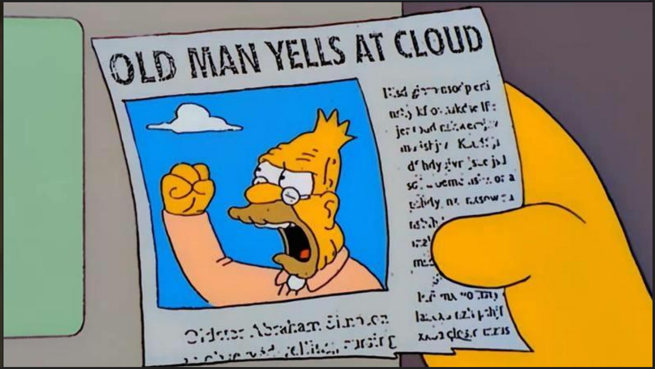
The cloud is still dark and more full of terrors

SEC-T - 0x10sion

Chris Farris
PrimeHarbor Technologies

Who Am I?

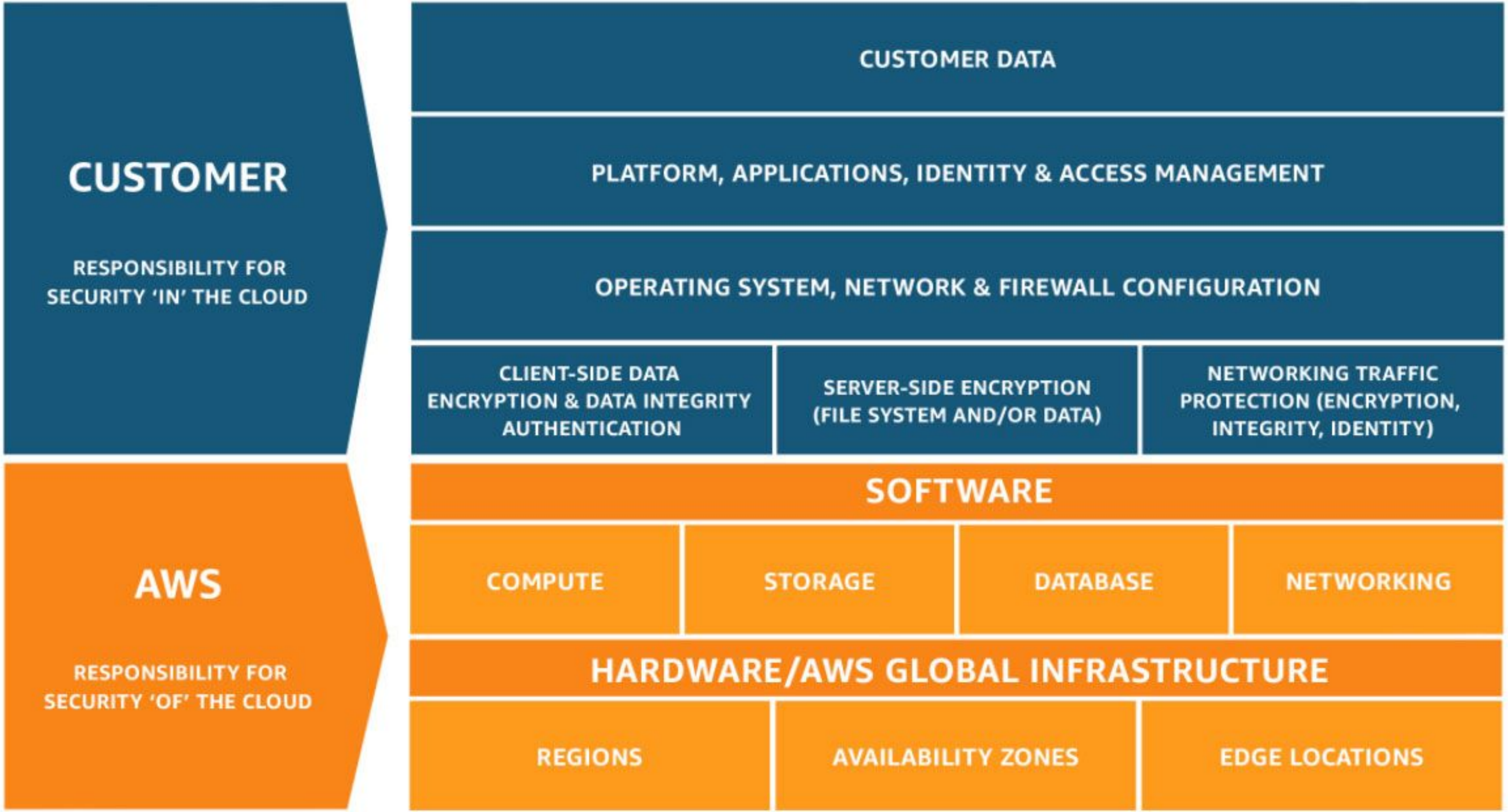
- Built the cloud security programs for some media companies
- Founder: fwd:cloudsec conference
- Rants a lot on Twitter
- Somehow was named a Security Hero by AWS
- Cloud Security Consultant



Agenda

- Major Cloud Incidents
- Themes
- Are the Cloud Providers to Blame?
- What we can do about it!

Link to the slides available at the end



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

Major Cloud Incidents

https://breaches.cloud

Code Spaces

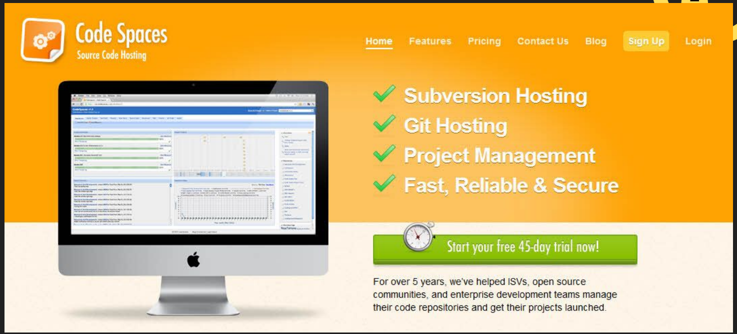
Anyone remember them?

Admin keys were leaked

Account was ransomed

Ransom wasn’t paid

Account deleted!



