ShinyHunters claims Santander breach, selling data for 30M customers

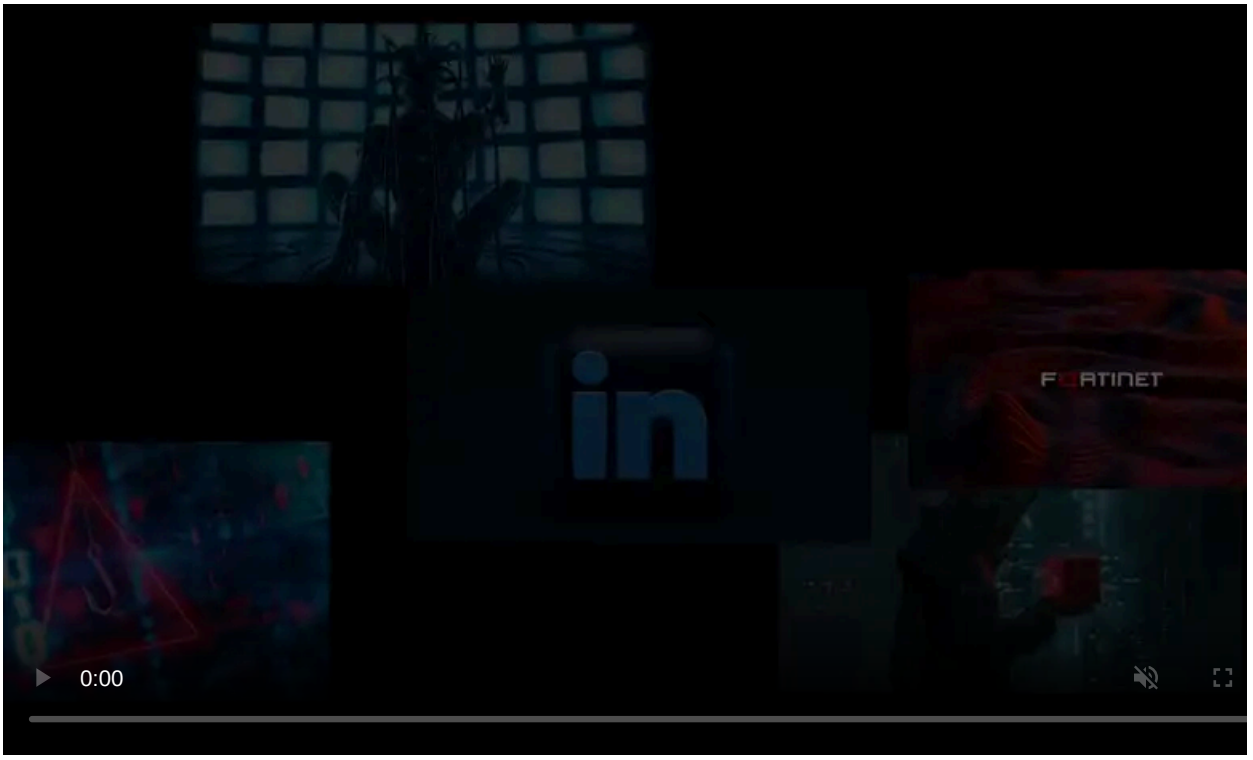
By Lawrence Abrams

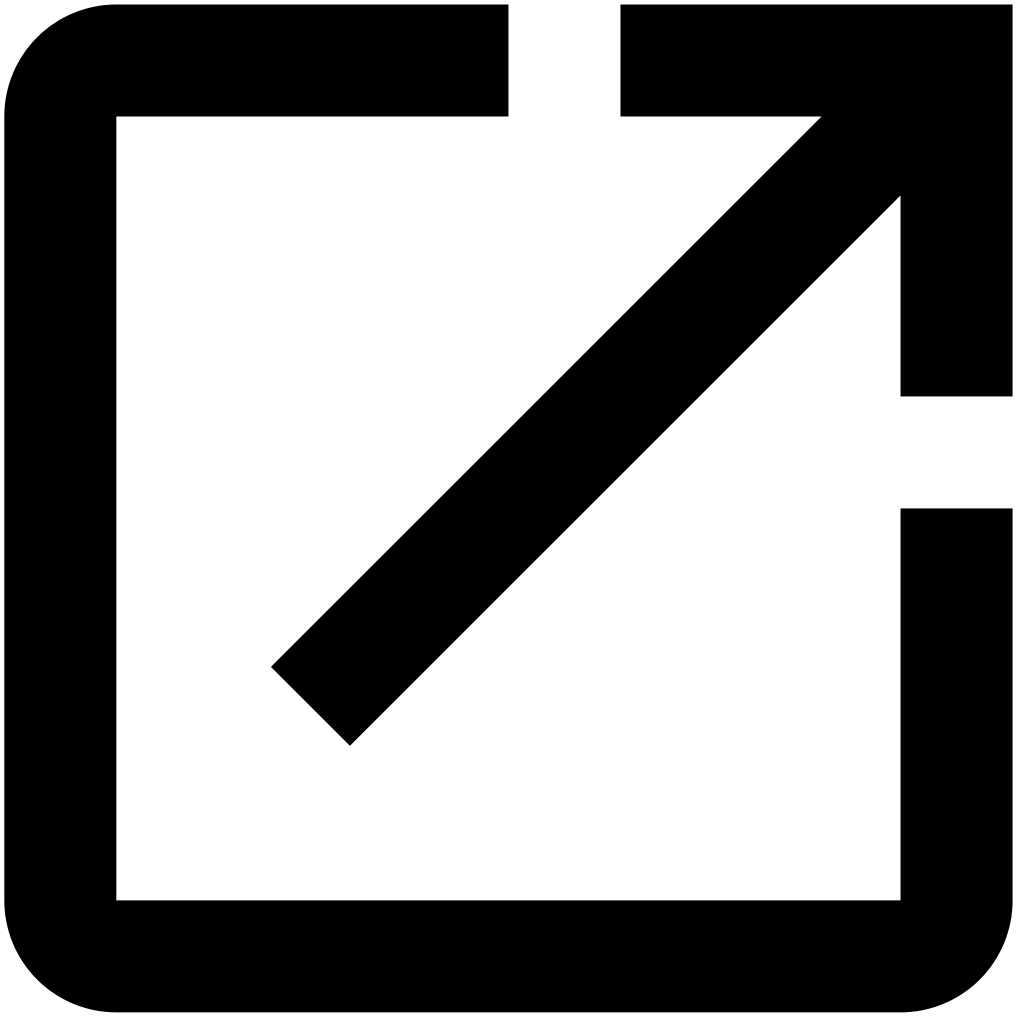
Published: 2024-05-31 · Archived: 2026-04-05 20:25:36 UTC

A threat actor known as ShinyHunters is claiming to be selling a massive trove of Santander Bank data, including information for 30 million customers, employees, and bank account data, two weeks after the bank reported a data breach.

ShinyHunters is known for selling and leaking data from numerous companies over the years, including this week's alleged massive Ticketmaster data breach impacting 560 million people.

They're also the owner of BreachForums, a notorious online community trafficking in the sale and leaking of stolen data which has survived several law enforcement takedowns over the past couple of years


