

Have my keys been pwned? - API Edition

By Jose Hernandez & Rod Soto

\$whoami

José Hernandez

Principal Security Researcher at Splunk. He started his professional career at Prolexic Technologies (now Akamai), fighting DDOS attacks against Fortune 100 companies perpetrated by “anonymous” and “lulzsec.” As an engineering co-founder of Zenedge Inc. (acquired by Oracle Inc.), José helped build technologies to fight bots and web-application attacks. He has also built security operation centers and run a public threat-intelligence service.

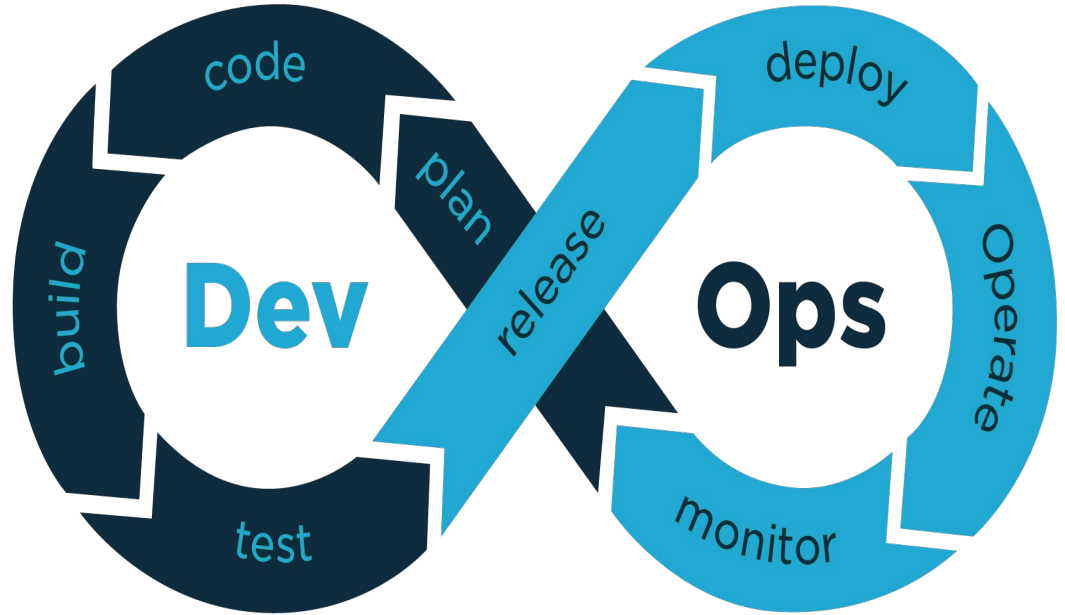
Rod Soto

Principal Security Research Engineer at Splunk. Worked at Prolexic Technologies (now Akamai), and Caspida. Cofounder of Hackmiami and Pacific Hackers meetups and conferences. Creator of Kommand && KonTroll / NoQrtr-CTF.

What is Devops?

DevOps is a set of practices that combines software development and IT operations. It aims to shorten the systems development life cycle and provide continuous delivery with high software quality. DevOps is complementary with Agile software development; several DevOps aspects came from Agile methodology.

[Wikipedia](#)



What are toolchains?

A DevOps toolchain is a set or combination of tools that aid in the delivery, development, and management of software applications throughout the systems development life cycle, as coordinated by an organisation that uses DevOps practices. [Wikipedia](#)

