

/Users/kirill/Downloads/\_0003\_malicious\_ip\_00000000000000000000000000000000

Default (curl)

# Data Breach Trends and Outlook

ATED ICT Ticino, AIEA, ISACA Switzerland Chapter, ISACA Milan Chapter in collaboration with SUPSI

Balazs Greksza



# kali:~ whoami Balazs Greksza

Threat Response Lead @ Open Systems

<https://www.linkedin.com/in/bgreksza/>

<https://github.com/inverzeio/talks>

[https://twitter.com/inverze\\_io](https://twitter.com/inverze_io)

~11 Exams / Certs(most expired): DevSecOps, Containers, Malware, DFIR, Sec Management & Auditing

Cavern Diving, 3D Printing, Hardware security, CTFs (mostly Forensics, Malware), Tennis, Hiking, Chess

Opinions are mine, and do not represent the view of my employer or others





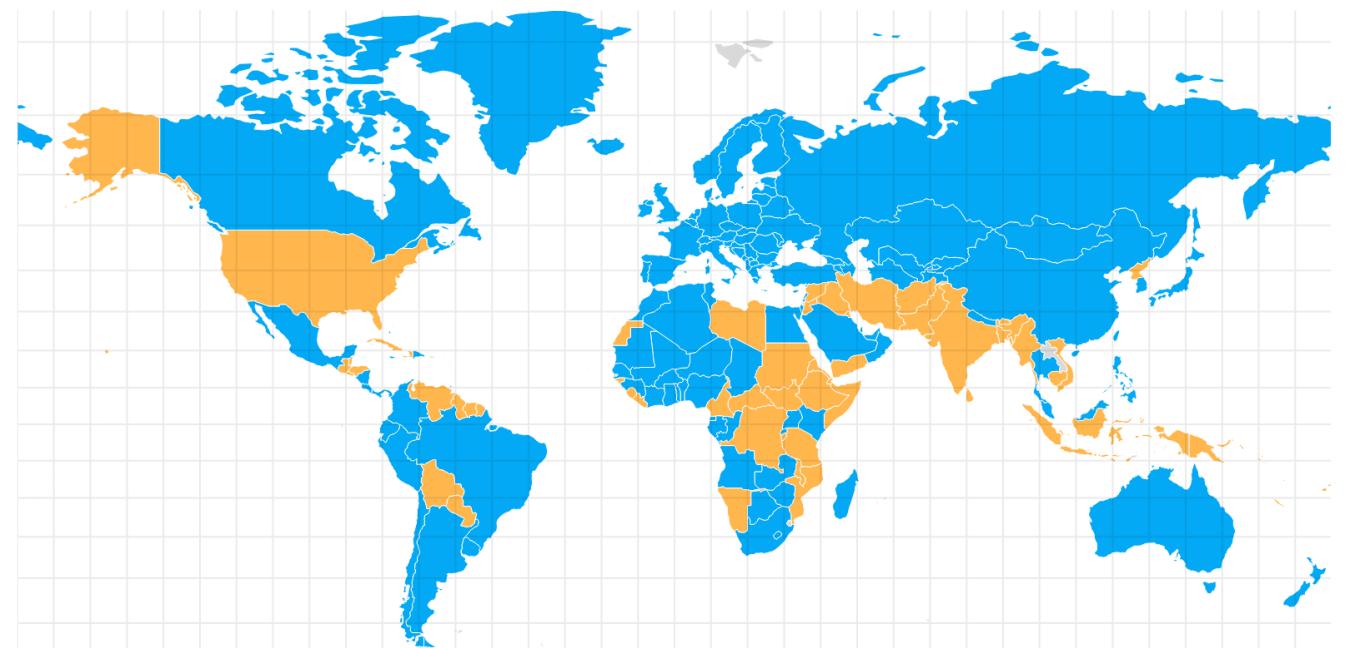
Why does it matter?



# Data Protection Regulations

Data Protection Law

Sectoral Coverage or No Data Protection

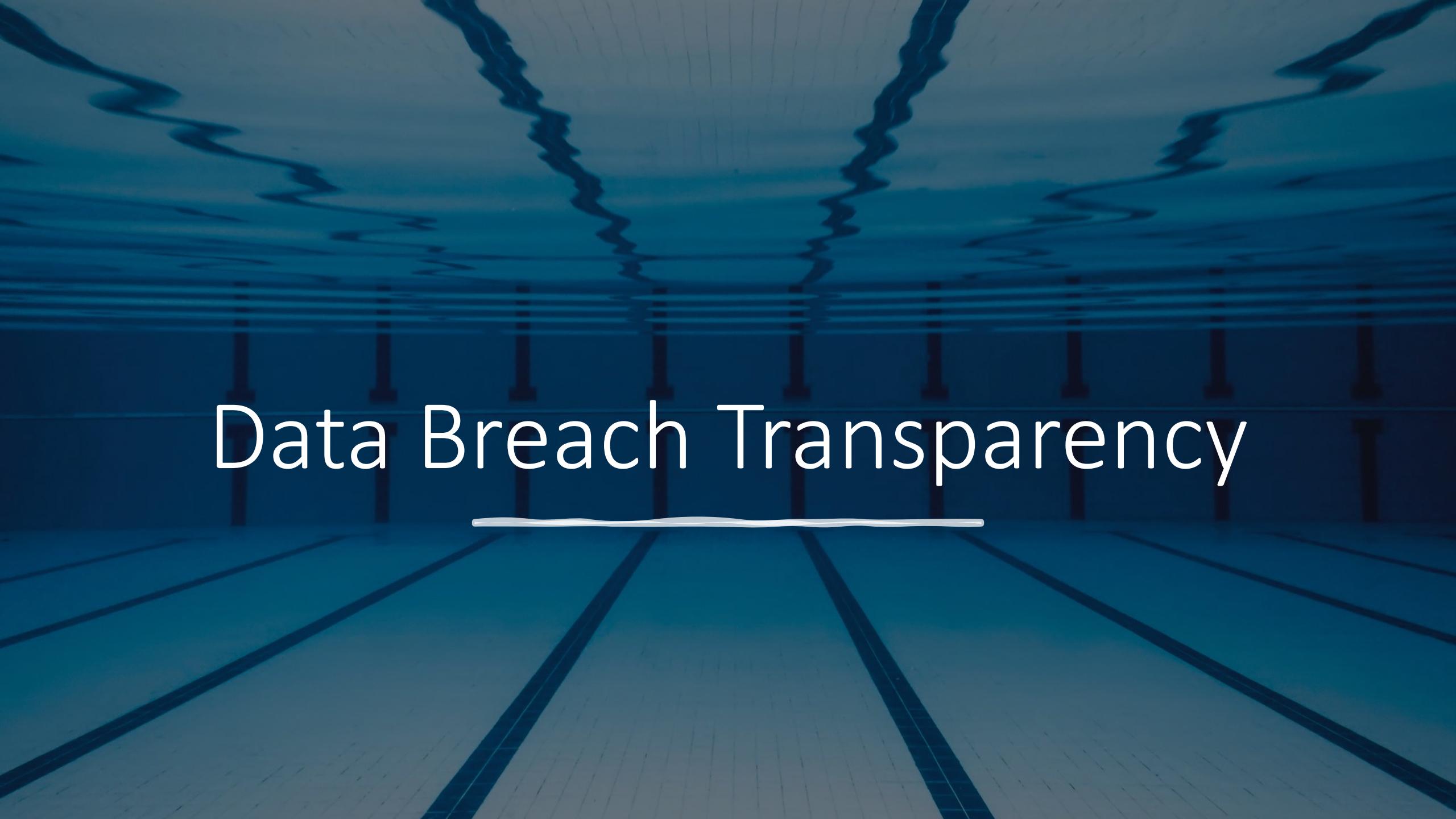




# The individual right to Privacy

"Privacy is the right to a free mind, (...) Without privacy, you can't have anything for yourself. Saying you don't care about privacy because you have nothing to hide is like saying you don't care about free speech because you have nothing to say."

