May 31, 2024

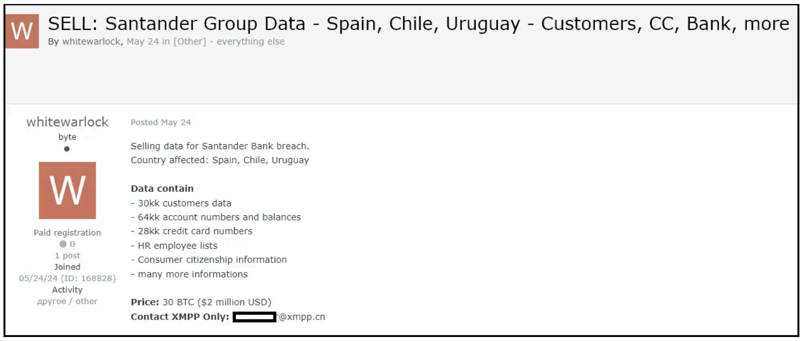
Snowflake, Cloud Storage Giant, Suffers Massive Breach: Hacker Confirms to Hudson Rock Access Through Infostealer Infection

Background

In this research, we aim to shed light on one of the largest data breaches to date. By directly communicating with the threat actor behind the massive data breach of cloud storage giant, Snowflake, we gained unprecedented insight into the devastating impact of Infostealer infections.

The story begins on May 26th, in a Telegram conversation with a threat actor claiming to have hacked two major companies, Ticketmaster and Santander Bank.

The data from these companies was put up for sale on the Russian-speaking cybercrime forum, exploit[.]in. Database samples provided by the threat actor led Hudson Rock researchers to believe that the data is genuine.



SELL: Santander Group Data - Spain, Chile, Uruguay - Customers, CC, Bank, more
By whitewarlock, May 24 in [Other] - everything else

whitewarlock
byte

Paid registration
0
1 post
Joined
05/24/24 (ID: 168828)
Activity
другое / other

Posted May 24

Selling data for Santander Bank breach.
Country affected: Spain, Chile, Uruguay

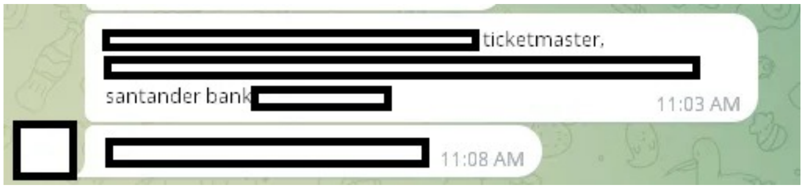
Data contain
- 30kk customers data
- 64kk account numbers and balances
- 28kk credit card numbers
- HR employee lists
- Consumer citizenship information
- many more informations

Price: 30 BTC ($2 million USD)
Contact XMPP Only: [redacted]@xmpp.cn

Santander bank data offered for sale on exploit.in

In the conversation with Hudson Rock, the threat actor reveals that there is much more to the story than these two breaches, and that additional major companies suffered a similar fate, allegedly including:

- Anheuser-Busch
- State Farm
- Mistubishi
- Progressive
- Neiman Marcus
- Allstate
- Advance Auto Parts

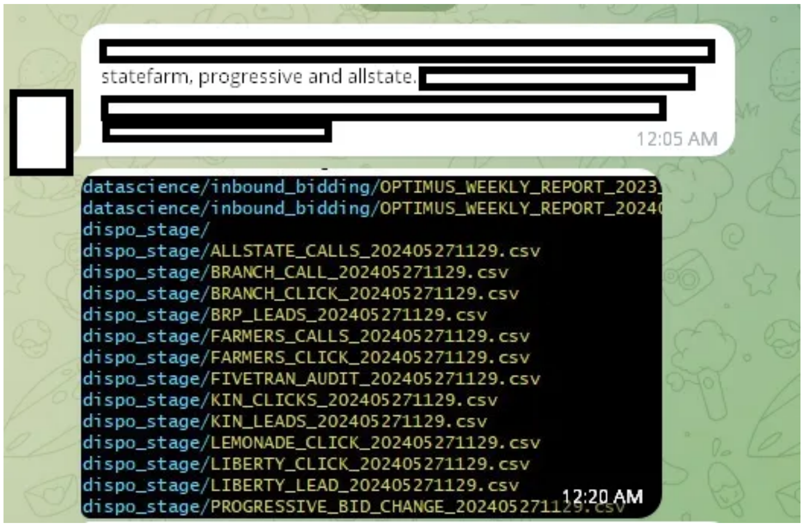


[redacted] ticketmaster, [redacted]
santander bank [redacted]
11:03 AM

[redacted]

