

Analyzing "Scattered Lapsus\$ Hunters" breaches since 2021

By Dan Green

Published: 2025-11-13 · Archived: 2026-07-28 02:00:39 UTC

The biggest cybersecurity story this year (so far) has been the emergence of “Scattered Lapsus\$ Hunters” and their record-breaking worldwide hacking spree.

Scattered Lapsus\$ Hunters is part of “The Com”, the name for the broad community of English-speaking cybercriminals with international criminal connections — including with nation-state sponsored groups. They are also known to collaborate with a range of cybercrime “as-a-Service” organizations for phishing, initial access, ransomware, and more.

It’s difficult to pin down exactly who the individuals are that make up this criminal collective. But what is known is their MO — making money through extortion by means of account takeover, mass data theft, and ransomware deployment.

How did we get here?

Earlier this year, the threat group known to most analysts as Scattered Spider (also tracked as Oktapus, Octo Tempest, Scatter Swine, Muddled Libra, and UNC3944) re-emerged after a series of arrests in late 2024.

This group has been active in peaks and troughs over the years, but are mainly known for high-profile ransomware attacks on Caesars and MGM Resorts in 2024.

The MGM hack resulted in a 36-hour outage, a \$100M hit to its Q3 results, one-time cyber consulting fees in the region of \$10M, and a class-action lawsuit later settled for \$45M. Less is known about Caesars, except that a ransom of \$15M was paid in an attempt to prevent stolen data being leaked online.

Scattered Spider hit the headlines again in April 2025 with attacks on UK retailers Marks & Spencer and Co-op, which resulted in significant, prolonged disruption, and a serious downstream impact on the retail supply chain.

The Marks & Spencer ransomware breach resulted in online shopping services being taken offline, stores running low on products, £300M in lost profits, and almost £1B wiped off the company’s stock market valuation at one stage. Co-op proactively pulled the plug on their network to prevent further damage, lessening the impact to a still-sizeable £107m in lost profits.

It didn’t stop there, though. What followed was a wide-scale campaign targeting Salesforce customers, with the attackers claiming to have stolen [over 1.5 billion records from 1000+ companies](#) across multiple verticals, including heavyweights like Google, Cloudflare, Workday, Adidas, FedEx, Disney, LVMH, and many more.

Around this time, the attackers began to refer to themselves as part of a wider collective, assuming the moniker “Scattered Lapsus\$ Hunters” (a mash-up of names given by analysts and self-adopted by attackers — Scattered

Spider, ShinyHunters, and Lapsus\$).

The most significant breach this year to-date impacted Jaguar Land Rover. A ransomware attack resulted in months of disruption that directly impacted the UK’s GDP, with the government underwriting a \$1.5B loan to alleviate the supply chain impact. **In fact, this was the most economically consequential cyber attack yet recorded in a G7 economy.**

