Unknown Title

Arda Büyükkaya

September 17, 2025

ShinyHunters Calling: Financially Motivated Data Extortion Group Targeting Enterprise Cloud Applications

Executive Summary

EclecticIQ analysts assess with high confidence that ShinyHunters is expanding its operations by combining AI-enabled voice phishing, supply chain compromises, and leveraging malicious insiders, such as employees or contractors, who can provide direct access to enterprise networks.

ShinyHunters is very likely relying on members of Scattered Spider and The Com to conduct voice phishing attacks that provide unauthorized access to single sign-on (SSO) platforms used by retail, airline, and telecom companies. The group uses this access to exfiltrate large volumes of customer data and extort victim organizations.

Analysts observed that ShinyHunters leader, ShinyCorp, is actively selling stolen datasets with ransomware affiliates and other eCrime actors, at prices exceeding $1M per company.

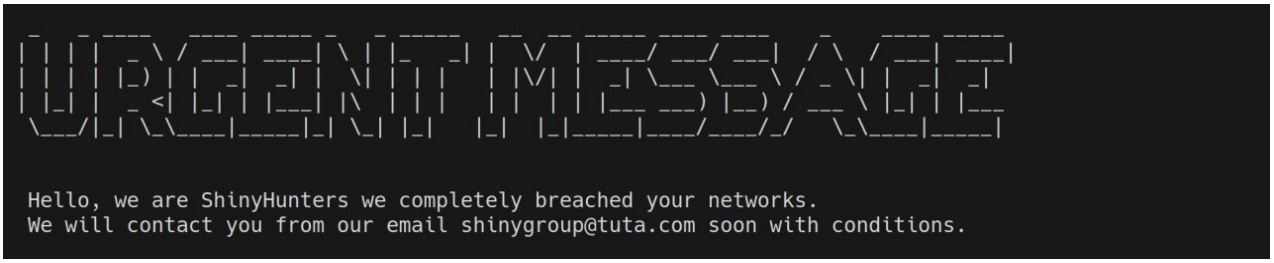


Figure 1 - Data extortion message received by a ShinyHunters victim.

ShinyHunters targets high privilege engineering accounts on Git version control, BrowserStack, JFrog, and cloud project management platforms to infiltrate CI/CD pipelines. Analysts assess with high confidence that this access is very likely intended to enable supply chain attacks, a favored tactic of ShinyHunters that allows threat actors to compromise thousands of enterprise systems through a single point of access in the software supply chain.

EclecticIQ analysts observed that the ‘shinysp1d3r’ ransomware-as-a-service (RaaS) network is currently in development, with features designed to encrypt VMware ESXi environments. Analysts assess with medium confidence that once operational, ShinyHunters will likely leverage this service to expand its victim base, attract new affiliates, and broaden its extortion capabilities.

ShinyHunters Group Structure and Leadership

ShinyHunters is a financially motivated threat group that first emerged in 2020 and operates under the leadership of the ShinyCorp persona [1]. Group members are active in Telegram and English-speaking cybercrime forums like BreachStars, OGUsers and DarkForums. EclecticIQ analysts observed that ShinyHunters members use these channels to sell or leak the sensitive data exfiltrated from various organizations.

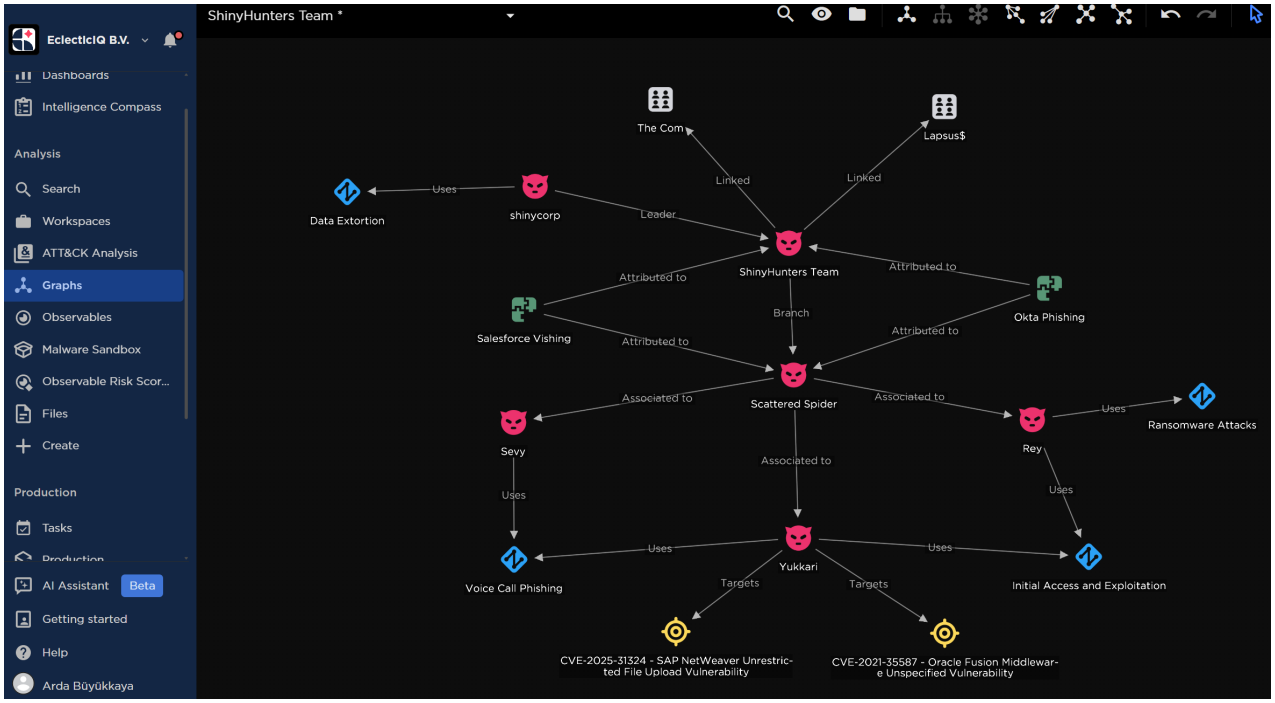


Figure 2 - Overview of ShinyHunters team and connection with Scattered Spider on the graph view within EclecticIQ's Threat Intelligence Platforms (TIP).

EclecticIQ analysts identified three of the most active ShinyHunters members who are likely responsible for recent campaigns in 2025. These members also have loose connections with other adversary groups like Scattered Spider [2], The Com [3] and Lapsus$ [4].

Despite this connection, there is no direct relationship between ShinyHunters and Scattered Spider. Analysts assess with high confidence that some Scattered Spider members are hired by ShinyHunters to perform voice call phishing and social engineering campaigns against enterprise victims. This collaboration between different eCrime groups also targeted Salesforce users in airline and retail sectors [5].

Connection Between ShinyHunters and eCrime Ecosystem

EclecticIQ analysts assess with high confidence that the threat actor persona named Yukari (aka Yuki, Yuka, yukimane or yukafeet) is an active member of both ShinyHunters and Scattered Spider, very likely responsible for initial compromise, SIM swapping attacks, and voice call phishing.

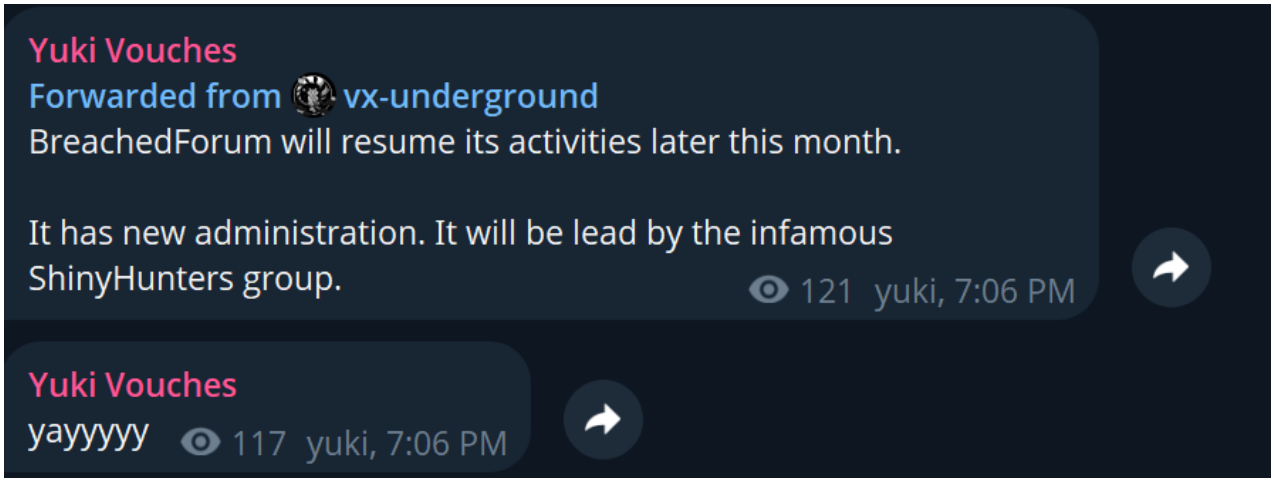


Figure 3 - Telegram channel operated by Yukari showing connection with ShinyHunters.

