PoisonSeed Campaign Targets CRM and Bulk Email Providers in Supply Chain Spam Operation

By Peggy Kelly

Published: 2025-04-03 · Archived: 2026-04-05 18:36:55 UTC

Key Findings

- Silent Push Threat Analysts are sharing our discoveries related to a cryptocurrency and bulk email provider phishing campaign targeting enterprise organizations and VIP individuals outside the cryptocurrency industry, along with a supply chain spam operation targeting individual crypto holders with a novel “crypto seed phrase” phishing effort. We are naming this new threat “**PoisonSeed**.”
    - Targeted crypto companies include **Coinbase** and **Ledger**, and targeted CRM and bulk email providers include: **Mailchimp, SendGrid, Hubspot, Mailgun**, and **Zoho**.
- We are classifying PoisonSeed distinctly from two loosely aligned threat actors: Scattered Spider and CryptoChameleon, both of which are associated with “The Comm” (also spelled “The Com”).
- Our team has confirmed connections between two attacks that occurred in March 2025:
    - A phishing attack targeting Troy Hunt to compromise his MailChimp account and a crypto phishing campaign sent from a compromised Akamai SendGrid account.
    - Bleeping Computer reported the Akamai SendGrid account sent out crypto spam after it had been compromised.
- Silent Push Threat Analysts are publicly revealing that the compromised Akamai SendGrid account sent out SendGrid phishing messages to at least one other enterprise organization, with a phishing email promoting the domain sso-account[.]com.

Table of Contents

Executive Summary

PoisonSeed threat actors are targeting enterprise organizations and individuals outside the cryptocurrency industry. They have been phishing CRM and bulk email providers’ credentials to export email lists and send bulk spam from the accounts. Email providers appear to be targeted mainly to provide infrastructure for cryptocurrency spam operations.

Recipients of the bulk spam are targeted with a cryptocurrency seed phrase poisoning attack. As part of the attack, PoisonSeed provides security seed phrases to get potential victims to copy and paste them into new cryptocurrency wallets for future compromising.

We detected similarities between PoisonSeed, Scattered Spider, and CryptoChameleon (the latter two being threat groups spun from “The Comm,” a threat actor community comprised mostly of young, Western individuals). Our team believes the ties to Scattered Spider are not definitive, which we will explain later in this report. It is important to note that while we see commonalities with CryptoChameleon, the PoisonSeed campaign is currently being classified separately due to multiple unique data points distinguishing the two and a general lack of code commonalities between the groups.

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

Background

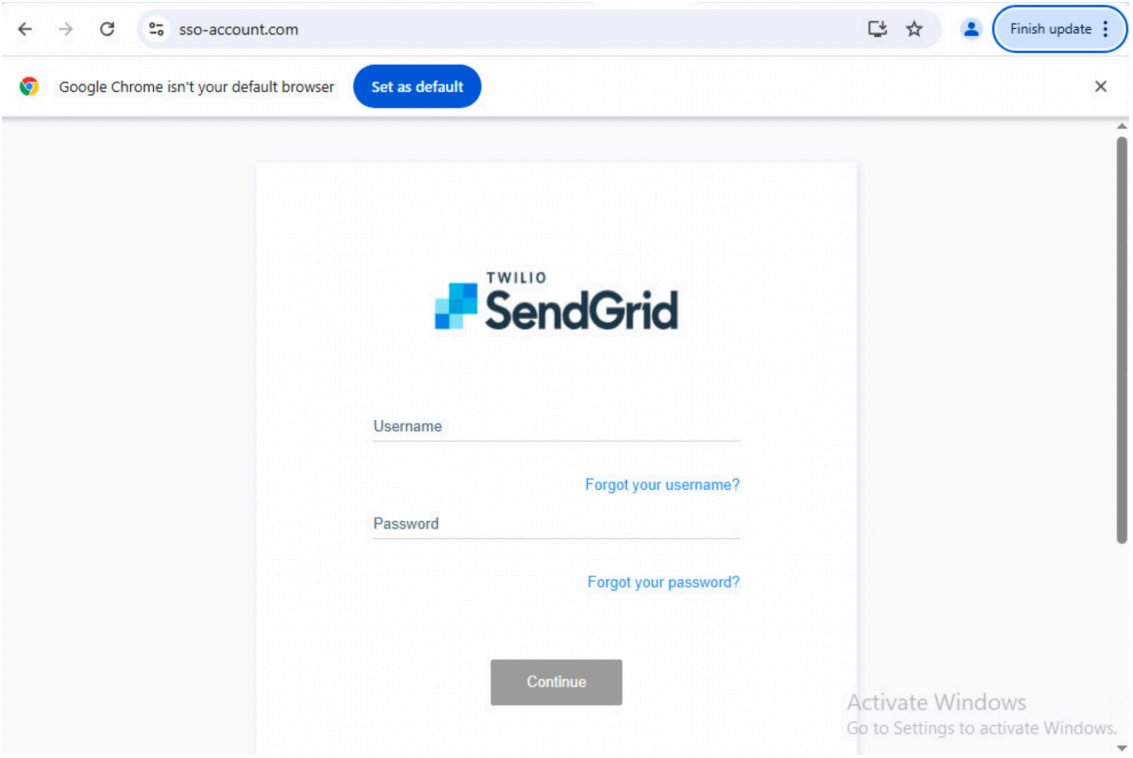
A few organizations and media outlets have individually covered the threat actors behind PoisonSeed without anyone connecting the dots to their true origin — until now.

PoisonSeed is in fact the same campaign that recently targeted Troy Hunt, which he wrote about on March 25, 2025, “A Sneaky Phish Just Grabbed my Mailchimp Mailing List”

It’s also the same campaign Lawrence Abrams wrote about for Bleeping Computer on March 14, 2025, “Coinbase phishing email tricks users with fake wallet migration”

The threat actor group has been setting up phishing pages for prominent CRM and bulk email companies, including: **Mailchimp, SendGrid, Hubspot, Mailgun**, **Zoho,** and likely others.

