

# Scattered Spider has a new Telegram channel to list its attacks - DataBreaches.Net

Published: 2025-08-09 · Archived: 2026-04-09 02:22:00 UTC

***Commenters on reading the new Telegram channel call it “schizo,” “complete chaos,” and “insane.” DataBreaches would just call it “overwhelming.”***

A new Telegram channel appeared on Friday afternoon with a name conflating three groups: Shiny Hunters, Scattered Spider, and Lapsus\$. How long it will last before it gets banned remains to be seen, but in less than 24 hours, it has already revealed numerous breaches, proof of claims, and data.

Unlike some leak/sales channels that provide a quick statement about a breach and then leak the data or post a sales link, initial posts on the channel were a mix of partial leaks, posts saying “HMU” (“hit me up”) if people were interested in buying the data, memes, commentary, and threats.

## Samples and Screenshots

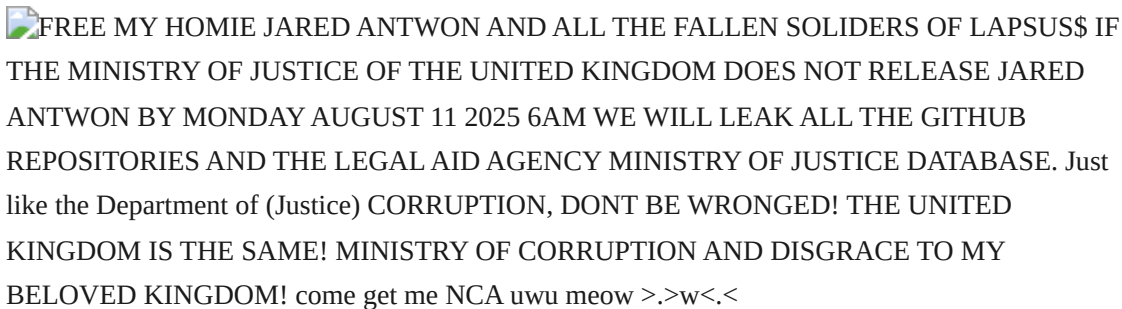
In a matter of hours, the group leaked a number of files, including the court filings related to the Qantas and Legal Aid Agency injunctions sent to ShinyHunters. Other legal documents that they leaked included the cover page of a subpoena served on Google, a request for mutual assistance that France sent to Moldova (and DataBreaches has no idea what that was about), and ShinyHunters’ [replies to the Qantas injunction](#), previously reported on DataBreaches.net.

Many of their posts revealed data about previously disclosed incidents. The following is not a complete list by any means:

- Although the [Victoria’s Secret](#) breach in May had been disclosed, it was not previously definitively linked to Scattered Spider. In yesterday’s posts, Scattered Spider posted a screenshot taken from the retailer’s console, and a note saying the data were up for sale.
- A sample of data from **Gucci** consisted of 100 entries with customer data including name, age range, birthdate (DDMM), email address, mobile phone, and other fields. Gucci is one of **Kering**’s brands, with Yves St. Laurent, Alexander McQueen and other high-end brands. DataBreaches does not recall ever seeing any Gucci data leaked before.
- A screenshot with a listing of .csv files and a note that they were selling a full **Neiman Marcus** database for 1 BTC. This appears to be the [2024 data breach](#) from the Snowflake campaign. There were also other posts that went back to Lapsus\$ attacks and the Snowflake campaign last year.
- A sample from **Chanel** with screenshots of negotiations, and a note that they are selling the data. Chanel only first found out about the breach on July 25 and sources had told both DataBreaches and [Bleeping Computer](#) that the breach was related to the Salesforce campaign.
- Other screenshots or posts included references to “Disney,” [“AirFrance,”](#) archive.org, S&P Global, T-Mobile, Nvidia, [Otelier](#), [Coinbase](#), Burger King Brazil, [Adidas](#), and CISCO. Some of these incidents had

already been linked to ShinyHunters or Scattered Spiders and the Salesforce and Snowflake campaigns. At one point, they leaked **Google**'s notification email to people affected by the attack on Google that Google disclosed on August 5. And before they took a break, they leaked Coca Cola Europacific Partners database.