– Edward Snowden



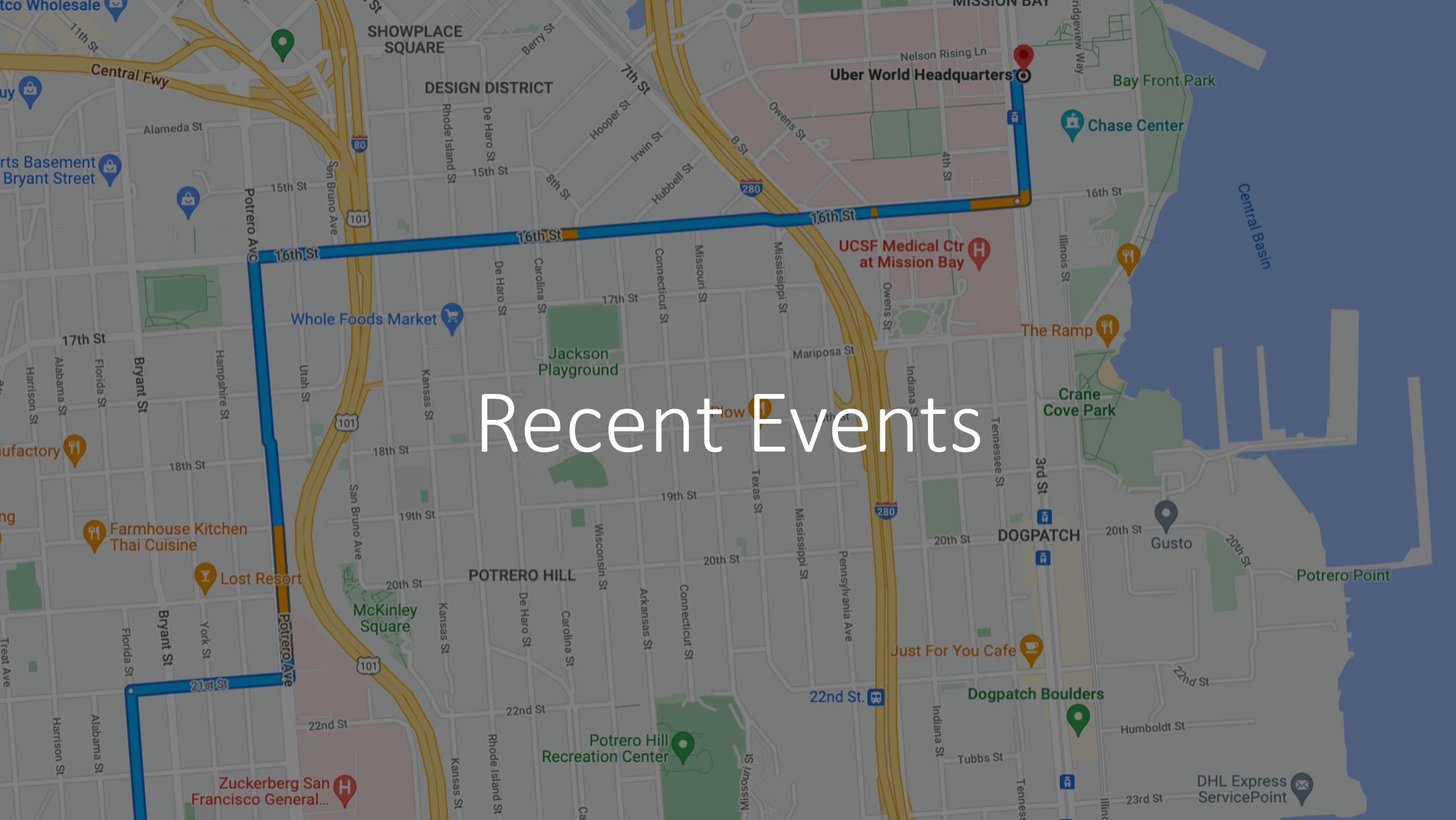
# Data Breach Transparency

---



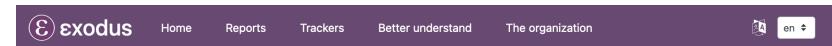
# Sharing, but how much?

# Recent Events





# Data Processing



5 trackers

Version 4.451.10003 - see other versions

Source: Google Play

Report created on Dec. 12, 2022, 10:46 p.m.

Uber

32 permissions

See on Google Play >

5 trackers

We have found code signature of the following trackers in the application:

Facebook Fliper >

(analytics)

Google AdMob >

(advertisement)

Google CrashLytics >

(crash reporting)

Google Firebase Analytics >

(analytics)

Uber Analytics >

(analytics)

A tracker is a piece of software meant to collect data about you or your usages. [Learn more](#)

32 permissions

We have found the following permissions in the application:

Let's Start with creating your account

First Name

Last Name

Email Address

Phone Number

+4

Password  
Enter your password

Show

City  
Enter your city



# Techniques

- Getting credentials via Phishing and accessing VPN via MFA exhaustion
- PowerShell Script with hardcoded credentials for PAM
- Using Intranet to search targets
- Thycotic PAM storing cloud credentials and API keys for AWS, Gsuite, DUA, Onelogin.
- Customer Information and Internal Documents are accessed



# Impact

- AWS Cloud admin access
- Google Cloud admin access
- VMware vSphere admin access
- Windows environments admin access
- Vulnerability Database access(bug bounty program managed by HackerOne)
- Duo Authenticator
- OneLogin IAM
- Access to Uber sales metrics
- Access to company-wide used Slack messenger
- Information about the endpoint detection and response (EDR) platform
- Reconfigured Uber's OpenDNS (internal defacement)
- -5.5% Share price (~3\$ billion , value hasn't recovered)



# Communication

Tea Pot  
last seen just now

ok so basically uber had a network share W:\ [REDACTED] lots. the share contained some powershell scripts.

one of the powershell scripts contained the username and password for a admin user in Thycotic (PAM) Using this i was able to extract secrets for all services, DA, DUO, Onelogin, AWS, GSuite

on an uber IP range? or v.v.v.v like GCP or AWS (\*.uberinternal)

in Uber intranet

\*.corp.uber.com

How'd you get access to the intranet then?

SE an employee -> access VPN -> scan intranet?

yes!

exactly

(I was spamming employee with push auth for over a hour) i then contacted him on WhatsApp and claimed to be from Uber IT, told him if he wants it to stop he must accept it

6:47 PM

And well, he accepted and I added my device

6:47 PM



From an Uber employee:

Feel free to share but please don't credit me: at Uber, we got an "URGENT" email from IT security saying to stop using Slack. Now anytime I request a website, I am taken to a REDACTED page with a pornographic image and the message "F\*\*\* you wankers."



Nwave  
Hi @here

I announce i am a hacker and uber has suffered a data breach.

Slack has been stolen, confidential data with Confluence, stash and 2 monorepos from phabricator have also been stolen, along with secrets from sneakers.

@Twitter | Berunderpaisdrives



Uber Comms ✅  
@Uber\_Comms

We are currently responding to a cybersecurity incident. We are in touch with law enforcement and will post additional updates here as they become available.

[Tweet](#) [Übersetzen](#)