0:00



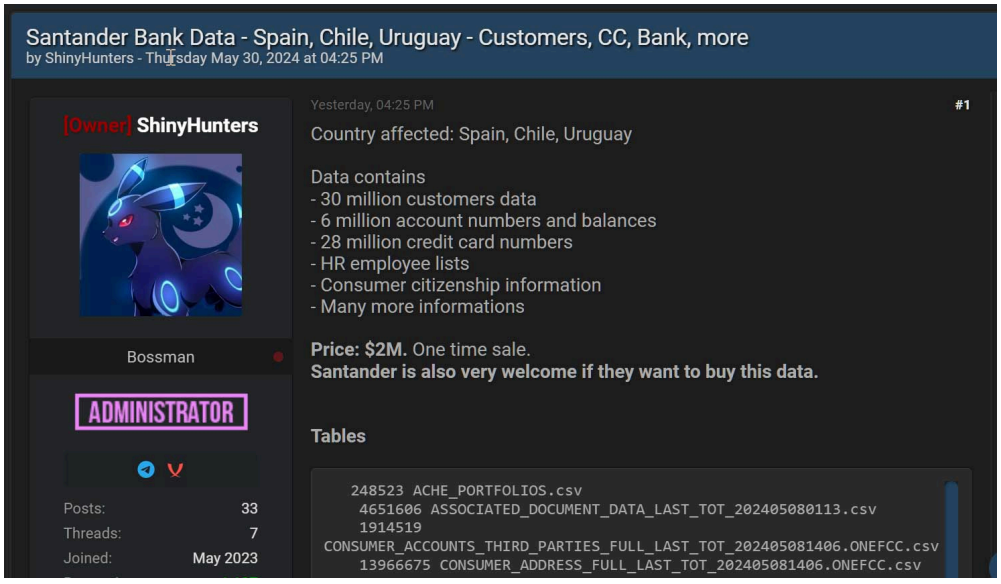
Two weeks ago, Spain's largest bank, Santander, disclosed a data breach after detecting unauthorized access to a database hosted by a third-party provider.

The company's investigation determined that the threat actor accessed data for employees and customers in Chile, Spain, and Uruguay.

"Following an investigation, we have now confirmed that certain information relating to customers of Santander Chile, Spain and Uruguay, as well as all current and some former Santander employees of the group had been accessed," reads a statement from Santander.

"Customer data in all other Santander markets and businesses are not affected."

Fast forward two weeks, and as first spotted by Dark Web Informer, ShinyHunters is now claiming to sell the data for Santander customers in Chile, Spain, and Uruguay for $2 million, the same data the bank reported was stolen.



Selling of Santander Bank data on a hacking forum

Source: BleepingComputer

ShinyHunters claims that the stolen data contains the personal information of 30 million customers and employees, 28 million credit card numbers, and 6 million account numbers and balances.

As part of the sale listing, the threat actor also shared samples of the data that contains the listed information but cannot be confirmed to belong to Santander.

It should be noted that Santander's Q1 2024 financial report states that there are only 19.5 million customers in those countries, rather than tht 30 million claimed by the threat actor.

This sales listing comes soon after the FBI seized BreachForums on May 15th, which was operated by ShinyHunters and another threat actor known as Baphomet.

While ShinyHunters says that Baphomet was arrested, he quickly restored the BreachForums site from a backup to a new domain.

Since then, the threat actor posted the sale of Ticketmaster and Santander, which some feel was done to restore the reputation of the site after its takedown by law enforcement.

However, what makes these sales unusual is that both were first listed on the Russian-speaking Exploit hacking forum days before they were listed on the newly-restored BreachForums.

Santander data sold on Exploit earlier in the week

Source: Kela

These sales were listed under the accounts of new members, with no reference to BreachForums or ShinyHunters, making others believe the sale on BreachForums is a fake.

However, ShinyHunters has commonly acted as a data breach broker for other threat actors in the past, and it is not uncommon for these threat actors to create new aliases on various forums to sell stolen data.

While TicketMaster has not confirmed whether a data breach occurred, ShinyHunters has a reputation for selling valid data breaches in the past.

In 2021, Shiny Hunters claimed to be selling the stolen data of 73 million AT&T customers, which the company repeatedly denied to BleepingComputer.

"I don't care if they don't admit. I'm just selling," ShinyHunters told BleepingComputer at the time.

In 2024, after the AT&T data was leaked on a hacking forum, AT&T finally confirmed that the data was legitimate and that they had suffered a breach.

In the past, ShinyHunters has breached or leaked the data for numerous companies, including Wattpad, Tokopedia, Microsoft's GitHub account, BigBasket, Nitro PDF, Pixlr, TeeSpring, Promo.com, Mathway, and many more.

Source: https://www.bleepingcomputer.com/news/security/shinyhunters-claims-santander-breach-selling-data-for-30m-customers/