[redacted] 11:08 AM

Part of the victim list shared by the threat actor



[redacted]
statefarm, progressive and allstate. [redacted]
12:05 AM

[redacted]

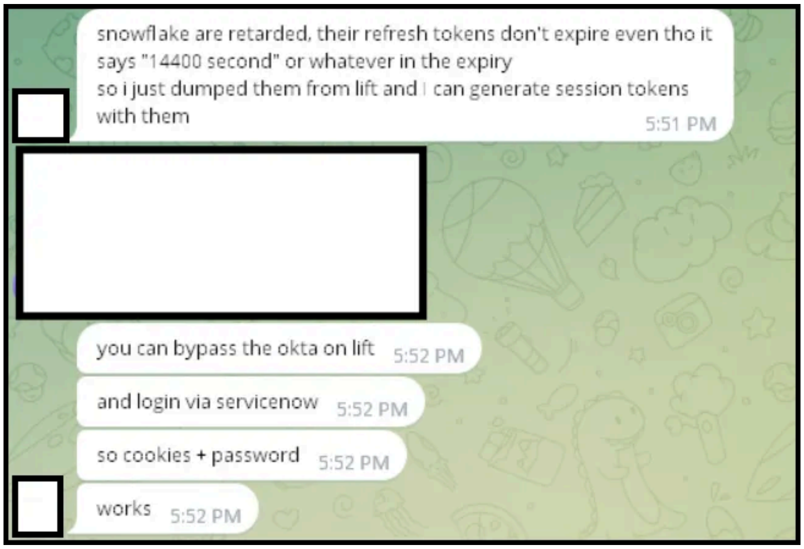
```
datascience/inbound_bidding/OPTIMUS_WEEKLY_REPORT_2023
datascience/inbound_bidding/OPTIMUS_WEEKLY_REPORT_2024
dispo_stage/
dispo_stage/ALLSTATE_CALLS_202405271129.csv
dispo_stage/BRANCH_CALL_202405271129.csv
dispo_stage/BRANCH_CLICK_202405271129.csv
dispo_stage/BRP_LEADS_202405271129.csv
dispo_stage/FARMERS_CALLS_202405271129.csv
dispo_stage/FARMERS_CLICK_202405271129.csv
dispo_stage/FIVETRAN_AUDIT_202405271129.csv
dispo_stage/KIN_CLICKS_202405271129.csv
dispo_stage/KIN_LEADS_202405271129.csv
dispo_stage/LEMONADE_CLICK_202405271129.csv
dispo_stage/LIBERTY_CLICK_202405271129.csv
dispo_stage/LIBERTY_LEAD_202405271129.csv
dispo_stage/PROGRESSIVE_BID_CHANGE_202405271129.csv
```

12:20 AM

Further explaining the source of the hack, the threat actor adds that all of these breaches stem from the hack of a single vendor — **Snowflake.**

To understand how the hack was carried out, the threat actor explains that they **were able to sign into a Snowflake employee's ServiceNow account using stolen credentials, thus bypassing OKTA** which is located on lift.snowflake.com.

Following the infiltration, the threat actor claims that they were able to generate session tokens, which enabled them to exfiltrate massive amounts of data from the company.



snowflake are retarded, their refresh tokens don't expire even tho it says "14400 second" or whatever in the expiry
so i just dumped them from lift and I can generate session tokens with them 5:51 PM

[redacted]

[redacted]

you can bypass the okta on lift 5:52 PM

and login via servicenow 5:52 PM

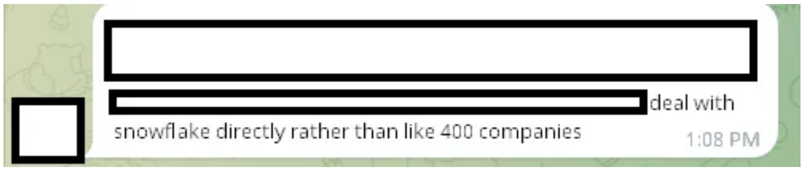
so cookies + password 5:52 PM

works 5:52 PM

[redacted]

