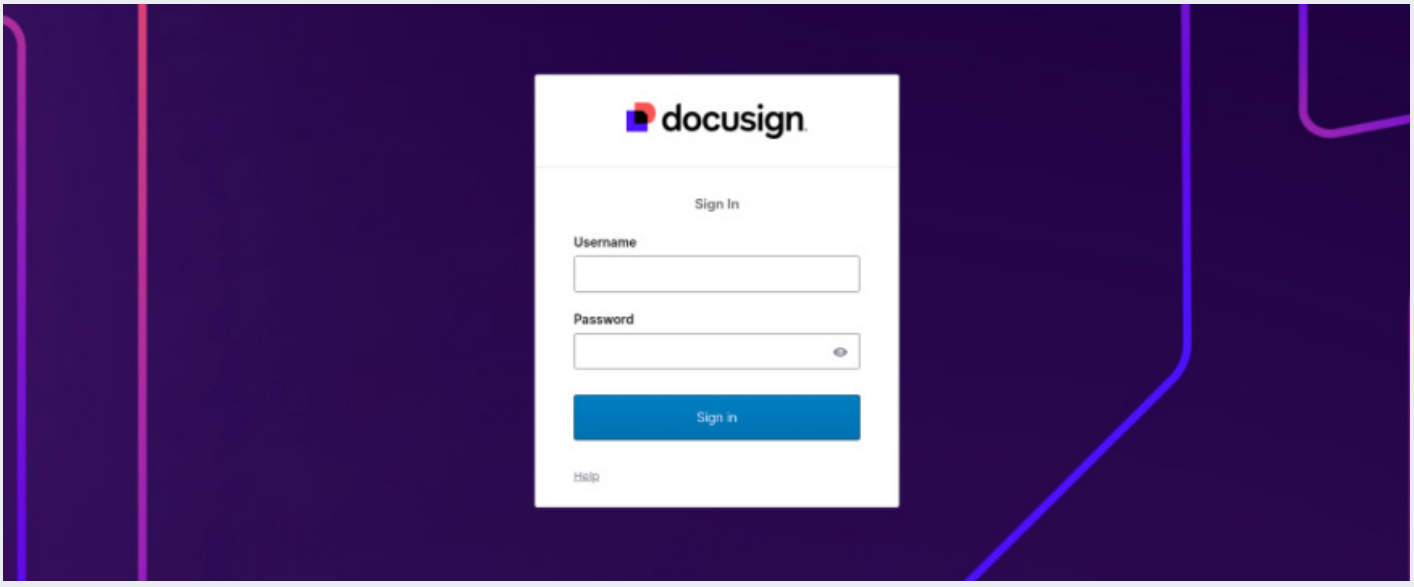
Phishing page 2



Phishing page 3



Phishing page 4



Phishing page 5

REGISTRARS AND HOSTING PROVIDERS

Despite the change in phishing kits, Scattered Spider operators made few changes to the naming pattern used in the domains sent to the victims over the past year. They have also consistently used a set of registrars and hosting providers to acquire and serve their malicious infrastructure.

Scattered Spider has consistently rented servers from different hosting providers. Many of its IPs are on DigitalOcean AS, Vultr AS, and BLNWX AS. The last AS is owned by BitLaunch, a service that provides anonymous virtual private servers (VPS). These are from its dedicated servers, but it also sub-rents servers on DigitalOcean and Vultr. It's likely that the group is getting all its distinct servers from BitLaunch.

The group consistently registered its domains on Hostinger, Hosting Concepts, Namecheap, GoDaddy, or NameSilo. However, toward the end of the first quarter of 2024, the majority of domains were registered on NiceNIC, and the operator began renting dedicated servers on other bullet-proof, lenient, or privacy-focused hosting providers such as Virtuo and Njalla.

LAST QUARTER OF 2024:

- **Registrar:** NiceNIC
  - Used since Q2 2024
  - Many domains registered after Q2 2024 were created through this service
- **Hosting Provider:** Njalla and Virtuo
  - Virtuo was last used in October 2024
  - Njalla was last used in November 2024

REUSE OF DEDICATED SERVERS

Analyzing historical DNS records of one of the IP addresses hosting a domain created in 2024 (onsolve-okta[.]com), revealed it also hosted a domain used in initial attacks of 2022 (tmobile-okta[.]com).

Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	Type
onsolve-okta.com	-	149.28.110.16	20473	2024-02-06 16:23:56	2024-09-15 13:02:48	A
tmobile-okta.com	-	149.28.110.16	20473	2022-05-31 19:59:28	2022-05-31 19:59:28	A

Analyzing information on onsolve-okta[.]com revealed it also hosted a domain used in 2022 attacks

ADVANCED TOOLS - EVILGNIX

While monitoring domains that triggered Silent Push's Scattered Spider sensors, our analysts noticed some domains had their apex domain serving a malicious page crafted from one of the phishing kits, and their subdomains redirected to the RickRoll prank video.

scan_date	origin_url	origin_hostname	origin_ip	htmltitle	favicon_icons
2024-05-16T00:04:38Z	http://login.securian-hr.com	login.securian-hr.com	137.220.43.146	Rick Astley - Never Gonna Give You Up (Official Music Video) - YouTube	
2024-05-16T06:42:31Z	https://securian-hr.com	securian-hr.com	137.220.43.146	CMS Dashboard Login	

Some subdomains redirected to the RickRoll prank video

The team noticed some of these "RickRoll" domains appeared to be serving pages with the HTML title "Log In to your Okta org."

Analysis of other fields returned in the webscan response revealed the domains weren't serving an Okta phishing page but were instead proxying the real login.okta[.]com page and working as a man-in-the-middle (MitM) attack, intercepting the inserted data.

This was determined by noting that the header[.]server value was AmazonS3, and the ETag of the page matched the ETag of the resource served from login.okta[.]com.

It appears Scattered Spider operators started using the Evilginx framework in 2024. Reading its documentation, we saw one of the tool's evasion techniques from automated scanners was redirecting to the RickRoll video, and the subdomains pattern was featured in many publicly available Okta phishlets designed for Evilgnix.

ADVANCED TOOLS - MALWARE

Our analysts observed a subset of potential, high-confidence domains registered consecutively in May 2024, targeting brands such as Namecheap and Telnyx, both organizations that the hacker collective had impersonated in previous attack waves. Additionally, all domains followed the same name pattern: <targeted_company>-cdn[.]com

The webscan record revealed some of these briefly had an open directory, which we accessed, extracted the malicious file, and analyzed it.

The webscan record revealed some of the domains briefly had an open directory

CRYPTOCHAMELEON

CryptoChameleon is a phishing kit first discovered in February 2024. When Silent Push first published about this threat, we didn't have complete clarity regarding who specifically was behind it. Soon after publication, we heard from trusted research partners who shared significant additional details and helped us connect this group to members of The Comm.

Our research soon revealed many IOFAs for CryptoChameleon Fast Flux infrastructure targeting Binance, Coinbase, and FCC users and a host of other platforms, including:

- Apple iCloud
- Google
- Gemini
- Kraken
- Gamdom
- Ledger
- Swan Bitcoin
- Trezor Hardware Wallet
- Uphold
- Nexo Crypto
- Shake Pay Crypto

The genesis of our CryptoChameleon investigation came from a surprising source. On February 6, 2024, Silent Push analysts noticed malicious activity targeting the FCC and reported it confidentially to CISA.

Subsequent research, published by cloud security vendor Lookout, referenced the same domain as our FCC report, which we now know to be CryptoChameleon infrastructure.

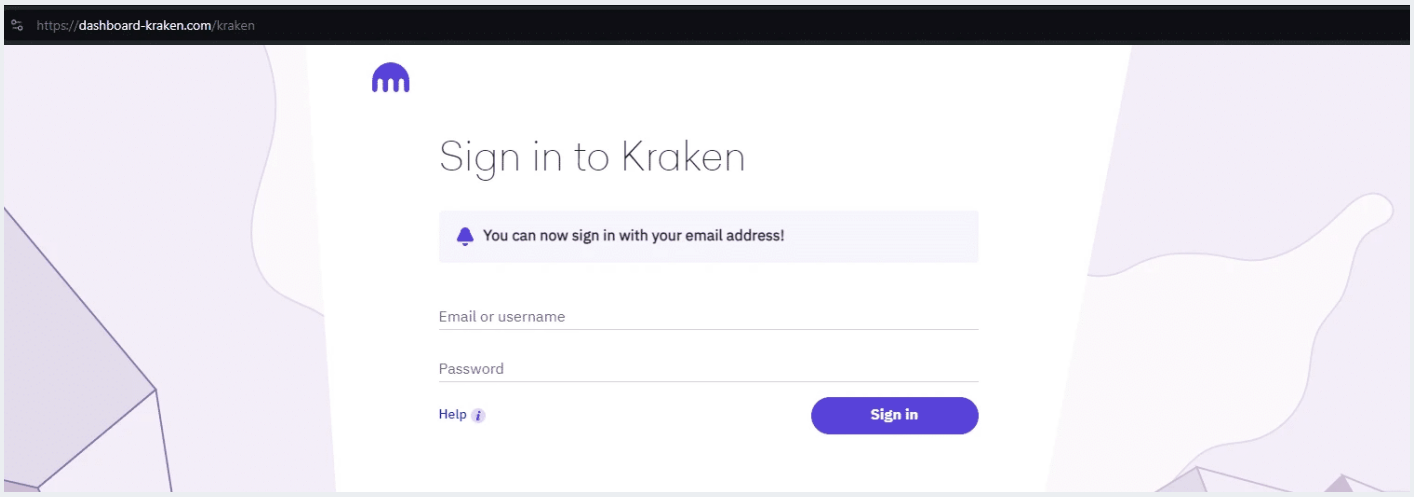
After confirming a new threat actor was targeting a U.S. government agency, we thought we would find additional government targeting, but found nothing else in 2024. CryptoChameleon quickly pivoted to targeting crypto companies and crypto users and remained consistent throughout 2024.

Our research discovered CryptoChameleon makes almost exclusive use of DNSPod nameservers.

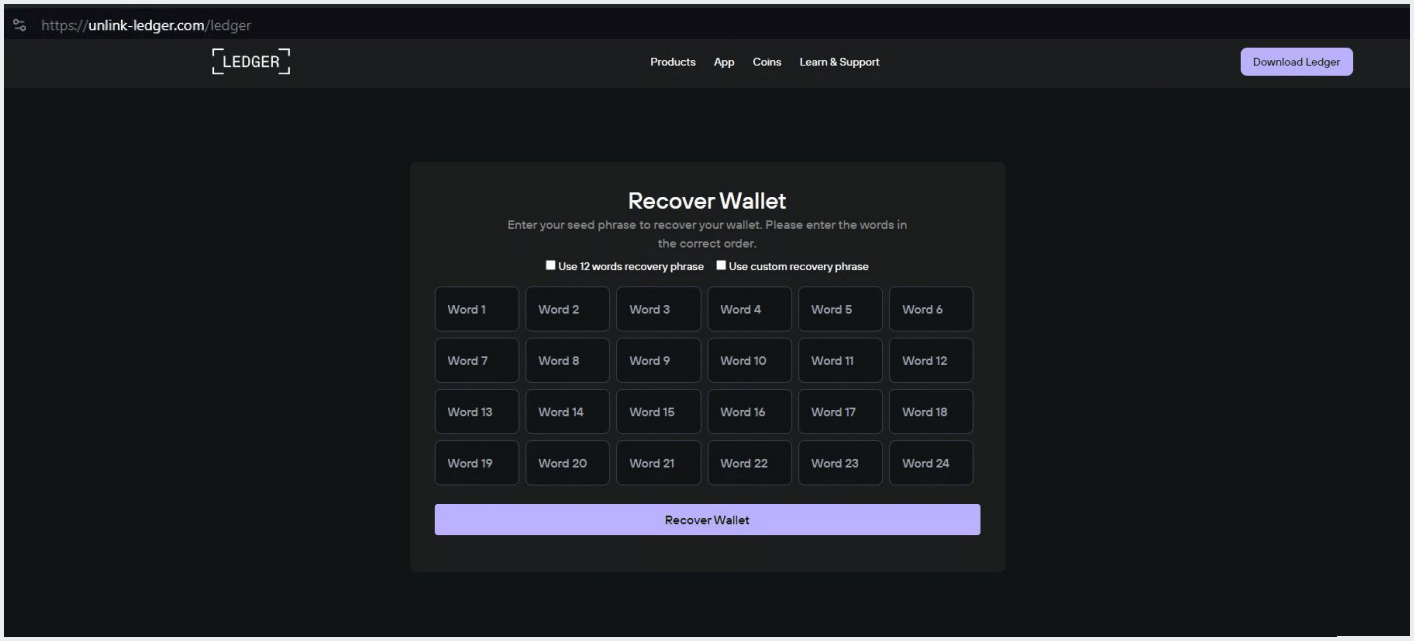
DNSPod is a self-proclaimed "intelligent DNS provider" used by botnets and bullet-proof hosting operators to propagate malicious activity for years, with an estimated 30% of its infrastructure engaged in malicious activity, according to a recent Unit42 report.

DNSPod is owned by Tencent Cloud and is based out of China.

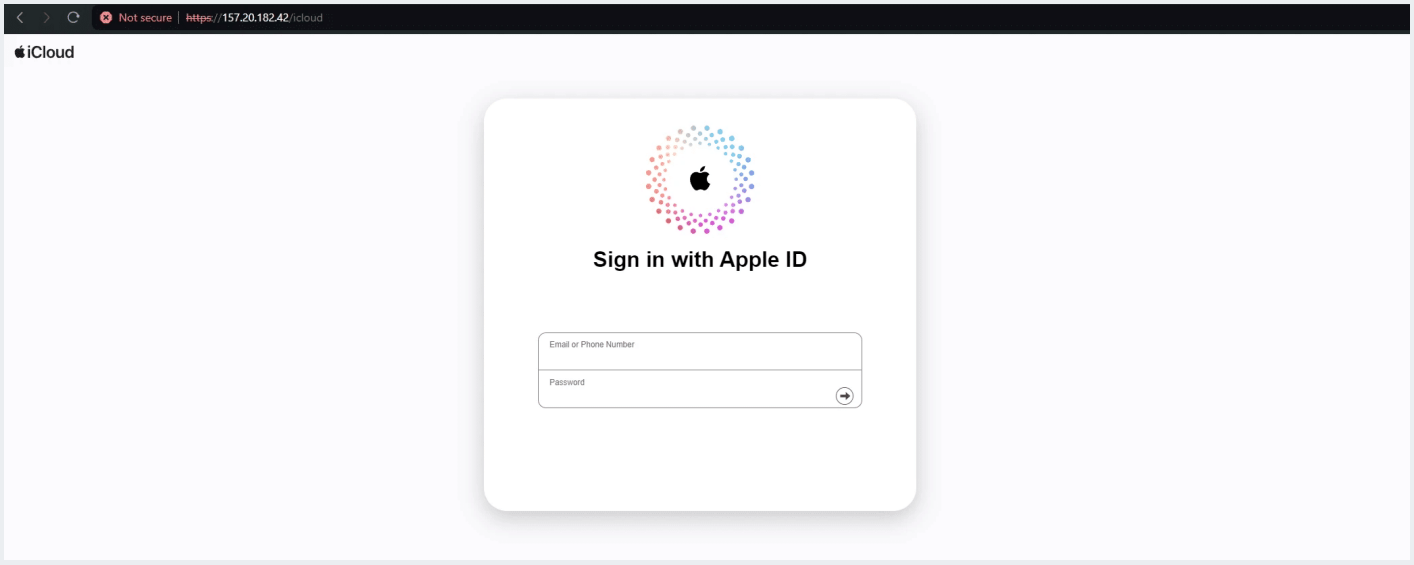
Here are a few screenshots that show CryptoChameleon phishing infrastructure across various websites:



Kraken phishing page



Ledger phishing page



Apple phishing page

Typically, research tools make it possible to search AS Numbers and then view the AS Name, but with Silent Push, we have fields for searching both AS Numbers and AS Names. This allows for simple, predictable queries with AS Numbers and more complex queries with AS Names -- essentially if you want to search for any ASN that includes "Russia" in its AS Name, Silent Push makes it easy.

An example ASN is "AS29470 JSC Retnet: Russia" -- with Silent Push, you merely need to search for "29470" in our Total View, and then you would find both the Number and the Common Name used by this ASN. Or, you could search the word "Russia" in our "asname" fields and you would be able to find any infrastructure hosted on an ASN with the word "Russia" in it. This feature is particularly useful for "DNS Dumpster Diving" where you are trying to review content hosted in specific locations.

Knowing the ASNs used by a threat actor provides a filter to help ensure a specific query doesn't introduce obscure false positives. At Silent Push, our analysts regularly find a query that works to find specific infrastructure, and then we put in additional rules like ASN filters to increase the rigor of the query. We still monitor broader queries to ensure we know about infrastructure changes and new ASNs that could be used, but we do those checks manually to prevent false positives.

Our IP diversity search allowed us to pinpoint numerous AS names and numbers that are actively involved in propagating CryptoChameleon attacks across the globe.

AS NAMES

- VDSina: Russian hosting provider
- Sannikov Kirill Vladimirovich (aka SANNIKOV): Russian hosting provider
- TIMEWEB-AS: Russian hosting provider
- Garant-Park-Internet LLC (aka GARANT): Russian hosting provider
- ALIBABA: Chinese hosting provider

AS NUMBERS

- AS29470 JSC Retnet: Russia
- AS212441 Cloud Assets LLC: Russia
- AS35278 Sprinthost LLC: Russia

Example IOFAs from CryptoChameleon found in 2024:

- 76153-coinbse[.]com
- 81758-coinbse[.]com
- 81920-coinbse[.]com
- 81926-coinbse[.]com
- 81958-coinbse[.]com
- 826298-coinbse[.]com
- 83216-coinbse[.]com
- 837613-coinbse[.]com
- 83956-coinbse[.]com

INVESTMENT SCAMS / PIG BUTCHERING

In 2024, Silent Push analysts researched numerous investment scam networks, sometimes referred to as "pig butchering" websites. Our team agrees with experts at Interpol who spoke with Wired that the language "pig butchering" is not sensitive to victims of these schemes, and we are shifting our language in 2025 to speak about these as "investment scams" and "job scams," depending on the specifics of any one campaign.