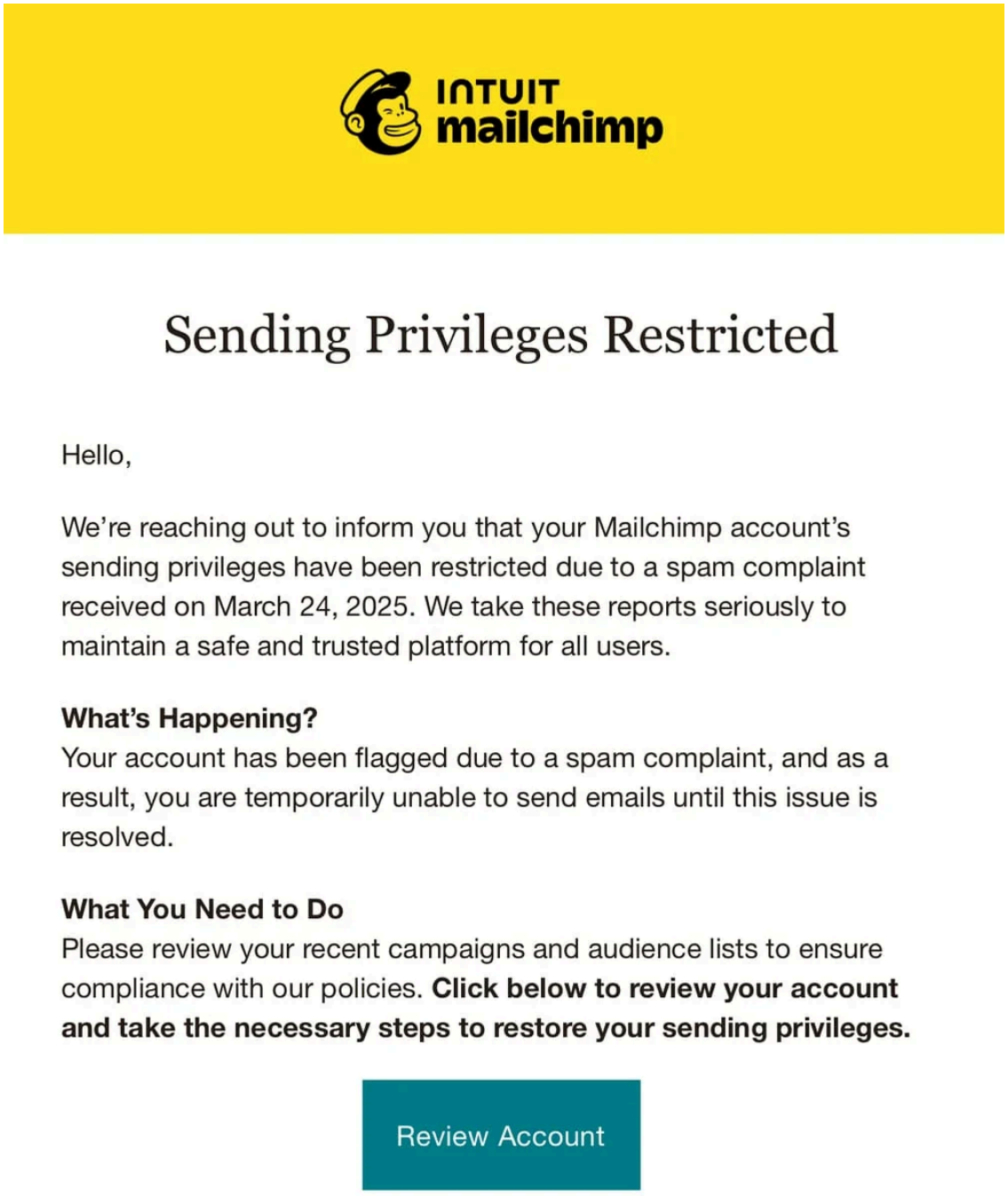
These phishing pages were essentially pixel-perfect matches for the real login pages:



Example of a SendGrid phishing page on sso-account[.]com that is part of an ongoing campaign

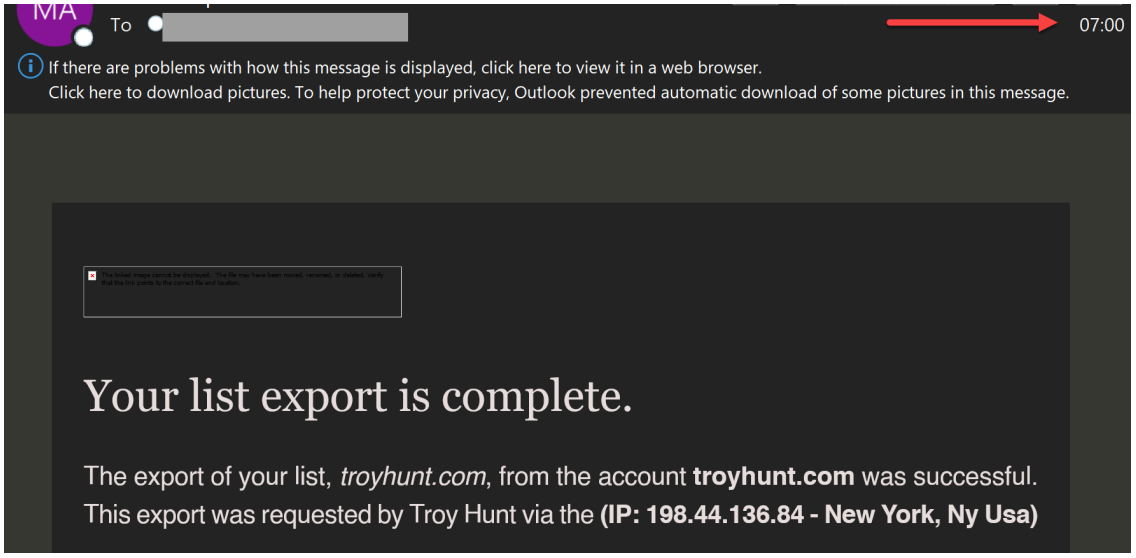
Once the phishing pages were set up, phishing emails were sent to very specific email addresses. In Troy Hunt's example, his "**mailchimp**@redacted" email was used (and it was only used to log in to Mailchimp).