✓ Subversion Hosting

✓ Git Hosting

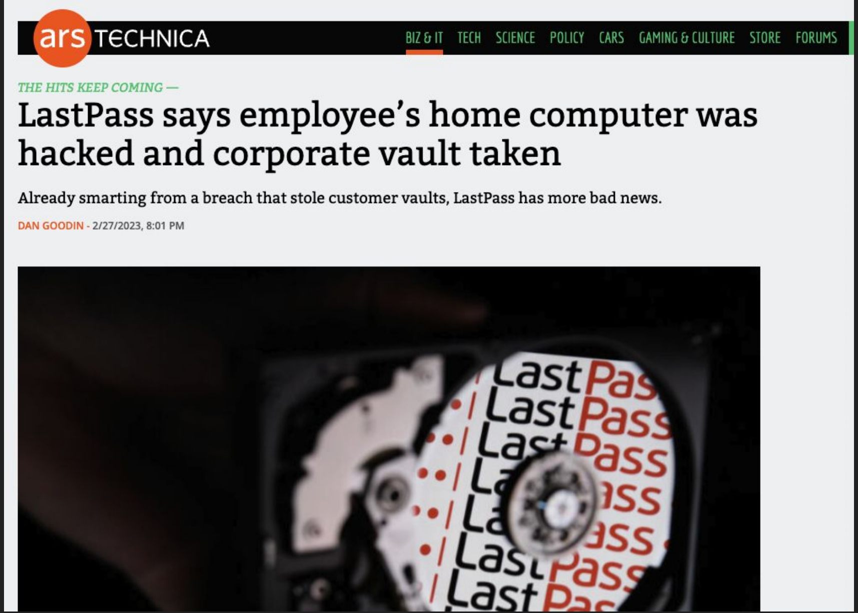
✓ Project Management

✓ Fast, Reliable & Secure

For over 5 years, we've helped ISVs, open source communities, and enterprise development teams manage their code repositories and get their projects launched.

LastPass

- Two incidents in 2022
- First was source code leak
- Second was targeted at Sr. DevOps Engineer
- Initial Access: Home Plex Server
- Client-Side encryption keys accessed
- Vaults were on-prem, but backed up to S3

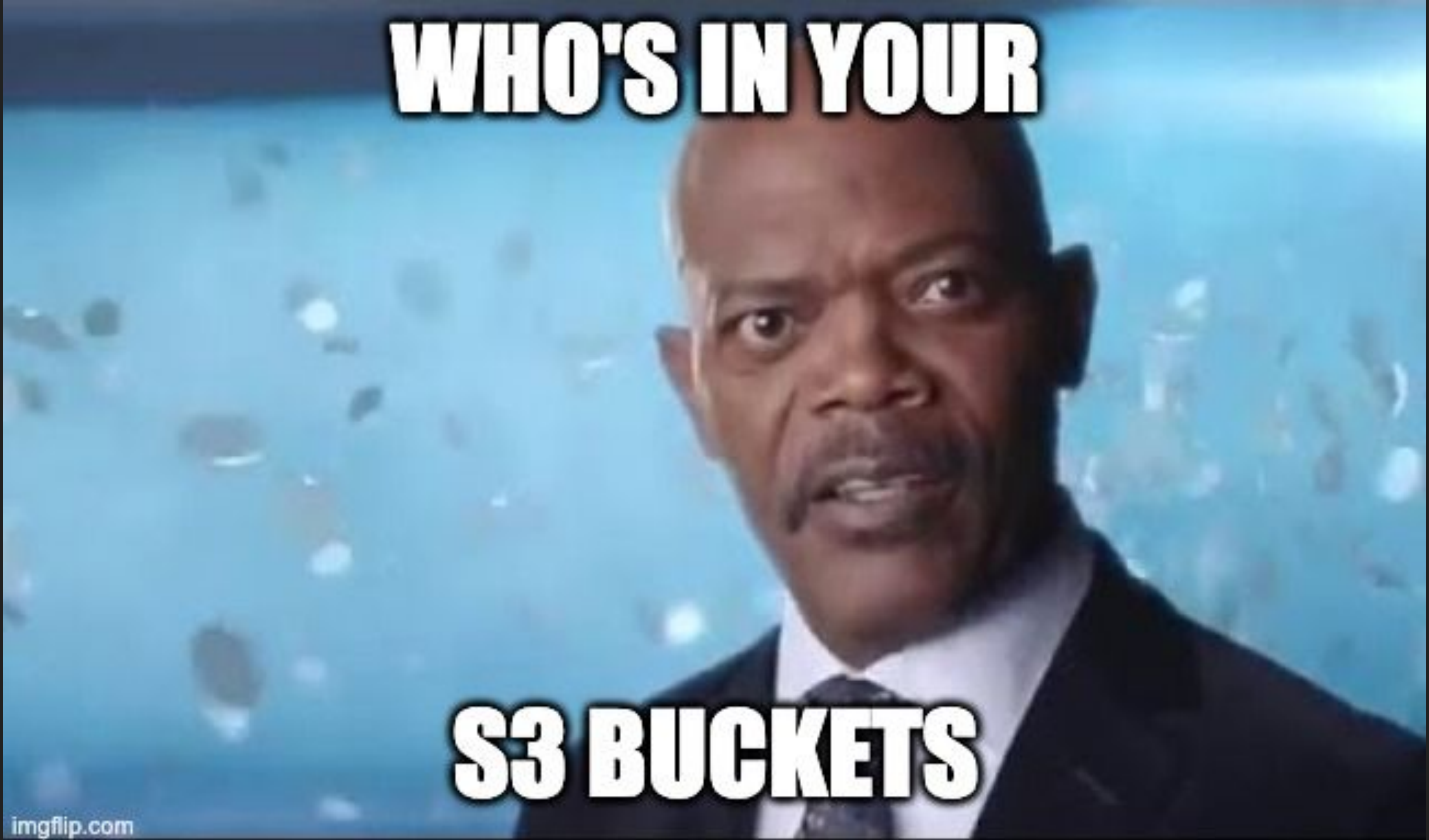


THE HITS KEEP COMING —

LastPass says employee's home computer was hacked and corporate vault taken

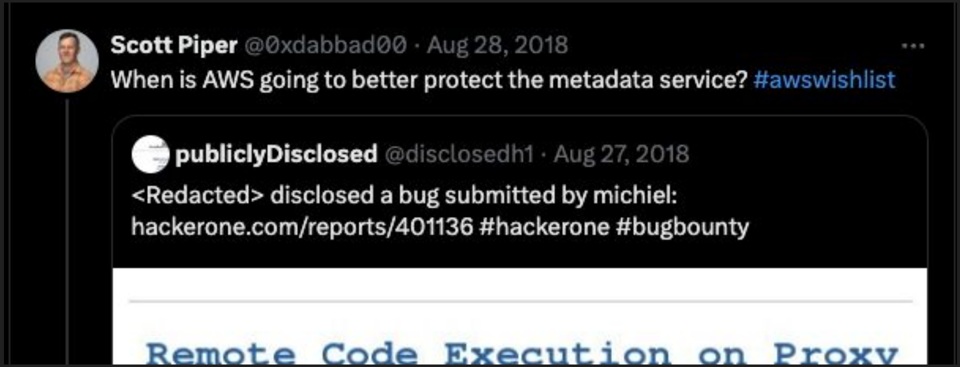
Already smarting from a breach that stole customer vaults, LastPass has more bad news.