EclecticIQ analysts assess with high confidence that ShinyHunters leader ShinyCorp (aka sp1d3rhunters or shinyc0rp in Telegram) recruited cybercriminals through eCrime actors including Scattered Spider and The Com.

Threat actor Rey, who leads the Angel RaaS program [6], directed initial access operations involving brute force attacks against edge network devices like VPN or firewall solutions and the exploitation of known vulnerabilities in internet facing servers. Threat actor Sevy focused on social engineering, carrying out voice call phishing campaigns against enterprise organizations.

EclecticIQ analysts assess with high confidence that ShinyHunters members operate interchangeably across multiple cybercriminal groups, with some maintaining ties to Ransomware-as-a-Service (RaaS) programs. This cross membership integrates ShinyHunters into the broader eCrime ecosystem, enabling the exchange of tools, techniques, and operational knowledge that enhances the effectiveness and success rate of their attacks.

Using AI Voice Agents and Scattered Spider Affiliate Network for Scalable Vishing Campaigns

ShinyHunters affiliates used VoIP based calling services including Twilio, Google Voice, and 3CX for vishing operations. The group also abused legitimate AI-powered voice call platforms such as Vapi [7] and Bland [8] to automate social engineering calls at scale.

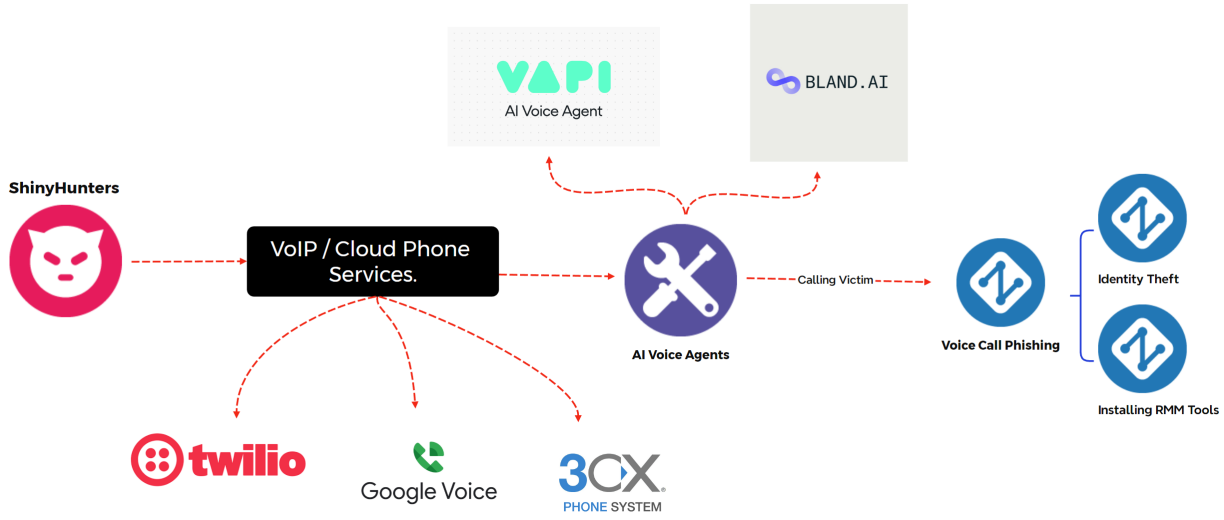


Figure 4 - AI Voice Agent workflow in Vishing campaigns.

ShinyHunters members abused Bland AI to power AI-driven social engineering agents that dynamically adjust their narratives and tactics in real time, tailoring responses to victim's reactions during phone calls. The built-in large language model (LLM) in Bland AI enables attackers to generate and design conversational pathways [9] tailored to specific scenarios, ensuring the call remains convincing even if the victim responds outside the scripted scenario.

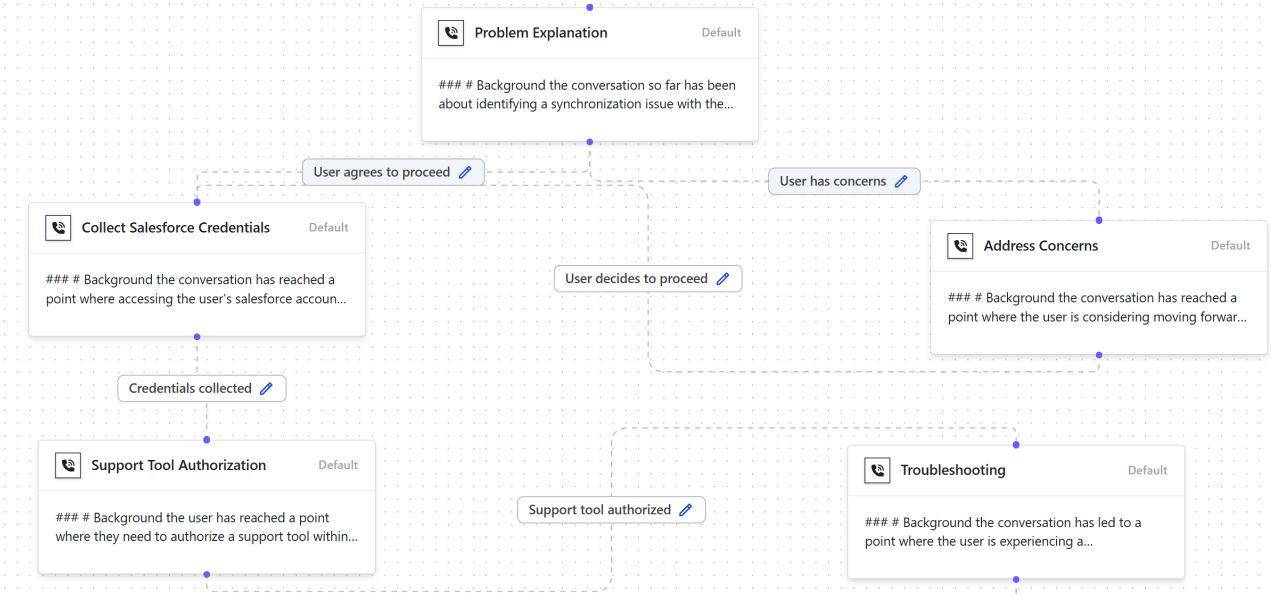


Figure 5 - Example of pathway feature in Bland AI.

Attackers can configure voice styles including gender and regional accents, making output sound human-like rather than robotic. Unlike static robot voice calls, the AI model dynamically generates voices and adjusts tone and responses to sustain credibility and manipulate the target. This combination of LLM-powered dialogue management and near-realistic synthetic voice allows ShinyHunters linked threat actors to run successful vishing operations at scale.

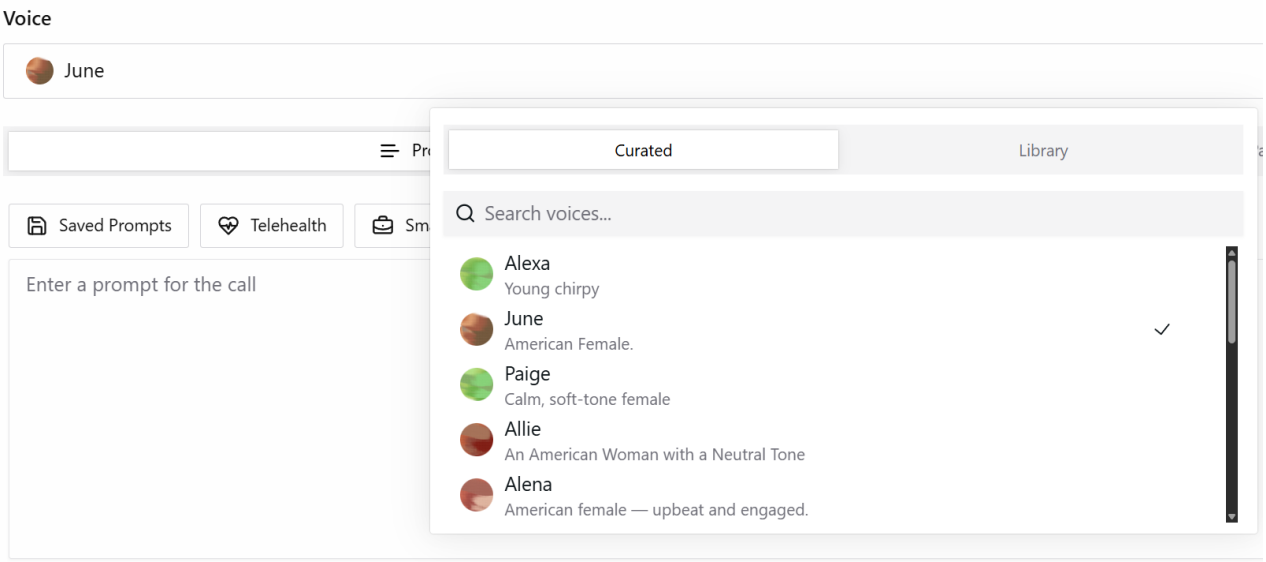


Figure 6 - AI voice agent options in the Bland AI user interface.

According to ShinyCorp, voice call phishing attacks are solely carried out by Scattered Spider members. EclecticIQ analysts observed that while Scattered Spider conducts its own vishing operations, some members also rely on outsourced services from other actors within *The Com* ecosystem.