The phishing email used a "Sending Privileges Restricted" lure, and it appeared to have been sent by another compromised business email account.



Screenshot of the phishing email sent to Troy Hunt

When credentials are successfully phished for an email provider, PoisonSeed appears to automate the process of bulk downloading the email lists. Troy Hunt shared the timeline to help confirm that the process of exporting the lists was extremely quick and likely automated.



Screenshot of the Mailchimp list export email sent to Troy Hunt

The threat actors created a new API key so they could maintain persistence if only the password was reset. This would likely have been used to send bulk emails:

Screenshot of Mailchimp API Keys from Troy Hunt

The threat actors behind PoisonSeed were observed attempting to acquire email lists and also sending spam from compromised accounts.

March 2025 Akamai SendGrid Compromise

Akamai had one of these bulk email account breaches earlier in March 2025, covered by Bleeping Computer. The breach involved spam sent from the Akamai SendGrid account in a Coinbase cryptocurrency seed phrase poisoning attack.

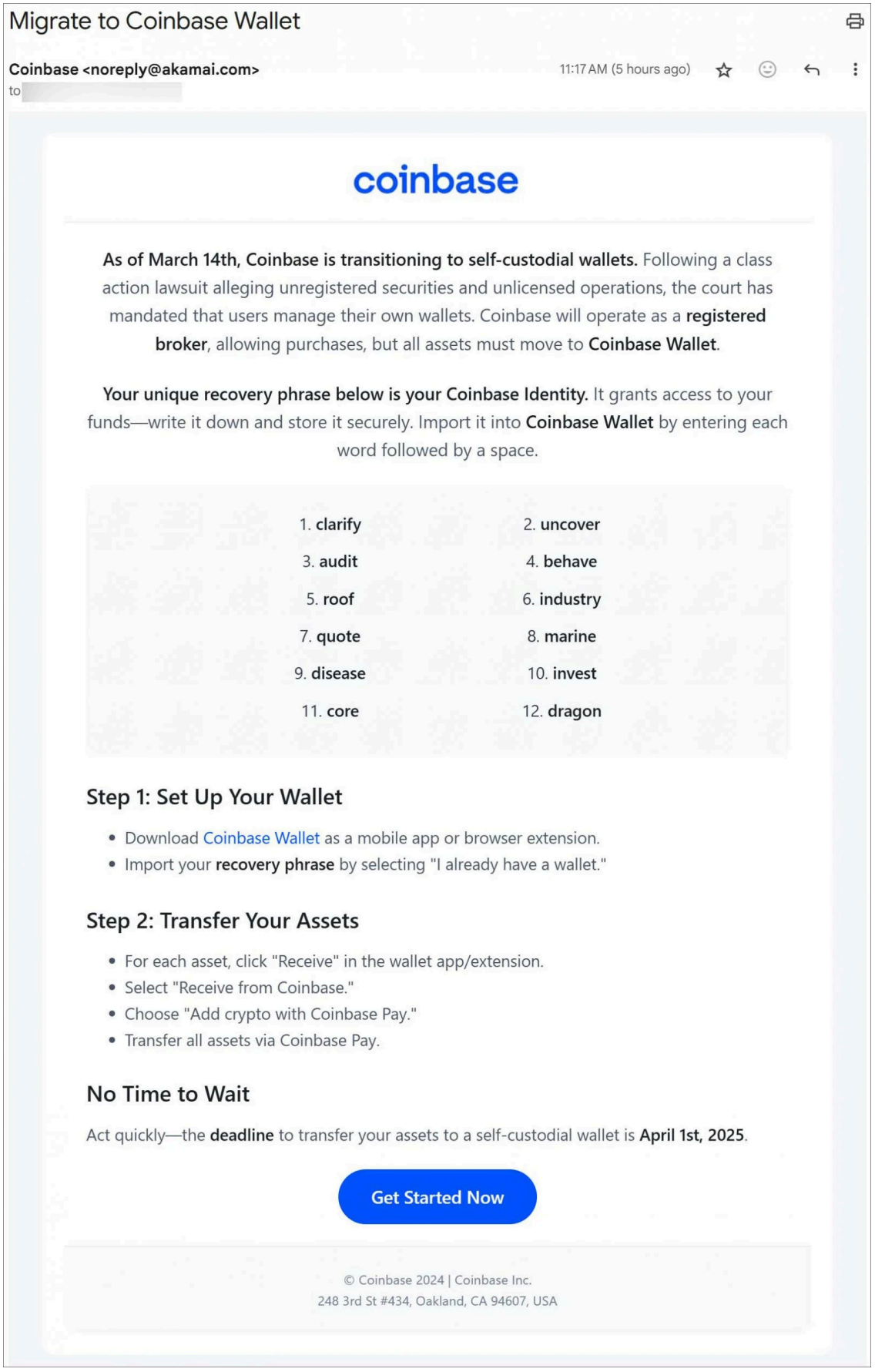
The email headers for the cryptocurrency phishing effort included @akamai[.]com as the “From sender” (which can be spoofed, but apparently wasn’t in this instance).