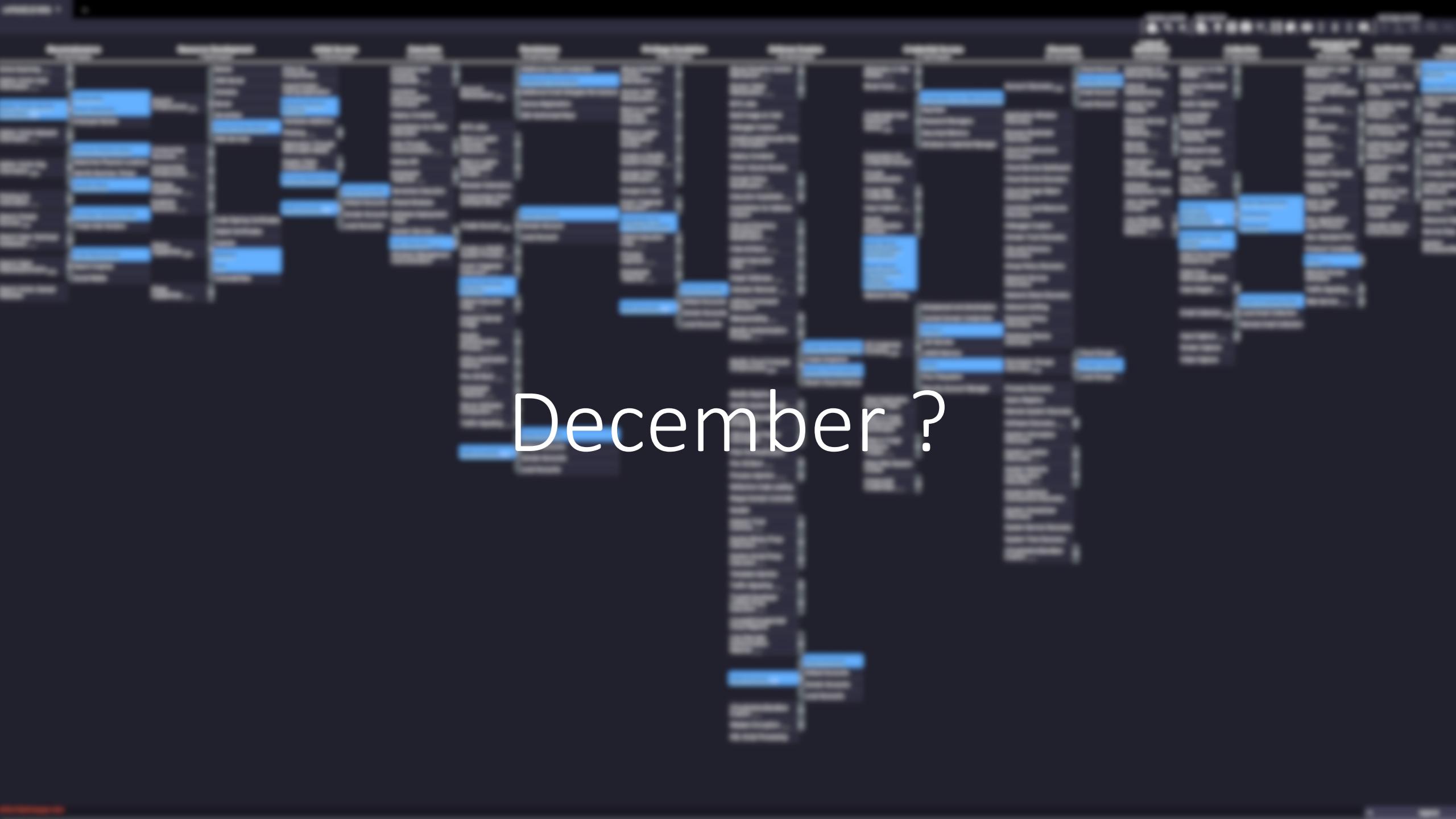
3:25 vorm. · 16. Sep. 2022 · Twitter Web App

...



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/7)	Drive-by Compromise	Command and Scripting Interpreter (0/5)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/3)	Account Access Removal	
Gather Victim Host Information (0/4)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Application Window Discovery	Communication Through Removable Media (0/3)	Data Transfer Size Limits	Data Destruction	
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/4)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Cloud Infrastructure Discovery	Brute Force (0/4)	Archive Collected Data (0/3)	Communication Through Removable Media	Data Encrypted for Impact	
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Service Discovery	Cloud Service Dashboard	Cloud Storage Object Discovery	Automated Collection	Exfiltration Over Alternative Protocol (0/2)	Defacement (0/2)	
Gather Victim Org Information (0/4)	Establish Accounts (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Inter-Process Communication (0/3)	Debugger Evasion	Forced Authentication	Container and Resource Discovery	Container and Resource Discovery	Container and Resource Discovery	Browser Session Hijacking	Exfiltration Over C2 Channel (0/2)	Disk Wipe (0/2)	
Phishing for Information (0/3)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Native API	Create Account (0/3)	Domain Policy Modification (0/2)	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Cloud Storage Object Discovery	Cloud Storage Object Discovery	Clipboard Data	Exfiltration Over Other Network Medium (0/1)	Endpoint Denial of Service (0/4)	
Search Closed Sources (0/2)	Scheduled Task/Job (0/5)	Scheduled Task/Job (0/5)	Serverless Execution	Direct Volume Access	Input Capture (0/4)	Input Capture (0/4)	Debugger Evasion	Debugger Evasion	Debugger Evasion	Data from Cloud Storage	Exfiltration Over Physical Medium (0/1)	Firmware Corruption	
Search Open Technical Databases (0/5)	Shared Modules	Software Deployment Tools	Event Triggered Execution (0/16)	Escape to Host	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Domain Trust Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Inhibit System Recovery	
Search Open Websites/Domains (0/3)	System Services (0/2)	User Execution (0/3)	External Remote Services	Event Triggered Execution (0/16)	Execution Guardrails	Multi-Factor Authentication Request Generation	File and Directory Discovery	Data from Cloud Storage	Ingress Tool Transfer	Multi-Stage Channels	Scheduled Transfer	Network Denial of Service (0/2)	
Search Victim-Owned Websites	Windows Management Instrumentation	Hijack Execution Flow (0/12)	Hijack Execution Flow (0/12)	Hijack Execution Flow (0/12)	Exploitation for Defense Evasion	Network Sniffing	Group Policy Discovery	Data from Local System	Non-Application Layer Protocol	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking	
		Implant Internal Image	Modify Authentication Process (0/7)	Impair Defenses (0/9)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	Network Service Discovery	Data from Network Shared Drive	Protocol Tunneling	Protocol Tunneling		Service Stop	
		Modify Authentication Process (0/7)	Office Application Startup (0/6)	Indicator Removal (0/8)	Hide Artifacts (0/10)	Steal Application Access Token	Network Share Discovery	Data from Removable Media	Proxy (0/4)	Proxy (0/4)		System Shutdown/Reboot	
		Office Application Startup (0/6)	Pre-OS Boot (0/5)	Indirect Command Execution	Malicious File Execution (0/7)	Steal or Forge Authentication Certificates	Network Sniffing	Data Staged (0/2)	Remote Access Software	Remote Access Software			
		Pre-OS Boot (0/5)	Scheduled Task/Job (0/5)	Masquerading (0/7)	Malicious File Execution (0/7)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing	Email Collection (0/3)	Traffic Signaling (0/2)	Traffic Signaling (0/2)			
		Scheduled Task/Job (0/5)	Server Software Component (0/5)	Modify Authentication Process (0/7)	Malicious File Execution (0/7)	Steal Web Session Cookie	Network Sniffing	Input Capture (0/4)	Web Service (0/3)	Web Service (0/3)			
		Traffic Signaling (0/2)	Traffic Signaling (0/2)	Modify Cloud Compute Infrastructure (0/4)	Malicious File Execution (0/7)	Unsecured Credentials (0/7)	Network Sniffing	Screen Capture					
		Valid Accounts (0/4)	Valid Accounts (0/4)	Modify Registry (0/9)	Malicious File Execution (0/7)	Software Discovery (0/7)	Network Sniffing	Video Capture					
				Modify User Image (0/2)	Malicious File Execution (0/7)	System Information Discovery	Network Sniffing						
				Network Boundary Bypassing (0/7)	Malicious File Execution (0/7)	System Location Discovery (0/7)	Network Sniffing						
				Obfuscated Files or Information (0/9)	Malicious File Execution (0/7)	System Network Configuration Discovery	Network Sniffing						
				Plist File Modification	Malicious File Execution (0/7)	System Network Connections Discovery	Network Sniffing						
				Pre-OS Boot (0/5)	Malicious File Execution (0/7)	System Owner/User Discovery	Network Sniffing						
				Process Injection (0/12)	Malicious File Execution (0/7)	System Service Discovery	Network Sniffing						
				Reflective Code Loading	Malicious File Execution (0/7)	System Time Discovery	Network Sniffing						
				Rogue Domain Controller	Malicious File Execution (0/7)	Virtualization/Sandbox Evasion (0/3)	Network Sniffing						
				Rootkit	Malicious File Execution (0/7)		Network Sniffing						
				Subvert Trust Controls (0/6)	Malicious File Execution (0/7)		Network Sniffing						
				System Binary Proxy Execution (0/13)	Malicious File Execution (0/7)		Network Sniffing						
				System Script Proxy Execution (0/7)	Malicious File Execution (0/7)		Network Sniffing						
				Template Injection	Malicious File Execution (0/7)		Network Sniffing						
				Traffic Signaling (0/2)	Malicious File Execution (0/7)		Network Sniffing						
				Trusted Developer Utilities Proxy Execution (0/1)	Malicious File Execution (0/7)		Network Sniffing						
				Unused/Unsupported Cloud Regions	Malicious File Execution (0/7)		Network Sniffing						
				Use Alternate Authentication Material (0/4)	Malicious File Execution (0/7)		Network Sniffing						
				Valid Accounts (0/4)	Malicious File Execution (0/7)		Network Sniffing						
				Virtualization/Sandbox Evasion (0/3)	Malicious File Execution (0/7)		Network Sniffing						
				Weaken Encryption (0/2)	Malicious File Execution (0/7)		Network Sniffing						
				XSL Script Processing	Malicious File Execution (0/7)		Network Sniffing						

# September



December ?