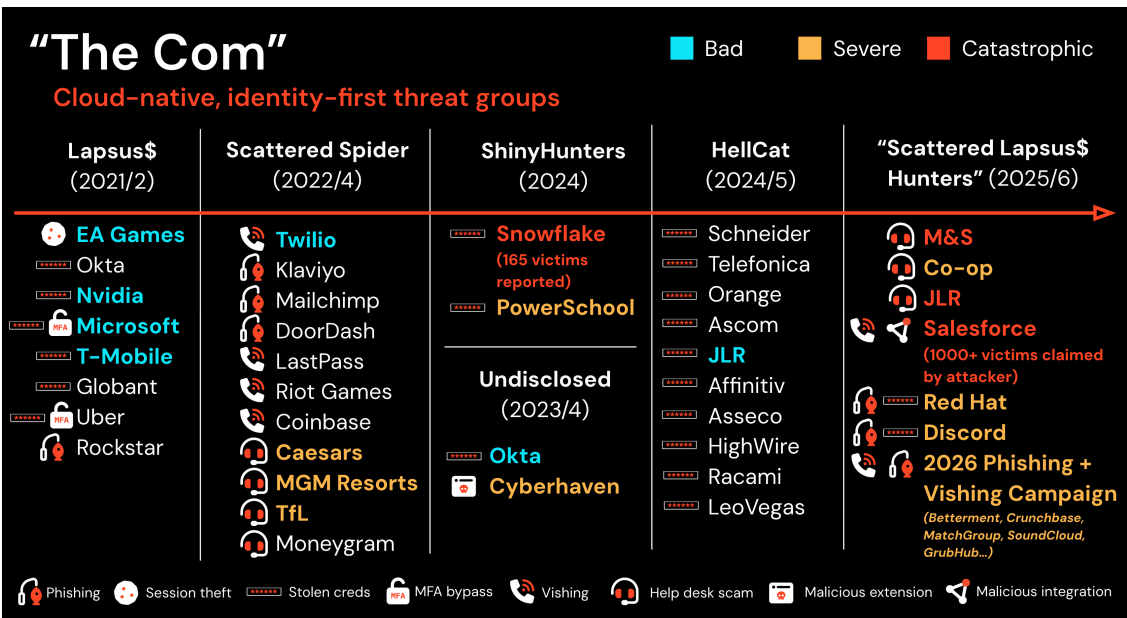
2025 wasn’t a one-off

The developments through 2025 have presented a stronger picture than ever before that cybercriminal operations are heavily interlinked. Groups overlap considerably, and individuals freely move between different cells.

When we scratch beneath the surface, this is evident in the tactics, techniques and procedures (TTPs) used by these attackers — even stretching as far back as 2021 with the initial rise of Lapsus\$. This is not an accident. **The TTPs used show a conscious move by attackers to move away from environments that are well-protected by traditional security tools.** This means avoiding targeting endpoints with malware, and not relying on software-based exploits. Instead, these attackers look to take over apps and services directly over the internet.

Most of the time, this is as simple as logging in to a SaaS app, or an enterprise SSO account (e.g. Microsoft, Okta, or Google) and dumping the data. For attackers that want to take it further, they can abuse the sprawl of interconnected apps that make up modern business IT, seeking out specific data or exploitable functionality. Or, they can leverage internet-accessible management portals to chart a path back to your on-premise assets, giving them everything they need to pivot toward more conventional methods such as ransomware deployment.

When we look at historical breaches, the pattern is clear. **Not one of the attacks attributed to Scattered Lapsus\$ Hunters, or its predecessors, started with an endpoint or network attack — they all began with account takeover.**



Big picture view of Scattered Lapsus\$ Hunters breaches since 2021.

TTP breakdown: Analyzing the top “Scattered Lapsus\$ Hunters” breaches since 2021

Phishing and stolen credentials

Stolen credentials were, and still are, one of the easiest ways in for an attacker. They're one of the most abundant resources available to attackers online, with billions leaked as a by-product of phishing, malware infections (infostealers), and data breaches, which are packaged up and resold to other criminals. Sure, [there's a lot of noise in credential feeds](#) — but it only takes the attacker to get lucky once. And the steady stream of breaches are living proof of the MFA gaps waiting to be exploited.

EA Games (2021)

Attackers used stolen session cookies to log into EA's Slack instance, purchased on a criminal forum. Combined with [social engineering via Slack](#), this was used to steal 750GB of data, including video game source code.

Nvidia (2022)

Attackers used stolen credentials to steal 1TB of data from Nvidia's internal shares, including a significant amount of sensitive information about the designs of Nvidia graphics cards, source code, and the usernames and passwords of more than 71,000 Nvidia employees.

Microsoft (2022)

Attackers used stolen credentials combined with SIM swapping and [MFA fatigue](#) attacks to steal Azure DevOps source code — leaked a 9GB archive of Microsoft source code – including ~90% of Bing and 45% of Cortana code.

T-Mobile (2022)

Attackers used stolen credentials to establish initial access, coupled with social engineering T-Mobile staff into approving the attacker's device for VPN access. This resulted in source code being stolen from over 30,000 repositories.

Snowflake (165 customers) (2024)

Attackers targeted [165 Snowflake customers](#) using stolen credentials from credential breaches dating back as far as 2020. Due to widespread MFA gaps and the presence of [ghost logins](#), attackers were able to simply log in to individual customer tenants, dump the data, and use it to extort the companies. In total, 9 public victims were named following the breach, with over 1B breached customer records.

PowerSchool (2024)

Attackers gained access to a community-focused customer support portal, PowerSource, using compromised credentials and stole data using an "export data manager" customer support tool, stealing the data of 62.4 million students and 9.5 million teachers. PowerSchool paid an undisclosed ransom fee, but hackers returned later to extort schools and individuals separately anyway.

