Scattered Spider: Still Hunting for Victims in 2025

By Peggy Kelly

Published: 2025-04-08 · Archived: 2026-04-05 16:10:30 UTC

2025 Key Findings

- Silent Push has determined the evolving threat Scattered Spider is still actively hunting for victims:
  - Services targeted by Scattered Spider in 2025 include Klaviyo, HubSpot, and Pure Storage.
  - Brands targeted in 2025 include Audemars Piguet, Chick-fil-A, Credit Karma, Forbes, Instacart, Louis Vuitton, Morningstar, New York Digital Investment Group, News Corporation, Nike, Paxos, Twitter/X, Tinder, T-Mobile, and Vodafone.
- Silent Push researchers are tracking five unique Scattered Spider phishing kits, which have been used since at least 2023. Some of these kits have seen several updates, alongside dozens of their code fingerprints and technical deployment decisions. **Right now, it appears their legacy phishing kits are being deprecated.**
- Our team is also sharing the discovery and analysis of a new version of Spectre RAT used by Scattered Spider. In our analysis section, we have included publicly available code for a Spectre RAT String Decoder and Command and Control (C2) Emulator to support defenders in their own analytical efforts.
- In 2024, Scattered Spider acquired a domain (twitter-okta[.]com) previously owned by Twitter/X. This domain was likely part of a previous brand protection effort, but it’s unclear if the domain will be used to target Twitter/X directly or users of the service.

Table of Contents

Executive Summary

Scattered Spider is a hacker collective that has been active since at least 2022. It is well-known for launching sophisticated social engineering attacks to obtain usernames, login credentials, and multi-factor authentication (MFA) tokens.

Silent Push analysts have successfully identified Scattered Spider infrastructure, tactics, techniques, and procedures (TTPs), and developed several methods for routinely and proactively identifying **Indicators of Future Attack**™ (IOFA™) that our customers can use against this threat. Changes to deployments and phishing kits in early 2025, however, suggest Scattered Spider is turning the page on some past decisions.

In our tracking of Scattered Spider, our team recently observed two significant developments: The discovery of a new version of Spectre RAT used by threat actors to gain persistent access to compromised systems and a boomerang domain ownership between the threat actor and Twitter/X.

Our team is continuing to track this evolving threat actor.

Attend “The Evolving Web of Scattered Spider” Webinar: April 15, 2025

Join Silent Push for a special Scattered Spider webinar on April 15, 2025. We will host in three time zones to support global interest in the evolving threat actor group.

Learn more and register now.

Scattered Spider Legacy TTPs & Behaviors

Silent Push analysts review all opportunities to track a threat, from on-page content, server details, and deployment processes to preferred technology solutions. Here are some of the legacy behaviors our team has observed for Scattered Spider:

- **Multiple variations of their phishing kits, each of which:**
  - Are visually equal
  - Use very distinct source code
- Reuse of dedicated servers
- Registration of a bulk domain within the same day or a few days, usually targeting a specific company or several companies in the same business sector.
- Creation of multiple domains targeting a specific company over distinct attack waves.
- **Last Seen Preferred Registrar**: NiceNIC
- **Last Seen Preferred Hosts:** Njalla, Virtuo, and Cloudflare
- **Historically Preferred Hosts & Registrars:** Porkbun, Namecheap, Hostinger, Tucows, and Hosting Concepts
- **Preferred ASNs:** Cloudflare (AS13335), Choopa (AS20473), DigitalOcean (AS14061), Hostinger (AS47583), Akamai-Linode (AS63949), and Namecheap (AS22612)

- **Targeting Sectors:** Financial, Retail, Entertainment, Telecommunications, Cloud Storage Platforms, and Software Providers
- **Use of Domain Keywords:** “connect,” “corp,” “duo,” “help,” “he1p,” “helpdesk,” “helpnow,” “info,” “internal,” “mfa,” “my,” “okta,” “onelogin,” “schedule,” “service,” “servicedesk,” “servicenow,” “rci,” “rsa,” “sso,” “ssp,” “support,” “usa,” “vpn,” “work,” “dev,” “workspace,” “it,” and “ops.” For top-level domains (TLDs): “com,” “co,” “us,” “net,” “org,” and “help.”

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

Background

Scattered Spider, also known as UNC3944, Star Fraud, Octo Tempest, Scatter Swine, or Muddled Libra, is a threat actor group associated with the larger hacking group known as “The Community,” “The Comm,” or also “The Com.”

Operating since the spring of 2022, Scattered Spider has been behind several significant ransomware and extortion efforts, targeting numerous major brands, mostly based in the U.S. Threat actors like Scattered Spider are known for launching sophisticated social engineering attacks. After acquiring data and encrypting resources, they blackmail victim organizations to pay exorbitant ransom.

Over the past three years, Scattered Spider has been responsible for numerous security incidents, with the two most notable being the Twilio breach in August 2022 and the MGM breach in September 2023.

The domain, klv1.it[.]com, targeting Klaviyo is based on the HTML title, but the subdomain name “klv1” isn’t terribly close to “Klaviyo” – making it harder to find with classic brand regex searches, especially those without foreknowledge of a given brand’s marketing campaigns. Scattered Spider is also using a Dynamic DNS vendor (it[.]com), so there are no domain registration fingerprints. The targeting of this domain via Scattered Spider further confirms the threat group does extensive research on targets.

In 2024, there were allegations that the threat actors who compromised Snowflake had connections to Scattered Spider. This was explained by Chris Morgan, a senior cyber-threat intelligence analyst at security firm ReliaQuest, to Wired, “…the threat actor’s profile picture is taken from an article referencing the threat group Scattered Spider, although it is unclear whether this is to make an intentional association with the threat group.” In 2025, Silent Push has also seen Scattered Spider targeting “Pure Storage,” a competitor to Snowflake, so it appears cloud storage solutions remain one of the group’s priority targets.

At least seven Scattered Spider members, including an alleged leader, were arrested in 2024. After five were charged by U.S. prosecutors in November 2024, operations started to slow down. Details from the arrests, among other reports, confirm most members are young and based in the U.S., U.K., and Europe.

Changes observed in 2025 allude to new developers and/or technical obfuscation decisions being made.

One of the most recent Scattered Spider domains, seen in February 2025, was **klv1[.]it[.]com**, a domain impersonating a “Custom Link Shortener” used by Klaviyo (klv1[.]io), which was part of their SMS marketing features.

Scattered Spider continues to use BitLaunch (bitlaunch[.]io), which provides instant launch servers from BitLaunch, DigitalOcean, Vultr, and Linode. Service includes hourly rental of servers paid for with crypto.

Silent Push published our first public blog on Scattered Spider in December 2023. This was followed by a detailed report for our enterprise customers in March 2024 and another significant recap report in March 2025. We’re making some of those details public now to support external tracking efforts.

Scattered Spider Brand Impersonation

Scattered Spider creates domains that impersonate a wide range of brands, both directly targeting major organizations and appearing to also target specific software vendors used by the targeted organizations.

When analyzing the list of Scattered Spider domains and brands we detected, our research team found it interesting that some brands, those we know have been directly targeted, didn’t have domains registered that explicitly mentioned their brand names. Essentially, this means that just because a brand’s name wasn’t included in the corporate brand list, it doesn’t mean the brand is safe from being on Scattered Spider’s radar.

Here is a comprehensive list of the corporate brand names we’ve seen Scattered Spider referencing in their domains since 2023:

Aflac, Allstate, Ally Bank, Amica, Apple, AT&T, Athene, Audemars Piguet, Ballet Crypto, BCB Group, Bell, Bitcoin Suisse, Blockdaemon, Blockstream, Charter Communications, Chik-fil-A, Cincinnati Financial, Comcast Corporation, Core Scientific, Costco, Credit Karma, DoorDash, Fireblocks, Forbes, Gemini, Grayscale, H&R Block, Hanover Insurance, Harrow Health, Iliad, Instacart, Jackson Hewitt, Kemper, Louis Vuitton, Luno, Marsh, Mercury, Morningstar, Mutual of Omaha, Nansen, NGRAVE, New York Digital Investment Group, New York Life Insurance, News Corporation, Nike, Orange, P.F. Chang’s, Paxos, PNC Bank, Revolut, RiteAid, 7-Eleven, Singtel, Stargate Industries, Synchrony Bank, Synovus, T-Mobile, Telstra, TIAA, Transamerica, Twitter/X, UScellular, Verizon, Vodafone, WINDTRE, and Xapo Bank.

Some of the software brands we’ve seen referenced in Scattered Spider domains since 2023 may have also been directly targeted:

Accenture, ActiveCampaign, Ada CX, Alchemy, Asurion, Bandwith, Bird CRM, Campaign Monitor, Concentrix, Constant Contact, Corporate Tools, CTS, eClerx, Expedia Group, FalconX, FICO, Five9, Foundever, Freshworks, Genesis Trading, Givebutter, GoDaddy, HubSpot, Incode, Intercom, iQor, Iterable, Jumio, Klaviyo, LinkedIn, Mixpanel, Nuance Communications, Onfido, OnSolve, Podium, Pure Storage, Ripple, Roblox, Salesforce, Shipbob, Sinch, Socure, SPOC, Squarespace, TaskUs, TriVista, Twilio, Ulta Beauty, Upland Software, Wix, Workday, Ziff Davis, and 247[.]ai.

Twitter Abandoned a Domain, Scattered Spider Picked It Up

One of the queries we used to track Scattered Spider detected a domain on October 6, 2024, that looked similar to past campaigns: **twitter-okta[.]com**

When investigating the domain, we noticed the WHOIS records had changed three times in three years. It's possible that Scattered Spider owned the domain, Twitter/X legal took it over and stopped re-registering it, and then Scattered Spider picked it back up.

The domain was registered on Porkbun in June 2022, around the time Scattered Spider first started its activity. Scattered Spider has used Porkbun in the past in other confirmed infrastructure.

By August 2022, Twitter had taken control of the domain, and WHOIS details noted they were working with the brand protection vendor CSC (Corporation Service Company) (corporatedomains[.]com).