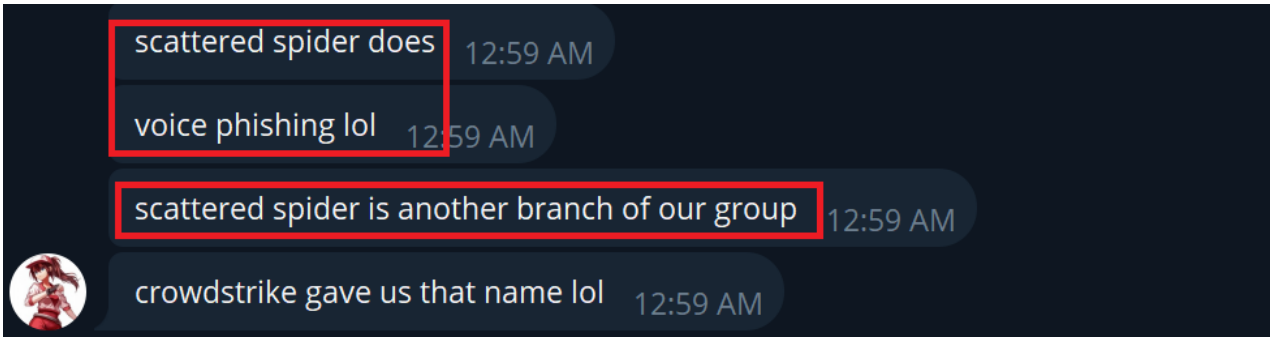
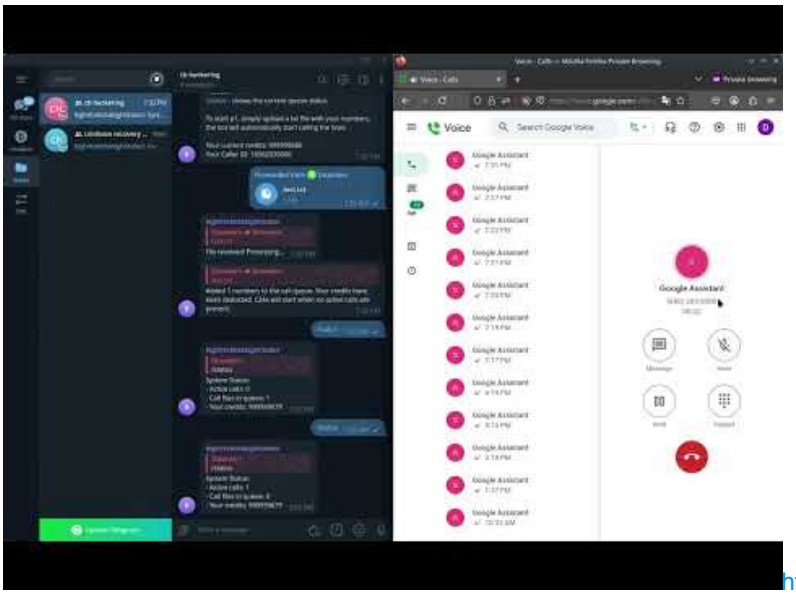


Figure 7 - Telegram message from ShinyCorp referencing Scattered Spider's involvement in voice call phishing operations.

These include so-called 'call center' platforms and 'P1' (press-one) services. The call center platforms are centralized dashboards that provide an interface for managing voice call phishing campaigns at scale. P1 services are automated vishing services typically managed through Telegram bots.

An example voice call with a P1 service can be seen in the below video:



https://youtu.be/yRN0UDA-21M

Figure 8 - Example of a P1 service abusing Google Voice to perform vishing attacks against Coinbase users.

These services allow threat actors to place calls over Google Voice or other VoIP providers and lure victims into pressing "1" to trigger pre-configured phishing templates. Attackers design and upload the templates to Telegram bots. The templates can simulate machine-generated voices, capture credentials, and automate the authentication flow, significantly lowering the barrier to entry for vishing campaigns.

Analysts identified that ShinyCorp actively recruits voice call phishing experts through Telegram groups such as *Sim Land (SL)*, an underground community operated by The Com members. The Sim Land channel enables financially motivated actors to exchange knowledge, sell services, and collaborate SIM swapping, voice call phishing, and financial fraud.

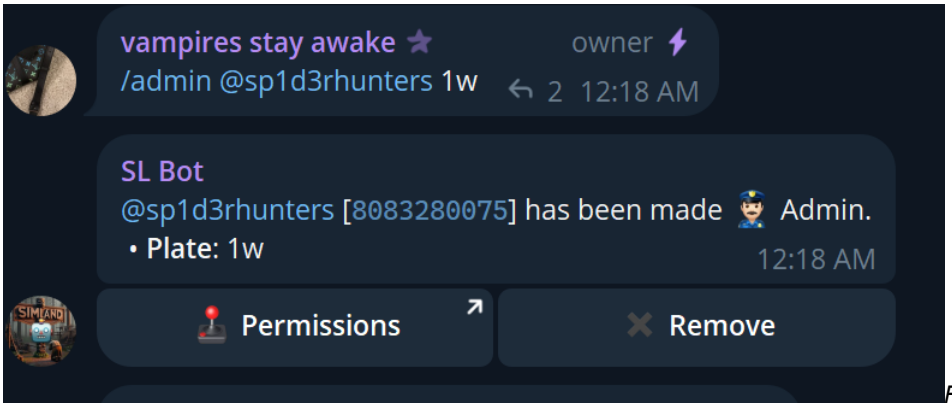


Figure 9 - ShinyCorp gaining admin access on the Sim Land Telegram channel.

ShinyCorp selects recruits based on proven social engineering skills via phone calls. Some of the selected threat actors previously conducted cryptocurrency scams by impersonating Coinbase or Apple/Gmail support staff. On August 19, 2025, ShinyCorp became an admin of the Sim Land Telegram channel [10], demonstrating close coordination between eCrime actors and the ShinyHunters leader ShinyCorp.

Vishing Attacks Against Enterprise Cloud Application Users Leading to Seven-Digit Extortion Demands

EclecticIQ analysts assess with high confidence that ShinyHunters orchestrated vishing operations to compromise Salesforce applications [11]. Attackers impersonated IT staff and called corporate support desks, directing employees to the legitimate Salesforce app connection page. During these calls, victims were deceived into entering connection codes that authorized actor-controlled applications, often a modified version of the Salesforce Data Loader thereby granting attackers access to organizational accounts.

Compromised Salesforce CRM (Customer Relationship Management) dashboards enabled bulk data exfiltration and lateral movement into Okta, Microsoft 365 and Amazon S3. In several data extortion campaigns, ShinyHunters used the LimeWire file-sharing service to leak samples of stolen data, amplifying pressure on victims to pay seven-digit extortion demands.

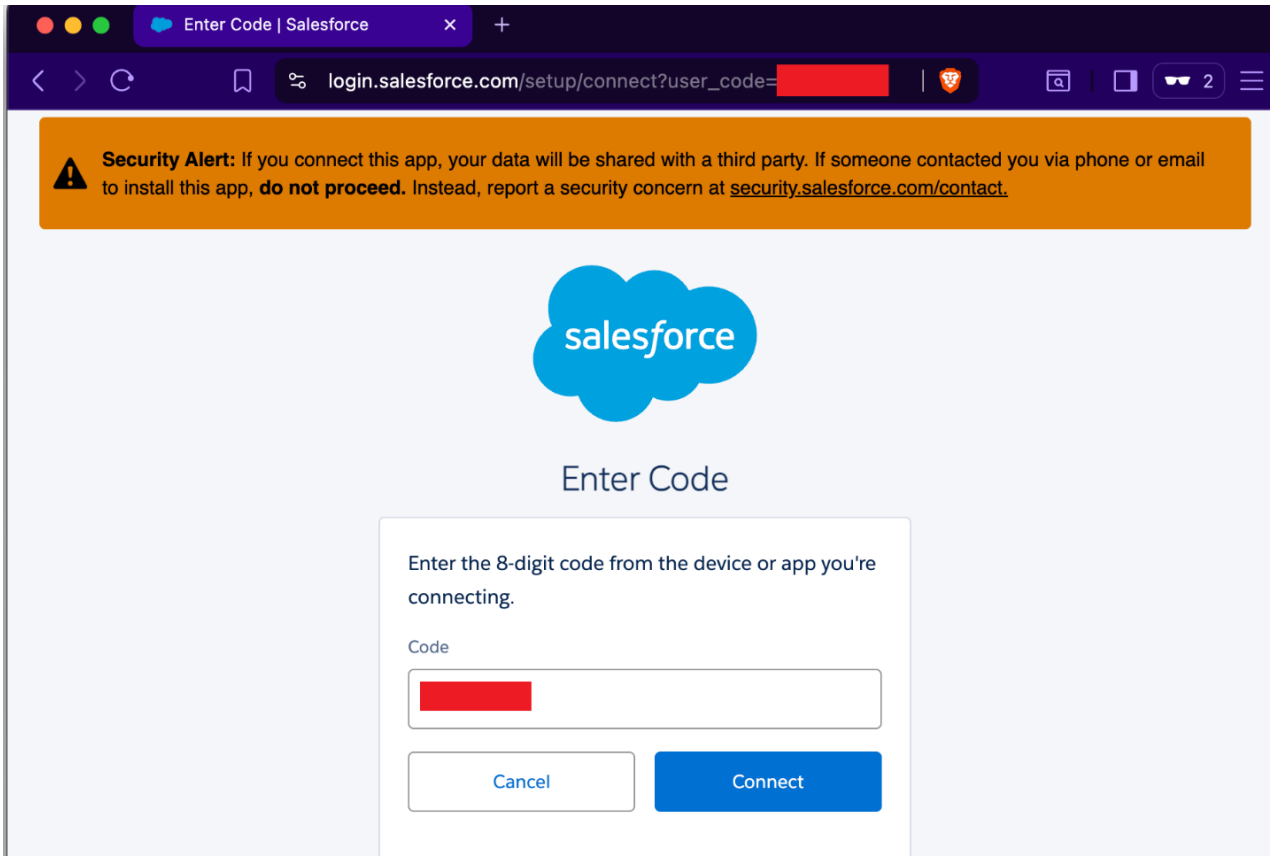


Figure 10 - Example of Salesforce connect code phishing, where attackers redirect victims to" /setup/connect" over voice call.

EclecticIQ analysts identified that attackers exfiltrated Salesforce datasets from enterprises in the airline and retail sectors.

Example exfiltrated dataset from an airline company:

- 26 GB of user account data
- 16 GB of customer contact records
- 5.5 GB of email logs
- 4.1 GB of flight records
- 1.3 GB of live chat transcripts

After gaining access, ShinyHunters used the victims Salesforce CRM dashboards to call their customers through the Omni-Channel feature [12], turning the trusted platform into a tool for vishing and data extortion.

EclecticIQ analysts identified that ShinyCorp is selling stolen airline data for up to $1 million per company. ShinyCorp used Telegram and qTox to communicate with potential buyers, showing his focus on high-value corporate data to maximize the financial gain.

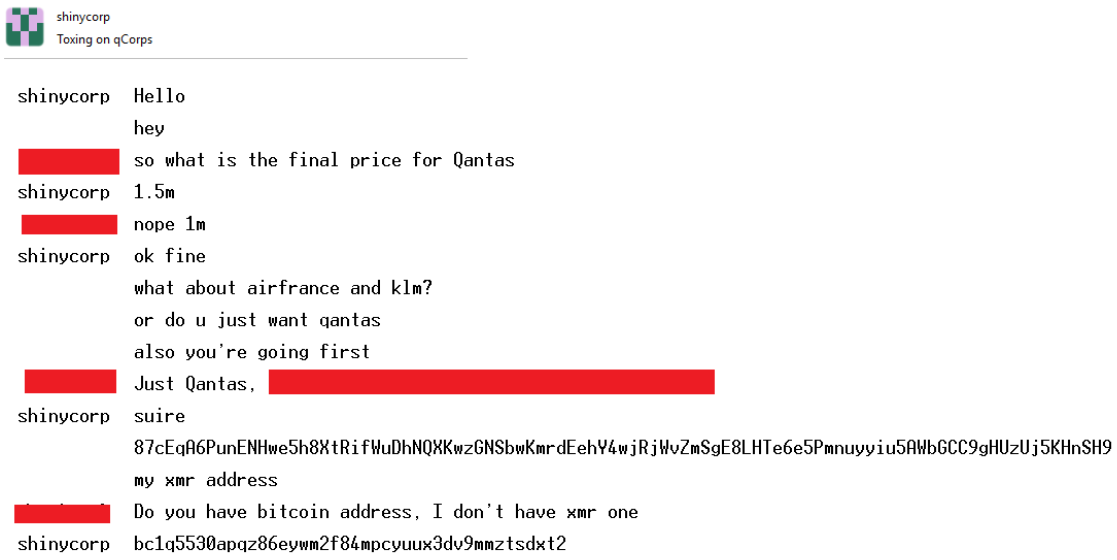


Figure 11 - Communication between ShinyCorp for selling exfiltrated Salesforce data from airline victims.

EclecticIQ analysts observed that, ShinyHunters using exfiltrated sensitive customer data as leverage to pressure victims during negotiations. The group achieves this objective through identity theft against high-privileged SSO users or by gaining initial access to data-rich systems via remote management tools (RMMs) such as ConnectWise ScreenConnect.

Analysis of recent incidents shows a consistent playbook across different styles of vishing operations. In some cases, attackers use non-pretexted calls, often run by experienced scammers, designed to directly capture user credentials. Some of the campaigns use pretexted calls, where the threat actor impersonates an employee or IT staff to request a password reset, MFA update, or application authorization. Increasingly, threat actors are also adopting AI-powered voice calls, which generate natural-sounding dialogue, adjust tone and content in real time, and sustain credibility even when victims respond unpredictably.

Across these different approaches, certain patterns recur. Calls often begin with a calm, cooperative tone and a fake IT help scenario, such as:

- **Escalating requests** - callers often pose as legitimate staff to persuade help desk employees into issuing temporary credentials or updating 2FA tokens or resetting phone numbers associated with MFA. These calls typically start with a simple request like a password reset before escalating to more sensitive changes such as modifying MFA settings or installing an RMM tool.
- **Convincing cover stories** – attackers frame requests around everyday IT problems such as forgotten passwords, login failures in VPN service, or delays in cloud applications.
- **Steering the process** – adversaries may provide specific technical cues to install RMM tools like Anydesk or gather sensitive information about their victims' networks.
    - A similar technique was observed in the Salesforce Data Loader phishing campaign, where callers posing as IT staff guided victims to navigate to "/setup/connect" under the pretext of resolving a technical issue. By steering the conversation step by step, the attackers created the illusion of legitimate troubleshooting while in fact directing the victim into establishing unauthorized OAuth access.
- **Polite delivery** – instead of urgency or aggression, the caller maintains a calm, cooperative tone, often reassuring the employee with phrases like "take your time" which reduces suspicion.

These tactics are effective because they exploit human trust while leaving minimal digital traces. IT help desk and other frontline support staff are particularly attractive targets, as they hold the access, permissions, and institutional knowledge to make critical changes in user accounts and authentication systems. Once attackers secure cooperation from these personnel, they can pivot quickly to data theft, financial fraud, or extortion. The evolution from scripted

pretexts to adaptive AI-driven vishing agents illustrates how voice-based intrusions are being scaled and professionalized within the eCrime ecosystem.

ShinyHunters Targets Enterprise Okta Users Since Early 2025

EclecticIQ analysts assess with high confidence that ShinyHunters has operated phishing infrastructure since early 2025. The group impersonated Okta SSO login pages to steal credentials from high-value sectors including investment banking, luxury retail, travel, U.S. payment processing, and major e-commerce.

Okta is an identity and access management (IAM) platform that centralizes authentication to many enterprise cloud applications through single sign-on (SSO). This makes it a high-value target for attackers. Compromising a single SSO-enabled Okta account bypasses authentication controls and grants access to multiple business-critical systems, including Slack, CI/CD pipelines, HR management tools, cloud data stores and other enterprise applications [13].

Reused Phishing Templates Impersonating Okta Login Page

EclecticIQ analysts observed that as part of ShinyHunters social engineering strategy, threat actors cloned the authentication flow and user interface of a legitimate Okta subdomain (trial-6857053.okta[.]com). They replicated the login form with target organization branding to create a convincing phishing page that mimicked official Okta environments.

Figure 12 - Pivoting from cloned Okta login form to other Phishing infrastructure.

Analysts pivoted from the domain name (trial-6857053.okta[.]com) and its phishing theme to identify 12 infrastructure artefacts linked to ShinyHunters phishing campaigns. EclecticIQ analysts observed that these phishing attacks targeted sectors consistent with previously reported ShinyHunters activity, including luxury retail (e.g., Louis Vuitton) and financial institutions [14].

The fake Okta login theme closely resembles phishing templates described in ReliaQuest's August 12 publication, suggesting overlap in both tactics and targeting [15]. Analysis of the phishing page indicates the Okta login form was first cloned on August 23, 2022 (Brazil time zone) [16].