- Posts with claims or proof of claims about government entities included posts about the governments of England, France, Brazil, and India, as well as posts about hacks involving the Brazilian police and courts and notably, the U.S. Department of Homeland Security. Scattered Spider seemed particularly angry of the 4 recent U.K. arrests and threatened the U.K. Ministry of Justice.

FREE MY HOMIE JARED ANTWON AND ALL THE FALLEN SOLIDERS OF LAPSUS\$ IF THE MINISTRY OF JUSTICE OF THE UNITED KINGDOM DOES NOT RELEASE JARED ANTWON BY MONDAY AUGUST 11 2025 6AM WE WILL LEAK ALL THE GITHUB REPOSITORIES AND THE LEGAL AID AGENCY MINISTRY OF JUSTICE DATABASE. Just like the Department of (Justice) CORRUPTION, DONT BE WRONGED! THE UNITED KINGDOM IS THE SAME! MINISTRY OF CORRUPTION AND DISGRACE TO MY BELOVED KINGDOM! come get me NCA uwu meow >.>w<.<

*Scattered Spider threatens to leak all of the data from the Legal Aid Agency (MOJ) if Jared Antwon is not released. The attached files are the MOJ's legal filings to secure an injunction against ShinyHunters. Image: DataBreaches.net.*

The U.S. Department of Homeland Security (DHS) has also been targeted:

Dhs redacted

*Scattered Spider posted some proof of claims concerning the U.S. Department of Homeland Security. Image and redaction by DataBreaches.net*

Dhs2b

*"@chinahunterz just popped the DHS again." Image and additional redaction: DataBreaches.net.*

In addition to mentioning exploits and source code that they would be willing to sell, Scattered Spider also used the platform to tease the ransomware that they are reportedly developing:

are CISA ready for whats coming 🙄  
n— not ready for the first kernel level esxi locker

DRAGONFORCE AND LOCKBIT IS NOTHING COMPARED TO SHINYSP1D3R UPCOMING  
RAAS!!!!!!!!!!!!!!

## Snowflake 3.0?

In a recent chat with ShinyHunters, Shiny [said](#):

If trillionaires like Google can't stop us then billionaires are nothing. Law enforcement doesn't have such funding or massive budgets either. They will forget about us in a month or two once we're done. Then we'll come back and launch another several months to year long sophisticated campaign, Snowflake 3.0. Next time it's going to be much much worse.

Is Snowflake 3.0 closer on the horizon? Scattered Spider wrote:

Hello, if you work for a Fortune 500 company in retail, insurance, aviation, credit bureaus, finance or banking, travel agencies, car companies or motor related, investment companies, gasoline companies, fastfood/restaurants, hotels, etc

Please contact @UNC5537

[UNC 5537](#) is the tracking number Google used for the Snowflake Campaign, although it has a double meaning in the post as @UNC5537 refers to one of the members of Scattered Spider.

## A Direct Message to Salesforce's CEO

In addition to posts addressing Mandiant, the U.K. Ministry of Justice, and other entities, Scattered Spider directly addressed Salesforce's CEO at one point:

Dear, Mr. Marc Benioff

Please pay us 20 bitcoins or else we will leak the data of exactly 91 organizations, multinational conglomerates, and governments.

Benioff has a net worth of more than \$8 billion according to Bloomberg and Forbes, and 20 BTC would not make a dent in his wealth, but DataBreaches would be very, very, very surprised if he paid them.

## What's Next?

Please do NOT use the Comments section to point out all the listings I did not include in this post. I know this is not a complete listing. And if Telegram doesn't ban the channel, there will be a lot more.

The overall impression the posters created was generally one of kids telling off governments and big businesses, demanding the release of Jared Antwon and others, and generally bragging about their unstoppable.

But there is one impression DataBreaches did come away with apart from thinking that they are angry kids who were somewhat impulsively revealing things last night instead of having and adhering to an organized plan. All that said, they really do come across as unstoppable at this point.

---

Source: <https://databreaches.net/2025/08/09/scattered-spider-has-a-new-telegram-channel-to-list-its-attacks/>