SaaSquatch Hunters:

Threat Detection in the Wild of SaaS

Julie Agnes Sparks
Detection Engineer

Welcome!

Loving the blue team life:

- Detection Engineering
- Incident Response
- Response Automation
- Log Ingestion
- Threat Hunting

Currently Security Research at Datadog,
Formerly doing D&R at Brex & Cloudflare

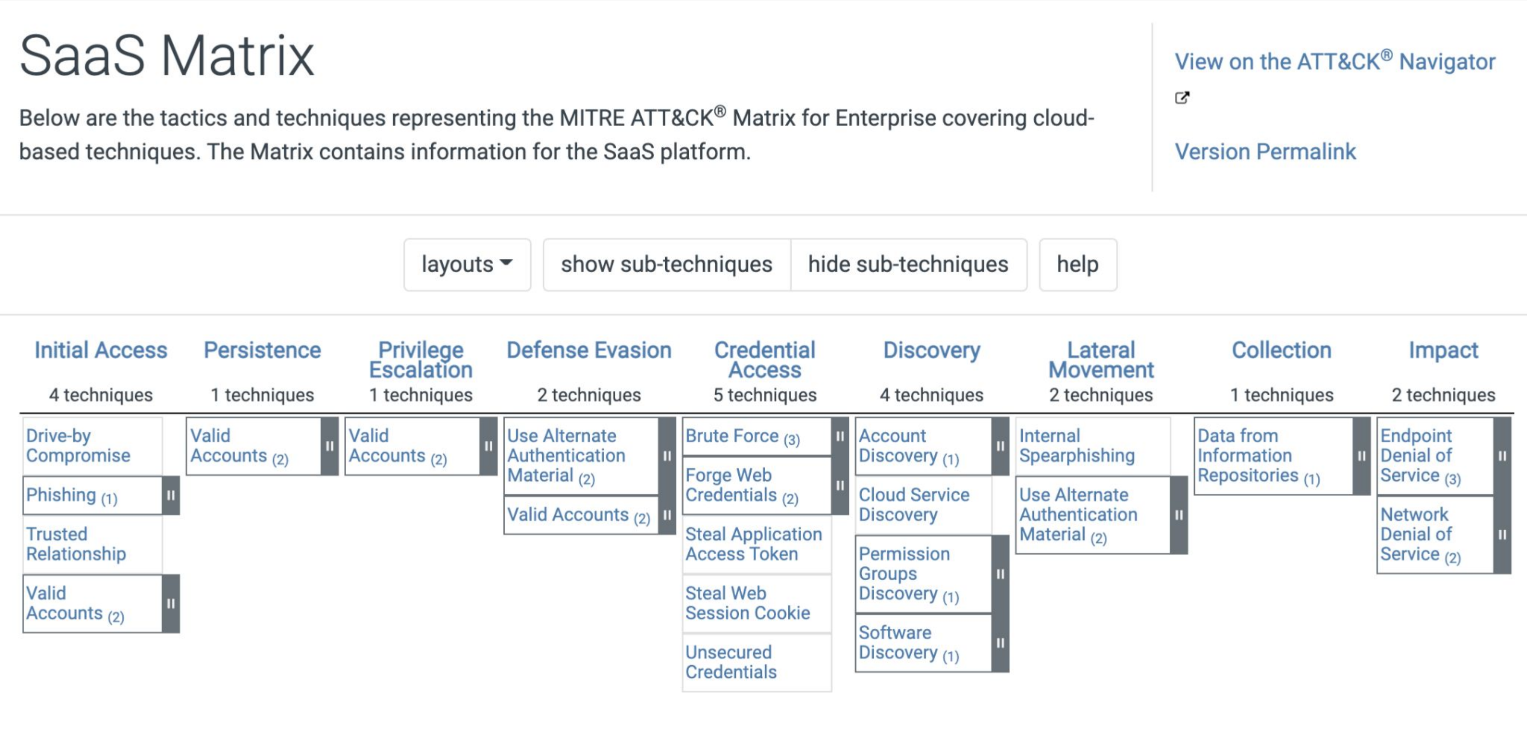
Agenda

- SaaS Matrix
- Logging & Data Quality
- SaaS Application Attacks
- Let’s Write Some Detections

01

Leveraging the Matrix

What tools do we have for guidance?