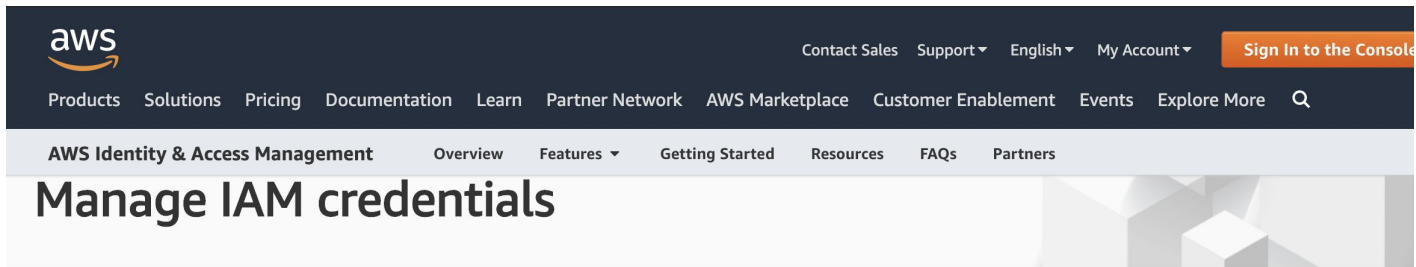


Credentials travel through the whole process

The fluidity of this process introduces new risks as well

- Developer usually have high privilege credentials
- Ephemeral environments dismissed and poorly monitored
- Disconnection between dev and sec ops
- Widely spread use of open source tools and code at times trusted by default
- Embedded credentials usually end up in public repositories
- Higher risk of rogue insider or abuse of high privilege credentials
- Due to the CI/CD nature link with production environments is immediate
- Cloud environments have made these risks even higher

How do cloud providers manage credentials



AWS Identity and Access Management (IAM) lets you manage several types of long-term security credentials for IAM users:

- **Passwords** – Used to sign in to secure AWS pages, such as the AWS Management Console and the AWS Discussion Forums.
- **Access keys** – Used to make programmatic calls to AWS from the AWS APIs, AWS CLI, AWS SDKs, or AWS Tools for Windows PowerShell.
- **Amazon CloudFront key pairs** – Used for CloudFront to create [signed URLs](#).
- **SSH public keys** – Used to authenticate to [AWS CodeCommit](#) repositories.

You can assign AWS security credentials to your IAM users by using the API, CLI, or AWS Management Console. You can rotate or revoke these credentials whenever you want.

In addition to managing these user credentials, you can further enhance the security of IAM user access to AWS by enforcing the use of [multi-factor authentication \(MFA\)](#).

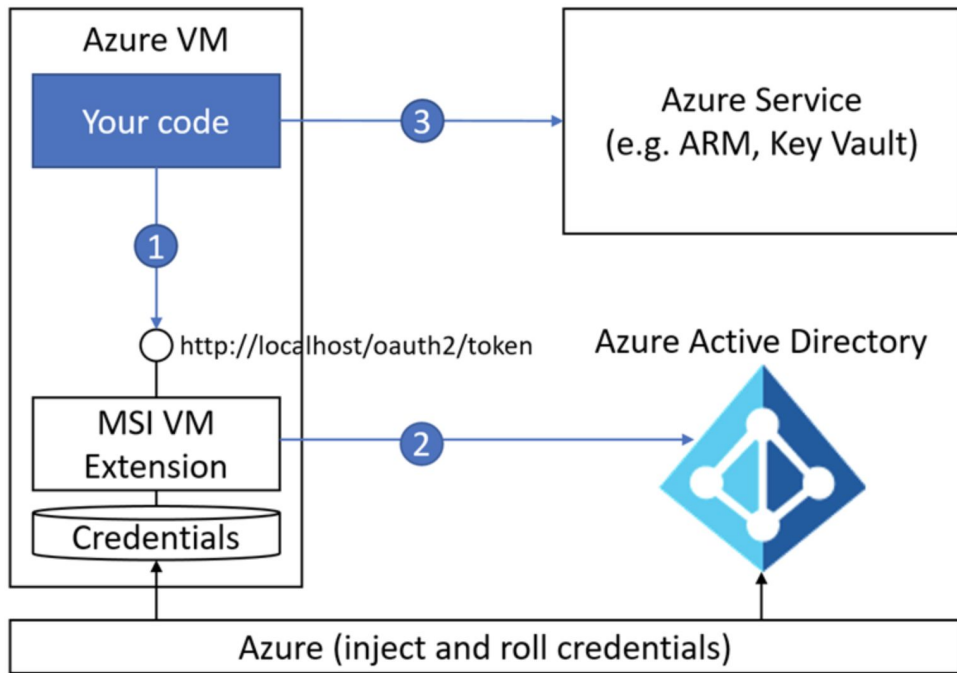
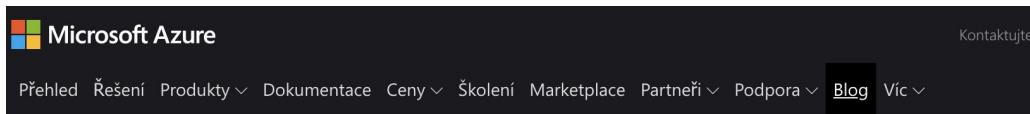
For more information about using long-term security credentials in AWS, see About [AWS Security Credentials](#).