Several of the investment and job scam campaigns we investigated were not connected to any one threat actor group, but we continue these investigations and look forward to reports in 2025 that will provide additional clarity. However, we were successful in identifying operators behind the Triad Nexus scheme, along with the AIZ Retail & Crypto scam network, and shared those leads with law enforcement. Summaries of all those investigations are included below.

TRIAD NEXUS

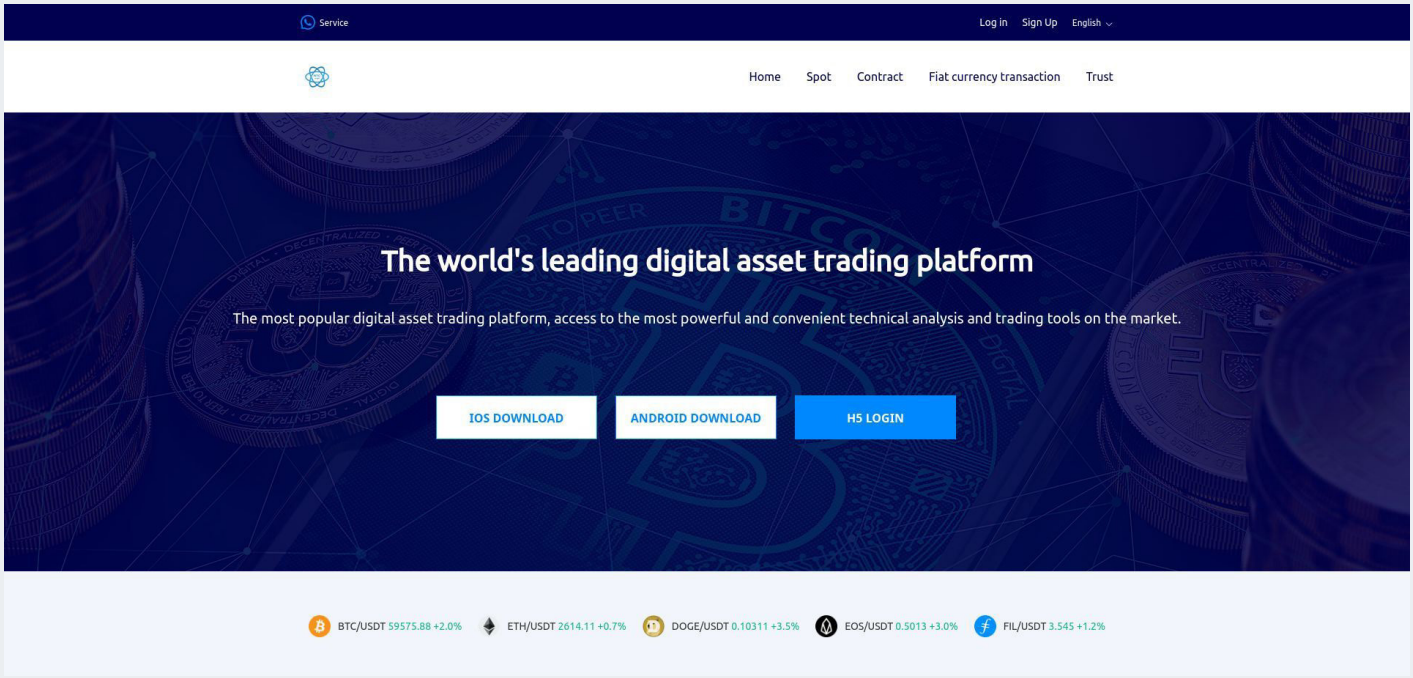
Our full public report on Triad Nexus, hosted on FUNNULL Content Delivery Network, is available here.

- Silent Push has been tracking FUNNULL, a Chinese CDN hosting persistent criminal campaigns, including investment scams, fake trading apps, and suspect gambling networks, for over two years.
- We dubbed FUNNULL's malicious domain cluster "Triad Nexus."
- 200,000 unique hostnames were proxied through FUNNULL, with a +95% DGA ratio.
- Thousands of suspect gambling websites hosted on FUNNULL were confirmed to be "fake" and abusing the trademark of popular casino organizations. Further details connected those fake gambling websites to a network of Telegram accounts promoting "money moving" services, which are essentially a form of money laundering.
- Polyfill JavaScript library exploits were used in a supply chain attack that impacted more than 110,000 of the top websites on the internet.
- FUNNULL-hosted retail phishing scams were discovered targeting major brands.

During a 2022 Silent Push investigation into a domain involved in investment fraud, our team uncovered a large cluster of fake trading apps impersonating well-known financial organizations, including the Australian Securities Exchange (ASX), Coinbase, CoinSmart, eToro, and Nasdaq.

This same investigation uncovered fake financial job scams employing pig-butchering techniques, and this is when our analysts first came across several malicious networks hosted on the FUNNULL CDN infrastructure.

Our **Triad Nexus** research discovered this is not a lone cluster of activity but is, in fact, part of a global financial fraud campaign.



Silent Push uncovered this fake trading app, hiflyk47344[.]top, was active as of late 2024

When updating our FUNNULL research for 2024, we discovered that this same malicious cluster, while reduced in scope, still has active hostnames, including cmegrouphkpd[.]info, which hosted a fake trading platform abusing CME Group's brand for the past two years.

Until recently, a nearly identical version of this site was hosted at hiflyk47344[.]top.

The timeline can be seen via current and historical CNAME records, which for cmegrouphkpd[.]info shows it had a record pointing to vk6a2rmn-u.funnull[.]vip between February and March 2022, changing to vk6a2rmn-u.funnull01[.]vip between March 2022 and June 2024, and since then, switching to 6ce0a6db.u.fn03[.]vip.

Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	TTL	Type
www.cmegrouphkpd.info	-	6ce0a6db.u.fn03.vip	-	2024-06-24 00:23:42	2024-08-04 22:45:59	300	CNAME
www.cmegrouphkpd.info	-	vk6a2rmn-u.funnull01.vip	-	2022-05-20 19:05:13	2024-06-20 04:27:48	300	CNAME
www.cmegrouphkpd.info	-	vk6a2rmn-u.funnull.vip	-	2022-02-27 06:55:26	2022-05-07 09:02:13	300	CNAME

Forward CNAME lookup on cmegrouphkpd[.]info

The apex domains seen in the Answer fields of these CNAME records – funnull[.]vip, funnull01[.]vip and fn03[.]vip – are all part of FUNNULL's CDN infrastructure.

By having a CNAME record pointing to FUNNULL's CDN infrastructure, every time a DNS client requests the hostname of a FUNNULL customer, the DNS resolver follows the resolution chain and redirects to the CDN, which answers with the IP address of its "Point of Presence" (PoP) with the fastest response, as seen below:

Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	TTL	Type
6ce0a6db.u.fn03.vip	-	0e6de73d2.n.fnvip100.com	-	2024-03-17 11:08:08	2024-08-06 07:08:25	600	CNAME

Second hop of cmegrouphkpd[.]info name resolution

Query	Answer	Answer ASN	First Seen	Last Seen	Type
0e6de73d2.n.fnvip100.com	137.220.202.119	152194	2024-04-25 06:04:16	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.150	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.151	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.148	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	137.220.225.183	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	52.247.251.209	8075	2024-07-21 07:48:11	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	20.205.19.56	8075	2024-06-27 19:28:27	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.153	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	223.26.61.46	152194	2024-06-09 05:53:39	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	20.205.129.121	8075	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	137.220.225.81	152194	2024-06-26 09:07:54	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.152	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A
0e6de73d2.n.fnvip100.com	27.124.12.149	152194	2024-06-08 06:54:48	2024-08-06 00:15:08	A

Third hop of cmegrouphkpd[.]info's name resolution

As a result, these CNAME chains can be used to map FUNNULL's entire customer infrastructure on its CDN and obtain the IP addresses of its PoP network.

We identified over 200,000 unique hostnames being proxied through this network in a single month alone, and 1.5 million reverse CNAME records/lookups have been collected since 2021.

FUNNULL CNAME CHAINS

Here is a diagram of the FUNNULL CNAME chains:

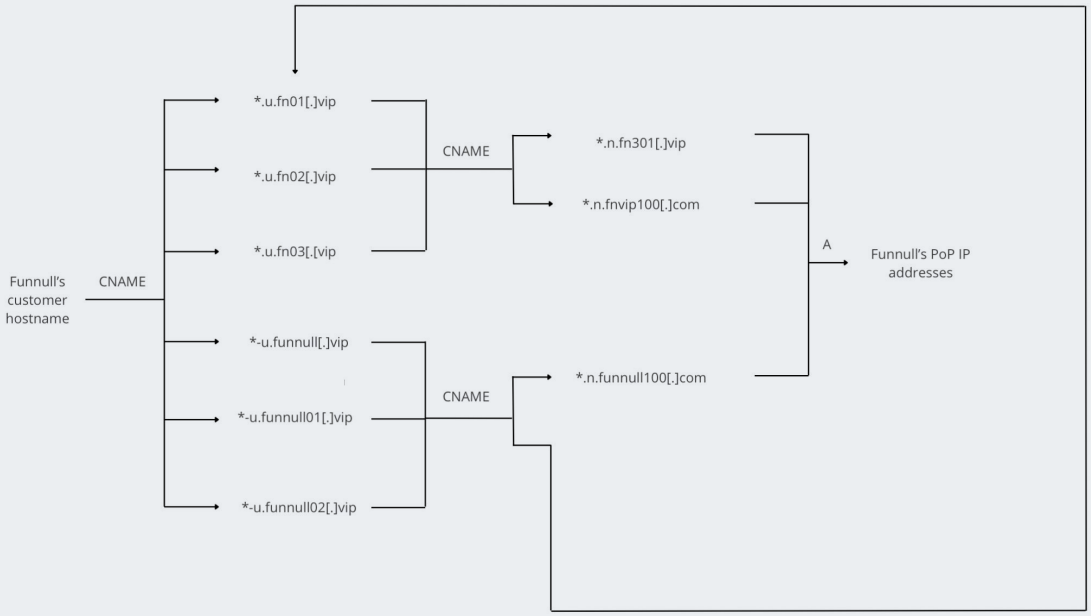
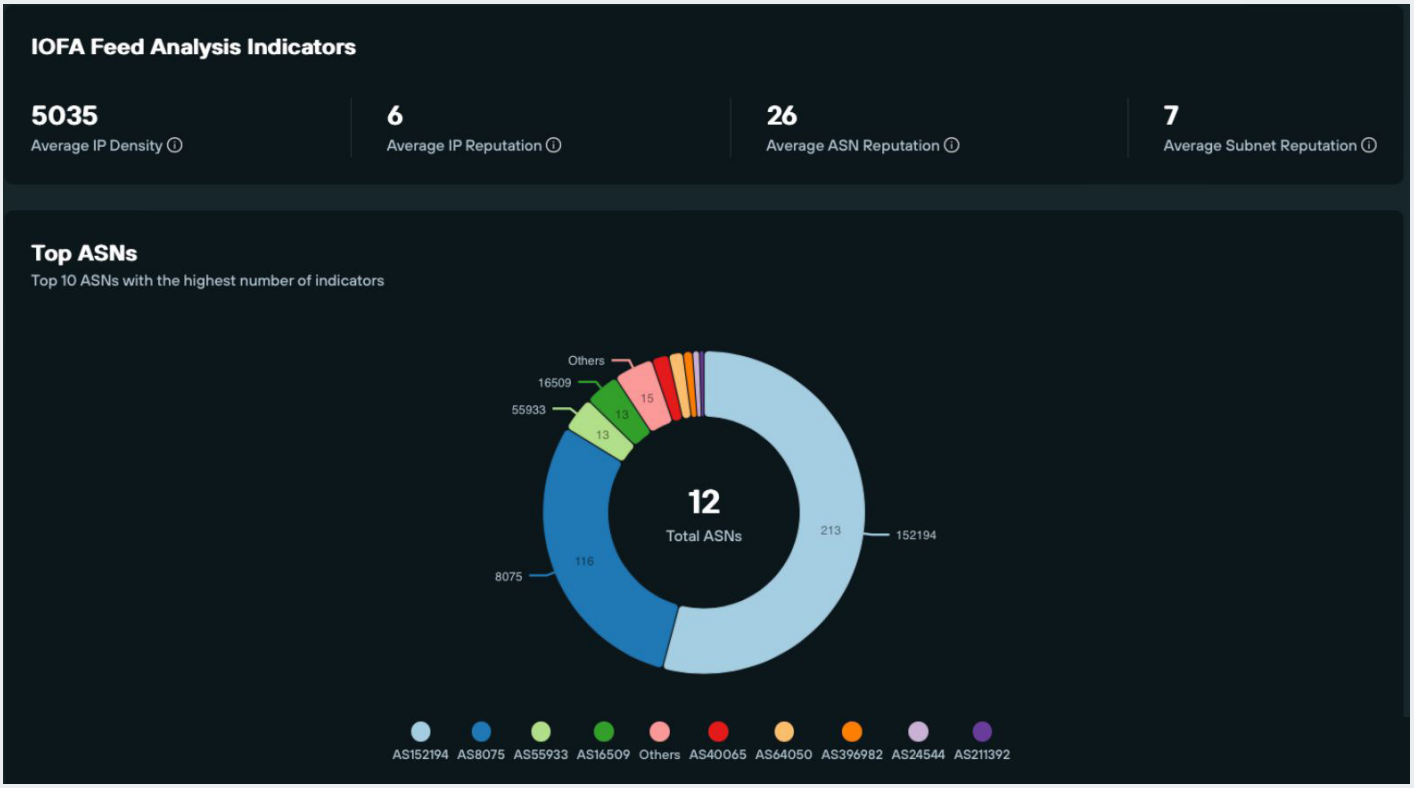


Diagram of FUNNULL CNAME chains

Utilizing the Silent Push platform to perform a high-level CNAME lookup of the hostnames leveraging this system, our analysis revealed that **more than 95%** of the hostnames were created with DGAs containing mostly numeric characters, with a few optional letters.

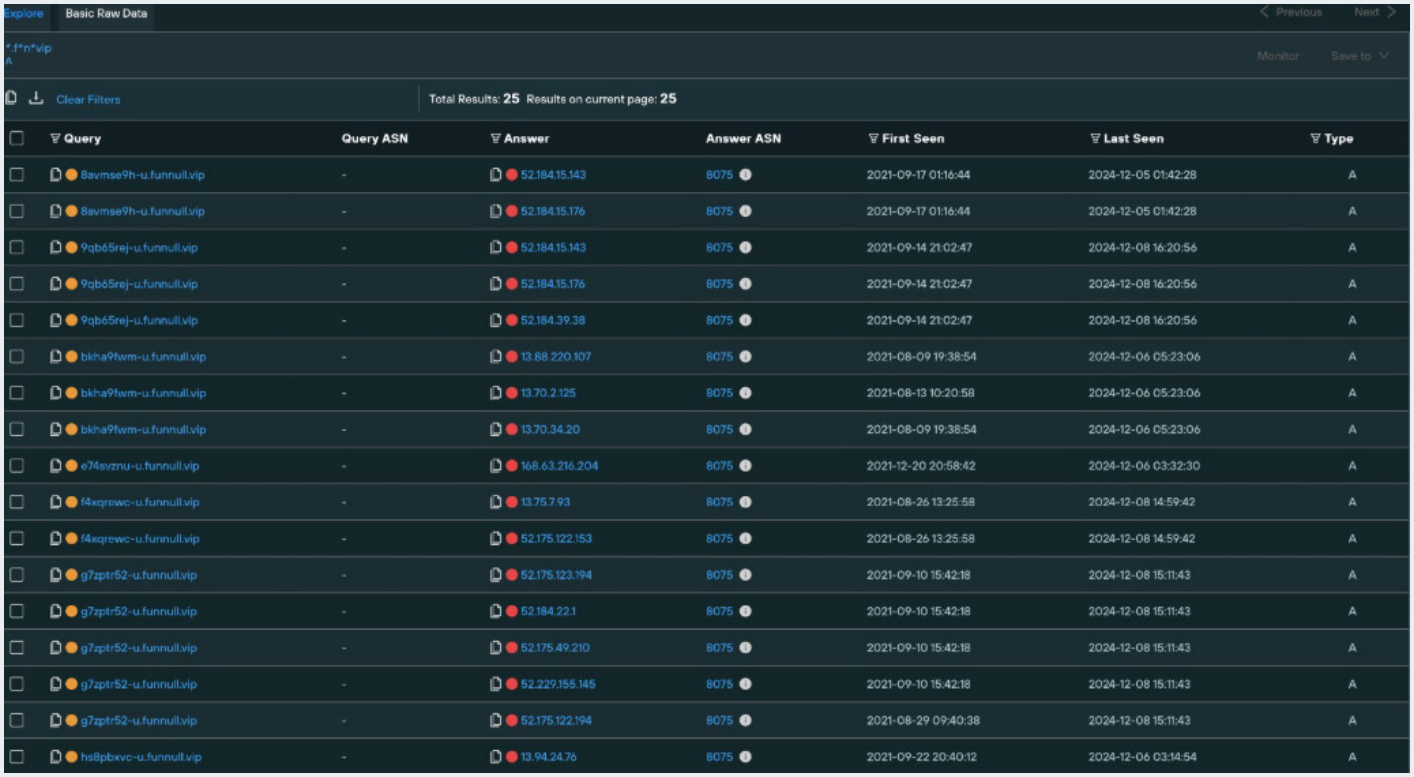


AS distribution of Funnull's PoP seen in late 2024

Silent Push identified close to 500 of FUNNULL's PoP active IP addresses. As expected, many were located in Asian ASNs, such as AS152194 (China Telecom Global), AS45753 (NETSEC-HK Netsec Limited), and AS55933 CLOUDIE-AS-AP Cloudie Limited, among others.