SaaS Matrix

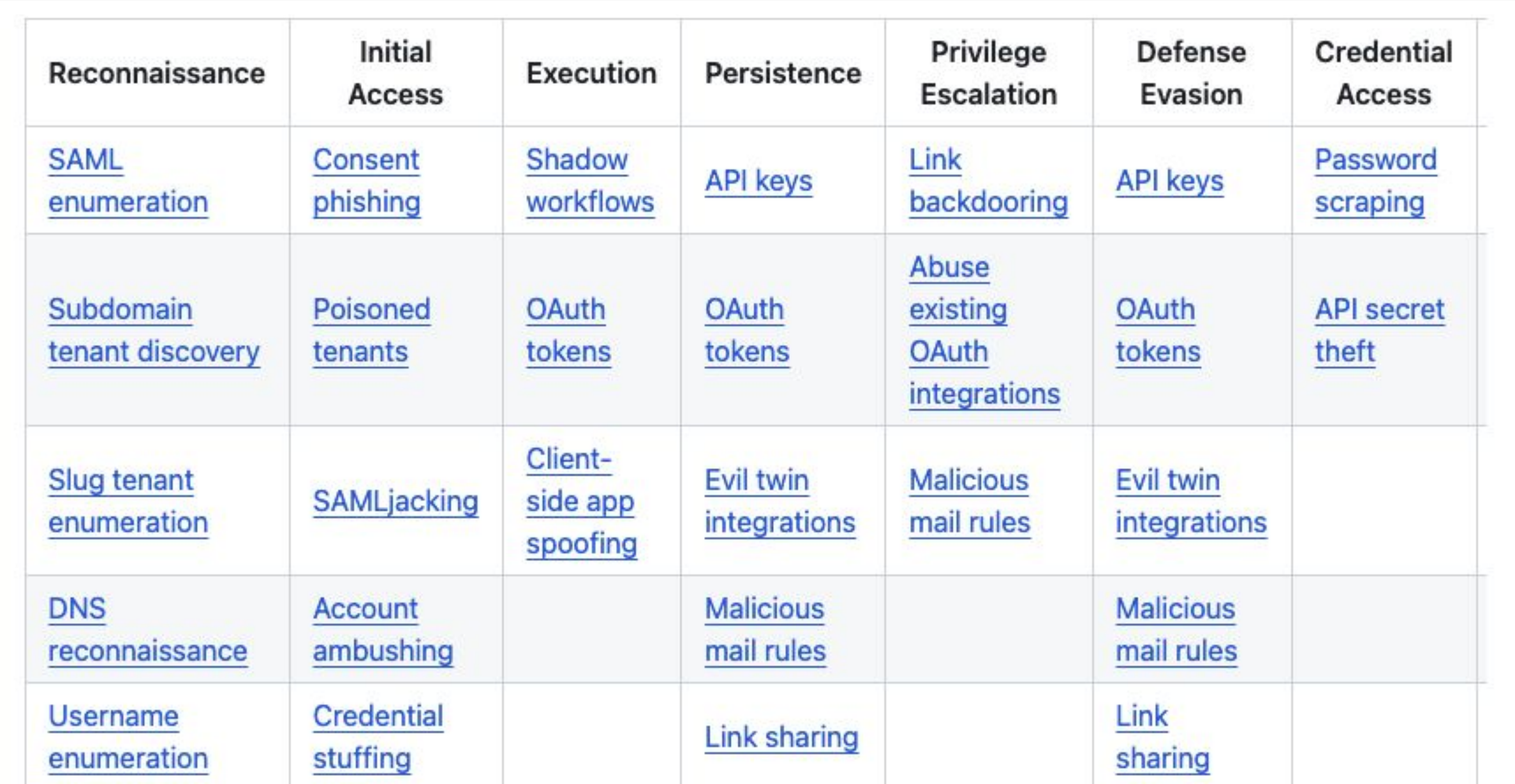
Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the SaaS platform.

View on the ATT&CK® Navigator

Version Permalink

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
4 techniques	1 techniques	1 techniques	2 techniques	5 techniques	4 techniques	2 techniques	1 techniques	2 techniques
Drive-by Compromise	Valid Accounts (2)	Valid Accounts (2)	Use Alternate Authentication Material (2)	Brute Force (3)	Account Discovery (1)	Internal Spearphishing	Data from Information Repositories (1)	Endpoint Denial of Service (3)
Phishing (1)			Valid Accounts (2)	Forge Web Credentials (2)	Cloud Service Discovery	Use Alternate Authentication Material (2)		Network Denial of Service (2)
Trusted Relationship				Steal Application Access Token	Permission Groups Discovery (1)			
Valid Accounts (2)				Steal Web Session Cookie	Software Discovery (1)			
				Unsecured Credentials				

SaaS Matrix from MITRE



Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
SAML enumeration	Consent phishing	Shadow workflows	API keys	Link backdooring	API keys	Password scraping
Subdomain tenant discovery	Poisoned tenants	OAuth tokens	OAuth tokens	Abuse existing OAuth integrations	OAuth tokens	API secret theft
Slug tenant enumeration	SAMLjacking	Client-side app spoofing	Evil twin integrations	Malicious mail rules	Evil twin integrations	
DNS reconnaissance	Account ambushing		Malicious mail rules		Malicious mail rules	
Username enumeration	Credential stuffing		Link sharing		Link sharing	

SaaS Matrix from Push Security

02
Logging & Data Quality

What logs can be available?