DAN GOODIN - 2/27/2023, 8:01 PM


WHO'S IN YOUR
S3 BUCKETS
imgflip.com

Capital One - Timeline

- June 2012 - Instance Metadata Released
- 2013 - GCP Implements headers for metadata service
- 2014 - First disclosure of a IMDS attack
- 2017 - Microsoft implements headers for Azure
- 2018 - Scott Piper calls for AWS to improve IMDS security



Scott Piper @0xdabbad00 · Aug 28, 2018

When is AWS going to better protect the metadata service? #awswishlist

publiclyDisclosed @disclosedh1 · Aug 27, 2018

<Redacted> disclosed a bug submitted by michiel: hackerone.com/reports/401136 #hackerone #bugbounty

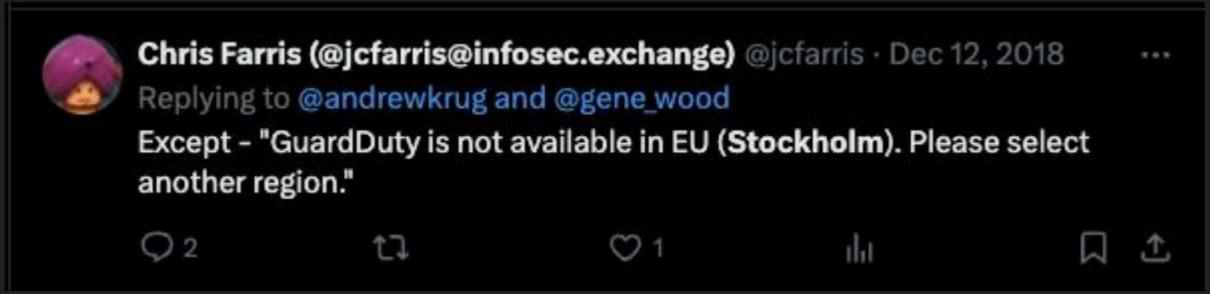
Remote Code Execution on Proxy

EC2 Metadata Abuse

```
[ec2-user@ip-10-XX-XX-234 ~]$ role_name=$( curl -s
http://169.254.169.254/latest/meta-data/iam/security-credentials/ )
[ec2-user@ip-10-XX-XX-234 ~]$ curl -s
http://169.254.169.254/latest/meta-data/iam/security-credentials/${role_name
}
{
  "Code" : "Success",
  "LastUpdated" : "2018-04-23T13:02:26Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAR5DV6JBZRSJH2ZZA",
  "SecretAccessKey" : "eEuERNfOREDACTED/9Ha0YGZ6bd",
  "Token" : "FQoDYXTHISISNOTAREALSESSIONTOKENTHISISJUSTATRIBUTEL31gU=",
  "Expiration" : "2018-04-23T19:06:48Z"
}
```

Capital One - Timeline

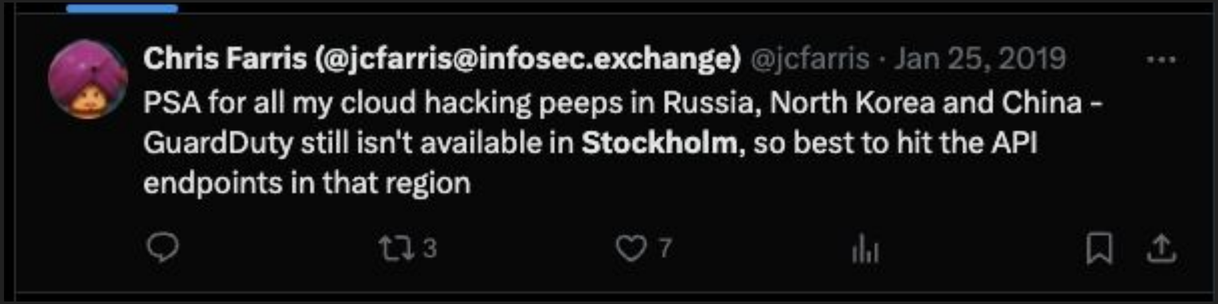
- December 2018 - eu-north-1 region (Stockholm) opened



Chris Farris (@jcfarris@infosec.exchange) @jcfarris · Dec 12, 2018

Replying to @andrewkrug and @gene_wood

Except - "GuardDuty is not available in EU (**Stockholm**). Please select another region."



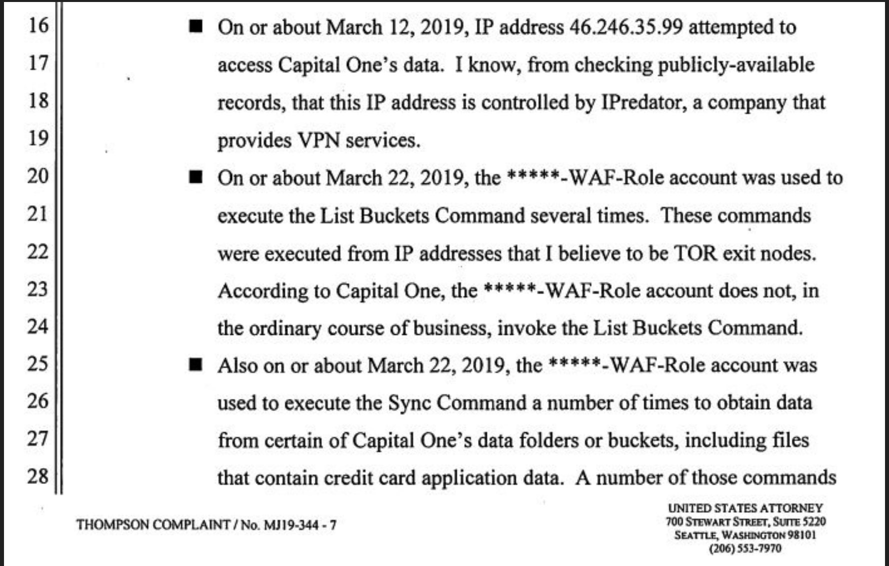
Chris Farris (@jcfarris@infosec.exchange) @jcfarris · Jan 25, 2019

PSA for all my cloud hacking peeps in Russia, North Korea and China - GuardDuty still isn't available in **Stockholm**, so best to hit the API endpoints in that region

Capital One - Timeline

March 2019

- The attacker finds “misconfigured WAF” and gains access to credentials.
- Downloads data from S3



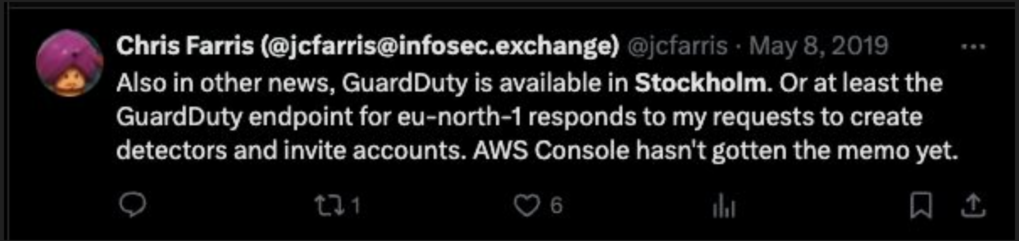
- On or about March 12, 2019, IP address 46.246.35.99 attempted to access Capital One’s data. I know, from checking publicly-available records, that this IP address is controlled by IPredator, a company that provides VPN services.
- On or about March 22, 2019, the *****-WAF-Role account was used to execute the List Buckets Command several times. These commands were executed from IP addresses that I believe to be TOR exit nodes. According to Capital One, the *****-WAF-Role account does not, in the ordinary course of business, invoke the List Buckets Command.
- Also on or about March 22, 2019, the *****-WAF-Role account was used to execute the Sync Command a number of times to obtain data from certain of Capital One’s data folders or buckets, including files that contain credit card application data. A number of those commands