The domain was then registered on NiceNIC, Scattered Spider's current registrar of choice, on October 6, 2024. The same day, we picked it up with a fingerprint we used to track one of Scattered Spider's phishing kits (detailed later). This October 2024 fingerprint confirmed that Scattered Spider currently controls this domain and potentially owned it in 2022.

Timeline of 2024 Arrests

- **January 2024:** Member Noah Michael Urban, aka "Sosa," "King Bob," and "Elijah," arrested in Florida for stealing approximately $800,000 in cryptocurrency (Krebs on Security).
- **June 2024:** Alleged leader Tyler Buchanan, aka "TylerB," arrested in Spain with $27 million in Bitcoin (Krebs on Security).
- **July 2024:** U.K. law enforcement in West Midlands arrested a 17-year-old connected to Scattered Spider (West Midlands Police).
- **November 2024:** Five Scattered Spider members charged by U.S. prosecutors – (including "King Bob" and "TylerB"); defendants were Tyler Buchanan, 22, of Scotland; Ahmed Elbadawy, 23, of College Station, TX; Joel Evans, 25, of Jacksonville, NC; Evans Osiebo, 20, of Dallas, TX; and Noah Urban, 20, of Palm Coast, FL, (Reuters).
- **December 2024:** Member Remington Goy Ogletree, a 19-year-old from Fort Worth, TX, was arrested after the FBI convinced him to engage in a fake cryptocurrency laundering operation called "Cash Service" (Dark Reading).

Scattered Spider and CryptoChameleon are both part of "The Comm," and each has been involved in multiple, high-profile attacks.

Throughout 2024, Silent Push Threat Analysts received private briefings and sensitive details from our research sharing partners about The Comm, and industry reports were able to make public that they use a "Developer-as-a-Service" (DaaS) group called "Telecom Enemies" aka "Telecom Clowns" that are building tools used by The Comm.

Telecom Enemies develop tools, including the "Gorilla Call Bot," which is used for voice phishing campaigns and abuse of Google Voice. They also develop "Suite's (All in One) AIO," a tool 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.

These services have been targeted by both Scattered Spider and CryptoChameleon.

Our team 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 complex attack methods but often do not code projects directly themselves.

Scattered Spider updated its phishing kits at least four times through 2024. The latest version, Phishing Kit #5, was seen in 2025 and had additional content changes. It was hosted on Cloudflare.

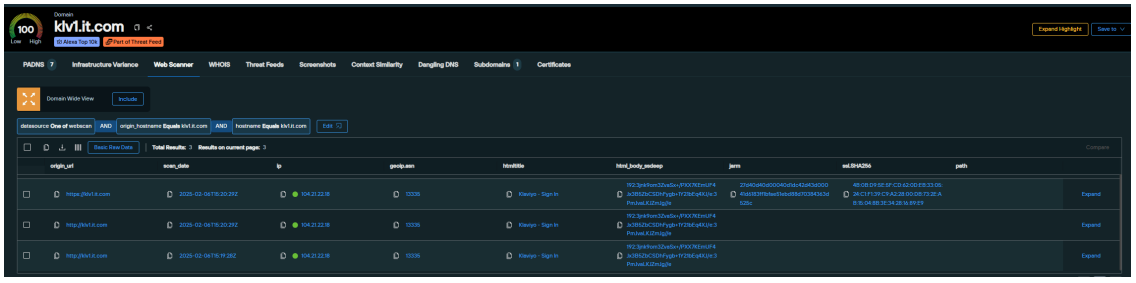
Over the last year, we have seen relatively significant changes in their deployment decisions and phishing kits. There has been a shift in preferred hosting providers, the underlying code of the phishing kits has changed, and several other changes have enabled our team to develop strong fingerprints against them, which, for operational security reasons, have been omitted from this blog.

One point we can include, however, is that we saw our first dynamic DNS/rented subdomain used by Scattered Spider this year, which further speaks to their evolving TTPs.

Silent Push enterprise customers have access to a **bulk data feed** that tracks dynamic DNS providers along with other third-party services that facilitate subdomain leasing.

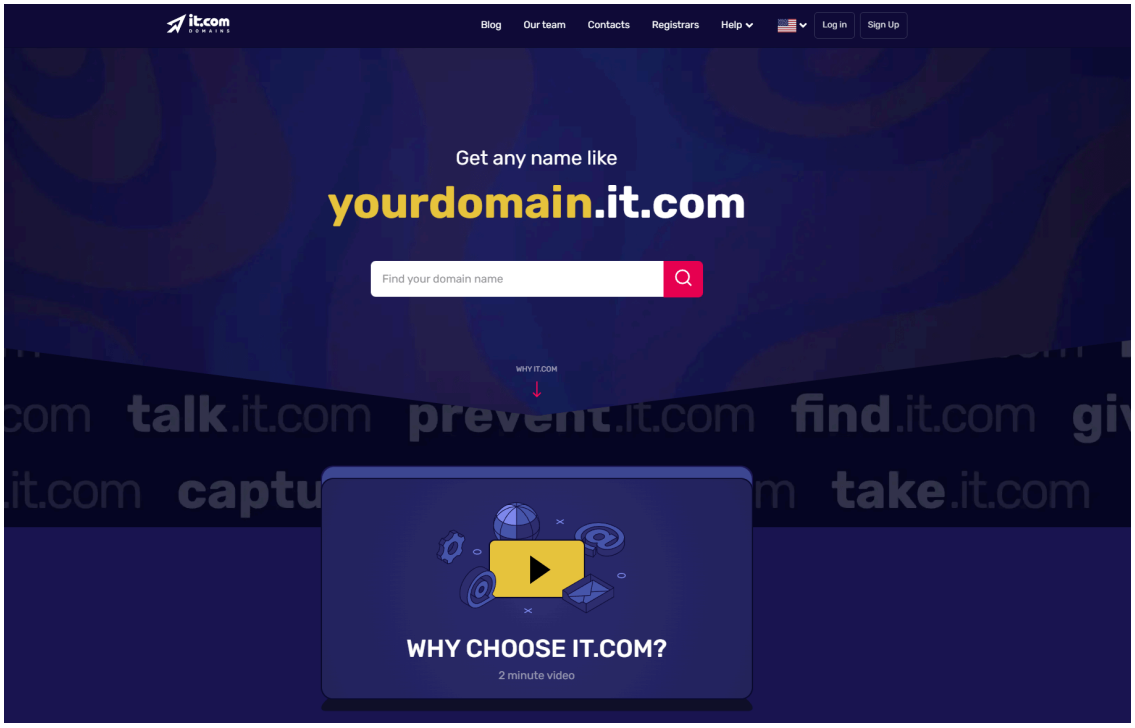
2025 Phishing Targeting Klaviyo

On February 6, 2025, one of our Scattered Spider fingerprints picked up a new host: **klv1.it[.]com**



Our Scattered Spider fingerprint picked up a new host: klv1.it[.]com

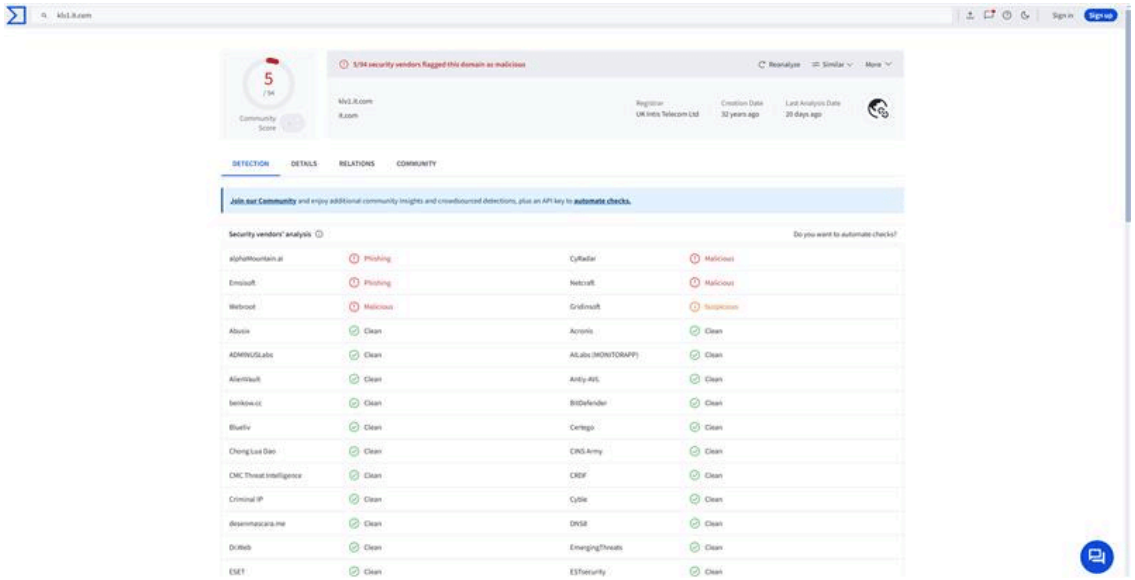
This Scattered Spider host is registered on a subdomain of it[.]com – a domain and service that allows public subdomain registrations.



The Scattered Spider host was registered on a subdomain of it[.]com

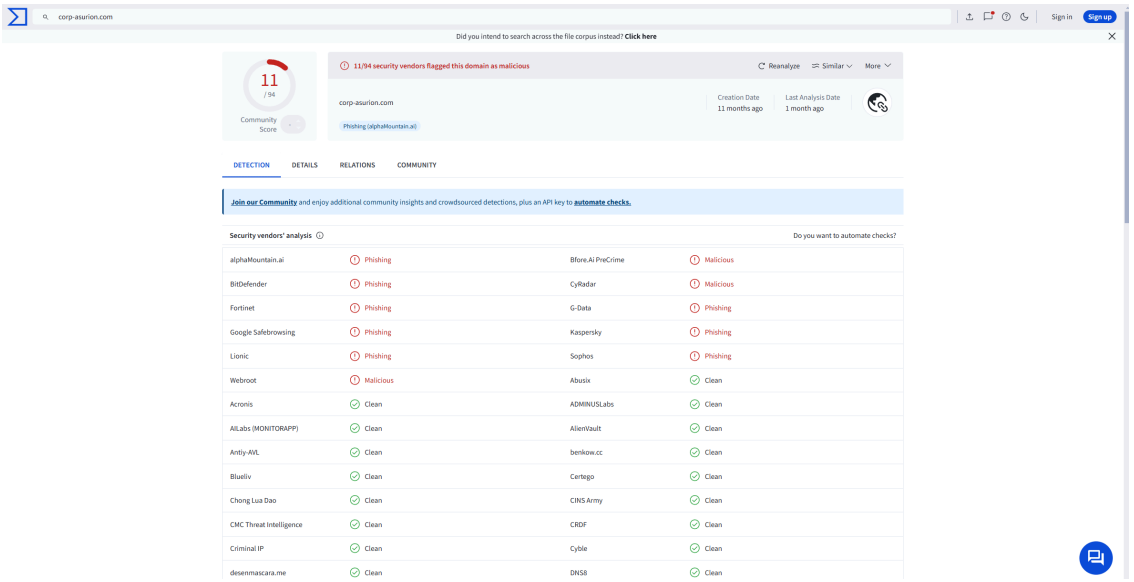
The new usage of a publicly rentable subdomain may create tracking challenges for some organizations.

It can be seen with the klv1[.]it[.]com host, which had only [five detections in VirusTotal](#) as of this writing:



VirusTotal results for klv1[.]it[.]com

One domain (corp-asurion[.]com), from December 2024, followed more of their normal patterns with [11 detections, including Google's safe browsing](#):



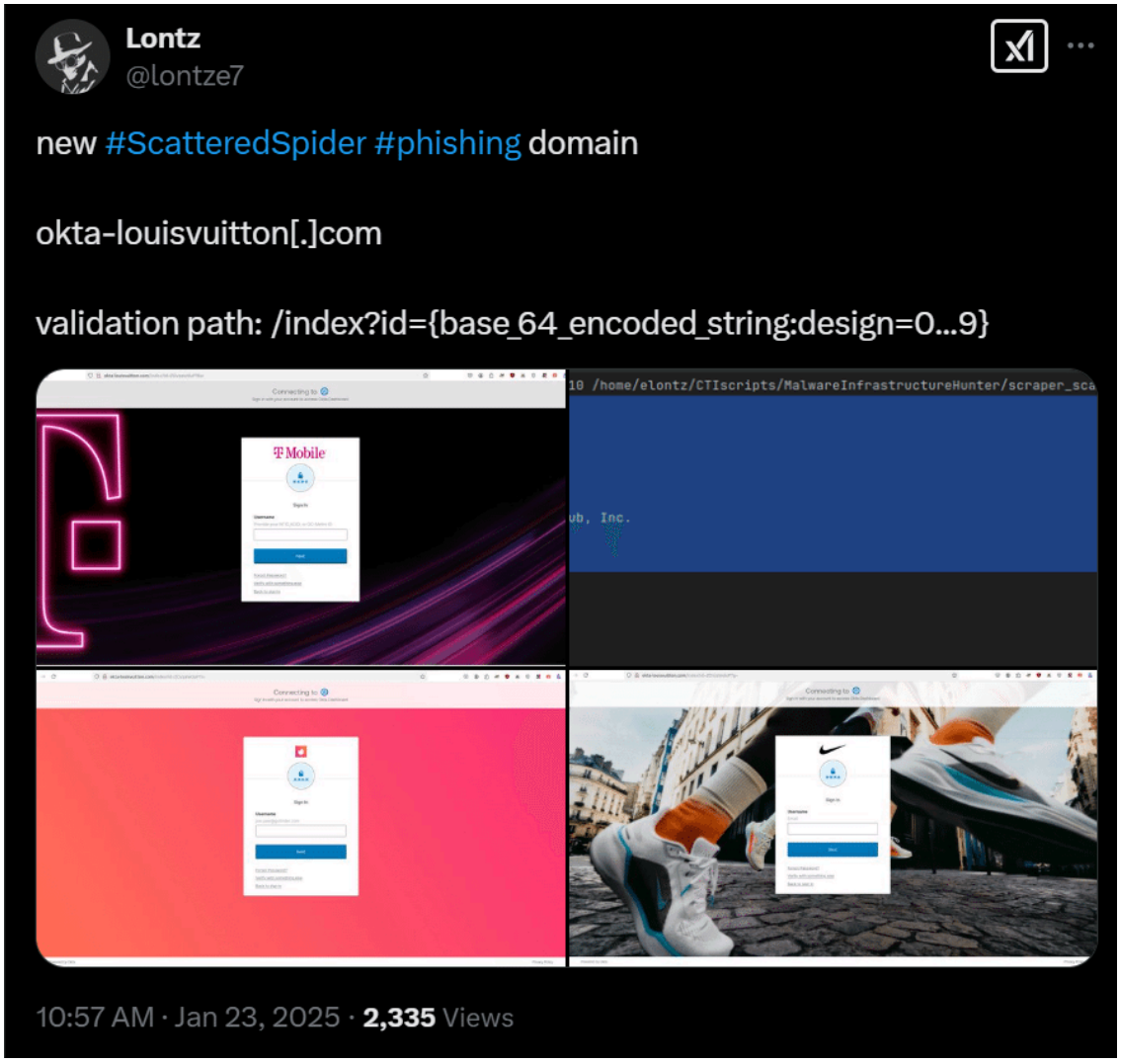
VirusTotal results for corp-asurion[.]com

If Scattered Spider keeps using dynamic DNS vendors (organizations that provide publicly rentable subdomains), it will be important for all targeted organizations to alert or block requests for the associated domains and all related DNS vendor subdomains.

New 2025 Scattered Spider Phishing Kit: #5

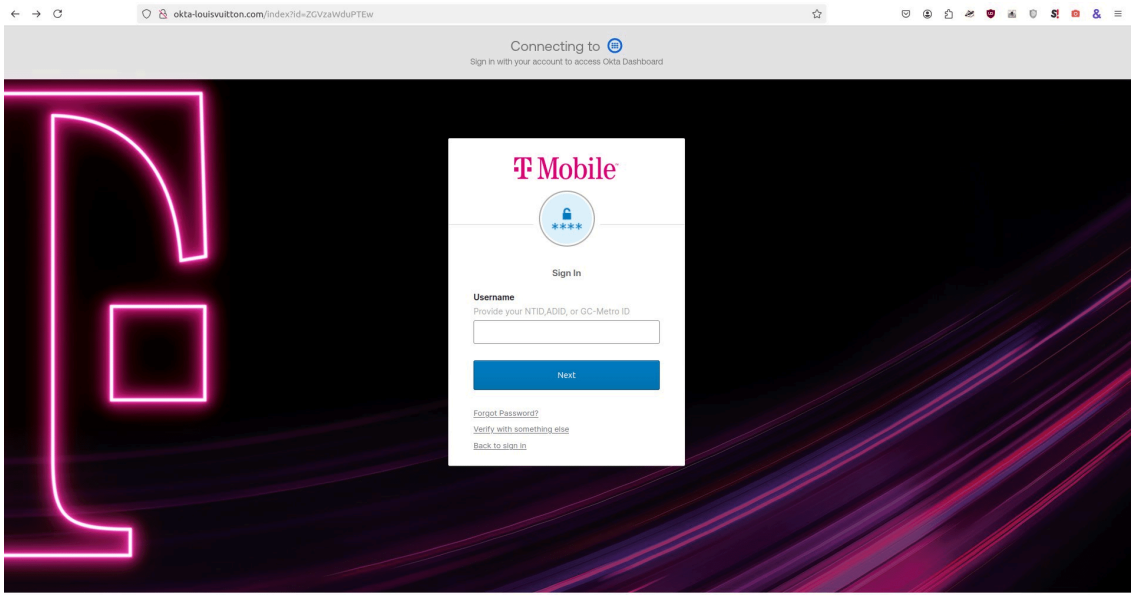
Our team regularly monitors our own data but also external conversations and data sources to ensure we investigate potential leads, especially for threats like Scattered Spider. Using this hybrid approach, our analysts were able to create fingerprints to track the four unique phishing kits used from 2023 to 2025.

On January 23, 2025, threat intel researcher Lontz published details about new potential Scattered Spider infrastructure, which led to the establishment of a fingerprint for Phishing Kit #5.

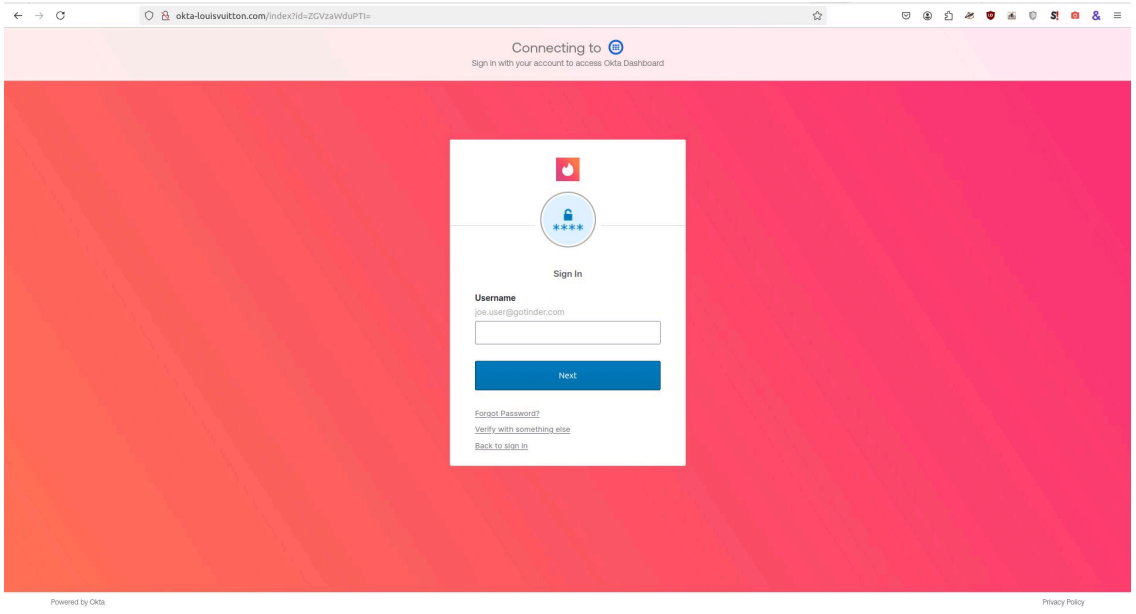


Observation from @lontze7 Scattered Spider research @ https://x[.]com/lontze7/status/1882367142823367121

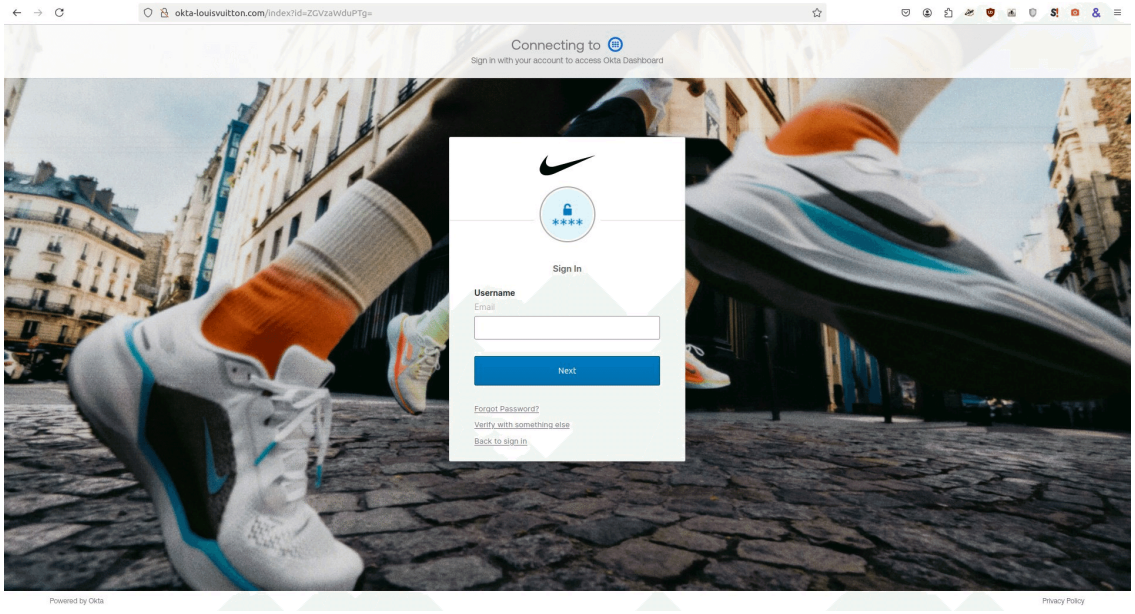
The shared template had different brands integrated into the same website, which almost appeared to be a development mistake. The example shared, okta-louisvuitton[.]com, can be seen with content targeting T-Mobile, Tinder, and Nike.



Another observation from @lontze7 Scattered Spider research @ https://x[.]com/lontze7/status/1882367142823367121



@lontze7 Scattered Spider research @ x[.]com/lontze7/status/1882367142823367121

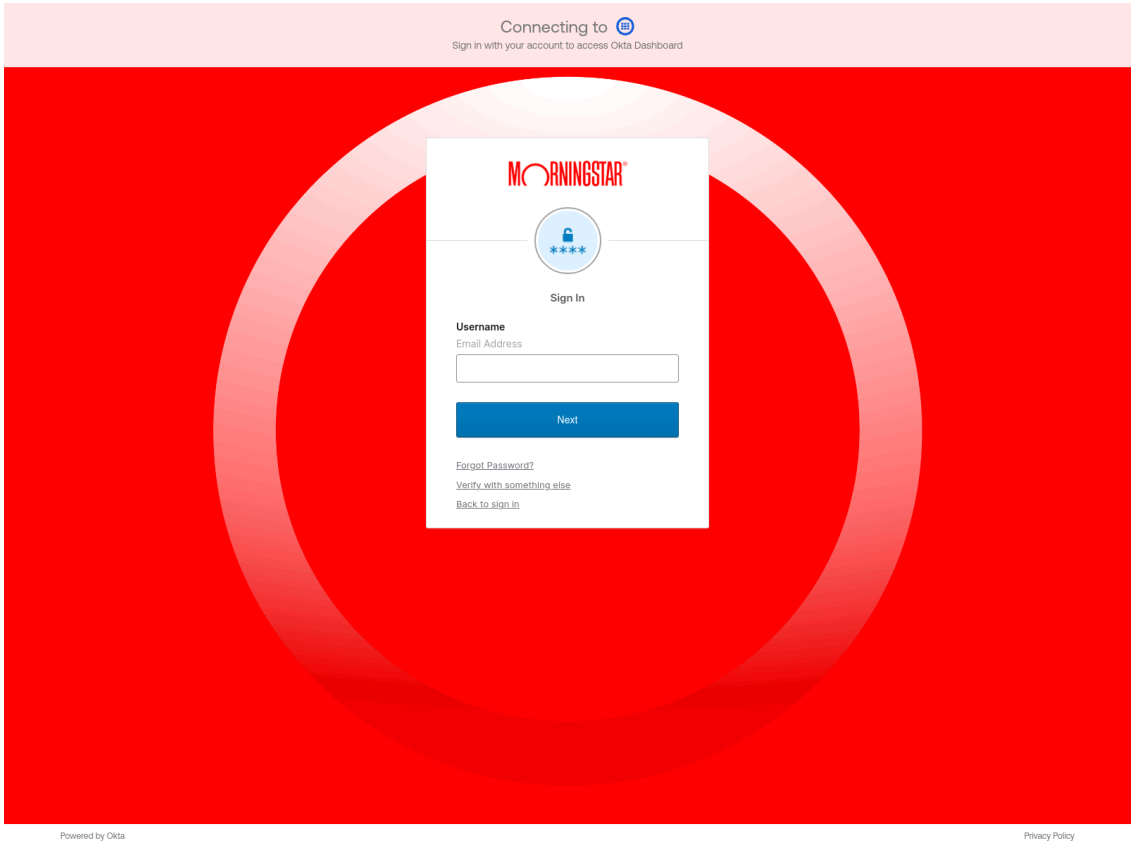


@lontze7 Scattered Spider research @ x[.]com/lontze7/status/1882367142823367121

Lontz wrote that the phishing pages trigger with the following path:

"https://[domain].[TLD]**/index?id=[base64 string=]**"

Our team replicated the research to confirm that the same phishing kit could be triggered on domains like Morningstar-okta[.]com, as shown below.



Morningstar-okta[.]com

Pivoting from fingerprints developed during our research, which we shared in our private enterprise client report, we found additional sites being targeted. A sample list of them includes the following:

- corp-hubspot[.]com – **HubSpot**
- morningstar-okta[.]com – **Morningstar**
- pure-okta[.]com – **Pure Storage**
- signin-nydig[.]com – **New York Digital Investment Group**
- sso-instacart[.]com – **Instacart**
- sts-vodafone[.]com – **Vodafone**

Legacy Phishing Kits and Analysis of Evolving TTPs

The details below this point cover four other legacy Scattered Spider phishing kits that we tracked previously. We will highlight the group's consistent decisions and unique infrastructure, which don't particularly align with past attacks.

Kit #1 – Okta Impersonation Modified to Match Target Information

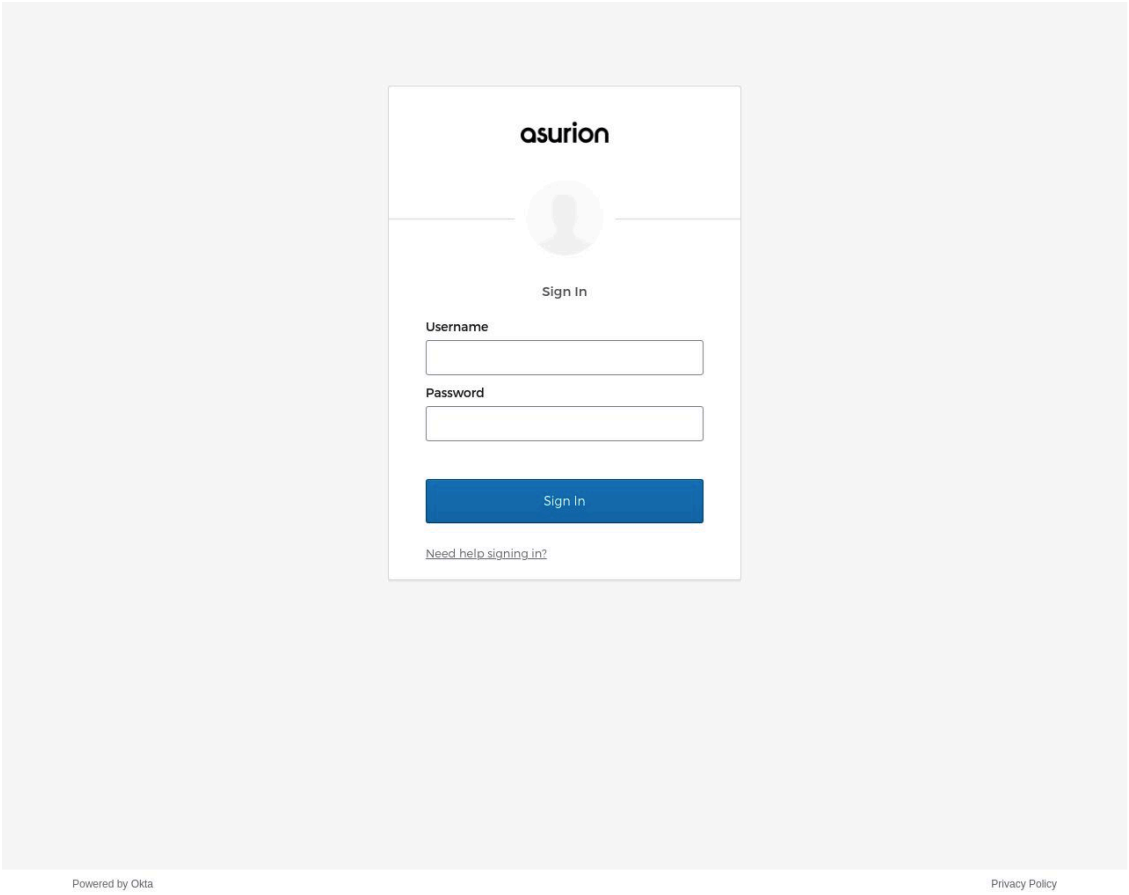
In September 2023, we picked up a new Scattered Spider phishing kit that impersonated Okta login pages for targeted organizations.