- User Activity
- API Activity
- Administrative Activity
- Integration Activity
- Authentication

Log Limitations

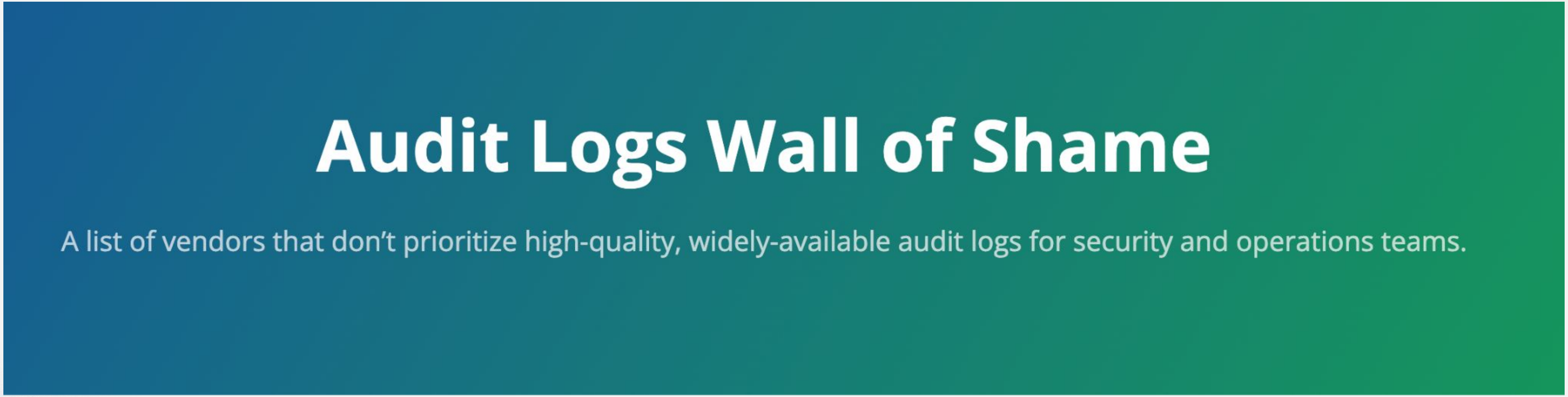
Lack of Log Content

Licensing & Cost

Poor Quality & Lack of Consistency in Formatting

Difficult Log Collection Mechanism

Want to know more?

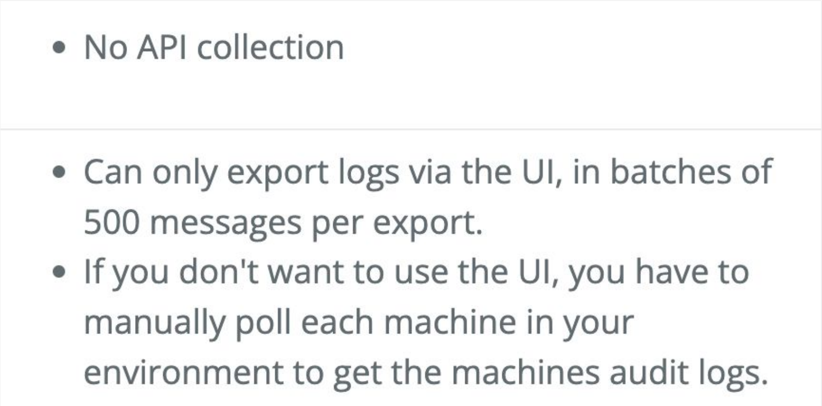


Audit Logs Wall of Shame

A list of vendors that don’t prioritize high-quality, widely-available audit logs for security and operations teams.