Surprisingly, during our investigation, we discovered nearly 40% of the CDN's PoPs were IP addresses belonging to AS8075 (MICROSOFT C) and AS16509 (AMAZON), two major U.S.-based cloud providers.

Using Silent Push's extensive PADNS data, we confirmed that FUNNULL has been renting Microsoft's IP space and using it to accelerate its customers' infrastructure since at least 2021.



Explore | Basic Raw Data | Previous | Next

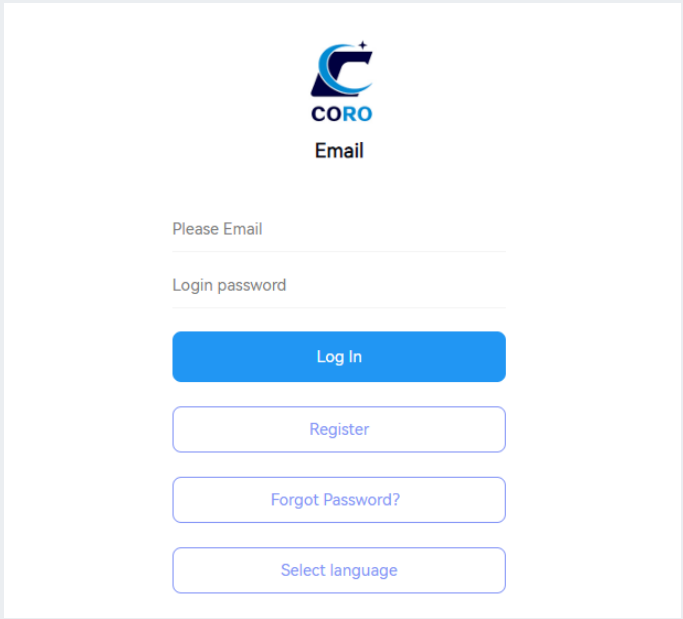
*.f*n*vip
A

Monitor | Save to

Clear Filters | Total Results: 25 Results on current page: 25

Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	Type
8avmse9h-u.funnull.vip	-	52.184.15.143	8075	2021-09-17 01:16:44	2024-12-05 01:42:28	A
8avmse9h-u.funnull.vip	-	52.184.15.176	8075	2021-09-17 01:16:44	2024-12-05 01:42:28	A
9qb65rej-u.funnull.vip	-	52.184.15.143	8075	2021-09-14 21:02:47	2024-12-08 16:20:56	A
9qb65rej-u.funnull.vip	-	52.184.15.176	8075	2021-09-14 21:02:47	2024-12-08 16:20:56	A
9qb65rej-u.funnull.vip	-	52.184.39.38	8075	2021-09-14 21:02:47	2024-12-08 16:20:56	A
bkha9fwm-u.funnull.vip	-	13.88.220.107	8075	2021-08-09 19:38:54	2024-12-06 05:23:06	A
bkha9fwm-u.funnull.vip	-	13.70.2.125	8075	2021-08-13 10:20:58	2024-12-06 05:23:06	A
bkha9fwm-u.funnull.vip	-	13.70.34.20	8075	2021-08-09 19:38:54	2024-12-06 05:23:06	A
e74svznu-u.funnull.vip	-	168.63.216.204	8075	2021-12-20 20:58:42	2024-12-06 03:32:30	A
f4xqrewc-u.funnull.vip	-	13.75.7.93	8075	2021-08-26 13:25:58	2024-12-08 14:59:42	A
f4xqrewc-u.funnull.vip	-	52.175.122.153	8075	2021-08-26 13:25:58	2024-12-08 14:59:42	A
g7zptr52-u.funnull.vip	-	52.175.123.194	8075	2021-09-10 15:42:18	2024-12-08 15:11:43	A
g7zptr52-u.funnull.vip	-	52.184.22.1	8075	2021-09-10 15:42:18	2024-12-08 15:11:43	A
g7zptr52-u.funnull.vip	-	52.175.49.210	8075	2021-09-10 15:42:18	2024-12-08 15:11:43	A
g7zptr52-u.funnull.vip	-	52.229.155.145	8075	2021-09-10 15:42:18	2024-12-08 15:11:43	A
g7zptr52-u.funnull.vip	-	52.175.122.194	8075	2021-08-29 09:40:38	2024-12-08 15:11:43	A
hs8pbxvc-u.funnull.vip	-	13.94.24.76	8075	2021-09-22 20:40:12	2024-12-06 03:14:54	A

FUNNULL CNAME records mapped to ASN 8075, owned by Microsoft, since 2021



coroexchange[.]com phishing login page

We also uncovered a retail scam campaign hosted through FUNNULL that uses phishing login pages to target major retail and luxury Western fashion brands. Targeted brands include Aldo, Asda, Bonanza, Cartier, Chanel, Coach, eBay, Etsy, Gilt Groupe, Inditex, Lotte Mart, LVMH, Macy's, Michael Kors, Neiman Marcus, OnBuy[.]com, Rakuten, Saks Fifth Avenue, Tiffany & Co., and Valentino.

From this retail scam campaign, our team discovered approximately 650 unique domains hosted on one specific FUNNULL CNAME: 12abb97f.u.fn03[.]vip.

We soon realized that a chunk of these were investment scam sites, such as coroexchange[.]com:

Beyond the investment scam sites, the only other websites hosted on this CNAME all appeared to be a retail phishing campaign targeting major Western brands, with phishing login pages such as bonanza.jdfraa[.]com:

bonanza.jdfraa[.]com phishing login page

The FUNNULL CDN hosting Triad Nexus infrastructure includes a newer strategy to conduct "infrastructure laundering" by registering IP space with prominent Western hosts, and Silent Push analysts believe this trend will continue or increase in popularity in 2025.

AIZ RETAIL & CRYPTO PHISHING NETWORK

Silent Push Threat Analysts have been tracking activity of a threat actor we dubbed "Aggressive Inventory Zombies" (AIZ) through 2024, which ramped up in the Winter holiday season. Read our full public report.

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

The threat actor behind the AIZ network had 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 featured 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 appeared 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 confirmed this threat actor had financial ties to India.

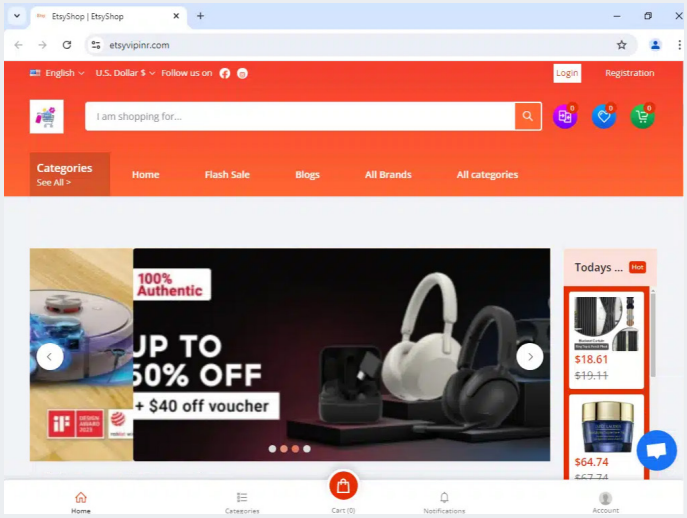
As the team dug deeper into the activities of the AIZ retail phishing network, we discovered the threat actor was also targeting crypto audiences. We researched reused metadata to find a huge pool of crypto phishing sites targeting Binance, Kraken, and a variety of other generic crypto brands.

After completing our initial research and starting the process of alerting impacted organizations, we requested that some domains hosted on Stark Industries (AS44477) be taken down. Within 30 minutes, Stark took down the offending host and connected the account that had registered that IP to 34 other IPs, some of which hosted similar retail phishing websites and several new groupings of crypto phishing websites. This lead from Stark also allowed us to pivot into even more of AIZ's infrastructure.

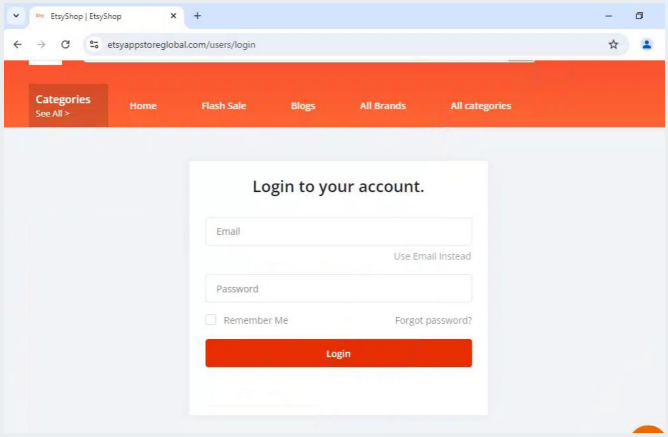
TARGETED BRANDS INCLUDED:

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

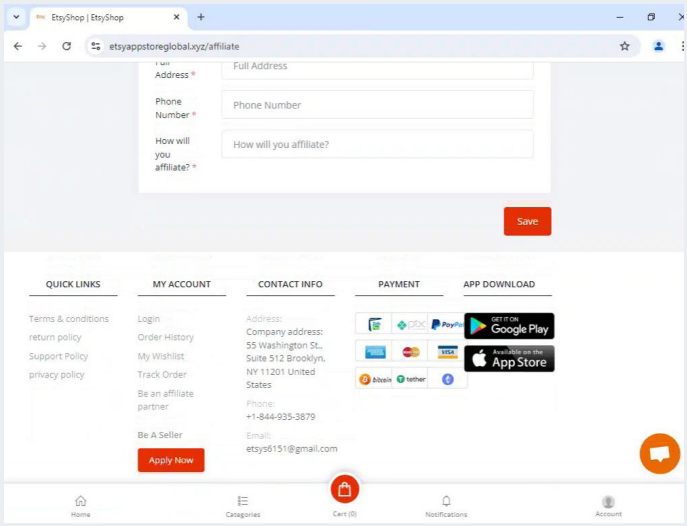
The six domains appearing to target Etsy were mapped to 2.56.178[.]87 – and four live sites all utilized the same theme:



Live site: etsyvipinr[.]com, targeting Etsy

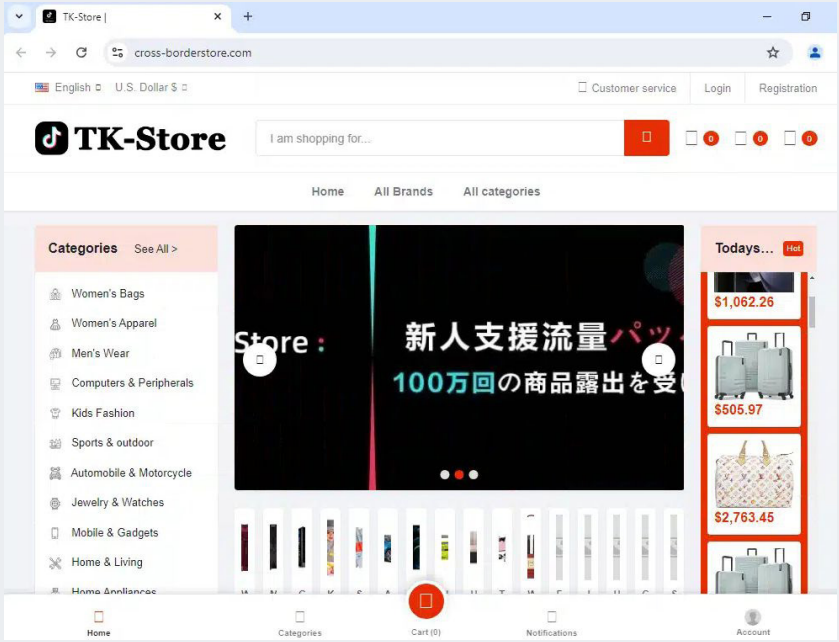


Live site: etsyappstoreglobal[.]com, targeting Etsy



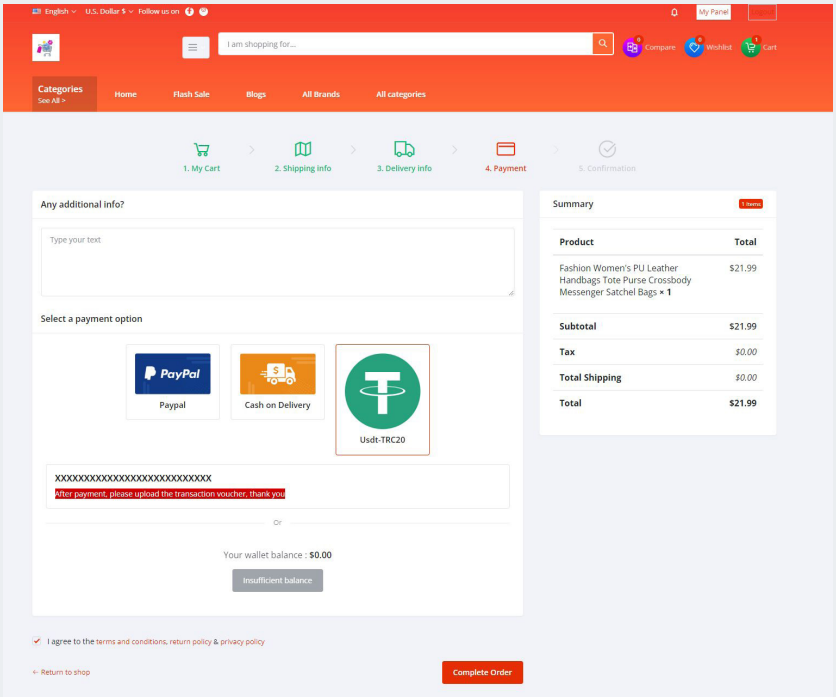
Live site: etsyappstoreglobal[.]xyz, targeting Etsy

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)

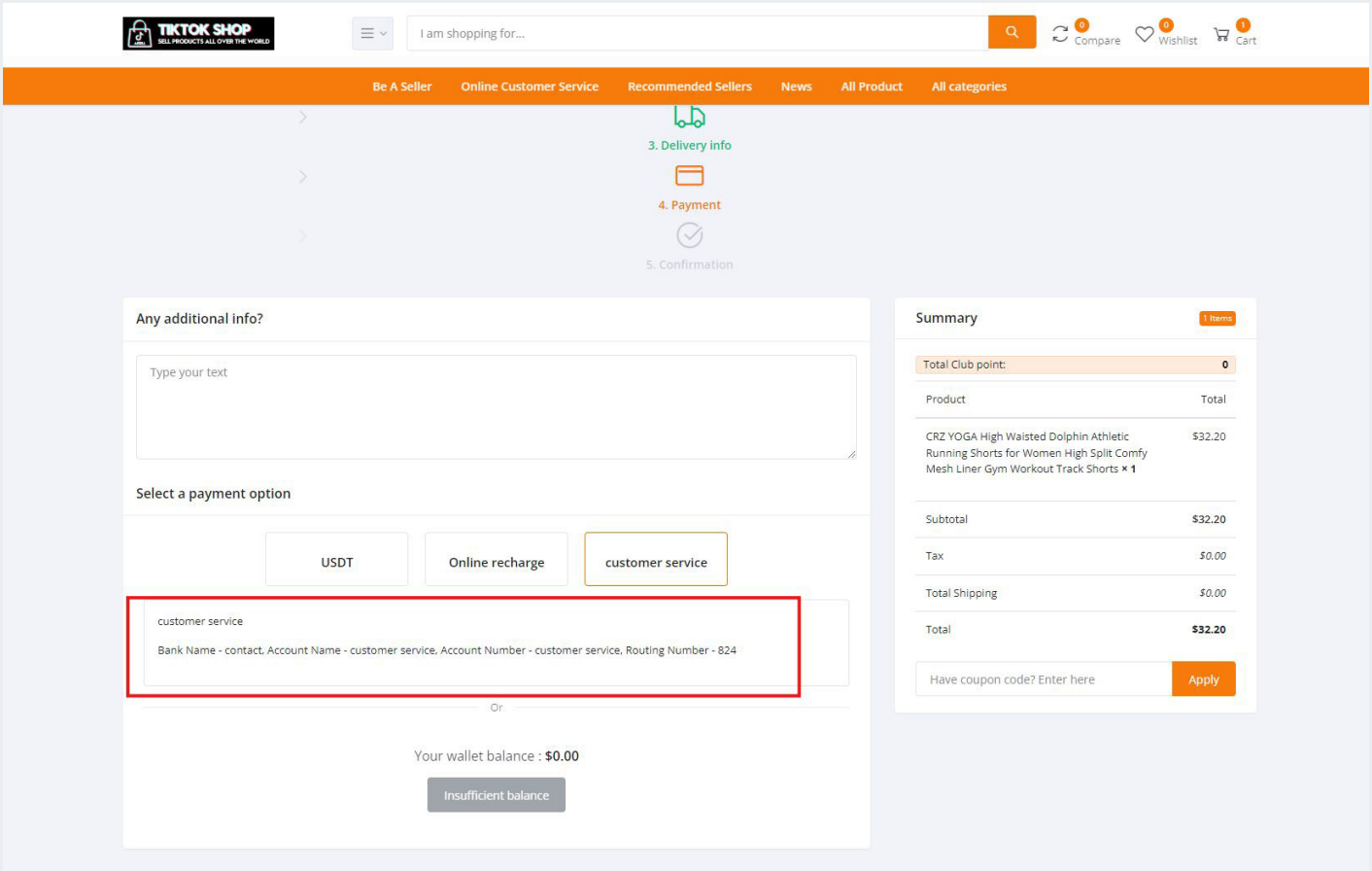
On some sites in the network, navigating to a product and then adding it to the cart starts the purchase process, which leads to a checkout page with three payment options: PayPal, "Cash on Delivery," or Tether/(USDT) cryptocurrency:



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.