# Techniques

- Hacker Breaches Tequivity AWS Server
- BreachForums communication, attributed to Lapsus\$ group
- Not many details shared about the exact methods used



# Impact

- 77.000 Uber Employees data is stolen
  - Full name
  - E-mail address
  - Location
- IT Asset information
  - Serial Number
  - Make
  - Models
  - Technical Specifications
- Corporate reports
- Mobile device management(MDM) source code
- Uber Eats internal access
- third-party vendor services,

UberLeak



BreachForums User

MEMBER

Posts:

Threads:

Joined:

Apr 202

Reputation:

1

December 10, 2022, 01:49 AM (This post was last modified: December 10, 2022, 01:51 AM by pompompurin.)

#1

~ hacked by autistic fisherman Arion and scammed all LAPSUS\$ members

<https://> /NHTUBD.tar  
<https://> /uber/NHTUBD.tar

## The Conviction of Uber's Chief Security Officer

I have been meaning to write about Joe Sullivan, Uber's former Chief Security Officer. He was convicted of crimes related to covering up a cyberattack against Uber. It's a complicated case, and I'm not convinced that he deserved a guilty ruling or that it's a good thing for the industry.

I may still write som

Tags: [courts](#), [cover-up](#)

Posted on November

## Uber Breached, Again, After Attackers Compromise Third-Party Cloud

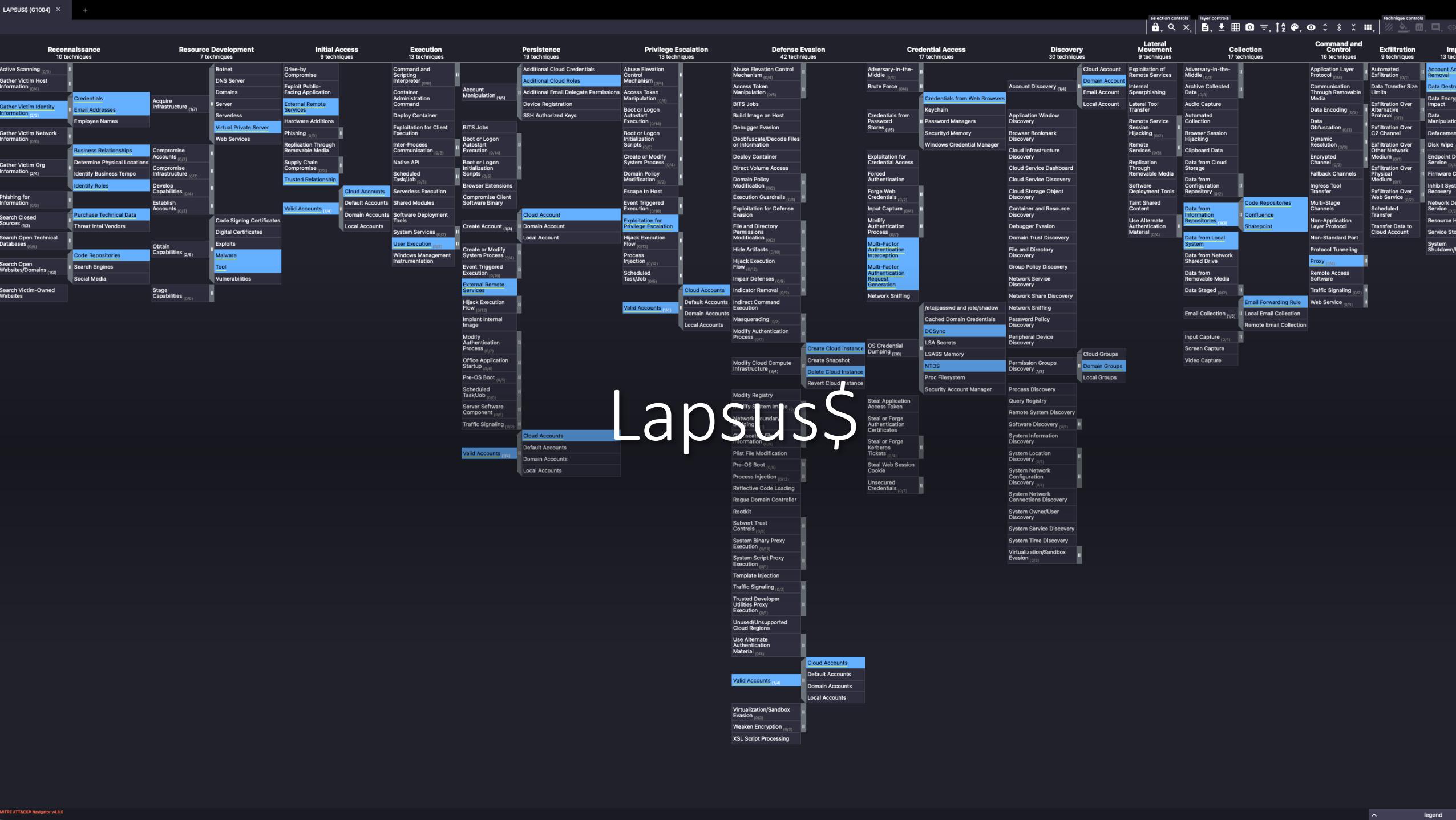
Threat actors leak employee email addresses, corporate reports, and IT asset information on a hacker forum after an attack on an Uber technology partner.