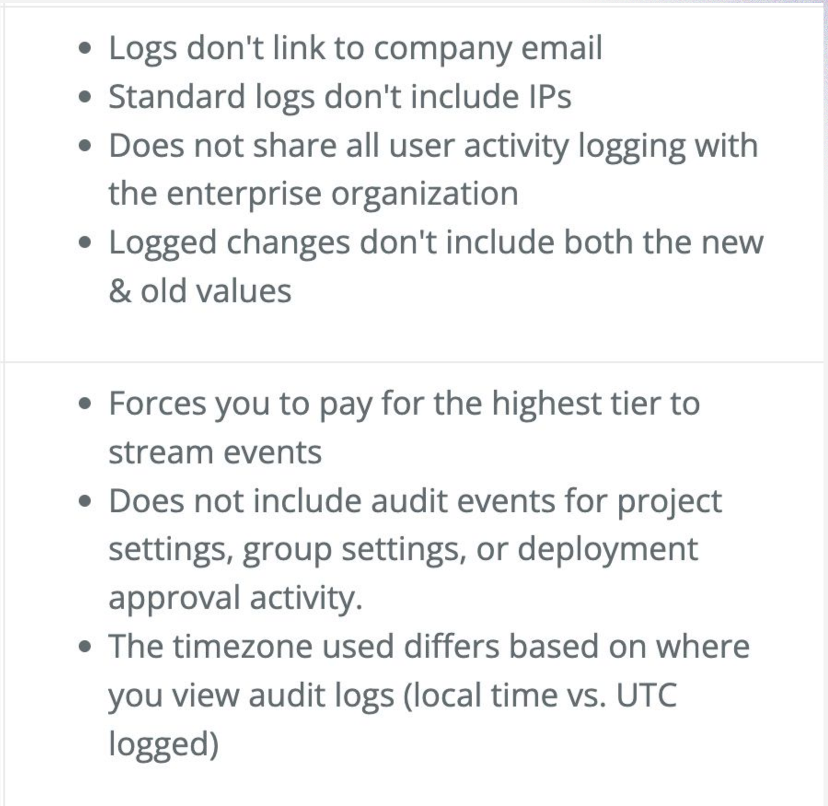
audit-logs.tax

Example Logging Issues for SaaS Apps



- No API collection

- Can only export logs via the UI, in batches of 500 messages per export.
- If you don't want to use the UI, you have to manually poll each machine in your environment to get the machines audit logs.



- Logs don't link to company email
- Standard logs don't include IPs
- Does not share all user activity logging with the enterprise organization
- Logged changes don't include both the new & old values

- Forces you to pay for the highest tier to stream events
- Does not include audit events for project settings, group settings, or deployment approval activity.
- The timezone used differs based on where you view audit logs (local time vs. UTC logged)

How can we make logs better ourselves?

Reference/Lookup Tables & Caching Data

Imagine... we had every IP address that checked in with our EDR provider in a table of lower risk device activity to reference our detections against.

Data Ingestion Cross Enrichment

Imagine... that same IP address is enriched into every other log source for that user to understand if they're accessing that application from a known location

03

SaaS Attacks & Detection

Detection Focus for SaaS

General Areas to Consider:

- Known bad patterns (Threat Research is your best friend)
- API activity
- User and service account pattern analysis
- Token usage
- Critical assets & data access

MITRE ATT&CK focus:

- Initial Access
- Persistence
- Collection
- Exfiltration

Inputs to Detection Engineering Research for SaaS

- Audit log documentation from the provider
- Past history of log data to use for hunting
- Research using current security articles and content
- Threat intelligence indicators

Let’s Focus on Two Cases

Github

Developer platform for Code Interaction & Storage

Snowflake

Cloud-based data storage and analytics service

Attackers Targeting Github
Attackers Targeting Snowflake

Google Security on Github Detection
Examining Github Security
Github Security Guide

Github Log Visibility

- Github has GA attribution of associated user email addresses to activities in audit logs.
- They allow the ability to include source_ip address in logs.
- Github provides granular detail on type of token taking the action, such as:
  - Personal Access Token (Regular or Fine Grained)
  - OAuth Access Token
  - Server to Server Access Token
  - User to Server Access Token
- There's now Github API request logs that provide granular usage of tokens to take actions via API.

Github token formats & usage

Github Threat Actors

Various Groups →

Malicious Payload Delivery & Packages

Github has been used to host and deliver malicious payloads and act as dead drop resolvers, command-and-control, and data exfiltration points.

ShinyHunters & Various Groups →

Credential Theft & Data Exfiltration

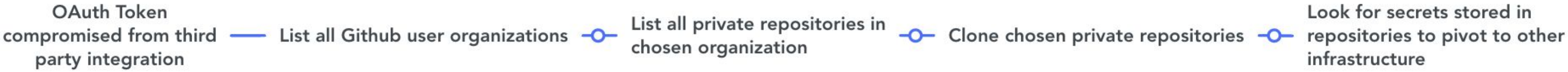
Compromising user accounts through credential theft and then exfiltrating data, stealing further access keys, or ultimately extorting the company

Threat Actors & Github
Gitloker Extortion

History of Access Token Usage

April 2022

GitHub Security announced it had detected the compromise of OAuth access tokens issued to Heroku and Travis-CI integrations to download data from dozens of organizations.



