

**Uber Data Breach Report**

Ahmed Rashwan

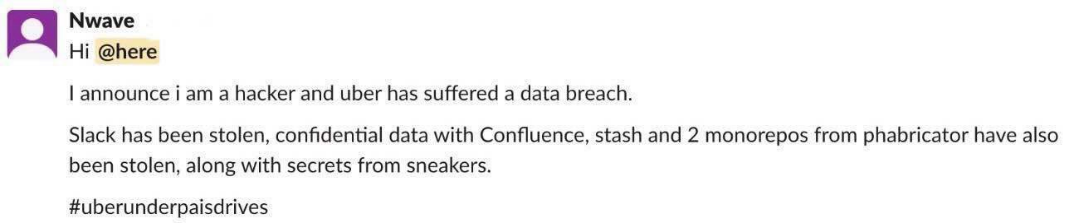
# Executive summary

## Brief breach description

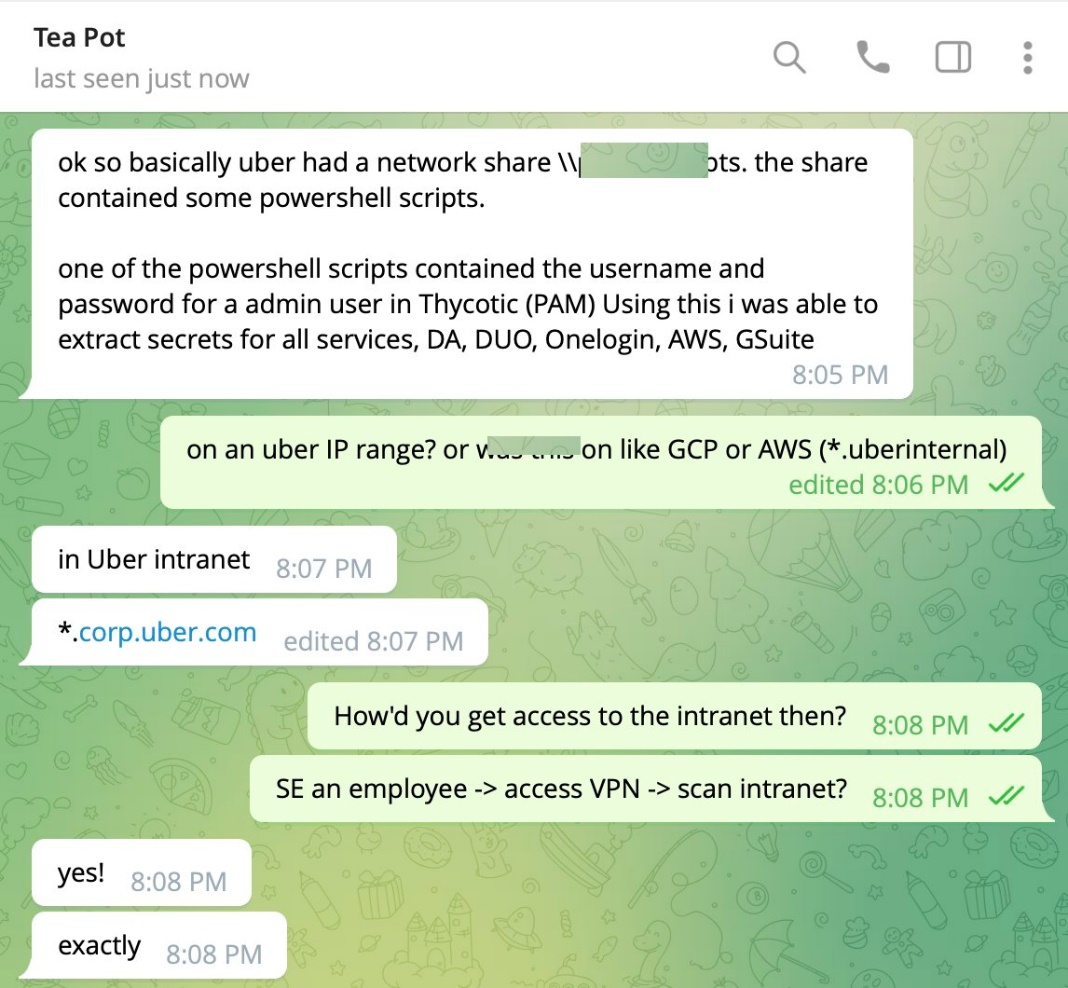
On the 15th of September, Uber fell victim to an organization-wide data breach. The threat actor claimed to be an 18-year-old hacker who compromised various assets and services including Uber’s internal network, slack channel, etc. using social engineering. (Browne, 2022)

Following an investigation, Uber believed that the hacker **Teapot** is allegedly working with the LAPSUS$ hacker group which has been known to hack other various big tech such as Microsoft.