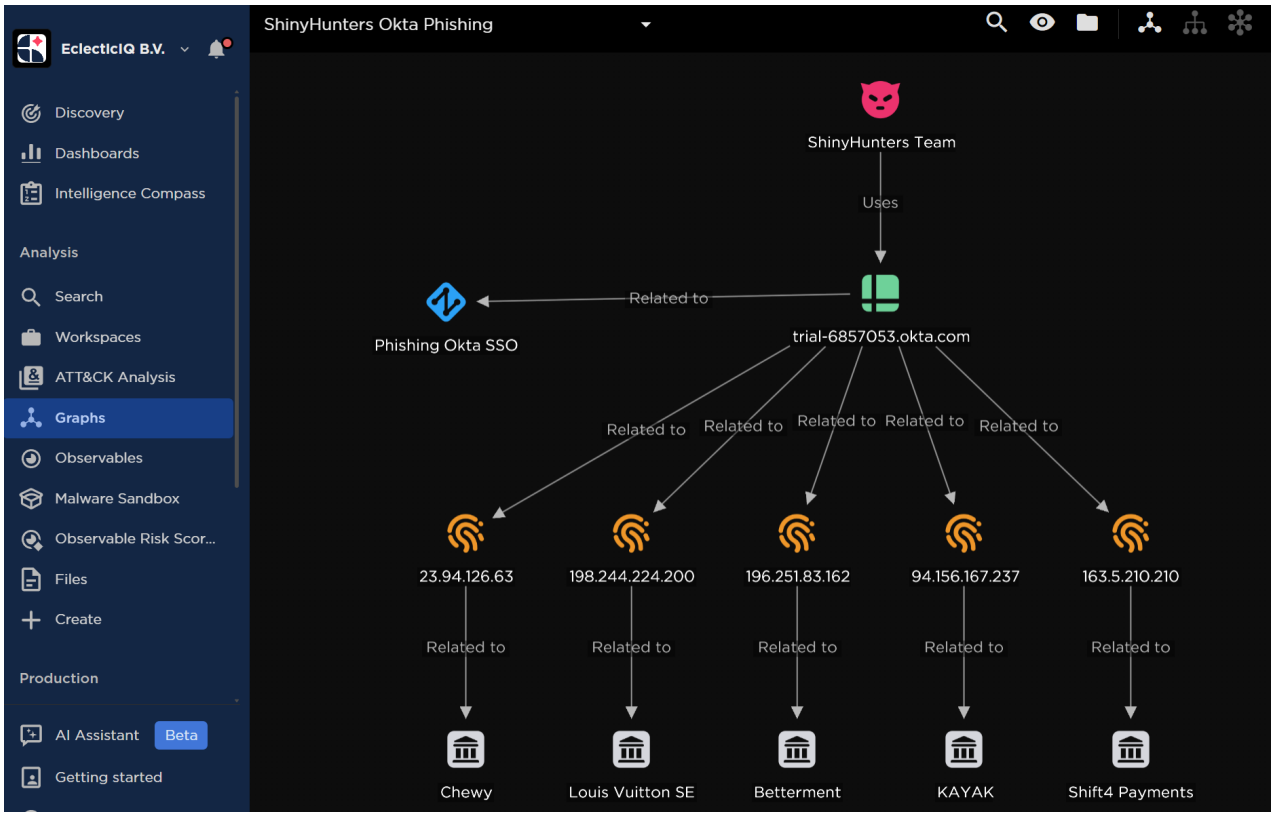


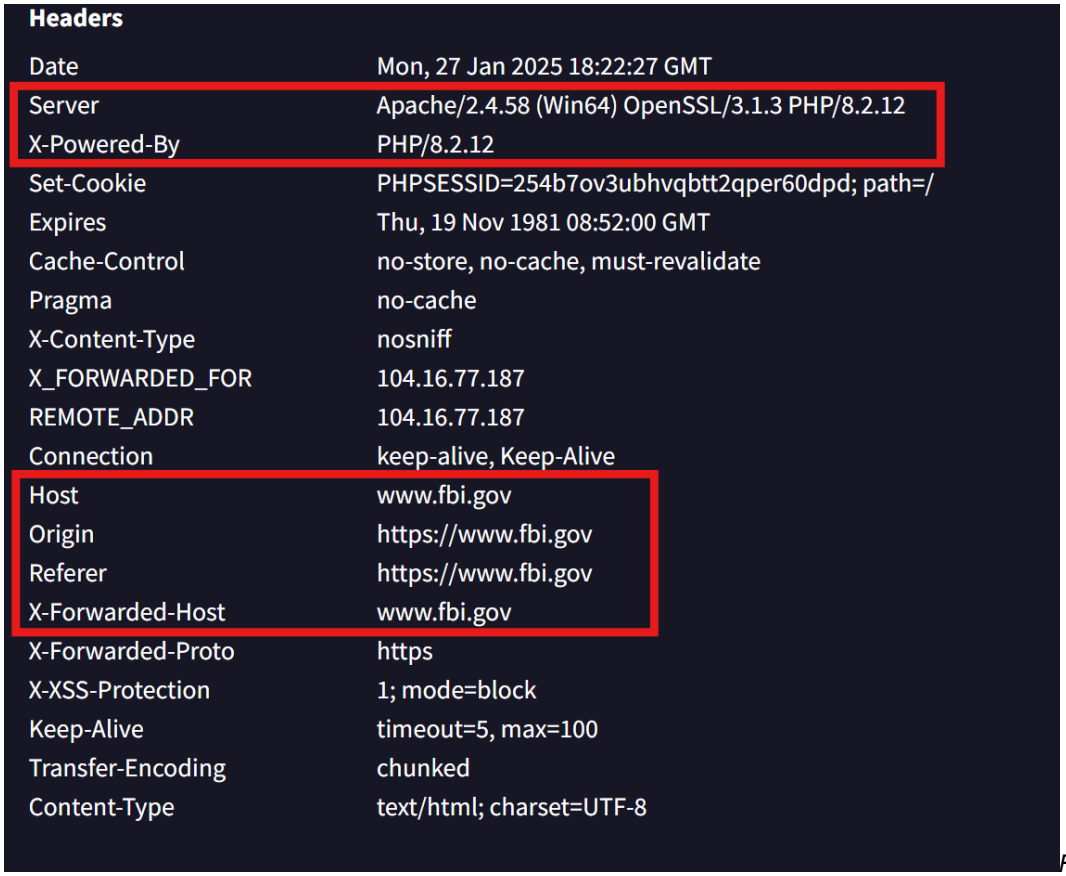
Figure 13 - Link analysis of the Phishing infrastructure in EclecticIQ's TIP.

The impersonated login form, copied from the legitimate Okta domain (trial-6857053.okta[.]com), has been observed across multiple campaigns, with samples collected between June 29, 2023, and June 10, 2025. Throughout this period, the same login form page was repeatedly reused with only branding adjustments to impersonate targeted organizations' Okta login panel.

```
<meta name="savepage-url" content="https://trial-6857053.okta.com/oauth2/v1/authorize?client_id=okta
<meta name="savepage-title" content="proton-trial-6857053 - Sign In">
<meta name="savepage-pubdate" content="Unknown">
<meta name="savepage-from" content="https://trial-6857053.okta.com/oauth2/v1/authorize?client_id=okt
<meta name="savepage-date" content="Tue Aug 23 2022 13:20:44 GMT-0300 (Brasilia Standard Time)">
<meta name="savepage-state" content="Standard Items; Retain cross-origin frames; Merge CSS images; R
<meta name="savepage-version" content="27.5">
<meta name="savepage-comments" content="">
```

Figure 14 - Time zone metadata inside the cloned Okta login forum.

Analysis of the pivoted Okta phishing infrastructure revealed identical HTTP response headers across hosts, including references to fbi.gov. The Server header consistently shows *Apache/2.4.58 (Win64) with OpenSSL/3.1.3* and minor variations in PHP versions (*8.0.30 vs. 8.2.12*), indicating centralized configuration and management under the same operation.



Headers	
Date	Mon, 27 Jan 2025 18:22:27 GMT
Server	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By	PHP/8.2.12
Set-Cookie	PHPSESSID=254b7ov3ubhvqbtt2qper60dpd; path=/
Expires	Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control	no-store, no-cache, must-revalidate
Pragma	no-cache
X-Content-Type	nosniff
X_FORWARDED_FOR	104.16.77.187
REMOTE_ADDR	104.16.77.187
Connection	keep-alive, Keep-Alive
Host	www.fbi.gov
Origin	https://www.fbi.gov
Referer	https://www.fbi.gov
X-Forwarded-Host	www.fbi.gov
X-Forwarded-Proto	https
X-XSS-Protection	1; mode=block
Keep-Alive	timeout=5, max=100
Transfer-Encoding	chunked
Content-Type	text/html; charset=UTF-8

Figure 15 - HTTP response headers on pivoted Okta phishing server.

The use of fbi.gov in the HTTP headers appears to be a deliberate act consistent with ShinyHunters history of mocking FBI agents in Telegram channels and underground forums.

One of the pivoted IP addresses, 196.251.83[.]162, was identified hosting the phishing domain BLESS-INVITE[.]COM. According to WHOIS records, the domain was created on 5 April 2025 and last updated on 4 July 2025, aligning with the likely operationalization of the infrastructure. The domain was registered through Tucows with privacy protection services provided by Njalla, a registrar frequently leveraged by threat actors to conceal ownership and hosting details.

Stolen BrowserStack User Access Keys Provide ShinyHunters a Pathway into CI/CD Pipelines and Supply Chain Attacks

EclecticIQ analysts assess with high confidence that ShinyHunters obtained BrowserStack API keys created by engineering teams and used them to target enterprise development environments. BrowserStack is a cloud-based testing platform that integrates into CI/CD pipelines, making it a high-value target for attackers seeking access to source code, build processes, and deployment workflows [17].