OAuth Token compromised from third party integration

List all Github user organizations

List all private repositories in chosen organization

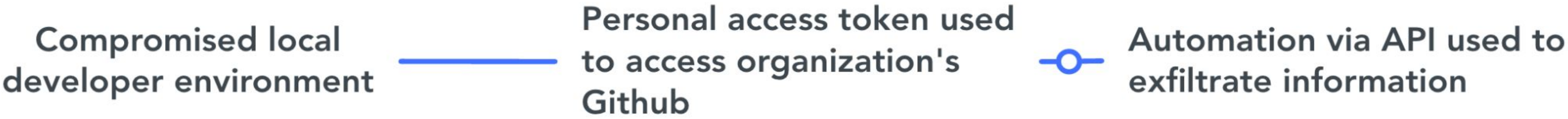
Clone chosen private repositories

Look for secrets stored in repositories to pivot to other infrastructure

History of Access Token Usage

October 2023

In another compromise, organizations found that attackers accessed their Github accounts using compromised PATs (Personal Access Token) – most likely exfiltrated silently from the victim’s development environment.

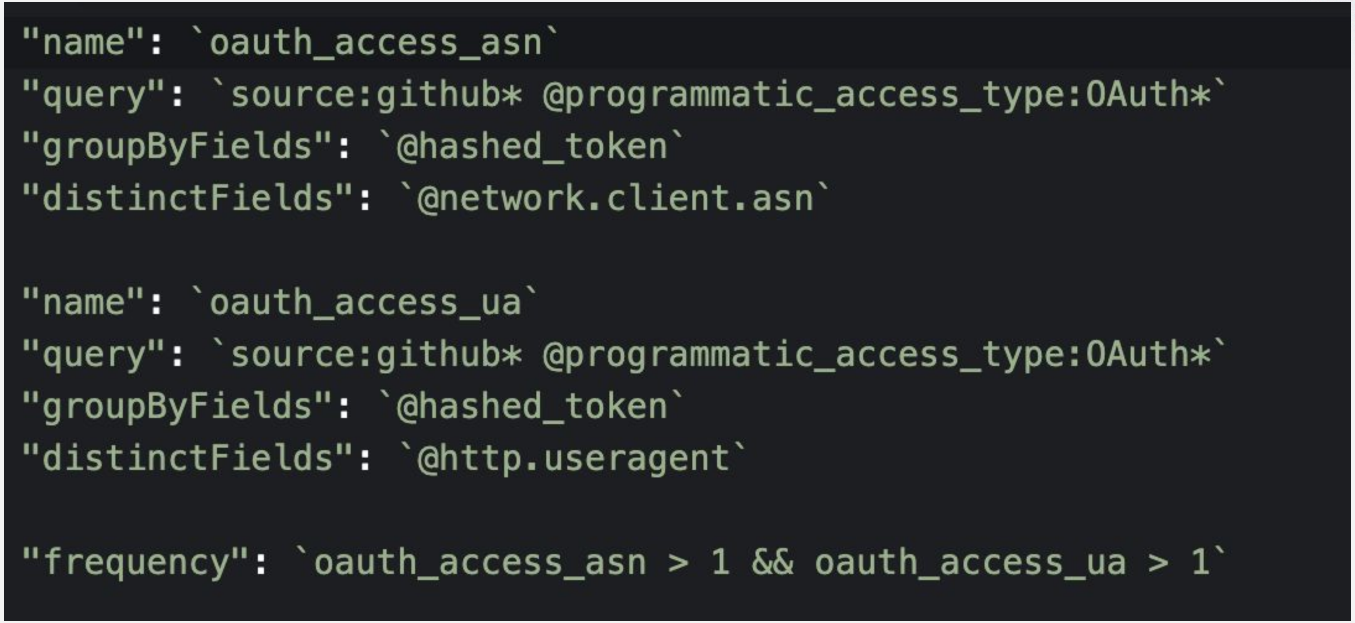


Compromised local developer environment

Personal access token used to access organization's Github

Automation via API used to exfiltrate information

Github OAuth Token Actions taken by Various ASNs and UAs



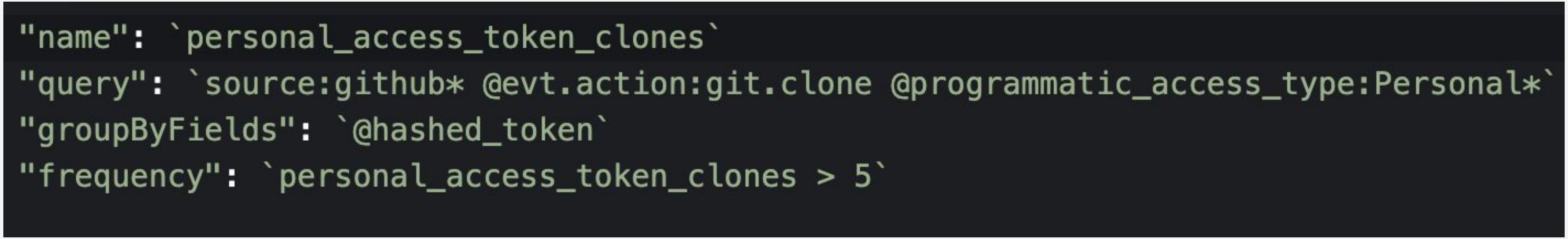
```
"name": `oauth_access_asn`
"query": `source:github* @programmatic_access_type:OAuth*`
"groupByFields": `@hashed_token`
"distinctFields": `@network.client.asn`

"name": `oauth_access_ua`
"query": `source:github* @programmatic_access_type:OAuth*`
"groupByFields": `@hashed_token`
"distinctFields": `@http.useragent`

"frequency": `oauth_access_asn > 1 && oauth_access_ua > 1`
```

