Threat Spotlight: ShinyHunters Targets Salesforce Amid Clues of Scattered Spider Collaboration

By ReliaQuest Threat Research Team 15 September 2025

Published: 2025-09-15 · Archived: 2026-04-06 00:44:34 UTC

Editor's note: This blog was originally published August 12.

Key Points

After a year of inactivity, “ShinyHunters” has resurfaced with a wave of attacks on Salesforce, targeting high-profile companies across various sectors.

ReliaQuest has identified **a coordinated set of ticket-themed phishing domains and Salesforce credential harvesting pages**, likely created for similar campaigns.

This resurgence has sparked speculation about collaboration between ShinyHunters and “Scattered Spider,” potentially dating back to **July 2024**.

Supporting this theory is evidence such as the appearance of a “BreachForums” user with the alias **“Sp1d3rhunters,”** who was linked to a past ShinyHunters breach, as well as overlapping domain registration patterns.

Domain analysis suggests that **financial services and technology service providers** are likely next targets for these attacks.

To defend against such campaigns, **prioritize mitigating tactics**—such as phishing, vishing, and credential harvesting, as threat actors continue to share tools and infrastructure across campaigns.

The “ShinyHunters” threat group has reportedly launched a new wave of attacks targeting Salesforce, hitting major organizations like Google. What’s particularly intriguing about this campaign is not only its scale and impact, but its resemblance to previous operations attributed to the “Scattered Spider” hacking collective. These similarities raise compelling questions about whether the groups are collaborating or sharing tactics and resources—a connection that could reshape how we view these adversarial groups.

To investigate this potential collaboration and reveal insights into future targeting, ReliaQuest conducted an in-depth analysis of domain registration patterns and infrastructure potentially linked to ShinyHunters over the past two months. By comparing tactics seen in this Salesforce campaign to recent Scattered Spider operations, this report provides actionable intelligence that enables organizations to defend against evolving threats, regardless of attribution.

Read on to learn:

- How ShinyHunters' tactics have shifted to mirror those of Scattered Spider.
- Key findings from ReliaQuest's discovery of ticket-themed and Salesforce-focused phishing infrastructure.
- How to monitor for domain impersonation threats tied to these campaigns.
- Why financial services organizations and technology service providers are likely the next targets of similar operations.

Who's Who: What You Need to Know About the Key Players

Before we dive into the details of our investigation, let's set the stage with a quick overview of the groups involved.

ShinyHunters: The Data Breach Actors

ShinyHunters is a financially motivated threat group that gained notoriety in 2020 through a series of large-scale data breaches and extortion campaigns targeting major global brands (see Figure 1). The group's operations revolve around monetizing stolen data via underground forums. ShinyHunters built a reputation for assertive self-promotion and direct engagement with the cybersecurity community, which was solidified when members acted as administrators of the popular cybercriminal platform "BreachForums." Traditionally, ShinyHunters favored stealthy, persistent attacks focused on **credential theft** and **database exploitation** over more overt tactics like vishing. Aside for an alleged attack on education software PowerSchool in December 2024, ShinyHunters remained largely quiet between June 2024 and June 2025, following the arrests of four of its members.

Figure 1: ShinyHunters first gained notoriety by advertising 91 million Tokopedia user records for sale on "Empire Market" in 2020

Scattered Spider: The Masters of Social Engineering

Scattered Spider is a financially driven cybercriminal group linked to the broader hacking collective "The Community" (aka The Com). Initially known for SIM-swapping operations, the group has advanced to executing

complex **social engineering** schemes. Fluent in English, its members manipulate help-desk systems and impersonate employees to infiltrate organizations. Scattered Spider is also well known for registering impersonating domains (e.g., companyname-okta[.]com) to facilitate phishing attacks. The group primarily targets high-value sectors like retail trade, technology, and finance—as well as companies with the resources to pay hefty ransoms or valuable data that can be used as leverage in negotiations.

The Com: Disparate Sub-Groups, Mixed Motivations

Suspected to include both Scattered Spider and ShinyHunters members, The Com is a sprawling network of disparate sub-groups and cliques that engage in **account takeover activity, SIM-swapping, cryptocurrency theft, swotting,** and **sextortion**. Some sub-groups have even engaged in more extreme activities like "violence for hire" and coercing individuals into self-harm. The Com is likely predominantly made up of technically savvy English-speaking teenagers and young adults, capable of diverse techniques to compromise complex hybrid environments and motivated by making money, humiliating their foes, and causing as much disruption as possible.

Are ShinyHunters and Scattered Spider Joining Forces?

There's plenty of circumstantial evidence indicating a deliberate partnership between ShinyHunters and Scattered Spider.