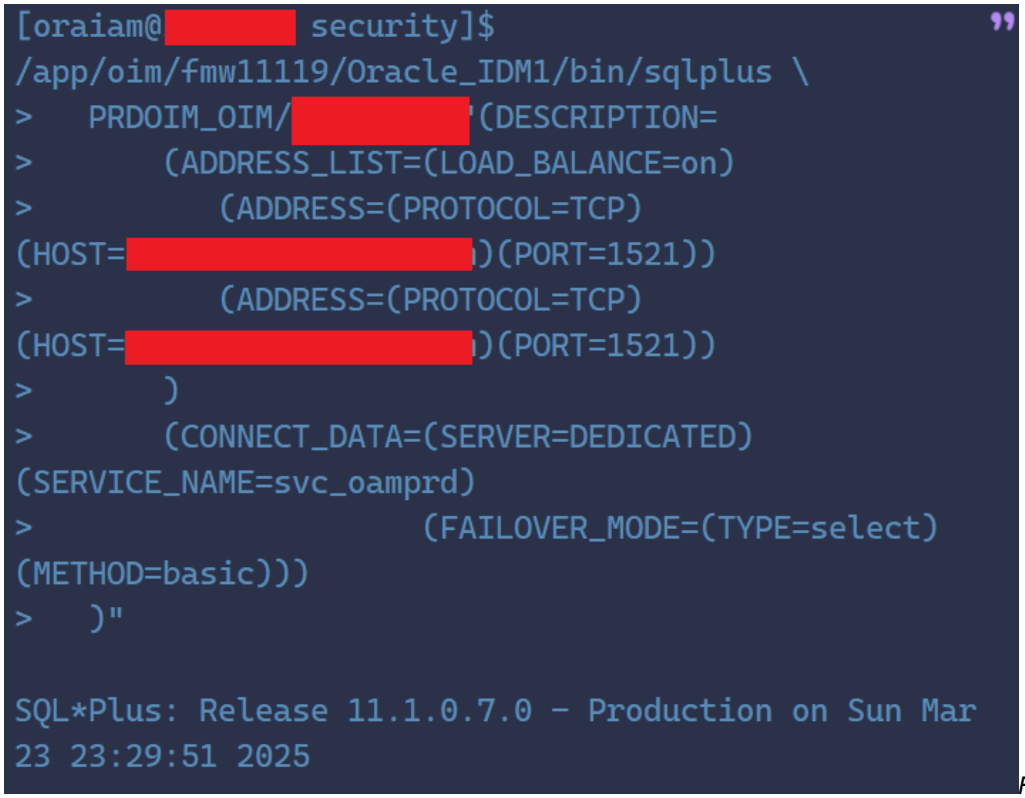


Figure 16 – Telegram post showing leaked API access keys linked to BrowserStack.

This assessment is based on activity observed in a short-lived Telegram channel named ‘Scattered Lapsus$ Hunters,’ operated by ShinyHunters and active from August 8, 2025. In this channel, ShinyHunters targeted a French cosmetics company by leaking multiple API keys, including:

- Valid BrowserStack access keys tied to enterprise domains, indicating access to testing credentials.
- API keys with no expiration dates, likely created by engineering teams for testing purposes.
- API Keys referencing Cloudflare Access domains and internal Azure-hosted applications, which differ in format from BrowserStack credentials and are likely associated with other internal development or authentication systems.

The origin of additional non-BrowserStack keys remains unclear. The mixed credential formats suggest that ShinyHunters obtained access from multiple sources, with some keys from testing environments and others from enterprise authentication systems.

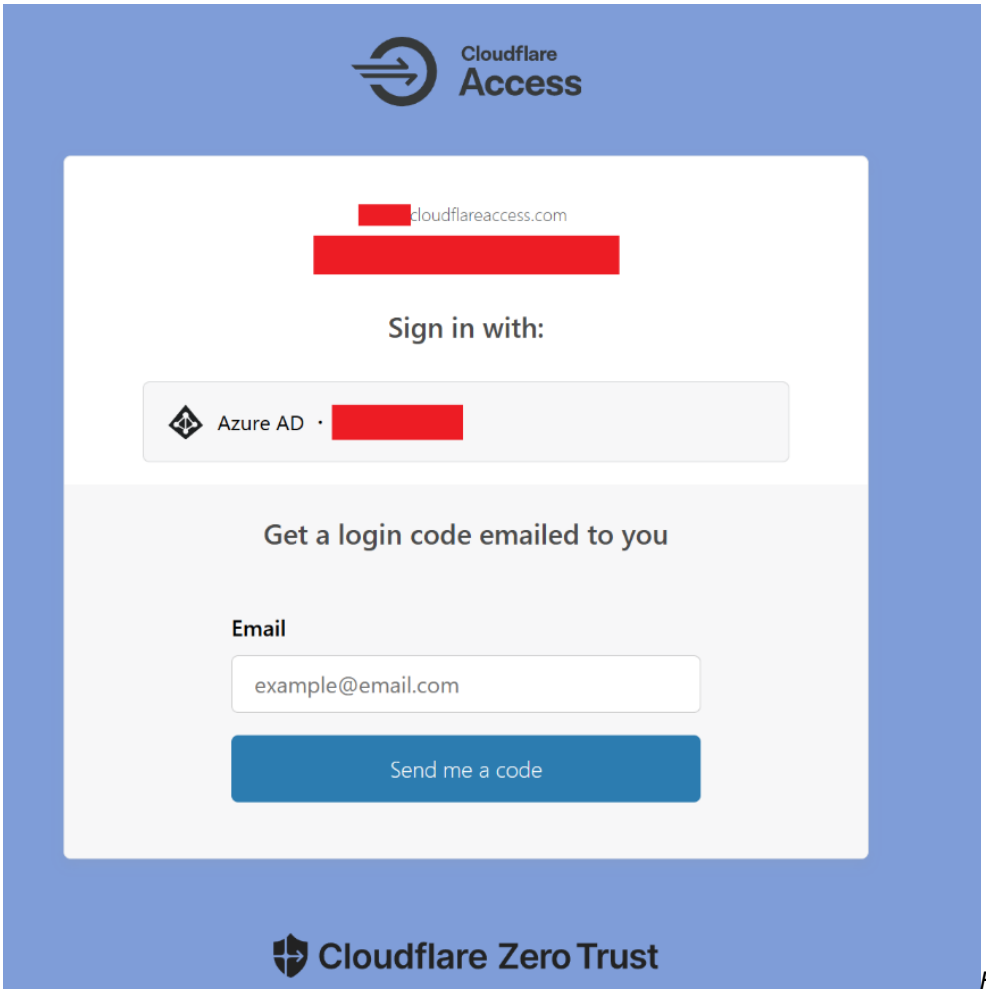


Figure 17 - Cloudflare Zero Trust panel linked to the stolen API keys.

EclecticIQ analysts assess with medium confidence that ShinyHunters likely targeted Cloudflare Zero Trust resources owned by the same company. This assessment was made by analyzing the leaked API keys that contained domain references tied to Cloudflare Access, indicating attempts to expand beyond testing environments into enterprise infrastructure.

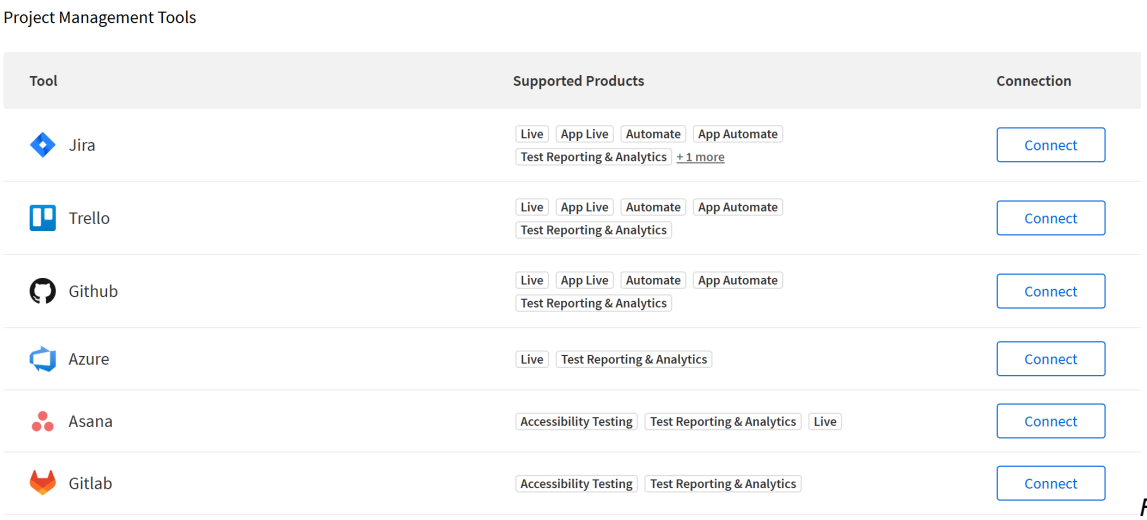


Figure 18 - BrowserStack integrations with project management tools and cloud applications.

BrowserStack's integration with CI/CD pipelines and collaboration platforms such as Jira, GitHub, Slack, and Azure DevOps amplifies the potential impact of API access theft. Even a single stolen key can extend attacker visibility from

testing environments into broader engineering workflows, creating opportunities for supply chain compromise and enterprise-wide data breaches.

Oracle Access Manager Exploitation Enables ShinyHunters to Steal Sensitive Customer Records

According to data obtained from a public Telegram channel operated by the ShinyHunters team, the threat actor persona 'Yukari' exploited an Oracle Access Manager vulnerability (CVE-2021-35587). The attack targeted a national bank and a Japanese car manufacturer. EclecticIQ analysts confirmed this breach by analyzing the targeted domains and promptly informed the victim organizations, preventing further compromise.