Method used to hack Snowflake as shared by the threat actor

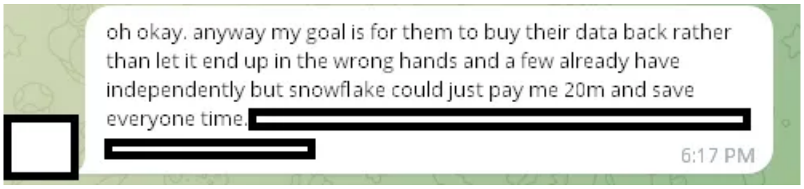
To put it bluntly, a single credential resulted in the exfiltration of potentially hundreds of companies that stored their data using Snowflake, with the threat actor himself suggesting **400 companies** are impacted.



[redacted]
[redacted] deal with snowflake directly rather than like 400 companies 1:08 PM

[redacted]

The goal of the threat actor, as in most cases, was to blackmail Snowflake into buying their own data back for $20,000,000.



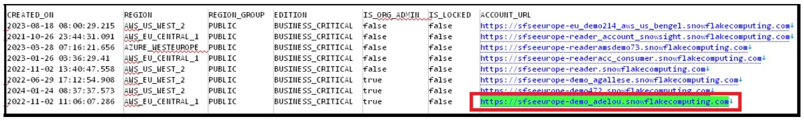
oh okay. anyway my goal is for them to buy their data back rather than let it end up in the wrong hands and a few already have independently but snowflake could just pay me 20m and save everyone time. [redacted]
[redacted] 6:17 PM

[redacted]

However it seems the company was not responsive.

Further evidence of the hack includes a CSV file that the threat actor shared with Hudson Rock's researchers, which shows the depth of their access to Snowflake servers.

This file documents over 2,000 customer instances relating to Snowflake's Europe servers.