Red Hat (2025)

Attackers breached Red Hat's GitLab instance via a compromised account — the result of [ghost logins](#) providing a backdoor to access an otherwise secure, SSO-connected account. Stolen data included approximately 800 Customer Engagement Reports (CERs), authentication tokens, full database URIs, and other private information in Red Hat code and CERs, which they claimed to use to gain access to downstream customer infrastructure.

A group calling themselves “The Crimson Collective” originally claimed the breach, with Scattered Lapsus\$ Hunters becoming the main voice behind the breach at the extortion phase — showing just how interconnected the ecosystem of cybercriminals is.

Discord (2025)

Attackers compromised a Zendesk customer support account, stealing 1.6TB of data. The hackers say this consisted of roughly 8.4 million tickets affecting 5.5 million unique users, and that about 580,000 users contained payment information.

SoundCloud, MatchGroup, Crunchbase, Betterment... (2026)

Scattered Lapsus\$ Hunters have already claimed several public victims in 2026, with over 60 million breached records. [SoundCloud](#), [Betterment](#), [Crunchbase](#) and [MatchGroup](#) have all reported breaches this month, powered by a brand [new real-time-operated AiTM phishing kit](#) targeting Okta, Entra, and Google SSO accounts. This is a developing situation, with more victims expected to be announced publicly soon.

Vishing and help desk scams

MGM Resorts & Caesars (2023)

MGM Resorts and Caesars were hit with twin breaches in 2023. Attackers socially engineered help desk personnel to take over accounts with Super Administrator privileges within MGM Resorts' Okta tenant, which they then used to register a second, attacker-controlled IdP via [inbound federation](#) — granting comprehensive access that was used to deploy ransomware.

Transport for London (2024)

Attackers socially engineered the Transport for London help desk to gain privileged access to the IT environment, resulting in prolonged disruption to key online services underpinning London's public transport network, theft of 5,000 users bank details, and all 30,000 staff members having to reset their online credentials in person.

Marks & Spencer (2025)

Attackers compromised a Microsoft Entra account belonging to a privileged user via a [help desk scam](#), which enabled them to steal sensitive data from cloud environments, as well as pivot to deploy ransomware via the [VMware admin console](#). This enabled ransomware to be deployed at the hypervisor layer, evading host-based protections like EDR.

An identical attack path was attempted against Co-op, but was detected early enough for the security team to pull the plug on their own network. This significantly reduced the disruption, although customer data was still taken by the attacker.

Jaguar Land Rover (2025)

Attackers compromised highly privileged admin accounts via a help desk scam, which they leveraged to access and deploy ransomware to all aspects of Jaguar's business, from CAD and engineering software, to payments tracking, to customer car delivery, using similar techniques to the Marks & Spencer breach.

[Jaguar's Jira tenant was breached](#) by the "Scattered Lapsus\$ Hunters" affiliated "HellCat" group earlier in 2025, which led to an alleged ~350GB of data being stolen. It is highly likely that this inside information from Jira (a platform storing huge amounts of business process information, architectural diagrams, and even improperly stored credentials and secrets) was leveraged in the later ransomware breach.

Malicious OAuth integrations

Salesforce & Salesloft (1000+ customers) (2025)

A vast campaign against Salesforce customers resulted in the compromise of 1000+ Salesforce tenants (according to the attacker) with more than 1.5 billion records stolen. This campaign can consist of three phases:

- **Phase 1:** The attacker conducted a large-scale phishing campaign against Salesforce customers, calling up users and socially engineering them into connecting a malicious version of the "Data Loader" app into their tenant. This was in fact an attacker-controlled app that enabled data to be mass-exfiltrated via API.
- **Phase 2:** The attacker conducted a supply-chain compromise against customers of Salesloft. Users of Salesloft's "Drift" integration were impacted by attackers stealing access tokens from Salesloft's AWS environment. This integration allowed the attacker to steal data from customers that had deployed Drift to connected environments — namely, Salesforce, and Google Workspace.
- **Phase 3:** The attacker then conducted a separate supply-chain compromise involving Gainsight (allegedly using OAuth tokens stolen in the Salesloft attack) which enabled them to [breach a further 285 Salesforce instances](#) using stolen OAuth tokens from Gainsight's integrations.