THOMPSON COMPLAINT / No. MJ19-344 - 7

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Capital One - Timeline

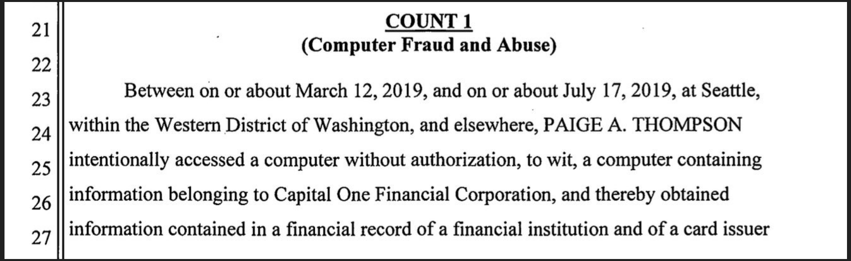
- May 2019 - GuardDuty Available in Stockholm Region



Chris Farris (@jcfarris@infosec.exchange) @jcfarris · May 8, 2019

Also in other news, GuardDuty is available in **Stockholm.** Or at least the GuardDuty endpoint for eu-north-1 responds to my requests to create detectors and invite accounts. AWS Console hasn't gotten the memo yet.

- July 2019 - Indictment issued, Capital One disclosed breach

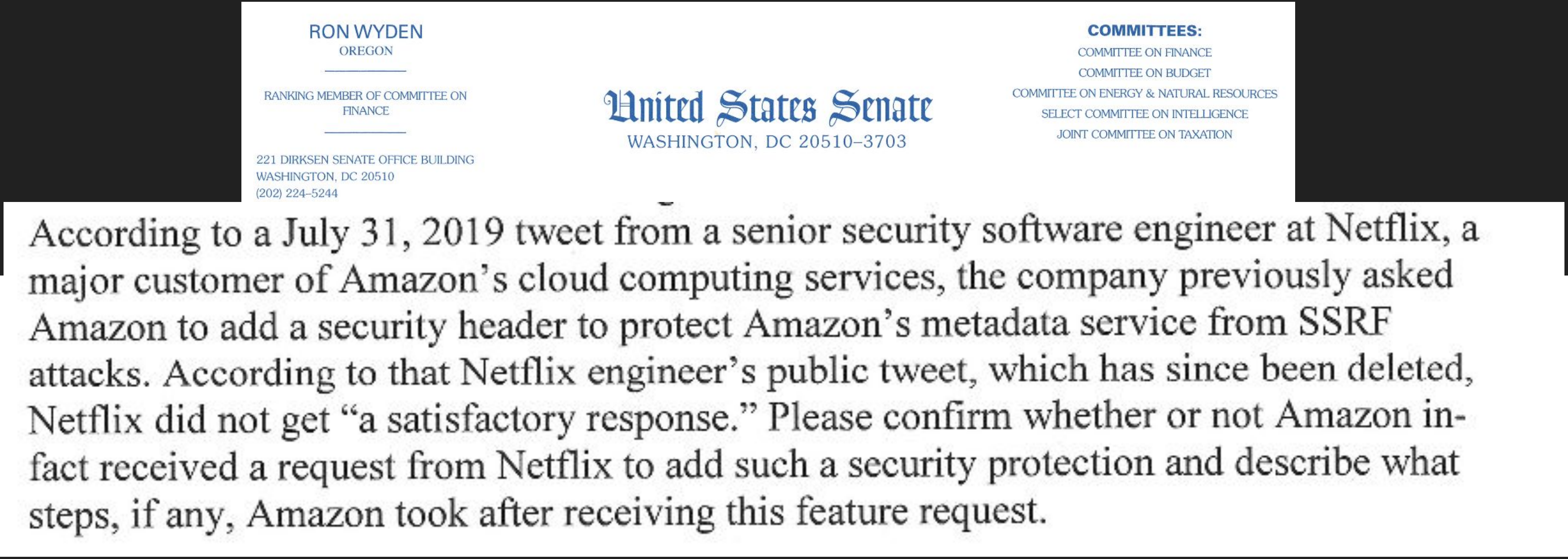


COUNT 1
(Computer Fraud and Abuse)

Between on or about March 12, 2019, and on or about July 17, 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON intentionally accessed a computer without authorization, to wit, a computer containing information belonging to Capital One Financial Corporation, and thereby obtained information contained in a financial record of a financial institution and of a card issuer

Capital One - Timeline

- August 2019 - Senator Wyden gets involved



RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224–5244

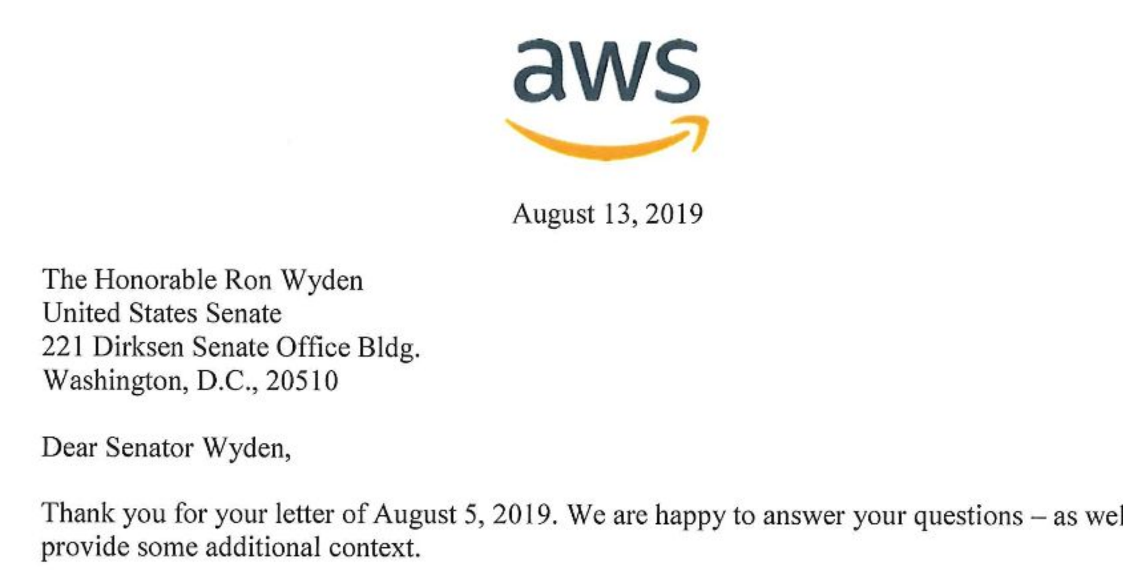
United States Senate
WASHINGTON, DC 20510–3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

According to a July 31, 2019 tweet from a senior security software engineer at Netflix, a major customer of Amazon's cloud computing services, the company previously asked Amazon to add a security header to protect Amazon's metadata service from SSRF attacks. According to that Netflix engineer's public tweet, which has since been deleted, Netflix did not get "a satisfactory response." Please confirm whether or not Amazon in-fact received a request from Netflix to add such a security protection and describe what steps, if any, Amazon took after receiving this feature request.