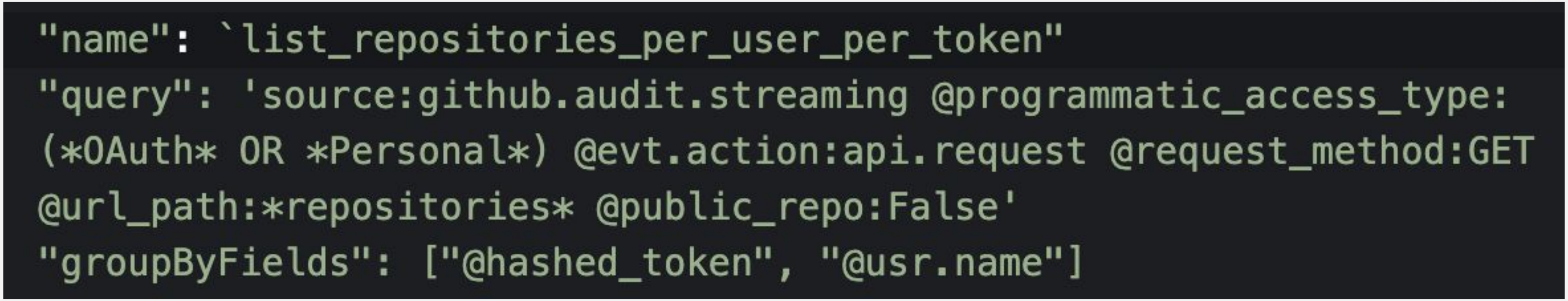
Okta Session Hijacking Research

GitHub Personal Access Token used to clone repositories



```
"name": `personal_access_token_clones`
"query": `source:github* @evt.action:git.clone @programmatic_access_type:Personal*`
"groupByFields": `@hashed_token`
"frequency": `personal_access_token_clones > 5`
```

Github LIST Repos via API Request from OAuth or Personal Access Token



```
"name": `list_repositories_per_user_per_token"
"query": 'source:github.audit.streaming @programmatic_access_type:
(*OAuth* OR *Personal*) @evt.action:api.request @request_method:GET
@url_path:*repositories* @public_repo:False'
"groupByFields": ["@hashed_token", "@usr.name"]
```

Additional Detection Ideas

- New OAuth application authorized
- OAuth application access restrictions removed
- Private Repository changed to Public
- Anomalous service account or bot activity
- SSH key added by suspicious IP