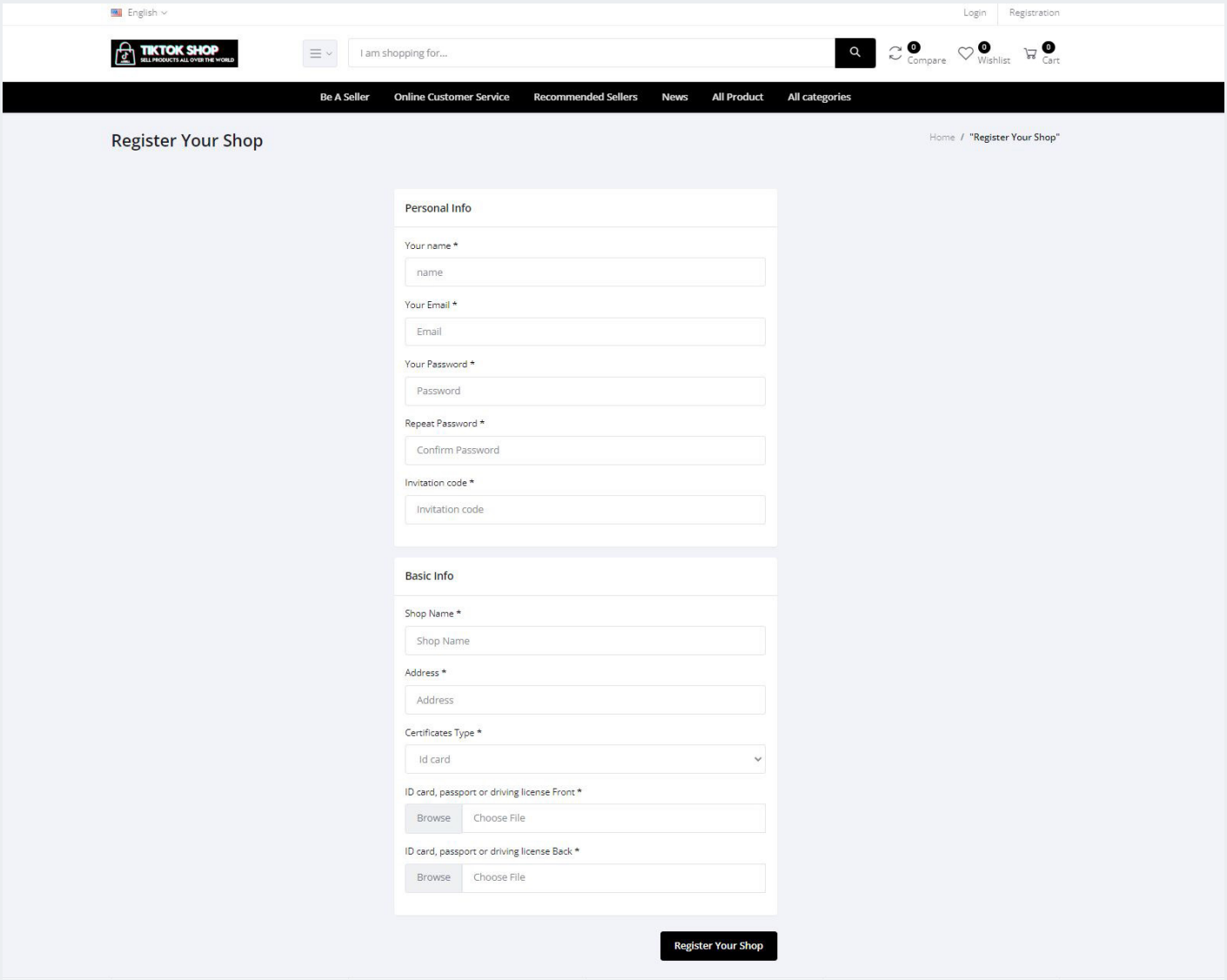
When we reviewed another store in the network, **ai-tiktok[.]top**, we uncovered different purchase options. The "Customer Service" option includes what appears to be an effort to obtain a bank account number and routing details—essentially a checking account phishing effort.



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

While hosting a seemingly inefficient phishing process on some of the websites, that relied on chat widgets, this network also seemed to operate like a common e-commerce phishing network.

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



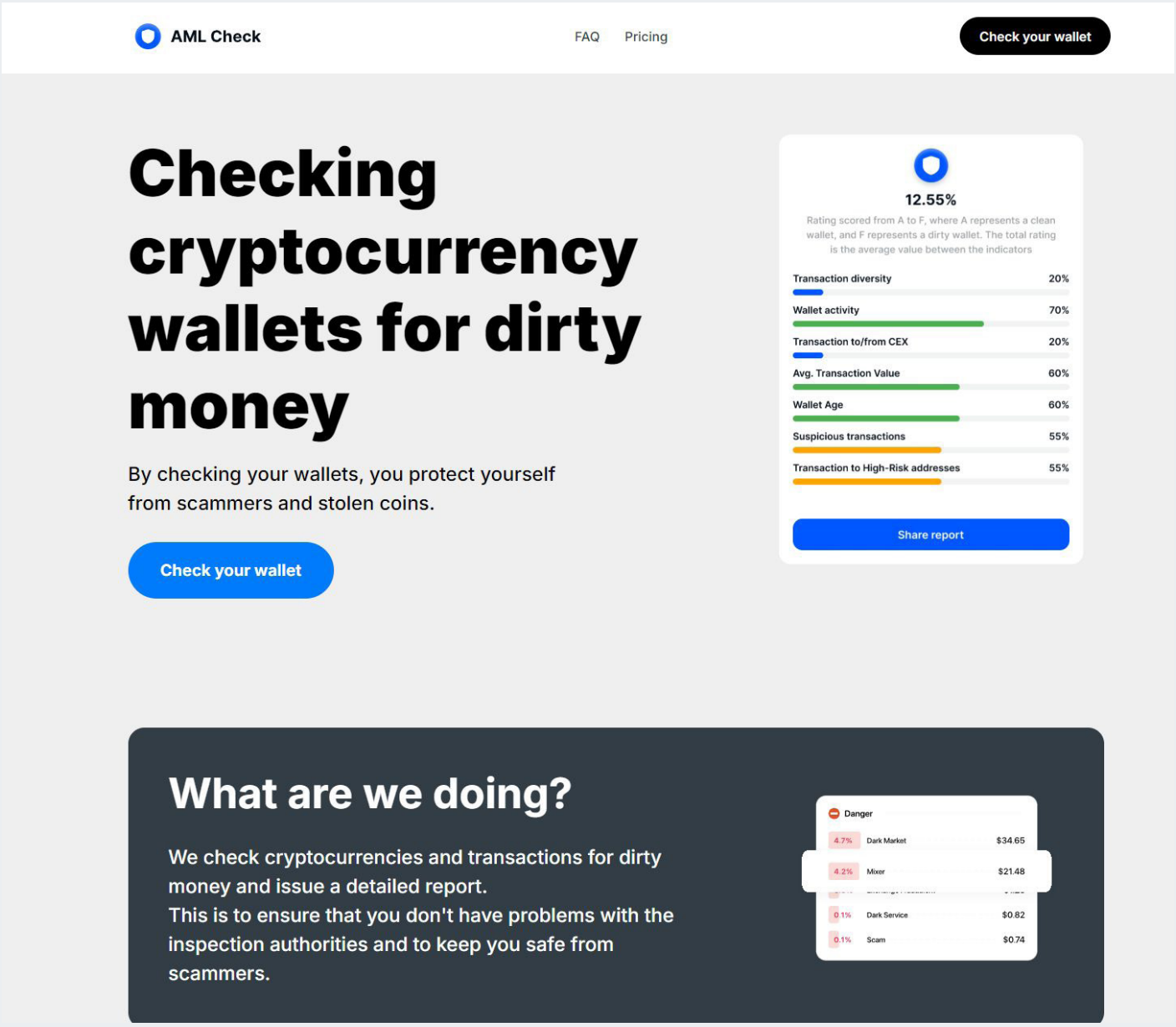
"Register Your Shop" option on ai-tiktok[.]top

As part of the Silent Push commitment to collaborating with hosts, our team sent an initial lead about the AIZ network 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.

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**.

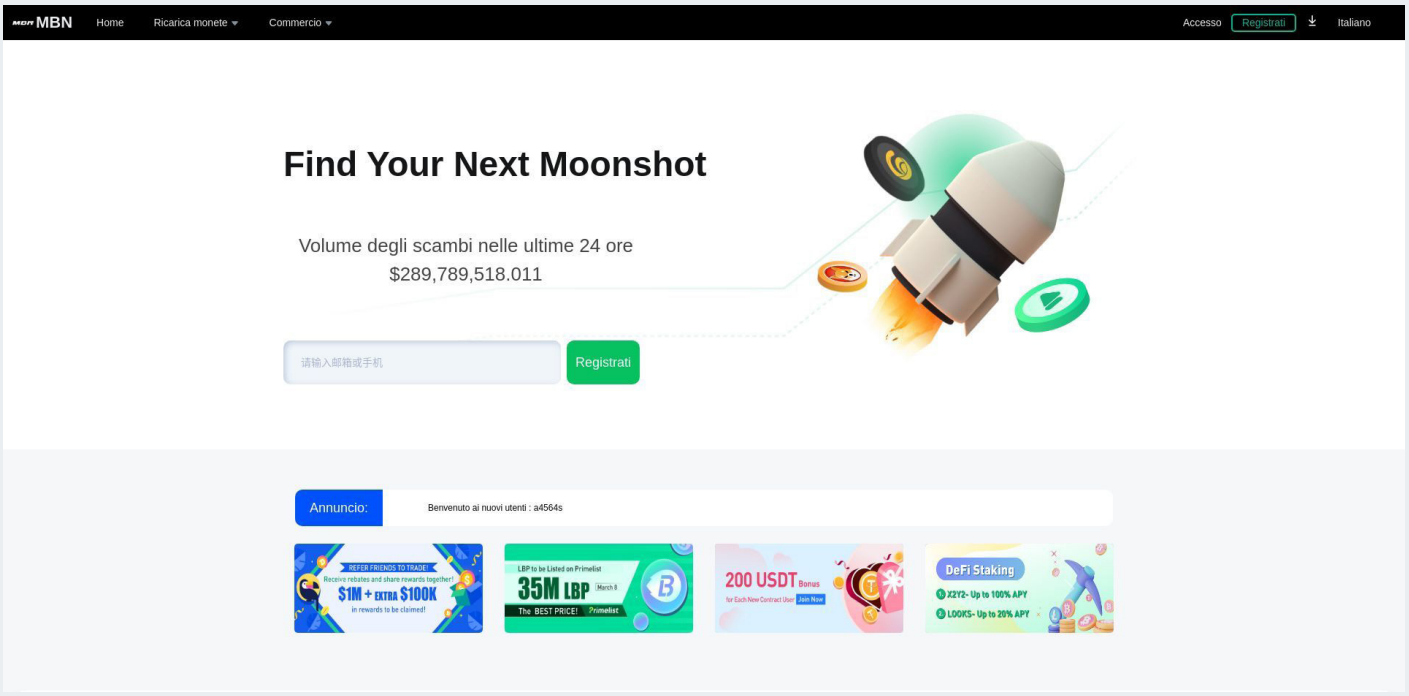
Performing a Web Scanner query confirmed that this domain used consistent metadata, which allowed us to pivot into several dozen other domains/hosts with the same content as the original source.

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



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

A huge pool of these crypto phishing sites could 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

From another IP shared by Stark Industries, we pivoted into a small group of domains, including **klo-ok[.]cc**.

This website had metadata similar to other new sites in the network. Creating a proprietary query, we pivoted into about a dozen unique hosts. Results included an IP with a live “crypto investment” website in Mandarin.

This host klo-ok[.]cc. had a live “crypto investment” website in Mandarin

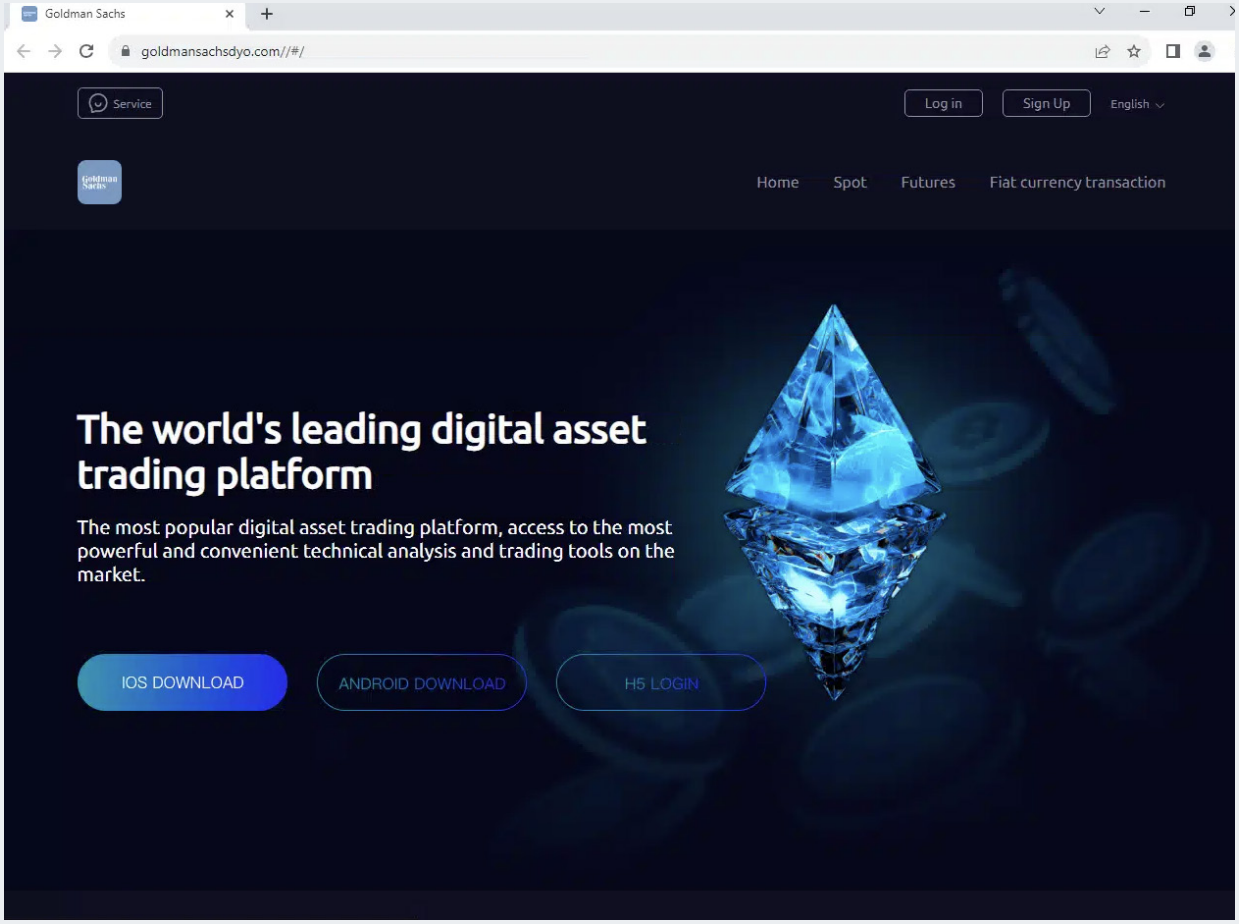
We’re continuing to track the **AIZ Retail & Crypto Phishing Network’s** activity and will continue to report on our findings in 2025.

JOB SCAMS & FAKE TRADING APPS

Silent Push previously reported on infrastructure used for fake trading web interfaces and mobile applications that mimicked AvaTrade, BitMEX, BlackRock, CBOE, Fidelity, Goldman Sachs, NYSE, and more. This infrastructure remains largely intact and has expanded substantially since our initial reporting.

The infrastructure comprises a web interface with an Android and iOS application that lures victims into depositing money and locking them out of their accounts once they try to withdraw their "gains."