Capital One - Timeline

- August 2019 - AWS places all blame on Capital One

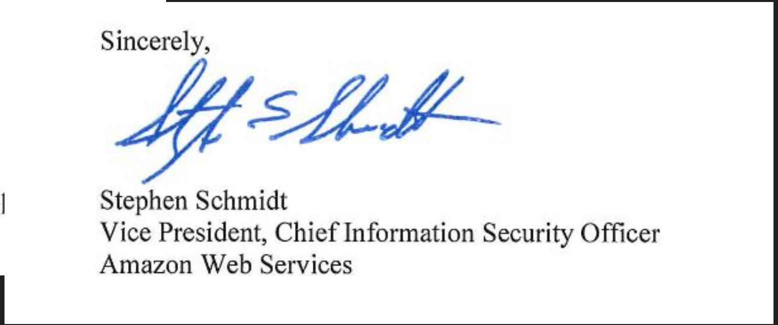


August 13, 2019

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Bldg.
Washington, D.C., 20510

Dear Senator Wyden,

Thank you for your letter of August 5, 2019. We are happy to answer your questions – as wel
provide some additional context.

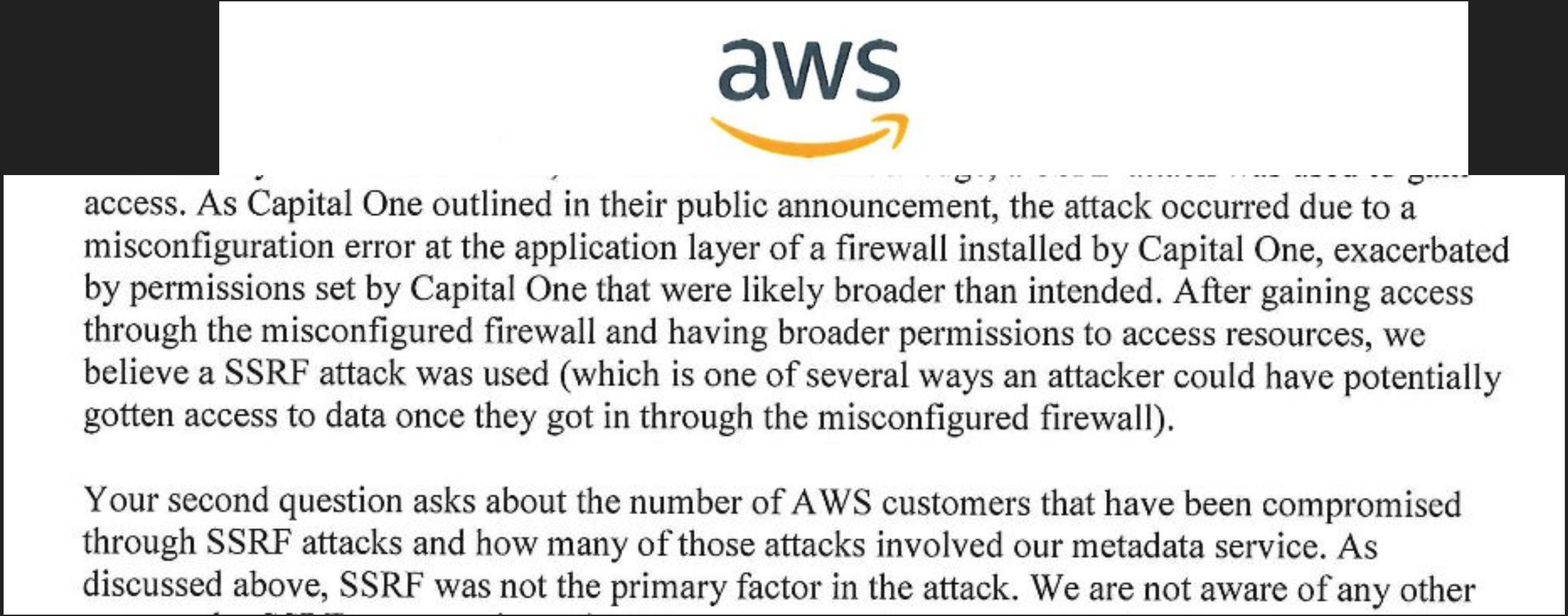


Sincerely,

Stephen Schmidt
Vice President, Chief Information Security Officer
Amazon Web Services

Capital One - Timeline

- August 2019 - AWS places all blame on Capital One

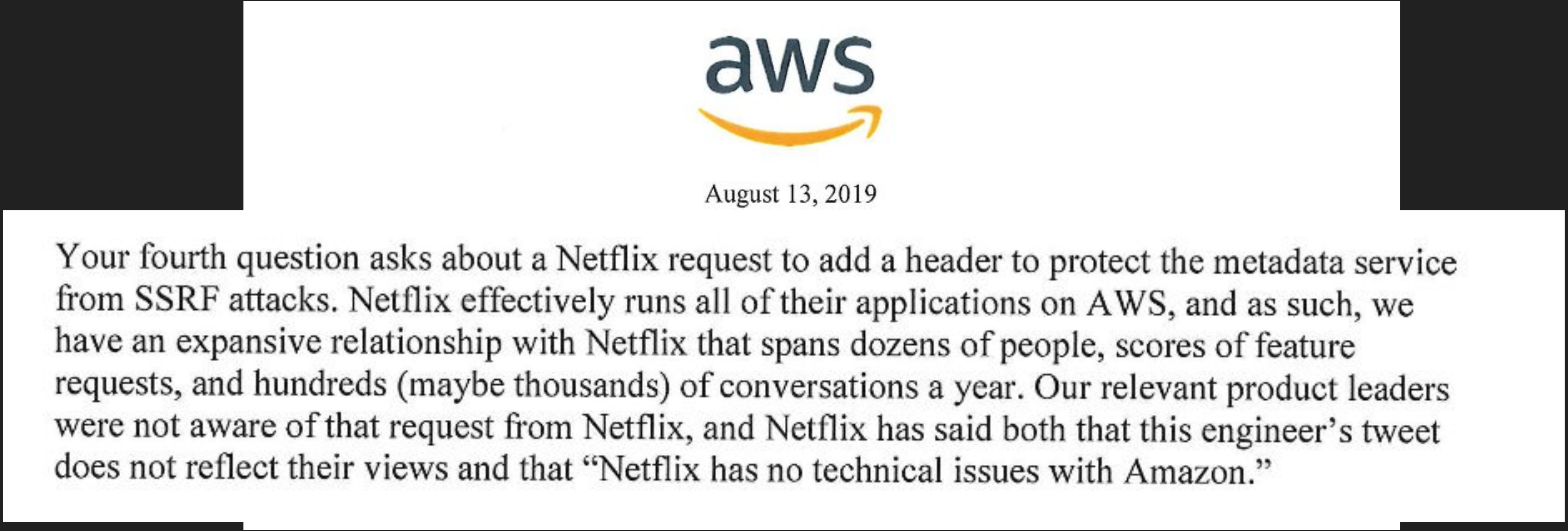


access. As Capital One outlined in their public announcement, the attack occurred due to a misconfiguration error at the application layer of a firewall installed by Capital One, exacerbated by permissions set by Capital One that were likely broader than intended. After gaining access through the misconfigured firewall and having broader permissions to access resources, we believe a SSRF attack was used (which is one of several ways an attacker could have potentially gotten access to data once they got in through the misconfigured firewall).