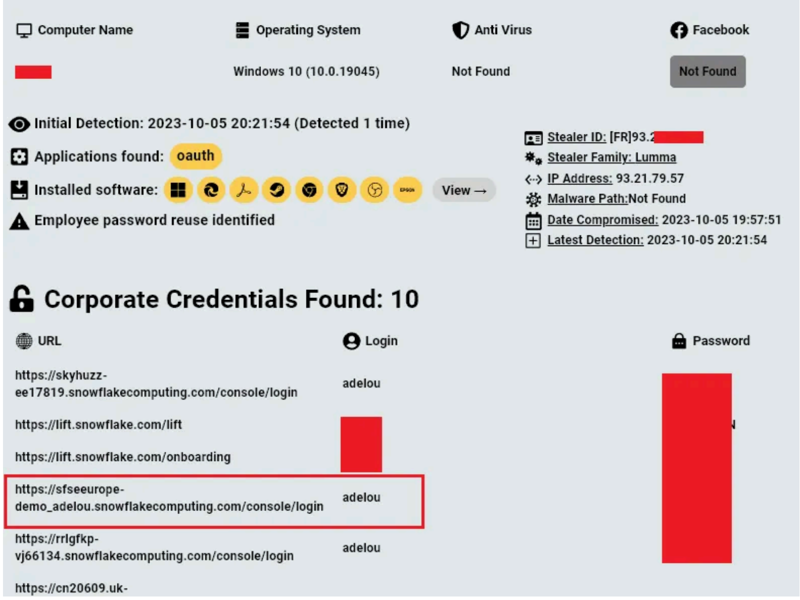


CREATED_ON	REGION	REGION_GROUP	EDITION	IS_ORG_ADMIN	IS_LOCKED	ACCOUNT_URL
2023-08-18 08:00:29.215	AWS_US_WEST_2	PUBLIC	BUSINESS_CRITICAL	false	false	https://sfseeurope-eu_demo214_aws_us_bengel.snowflakecomputing.com↓
2021-10-26 23:44:31.091	AWS_EU_CENTRAL_1	PUBLIC	BUSINESS_CRITICAL	false	false	https://sfseeurope-reader_account_snowsight.snowflakecomputing.com↓
2023-03-28 07:16:21.656	AZURE_WESTEUROPE	PUBLIC	BUSINESS_CRITICAL	false	false	https://sfseeurope-readeramsdemo73.snowflakecomputing.com↓
2023-01-26 03:36:29.41	AWS_EU_CENTRAL_1	PUBLIC	BUSINESS_CRITICAL	false	false	https://sfseeurope-readeracc_consumer.snowflakecomputing.com↓
2022-11-02 13:40:47.558	AWS_US_WEST_2	PUBLIC	BUSINESS_CRITICAL	false	false	https://sfseeurope-reader.snowflakecomputing.com↓
2022-06-29 17:12:54.908	AWS_EU_WEST_2	PUBLIC	BUSINESS_CRITICAL	true	false	https://sfseeurope-demo_agallese.snowflakecomputing.com↓
2024-01-24 08:37:37.573	AWS_US_WEST_2	PUBLIC	BUSINESS_CRITICAL	true	false	https://sfseeurope-demo472.snowflakecomputing.com↓
2022-11-02 11:06:07.286	AWS_EU_CENTRAL_1	PUBLIC	BUSINESS_CRITICAL	true	false	https://sfseeurope-demo_adelou.snowflakecomputing.com↓

Screenshot of “snowflake_eu-orgadmin.csv shared with Hudson Rock researchers

One credential to rule them all

Going over the data found in the CSV file, Hudson Rock researchers identified a Snowflake employee who was infected by a Lumma-type Infostealer on October 5th, 2023. Along with other sensitive credentials to Snowflake's infrastructure, this employee's login details (adelou) to a specific server (https://sfseeurope-demo_adelou.snowflakecomputing.com) were also compromised.



Computer Name	Operating System	Anti Virus	Facebook
[redacted]	Windows 10 (10.0.19045)	Not Found	Not Found

Initial Detection: 2023-10-05 20:21:54 (Detected 1 time)

Applications found: oauth

Installed software: View →

Employee password reuse identified

Stealer ID: [FR]93.2[redacted]