Snowflake Threat Actors

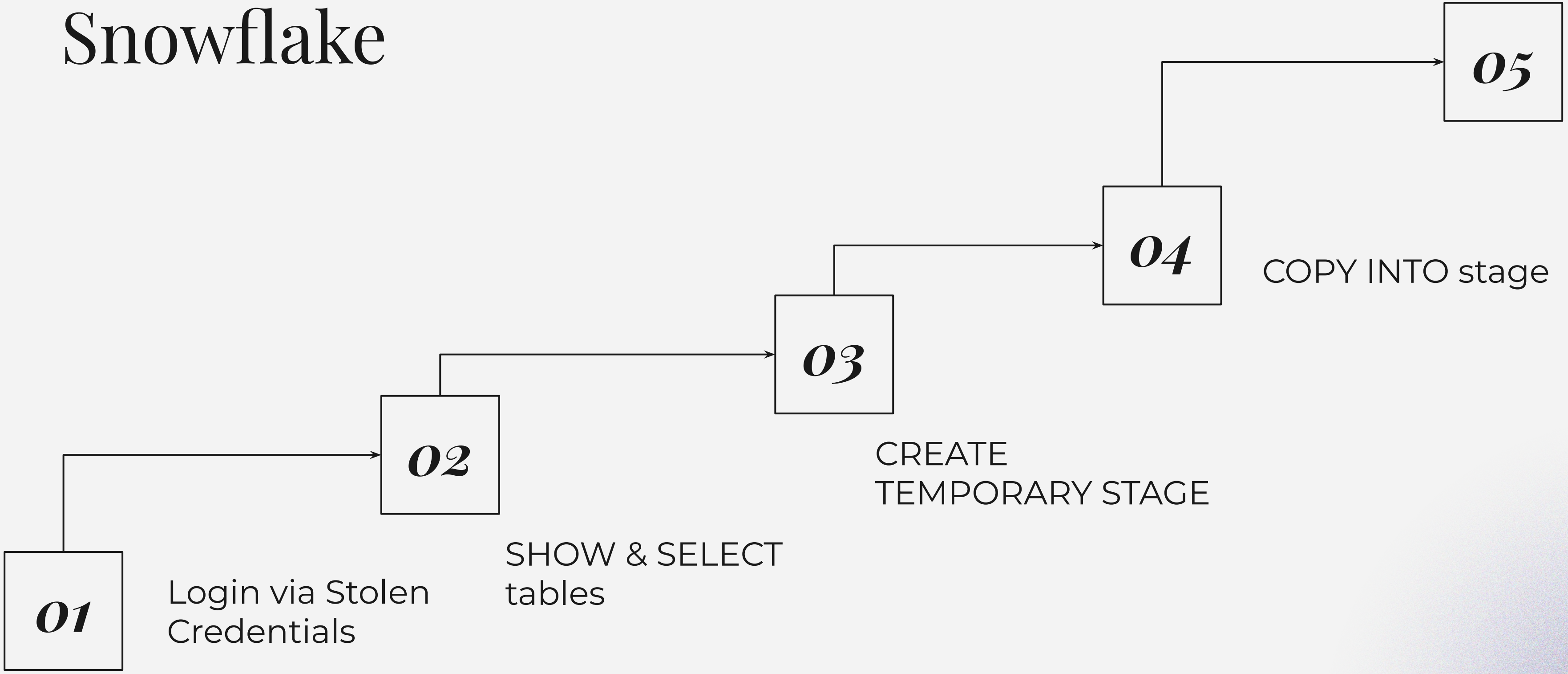
UNC 5537

Active 2024 - Present

Infostealer Malware Used to Gain User Account Access

A financially motivated threat actor suspected to have stolen a significant volume of records from Snowflake customer environments