ShinyHunters Adopts Scattered Spider's Signature Moves

This latest wave of ShinyHunters-attributed attacks reveals a dramatic shift in tactics, moving beyond the group's previous credential theft and database exploitation. These campaigns have included hallmark Scattered Spider techniques:

- Highly targeted vishing campaigns, impersonating IT support staff to trick employees into authorizing access to malicious "connected apps"
- Apps that often masquerade as legitimate tools (in this case, Salesforce), allowing attackers to steal sensitive business data
- Okta-themed phishing pages to trick victims into entering credentials during vishing calls
- VPN obfuscation using Mullvad VPN to perform data exfiltration (here, on victims' Salesforce instances)

These tactics align closely with Scattered Spider's trademark methods and those of the broader collective, The Com, fueling speculation about active collaboration between the groups.

Claims of Collaboration in Interviews and Forum Activity

Recent reports further support the theory of an alliance between these groups. Cybersecurity news outlet DataBreaches revealed that a threat actor on Telegram using the alias "**Sp1d3rhunters**," who reportedly has ties to ShinyHunters, claimed that the two groups "are the same" and "have always been the same."

This Sp1d3rhunters alias, cleverly combining the two groups' names, also appeared on BreachForums under an account created in May 2024. Two months later, the account leaked data connected to the Ticketmaster breach—a data leak previously advertised by ShinyHunters (see Figure 2).

If these connections are legitimate, they suggest that **collaboration or overlap between ShinyHunters and Scattered Spider may have been ongoing for more than a year.**

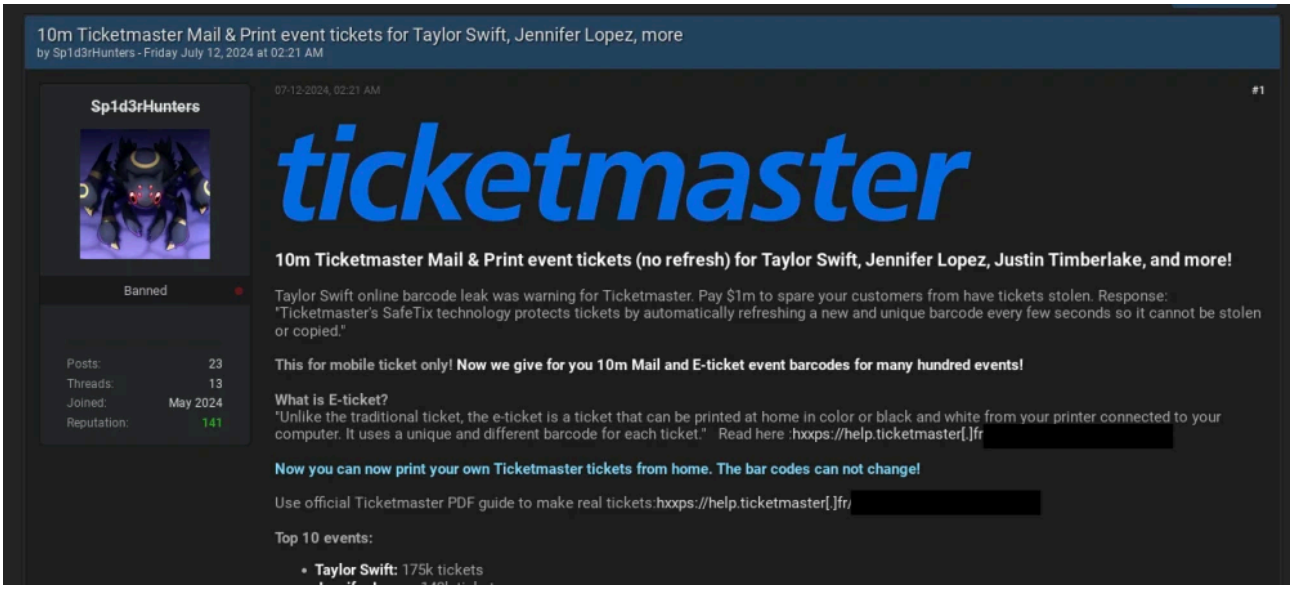

Figure 2: Sp1d3rHunters' first appearance on BreachForums in July 2024

Simultaneous Campaigns Across Sectors

Adding further weight to the collaboration theory, ShinyHunters and Scattered Spider have been targeting the same sectors during overlapping timeframes.

- April–May 2025: Retail trade
- June–July: Insurance
- June–August: Aviation

Previously, ShinyHunters operated sporadically, often focusing on one target at a time. Even though recent campaigns linked to ShinyHunters have targeted organizations across various sectors—including retail trade and aviation—**the synchronized timing and similar targeting of these previous attacks strongly support the likelihood of coordinated efforts between the two groups.**

Domain Registration Patterns Signal ShinyHunters Targeting

As ShinyHunters used Okta phishing pages in these latest campaigns—a tell-tale Scattered Spider move—we investigated malicious infrastructure likely linked to ShinyHunters or similar threat actor activity to uncover further evidence of possible collaboration and indications of the group's next moves.

Infrastructure Connection

Similar Domain Formats

Our previous research revealed that Scattered Spider frequently registered domains with keywords like "okta," "helpdesk," and "sso," often formatted with hyphens (e.g., SSO-company[.]com).

In June 2025, we discovered a small cluster of domains targeting high-profile organizations—including alleged ShinyHunters victims—that followed a very similar format:

- ticket-lvmh[.]com
- ticket-dior[.]com
- ticket-louisvuitton[.]com

All these domains were registered between June 20 and June 30, 2025, just before Louis Vuitton reportedly became aware of a data breach on July 2, 2025. At this time, Louis Vuitton has not confirmed that ShinyHunters was responsible for the attacks. However, some media reports have suggested a possible link between ShinyHunters and the incident.

Common Registry Characteristics

As well as similar formats (e.g., ticket-companyname[.]com), these domains also shared registry details with each other, evidencing their connection:

- Registration through GMO Internet
- Temporary registrant email addresses (e.g., email[at]mailshan[.]com)
- Cloudflare-masked nameservers

These domains were registered using infrastructure associated with phishing kits commonly used to host single sign-on (SSO) login pages—a calling card of Scattered Spider's previous SSO-themed attacks spoofing brands like Okta.

Recurring Domain Themes

In addition to being connected with SSO-linked phishing kits via registrar details, these ticket-themed domains all led to Okta-branded phishing pages (see Figure 3) purporting to provide access to a "Ticket Dashboard." This matches tactics described in other research reports, where attackers rebranded a malicious version of the Salesforce "Data Loader" application under the name "My Ticket Portal" during vishing campaigns. They then used this pretext to convince victims to authorize malicious connected apps and enable large-scale Salesforce data exfiltration.

Given the timing, naming conventions, and domain themes, we assess with medium confidence that these domains contributed to the most recent widespread attacks targeting Salesforce instances.

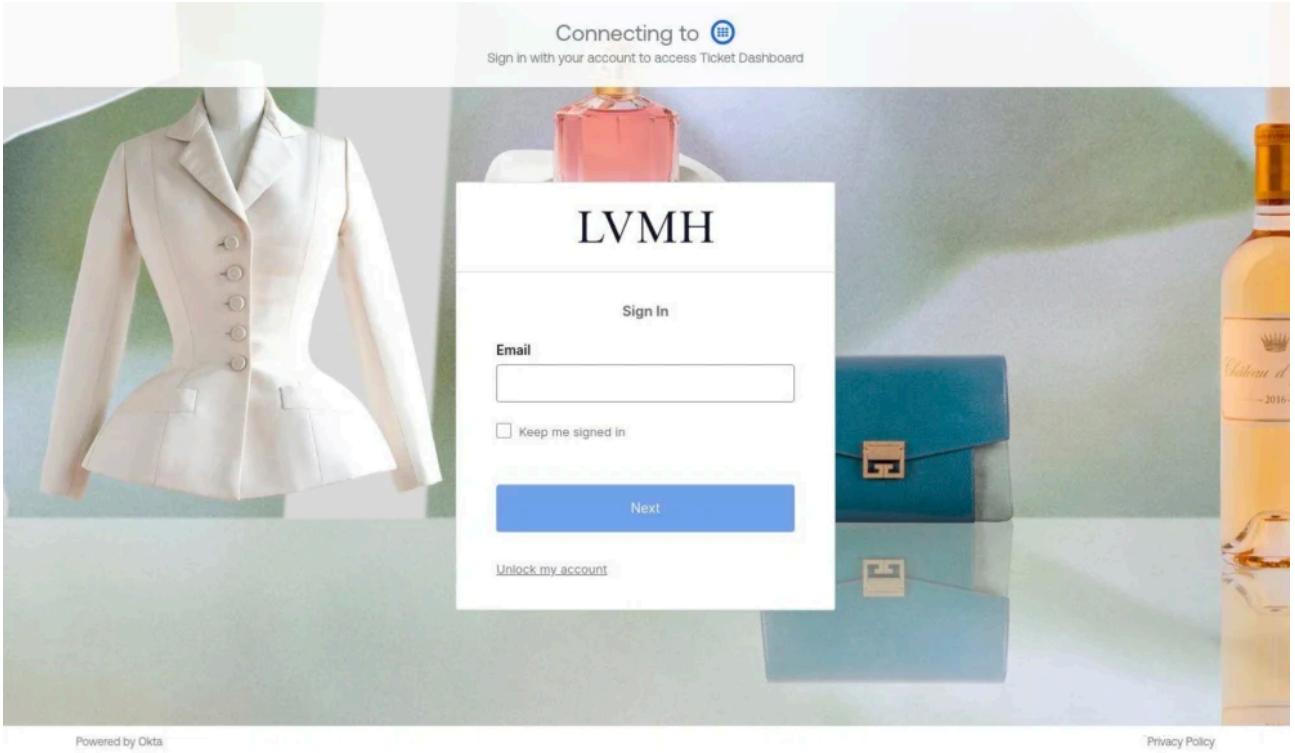

Figure 3: Okta phishing page hosted at ticket-dior[.]com in June 2025

Further investigation revealed other impersonating domains using the same infrastructure and naming conventions, including:

- ticket-nike[.]com—registered on June 26, 2025
- ticket-audemarspiguet[.]com—registered on June 20, 2025 (see Figure 4)

Both domains matched the exact registry information as the previously mentioned ticket-themed domains, suggesting they were part of the same campaign.

These findings highlight the critical need for organizations to track impersonating domain threats, as these can serve as crucial early indicators of attacks by ShinyHunters, Scattered Spider, and similar threat groups.

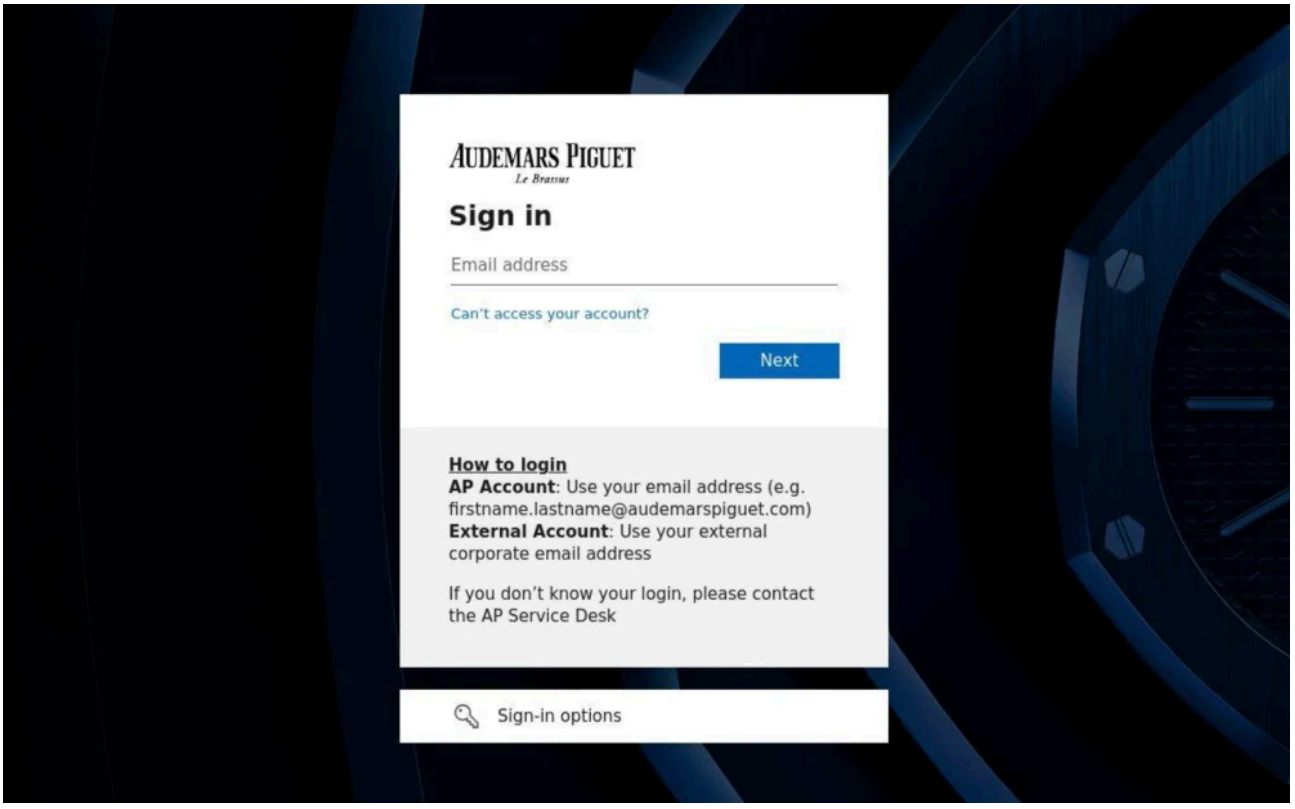

Figure 4: Phishing page hosted at ticket-audemarspiguet[.]com

Domain Registrations Reveal Further Patterns

Newly Registered Salesforce Domains Suggest Ongoing Campaign

The second part of our investigation zeroed in on Salesforce-themed phishing domains, due to ShinyHunters repeatedly targeting this platform.

We uncovered multiple domains registered in 2025 that used the naming conventions "**companyname-my-salesforce[.]com**" and "**keyword-salesforce[.]com**"—patterns consistent with targeted Salesforce phishing campaigns.

Notably, "**dashboard-salesforce[.]com**" was registered on August 1, 2025 and was actively hosting a phishing page at the time of our investigation (see Figure 5).

These domains are significant:

- The structure of the domains matches Scattered Spider's typical domain registration patterns (for example, SSO-company[.]com), which could be linked to ShinyHunters or other threat actors using similar tactics, techniques, and procedures (TTPs).
- It is realistically possible that ShinyHunters registered similar domains as part of their current Salesforce attacks.

- The recency of the domain registration dates indicates that campaigns targeting Salesforce are likely ongoing, so organizations should remain vigilant.

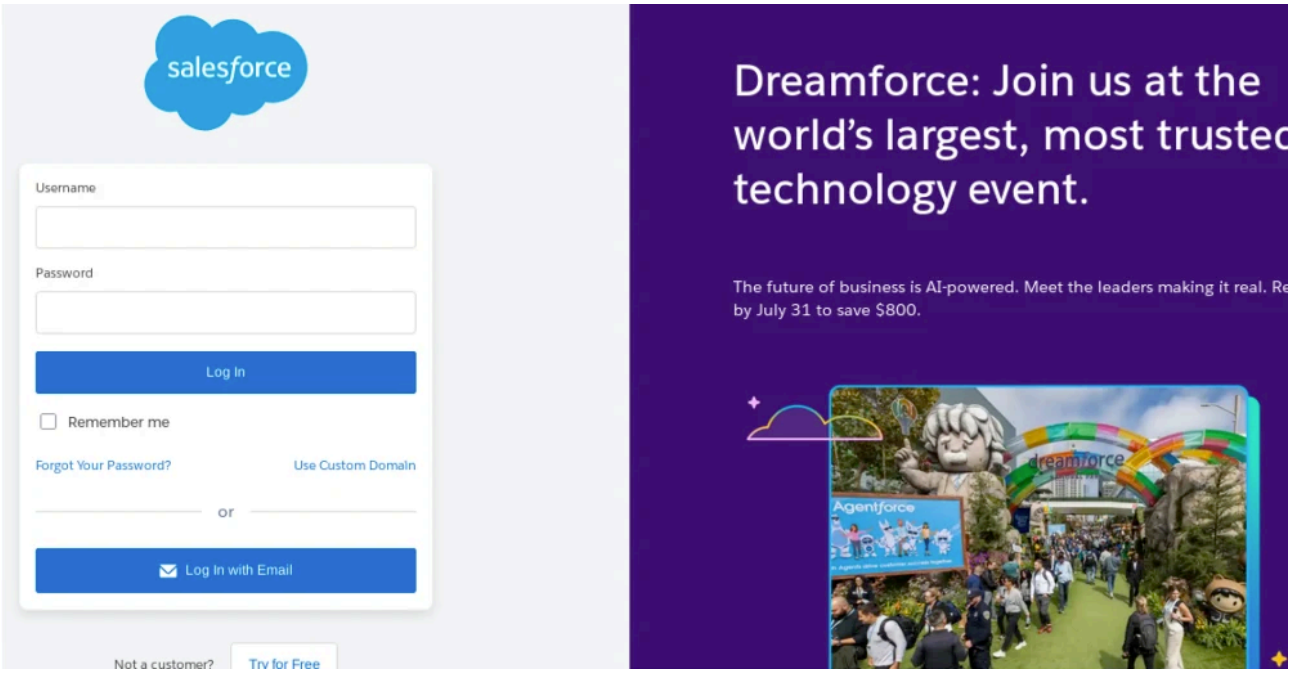

Figure 5: Phishing page hosted at dashboard-salesforce[.]com

Additional Impersonating Domain Findings

In a broader investigation, we identified over **700 domains** registered in 2025 that matched Scattered Spider phishing patterns (e.g., company-okta[.]com).

Targeting Shifts from PSTS to Finance

Early in 2025, **professional, scientific, and technical services** (PSTS) organizations accounted for the largest share of these targets (see Figure 6).

However, since July 2025, domain registrations targeting **financial companies** have increased by 12%, while targeting of technology firms has decreased by 5%.

This shift suggests that financially motivated groups like **ShinyHunters are now prioritizing banks, insurance companies, and financial services**, though technology and professional services remain at high risk due to the value of the data and access they provide.

No Respite for Technology Firms

We also expect cloud and technology providers such as Salesforce and Okta to continue to be targeted, as these platforms are widely used by high-profile organizations and often contain valuable business data.

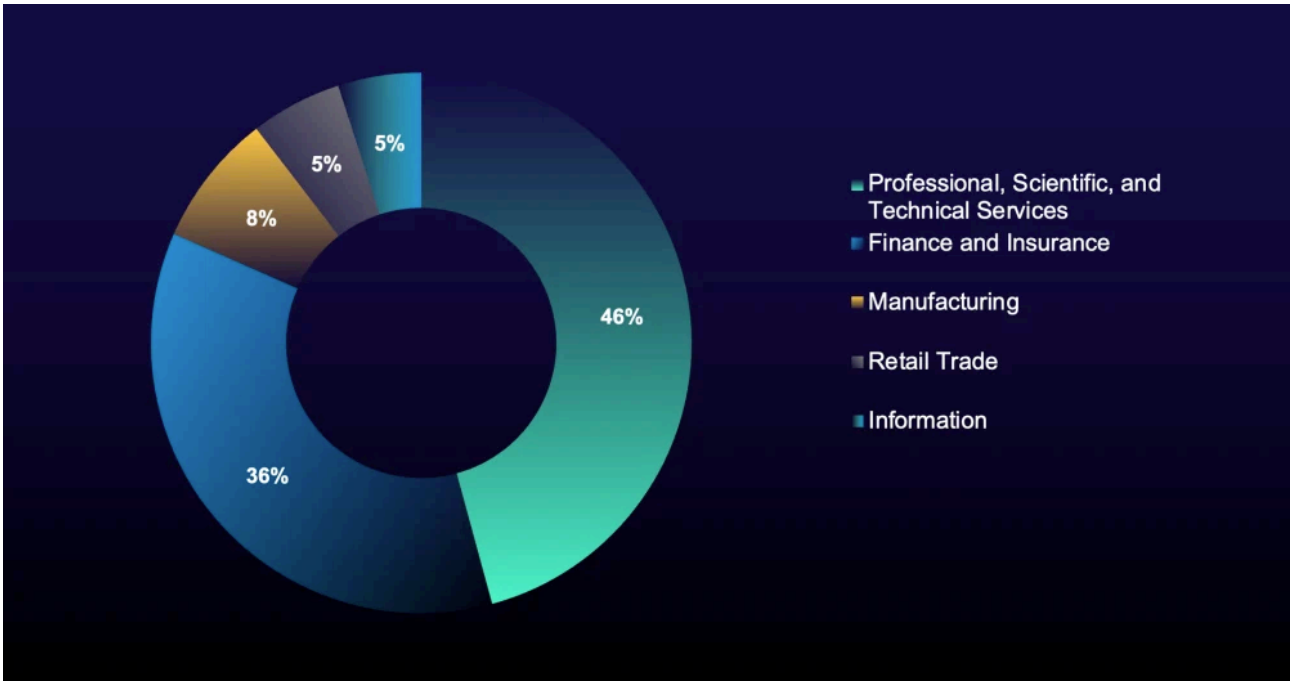

Figure 6: Most targeted sectors in impersonating domains in 2025

US Continues to Top Impersonating Domain Creation Tables

Despite recent reports of attacks by Scattered Spider focusing on organizations in the UK in 2025, the **US continues to be the most targeted country by impersonating domains**, by a wide margin (see Figure 7).

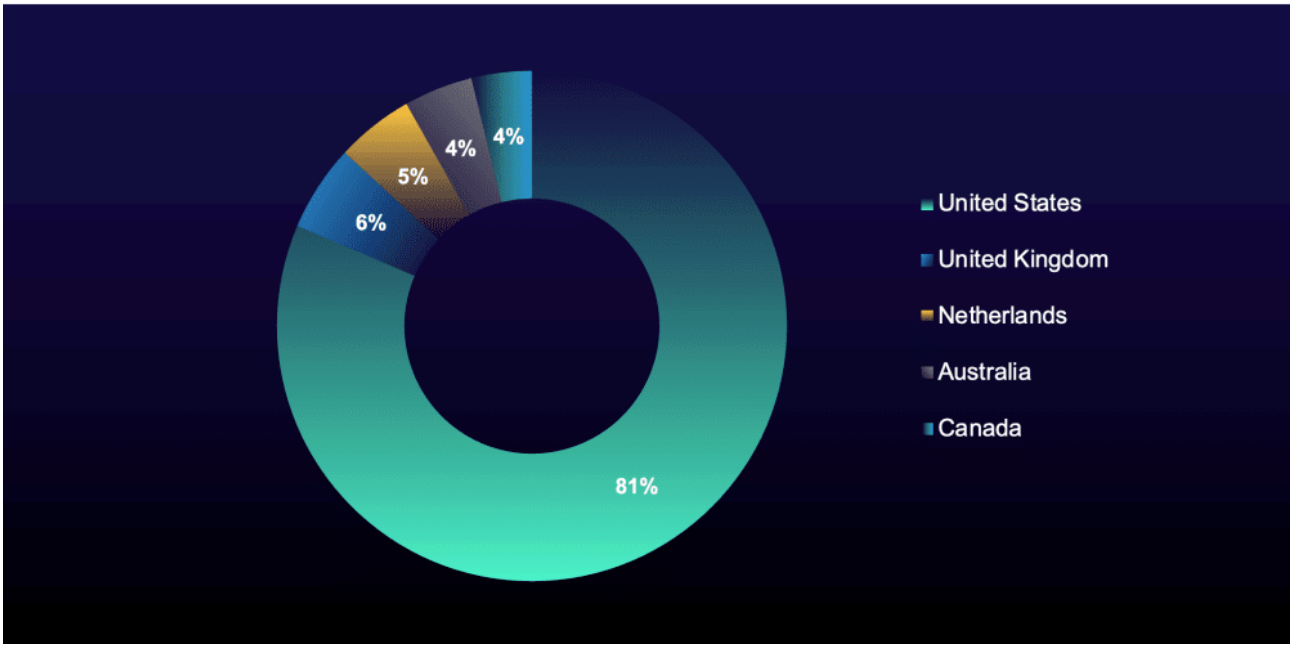

Figure 7: Most targeted countries in impersonating domains in 2025

This number is likely due to the high concentration of technology companies operating in the US, many of which serve as third parties for organizations worldwide and are frequent targets for threat actors.

This is a trend that we observed in cybercrime across multiple different cyber threats, such as ransomware, data extortion, and other cybercriminal activity. For example, in Q2 2025, we discovered that 67% of all organizations named on ransomware leak sites were US companies.

The recent surge in impersonating domain registrations mimicking high-profile brands showcases a persistent and evolving threat to organizations across all sectors and geographies.

The most important takeaway is the clear effectiveness and adaptability of these tactics. Whether targeting luxury brands, financial institutions, or other high-profile organizations, these campaigns illustrate that no sector is immune to the risk of highly targeted social engineering attacks.

Step Up Your Defenses Against TTPs, Not Groups

Security researchers could spend months dissecting the clues indicating that these groups are working together, but enterprises should not lose sight of the broader significance: **These attacks succeed not because of who conducted them, but because of how they're executed.**

Threat actors constantly rotate infrastructure, change names, and adapt their TTPs to evade detection and maximize impact. As a result, tracking the behavioral patterns and evolving TTPs behind these campaigns is far more valuable than focusing solely on indicators of compromise (IOCs) or attribution. For security leaders, understanding this fluid and persistent threat landscape is critical to anticipating future attacks and making informed decisions about security strategy and resource allocation.

ReliaQuest's Approach

ReliaQuest empowers its customers with advanced detection and response capabilities to identify threats related to the TTPs outlined in this report and respond quickly and effectively.

ReliaQuest GreyMatter DRP: Monitoring for impersonating domains is crucial. As these domains are often registered for short-lived campaigns—sometimes becoming inactive within days or even hours—fast detection and response are essential. The GreyMatter Digital Risk Protection (DRP) solution provides early visibility into domain registrations that mimic your brand or key partners. This enables security teams to act quickly, preventing these domains from being used to harvest credentials or launch further attacks.

Detection Rules: ReliaQuest's tailored detection rules, built on the latest threat intelligence and research, help organizations identify suspicious activity resembling Scattered Spider's tactics within their environment:

Organizations can drastically reduce their mean time to contain (MTTC) threats—from hours to just minutes—and minimize the impact of social engineering campaigns by deploying detection rules alongside these corresponding GreyMatter Automated Response Playbooks:

Top of Form

Bottom of Form

- **Terminate Sessions** and **Reset Passwords:** Immediately cut off attacker access to compromised accounts by ending active sessions and forcing credential resets. This is crucial when infostealers or suspicious MFA activity are detected.
- **Initiate Host Scan:** Initiate a comprehensive scan of affected endpoints following a successful MFA attack to identify signs of compromise, malware, or unauthorized changes. This enables rapid containment and remediation.
- **Disable User:** Immediately disable compromised user or service accounts to block attacker movement after successful phishing or MFA bypass attempts.

Your Action Plan

To protect your organization from the latest tactics by ShinyHunters and Scattered Spider, follow these proactive steps:

- **Harden Against Social Engineering:** Implement strong internal processes to verify sensitive requests, particularly those involving access changes or data exports. Conduct regular vishing and phishing simulations for help-desk and privileged users to help them recognize and stop social engineering attempts early.
- **Fortify Salesforce Access and Data Controls:** Restrict powerful permissions like “API Enabled” and “Manage Connected Apps” to trusted administrators only. Enforce IP allowlists for user profiles and connected apps, and deploy automated monitoring (e.g., Salesforce Shield) to detect and block anomalous downloads or suspicious API activity.
- **Build a Resilient Security Culture:** Mandate MFA for all users and regularly train employees to recognize MFA fatigue, phishing, and other SaaS-targeted threats. Foster vigilance through ongoing awareness campaigns and scenario-based tabletop exercises.

To expand detection and identify additional malicious domains, consider the following pivoting strategies:

- **Search for domains using one of the following keywords:** “ticket,” “tickets,” “ticketportal,” “okta,” “sso,” “helpdesk,” or “servicedesk,” **and combine with:**
    - Company names (e.g., **company-ticket[.]com**).
    - SaaS brands like ServiceNow, Microsoft, Google, Okta, Zendesk, or Salesforce (e.g., **company-salesforce[.]com**).
- **Query domain intelligence sources for domains registered with:**
    - GMO Internet, NiceNIC, NameSilo, Hosting Concepts B.V., Prokbun, or PDR Ltd., in the past seven days.
    - PrivacyGuardian, Super Privacy Service LTD c/o Dynadot, Domains By Proxy, Withheld for Privacy ehf, or Whois Privacy Protection Service.

Key Takeaways and What's Next

ShinyHunters' Attack Sophistication Grows

ShinyHunters' recent campaigns highlight the escalating threat posed by collaboration between advanced, English-speaking threat groups.

What's more, the coordinated use of vishing and domain impersonation marks a clear increase in both sophistication and impact for ShinyHunters.

At this time, the group has not made any public announcements regarding its latest activity; however, it's likely that ShinyHunters will begin naming and leaking victims from its recent attacks on cybercriminal forums or a dedicated data-leak site in the coming days or weeks. Targeted organizations should remain highly alert for mentions by ShinyHunters on criminal forums.

Domain Registrations Suggest Finance and Technology at Risk

Looking ahead, our analysis of domain registration patterns and targeting trends suggests that banks, financial services organizations, and technology service providers are at heightened risk.

The prevalence of phishing domains mimicking high-value brands and SaaS platforms indicates that attackers are prioritizing organizations with monetizable data or those providing access to large client environments. While luxury brands and technology firms have borne the brunt of recent attacks, the opportunistic nature of these campaigns means that no sector should consider itself immune.

Focus on Techniques, Not Names

For defenders, the key lesson is that successful security strategies must center on TTPs—not just actor attribution.

Regardless of whether the collaboration between these groups is genuine or the names they use are legitimate, these recent campaigns showcase the effectiveness of a new wave of English-speaking threat actors highly skilled in social engineering. Many threat actors are now emulating the success of Scattered Spider and related groups—registering fake corporate login pages, setting up impersonating domains, and launching sophisticated social engineering attacks. These TTPs pose a significant threat to organizations, as their focus on exploiting the human element increases the likelihood of successful attacks, data loss, and extortion.

As threat groups rotate infrastructure, change aliases, and borrow from each other's playbooks, focusing on behavioral patterns and proactive detection is essential. Organizations should monitor for impersonating domains like those discussed in this report, harden defenses around widely used SaaS applications such as Salesforce, and strengthen the human element through ongoing employee education and simulation.

Ultimately, the collaboration between ShinyHunters and Scattered Spider represents a high and evolving threat. Organizations should take immediate action to strengthen their defenses, as the speed, scale, and adaptability of these campaigns continue to test the limits of traditional security operations.

Source: https://reliaquest.com/blog/threat-spotlight-shinyhunters-data-breach-targets-salesforce-amid-scattered-spider-collaboration/