**Elizabeth Montalbano**

Contributor, Dark Reading

December 13, 2022

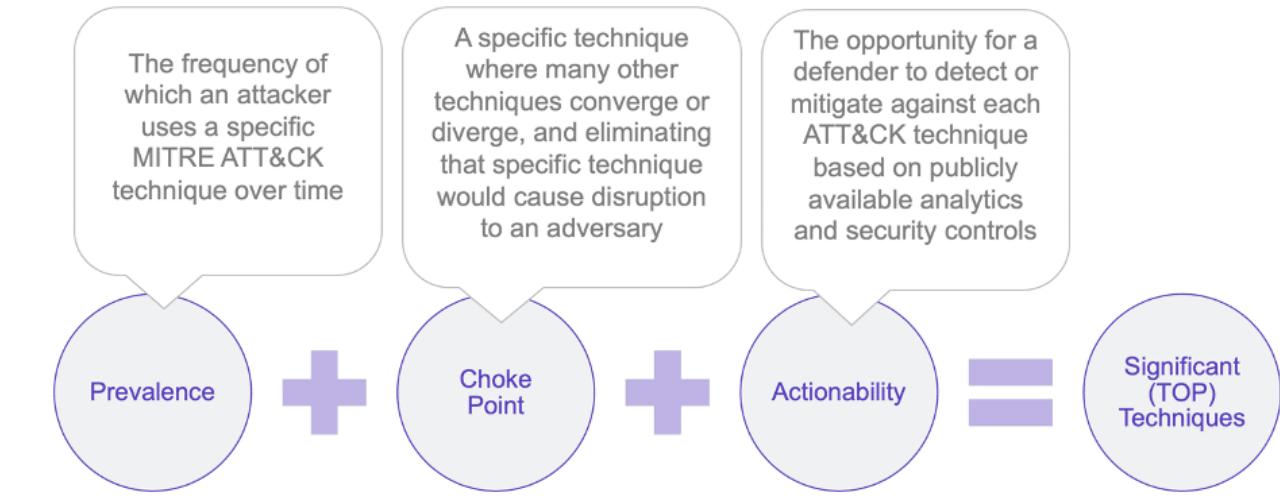


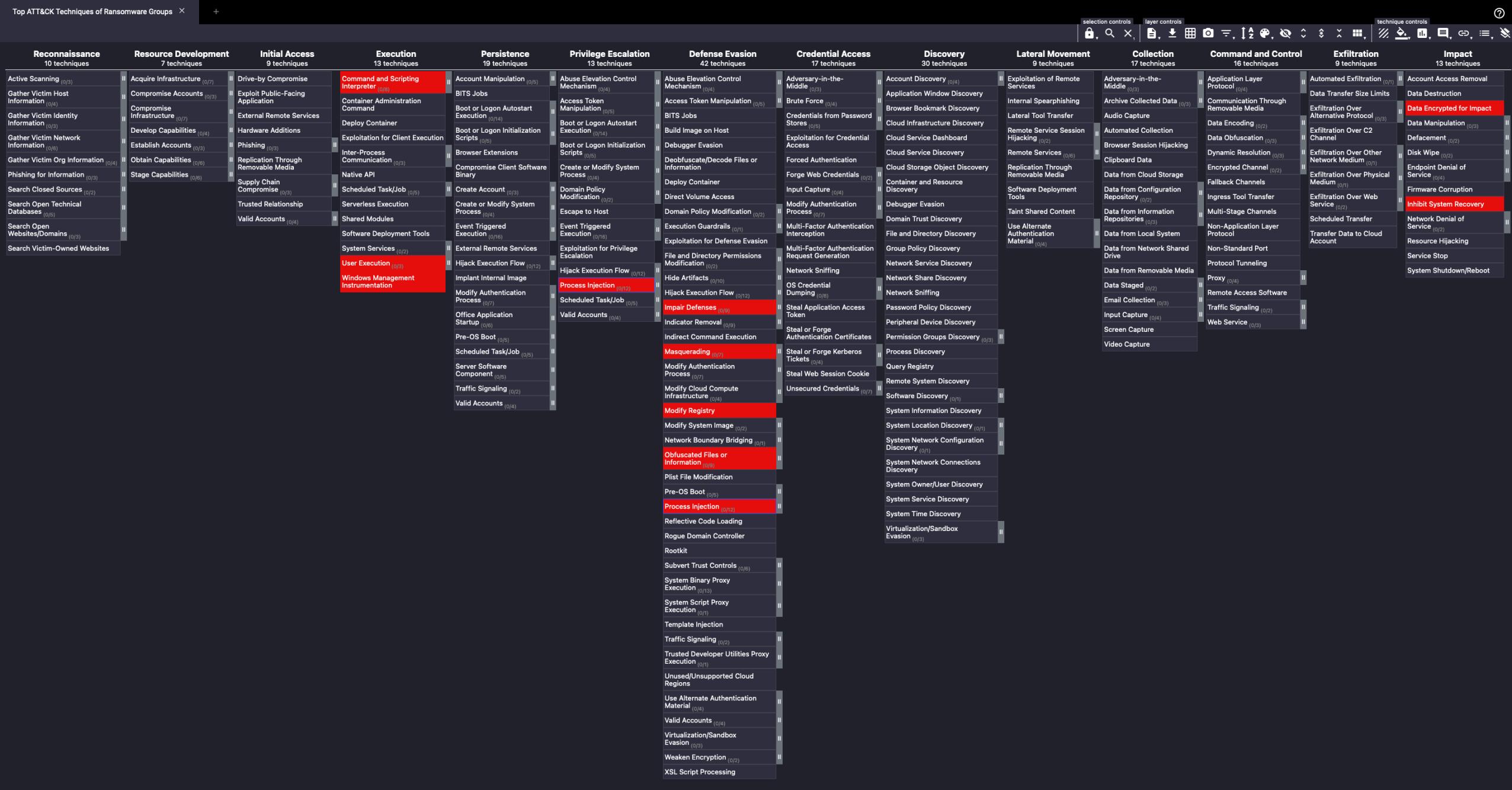
A stack of approximately ten books of various colors, including red, blue, green, and yellow, is arranged vertically on the right side of the frame. The books are slightly overlapping, creating a sense of depth. The background is a solid, dark teal color.

Lessons ... Globally

# Top ATT&CK Techniques

- [T1486: Data Encrypted for Impact](#)
- [T1490: Inhibit System Recovery](#)
- [T1027: Obfuscated Files or Information](#)
- [T1047: Windows Management Instrumentation](#)
- [T1036: Masquerading](#)
- [T1059: Command and Scripting Interpreter](#)
- [T1562: Impair Defenses](#)
- [T1112: Modify Registry](#)
- [T1204: User Execution](#)
- [T1055: Process Injection](#)



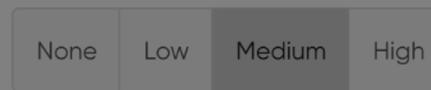


## Filters

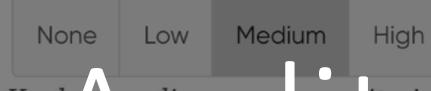
NIST 800-53  
ControlsCIS Security  
ControlsDetection  
AnalyticsOperating  
Systems

Generate Results

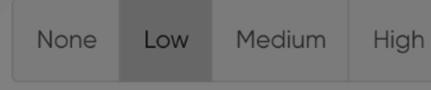
## Network Monitoring Components

*You have medium network monitoring.*

## Process Monitoring Components

*You have medium process monitoring.*

## File Monitoring Components

*You have low file monitoring.*

## Cloud Monitoring Components

*You have low cloud monitoring.*

## Your Top 10 Techniques

- ✗ 1. T1059 - Command and Scripting Interpreter

- ✗ 2. T1047 - Windows Management Instrumentation

- ✗ 3. T1053 - Scheduled Task/Job

- ✗ 4. T1574 - Hijack Execution Flow

- ✗ 5. T1562 - Impair Defenses

- ✗ 6. T1018 - Create or Modify System Process

- ✗ 7. T1021 - Remote Services

- ✗ 8. T1003 - OS Credential Dumping

- ✗ 9. T1036 - Masquerading

- ✗ 10. T1055 - Process Injection

## Technique Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](#) while Windows installations include the [Windows Command Shell](#) and [PowerShell](#).