Your second question asks about the number of AWS customers that have been compromised through SSRF attacks and how many of those attacks involved our metadata service. As discussed above, SSRF was not the primary factor in the attack. We are not aware of any other

Capital One - Timeline

- August 2019 - AWS places all blame on Capital One



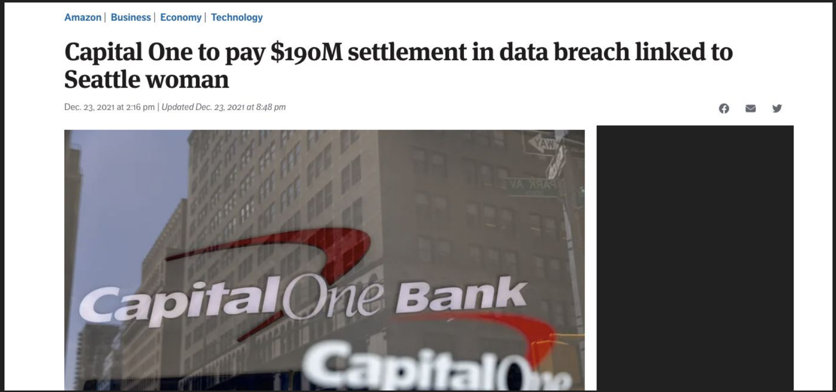
aws

August 13, 2019

Your fourth question asks about a Netflix request to add a header to protect the metadata service from SSRF attacks. Netflix effectively runs all of their applications on AWS, and as such, we have an expansive relationship with Netflix that spans dozens of people, scores of feature requests, and hundreds (maybe thousands) of conversations a year. Our relevant product leaders were not aware of that request from Netflix, and Netflix has said both that this engineer's tweet does not reflect their views and that "Netflix has no technical issues with Amazon."

Capital One - Timeline

- November 19th, 2019 - AWS introduced IMDSv2
  - 113 days after the incident
- September 2022 - Class action lawsuit settled for $190M



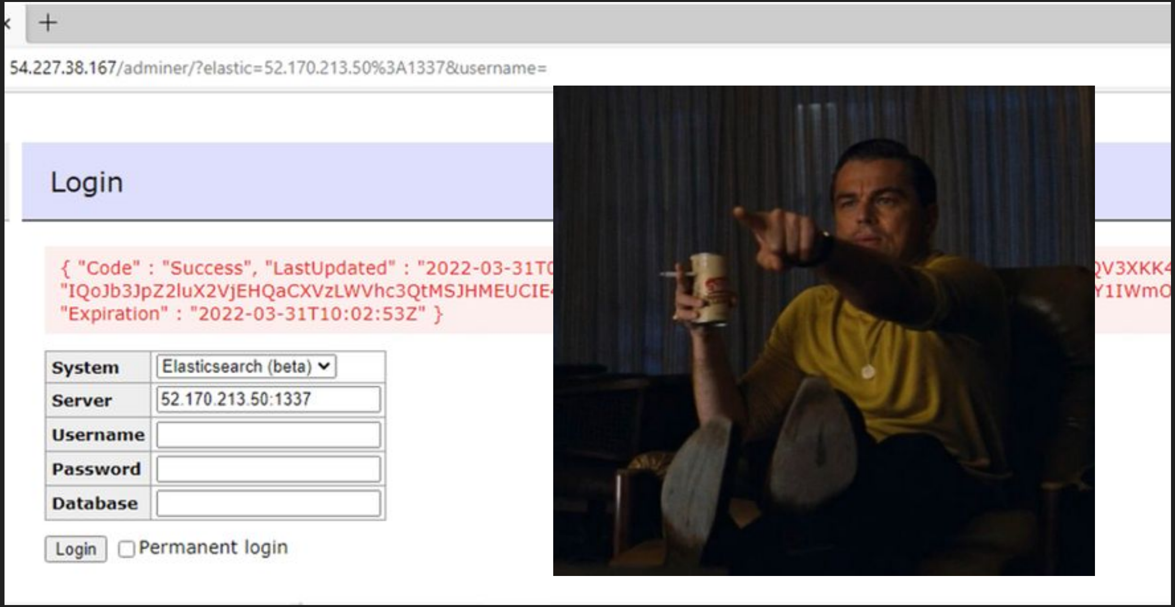
Amazon | Business | Economy | Technology

Capital One to pay $190M settlement in data breach linked to Seattle woman

Dec. 23, 2021 at 2:16 pm | *Updated Dec. 23, 2021 at 8:48 pm*

UNC2903

- Public Server with CVE-2021-21311
- Victim unknown
- IMDSv1
- S3FullAccess



54.227.38.167/adminer/?elastic=52.170.213.50%3A1337&username=

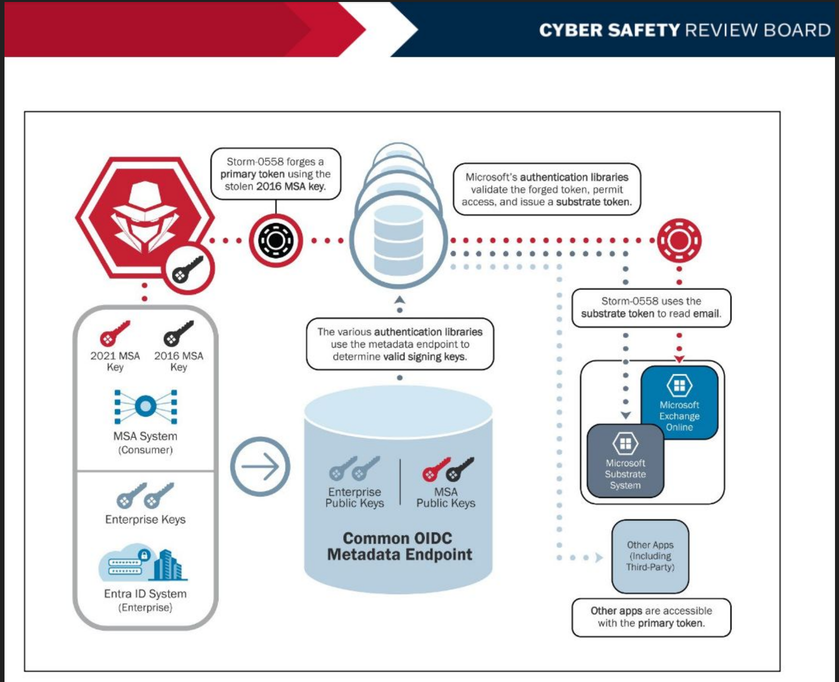
Login

```
{ "Code" : "Success", "LastUpdated" : "2022-03-31T0          QV3XKK4
"IQoJb3JpZ2luX2VjEHQaCXVzLWVhc3QtMSJHMEUCIE4          Y1IWmO
"Expiration" : "2022-03-31T10:02:53Z" }
```