UNC 5537 behaviors in Snowflake



01 Login via Stolen Credentials

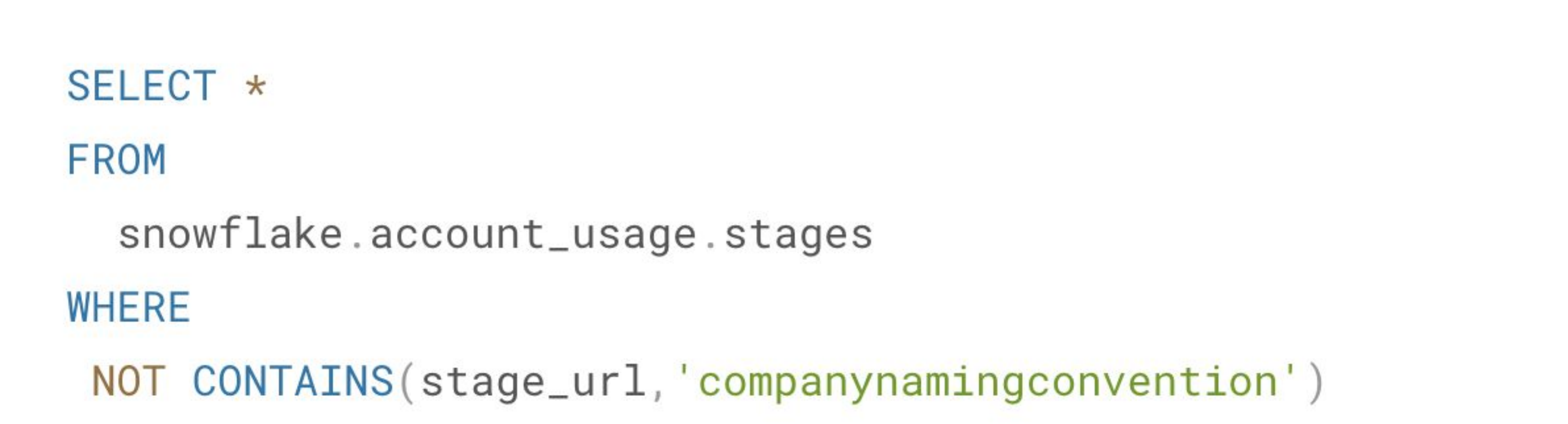
02 SHOW & SELECT tables

03 CREATE TEMPORARY STAGE

04 COPY INTO stage

05 GET data through stage to local machine

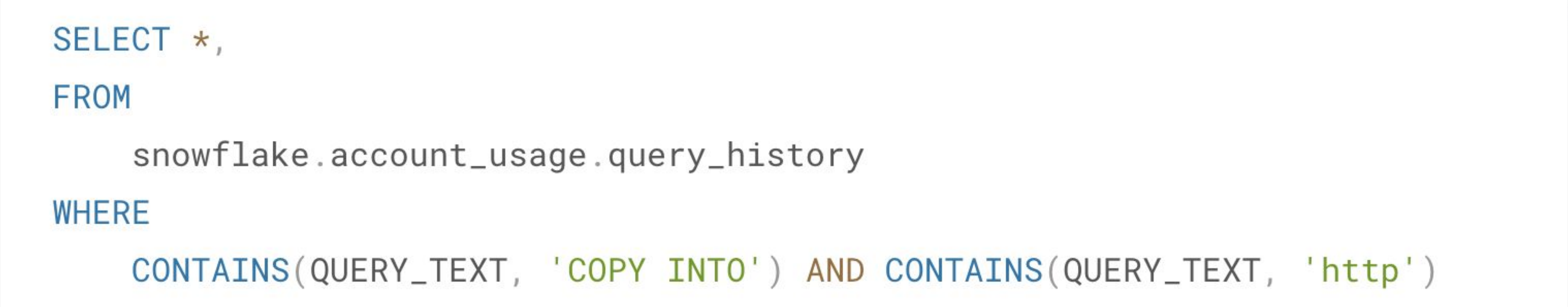
Snowflake stage set to anomalous external location



```
SELECT *
FROM
  snowflake.account_usage.stages
WHERE
 NOT CONTAINS(stage_url,'companynamingconvention')
```

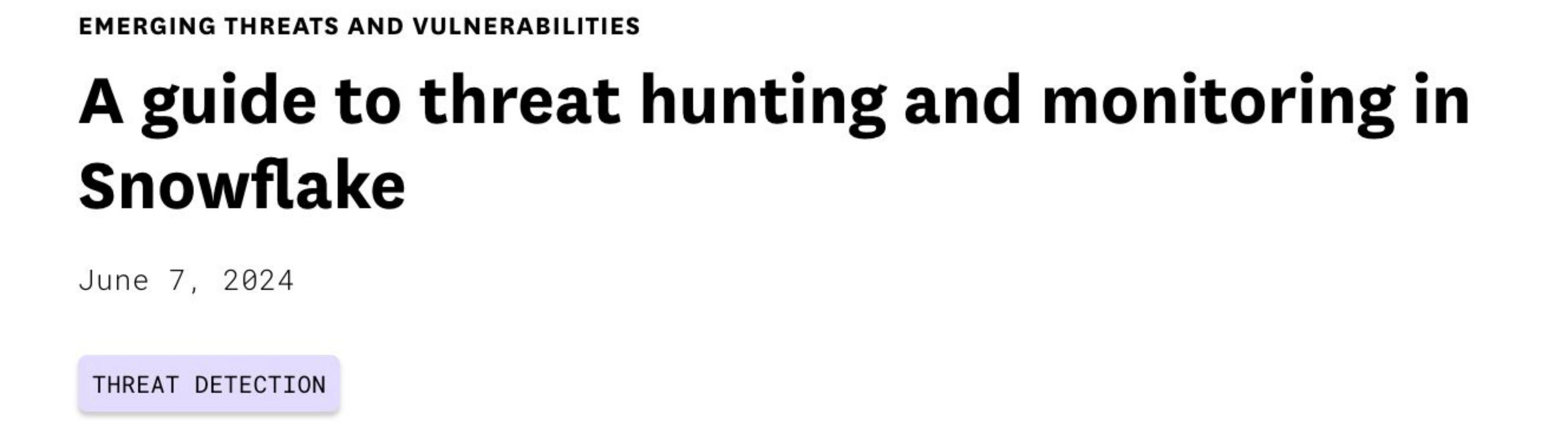
Okta Session Hijacking Research

Snowflake user COPY INTO new location



```
SELECT *,
FROM
    snowflake.account_usage.query_history
WHERE
    CONTAINS(QUERY_TEXT, 'COPY INTO') AND CONTAINS(QUERY_TEXT, 'http')
```

If you want to read more about threat hunting in Snowflake..



EMERGING THREATS AND VULNERABILITIES

A guide to threat hunting and monitoring in Snowflake

June 7, 2024

THREAT DETECTION

Additional Detection Ideas

- New Client Application Authorized for Snowflake Instance
- Grants of Administrator role to User
- Network Policy Modified to Allow External IPs
- Anomalous amount of tables queried

Thanks!

Do you have any questions?

Reach out to me on LinkedIn or after the talk.

https://www.linkedin.com/in/julie-a-sparks/

Check out a list of OOTB detections from here and here.

Read more about Github Detections in a previous BSidesLV talk, here.

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**

Please keep this slide for attribution