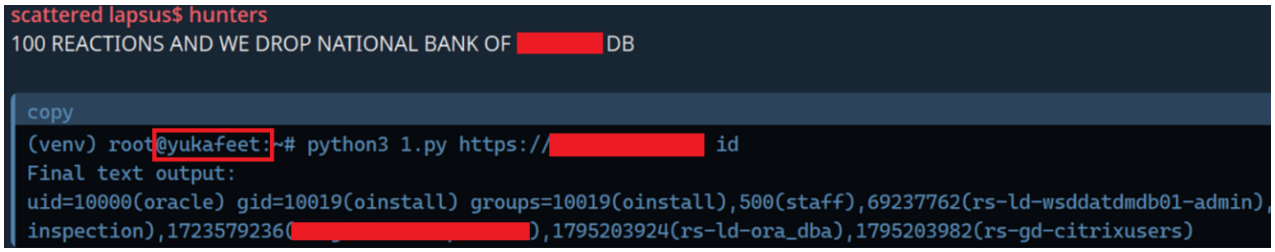


Figure 19 - Console output from Yukari, that was posted on a Telegram channel operated by ShinyHunters.

EclecticIQ analysts assess with high confidence that following exploitation, the threat actor gained access to the Oracle 12c (12.2.0.1.0) production database. The actor abused a weak, hard-coded credential stored on the application server. Once authenticated, the actor used SQL*Plus to run queries and exfiltrate customer data.

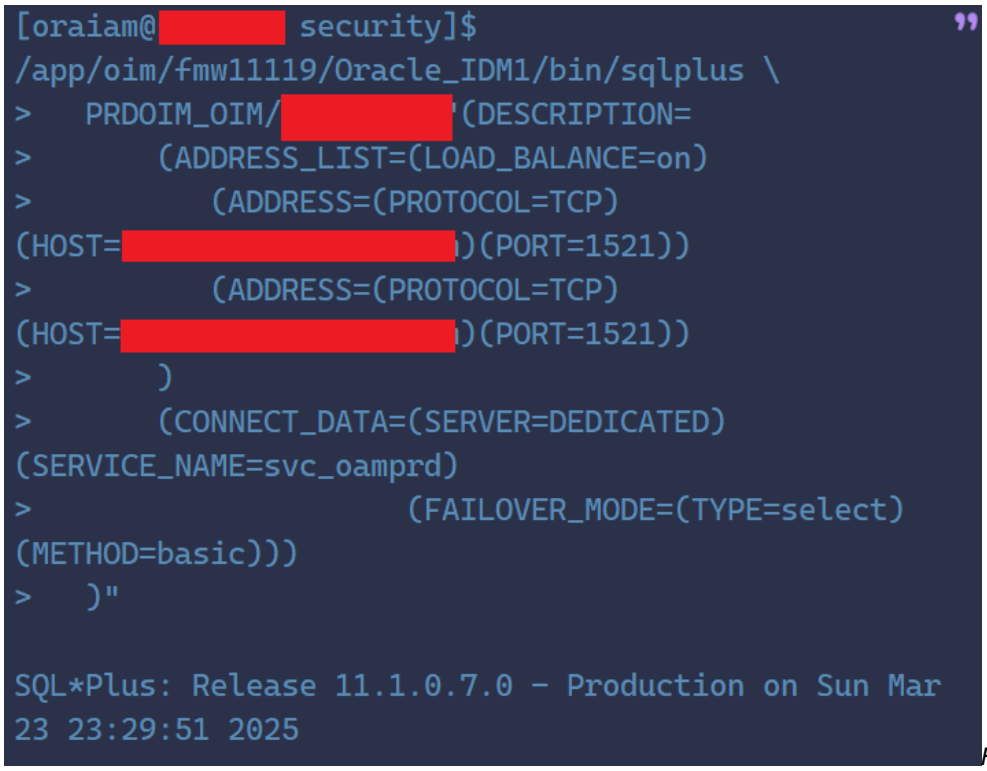


Figure 20 - Execution of SQL command to dump customer data inside Oracle Access Manager.

After this console output publication, the threat actor also shared screenshots of the compromised Oracle Access Manager dashboard which increases the confidence of this assessment.

EclecticIQ analysts assess with high confidence that other members of Scattered Spider including the personas Sevy (aka Sevyuwu, Famous, FC, SV, or Sev) and Rey, collaborated with the ShinyHunters team to perform similar exploitations to breach companies in retail, telecom, manufacturing, and airline sectors.

Recruiting Insiders for Unauthorized Access on Edge Network Devices and Cloud Applications

On August 31, 2025, the Telegram channel “scattered LAPSUS$ hunters 4.0,” operated by ShinyHunters, posted a recruitment message. The group recruited insiders at enterprise organizations who could provide access to Okta, Microsoft SSO, Citrix VPN, or Git version control solutions Github, Gitlab. This demand for cloud applications aligns with observed phishing campaigns attributed to the ShinyHunters team.

ShinyCorp offered financial rewards to employees in finance, insurance, aviation, telecoms, automotive, retail, hospitality, energy, and investment companies in exchange for providing network access.

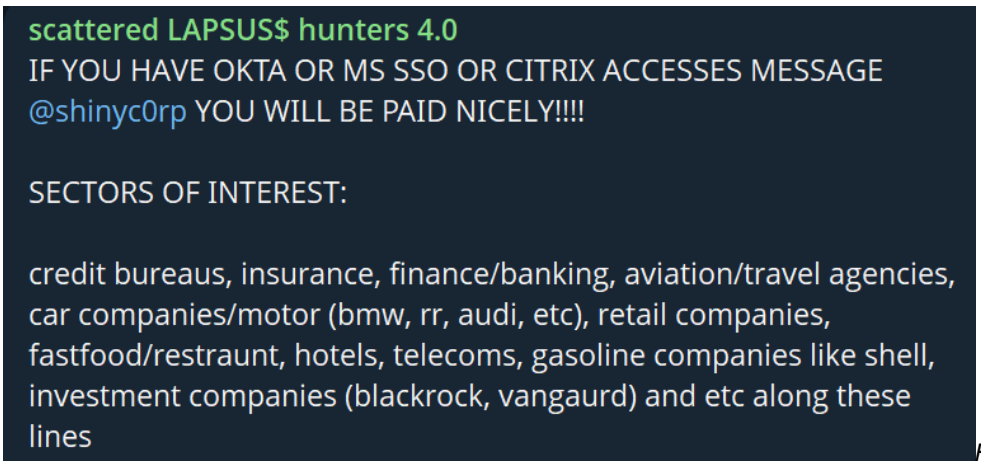


Figure 21 - ShinyCorp looking for insider access to enterprise networks.

This call for insider cooperation highlights ShinyHunters motivation and reliance on trusted employees to bypass enterprise defenses. Insider access to SSO or VPN platforms would enable lateral movement, data theft, ransomware deployment, and service disruptions in critical sectors.

This tactic shows the increasing danger of insider threats. EclecticIQ analysts recommend that organizations should add insider threat scenarios to their threat modelling, deploy honeypots to detect suspicious insider activities, enforce strict access controls, and limit employee access to sensitive data on a need-to-know basis.

Lessons Learned from ShinyHunters Data Extortion Attacks

EclecticIQ analysts assess with high confidence that ShinyHunters team collaborated with other eCrime actors, such as Scattered Spider and RaaS members in DragonForce, to increase the success rate of their attacks.

ShinyHunters team preferred to target high privilege user accounts in cloud applications, cloud hosted project management and engineering collaboration platforms to breach enterprise networks and the software supply chain.

EclecticIQ analysts observed that social engineering-led identity compromise attacks successfully bypassed prevention of enterprise security controls, providing real-world proof of a significant and critical blind spot in enterprise defenses.

Social engineering techniques like voice call phishing were very likely adopted from Scattered Spider actors working with ShinyHunters. Analysts observed that ShinyHunters focused on exfiltrating large amounts of customer data from victim organizations and threatening to leak the data if the extortion money was not paid. Since customer data leaks result in direct financial loss, threat actors use this as a pressure tactic against victim organizations.

EclecticIQ assesses with moderate confidence that ShinyHunters cloud centric tradecraft is likely to be replicated by other threat actors, including ransomware groups, in future operations. This assessment is supported by observed

ransomware affiliates discussing and evaluating ShinyHunters recent successes in underground forums and Telegram channels, indicating intent to integrate similar techniques into their own campaigns.

Detection and Prevention Opportunities

EclecticIQ analysts assess that threat actors increasingly target enterprise cloud applications to exfiltrate customer related data and conduct data extortion. Organizations must enforce strict access controls and monitoring to reduce risk. Analysts recommend the below security policy hardening list to protect organisations against ShinyHunters attack patterns observed in this threat research.

Apply Least Privilege for Data Access Tools

- Restrict “API Enabled” and mass export permissions (e.g., Data Loader) to essential roles only.
- Audit SSO-integrated applications for excessive privileges.

Harden SSO-Enabled Cloud Applications

- Limit high-privilege accounts on platforms like Salesforce, Okta, and Microsoft 365.
- Enforce Just-In-Time (JIT) access for sensitive operations.
- Monitor authentication logs for anomalous SSO usage.

Control Connected and Third-Party Applications

- Allowlist only vetted cloud and connected apps.
- Restrict permissions like “Manage Connected Apps” to trusted admins.
- Regularly review and revoke unused integrations.

Enforce IP and Network-Based Restrictions

- Define trusted IP ranges for both user profiles and connected apps.
- Block or challenge access from unknown networks, especially commercial VPNs.

Strengthen Monitoring and Detection

- Use Salesforce Shield, Okta ThreatInsight, and Microsoft security logs for anomaly detection.
- Set transaction security policies to flag or block large data exports.