Temporary security credentials

IAM also lets you grant users temporary security credentials with a defined expiration for access to your AWS resources. For example, temporary access is useful when:

- Creating a mobile app with third-party sign-in.

How do cloud providers manage credentials



How do cloud providers manage credentials

Authentication strategies

Google Cloud APIs use the [OAuth 2.0 protocol](#) for authenticating both user accounts and service accounts. The OAuth 2.0 authentication process determines both the principal and the application.

Most Google Cloud APIs also support anonymous access to public data using API keys. However, API keys only identify the application, not the principal. When using API keys, the principal must be authenticated by other means.

Google Cloud APIs support multiple authentication flows for different runtime environments. For the best developer experience, we recommend using [Google Cloud Client Libraries](#) with Google Cloud APIs. They use Google-provided authentication libraries that support a variety of authentication flows and runtime environments.

To build an application using Google Cloud APIs, follow these general steps:

- Choose and use the provided Google Cloud Client Libraries
- Determine the correct authentication flow for your application
- Find or create the application credentials needed for your application
- Pass the application credentials to the client libraries at application startup time, ideally through [Application Default Credentials](#) (ADC)

Other credentials often used

- Email & password
- IAM username & Password
- MFA
- Access Keys
- Key pairs
- Account identifiers
- X.509 Certificates

Primary source of leaked credentials

GitHub

IT service management company



GitLab



GitLab

Software



More images



Amazon S3

[Overview](#)

Features ▾

Storage classes

Pricing

Security


Resources ▾

FAQs


Amazon S3





Object storage built to store and retrieve any amount of data from anywhere


Anywhere you store code or EVEN snippets


 PASTEBIN


GO **PRO** API TOOLS FAQ **+ paste**

 **Untitled**

 A GUEST  JUN 14TH, 2019  84  NEVER

 SHARE

 TWEET

 Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!

Python 0.58 KB

raw download clone embed report print

```
1. import boto3
2.
3. AWS_ACCESS_KEY = "AKIA*****UAA"
4. AWS_SECRET_ACCESS_KEY = "GA93*****Kke6"
5. REGION_NAME = "eu-west-1"
6.
7.
8. session = boto3.session.Session(aws_access_key_id=AWS_ACCESS_KEY,
9.                                 aws_secret_access_key=AWS_SECRET_ACCESS_KEY,
10.                                region_name=REGION_NAME)
11. ec2 = session.resource('ec2')
12. volumes = ec2.get_all_volumes(filters={'status': 'available'})
13. for volumen in volumens:
14.     print 'Deleteing volume: ID - {}, status = {}'.format( vol.id, vol.status)
15.     ec2.delete_volume(volumen.id)
```

Unsecured credentials - Mitre Cloud ATT&CK Matrix

Cloud 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 following platforms: AWS, GCP, Azure, Azure AD, Office 365, SaaS.

[View on the ATT&CK® Navigator ↗](#)

[About the Enterprise domain](#)

[Version Permalink](#)

layouts ▼

show sub-techniques

hide sub-techniques

help

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	5 techniques	1 techniques	5 techniques	4 techniques	10 techniques	2 techniques	4 techniques	1 techniques	4 techniques
Drive-by Compromise	Account Manipulation (3)	Valid Accounts (2)	Impair Defenses (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Defacement (1)
Exploit Public-Facing Application	Create Account (1)		Modify Cloud Compute Infrastructure (4)	Steal Application Access Token	Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data from Information Repositories (2)		Endpoint Denial of Service (3)
Phishing (1)	Implant Container Image		Unused/Unsupported Cloud Regions	Steal Web Session Cookie	Cloud Service Discovery		Data Staged (1)		Network Denial of Service (2)
Trusted Relationship	Office Application Startup (6)		Use Alternate Authentication Material (2)	Unsecured Credentials (2)	Network Service Scanning		Email Collection (2)		Resource Hijacking
Valid Accounts (2)	Valid Accounts (2)		Valid Accounts (2)		Network Share Discovery				
					Permission Groups Discovery (1)				
					Remote System Discovery				
					Software Discovery (1)				
					System Information Discovery				
					System Network Connections Discovery				

Last modified: 02 July 2020

Valid Accounts: Cloud Accounts - Mitre Att&ck T1078.004

[Home](#) > [Techniques](#) > [Enterprise](#) > [Valid Accounts](#) > [Cloud Accounts](#)

Valid Accounts: Cloud Accounts

Other sub-techniques of Valid Accounts (4) 

Adversaries may obtain and abuse credentials of a cloud account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. In some cases, cloud accounts may be federated with traditional identity management system, such as Window Active Directory.^{[1][2][3]}

Compromised credentials for cloud accounts can be used to harvest sensitive data from online storage accounts and databases. Access to cloud accounts can also be abused to gain Initial Access to a network by abusing a [Trusted Relationship](#). Similar to [Domain Accounts](#), compromise of federated cloud accounts may allow adversaries to more easily move laterally within an environment.