On Thursday afternoon a few moments before slack were taken offline, Uber and its employees got a message reading ***“I announce I am a hacker and Uber has suffered a data breach”.***



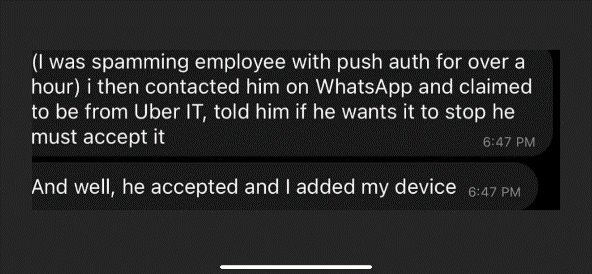
(M. Qasim Munir, 2022)

 (Jackson, 2022)

# Breach incident analysis

The hacker compromised an external uber contactor by infecting them with malware that leaked data which was used to login into the account

Whilst the account was protected with multi-factor authentication, the hacker used an MFA fatigue attack which repeatedly sent MFA login code requests to the victim, when the hacker texted the victim on WhatsApp, they used the pretext of an Uber IT team and that if the MFA spam login requests were to stop, they had to accept.

 (Sjouwerman, 2022)

Following the attacker gaining access to the account, the hacker found VPN credentials to Uber’s intranet, and it is believed that the attacker used the widely used open-source enumeration and port scanning tool “*Nmap*”, to scan and enumerate the internal network, this would have led the attacker to find other potential attack vectors, and points of potential compromise.

The hacker found a network share where one of the windows PowerShell scripts had hardcoded username and password for an admin user to Uber’s thycotic privacy and access management (PAM) system.

Thycotic is a PAM solution which uses tools to control and manage has a large variety of privilege including access to internal and external third-party applications as well as critical DevOps information, users privilege access, etc.

## Breakdown of compromised services and their severity

|  |  |
| --- | --- |
| Services Compromised | Severity |
| Thycotic PAM | Critical |
| AWS Instance | Critical |
| VMware vSphere | Critical |
| SentinelOne | High |
| Slack Workspace | Medium |
| GSuite Admin | Medium |
| HackerOne | Medium |

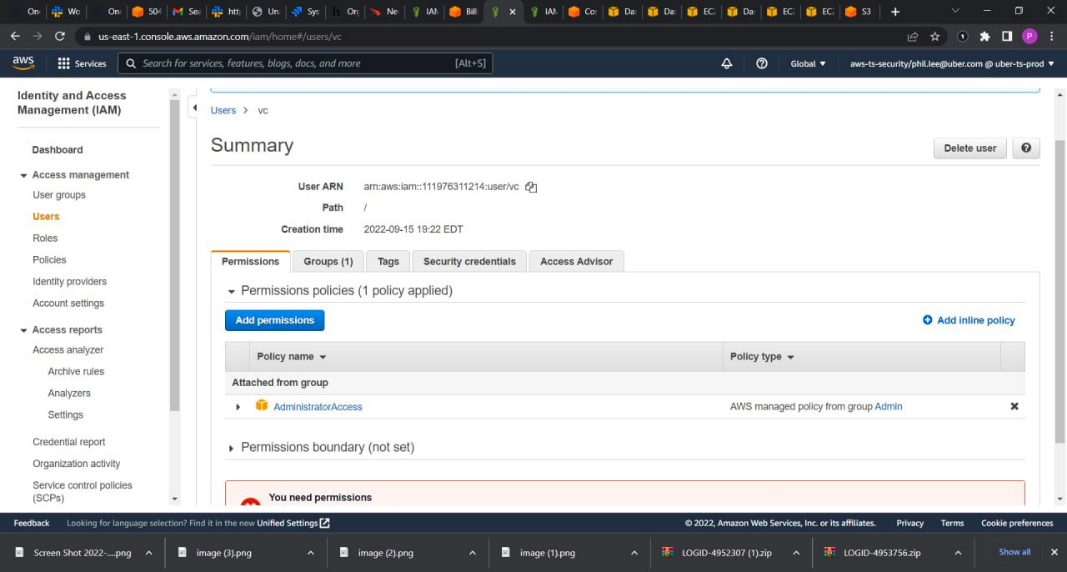
(Jackson, 2022)

### Thycotic PAM

Gaining access to the Thycotic privileged access management systems (PAM) meant that the attacker was able to retrieve high-level credentials to many different services including such as aws.

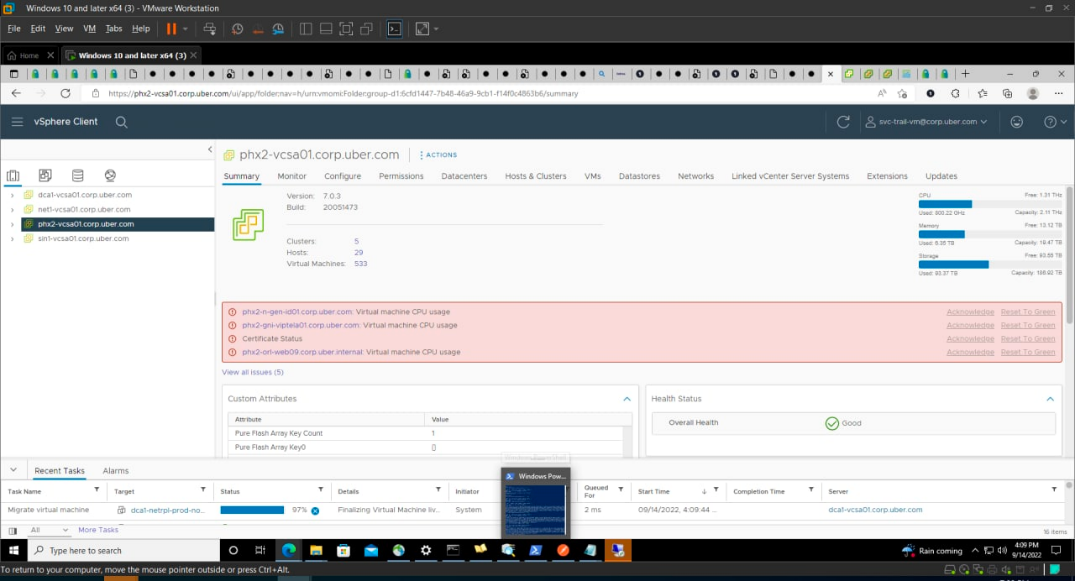
### AWS Instance

A big achievement for the hacker was gaining access to Uber’s applications hosted on AWS (Amazon Web Services) cloud infrastructure. The attacker had all the ABILITY to modify data, stop and turn off running services, or even exfiltrate and steal data.

 (Jackson, 2022)

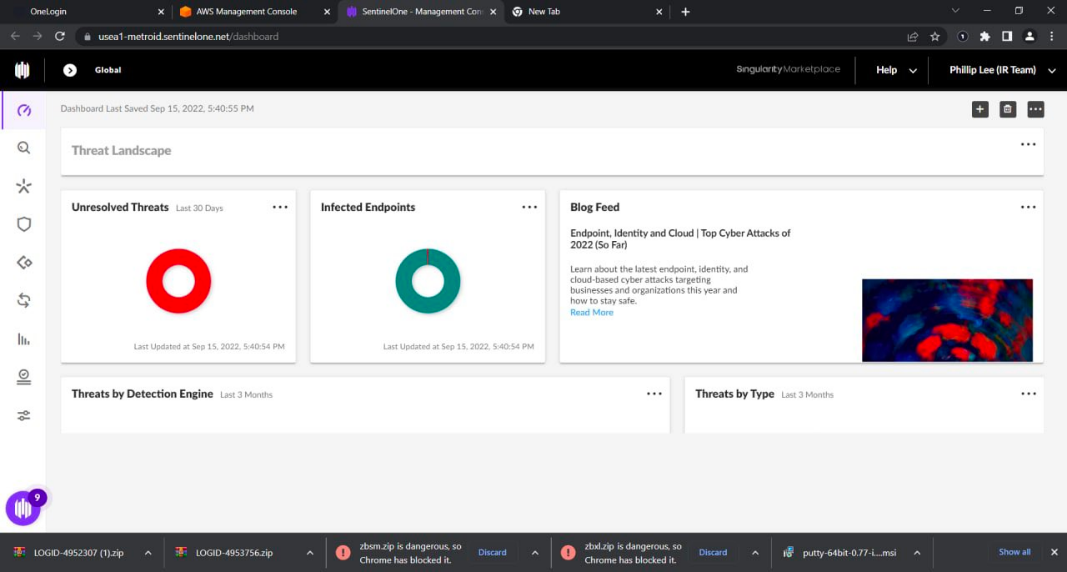
### VMware vSphere

VMware vSphere is used to bridge cloud computing and on-premises servers together. Obtaining access to such service gives the attacker a new potential point of compromise to go even further with the attack

 (Jackson, 2022)

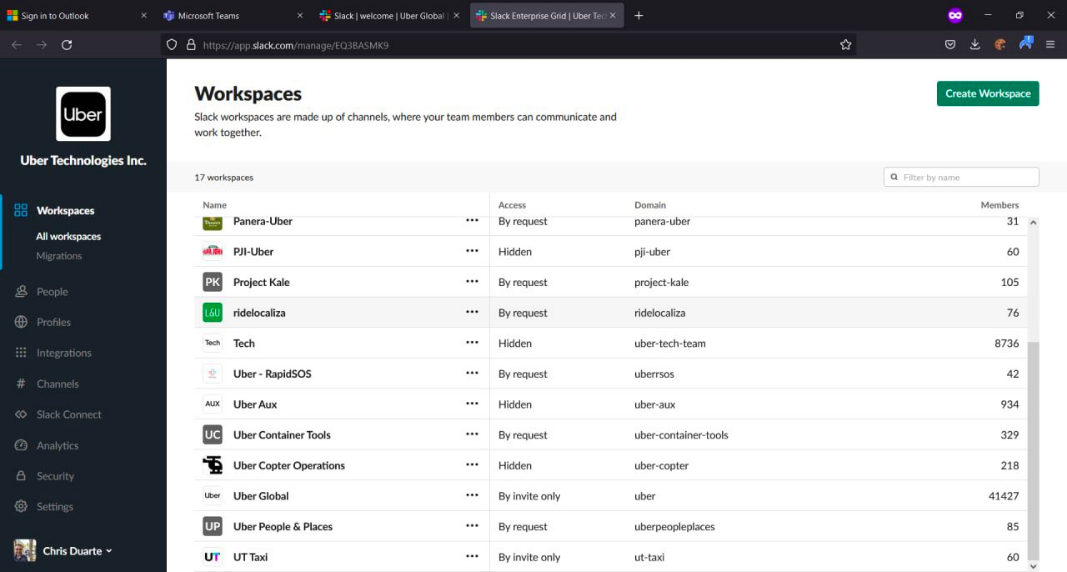
### SentinelOne

SentinelOne is an XDR (extended detection and response) platform that can log and alert in the case of an intrusion, having access to such a crucial platform could lead the attacker to falsely amend data and activity gathered by the platform. This would give the possibility of breaching Integrity of the CIA triad. As part of SentinelOne’s XDR platform, it provides the ability to access employee machines, whilst useful for incident response and forensics, it also makes it a goldmine for hackers.

 (Jackson, 2022)