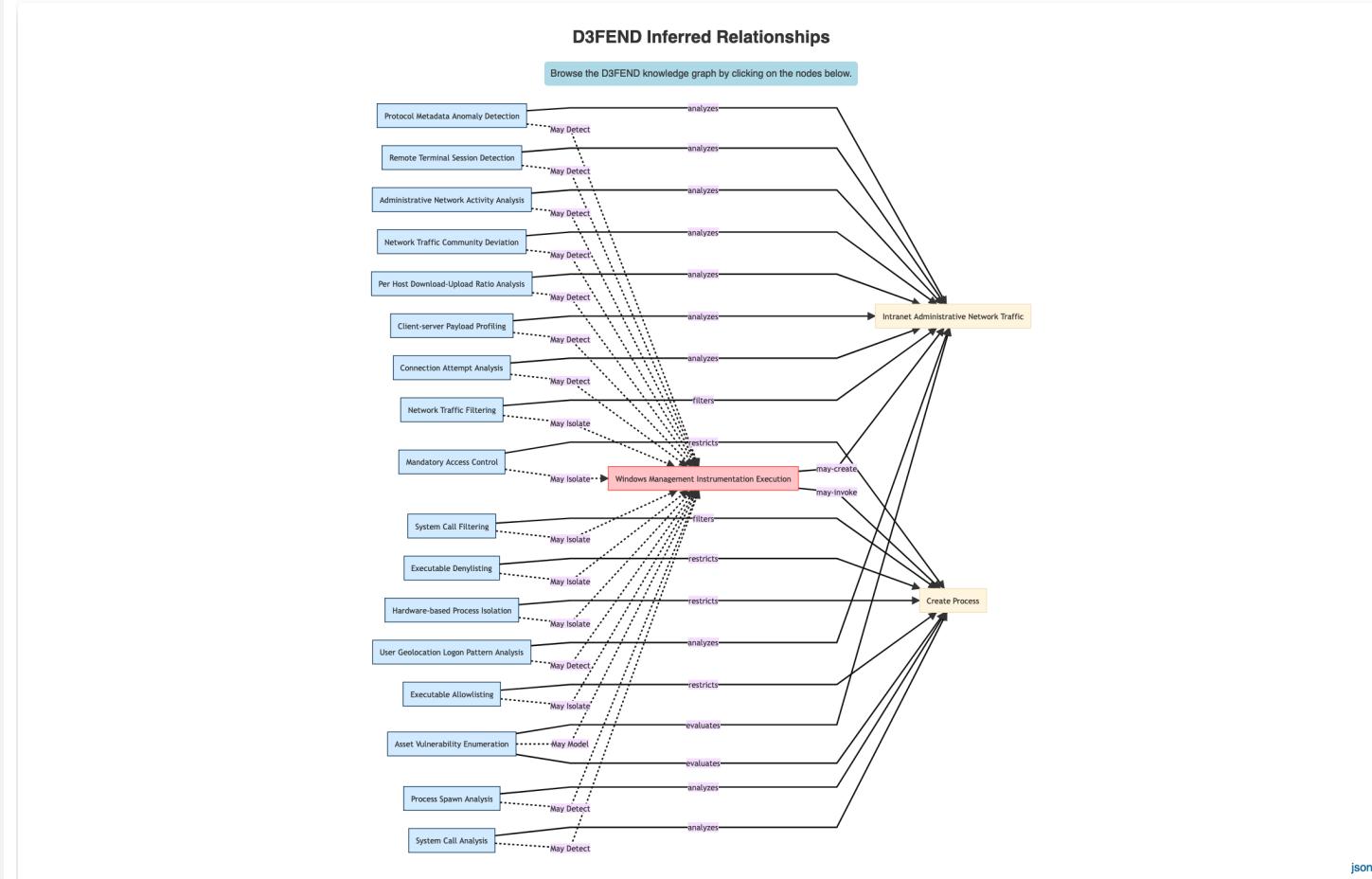
There are also cross-platform interpreters such as [Python](#), as well as those commonly associated with client applications such as [JavaScript](#) and [Visual Basic](#).

Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](#) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](#) in order to achieve remote Execution.(Citation: Powershell Remote Commands) (Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

## Subtechniques

T1059-001 - Command and Scripting Interpreter

# Prioritizing Controls based on Choke Points



# Statistics



# Data Breach Metrics 2022



277 days – Time to Identify  
and Contain



+41% – Caused by  
ransomware



45% of total – In the Cloud



# Average Cost Saving Factors



\$2.66M – Tested IR plan



\$2.30M – Low level of compliance failures



\$1.76M – Zero Trust Deployed



\$1.12M – Containment <200 days



\$3.80M – hybrid cloud model (vs. public/private)



# Average Cost of Data Breaches



\$9.44M – US



\$4.35M – Global



\$4.24M – Private cloud



\$5.02M – Public clouds

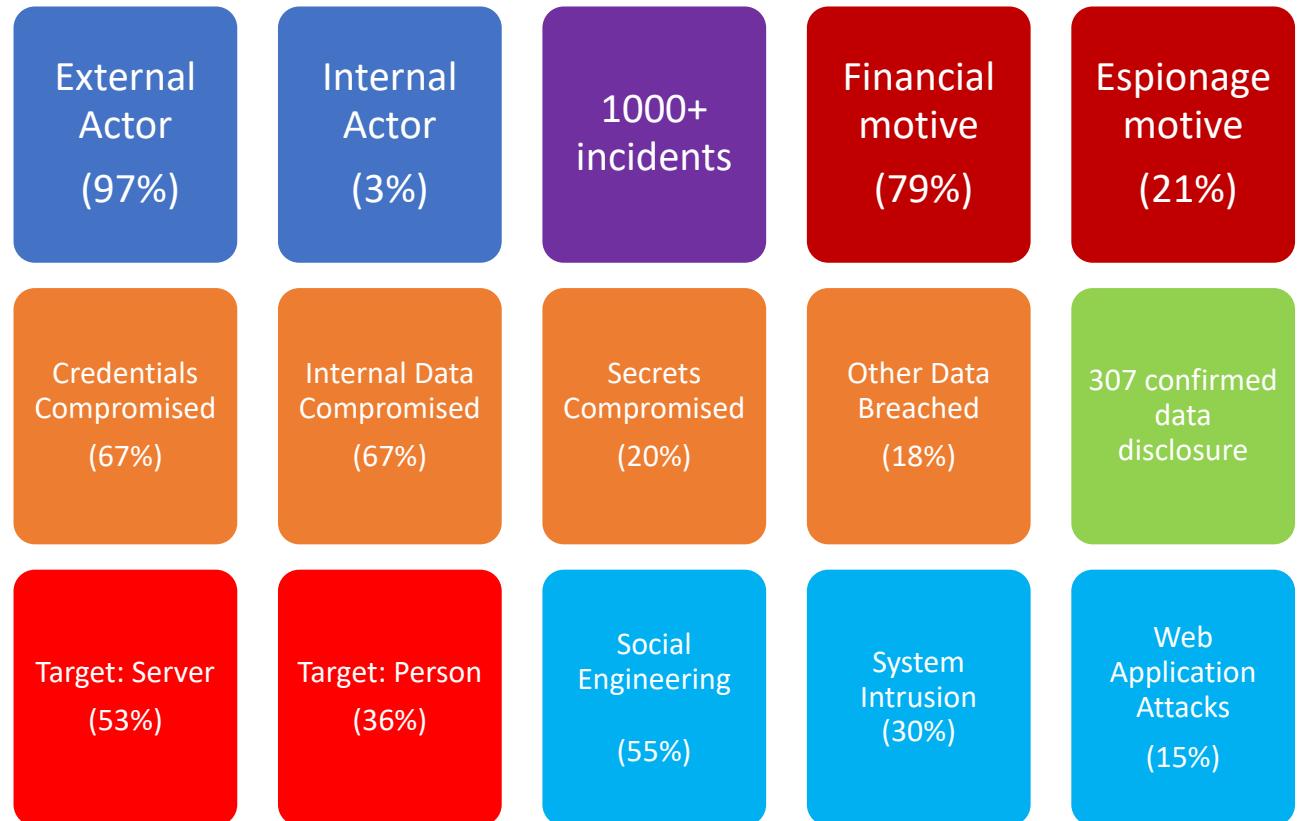


\$4.18M – \$4.91M range  
per initial access

(Insider, Stolen/Compromised  
Creds, 3<sup>rd</sup> Party Vulnerability, BEC,  
Phishing)