ID: T1078.004

Sub-technique of: [T1078](#)

Tactics: Defense Evasion, Persistence, Privilege Escalation, Initial Access

Platforms: AWS, Azure, Azure AD, GCP, Office 365, SaaS

Permissions Required: Administrator, User

Data Sources: AWS CloudTrail logs, Authentication logs, Azure activity logs, Stackdriver logs

Version: 1.0

Created: 13 March 2020

Last Modified: 23 March 2020

[Version Permalink](#)

Lateral Movement / Escalation of Privilege

Example:

AWS Security Token Service:

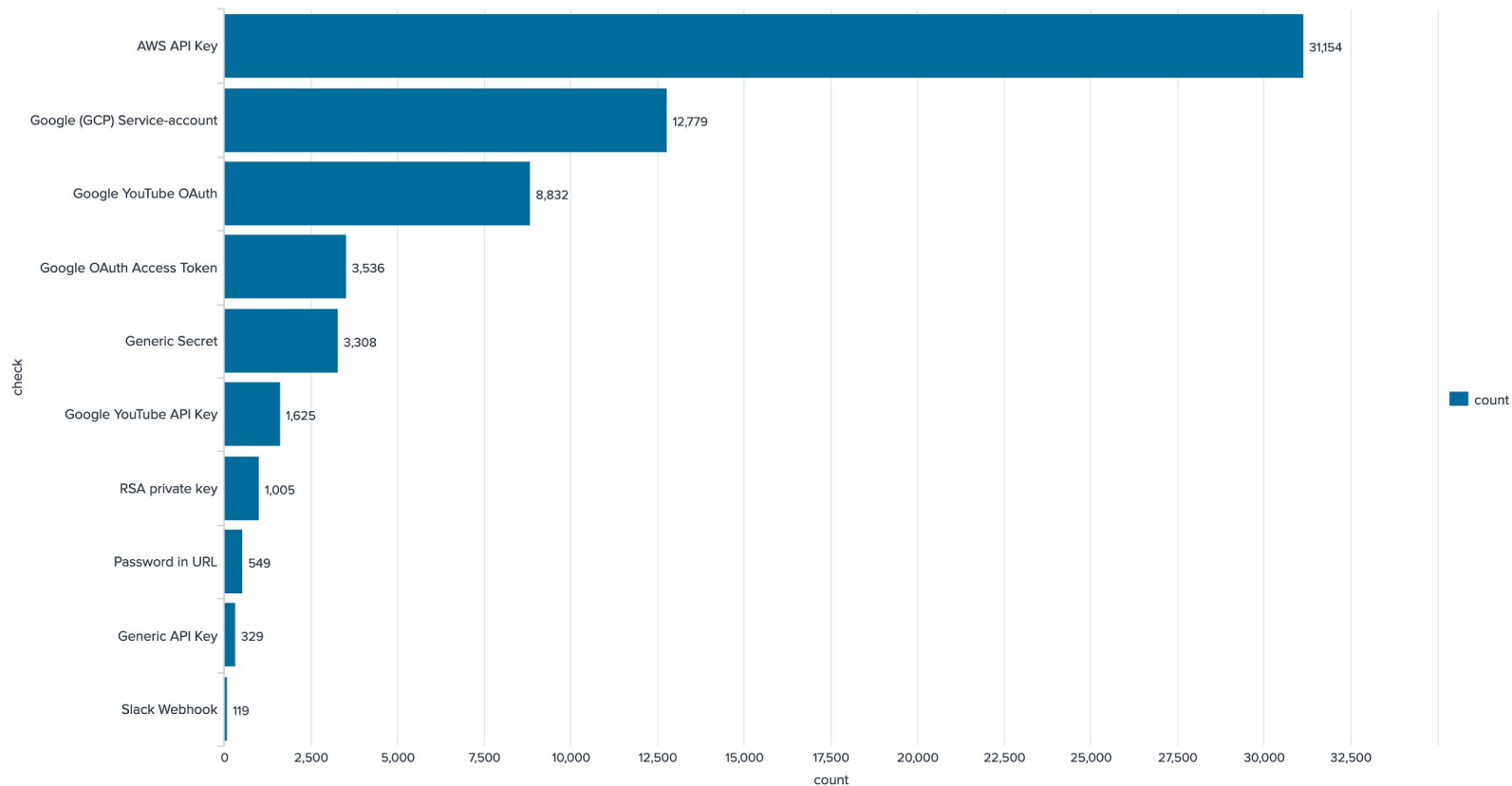
- Create temporary keys = ASIA*
- Create permanent keys = AKIA*
- Create new role trust policies or at yourself to current
- Abuse temporary tokens: sts:AssumeRole /
GetSessionToken