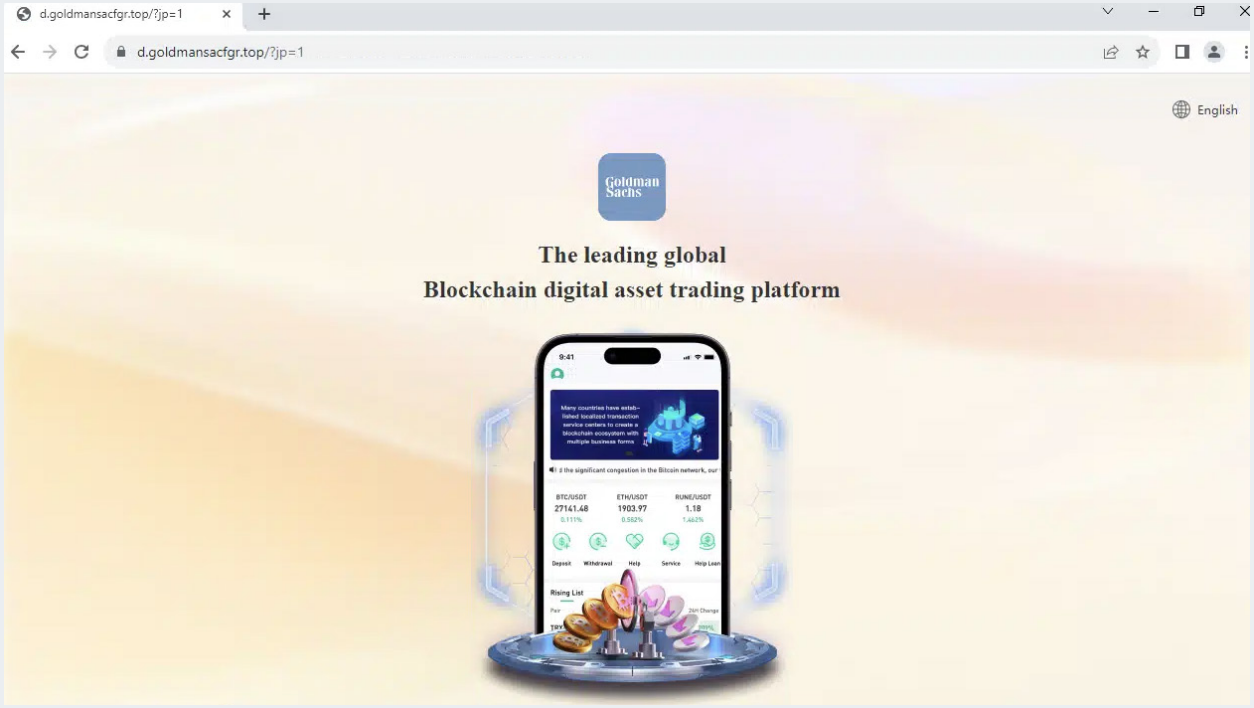
When viewing one of the domains from this campaign, www.goldmansachsgpy[.]com, we saw that the HTML title displayed is 'Goldman Sachs' and not 'Exchange' as we had captured in our Web Scanner, which indicates this information is *dynamically changed* for each website visit.



Fake trading web interface mimicking Goldman Sachs

A huge amount of these fake trading apps and job scams reuse HTML templates across their sites, which created solid pivots for tracking the campaign.

When browsing these domains, we noticed that the www subdomains hosted the web interfaces while the single letter subdomains hosted the Android and IOS download pages.



Single letter subdomain shows an iOS app download

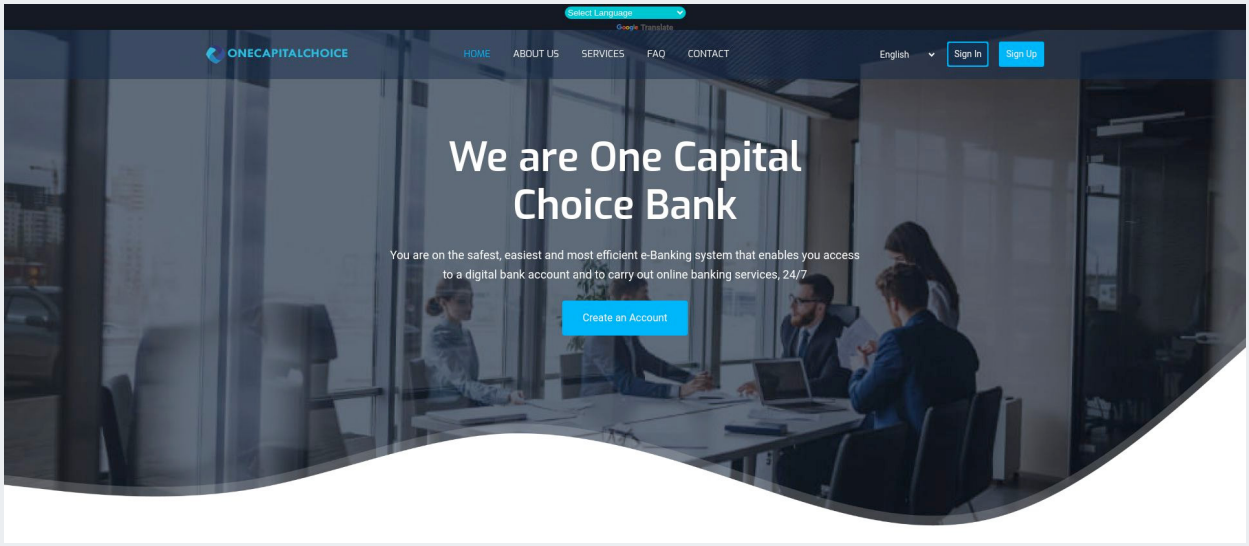
Our team has tracked nearly 7,000 of these fake trading apps and job scams and can report there is significant diversity in the domain TLDs being used, the ASNs hosting the IPs, and the Registrars.
The majority of the Nameservers are from DNS[.]com, a Chinese host.

Summary of the job scam and fake trading apps infrastructure

VISERBANK INVESTMENT SCAMS

- "ViserBank" templates, sold on Envato, were used to create scam banking websites
- Brands impersonated include Capital One, Wells Fargo, Bank of America, JPMorgan Chase, Santander Bank, and Virgin Money
- Domains were discovered in the wild attempting to harvest identity data and login information

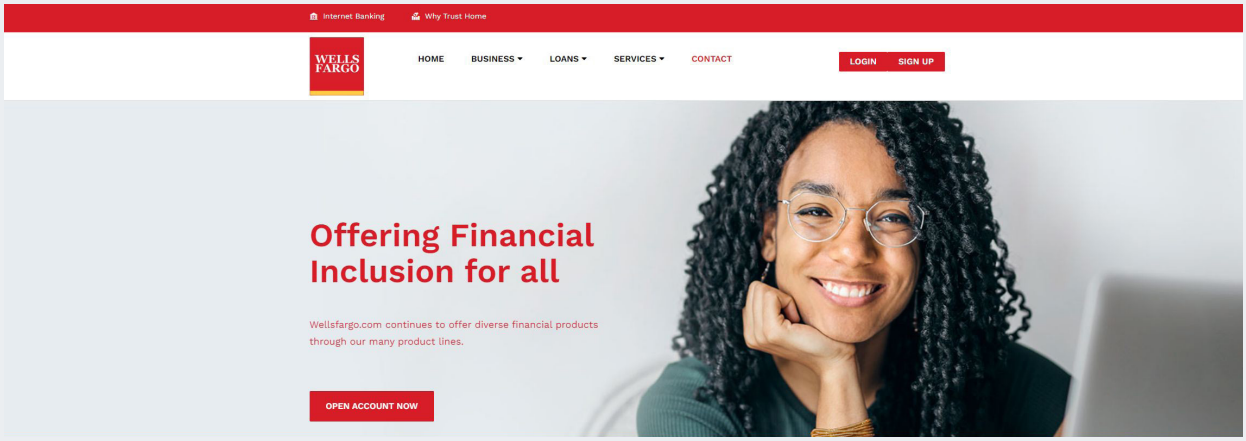
In Fall 2024, our analysts noticed several websites, including **onecapitalschoicebank[.]com**, **santender[.]net**, and **eastwestpremeircorp[.]com** shared similar content traits, even though the domains themselves and the corresponding websites were unrelated.



onecapitalschoicebank[.]com

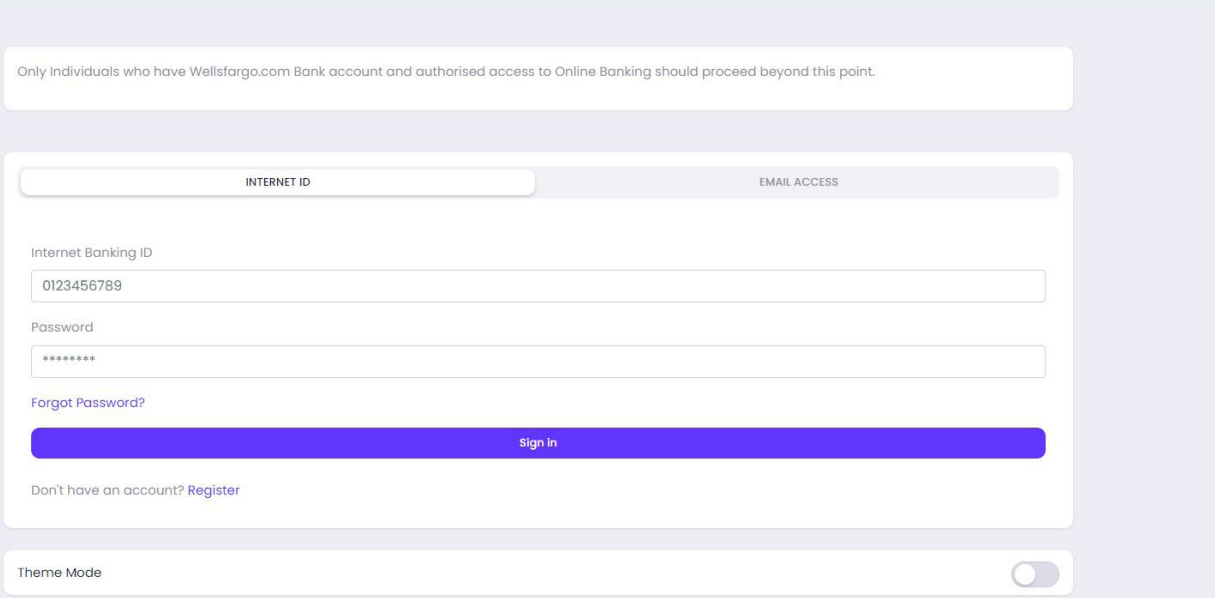
Combining several more ViserBank Web Scanner parameters, we discovered over **2,000 unique domains and IPs**, all using the same questionable platform, with many impersonating major brands.

Here is an example of the phishing domain **wellsfargo-inc[.]com** attempting to steal Wells Fargo banking credentials:



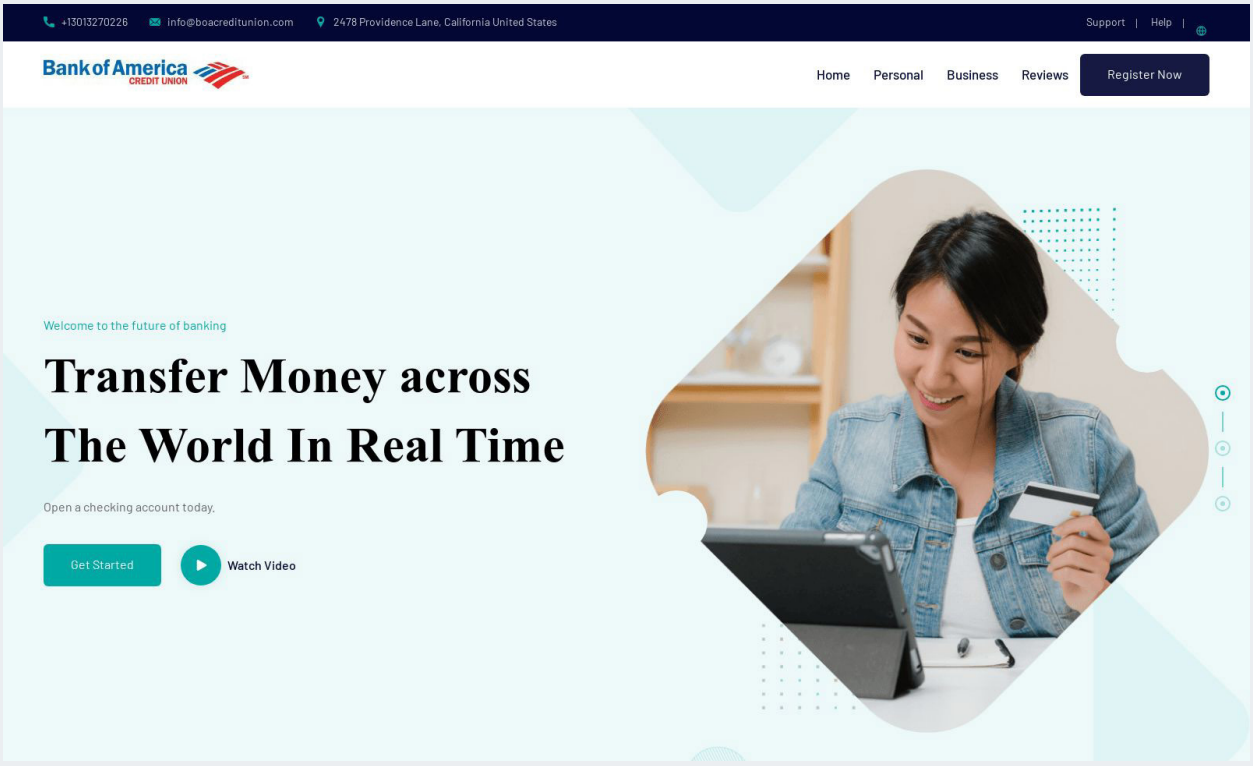
wellsfargo-inc[.]com

The domain features a form that asks for a “Wells Fargo Banking ID” and the user’s password:



Malicious web form on wellsfargo-inc[.]com

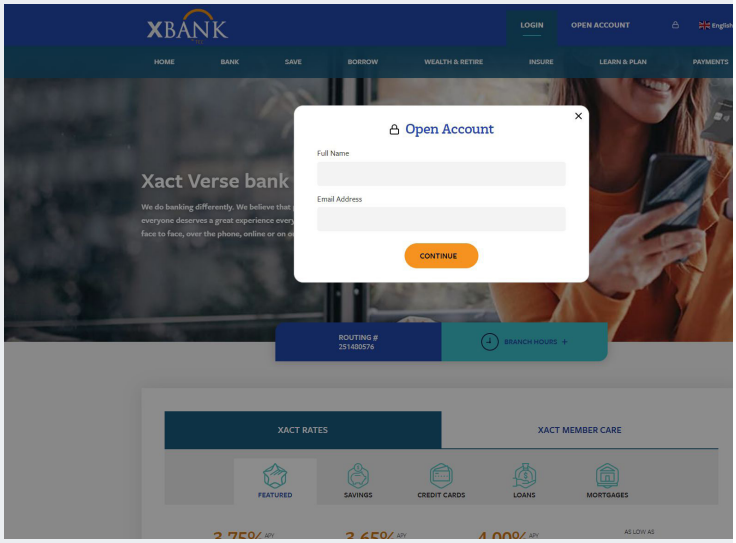
Here’s another phishing domain, **boacreditunion[.]com**, targeting Bank of America customers:



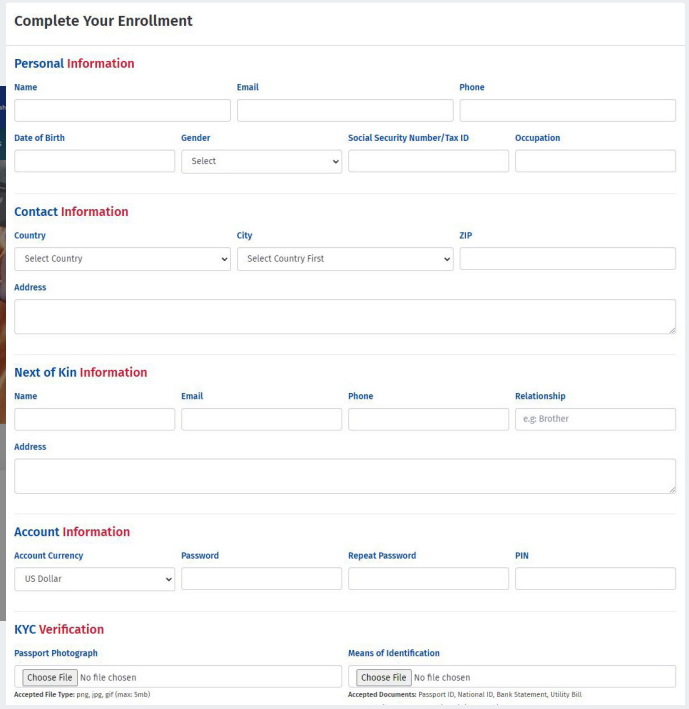
Domain boacreditunion[.]com targeted Bank of America customers

In addition to spoofing legitimate brands, threat actors used ViserBank templates to trick users into signing up for obscure banking services and handing over private data at the point of registration.

An “XBANK” registration form hosted on one such phishing domain – **xactverse[.]com** – had a prompt to include the user’s **name, address, phone number, social security number, and passport photo:**



Phishing page on xactverse[.]com



Registration form on xactverse[.]com

ViserBank templates appear to have been used by multiple threat actor groups last year. In 2025, we look forward to sharing additional research about one specific threat actor we’ve been able to associate with using some of these ViserBank templates.

SMISHING TRIAD

Smishing Triad is a cybercrime group allegedly operating from China that sends SMS phishing messages (“smishing”) containing fake notifications about parcel delivery status. The group, which was uncovered in a Defcon 2024 presentation, uses many domain names that often impersonate postal services from around the world.

Silent Push continues actively tracking this group through the dozens of new domains they register, which show that despite the public reporting, their activities haven’t slowed down.