System	Elasticsearch (beta)
Server	52.170.213.50:1337
Username	
Password	
Database	

Microsoft - Storm-0558

- 2016 Consumer MSA Key
  - still used in 2023
- Failed to validate key purpose
- Failed to detect the intrusion
- Failed to figure out how the 2016 key was compromised


CYBER SAFETY REVIEW BOARD
2021 MSA Key
2016 MSA Key
MSA System (Consumer)
Enterprise Keys
Entra ID System (Enterprise)
Enterprise Public Keys
MSA Public Keys
Common OIDC Metadata Endpoint
Microsoft Exchange Online
Microsoft Substrate System
Other Apps (Including Third-Party)

Storm-0558 forges a primary token using the stolen 2016 MSA key.

Microsoft's authentication libraries validate the forged token, permit access, and issue a substrate token.

The various authentication libraries use the metadata endpoint to determine valid signing keys.

Storm-0558 uses the substrate token to read email.

Other apps are accessible with the primary token.

Figure 1: Storm-0558 Token Abuse with Stolen 2016 MSA Key

Microsoft - Storm-0558 - Detection

- Found by US State Department
- They had G5 Licensing
- “Big Yellow Taxi” rule
    - MailItemsAccessed
- State Dept notified Microsoft
- MS discovered access signed by the consumer MSA Key

© 2024 PrimeHarbor Technologies, LLC

The Board identified a series of Microsoft operational and strategic decisions that collectively point to a corporate culture that deprioritized both enterprise security investments and rigorous risk management.

– Cyber Safety Review Board
March, 2024

Microsoft - Storm-0558

Meme of unknown origin

Microsoft - Midnight Blizzard

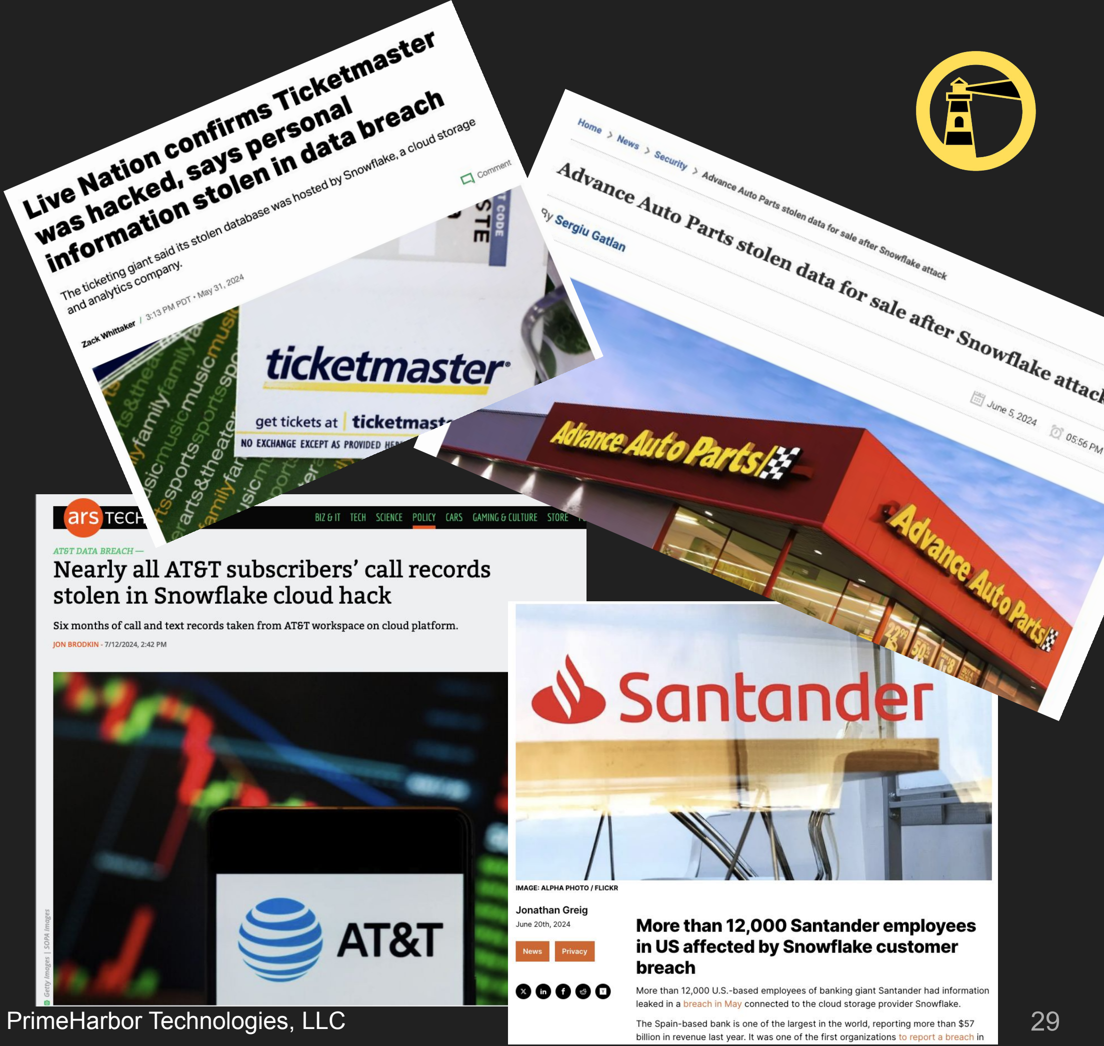
- Russian SVR
- Test User in Test Tenant
- Self Enrollment Abuse
- Cloud-Plane lateral movement
- Most Narcissistic objective ever

"two cozy bears in a midnight blizzard" (DALL-E 2)

Snowflake

Victims

- TicketMaster
- Santander
- Lending Tree
- AT&T
- Advanced Auto Parts



Live Nation confirms Ticketmaster was hacked, says personal information stolen in data breach

The ticketing giant said its stolen database was hosted by Snowflake, a cloud storage and analytics company.

Zack Whittaker / 3:13 PM PDT • May 31, 2024

Comment

Home > News > Security > Advance Auto Parts stolen data for sale after Snowflake attack

Advance Auto Parts stolen data for sale after Snowflake attac

By Sergiu Gatlan

June 5, 2024 05:56 PM

ars TECH

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

AT&T DATA BREACH —

Nearly all AT&T subscribers' call records stolen in Snowflake cloud hack

Six months of call and text records taken from AT&T workspace on cloud platform.