Created at:	Fri, Mar 14, 2025 at 11:17 AM (Delivered after 1 second)
From:	Coinbase <noreply@akamai.com>
To:	
Subject:	Migrate to Coinbase Wallet
SPF:	PASS with IP 167.89.33.244 Learn more
DKIM:	'PASS' with domain akamai.com Learn more
DMARC:	'PASS' Learn more

Email headers for the Coinbase phishing effort sent from Akamai

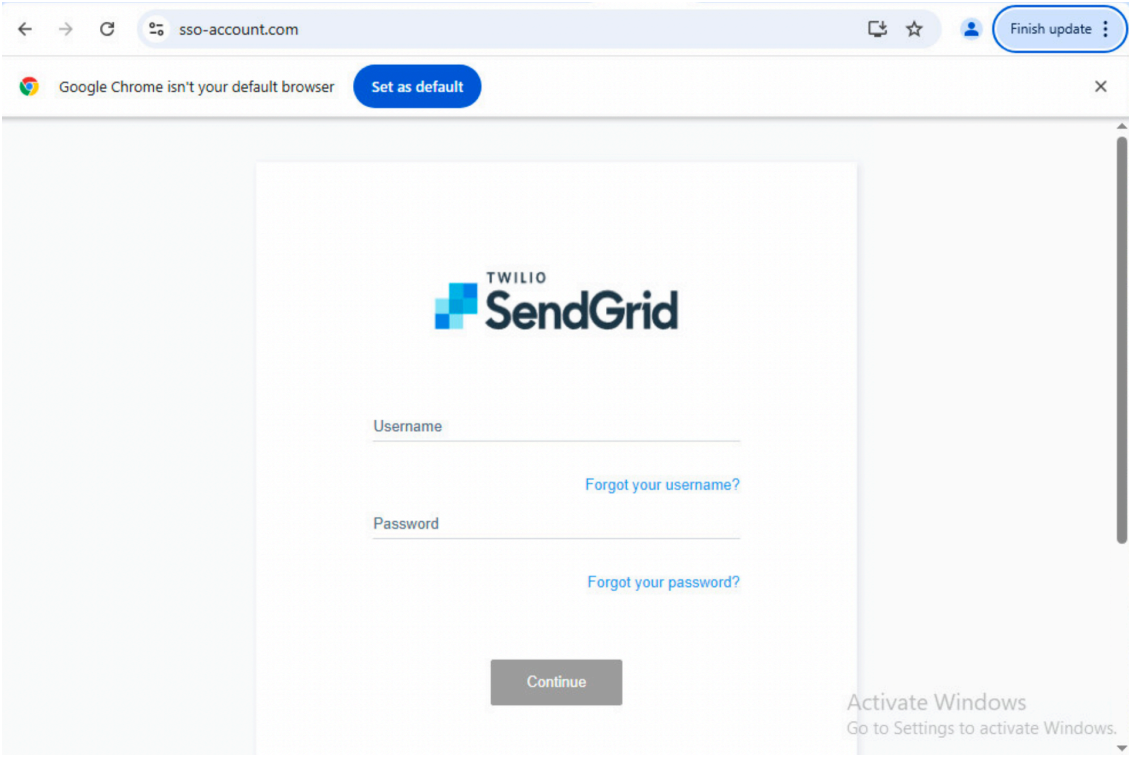
Some of the post-CRM-compromise supply chain spam phishing attempts used a complex cryptocurrency seed phrase poisoning effort with an urgent notice claiming “Coinbase is transitioning to self-custodial wallets.”

The prompt told the targeted victim that they needed to set up a new Coinbase Wallet. The threat actor then introduced the phishing aspect by providing seed phrases, hoping the victim would manually enter them into the account creation flow so the threat actor could use the specific phrases to later “recover” the account and transfer away stolen funds.



Phishing example directing victims to "update" their Coinbase Wallets

Silent Push Threat Analysts privately received details from a research sharing partner about the Akamai SendGrid compromise. At the same time that Akamai's compromised SendGrid account was sending Coinbase phishing messages, it also sent out phishing messages to at least one business (and likely many others) with a message that directed users to a phishing page attempting to compromise their SendGrid account – likely to continue the scam with even more bulk email accounts.



Screenshot of sso-account[.]com, a domain that Akamai's SendGrid was sending out, according to one of our research sharing partners

Akamai acknowledged the recent threat but hasn't provided significant updates, telling Bleeping Computer on March 14, "Akamai is aware of reports regarding a potential phishing scam targeting Coinbase users that involves an Akamai email domain. We take information security very seriously and are actively investigating the matter."

It's unclear how many messages were sent out via Akamai, but many email accounts beyond Akamai appear to have been compromised by the threat actors and used for phishing spam. After a few days (or sooner), the accounts appeared to be cleaned up, but by then, the threat actors had phished new email accounts for their spamming operations.

Research Methodology

For operational security reasons, we are unable to make all fingerprints used to track this campaign public. We are sharing what we can below, in the hopes that other organizations and researchers can benefit.

Initial Research Lead

After the March 14, 2025, Akamai-compromised phishing campaign, Silent Push analysts were given a related domain that was sent to one of our research sharing partners: sso-account[.]com.

We captured a SendGrid phishing page on this domain and fingerprinted the kit so that we could find variations of it on other domains.

Looking deeper, our team found 49 unique domains that featured references to the targeted email platforms and Coinbase. Two domains mentioning “firmware” (firmware-llive[.]com and firmware-server12[.]com) were both used for a Ledger Wallet phishing effort, which helped our team uncover some of PoisonSeed’s command and control (C2) domains.

WHOIS Pivots

When checking this PoisonSeed grouping, most of the domains found via the phishing kit fingerprint pivot were unique within the WHOIS “State” field. Other threat analysts have mentioned this detail publicly, so we are making the following details available as well to support defenders in their efforts.

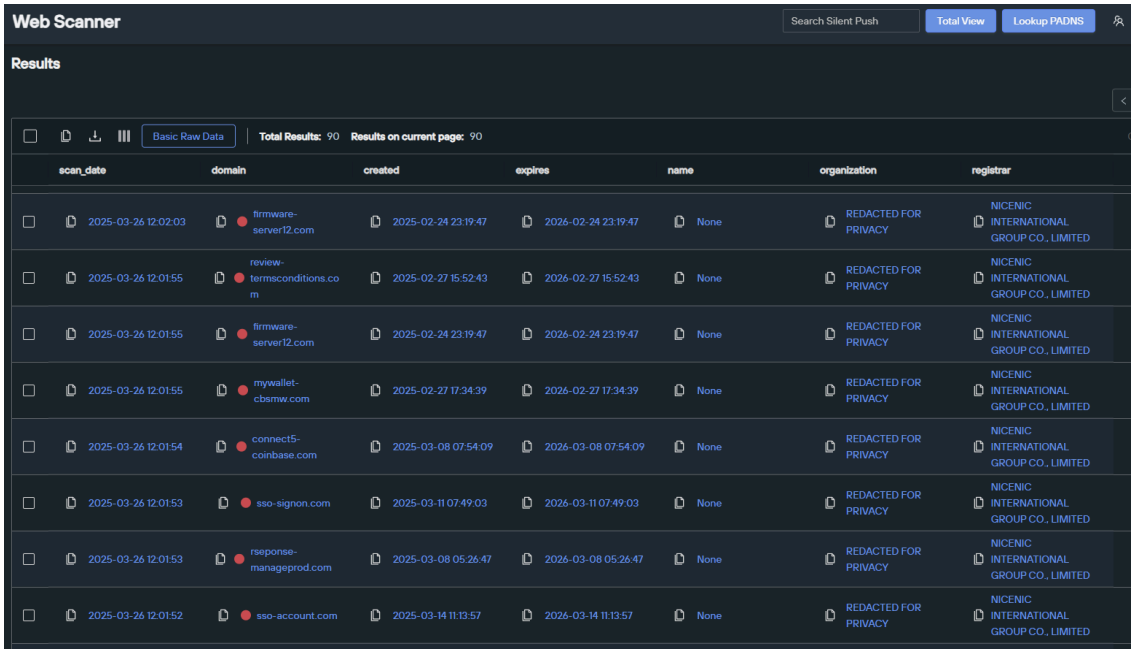
Within the domains we had tracked with our phishing kit fingerprint, there were groupings of domains found which included one of four strings in this WHOIS “State” field—two with obscene phrases—being reused over and over in that field: **“headstompn⬛ggerfucke”, “creampie city”, “asdf” or “123123”***.

**Note: For community users following along with the query below, please note that we have redacted the racist word above—the “i” has been replaced with a “⬛”.*

Our team then created a simple WHOIS “State” query with the two specific (obscene) words that are not likely to be reused in that field by other registrants to identify part of the infrastructure:

Silent Push WHOIS Scanner search:

- datasource = “whois” AND state = [“headstompn⬛ggerfucke”, “creampie city”]

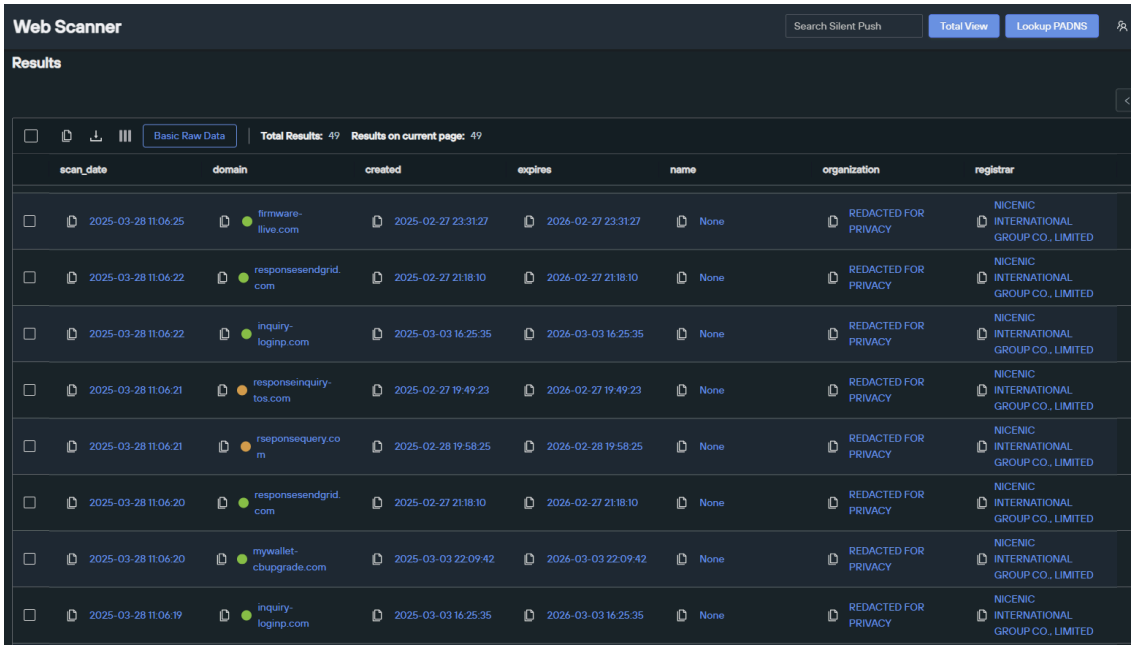


Web Scanner WHOIS and “State” search results

Our team also created two additional WHOIS queries for the more generic “asdf” and “123123” WHOIS “State” fields. Combining those “state” names with other empty WHOIS fields and the registrar name helped to narrow the search down to the single entity likely behind all of the recent domains:

Silent Push WHOIS Scanner search:

- datasource = “whois” AND state = “asdf” AND country = “AD” AND name = “None” AND city = “None” AND registrar = “NICENIC INTERNATIONAL GROUP CO., LIMITED”

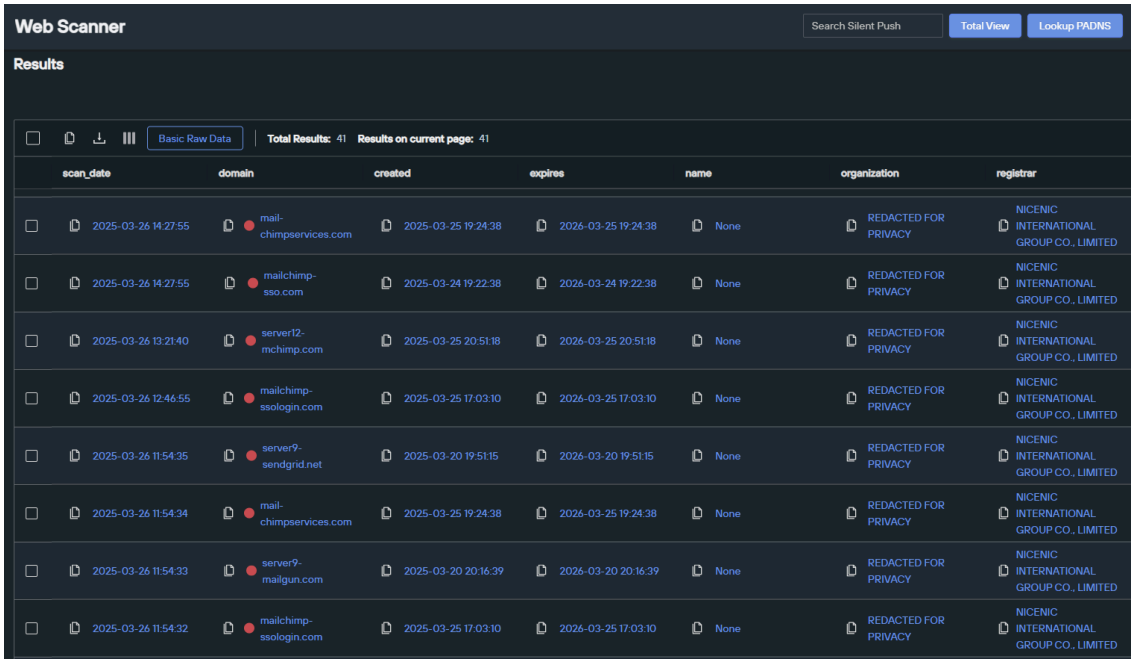


Web Scanner WHOIS with “City,” “State,” “Country,” “Name,” and “Registrar” search results

We conducted the same search for the WHOIS State “123123” to pick up more recent domains. These types of queries are often not safe enough to “leave running” because they could generate false positives in the future. As they can occasionally provide further pivots for tracking a given campaign, they can be useful for investigation purposes. Such was the case here:

Silent Push WHOIS Scanner search:

- datasource = “whois” AND registrar = “NICENIC INTERNATIONAL GROUP CO., LIMITED” AND state = “123123” AND country = “AE” AND zipcode = “None” AND address = “None”



The Web Scanner WHOIS plus “Registrar,” “State,” “Country,” “Zipcode,” and “Address” search yielded 41 results

C2 Domains Exposed in Ledger Phishing Page Template

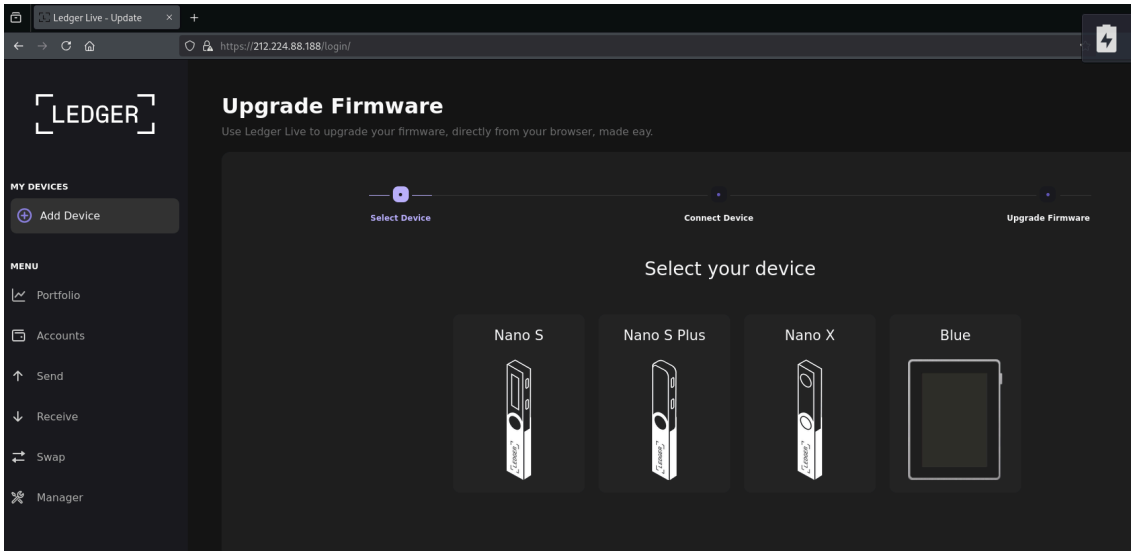
We discovered that the domain **firmware-server12[.]com**, found in the original phishing kit fingerprint pivot, was also referenced within the SSL certificate “ssl.subject.common_name” field for two IP addresses:

Silent Push Web Scanner search:

-
- datasource = [“webscan”] AND ssl.subject.common_name = “firmware-server12.com”

From these results, one IP address, 86.54.42[.]92, had no significant pivots, but the other IP address, 212.224.88[.]188, was recently found to be hosting a Ledger Wallet “Upgrade Firmware” page, which appeared to be another complex lure for stealing cryptocurrency.

This is what the page looked like at the time of our discovery in March 2025:



Ledger Wallet "Upgrade Firmware" phishing content found on 212.224.88[.]188/login/

This login page had C2 domains exposed in the JavaScript:

JavaScript from an exposed Ledger phishing page on 212.224.88[.]188/login/

C2s found in the JavaScript included:

- mysrver-chbackend[.]com
- nikafk244[.]com
- iosjdfsmdkf[.]com
- barefoots-api[.]com

Common Directories Further Connect Bulk Email and Cryptocurrency Phishing Campaigns

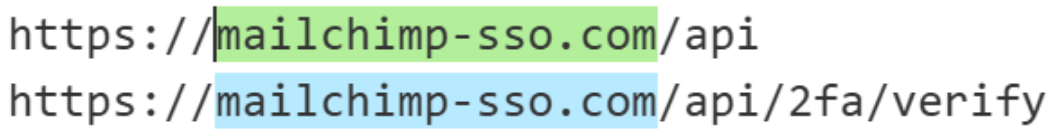
When analyzing the JavaScript on hubservices-crm[.]com found through the original phishing kit fingerprint query, we discovered two directories PoisonSeed had used for the CRM/bulk email phishing pages flow:

- /api
- /api/2fa/verify

```
https://app.hubspot.com/signup-hubspot/crm
https://hubservices-crm.com/api
https://hubservices-crm.com/api/2fa/verify
```

Unique paths retrieved from the JavaScript file

When the Troy Hunt phishing campaign was made public, Silent Push Threat Analysts quickly grabbed the JavaScript from mailchimp-sso[.]com, (Cloudflare NameServer records were removed on March 25, 2025, likely due to a ban). Our team noted the specific JavaScript configuration on mailchimp-sso[.]com and matched the same paths that we saw on hubservices-crm[.]com:



Unique path configuration retrieved from the JavaScript file

The identical directories between the bulk email phishing campaigns and the cryptocurrency seed phrase poisoning campaign, along with their WHOIS “State” connections, further confirmed what we had already known due to the Akamai SendGrid compromise: Both campaigns are from the same actor.

PoisonSeed Domain Patterns, Registrar & WHOIS Keywords Align to CryptoChameleon, Explaining the Scattered Spider Connection

Many threat analysts and researchers have been trying to link the current PoisonSeed threat actors to Scattered Spider, but few have been connecting them to CryptoChameleon, even though both threat actor groups are associated with The Comm.

Our team believes it’s important to highlight and explain our thought processes behind classifying this as an independent threat actor group as the technical details in this case, on close examination, reveal a closer alignment to CryptoChameleon over Scattered Spider.

WHOIS Registration Connections

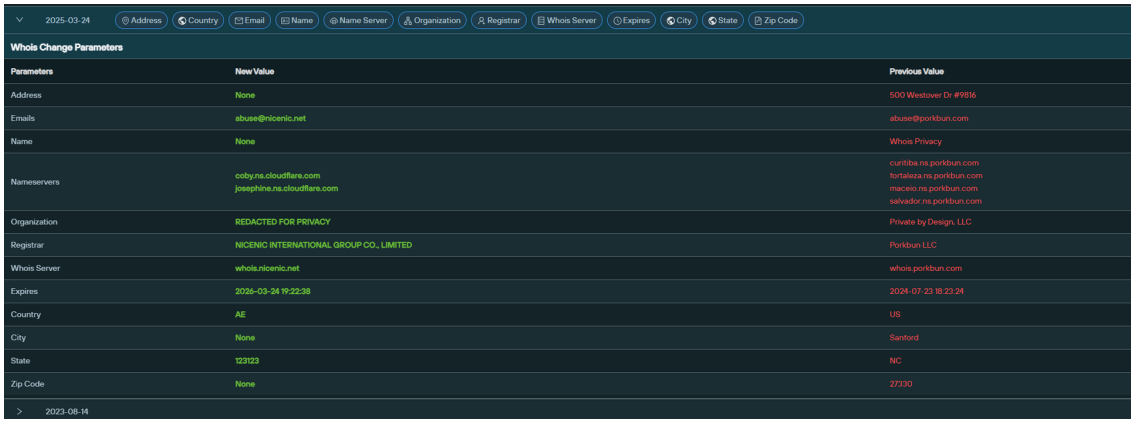
According to Group IB research, the “mailchimp-sso [.] com” domain used in the recent Troy Hunt phishing effort was first seen in attacks in 2022 and was used by Scattered Spider.

Now, three years past the first attack, anyone could have re-registered the domain. Just because one specific threat actor previously controlled a domain doesn’t mean attribution of that domain to the same threat actor remains indefinitely, especially after it changes registration.

The mailchimp-sso[.]com domain was registered on Porkbun from the previous attack up until March 24, 2025, when it was re-registered on NiceNIC, a registrar of choice for both Scattered Spider and CryptoChameleon.

Silent Push Total View Search:

-
- mailchimp-sso[.]com



2025-03-24 | Address | Country | Email | Name | Name Server | Organization | Registrar | Whois Server | Expires | City | State | Zip Code

Whois Change Parameters

Parameters	New Value	Previous Value
Address	None	500 Westover Dr #9816
Emails	abuse@nicenic.net	abuse@porkbun.com
Name	None	Whois Privacy
Nameservers	coby.ns.cloudflare.com josephine.ns.cloudflare.com	curitiba.ns.porkbun.com fortaleza.ns.porkbun.com maceio.ns.porkbun.com salvador.ns.porkbun.com
Organization	REDACTED FOR PRIVACY	Private by Design, LLC
Registrar	NICENIC INTERNATIONAL GROUP CO., LIMITED	Porkbun LLC
Whois Server	whois.nicenic.net	whois.porkbun.com
Expires	2026-03-24 19:22:38	2024-07-23 18:23:24
Country	AE	US
City	None	Sanford
State	123123	NC
Zip Code	None	27330

2023-08-14

Total View WHOIS search results for mailchimp-sso[.]com

Our team believes it's too early to classify mailchimp-sso[.]com as part of Scattered Spider merely because the threat actor group previously controlled it, or because it was re-registered on a popular registrar they are using – especially when the recent campaign had a cryptocurrency cash-out scheme, which would be a significant change for them. It is important to note: **None of the previously documented Scattered Spider attacks included allegations of trying to phish individual cryptocurrency wallets using complex email supply chain spam operations.**

In the previous Scattered Spider attack on Mailchimp, the group was likely targeting the brand because any ransomware on Mailchimp environments could potentially prevent clients from sending emails, and this would put enormous pressure on Mailchimp to pay a ransom. Early attacks from Scattered Spider followed similar targeting strategies – they went after Western companies with a large number of customers who would be immediately impacted if the attack was successful.

Another domain registration connection between the current PoisonSeed campaign and threat actors associated with The Comm (both Scattered Spider and CryptoChameleon) is the racist and obscene language used in the WHOIS "State" field. Using such language within infrastructure is consistent with what has been seen with threat actors associated with The Comm, (including both Scattered Spider and CryptoChameleon). But this observation isn't strong enough by itself to definitively say PoisonSeed is from either threat actor group associated with The Comm.