Basic Raw Data | **Total Results:** 73382 **Results on current page:** 100

scan_date	url	domain	ip
2024-12-12T18:29:02Z	https://vip-candapost.cc/	vip-candapost.cc	87.120.126.38
2024-12-12T18:21:26Z	http://usps.tube	usps.tube	38.54.88.120
2024-12-12T18:21:26Z	https://usps-packages-wbg.com/	usps-packages-wbg.com	43.166.254.36
2024-12-12T18:21:19Z	https://usps-packages-fkd.com/	usps-packages-fkd.com	43.166.254.36
2024-12-12T18:21:17Z	https://usps-packages-omz.com/	usps-packages-omz.com	43.166.254.36
2024-12-12T18:19:22Z	https://uqsposta.cc/	uqsposta.cc	47.251.61.22
2024-12-12T18:17:49Z	https://upspostr.cc/	upspostr.cc	47.251.61.22
2024-12-12T18:05:43Z	https://transportuk.guru/	transportuk.guru	47.243.13.50
2024-12-12T18:05:43Z	https://transportuk.cfd/	transportuk.cfd	47.243.13.50
2024-12-12T18:05:42Z	https://transportuk.services/	transportuk.services	47.243.13.50
2024-12-12T18:05:42Z	https://transportuk.cyou/	transportuk.cyou	47.243.13.50

Web Scanner of smishing campaign domains

ILLEGAL ONLINE PHARMACIES

Building on the work of the DEA, Silent Push Threat Analysts used content similarity and page metadata scans to reveal approximately 2,500 unique IOFA domains and dedicated IPs actively hosting illegal pharmacy content.

The websites were actively engaged in numerous criminal acts, including the sale of illegal drugs and Counterfeit or Falsified Medication (CFM).

Domains were largely hosted via U.S.-based ASNs and dedicated IPs, using Dynadot and Russian nameservers.

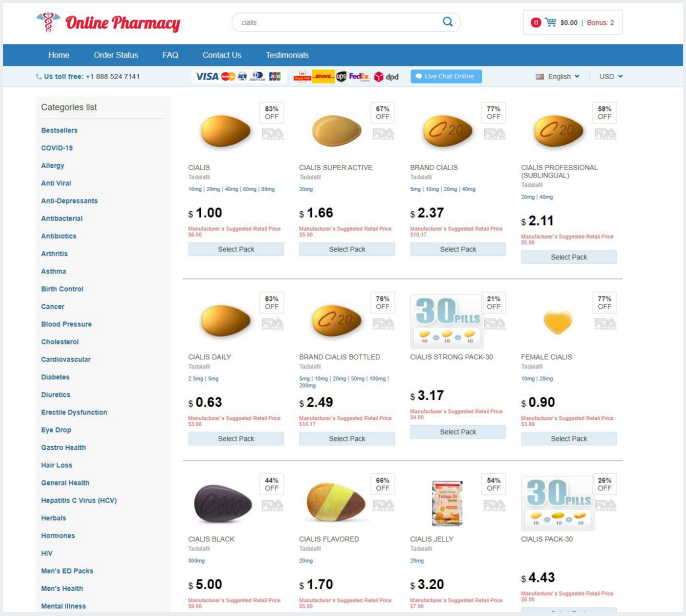
As part of our investigation, we began by looking at the nine fake online pharmacies shared by the DEA:

- www.curecog[.]com
- www.pharmacystoresonline[.]com
- www.careonlinestore[.]com
- www.yourphamacy[.]online
- www.md724[.]com
- www.greenleafdispensarystore[.]com
- www.whatishydrocodone.weebly[.]com
- www.orderpainkillersonline[.]com
- www.usamedstores[.]com

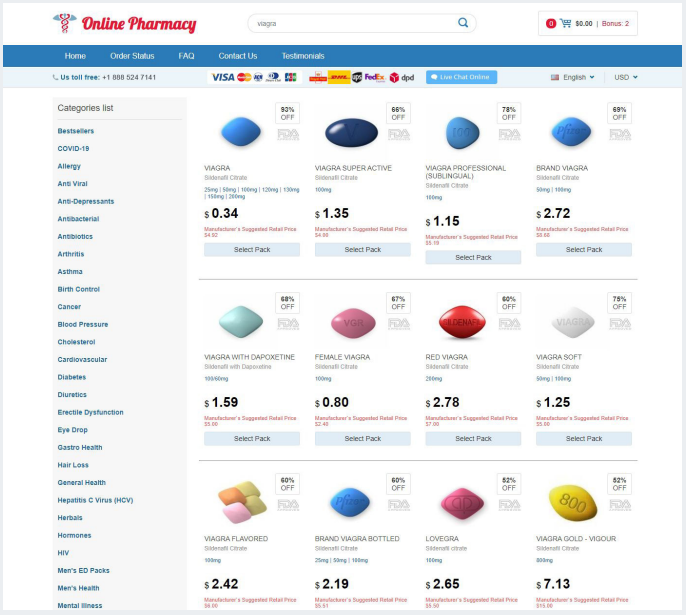
The content on these sites varies, but there were clear indications that they were part of the illegal online pharmacy networks that have operated for many years. The sites operate across hundreds, if not thousands, of domains at any given moment, and they heavily reuse content across the sites.

To find some fresh live websites, our analysts conducted a Google search for “shop + cheap viagra” which returned a list of templated domains that rank due to blackhat SEO tactics, with content templates that, while similar, contain subtle differences.

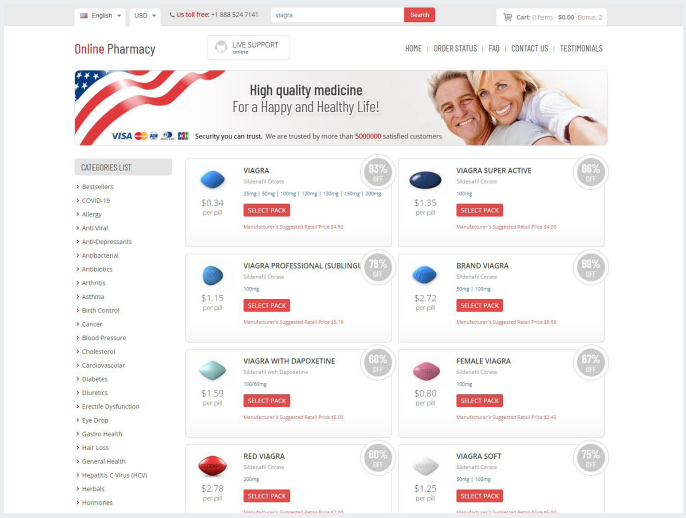
Here are a few examples:



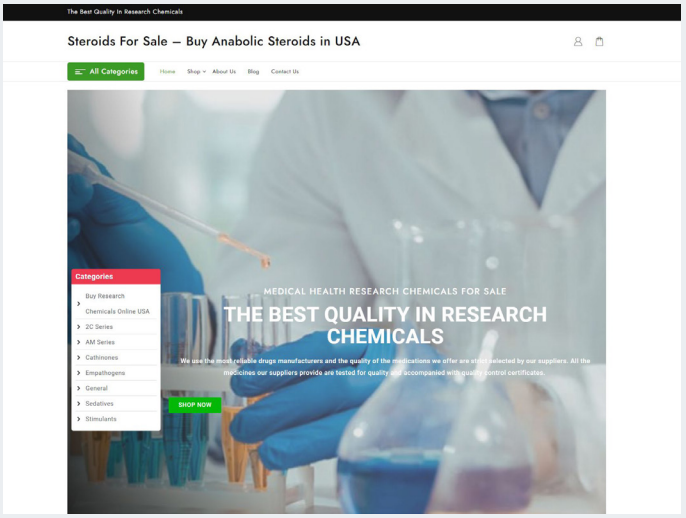
rx-qualityshop[.]com



safe-shop-it[.]com



best-shop-it[.]com

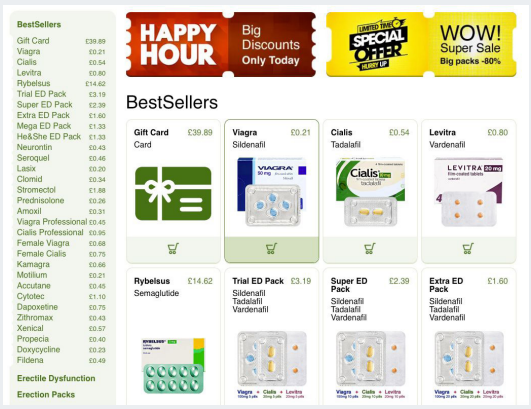


biosteroitschem[.]com

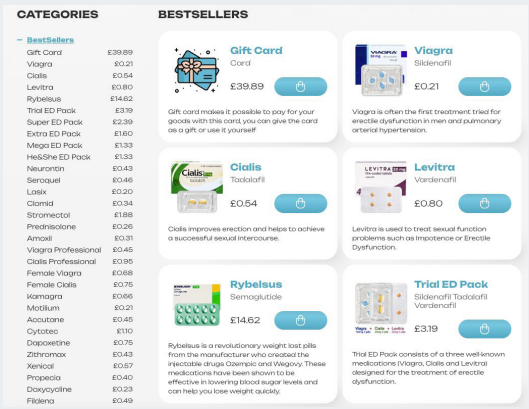
After analyzing the domains returned, our team identified several key on-page elements that we were able to use as parameters in a Silent Push Web Scanner query to reveal linked infrastructure.

Our scans returned an initial dataset of 1,000+ domains and IPs, containing 100% true positive results of websites engaged in the sale of CFMs and illegal drugs.

Looking at what we discovered, some of the new websites were re-using content templates in line with previously observed TTPs, which helped confirm they were created by the same threat actor group:

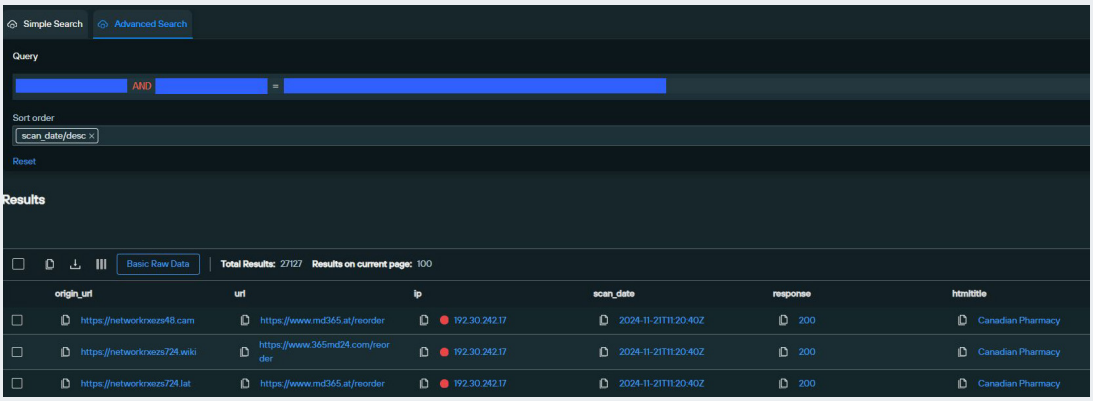


10-drugs[.]com



5-pharmacy[.]com

Once we knew our datasets contained true positive linked domains, we used further Silent Push Web Scanner queries to create a proprietary behavioral fingerprint made up of back-end web infrastructure elements, which revealed more associated CFM websites. We shared these details privately with our clients but were unable to make them public due to the threat actors continuing to launch their illegal online pharmacy infrastructure with similar fingerprints.



We created a proprietary fingerprint that revealed more CFM websites

This secondary pivot led to the discovery of nearly **4,000 unique domains and dedicated IPs** that were all part of the same active CFM campaign. Not all were active.

Many of the dedicated IPs we discovered mapped to additional domains, as well as rendering an illegal online pharmacy website.

Here's a sample of IPs that are part of this illegal online pharmacy infrastructure seemingly controlled by one threat actor group:

- 146.70.87[.]241
- 89.117.226[.]128
- 23.236.66[.]213
- 192.30.242[.]17
- 162.253.153[.]78
- 216.73.156[.]103
- 23.236.66[.]178
- 206.168.240[.]120
- 154.12.59[.]150
- 146.70.87[.]241

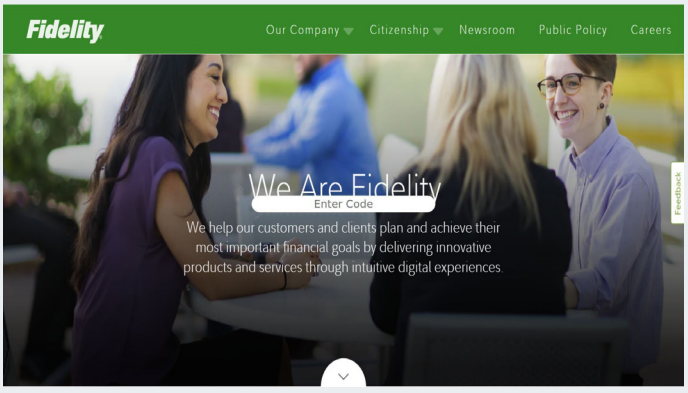
BAZARCALL

During 2024, the Bazarcall threat actors, known for posing as call center employees on behalf of reputable organizations and requesting that victims download remote desktop protocol (RDP) software to gain access to their computers, have continued to expand their infrastructure.

origin_url	url	ip	scan_date	response	htmltitle	favicon_icons
http://rtkhelp.top	https://rtkhelp.top	194.59.31.27	2024-12-11T08:55:10Z	200	Support	
http://mgbhelp.top	https://mgbhelp.top	79.110.49.101	2024-12-11T08:19:44Z	200	Support	
http://skahelp.top	https://skahelp.top	194.59.30.60	2024-12-09T07:06:55Z	200	Support	
http://mgbhelp.top	https://mgbhelp.top	79.110.49.101	2024-12-09T06:57:38Z	200	Support	
http://rtkhelp.top	https://rtkhelp.top	194.59.31.27	2024-12-09T06:56:57Z	200	Support	
http://mgbhelp.top	https://mgbhelp.top	79.110.49.101	2024-12-09T06:56:37Z	200	Support	
http://skahelp.top	https://skahelp.top	194.59.30.60	2024-12-09T06:54:44Z	200	Support	
http://rtkhelp.top	https://rtkhelp.top	194.59.31.27	2024-12-09T06:54:38Z	200	Support	
http://vrehelp.top	https://vrehelp.top	194.59.30.213	2024-12-09T06:52:59Z	200	Support	
http://kaptohelp.top	https://kaptohelp.top	194.59.30.60	2024-12-09T06:52:28Z	200	Support	
http://vrehelp.top	https://vrehelp.top	194.59.30.213	2024-12-08T06:54:37Z	200	Support	
http://skahelp.top	https://skahelp.top	194.59.30.60	2024-12-08T06:52:40Z	200	Support	
http://rtkhelp.top	https://rtkhelp.top	194.59.31.27	2024-12-08T06:52:35Z	200	Support	
http://mgbhelp.top	https://mgbhelp.top	79.110.49.101	2024-12-08T06:52:10Z	200	Support	
http://kaptohelp.top	https://kaptohelp.top	194.59.30.60	2024-12-08T06:52:06Z	200	Support	

Webscan query tracking Bazarcall – all domains on the .top suffix along with other metadata commonalities

PayPal phishing page with the phishing content gated behind a password



Fidelity phishing page, with the phishing content gated behind a password

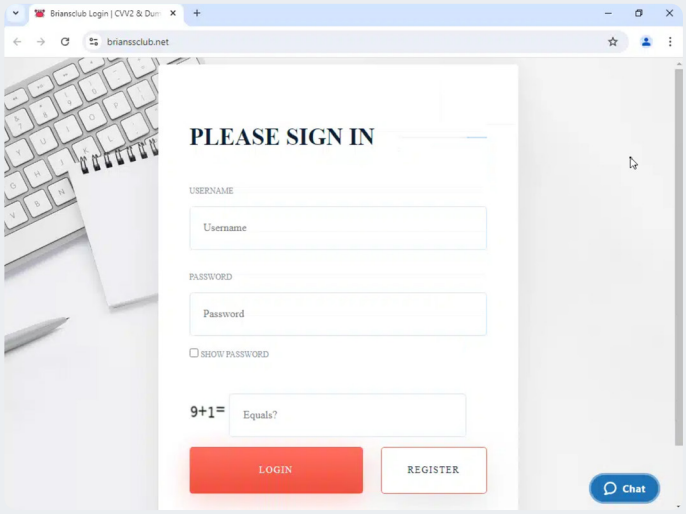
UNDERGROUND MARKETS

Silent Push has been actively tracking underground markets and underground criminal activity selling credit card information, hacking forums and other information such as sale of personal data, social media account and passwords, sale of hacked financial accounts for banks and crypto wallets, and other illicit goods.