The phishing pages had the HTML title "Sign In" and were always hosted on short-lived domains that included specific keywords such as "okta," "sso," "help," "hr," "corp," "my," "internal," "sso," or "vpn," among others.

After registering these domains, usually a couple per day, with multiple typo-squats of a particular organization or organizations that operate in the same business sector, the Scattered Spider operators immediately acquired an SSL certificate for them and rapidly hosted the phishing content.

The phishing pages were up for 5 to 30 minutes after a domain was registered, but never for more than a couple of hours. The domains were usually abandoned after that, being parked or taken down by the registrars.

We've seen some legacy infrastructure maintain MX records or other DNS records, but content typically was only hosted briefly and then removed, never to return.



Phishing page example from asurion-idp[.]com

The web pages crafted from this phishing kit mimicked the targeted organization's Okta portal by displaying its logo and organization name and having a "Powered by Okta" footer.

After a visitor successfully submitted their credentials, a PHP script named "f⬛ckyou[.]php" was executed to process the exfiltrated data further. The use of obscene language like this aligns with other Scattered Spider efforts.*

Note: For community users following along with the q*uery *below, please note that we have replaced the "u**" with a "⬛" in the above script name.*

Phishing Kit #1 Activity

First seen: September 2023

Last seen: Feb 2025

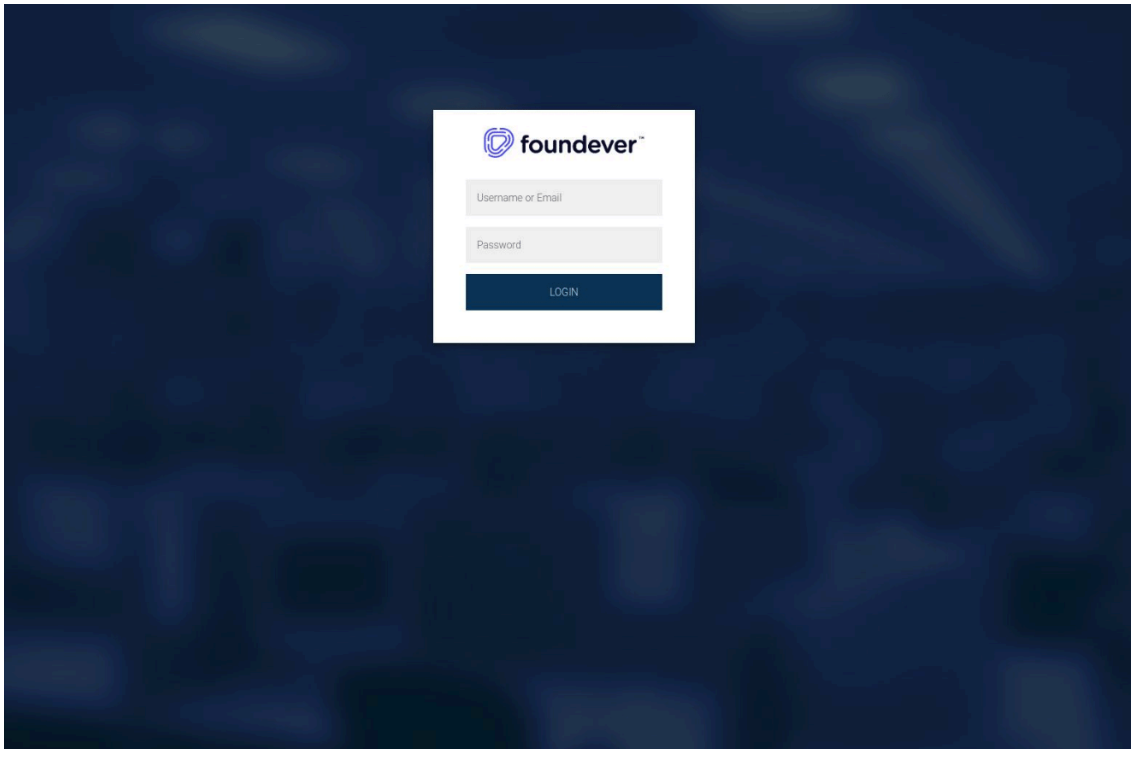
Despite some hiatus in activity in 2024, this phishing kit was consistently in use until February 2025.

When we compare any of the domains we are tracking with details available on VirusTotal, it becomes clear there are some inconsistencies in what is being used to track their infrastructure, as seen below:

Scattered Spider Phishing Kit #1 Domain	Number of VirusTotal Detections (March 2025)
sytemstern[.]net	0
xn--gryscale-ox0d[.]com	5
iyft[.]net	10
bbtplus[.]com	10
squarespacehr[.]com	10
mytsl[.]net	11
gemini-sso[.]com	12
prntsrc[.]net	14

Kit #2 – Kit #1 Variation, Simple Layout

The web pages hosted with Phishing Kit #2 appeared less polished than the ones crafted from Phishing Kit #1. These displayed a simple form and did not mention Okta anywhere on the page.



Foundever phishing page (corp-foundever[.]net)

Nearly all of the domains hosting Phishing Kit #2 used dashes (“-”) in their domains, along with brand names and some generic keywords.

Phishing Kit #2 domain names typically matched patterns similar to those seen here:

- freshworks-hr[.]com
- klaviyo-hr[.]com
- login.freshworks-hr[.]com
- login.hr-intercom[.]com

Phishing Kit #2 Activity

First seen: February 2024

Last seen: October 2024

This phishing kit was consistently used between February 2024 and June 2024, after which it went back to a lengthy period of inactivity, despite a sporadic hit in August and October 2024.

WHOIS and PADNS information of the domains showed that, contrary to the domains seen in Phishing Kit #1, many had multiple subdomains, with account, corporate, and login being the most popular.

The majority of the domains were registered on Hosting Concepts and used its default name servers, whereas a couple were registered on NiceNIC and used "*.1984.is" name servers. All domains were served from IP addresses owned by Vultr, BitLaunch, or DigitalOcean.

Some of the subdomains were seen redirecting to "Rick Roll" videos on YouTube. The Rick Roll video redirect is a feature of Evilginx (https://github[.]com/kgretzky/evilginx2), a "man-in-the-middle attack framework used for phishing login credentials."

Kits #1 and #2 – ASN Breakdown

Over the last year, 79 unique domains that matched Phishing Kits #1 or #2 were hosted on 49 dedicated IP addresses across 3 different ASNs.

ASN	AS Name	Percentage
14061	DIGITALOCEAN-ASN, US	37
20473	AS-CHOOPA, US	43
399629	BLNWX, US	20

The community has extensively covered news of Scattered Spider acquiring some of these servers through BitLaunch (bitlaunch[.]io), a company that provides hourly hosting plans, paid in crypto, with servers on DigitalOcean, Vultr, and Linode.

Phishing Kits #1 and #2 – IP Pivoting

Pivoting on the dedicated IP addresses found hosting any of the Scattered Spider domains picked up with our previous pivots returned a couple of dozen new indicators hosted within the same timeframe.

These domains mostly followed legacy domain patterns to include a dash (“-”) in the URL, along with a brand and generic keyword:

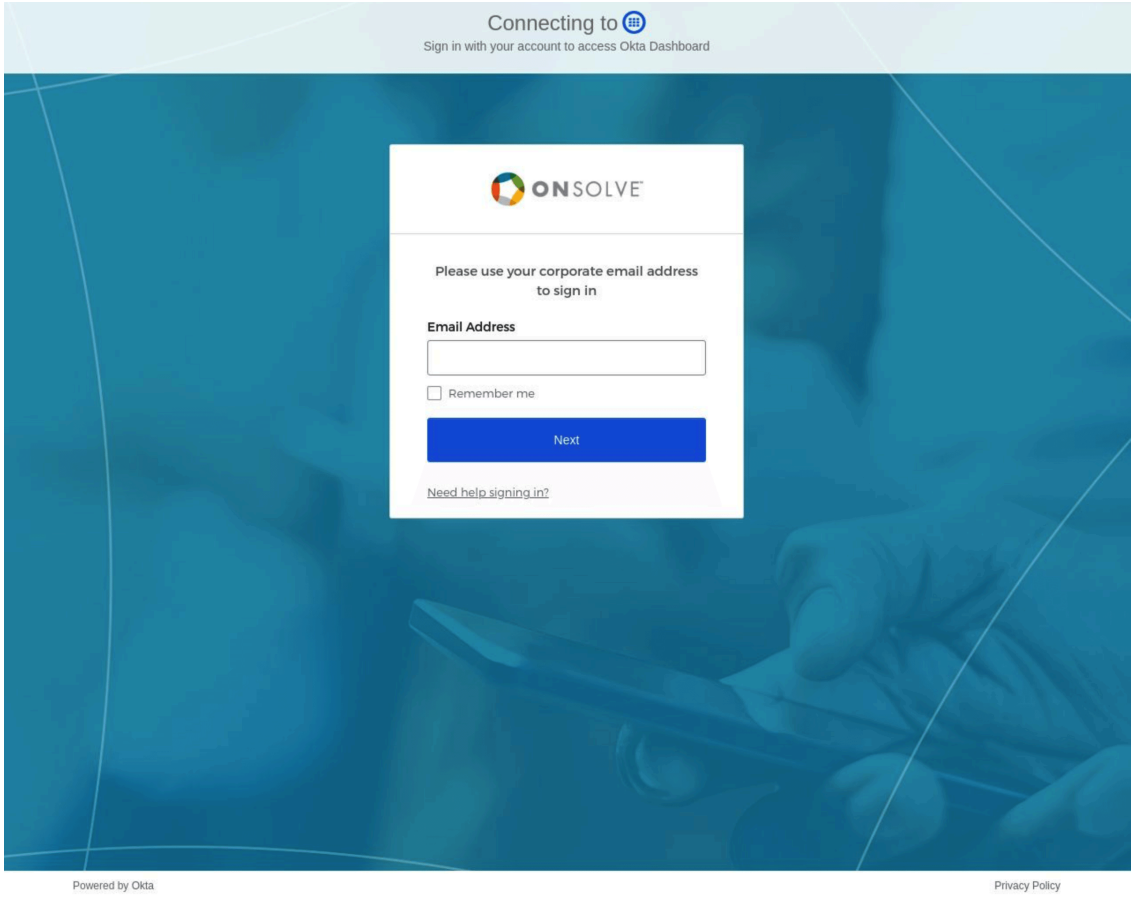
- activecampiagn[.]net
- acwa-apple[.]com
- birdsso[.]com
- okta-ziffdavis[.]com
- pfchangs-support[.]com
- x-sso[.]com

Kit #3 – “Powered by Okta” Phishing Pages

The web pages crafted from the third phishing kit mimicked the targeted organization’s Okta dashboard by displaying its logo and organization name, as well as a “Powered by Okta” header and footer.

The kit was first seen in early 2024, but it has also been seen recently—one such domain was launched on February 3, 2025 (paxos-my-salesforce[.]com), targeting the Paxos blockchain.

Phishing Kit #3 looks like this:



Phishing Kit #3 example (okta-onsolve[.]com)

Phishing Kit #3 domains featured a dash (“-”) in the URL, and almost all contain the word “okta” along with a brand name. Examples include:

- okta-onsolve[.]com
- okta-ripple[.]com
- dashboard-iterable[.]com
- paxos-my-salesforce[.]com

One fingerprint tracking this phishing kit has had notably consistent hits from February 2024 to May 2024, then only a single hit in September 2024, and once again in February 2025.

Contrary to the domains from the clusters that matched Kits #1 and #2, which hosted phishing pages almost immediately after creation, we found the domains from this group might take hours, days, or even weeks to host the actual phishing page.

Phishing Kit #3 started matching hits again in June 2024 and continued until August 2024. After another pause, it was seen again in early October 2024 and has not been seen since.

Kit #3 – Legacy IP Address

Analyzing historical DNS records from one of the IP addresses (149.28.110[.]16) that hosted Phishing Kit #3 (onsolve-okta[.]com) revealed that it also hosted a domain used in the initial 2022 attacks: 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

Results of reverse A lookup on 149.28.110[.]16

Evilginx Cluster

Across the first three phishing kits, we regularly saw redirects to the YouTube video for Rick Astley, aka the “Rick Roll meme.” Our analysts are also aware that Evilginx (https://github[.]com/kgretzky/evilginx2), the previously mentioned “Standalone man-in-the-middle attack framework,“ features this type of redirect as an option for hiding malicious payloads.

Some Scattered Spider domains seen hosting this software include:

- corp-azure[.]com
- corporatetools-okta[.]com
- hr-myccmortgage[.]com
- hr-synovus[.]com

Looking over the full list, our team noticed the domains found matched previously seen patterns:

- Domains were registered on Hosting Concepts, GoDaddy, and NiceNIC.
- They were hosted on Virtuo, DigitalOcean, and Choopa.

We then pivoted into dedicated IP ranges that hosted these and found several new domains matching similar patterns during the same timeframe.

Domains found from dedicated IP pivots:

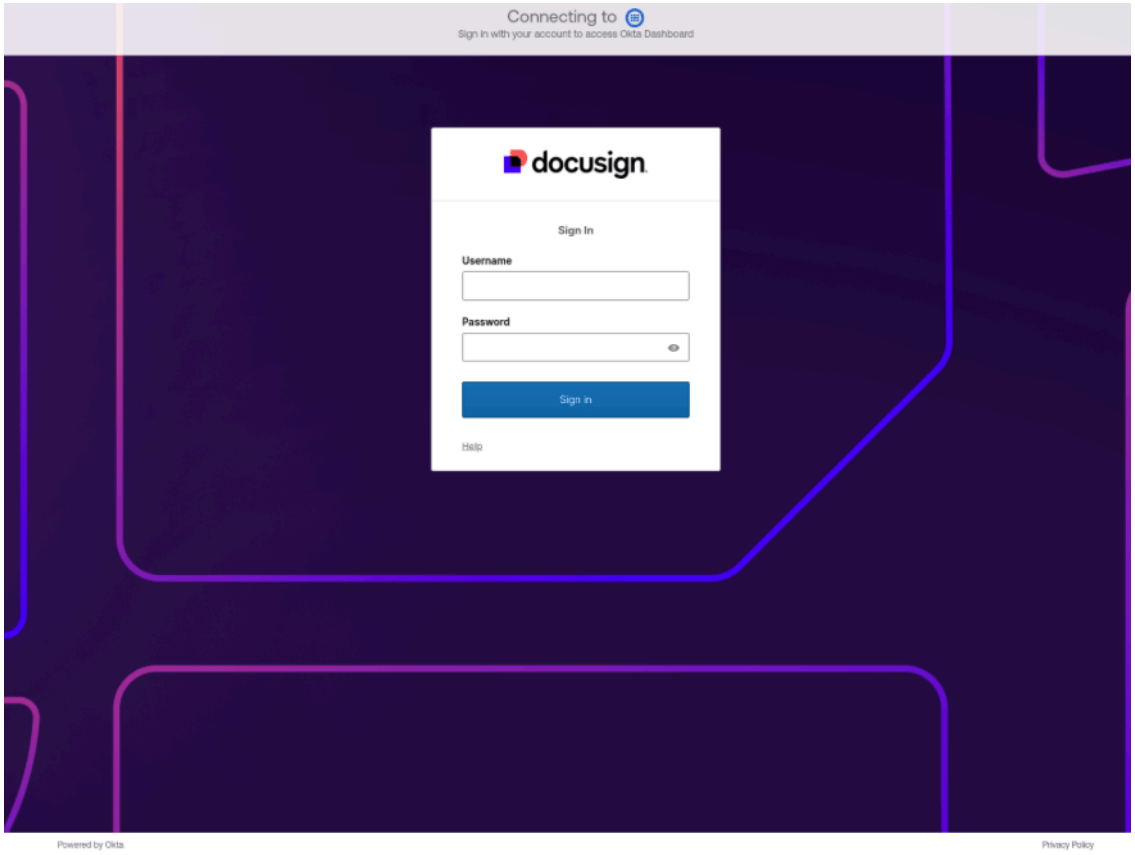
- 7-eleven-hr[.]com
- bell-hr[.]com
- cts-comcast[.]com
- doordash-support[.]com

Note: The domains were registered on NameSilo, NiceNIC, and Hosting Concepts.

Kit #4 – Minor Change from Kit #3

When reviewing some of the phishing pages captured via previous phishing kits, we noticed some domains serving a kit that looked visually identical to Phishing Kit #3, mimicking the targeted organization's Okta dashboard by displaying the logo, organization name, and having a "Powered by Okta" header and footer.

The only subtle difference we observed was within some of the code—minor tweaks, but largely the same as Kit #3.



docusign-okta[.]com

This slight variation on Kit #3, which we classified as Kit #4, was one of the more recent kits seen in the wild.

First seen: September 2024

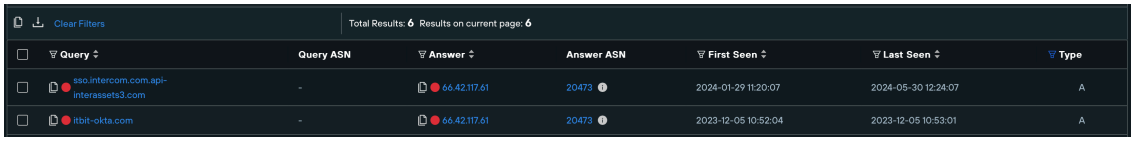
Last seen: February 2025

Sample of new domains found:

- commonspiritcorp-okta[.]com
- citrix-okta[.]com
- consensys-okta[.]com
- twitter-okta[.]com
- itbit-okta[.]com

We saw that the new domains were served from Njalla VPS servers, AS39287 (ABSTRACT, FI), a new AS for this threat group.

However, by analyzing historical DNS records of the domains, we saw that itbit-okta[.]com had been hosted on a Vultr IP address, AS20473 (AS-CHOOPA), which aligns with historical Scattered Spider activities.



66.42.117[.]61

2024-2025 Hosting Providers Timeline

Analyzing the ASNs of IP addresses collected in 2024, we saw that Scattered Spider consistently used IPs from DigitalOcean, Vultr, and BitLaunch. Recalling that BitLaunch (bitlaunch[.]io) provided anonymous VPS on BitLaunch servers, DigitalOcean, and Vultr, it's likely that Scattered Spider operators are renting significant numbers of servers on this service. Our analysts believe, based on our research, that this has been the group's service of choice for a long time, as previous articles from organizations like Okta have confirmed separately as well.

However, since the second quarter of 2024, Scattered Spider started renting dedicated servers on other BPH hosts, including "privacy-focused" hosting providers such as Virtuo and Njalla. In January 2025, our researchers picked up a campaign using Cloudflare, which is new for Scattered Spider.

ASN	Hosting Provider	First Seen
AS47583 (AS-HOSTINGER, CY)	Hostinger	September 2023
AS20473 (AS-CHOOPA, US)	Vultr (Constant)	September 2023
AS399629 (BLNWX, US)	BitLaunch (BL Networks)	March 2024

AS14061 (DIGITALOCEAN-ASN, US)	DigitalOcean	April 2024
AS214943 (RAILNET, US)	Unknown (theodexer@gmail[.]com, railnet@gmail[.]com)	April 2024
AS57043 (HOSTKEY-AS, NL)	HostKey	June 2024
AS42624 (SIMPLECARRIER, US)	GlobalData Cloud (globaldata-cloud[.]com)	July 2024
AS399486(VIRTUO, CA)	Virtuo Host (BPH)	August 2024
AS39287 (ABSTRACT, FI)	Njalla	October 2024
AS13335 (Cloudflare, Inc)	Cloudflare	January 2025
AS39287 (ABSTRACT, FI)	Njalla	February 2025

Current Scattered Spider Infrastructure Preferences

- **Registrar:** NiceNIC
  - Used since the second quarter of 2024
  - Many of the domains registered after 2024 were created through this service
- **Hosting Provider:** Njalla, Virtuo, Cloudflare
  - Virtuo was last used in October 2024
  - Njalla was last used in November 2024

Malware Delivery Cluster

Scattered Spider registered domains featuring the same keywords in waves – essentially using specific generic keywords to target multiple brands.

We saw that a subset of the high-confidence potential domains was registered consecutively in May 2024 and targeted some niche brands that Scattered Spider had impersonated in previous attacks.

All of the domains followed the same name pattern: **<targeted_company>-cdn.com**

First seen: May 2024

Last seen: May 2024

Some of the domains seen include:

- bestbuy-cdn[.]com
- duelbits-cdn[.]com

- gucci-cdn[.]com
- simpletexting-cdn[.]com

These domains were all registered on NiceNIC, further indicating a shared developer.

The Web Scanner records revealed that some of these had an Open Directory for a while, which we then accessed, extracted the malicious file, and analyzed it. We will cover this analysis in the next section.

Open Directory on telnyx-cdn[.]com

Malware Analysis Introduction

Once we analyzed the file referenced above, we discovered that Scattered Spider was using an updated version of Spectre RAT.

Spectre RAT is a remote access Trojan (RAT) that enables threat actors to gain persistent access to compromised systems. Like many such tools, it provides capabilities for data exfiltration, command execution, and system reconnaissance. Its design allows it to be stealthy and flexible, features that make it attractive to sophisticated attackers.

The updated version used by this group featured a set of techniques ranging from obfuscation to the use of a sophisticated crypter. The malware was compiled in both 32-bit and 64-bit versions for Intel processors. It also included a wide range of newly implemented C2 commands. Additionally, some commands and features are still being implemented or only partially added, suggesting this malware is still in a heavy developmental phase. As time goes on, we expect the malware to further evolve through the incorporation of additional features and protections.

The malware started by initializing a large list of initialization functions, which were present in the "_initterm" function of MSVC.

```
start_PTR       db    0                 ; DATA XREF: sub_419BC6+
                db    0
                db    0
                db    0
                dd offset sub_419BB4
                dd offset sub_4020A2
                dd offset sub_4020D0
                dd offset sub_4020E6
                dd offset sub_4020C4
                dd offset sub_4020B8
                dd offset sub_4016D6
                dd offset sub_401CC8
                dd offset sub_401E4D
                dd offset sub_401EAB
                dd offset sub_401E7C
                dd offset sub_40198F
                dd offset sub_4018C3
                dd offset sub_401C81
                dd offset sub_4017F7
                dd offset sub_4017A4
                dd offset sub_401711
                dd offset sub_401A77
                dd offset sub_401AA6
                dd offset sub_401AD5
                dd offset sub_401FB0
                dd offset sub_401391
                dd offset sub_40141E
                dd offset sub_401277
                dd offset sub_40119E
```

Example of the malware's initialization functions

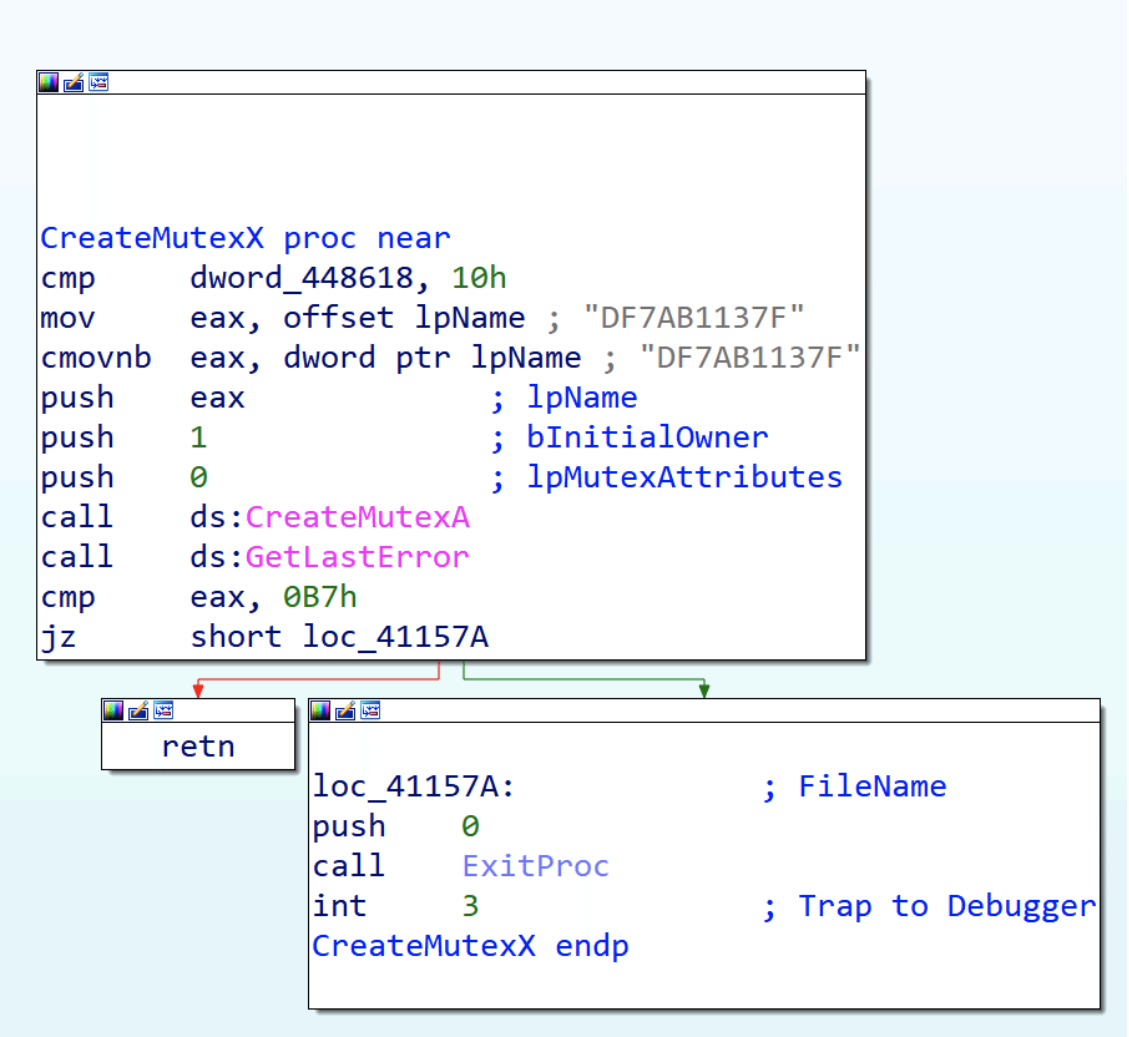
Some of the functions in this list were null functions, further indicating the malware is/was still in a heavy developmental stage. Strings in the malware were also encoded, using an XOR-based algorithm. The following IDA script helps in recovering the strings:

Spectre RAT String Decoder Code on GitHub

- https://raw.githubusercontent.com/Silent-Push/Shared/refs/heads/main/specter_rat_string_decoder.py

---

For persistence, it set up a mutex to prevent duplicate instances of the malware from running. This mechanism could also serve as a malware vaccine for Spectre RAT, as seen here:



A mutex was set up to prevent multiple instances of malware from running

If the mutex was not found, the malware proceeded to initialize the system with the following actions:

- Decoding hardcoded command and control servers from memory.
- Setting up the C2 URI.
- Retrieving user folder paths, install paths, package name, and configuration file name.
- Gathering system information (e.g., drives and processes).
- Utilizing LOL Bin binaries (such as nircmdc.exe and 7Zip) along with a downloader payload (aizk.exe).
- Reading the 89CC88 configuration for the dynamic C2 configuration file.
- Reading the 733949 configuration for system information.

The hardcoded C2 server was a decoy, used only once to retrieve the list of dynamic C2 servers, which were saved in the 89CC88 configuration and then never used again. This hardcoded C2 server was embedded in the binary and encoded with Base64 in combination with bitwise AND and XOR operations, seen below:

00407DA6 |. 24 0A |AND AL,0A

00407DA8 |. 320429 |XOR AL,BYTE PTR DS:[ECX+EBP]

Inside the binary, the string data type is represented in a specific format, and many helper functions are provided to manage this data type.