Stealer Family: Lumma

IP Address: 93.21.79.57

Malware Path:Not Found

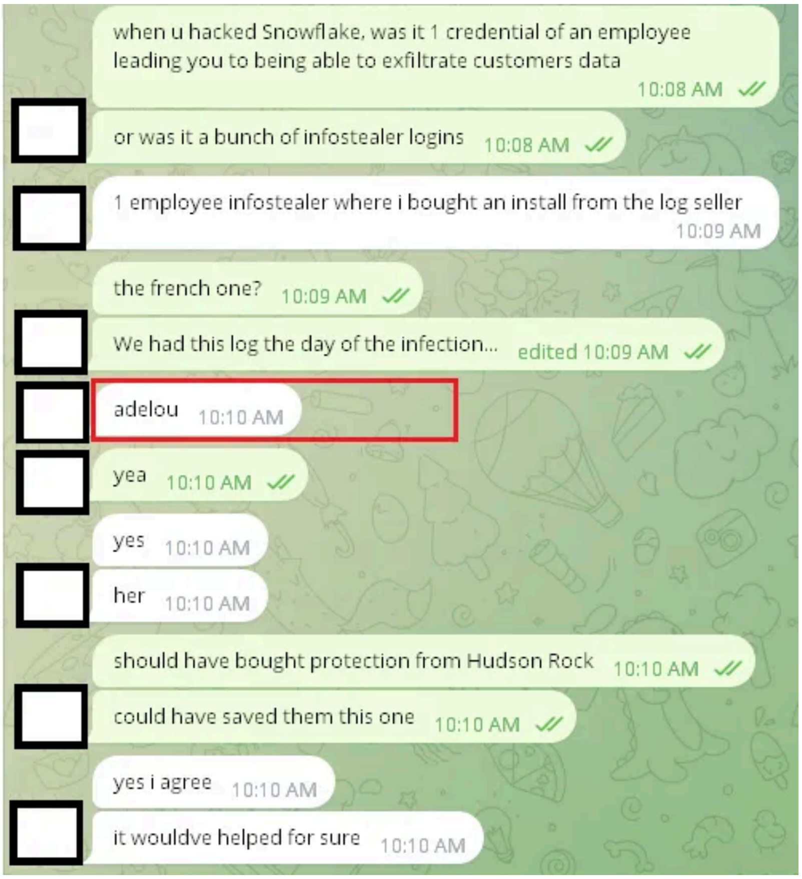
Date Compromised: 2023-10-05 19:57:51

Latest Detection: 2023-10-05 20:21:54

Corporate Credentials Found: 10

URL	Login	Password
https://skyhuzz-ee17819.snowflakecomputing.com/console/login	adelou	[redacted]
https://lift.snowflake.com/lift	[redacted]	[redacted]
https://lift.snowflake.com/onboarding	[redacted]	[redacted]
https://sfseeurope-demo_adelou.snowflakecomputing.com/console/login	adelou	[redacted]
https://rrlgfkp-vj66134.snowflakecomputing.com/console/login	adelou	[redacted]
https://cn20609.uk-		

When asked about the specific credentials used to carry out the hack, the threat actor confirmed to Hudson Rock researchers that indeed these are the same credentials they used, and shared a mutual sentiment with us around the absolute ease in which this gigantic hack could have been prevented.



when u hacked Snowflake, was it 1 credential of an employee leading you to being able to exfiltrate customers data 10:08 AM

or was it a bunch of infostealer logins 10:08 AM

1 employee infostealer where i bought an install from the log seller 10:09 AM

the french one? 10:09 AM

We had this log the day of the infection... edited 10:09 AM

adelou 10:10 AM

yea 10:10 AM

yes 10:10 AM

her 10:10 AM

should have bought protection from Hudson Rock 10:10 AM

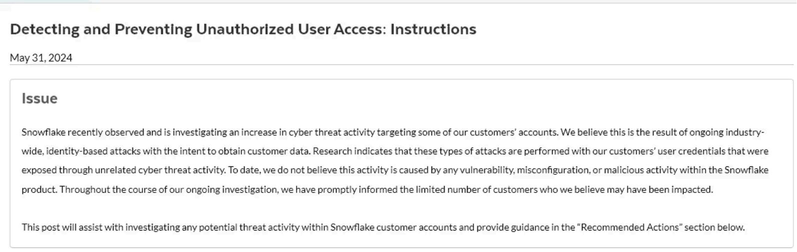
could have saved them this one 10:10 AM

yes i agree 10:10 AM

it wouldve helped for sure 10:10 AM

It is still undetermined what other companies were impacted by the hack. We expect that this information will be revealed slowly and over time as negotiations with the impacted companies are still ongoing.

On may 31st, Snowflake released a statement in which they claim that they are investigating an industry-wide identity-based attacks that have impacted "some" of their customers.



Detecting and Preventing Unauthorized User Access: Instructions

May 31, 2024

Issue

Snowflake recently observed and is investigating an increase in cyber threat activity targeting some of our customers' accounts. We believe this is the result of ongoing industry-wide, identity-based attacks with the intent to obtain customer data. Research indicates that these types of attacks are performed with our customers' user credentials that were exposed through unrelated cyber threat activity. To date, we do not believe this activity is caused by any vulnerability, misconfiguration, or malicious activity within the Snowflake product. Throughout the course of our ongoing investigation, we have promptly informed the limited number of customers who we believe may have been impacted.

This post will assist with investigating any potential threat activity within Snowflake customer accounts and provide guidance in the "Recommended Actions" section below.

Hudson Rock will follow up with updates relating to this hack.

• •   • •   • •

Info-stealer infections as a cybercrime trend surged by an incredible 6000% since 2018, positioning them as the primary initial attack vector used by threat actors to infiltrate organizations and execute cyberattacks, including ransomware, data breaches, account overtakes, and corporate espionage.

To learn more about how Hudson Rock protects companies from imminent intrusions caused by info-stealer infections of employees, partners, and users, as well as how we enrich existing cybersecurity solutions with our cybercrime intelligence API, please schedule a call with us, here: https://www.hudsonrock.com/schedule-demo

We also provide access to various free cybercrime intelligence tools that you can find here: www.hudsonrock.com/free-tools

Thanks for reading, **Rock Hudson Rock!**

Follow us on LinkedIn: https://www.linkedin.com/company/hudson-rock

Follow us on Twitter: https://www.twitter.com/RockHudsonRock

Schedule a Demo **Are you Compromised?**

More posts: