What Salesforce Organizations Need to Know About ShinyHunters and Vishing

By Varonis Threat Labs

Published: 2025-07-25 · Archived: 2026-04-02 12:44:50 UTC

In the world of cybersecurity, the most dangerous adversaries aren't always the ones exploiting zero-days or deploying sophisticated malware. Increasingly, they're the ones who simply talk their way in.

The recent wave of Salesforce-related breaches orchestrated by Scattered Spider (UNC3944) and UNC6040, also known as ShinyHunters, is a chilling example of this shift. These groups didn't need to break down the door — they convinced someone to open it for them.

These attacks are designed to steal sensitive data and extort organizations — posing a serious risk to any business that relies on Salesforce as a central hub for customer, sales, and operational data, which is an attractive target for attackers like UNC6040 and UNC3944.

A successful breach could result in data loss, regulatory consequences, reputational damage, and financial extortion. Understanding and defending against vishing threats is critical to safeguarding the integrity of Salesforce environments and maintaining trust with clients, partners, and stakeholders.

Who are ShinyHunters and Scattered Spider?

In today's cybersecurity landscape, the most dangerous adversaries aren't necessarily those exploiting zero-days or deploying advanced malware — they're the ones who talk their way in.

UNC6040 (also known as ShinyHunters) and **UNC3944** (known as Scattered Spider) are two of the most active threat groups targeting cloud platforms like Salesforce. Their campaigns rely heavily on social engineering, particularly vishing, to gain unauthorized access to sensitive customer data.

- Scattered Spider is a young, US/UK-based crew known for breaching organizations in the hospitality, telecommunications, financial services, and retail sectors. Their tactics include SIM swapping, phishing, and MFA bypass. Despite arrests in 2024, copycat operations continue to surface.
- ShinyHunters began as a mass data theft gang and pivoted in 2024 to cloud platform extortion. They've targeted companies across luxury goods, airlines, insurance, and e-commerce, stealing customer data and demanding ransoms. Their recent campaigns have focused on Salesforce environments, often in collaboration with Scattered Spider.

These groups have impacted dozens of organizations globally, compromising millions of customer records. The industries affected include:

- **Luxury retail**: High-end brands saw breaches involving VIP customer data and regional client platforms.
- **Travel & airlines**: Frequent-flyer databases were accessed, exposing contact and travel details.
- **Financial services & insurance**: Cloud-based CRM systems were infiltrated, affecting policyholder data.
- **Consumer goods & apparel**: Customer service platforms were compromised, leaking personal information.
- **Technology & telecom**: Attackers used SIM swaps and phishing to bypass authentication and access internal systems.

How the attack works

Rather than exploiting software vulnerabilities, these attackers manipulated human behavior like impersonating IT support, abusing helpdesk workflows, and leveraging Salesforce's OAuth model to maintain persistent access. Their campaigns demonstrate how trust and routine processes can be weaponized to devastating effect.

These attacks typically begin with a phone call from someone posing as IT support. The attack operators use a combination of live calls and automated phone systems with pre-recorded messages and interactive menus. These systems help them gather reconnaissance, such as internal application names, support team contacts, and company-wide technical issues, before engaging targets directly.

Once on the call, the attacker instructs the victim to install a modified version of Salesforce's Data Loader — a legitimate tool used to import, export, and update Salesforce data in bulk. The malicious version is often disguised under a different name, like "My Ticket Portal."

Victims are guided to Salesforce's connected app setup page and asked to authorize the malicious app. This grants the attacker access to the organization's Salesforce environment, enabling them to exfiltrate large volumes of customer and operational data.

From there, the attackers move laterally across the network, targeting other platforms. The group harvests credentials and sensitive data from these systems, often without triggering security policies and alerts.

Here is a technical breakdown of the attack flow:

- **Device code generation**
  - The attacker (hacker) initiates the OAuth Device Flow using their local Salesforce Data Loader.
  - This generates an 8-character device code that is meant to be entered by a legitimate user.
- **Data Loader waits for authentication**
  - The attacker's Data Loader instance is now listening for a successful authentication tied to that device code, completed by the victim.
- **Social engineering**
  - The attacker tricks an employee (e.g., via phishing, impersonation, or urgent request) into visiting: https://login.salesforce[.]com/setup/connect
  - The victim is then asked to enter the 8-character code, believing it's a legitimate request by a trusted entity.
- **User consent and credential entry**
  - The employee authorizes the request, unknowingly granting access to the attacker's Data Loader.
  - They also enter their Salesforce credentials, completing the OAuth flow.
- **Access token granted**
  - Salesforce issues an access token to the attacker's Data Loader instance.
    This token allows the attacker to act on behalf of the victim, accessing data or performing actions within Salesforce.

In some cases, extortion attempts occur months after the initial breach. During these campaigns, UNC6040 has claimed affiliation with the ShinyHunters group, which is likely to increase pressure on victims and accelerate ransom payments.

Why Salesforce orgs should be concerned

Salesforce environments are increasingly targeted by threat actors like UNC6040 and Scattered Spider due to the rich customer, sales, and operational data they contain. The 2025 campaign has already impacted organizations across a wide range of industries, including:

These breaches didn't stem from vulnerabilities in Salesforce itself. Instead, attackers exploited human trust and workflow gaps — impersonating IT support, abusing helpdesk protocols, and leveraging Salesforce's OAuth model to maintain persistent access.

The consequences have been severe:

- **Millions of customer records** were exposed, including names, contact details, birthdates, and loyalty information.
- **Financial losses** ranged from hundreds of thousands to tens of millions of dollars, including ransom payments, incident response costs, and regulatory fines.
- **Reputational damage** was especially significant for luxury and financial brands entrusted with sensitive client data.

In many cases, the breaches went undetected until attackers sent extortion emails or law enforcement tipped off the victims. This underscores the need for proactive monitoring, user education, and robust identity controls to defend against social engineering and cloud data theft.

Mandiant, a Google-owned threat intelligence firm, emphasized that vishing campaigns like UNC6040's are built on extensive reconnaissance. The normalization of remote IT support and outsourced service desks has made employees more susceptible to engaging with unfamiliar personnel — creating fertile ground for social engineering.

While Salesforce has issued guidance to help customers protect themselves, implementing these controls manually can be time-consuming and error-prone. That's where Varonis comes in.

Salesforce acknowledged UNC6040's campaign in March 2025, warning that attackers were impersonating IT support to trick employees into giving away credentials or approving malicious connected apps. The company emphasized that these incidents did not involve or originate from any vulnerabilities in its platform.

Salesforce also published guidance to help customers protect their environments from social engineering, including best practices for app authorization and user training.

How Varonis helps secure data in Salesforce

Varonis isn't just compatible with Salesforce — it's purpose-built to secure it.

With Varonis for Salesforce, users can automatically eliminate risky misconfigurations, find and remediate exposed sensitive data, and detect anomalous behavior. Our platform bridges the gap between security and Salesforce teams, helping both sides work together to reduce risk.

Varonis also simplifies Salesforce's complex permissions and automatically surfaces users assigned high-risk entitlements with a real-time, interactive view across users, profiles, and permission sets.

When it comes to defending against threats like UNC6040, Salesforce recommends a series of best practices that Varonis automates and simplifies:

How to defend against vishing

When it comes to protecting your data from threat actors like UNC3944 (aka Scattered Spider), organizations should consider the following proactive defenses:

- **Educate employees** about social engineering tactics. Make it clear that IT will never ask them to install or authorize apps over the phone.
- **Implement strict app authorization policies** in platforms like Salesforce and Microsoft 365.
- **Monitor connected apps** and audit for unusual authorizations or access patterns.
- **Use behavioral analytics** to detect lateral movement and data exfiltration.
- **Adopt a Zero Trust model** — never trust, always verify.
- **Harden identity infrastructure** by enforcing phishing-resistant MFA, restricting self-service password resets, and monitoring for suspicious identity activity.
- **Limit access to administrative tools** and enforce just-in-time access provisioning.
- **Simulate vishing attacks** as part of regular security awareness training to test and reinforce employee vigilance.

Immediate recommended actions from Salesforce include:

- Audit and restrict connected app permissions in Salesforce.
- Enforce least privilege access across all systems
- Apply IP-based login controls
- Configure and deploy Salesforce Shield and other monitoring tools for early detection

Detection and hunting strategies

UNC6040 and Scattered Spider are experts at blending in. Their attacks often mimic legitimate user behavior, making early detection difficult. But with the right visibility and controls, security teams can catch subtle signs before damage is done.

Here’s how to stay ahead.

Monitor connected app activity

Salesforce allows users to self-authorize external connected apps by default. Attackers exploit this to install rogue apps that quietly siphon data.

To reduce risk:

- Audit new connected apps regularly. Flag anything authorized by non-admins, especially apps with names like “MyTicketingPortal” or “SalesforceDataLoader123.”
- Restrict app access by setting the OAuth policy to “Admin approved users are pre-authorized.” Then manage access via profiles or permission sets.
- Enforce IP restrictions, limit refresh token validity, and set session timeouts to prevent indefinite access.

Use Salesforce audit logs

Salesforce’s built-in logging, or Shield event monitoring, can surface suspicious behavior:

- OAuth token abuse. Watch for high-volume API calls from users who don’t normally access large datasets.
- Concurrent sessions. If a user is logged in via SSO and also active via API from a different IP, investigate.
- New app authorizations. Treat unexpected app installs as potential compromise.

Watch for authentication anomalies

Attackers often trigger subtle authentication red flags:

- Impossible travel. If a user logs in from New York and then Belarus minutes later, raise an alert.
- Off-hours access. Data pulls at 3 AM from a 9-to-5 user? That’s suspicious.
- MFA fatigue. A flood of push notifications could mean someone is trying to wear down a user into approving access.

Empower employees to report suspicious IT contact

One fake IT call can open the door. Encourage staff to speak up:

- If someone says, “I got a weird call asking me to do something in Salesforce,” treat it like a fire alarm.

- Make it easy to verify IT requests, whether through a callback process or a dedicated reporting channel.

Use threat intelligence

Stay plugged into threat intel feeds from CISA, FBI, and ISACs. Known indicators of compromise, such as attacker VoIP numbers, phishing domains, or extortion email addresses, can help you spot active campaigns in your environment.

Worried about your Salesforce exposure?

UNC6040's campaign is a stark reminder that attackers aren't breaking in — they're logging in. Their use of vishing, legitimate tools, and delayed extortion tactics shows how human error can compromise even the most secure platforms.

To stay ahead, organizations must combine technical controls with user education. The best way to understand your Salesforce data security posture and determine if UNC6040 is a serious threat is with a free Salesforce Data Risk Assessment from Varonis.

Our Salesforce Data Risk Assessments are built to not only summarize your data security risks but also provide actionable recommendations for simpler, safer permission structures. Discover all Varonis for Salesforce has to offer in this quick 4-minute demo.

If you believe your organization has been impacted by UNC6040 or UNC3944, contact our team immediately.