Demo



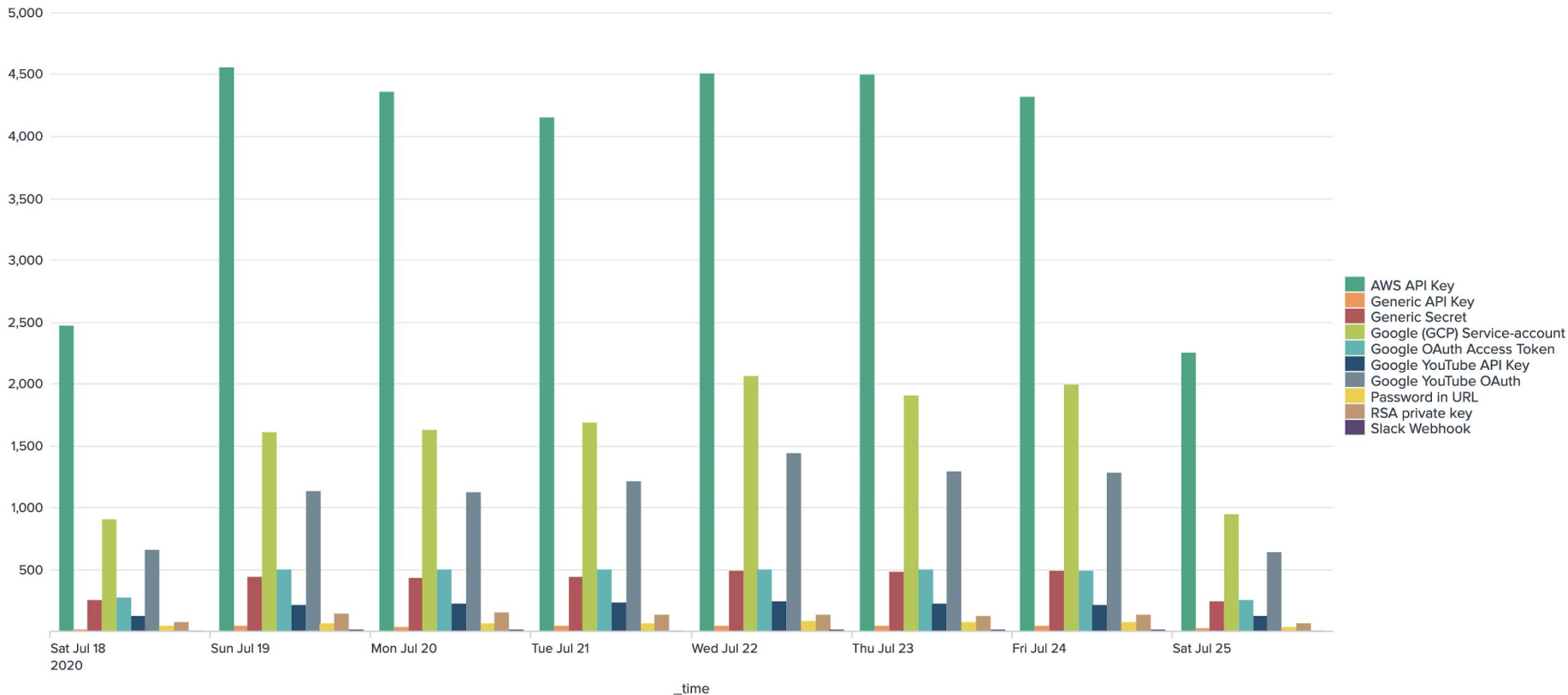
What we found - Top Leaks

Top Leaks

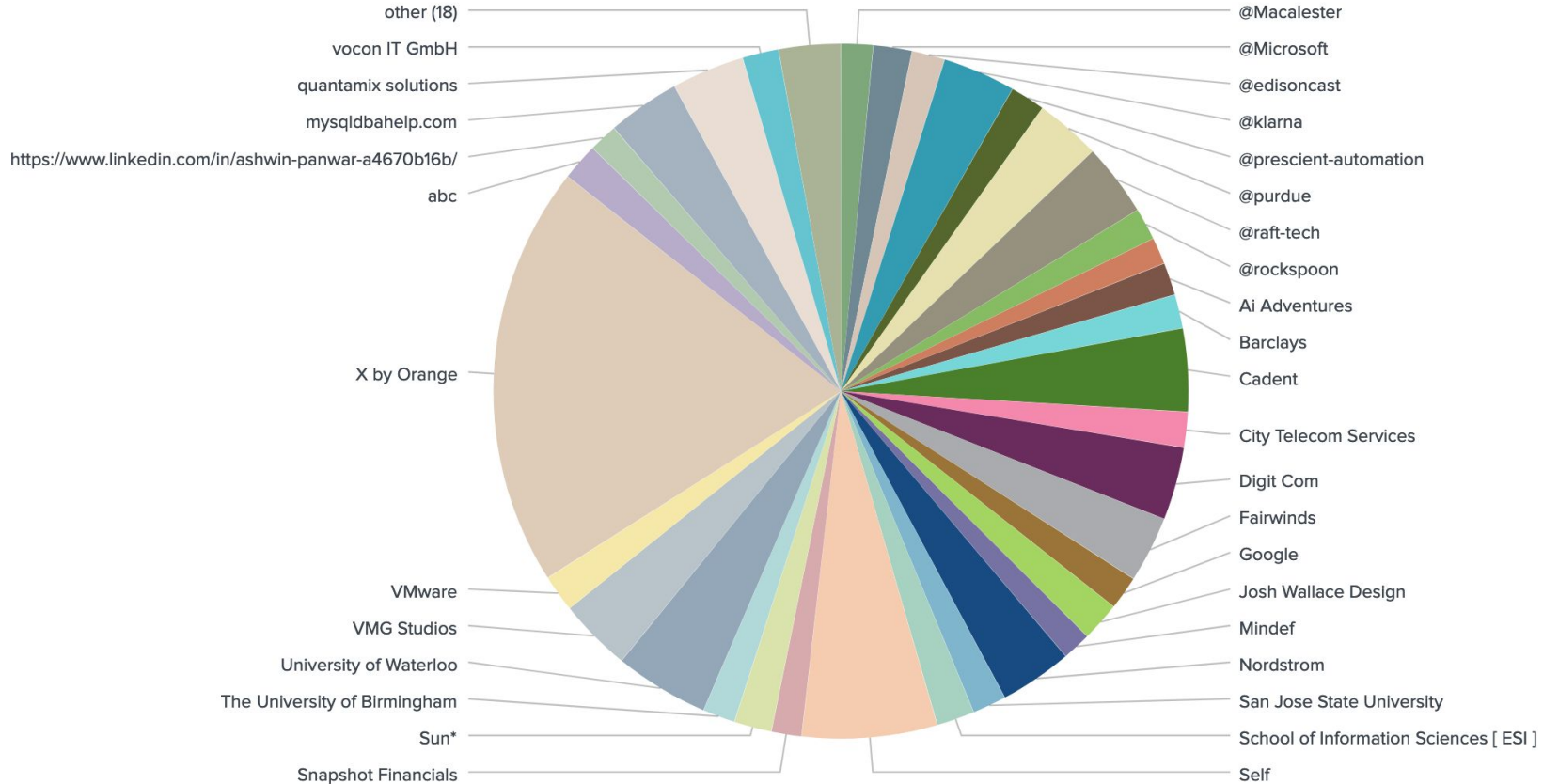


What we found - Leaks in the last 7 Days

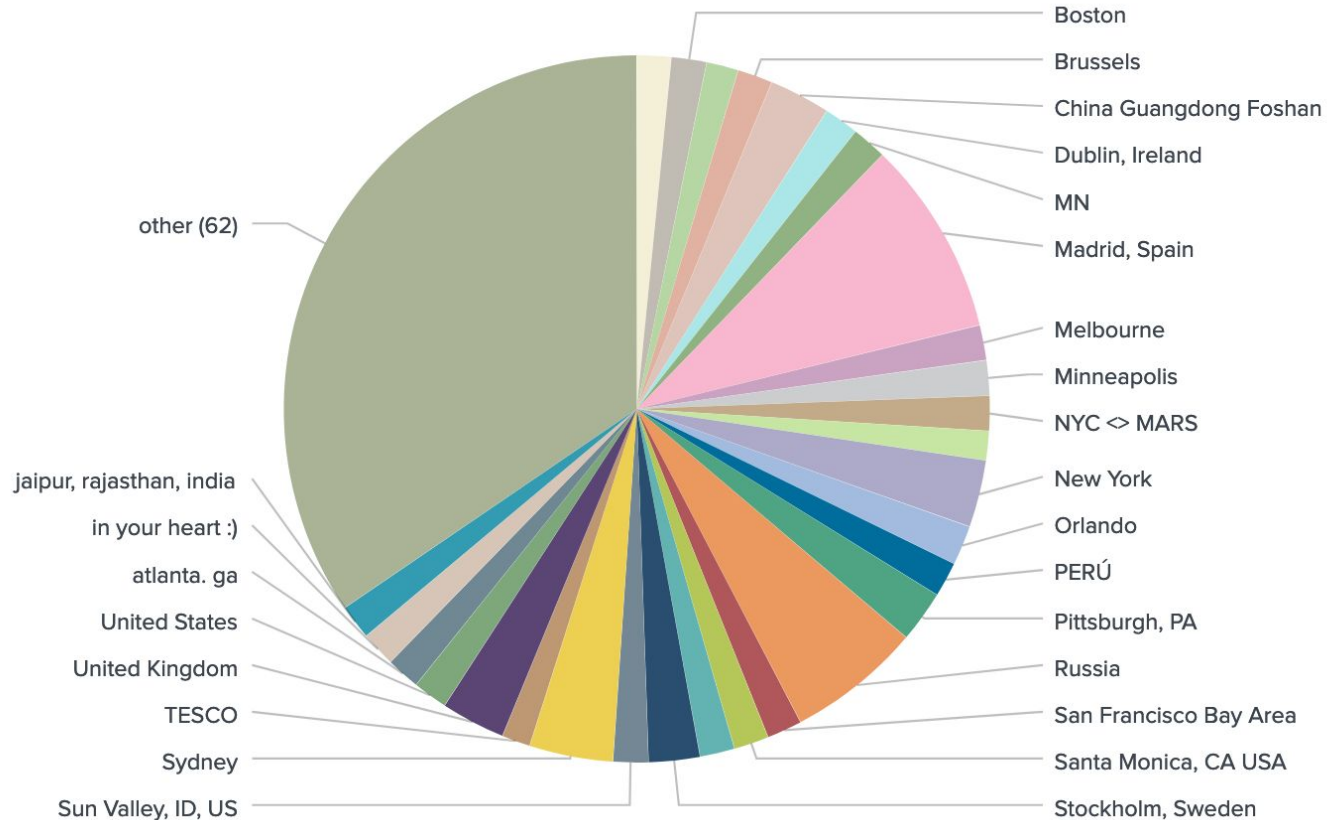
Leaks over Time



What we found - Top Companies



What we found - Top Regions




Code can get very personal...

1 lines (1 sloc) | 119 Bytes

RawBlame

1 {"cid": "180...bf.app...nt.com", "cs...t": "2"}

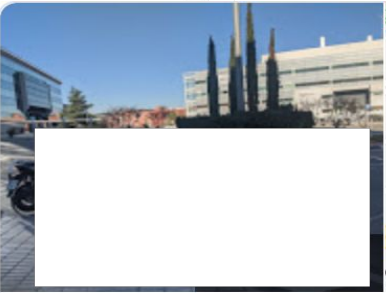


• 2nd

Chief Technology Officer

• [Contact info](#)

ConnectView in RecruiterMore...



Map data ©2020 Inst. Geogr. Naciona

DirectionsSave

3.8 ★★★★★ 24 Google reviews

Address: ()
A

Q&A

Thank you

Rod Soto @rodsoto

Jose Hernandez @d1vious