Mandate Strong Authentication

- Enforce MFA universally across all SSO-enabled apps.
- Educate users on MFA fatigue and social engineering risks.
- Enforce FIDO 2 security keys for users who are managing sensitive data.

Employee Training & Vishing Awareness

- Run phishing simulations that include voice based social engineering scenarios.
- Train staff to verify unexpected IT support calls by initiating a callback using internal directories.
- Implement internal verification challenges for high-risk requests such as MFA resets or credential changes. Instead of actioning the request directly, require the caller to provide a predefined code phrase or, for added assurance, escalate to a video call where the employee must visually confirm their identity (e.g., by showing a corporate badge).
- Educate employees on common vishing pretexts: urgent consequences, fake system errors, or unexpected MFA prompts.

Security Monitoring & Alerting

- Use SIEM and SOAR tools to monitor sign-ins and service desk activity.

- Configure alerts for:
  - Password resets on privileged accounts or outside normal patterns.
  - New MFA enrolments or modifications.
  - Multiple failed logins followed by a successful reset.
  - MFA fatigue activity.
- Ensure all abnormal events are reviewed by security teams in coordination with affected employees and managers.

MITRE ATT&CK TTPs

- Phishing: Spearphishing Link (T1566.002)
- Valid Accounts (T1078)
- Exploit Public-Facing Application (T1190)
- External Remote Services (T1133)

- User Execution: Malicious Link (T1204.001)
- Command and Scripting Interpreter: Unix Shell (T1059.004)

- Exploitation for Privilege Escalation (T1068)

- Acquire Infrastructure: Web Services (T1583.006)
- Acquire Infrastructure: Virtual Private Server (T1583.003)

- Brute Force (T1110)

- Software Discovery (T1518)
- Cloud Service Discovery (T1526)

- Exploitation of Remote Services (T1210)

- Data from Information Repositories (T1213)
- Automated Collection (T1119)
- Data Staged: Remote Data Staging (T1074.002)

- Application Layer Protocol: Web Protocols (T1071.001)
- Web Service (T1102)
- Proxy (T1090)

- Exfiltration to Cloud Storage (T1567.002)
- Exfiltration Over C2 Channel (T1041)
- Data Encrypted for Impact (T1486)
- Data Manipulation (T1565)
- Create Account: Cloud Account (T1136.003)
- Modify Cloud Compute Infrastructure: Modify Cloud Compute Configurations (T1578.005)
- Multi-Factor Authentication Interception (T1111)
- Steal Application Access Token (T1528)
- Steal Web Session Cookie (T1539)
- Credentials from Password Stores: Cloud Secrets Management Stores (T1555.006)
- OS Credential Dumping: NTDS (T1003.003)
- Supply Chain Compromise (T1195)

Indicators of Compromise (IOC)

Phishing infrastructure assessed with high confidence as very likely linked to ShinyHunters:

191[.]96[.]207[.]179
196[.]251[.]83[.]162
163[.]5[.]210[.]210
94[.]156[.]167[.]237
23[.]94[.]126[.]63
198[.]244[.]224[.]200
admiring-shockley[.]196-251-83-162[.]plesk[.]page
bless-invite[.]com
get-carrot-zoom[.]com
modernatx-zoom[.]com
recurly-zoom[.]com

Evilginx Phishing infrastructure assessed with high confidence as very likely linked to Scattered Spider, this assessment is done by infrastructure similarities on previously attributed domains by Silent Push :

sharepoint-comcast[.]com
workday-nike[.]com
workday-hubspot[.]com
sharepoint-workplaceview[.]com
newscorp-okta[.]com
corporate-microsoft[.]com
okta-louisvuitton[.]com
corporate-okta[.]com
pure-okta[.]com
morningstar-okta[.]com
sts-vodafone[.]com
corp-hubspot[.]com
signin-okta[.]com
bmcorpuser.internal-okta[.]com
help-allvuesystems[.]com
allvuesystems-okta[.]com
163[.]5[.]169[.]142

Sha-256 Hash of Okta phishing theme:

0383c0d109b7cfdef058b0197125c85d276510724be33a746056f9a7c181d761
e5c5617c8676e9a5cf6108d344fe7fcb6590671efd6baccb02b9313da0f0d289
36de93aaf26727f6dd55ff2100b08dfb52abccfb57a7bf4d07a7fb703a86623d
6aa51de51a6b352fd073b5b9080011d358d42fa190a8a9ee216e3ef6e657b801
4e20f2c4c90e3654a8c43fb10003978d61d2b48426414dede3b1bd5a2c891b54

qTox ID owned by ShinyCorp:

BD1B683FD3E6CB094341317A4C09923B7AE3E7903A6CDB90E5631EC7DC1452636FF35D9F5AF2

Cryptocurrency Address owned by ShinyCorp:

- **Bitcoin Address:** bc1q5530apqz86eywm2f84mpcyuux3dv9mmztsdxt2
- **XMR Address:** 87cEqA6PunENHwe5h8XtRifWuDhNQXKwzGNSbwKmrdEehY4wjRjWvZmSgE8LHTe6e5Pmnuyyiu5AWbGCC9gHUzUj5

References

[1] M. K. Vaya Chandni, “Bling Libra’s Tactical Evolution: The Threat Actor Group Behind ShinyHunters Ransomware,” Unit 42. Accessed: Aug. 31, 2025. [Online]. Available: https://unit42.paloaltonetworks.com/shinyhunters-ransomware-extortion/

[2] “Defending Against UNC3944: Cybercrime Hardening Guidance from the Frontlines,” Google Cloud Blog. Accessed: Aug. 31, 2025. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/unc3944-proactive-hardening-recommendations

[3] “Internet Crime Complaint Center (IC3) | Hacker Com: Cyber Criminal Subset of The Community (Com) is a Rising Threat to Youth Online.” Accessed: Aug. 31, 2025. [Online]. Available: https://www.ic3.gov/PSA/2025/PSA250723

[4] “Review Of The Attacks Associated with Lapsus$ And Related Threat Groups Report | CISA.” Accessed: Sep. 05, 2025. [Online]. Available: https://www.cisa.gov/resources-tools/resources/review-attacks-associated-lapsus-and-related-threat-groups-report

[5] “The Cost of a Call: From Voice Phishing to Data Extortion,” Google Cloud Blog. Accessed: Sep. 01, 2025. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion

[6] “Telegram: View @angelraasreborn.” Accessed: Sep. 01, 2025. [Online]. Available: https://t.me/angelraasreborn

[7] “Vapi - Build Advanced Voice AI Agents,” Vapi. Accessed: Sep. 01, 2025. [Online]. Available: https://vapi.ai

[8] “Bland AI | Automate Phone Calls with Conversational AI for Enterprises.” Accessed: Sep. 01, 2025. [Online]. Available: https://www.bland.ai

[9] “Conversational Pathways,” Bland AI. Accessed: Sep. 01, 2025. [Online]. Available: https://docs.bland.ai/tutorials/pathways

[10] vx-underground [@vxunderground], “The Simland Telegram channel was banned on Telegram — although a new one has already been created. Following the arrest of Pavel Durov in France, Telegram users are reporting a significant increase in Telegram taking action on crime-related channels.,” Twitter. Accessed: Sep. 01, 2025. [Online]. Available: https://x.com/vxunderground/status/1850975928421167171

[11] D. Ruiz, “How Google, Adidas, and more were breached in a Salesforce scam,” Malwarebytes. Accessed: Sep. 01, 2025. [Online]. Available: https://www.malwarebytes.com/blog/news/2025/08/how-google-adidas-and-more-were-breached-in-a-salesforce-scam

[12] “Salesforce Help | Article,” Salesforce. Accessed: Sep. 01, 2025. [Online]. Available: https://help.salesforce.com/s/articleView?language=en_US&id=service.voice_agents_make_calls.htm&type=5

[13] “Okta Integration Network Catalog.” Accessed: Sep. 01, 2025. [Online]. Available: https://www.okta.com/integrations/

[14] J. Eom, “Louis Vuitton Korea Suffers Cyberattack as Customer Data Leaked,” *Bloomberg.com*, Jul. 04, 2025. Accessed: Sep. 01, 2025. [Online]. Available: https://www.bloomberg.com/news/articles/2025-07-04/louis-vuitton-korea-suffers-cyberattack-as-customer-data-leaked

[15] “ShinyHunters Targets Salesforce Amid Clues of Scattered Spider Collaboration,” ReliaQuest. Accessed: Sep. 01, 2025. [Online]. Available: https://reliaquest.com/blog/threat-spotlight-shinyhunters-data-breach-targets-salesforce-amid-scattered-spider-collaboration/

[16] “VirusTotal - File - 0383c0d109b7cfdef058b0197125c85d276510724be33a746056f9a7c181d761.” Accessed: Sep. 01, 2025. [Online]. Available: https://www.virustotal.com/gui/file/0383c0d109b7cfdef058b0197125c85d276510724be33a746056f9a7c181d761/

[17] “Browserstack Integrations.” [Online]. Available: https://www.browserstack.com/integrations

[18] P. Kelly, “Scattered Spider: Still Hunting for Victims in 2025,” Silent Push. Accessed: Aug. 31, 2025. [Online]. Available: https://www.silentpush.com/blog/scattered-spider-2025/

Talk to one of our experts

Protect your organization with cutting-edge threat intelligence. Book your free demo today and explore how our products and services can help you meet your security needs.

Book a call ✦