Looking at the Behaviors Behind Poison Seed, Crypto Chameleon, and Scattered Spider

Scattered Spider is a group of **big game corporate hunters** who are looking to collect massive ransoms from encrypting and disrupting major corporate operations. Scattered Spider uses **social engineering, malware, and hands-on keyboard tactics** to gain access to corporate environments. We have seen some light targeting of crypto companies by Scattered Spider since 2023, but there is no indication that these attacks were different from the other corporate attacks, many of which we know a considerable amount about.

Our team believes the new campaign we're classifying as PoisonSeed is **not** likely to be Scattered Spider because we've seen Scattered Spider continue to conduct attacks in 2025 in ways strikingly similar to its legacy attacks. In 2025, Scattered Spider has targeted brands including: Audemars Piguet, Chick-fil-A, Credit Karma, Forbes, Instacart, Louis Vuitton, Morningstar, New York Digital Investment Group, News Corporation, Nike, Paxos, Twitter/X, and Vodafone.

None of the 2025 brands targeted by Scattered Spider align with PoisonSeed's efforts.

The recent cryptocurrency seed phrase poisoning attack utilizing a supply chain spam operation **does not align** with Scattered Spider TTPs – doing so would be a significant change for them.

These tactics and the recent campaign do somewhat align with CryptoChameleon, however, which *is a* part of the same threat actor group: "The Comm."

In May 2024, we published a client-only report on CryptoChameleon and a public blog. Since then, we've engaged with several research sharing partners to further our understanding of these threat actors.

CryptoChameleon has conducted VIP spear phishing targeted at high net worth crypto holders, cell phone SIM swaps, email hacks, and all types of voice and email phishing techniques to get access to accounts holding large amounts of crypto. They likely buy access to lists of crypto holders and/or work with partners to find potential targets. To date, Silent Push analysts have not observed CryptoChameleon conducting a cryptocurrency seed phrase poisoning effort – but this new campaign is a novel phishing effort, and that does align with their innovative methodology.

CryptoChameleon heavily targets Coinbase and Ledger (just like PoisonSeed), along with several other crypto brands. Our team has never seen CryptoChameleon directly target email providers other than GMAIL and iCloud. CryptoChameleon attacks are performed quickly, with the cryptocurrency being moved immediately from a victim's wallet once the attack is successful. The PoisonSeed campaign has more of a delay with cash-out efforts, requiring a victim to add the threat-actor-provided seed phrase to their account, and later the threat actor would bulk check accounts for the phrases, and then take over the accounts to cash out.

CryptoChameleon also allegedly walks victims through their phishing pages, manually triggering the next page from their admin panel to prevent automatic scanners from working on their sites. We've seen nothing like this from the PoisonSeed campaign; in fact, more of an opposite strategy is being taken.

Whenever our team finds two efforts (CryptoChameleon and PoisonSeed) that are heavily aligned on infrastructure decisions and only partially aligned on victim targeting and tactical behavior but have no current on-page code overlap, we delay merging the two groups until **definitive** information is acquired.

Known CryptoChameleon and Scattered Spider Phishing Kits Don't Align with PoisonSeed

Silent Push analysts are tracking multiple phishing kits used by Scattered Spider, including their recent 2025 variations. For CryptoChameleon, we're tracking several variations (some with subtle changes) and have analyzed many details of how their kits work.

None of these kits aligns with what we're seeing with PoisonSeed, leading us to the conclusion that it's either a completely new phishing kit from CryptoChameleon or a separate threat actor who just happens to use similar tactics and infrastructure decisions.

Therefore, until **definitive** information is discovered pairing the two, our team will continue to classify this threat separately under the name: PoisonSeed.

Continuing to Track PoisonSeed

Silent Push will continue to report on our work tracking this cryptocurrency and CRM phishing threat actor, especially if it continues to target enterprises outside the cryptocurrency industry.

If you or your organization have any leads related to this effort that you would like to share, particularly those being used by these threat actors, we would love to hear from you.

PoisonSeed Mitigation

Silent Push believes all domains related to PoisonSeed may offer some level of risk to enterprise organizations. We provide client-only Indicators of Future Attack™ (IOFA™) feeds for tracking PoisonSeed domains and IPs.

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

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

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

Indicators of Future Attack™ (IOFA™)

Silent Push is sharing a sample IOFA™ list we have associated with the PoisonSeed phishing campaign to support ongoing efforts within the community. Our enterprise users have access to an IOFA™ feed currently containing many times this number, with more being added in real time as our investigation continues.

- active-mailgun[.]com
- barefoots-api[.]com
- cloudflare-sendgrid[.]com
- complete-sendgrid[.]com
- connect1-coinbase[.]com
- connect5-coinbase[.]com
- firmware-llive[.]com
- firmware-server12[.]com
- hubservices-crm[.]com
- inquiry-loginp[.]com
- iosjdfsmdkf[.]com
- live-sso[.]com
- mail-chimpservices[.]com

- mailchimp-sso[.]com
- mailchimp-ssologin[.]com
- myaccount-hbspot[.]com
- mysite-clflre[.]com
- mysrver-chbackend[.]com
- myw-cbw[.]com
- mywallet-cbsmartw[.]com
- mywallet-cbsmw[.]com
- mywallet-cbupgrade[.]com
- nikafk244[.]com
- password-proxy-redirect[.]com
- redirect-sso[.]com
- response-crmsg[.]com
- response-loginportal[.]com
- response16-sendgrid[.]com
- response20-sendgrid[.]com
- responseinquiry-tos[.]com
- responsesendgrid[.]com
- review-termsconditions[.]com
- revokecblink[.]com
- rseponse-manageprod[.]com
- rseponse25-sendgrid[.]com
- rseponsequery[.]com
- server12-mchimp[.]com
- server9-hubspot[.]com
- server9-mailgun[.]com
- server9-sendgrid[.]net
- sso-account[.]com
- sso-signon[.]com
- support-zoho[.]com
- swallet-coinbase[.]com
- 212.224.88[.]188
- 86.54.42[.]92

Source: https://www.silentpush.com/blog/poisonseed/