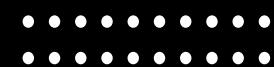


# Europe, Middle East, Africa (2021)

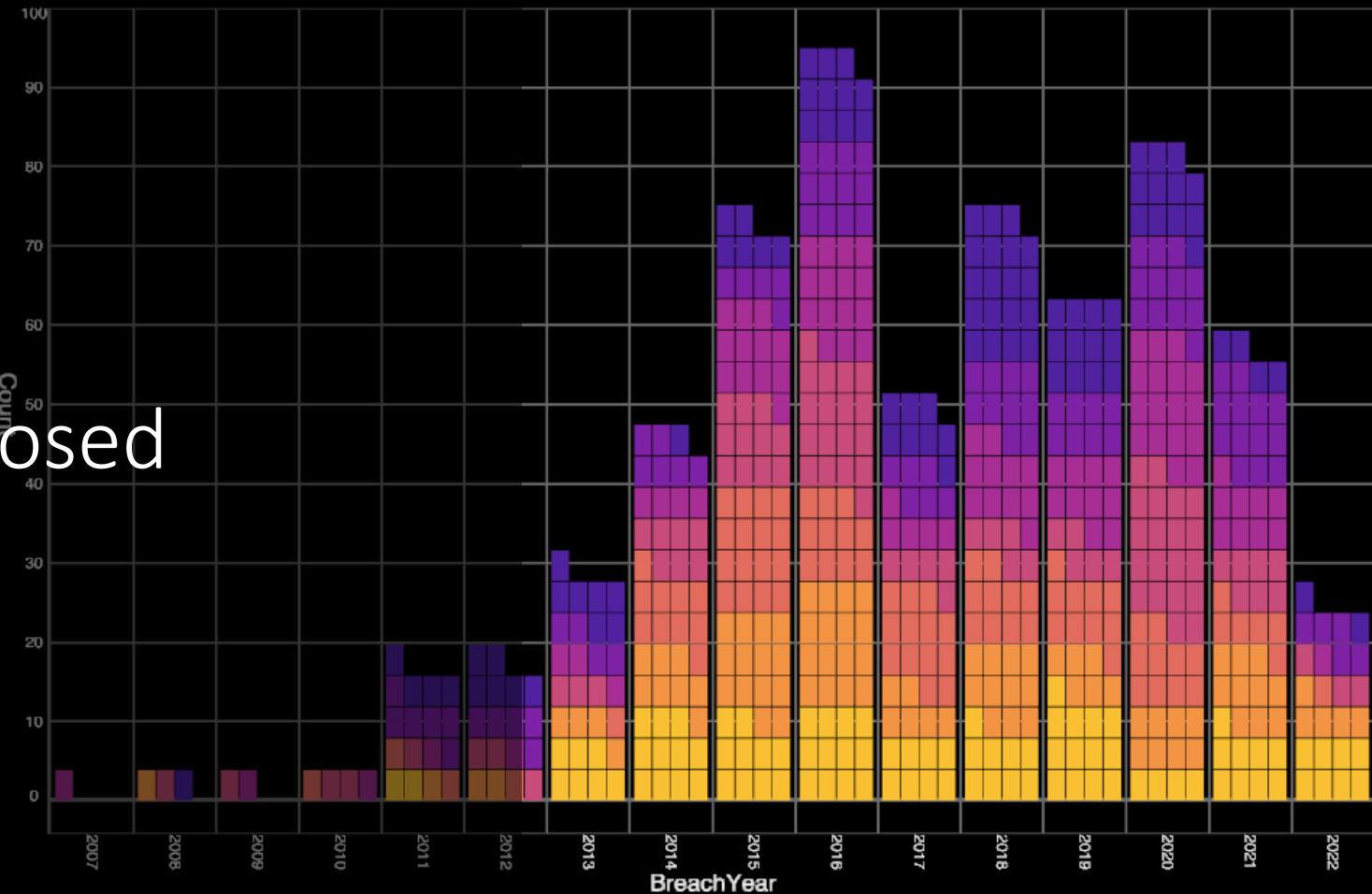


# Trends





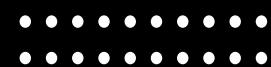
# of disclosed  
records



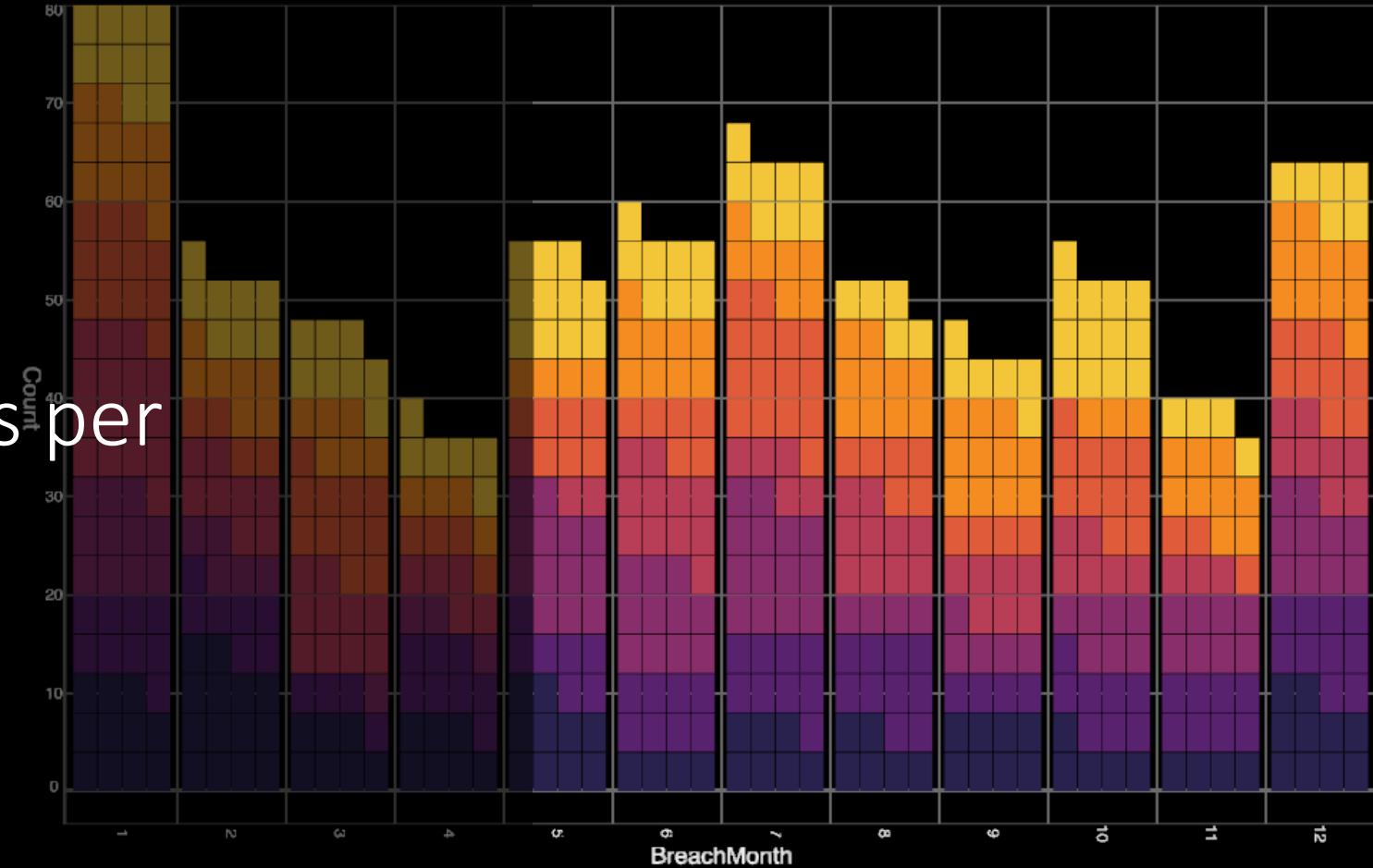
PwnCount

- < 11000
- 11000 - 400000
- 400000 - 780000
- 780000 - 1600000
- 1600000 - 4800000
- 4800000 - 21000000
- ≥ 21000000