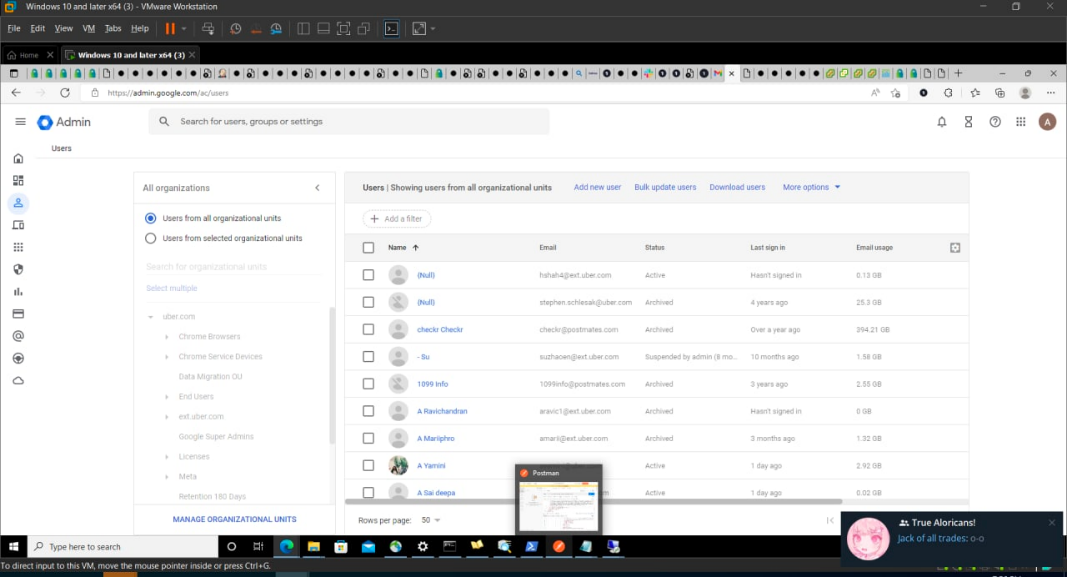
### Slack Workspace

Businesses use Slack to message and communicate. Since there is already a high level of between everyone. By running a social engineering campaign on other employees, an attacker could possibly expand the scope of the breach. If successful, more sensitive data would be compromised.

 (Jackson, 2022)

### GSuite Admin

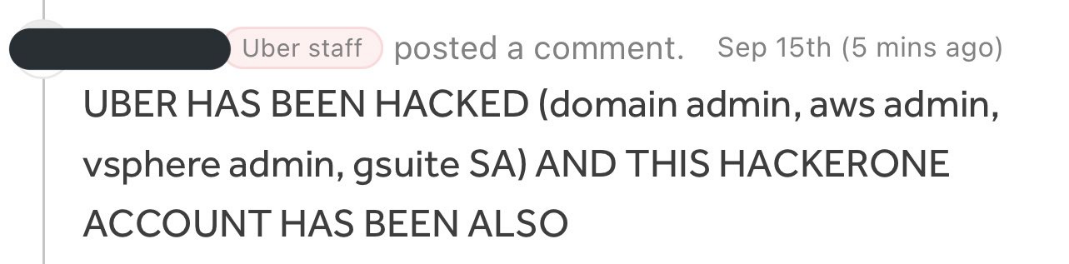
GSuite is an application used to manage users data, manage tasks, and collaborate with one another. Obtaining admin access, the attacker would be able to create, delete, and amend accounts and its information.

 (Jackson, 2022)

### HackerOne

HackerOne is a bug-bounty platform that brings together security researchers from around the world and if a researcher manages to find a weakness or vulnerability, they are rewarded by giving them a bounty as a reward.

Security researchers usually write vulnerability reports with detailed proof of concepts, it’s probable that the hacker could have access to those vulnerability reports and would have been able to do more harm if the hacker was to use a report disclosed by a vulnerability researcher.

 (Jackson, 2022)

## More breached services

### Financial data

Financial data was accessed showing all the statistics of travel and entertainment expenses on a subdomain for uberinternal.com (avengers.uberinternal.com).