The Salesloft breach in fact originated from a developer's GitHub account being phished, which enabled the attacker to pivot into AWS, steal access tokens, and pivot to downstream customer environments.

Malicious browser extensions

CyberHaven (2024)

Hackers phished a CyberHaven extension developer and uploaded a malicious version of the CyberHaven extension to the Chrome Web Store, leading to customer data breaches where installed in user browsers, impacting

CyberHaven's estimated ~400 business customers. This was part of a broader campaign that targeted 35 Chrome extensions, collectively impacting over 2.5 million users.

While the CyberHaven attacks were conducted by an unknown threat group, the MO of the attacker — pursuing financial gain, bypassing traditional defenses — is very much in-line with the Scattered Lapsus\$ Hunters TTPs observed.

The bigger picture

Scattered Lapsus\$ Hunters are dominating the headlines right now, but they aren't the only attackers using these modern techniques and consciously evading established security controls.

Threat reports agree that attackers are steering away from traditional exploit and malware-driven breaches towards identities:

- Identity-based attacks surged 32% in the last year, while 97% of identity attacks are password-based, driven by credential leaks and infostealer malware. ([Microsoft](#))
- 79% of detections were malware-free in the last year, up from 40% in 2019. ([CrowdStrike](#))
- Credential abuse and phishing combined accounted for 38% of breaches, making identity the primary breach vector observed. ([Verizon](#))

And other public breaches from this year alone demonstrate similar TTPs from outside of the Scattered Lapsus\$ Hunters orbit:

- **Nikkei:** Japanese publishing giant Nikkei's Slack messaging platform was compromised using stolen credentials, leaking the names, email addresses, and chat histories for 17,368 individuals registered on Slack.
- **Everttec:** Hackers tried to steal \$130 million from Everttec's Brazilian subsidiary Sinqia S.A. after gaining unauthorized access to its environment on the central bank's real-time payment system (Pix) using stolen credentials.
- **Hy-Vee:** Was hit with a data breach after hackers logged in with stolen credentials, exposing 53GB of sensitive data.
- **Scania:** Automotive giant Scania confirmed it suffered a cybersecurity incident where threat actors used compromised credentials to breach its Financial Services systems and steal insurance claim documents.

Scattered Lapsus\$ Hunters may be grabbing the headlines — but this is a huge movement in a vast and flexible community of attackers. And criminals around the world are learning from their success.

Lessons learned

The common thread with all of these attacks is that they are evading established security controls by targeting applications directly, over the internet, via account takeover.

Clearly, the success of these attacks shows the limitations of multiple control layers. Endpoint and network layer controls have no visibility of this attack surface. Identity-focused controls are being undermined by ghost logins and shadow IT. And the limitations of cloud security controls in their ability to encompass all apps, and detect and stop malicious actions in real-time (that often blend in seamlessly with normal user activity).

One of the common threads from all of these breaches is the risk posed by [help desk attacks](#), but it's easy to over-index here. Naturally, making it possible for help desk operators to reset MFA for all users (including accounts with dangerous privileges) is always going to be targeted — but is fairly easy to address in principle by requiring escalations for high-risk changes. What is more interesting is that the vast majority of the help desk attacks featured in this article involved a single provider that is now no longer contracted by a number of the victims.

How Push can help

Stopping attacks that are designed to evade established controls is in our DNA — it's the reason Push was founded.

The browser is the gateway to the apps and identities that attackers are now targeting, with many attacks taking place inside the user's browser — whether that's entering credentials onto a phishing page, approving a malicious OAuth grant, installing a risky browser extension, or insecurely accessing an app with a weak password and no MFA.

Push's browser-based security platform provides comprehensive detection and response capabilities against attacks like AiTM phishing, credential stuffing, malicious browser extensions, malicious OAuth grants, ClickFix, and session hijacking. You don't need to wait until it all goes wrong either — you can use Push to proactively find and fix vulnerabilities across the apps that your employees use, like ghost logins, SSO coverage gaps, MFA gaps, vulnerable passwords, and more to harden your attack surface.

To learn more about Push, [check out our latest product overview](#) or [book some time with one of our team for a live demo](#).

Source: <https://pushsecurity.com/blog/scattered-lapsus-hunters/>