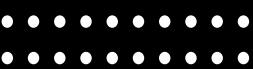
# Breaches per months



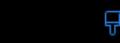
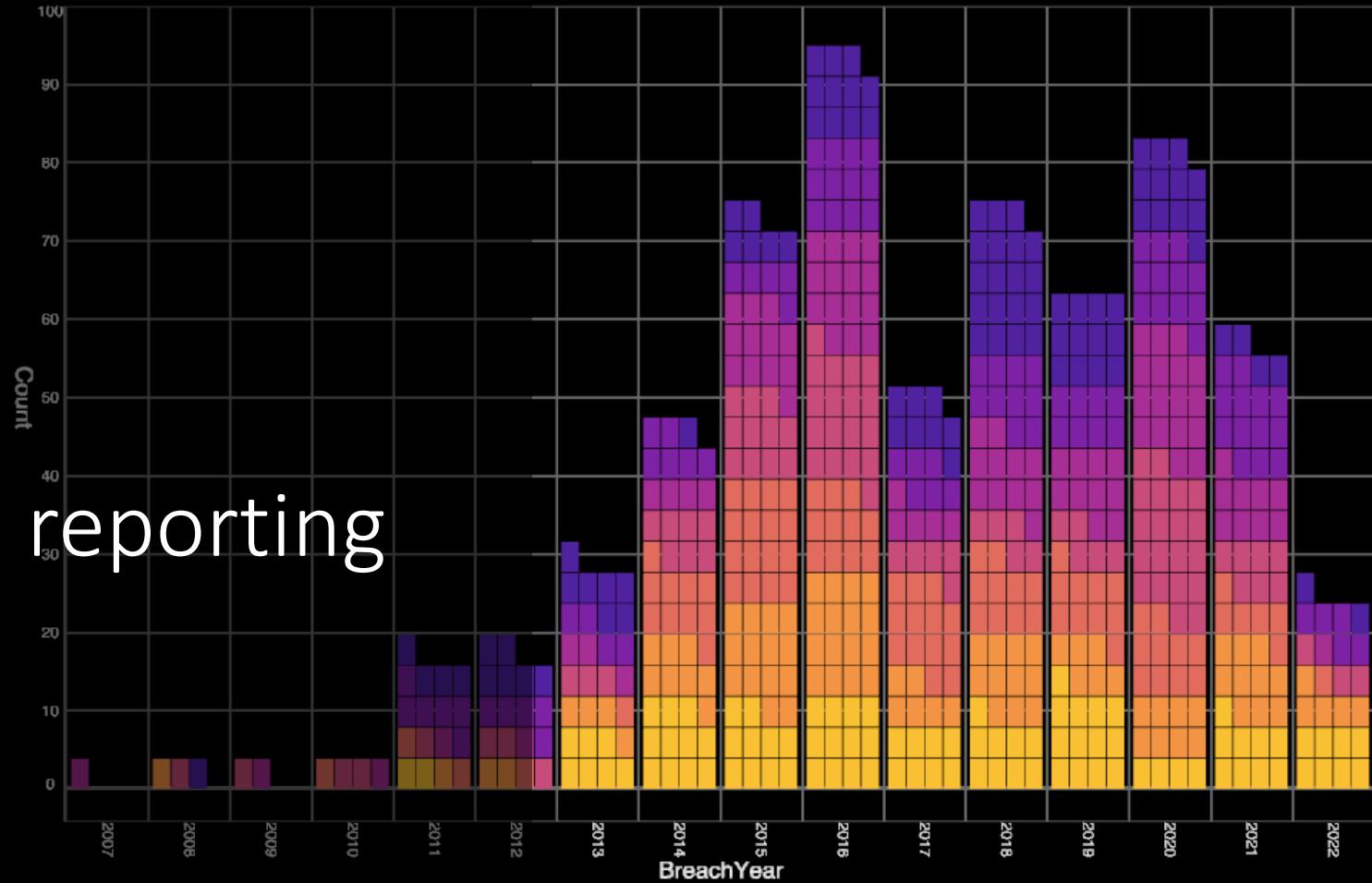
PwnCount

- < 110000
- 110000 – 400000
- 400000 – 780000
- 780000 – 1600000
- 1600000 – 4800000
- 4800000 – 21000000
- ≥ 21000000





# Delay in reporting





# Keywords

accounts addresses attack attributed bcrypt birth breach card com contained customer data dates email exposed forum hacking hashes hibp https impacted incident included information ip million names net news numbers passwords personal phone physical popular provided records requested salted security service source stored suffered target twitter unique user usernames website



# What does AI have to say about all of this?



what are the main reasons for data breaches



There are several common reasons for data breaches:

1. Hackers or cybercriminals who gain unauthorized access to systems to steal sensitive information.
2. Insiders who misuse their access to company systems or data.
3. Unsecured networks or systems that are vulnerable to attack.
4. Weak or easily guessable passwords.
5. Lack of proper security measures, such as failure to patch vulnerabilities or implement proper access controls.
6. Accidental disclosure, such as sending sensitive information to the wrong person or posting it publicly by mistake.
7. Physical theft, such as stealing a laptop or hard drive with sensitive information on it.
8. Malware or ransomware attacks that can compromise data or lock users out of systems until a ransom is paid.



# Prognosis

GR

what data breach trends are likely to continue in 2023?



It's difficult to predict exactly what data breach trends will continue in 2023, as the threat landscape is constantly evolving and new types of attacks and vulnerabilities are constantly emerging. However, some trends that have been seen in recent years are likely to continue, such as:

1. Ransomware attacks: Ransomware attacks, in which hackers encrypt a victim's data and demand a ransom to restore access, have been a major trend in recent years and are likely to continue in the future.
2. Targeting of small and medium-sized businesses: Small and medium-sized businesses often have fewer resources to devote to cybersecurity and may not have the same level of protection as larger enterprises. As a result, they can be attractive targets for hackers.
3. Increasing use of artificial intelligence: Hackers are increasingly using artificial intelligence and machine learning to automate and scale their attacks.
4. Supply chain attacks: Hackers may target a company's suppliers or other partners in the supply chain as a way to gain access to the company's systems.
5. Attacks on the cloud: As more companies move their data and applications to the cloud, hackers are increasingly targeting cloud-based systems.
6. Social engineering attacks: Social engineering attacks, which rely on manipulating people rather than exploiting technical vulnerabilities, are also likely to continue. These can take the form of phishing attacks, pretexting (creating a false identity to gain access to sensitive information), or baiting (offering something enticing to get the victim to reveal sensitive information).



# Controls?

GR

how to be prepared against data breaches in 2023?



There are several steps you can take to help protect your organization against data breaches in 2023 and beyond:

1. Implement strong cybersecurity measures: This includes things like installing and maintaining firewalls, using antivirus and anti-malware software, and implementing strong password policies.
2. Train employees: Teach your employees how to recognize and prevent phishing attacks and other types of social engineering attacks.
3. Regularly update software: Keep all software and systems up to date with the latest patches and updates. These often include important security fixes.
4. Use multi-factor authentication: Requiring multiple forms of authentication can make it much more difficult for hackers to gain access to your systems.
5. Conduct regular security audits: Regularly assess your organization's security posture and identify any vulnerabilities that need to be addressed.
6. Use encryption: Encrypting data at rest (when it is stored) and in transit (when it is being transmitted) can help protect it from being accessed by unauthorized parties.
7. Implement a data backup and recovery plan: Having a plan in place to backup and recover data in the event of a breach can help minimize the damage and get your organization back up and running as quickly as possible.



# DBIR – Very Small Business Cybercrime Protection Sheet

## What to do to avoid becoming a target?

1. Use two-factor authentication
2. Do not reuse or share passwords
3. Use a password keeper/generator app
4. Be sure to change the default credentials of the Point of Sale (Pos) controller or other hardware/software
5. Ensure that you install software updates promptly so that vulnerabilities can be patched
6. Work with your vendors to be sure that you are as secure as you can be, and that they are following these same basic guidelines
7. Keep a consistent schedule with regard to backups and be sure to maintain offline backups—meaning that they are not on a device connected to a computer
8. Ensure that the built-in firewall is switched on for user devices such as laptops and desktops (“on” may not be the default)
9. Use antivirus software, for all your devices. Smart phones, tablets and credit card swipers are just as important as laptops and computers. It won’t catch everything, but it will help
10. Do not click on anything in an unsolicited email or text message
11. Set up an out of band method for verifying unusual requests for data or payments
12. Make sure the computer used for financial transactions is not used for other purposes such as social media or email
13. Use email services that incorporate phishing and pretexting defenses and use a web browser that warns you when a website may be spoofed



# Resources

- Slides:
  - <https://github.com/inverzeio/talks>
- Data Sources:
  - <https://haveibeenpwned.com>
  - <https://github.com/mitre-attack/attack-stix-data/blob/master/enterprise-attack/enterprise-attack-12.1.json>
  - <https://github.com/vz-risk/VCDB/blob/master/data/csv/vcdb.csv.zip>
  - <https://www.mockaroo.com/>
- References:
  - <https://top-attack-techniques.mitre-engenuity.org/>
  - <https://top-attack-techniques.mitre-engenuity.org/calculator>
  - <https://ibm.com/security/data-breach>
  - <https://www.ibm.com/reports/data-breach>
  - <https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxnhfhgj9bxgi9/sophos-state-of-ransomware-2022-wp.pdf>
  - <https://reports.exodus-privacy.eu.org>
- Complementary Resources:
  - <https://marketplace.visualstudio.com/items?itemName=msrvida.vscode-sanddance>



# Questions