Automate Export | Manual Export | Search Observable Name | Clear Filters | All | Feeds | Collections

Threat Name	IOC Type	Source	Vendor	Date Added (3)	Source Score (2)	Enriched Score (1)	Total Score
fresh-login.ru	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-18 14:34	100	100	100
ludipro.ru	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-14 14:32	100	100	100
moneyvalley.ru	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-13 14:31	100	100	100
dumpkingdom24.su	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-13 14:31	100	100	100
tumblr.su	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-12 14:31	100	100	100
vclub-bazar.su	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-12 14:31	100	100	100
omerta-cc.ru	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-12 14:31	100	100	100
shop-cvvme.ru	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-12 14:31	100	100	100
goldplasticnet.ru	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-12 14:31	100	100	100
maza-carder-forum.ru	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-12 14:31	100	100	100
paypalacc.ru	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-12 14:31	100	100	100
yalelodge-store.su	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-12 14:31	100	100	100
coinodeal.ru	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-12 14:31	100	100	100
best-credit-card-dump-sites.ru	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-12 14:31	100	100	100
ccshopbest.ru	Domain	Underground Threats - PII Markets and Leaks Domains	Silent Push	2024-11-12 14:31	100	100	100

Underground Marketplace IOFA feed

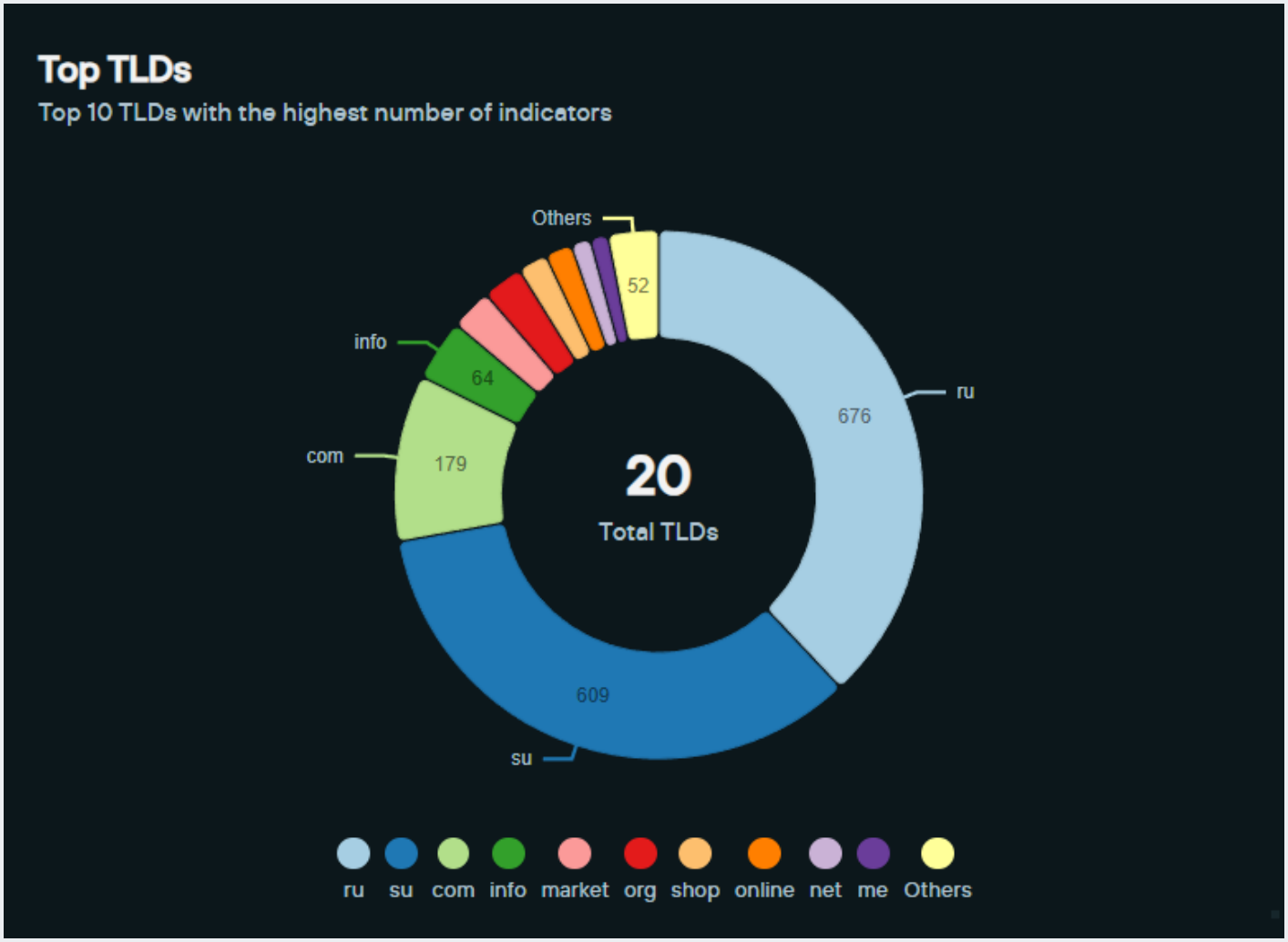


Screenshot of a BriansClub Marketplace Mirror via briansclub[.]net

Over the past year, we've identified thousands of persistent domains hosting mirrors for the drug-focused BlackSprut, Blackwave, Kraken and Mega marketplaces, as well as the popular CVV and PII dump shops Brian's Club and Ferum Shop.

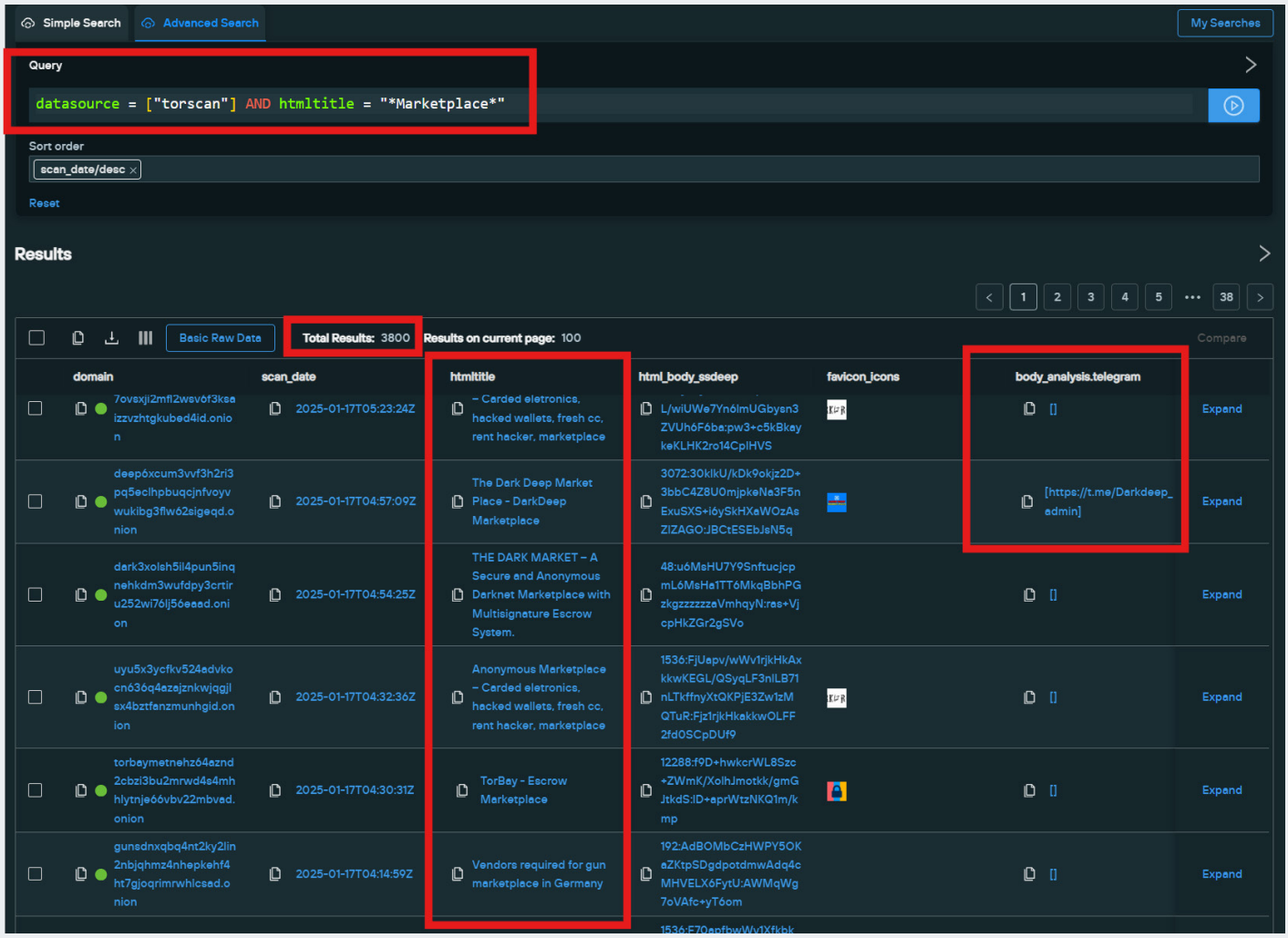
Across this feed of illicit marketplaces, the domains are hosted across 20 TLDs, but with nearly 75% of the domains either on a .ru or .su suffix – .ru is the current Russia TLD and .su is the legacy TLD for the Soviet Union.

This aligns to our understanding of Russian threat actors being behind many of these illicit online marketplaces.



Screenshot of the Underground Markets domain suffixes

Silent Push not only has a feed for illicit marketplaces on the clear web, we've also got tools for easily searching "marketplaces" on the dark web. Not only that, on these dark web websites we capture any Telegram URLs and make them easily searchable for additional pivots.



*Web Scanner query: datasource = ["torscan"] AND htmltitle = "*Marketplace*"*

5 MALWARE AND THREAT ACTOR INFRASTRUCTURE TRENDS

Trends observed by our analysts in malware and across all malicious infrastructure we tracked throughout 2024 underscored the growing sophistication and adaptability of threat actors.

Silent Push's research revealed the increasing use of custom encryption algorithms, indirect API calls, and AI-enhanced evasion tactics in malware like the BlackMoon Trojan and Lumma Stealer. Meanwhile, infrastructure trends highlighted the reliance on bulletproof registrar services, such as NiceNIC and BitLaunch, and the reuse of aged domains to obscure malicious operations.

The rise of infrastructure laundering is particularly troubling. Attackers leverage reputable cloud providers like Microsoft and Amazon to add legitimacy to their campaigns while remaining seemingly unnoticed by their hosting providers and the security world.

From an industry perspective, the shift toward more resilient and anonymized infrastructure poses significant challenges to traditional detection and takedown efforts. The integration of Fast Flux DNS, wildcard SSL certificates, and highly distributed hosting environments has made it increasingly difficult to pinpoint and disrupt malicious campaigns.

Silent Push's work in mapping these infrastructures and providing actionable IOFAs has been instrumental in helping organizations proactively address these challenges. As malware continues to evolve and threat actor infrastructure becomes more robust, the cybersecurity industry must prioritize innovative detection methods and global collaboration to stay ahead of these persistent threats.

Note: *For more information on how your organization can leverage Silent Push to defeat the rising number of cyber threats it faces, please contact our Sales team.*

FIN7 MALWARE CAMPAIGNS

In late Summer 2024, Silent Push analysts discovered a new FIN7 campaign that used a series of AI "deepfake nude generator" websites that were actually honeypots serving malware to unsuspecting visitors. The public details of that report can be found here.

One interesting tactic observed in our analysis of the campaign was FIN7's use of SEO tactics to spread their malware. All FIN7 AI deepfake honeypots we found contained a footer link for "Best Porn Sites," which redirected users to aipornsites[.]ai – a website that promotes the domain "ainude[.]ai" – that is currently down – but appeared to be the same website template used on the FIN7 honeypots. Additional details, analysis, and IOFAs found from this campaign and its malware can be found in our enterprise-only TLP: Amber report and FIN7 intelligence feeds.

MALWARE IDENTIFIED ON OPEN DIRECTORIES

BLACKMOON TROJAN

The BlackMoon Trojan, first identified in 2014, is a banking malware known for targeting users in South Korea, using phishing tactics and malicious redirects to compromise credentials and facilitate unauthorized access to financial accounts.

Our team identified a new malware variant currently under development, showcasing advanced evasion techniques. Developed in MFC C++, the malware employs encrypted strings and indirect API calls to significantly complicate analysis.

A standout feature is its custom Base64 encoding algorithm, specifically designed to bypass standard decoding methods. Additionally, the presence of debug logs and several unimplemented functions suggests this malware is still in its early stages. These findings highlight the potential for further sophistication as development continues.

LUMMA STEALER

Our team observed the emergence of a new tactic utilized by the Lumma Stealer malware in 2024. This variation of the threat builds its own HTTPS connections independently, circumventing conventional Windows APIs and making detection and analysis significantly more challenging. Our investigation also revealed this variant leverages Steam-related elements in its communications, further emphasizing its evolving sophistication.

CHROME APPBOUND ENCRYPTION

During 2024, our team observed some pushback against malware stealers with protection enhancements in Chrome for users, but later discoveries have since shown that newer threats, like the Glove Infostealer, have managed to bypass these safeguards.

BULLETPROOF HOSTS

The practice of bulletproof hosting (BPH) is described as a service provided by an internet hosting operator that is resistant to takedown efforts and is usually located in jurisdictions with more lenient regulations and/or countries where law enforcement has fewer resources to monitor and control. Hosting service providers involved in BPH support all types of unwanted activities, including but not limited to the abuse of copywritten materials, hosting of malware and botnet command and control (C2) servers, hate speech and misinformation support, illegal gambling, pornography, and spam.

Our team put considerable effort into researching bulletproof hosts throughout 2024 by a wide array of threat actors, and while covering the full extent of our research is unfortunately beyond the scope of this paper, we have several releases currently planned to fill this gap. We encourage readers to look forward to our BPH-focused publications coming later this year!

THE RISE OF THE BULLET PROOF REGISTRAR

NiceNIC International is an ICANN-accredited registrar and hosting provider founded in 2012 in Hong Kong by Zheng Wang.

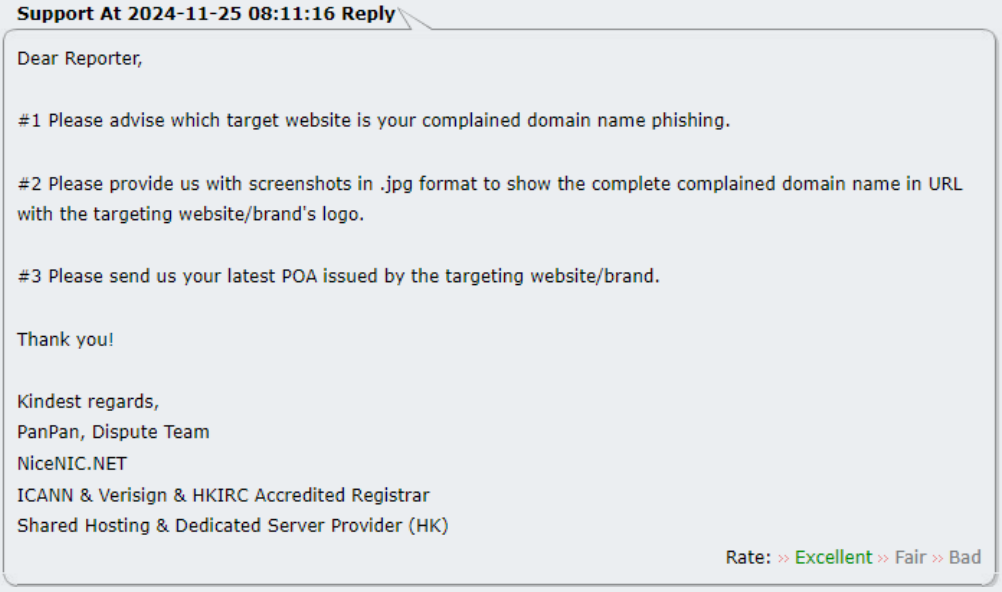
The main website, nicenic.net, has the HTML title: "Register Domain by Bitcoin | Buy Domain with Crypto Payment | Buy Web Domain," which emphasizes this service's acceptance of digital currencies. Reviewing their documentation and knowledge base reveals *.my-ndns[.]com are this service's default name servers.

During 2024, Silent Push identified an increasing number of threat actors resorting to NiceNIC for registering their malicious infrastructure, including Scattered Spider, FIN7, CryptoChameleon, and Hunters International.

The ratio of malicious domains registered on this service from the total of new registrations is out of proportion for an innocuous service, as the vast majority has been serving campaigns ranging from phishing, malware C2, crypto scams, and underground markets, among others.

Silent Push analysts were also able to confirm in 2024 that NiceNIC continues to have a process for requesting the takedown of domains that is nearly impossible to accomplish – they require having a "Power of Attorney" over a victim and a letter to prove that relationship.

As you can see in the screenshot below, the third requirement from NiceNIC to get infrastructure taken down is, "Please send us your latest POA issued by the targeting website/brand."



Support At 2024-11-25 08:11:16 Reply

Dear Reporter,

#1 Please advise which target website is your complained domain name phishing.

#2 Please provide us with screenshots in .jpg format to show the complete complained domain name in URL with the targeting website/brand's logo.

#3 Please send us your latest POA issued by the targeting website/brand.

Thank you!

Kindest regards,
PanPan, Dispute Team
NiceNIC.NET
ICANN & Verisign & HKIRC Accredited Registrar
Shared Hosting & Dedicated Server Provider (HK)

Rate: » Excellent » Fair » Bad

Screenshot of an email from the NiceNIC Dispute Team

BITLAUNCH

Throughout 2024, our team observed various threat actors (Scattered Spider, Gamaredon, and Prolific Puma) acquiring servers on Vultr and DigitalOcean through BitLaunch, a company that provides “anonymous cloud VPS hosting from DigitalOcean, Vultr, Linode and on their own hardware, payable with Bitcoin and 10+ other cryptocurrencies.”

PROLIFIC PUMA

Prolific Puma provides URL shortening services to cybercriminals, allowing threat actors to hide their infrastructure during the initial distribution hop, having served almost every type of malicious campaign, from phishing and spam to malware.

Similar to popular, legitimate URL shortening services, the URLs generated by Prolific Puma follow the pattern: http(s|)://<prolific_puma_controlled_domain>/<encoded_string>

If the correct path is provided, the string will be decoded, and the victim redirected to the attacker-controlled malicious page.

Silent Push identified thousands of new domains created by Prolific Puma operators in 2024, as this network consistently had hundreds of redirects active simultaneously.

6 SILENT PUSH HIGHLIGHTS & APP IMPROVEMENTS

CLOUDFLARE UNMASKING

Throughout 2024, Silent Push researchers noted a trend among several malicious campaigns where threat actors used Cloudflare services to proxy their infrastructure, thus hiding the real IP addresses the campaigns were being served from.

Analyzing DNS records of the domains registered on NiceNIC during a one-week period revealed about 1,000 of the domains used Cloudflare to proxy their web pages within the first 48 hours of creation. This accounted for about 68% of the total infrastructure registered on that service during the timeframe.