---

struct CXXStringStruct

{

char *ptr; // Pointer to buffer 0x00

int *UN1;

int UN2;

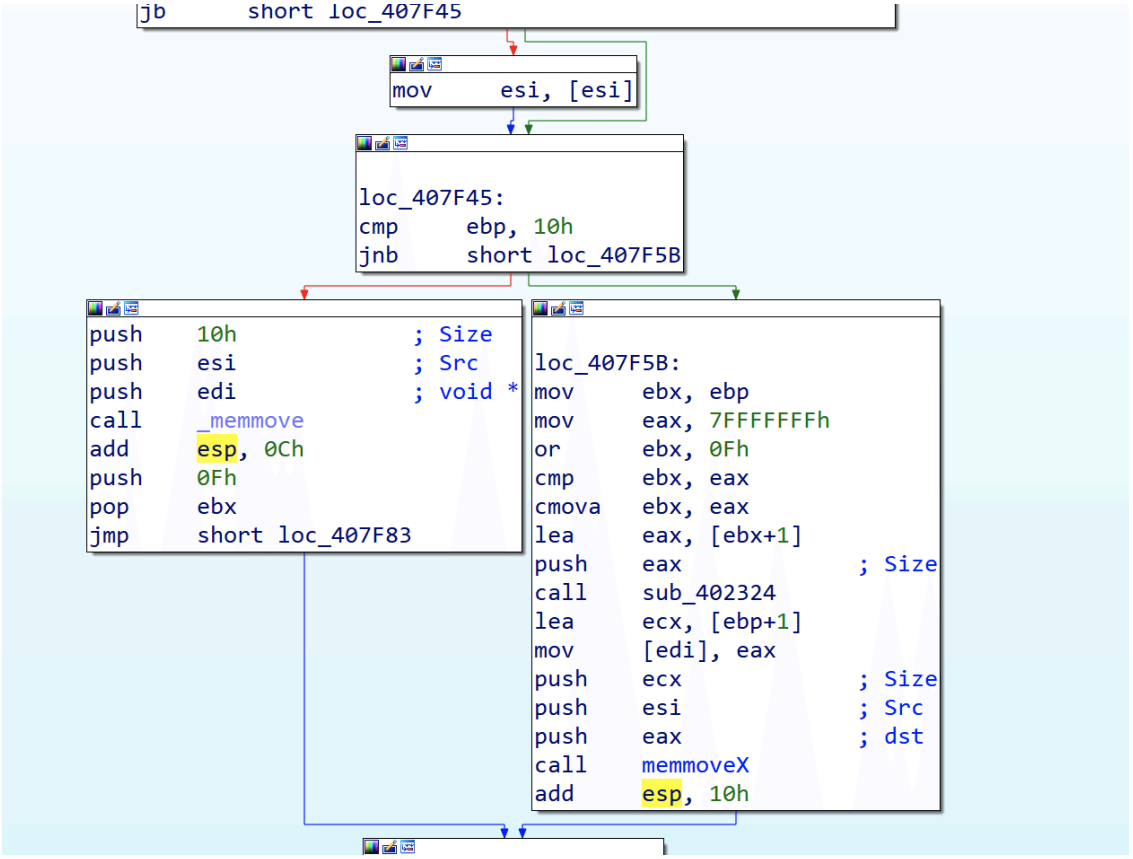
const sizeHdr; // 0x0a 0x0c size of header

unsigned int length; // length of buffer 0x10

unsigned int max_length;

};

Strings may be static instead of being pointers to a character, and a character array may also be supplied. The maximum static string size is 0x10; so if the string is less than 10 characters, it is stored within the structure, as seen here:



If the string is less than 10 characters, it is stored within the structure

“733949” file config

During the malware’s initialization phase, a file named “733949” is created. This file stores system-related information, which is also sent to the command and control server upon request. It consists of a combination of Boolean and string values separated by ‘*’. Some of these values are hardcoded and remain unexplained in the binary, yet another indication that the malware is still in development.

0: trxu

1: USER

2: COMP_NAME

3: OS Name

4: true

5: true

6: false

7: 0

8: 0

9: void

10: void

11: false — wait for c2 to signal work (will not start main thread unless c2 gives a green signal)

Communication Protocol

The communication protocol is based on HTTP and includes a URI parameter with the following breakdown:

- **wber**

***wber* Parameters**	**Purpose**	**ACK response**
6	beacon packet	“txru” or fail
5	Ping Back with no data	
35 & **kiqa** == filename_base64	Download resource from c2	“void” – supply a filename base64 encoded packet of data containing file contents

36 & &lhpg= and	Download resource from C2 (route 1) plugin	
31	GetXqls – BotnetID	None
34 lhpg== debuglog	Send DebugLog (debuglog Encoded using XOR encoding algorithm + base64)	
3	Ping Back C2 with &dpna= subcmd	dpna=5 == Uninstall Complete
10 (POSTDATA)	Send system info&jkux= Available Drives	
1	Request CMD from C2 (DecodeRevData == 1)	

Command List

The most interesting wber command for us to analyze was the wber=1 parameter, which relates to the operational command from the C2 (i.e., instructing the bot to perform a task). We were then able to reverse-engineer a variety of commands. Parameters are tokenized using the “|” character.

CMD number	**Parameter (tokenized by ‘|’)**	**Description**
1	Filename	Download a file from infected machine
2	Type*http payload *	Upload a file on infected machine
3	FolderPath*filename	Execute an executable on the infected machine based on the folder path type, which can range from 3 to 9 to represent different file paths. For example, type 3 corresponds to the Roaming folder.
5	Additional File to Remove	Uninstall Bot
6	wber3_trigger a pingback to c2	wber3_trigger switch
7		Get Infection Info
9	Process Name	Terminate a Process
10		Send list of all Running Processes

12		Send DebugLogs
13	C2Server	Add Additional C2 Server (write to *SaveAndWrite89CC88* file
14	num*command	execute cmd.exe /c command
15		Retrieve monitor Info + Recon info from psinfo.exe – applications, etc

Leveraging all this information, we implemented a testing C2 server for Spectre RAT to facilitate captive bot testing. This setup served multiple purposes, the code for which is included below:

- **Simulation and Analysis:** This allows researchers to simulate real-world scenarios and analyze how the malware responds to various operational commands, thereby deepening our understanding of its functionality.
- **Operational Takeover Utility:** In the event of a successful takeover of a Spectre RAT C2 infrastructure, the same mechanism can be used to send commands to infected systems. For example, law enforcement agencies could potentially use such a command channel to instruct the malware to uninstall itself from compromised devices.
- **Mitigation Strategy:** This capability represents a proactive mitigation strategy, offering a controlled method to neutralize the threat while minimizing collateral damage.

Spectre RAT String Emulator on GitHub

-
- https://raw.githubusercontent.com/Silent-Push/Shared/refs/heads/main/specter_rat_c2_emulator.py

---

Debug Logging System

The malware incorporates a logging system that records all error and debug messages generated during its runtime. This system serves multiple purposes:

- **Diagnostic Data:** It collects information on failures or unexpected behavior, which can help the malware adapt its operations dynamically.
- **Operational Stealth:** By logging errors internally rather than displaying them, the malware minimizes external clues that might alert security systems or users.
- **Feedback Loop:** The logs provide a feedback mechanism for the malware, enabling it to modify its behavior or troubleshoot issues without relying on external inputs.
- **Post-Infection Analysis:** In some cases, malware may transmit these logs back to a command and control server, offering attackers insights into its performance and potential vulnerabilities in the infected system.

Some of the error logs with error codes included:

Error Code A	Error Code B	Description
100	10010	beacon command 6 invalid response
100	10002	install path after installation does not exist

Continuing to Track Scattered Spider

As Scattered Spider continues to demonstrate its resilience in the global cyber threat landscape, Silent Push remains committed to equipping defenders with the intelligence they need to pre-emptively detect and counter this evolving threat.

We will continue to report on our work tracking Scattered Spider and share any new findings as our research progresses throughout 2025. If you or your organization have any leads related to this effort, particularly those being used by these threat actors, we would love to hear from you.

Mitigation

Silent Push believes all Scattered Spider-related domains present some level of risk.

Our analysts constructed **Silent Push IOFA™** Feeds, which provide **Indicators of Future Attack™** domains and IPs used by Scattered Spider.

Also, as Scattered Spider now uses “Publicly Rentable Domains”—essentially, Dynamic DNS providers that allow people to register subdomains on a central domain—tracking its future infrastructure has become slightly more complex.

Silent Push Threat Analysts created a Bulk Data Feed for all domains we’re tracking that rent subdomains and provide Dynamic DNS services. We suggest alerting on connections to any subdomains on these domains and, for some organizations, blocking connections to them.

Silent Push **Indicators of Future Attack™** (IOFA™) Feeds and Bulk Data 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.

Register for Community Edition

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.

Scattered Spider Sample Indicators of Future Attack™ (IOFA) List

Below is a sample IOFA™ list associated with Scattered Spider. Our full list is available for enterprise users. Silent Push Enterprise clients have access to domain and IP feeds containing all Scattered Spider infrastructure.

Scattered Spider Indicators of Future Attack™:

- 7-eleven-hr[.]com
- activecampiagn[.]net
- acwa-apple[.]com
- bbtplus[.]com
- bell-hr[.]com
- bestbuy-cdn[.]com
- birdsso[.]com
- citrix-okta[.]com
- commonspiritcorp-okta[.]com
- consensys-okta[.]com
- corp-hubspot[.]com
- cts-comcast[.]com
- doordash-support[.]com
- duelbits-cdn[.]com
- freshworks-hr[.]com
- gemini-sso[.]com
- gucci-cdn[.]com
- itbit-okta[.]com
- iyft[.]net
- klaviyo-hr[.]com
- login.freshworks-hr[.]com
- login.hr-intercom[.]com
- morningstar-okta[.]com
- mytsl[.]net
- okta-ziffdavis[.]com
- pfchangs-support[.]com
- prntsrc[.]net
- pure-okta[.]com
- signin-nydig[.]com
- simpletexting-cdn[.]com
- squarespacehr[.]com
- sytemstern[.]net
- sso-instacart[.]com
- sts-vodafone[.]com
- twitter-okta[.]com
- xn--gryscale-ox0d[.]com

- x-sso[.]com

Source: https://www.silentpush.com/blog/scattered-spider-2025/