JON BRODKIN - 7/12/2024, 2:42 PM

Getty Images | SOPA Images

IMAGE: ALPHA PHOTO / FLICKR

Jonathan Greig

June 20th, 2024

News Privacy

More than 12,000 Santander employees in US affected by Snowflake customer breach

More than 12,000 U.S.-based employees of banking giant Santander had information leaked in a breach in May connected to the cloud storage provider Snowflake.

The Spain-based bank is one of the largest in the world, reporting more than $57 billion in revenue last year. It was one of the first organizations to report a breach in

Snowflake

Infostealers
Lots of Personal Data
No MFA!
No MFA?
imgflip.com

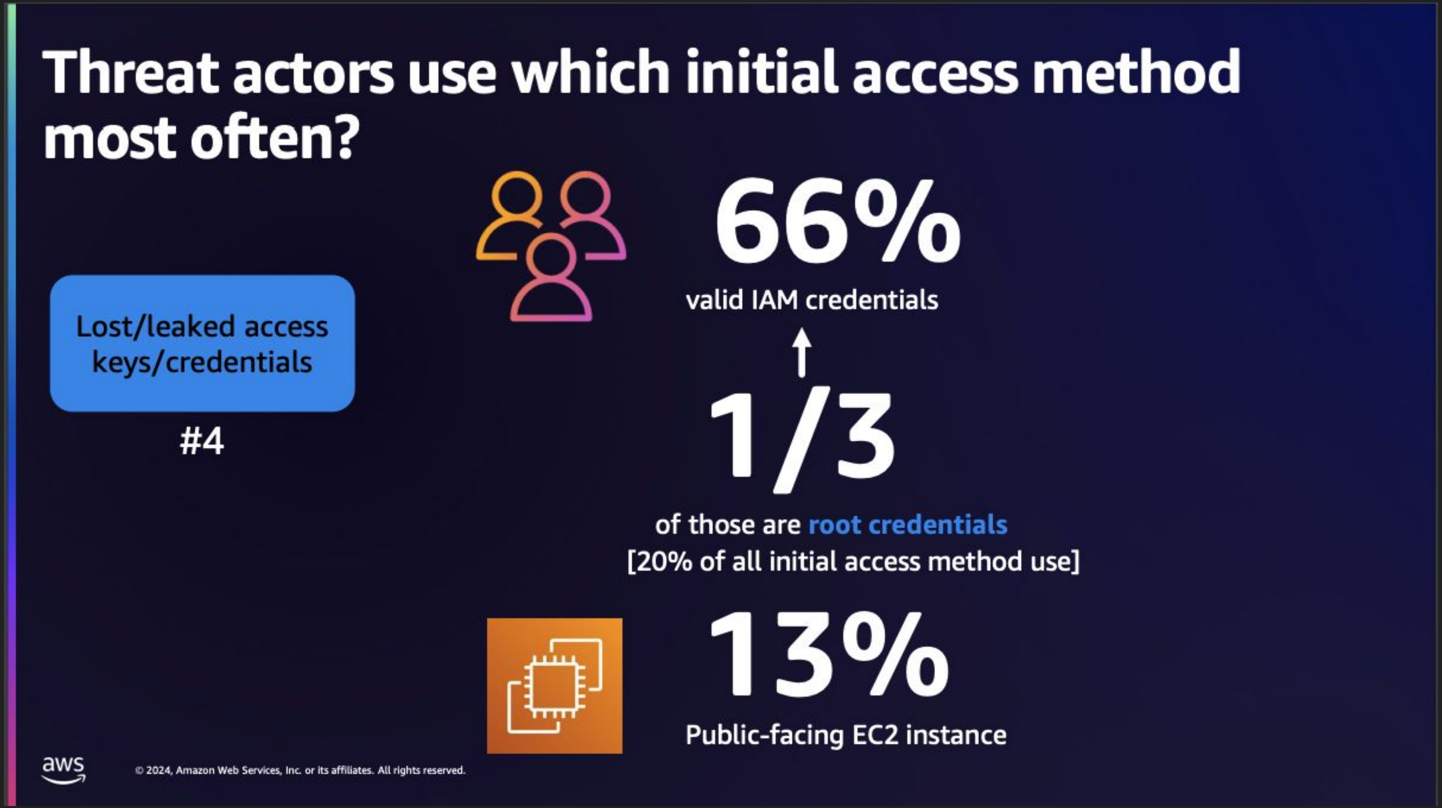
Themes

Threat Actors have ***Objectives*** against ***Targets*** using ***Attack Vectors***

Attack Vectors

1. Lost, stolen, or exposed credentials
2. Publicly exposed resources
3. Credentials exposed via application security flaws
4. Unpatched vulnerabilities and 0-days in exposed systems
5. Denial of Service attacks
6. Subdomain takeover
7. Supply chain compromise

AWS Customer Incident Response Team



Threat actors use which initial access method most often?

Lost/leaked access keys/credentials

#4

66%

valid IAM credentials

↑

1/3

of those are **root credentials**

[20% of all initial access method use]

13%

Public-facing EC2 instance

Are the cloud providers to blame?

YES

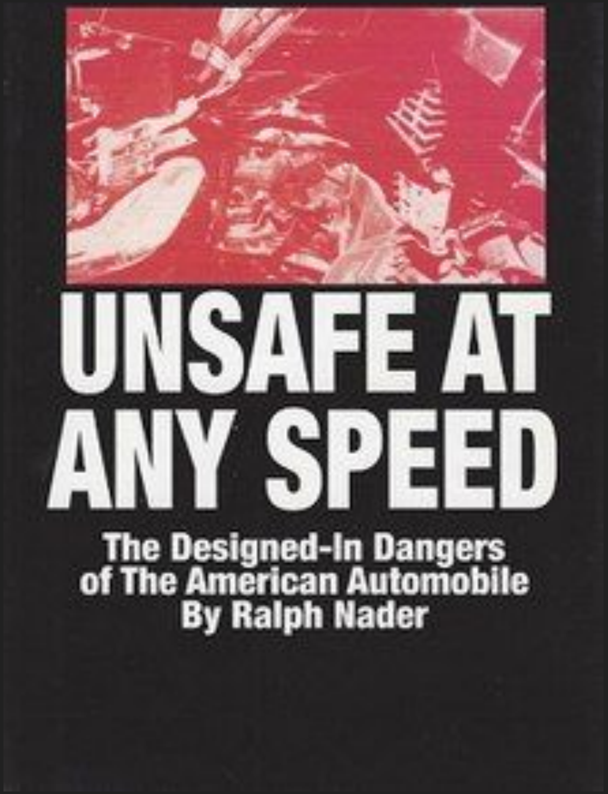
NOT

SECURITY IS JOB ZERO

Side from SEC201 - re:invent 2014

It’s time to demand more from the cloud providers

Or it's time for Governments to step in



UNSAFE AT ANY SPEED

The Designed-In Dangers of The American Automobile

By Ralph Nader

- @jcfarris
- https://github.com/jchrisfarris
- https://www.linkedin.com/in/jcfarris
- http://www.chrisfarris.com

https://chrisfarris.com/sect2024
https://breaches.cloud