The Silent Push app offers many Cloudflare unmasking techniques using PADNS and Webscan datasets.

One threat actor that consistently uses this technique is CryptoChameleon.

Query	Query ASN	Answer	Answer ASN	First Seen	Last Seen	Type
285089-coinbase.com	-	104.26.6.96	13335	2024-11-23 23:50:31	2024-11-25 13:03:18	A
285089-coinbase.com	-	172.67.72.75	13335	2024-11-23 23:50:31	2024-11-25 13:03:18	A
285089-coinbase.com	-	104.26.7.96	13335	2024-11-23 23:50:31	2024-11-25 13:03:18	A
285089-coinbase.com	-	104.234.204.217	399486	2024-11-23 23:31:38	2024-11-23 23:31:38	A
285089-coinbase.com	-	127.0.0.127	-	2024-11-18 13:52:11	2024-11-23 11:48:37	A
285089-coinbase.com	-	lucy.ns.cloudflare.com	-	2024-11-23 23:50:31	2024-11-25 11:25:44	NS
285089-coinbase.com	-	langston.ns.cloudflare.com	-	2024-11-23 23:50:31	2024-11-25 11:25:44	NS
285089-coinbase.com	-	ns3.my-ndns.com	-	2024-11-18 12:15:35	2024-11-23 23:31:38	NS
285089-coinbase.com	-	ns4.my-ndns.com	-	2024-11-18 12:15:35	2024-11-23 23:31:38	NS

Advanced domain query showing part of the CryptoChameleon infrastructure

NEW DATA SOURCES

Ad tech data | Telegram URLs | ICP License Numbers

In 2024, we continued our bulk scanning and resolving of content on the internet, capturing DNS changes, certificates, and WHOIS data to empower organizations with over 100 metadata fields available for search. We never delete data, and now have over three years of data available for searching.

We've also been able to add several requested fields of data, which provides unique opportunities for pivots.

In April 2024, we started scanning for ads.txt, app-ads.txt, and sellers.json data, which are public files hosted on domains that contain "authorized advertising partners" and use a specific schema introduced by the IAB[.]com. We captured this data across the internet and found a series of UK government websites that were sending user data to a controversial Chinese ad tech vendor. Hours after our piece had been published, the Chinese vendor was purged from the Government websites, preventing them from collecting data on visitors of those sites and monetizing their visits.

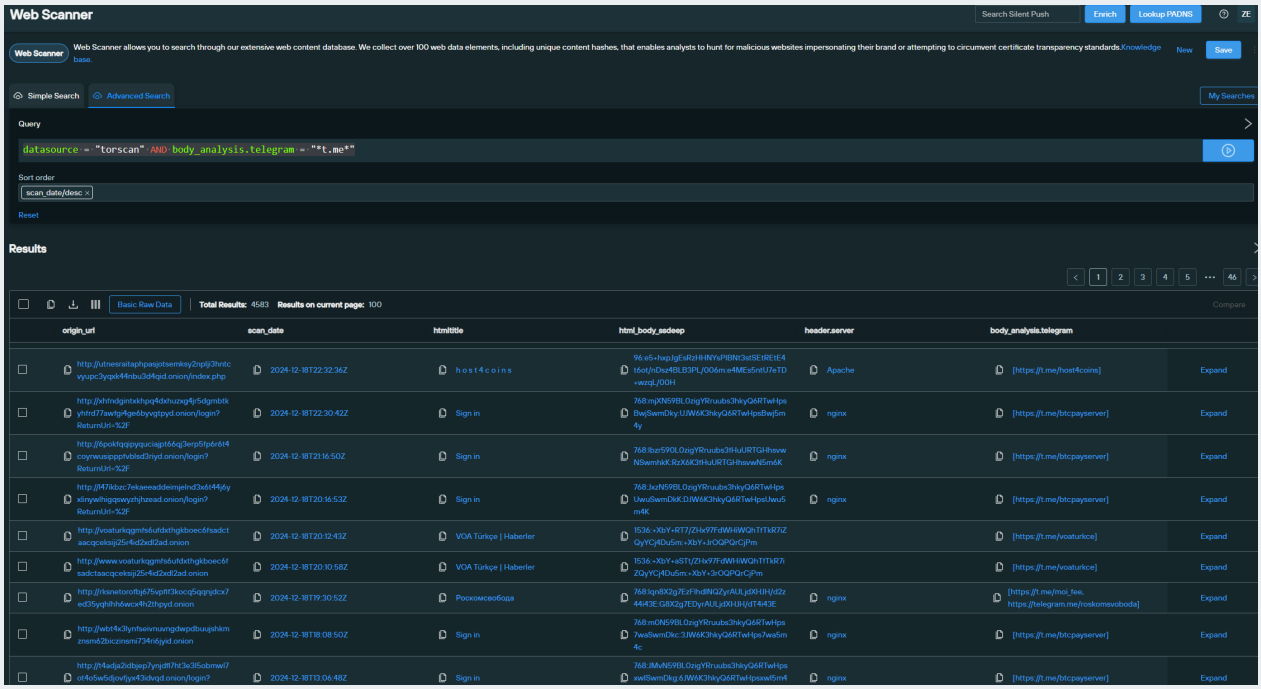
Since starting this collection of advertising data, we now have SHA256 hashes available for search in our Web Scanner for these fields:

adtech.ads_txt	adtech.app-ads_txt_sha256
adtech.ads_txt_sha256	adtech.sellers_json
adtech.app_ads_txt	adtech.sellers_json_sha256

About halfway through 2024, we started to collect a new, valuable field of data from our web scanning: Telegram URLs. This feature makes it possible to search for exact Telegram URLs that we've seen on various homepages, often included by specific threat actors and some corporate organizations.

Combining this Telegram feature with our source of dark web data allows us to quickly parse the approximately 6,000 results in our Web Scanner that embed specific Telegram URLs. This offers a great source for finding potentially problematic Telegram channels.

Here's a query to see these results:



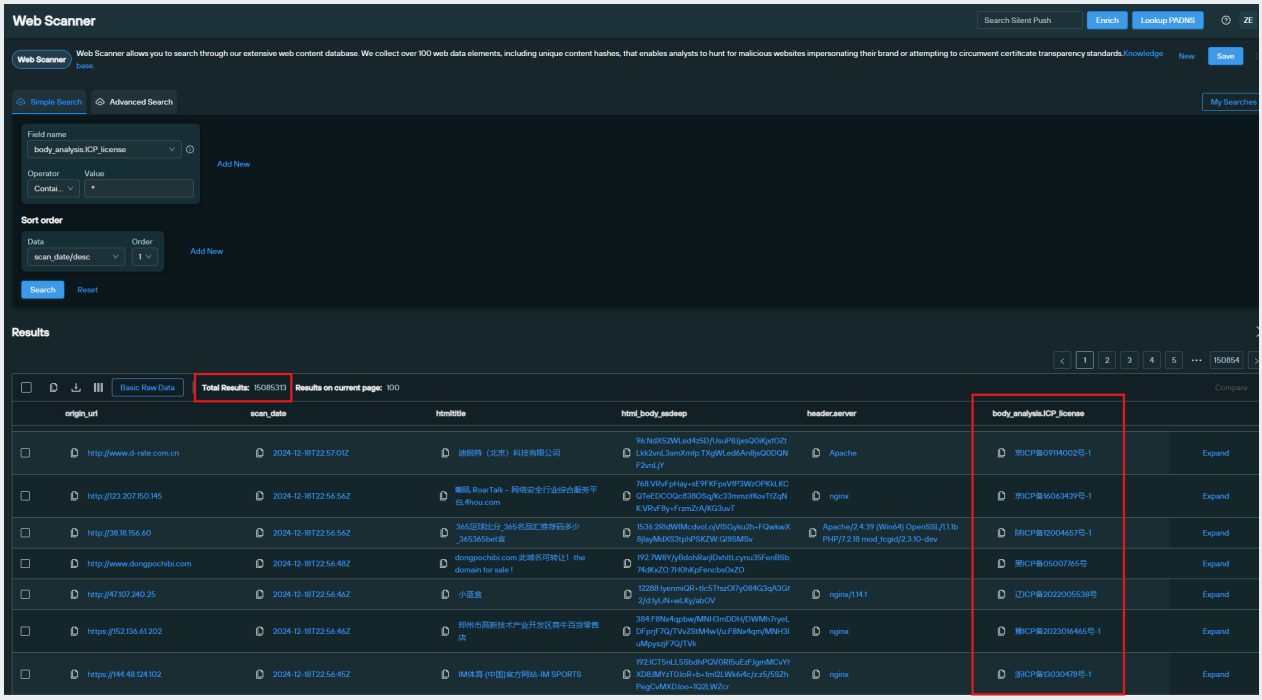
*Datasource = "torscan" AND body_analysis.telegram = "*t.me*"*

Across both the dark and clear webs, we currently have over 3.1 million results in our Web Scanner that contain this body_analysis.telegram field – creating numerous opportunities for new pivots.

In the Spring of 2024, our team quietly started collecting Chinese Internet License Numbers known as "ICP Licenses." These are consistently structured IDs embedded into the footer of some Chinese websites that are needed to apply for a license to send data through the Great Firewall. An example of one of these ICP License IDs can be seen in our recent research into the AIZ Retail and Crypto phishing network:

ssrchat[.]com ICP license

Since starting our ICP scanning earlier this year, we now have over 15 million records available in Web Scanner with this field.



Web Scanner query for body_analysis.ICP_license = ""*

Moving into 2025, we look forward to adding new fields to our collections and appreciate any suggestions – please share them with info@silentpush.com or through your Silent Push representative.

7 STRATEGIC RECOMMENDATIONS

As the prevalence and complexity of 2024's cyber threats showed, preemptive threat intelligence is the evolution necessary for proactive defense over prior, stale methodologies. Mapping malicious infrastructure from a global rather than a limited field of view is the optimum way to combat the scaling capacity and effectiveness of AI-enabled cyber threats.

Silent Push's approach, which involves providing organizations with IOFAs to enable detection of threats *before* they are weaponized, is the most effective means of securing an organization's threat surface. By consuming our actionable intelligence reports and utilizing our first-party data, organizations can empower their security teams to appropriately challenge and defend against cyber threats.

UTILIZING SILENT PUSH OFFERINGS

- **IOFAs for Proactive Defense:** Silent Push IOFA feeds enable organizations to detect adversary infrastructure early, providing a critical advantage in the prevention of attacks when every second matters.
- **Enriched DNS Data:** Silent Push's world-renowned platform enables threat hunters to pivot through unparalleled datasets with surgical precision, uncovering hidden connections and creating expansive fingerprints to continuously track malicious infrastructure even as more is spun up.
- **Threat Intelligence Reports:** Silent Push provides in-depth TLP: Amber reports, detailing threat actors' activities in step-by-step analytical breakdowns complete with examples and immediately useable (and actor-transferrable) pivots in-platform.

ACTIONABLE STEPS FOR ORGANIZATIONS

1. **Integrate IOFAs:** Incorporate Silent Push feeds into existing monitoring tools to mitigate threats before they can strike.
2. **Leverage DNS Data:** Access our enriched DNS datasets and "Total View" breakdowns of domains and IP addresses to proactively hunt for threats and discover new attack patterns.
3. **Digest Gold Standard Intelligence Reports:** Consume Silent Push's reports as an upskill opportunity for your organization's defenders as well as critical awareness of threat actor trends and capabilities.

By adopting a pivotal shift in focus, security teams can move from providing *reactive* threat intelligence to *preemptive* threat intelligence. As seen in this report, that insight has allowed Silent Push to "open the aperture" and shine our light on previously unknown, unseen, and *unmitigated* attacker infrastructure. Adopting our methods will enable organizations to better position themselves to proactively mitigate cyber threats – stopping adversaries not just at the gates but before their attacks are ever launched.

8 PREDICTIONS FOR 2025

As threat actors continue to evolve, 2025 is poised to bring both new challenges and novel strains for organizations striving to secure their environments. The wide-ranging growth in malicious activity observed in 2024 highlights the urgent, industry-wide need for preemptive threat intelligence.

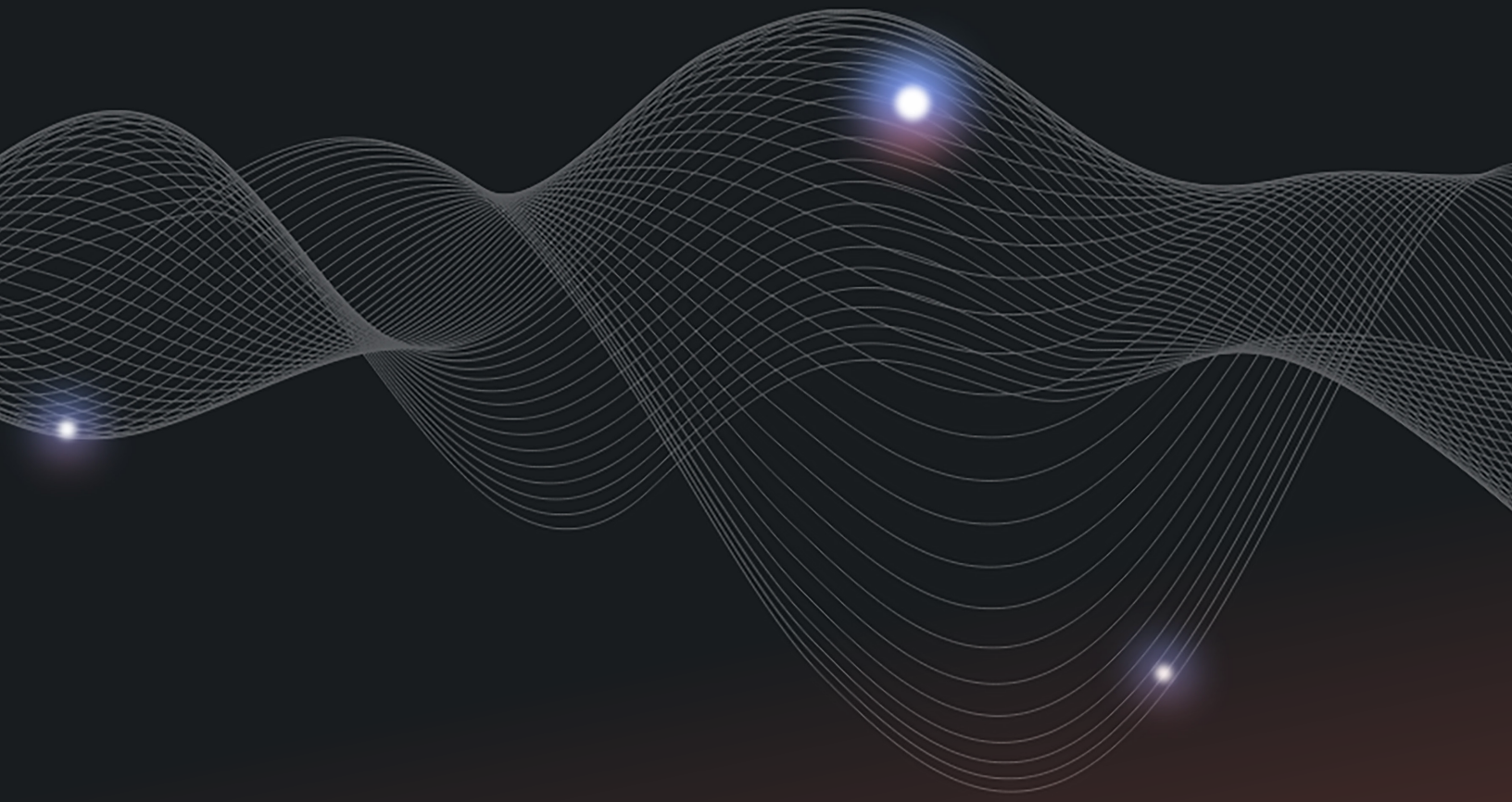
Silent Push expects to see threat actors leveraging AI even more aggressively in the coming years, using it to deploy ever-more-scalable malicious infrastructure, automate their phishing campaigns, and obfuscate malware packages in many ways. This trend is likely to exacerbate the complexity of cyber attacks, forcing organizations to change their security approaches and adopt the use of more sophisticated tools to stay ahead.

The growing reliance on advanced infrastructure management tactics, such as bulletproof hosting, Fast Flux DNS, and proxying malicious infrastructure via Cloudflare after aging it, is likely to become more prevalent in 2025. Threat actors' ability to adapt quickly to takedowns and pivot into alternate infrastructure will demand continuous monitoring and the application of purpose-driven detection methods. Collaboration between cybersecurity providers, enterprise organizations, and law enforcement the world over will be more essential to disrupting and mitigating adversaries' operations.

9

PUSHING THE BOUNDARIES OF MODERN THREAT INTELLIGENCE

Silent Push's preemptive approach to threat intelligence and continuously expanding observation of global internet architecture, backed by game-changing first-party data, are critical in helping organizations navigate and mitigate the advanced threats facing them now and in the future. As our industry shifts to combat increasingly resourced and sophisticated cyber threats, the ability to preemptively ruin adversaries' plans by mitigating attacks ***before*** they are launched will define the success of cybersecurity strategies in 2025 and beyond.



SILENT PUSH

PREEMPTIVE CYBER INTELLIGENCE WITH
INDICATORS OF FUTURE ATTACK

Silent Push provides preemptive cyber intelligence exposing threat actor infrastructure as it's being set up. Our Indicators of Future Attack (IOFA) act as an early warning system to defend against threats. We go beyond stale IOCs and create a unique digital fingerprint of adversary behavior enabling you to proactively block hidden attacks before they're launched.

Get started today.

silentpush.com