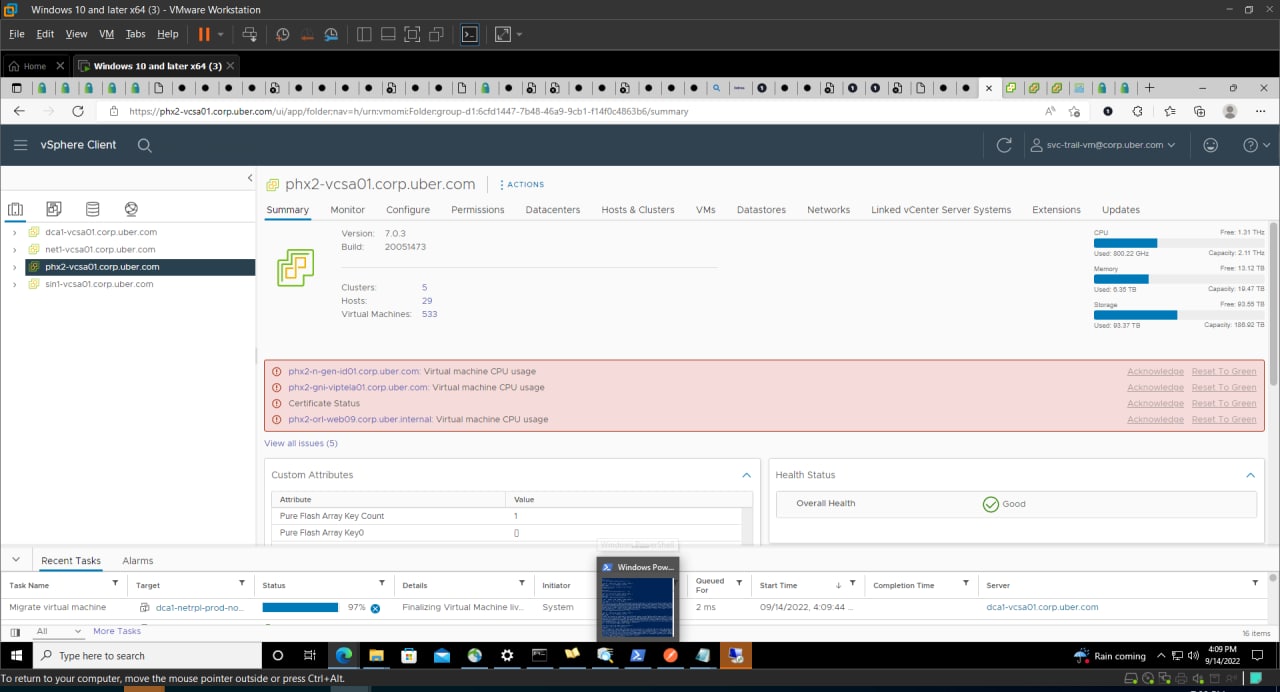
Graphical user interface

Description automatically generated

(vx-underground, 2022)

### vSphere Client

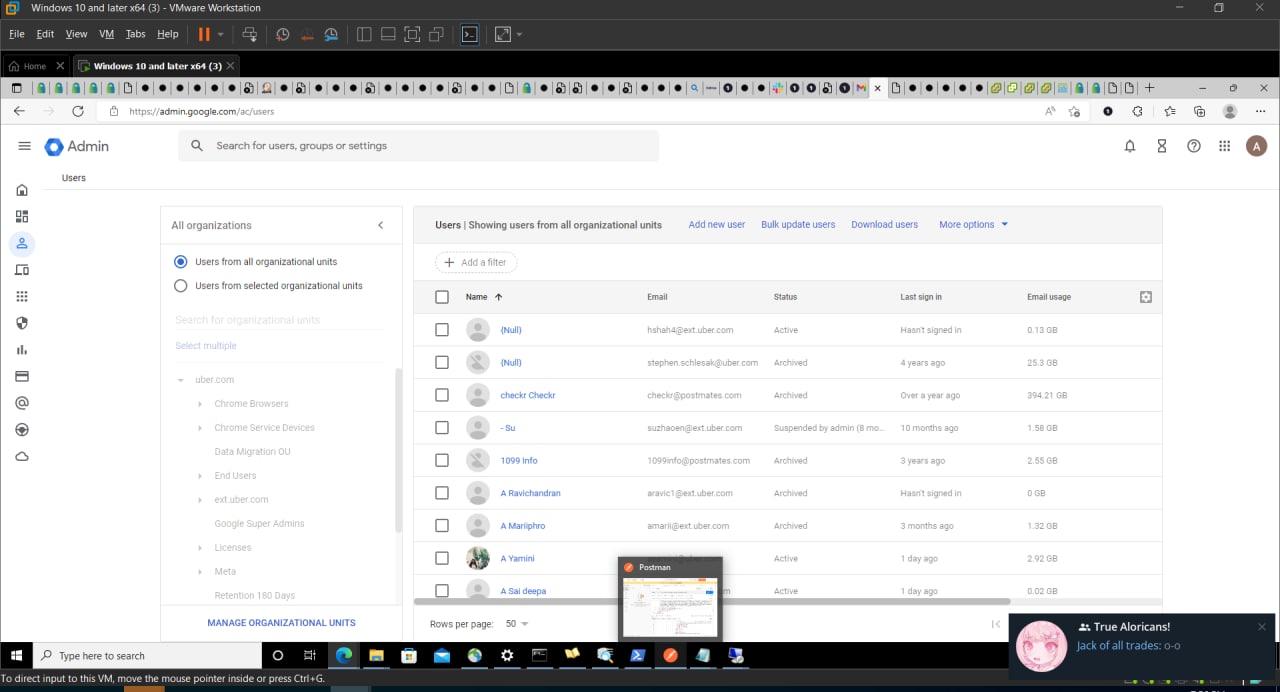
the vSphere client is used to manage multiple VMware machines.

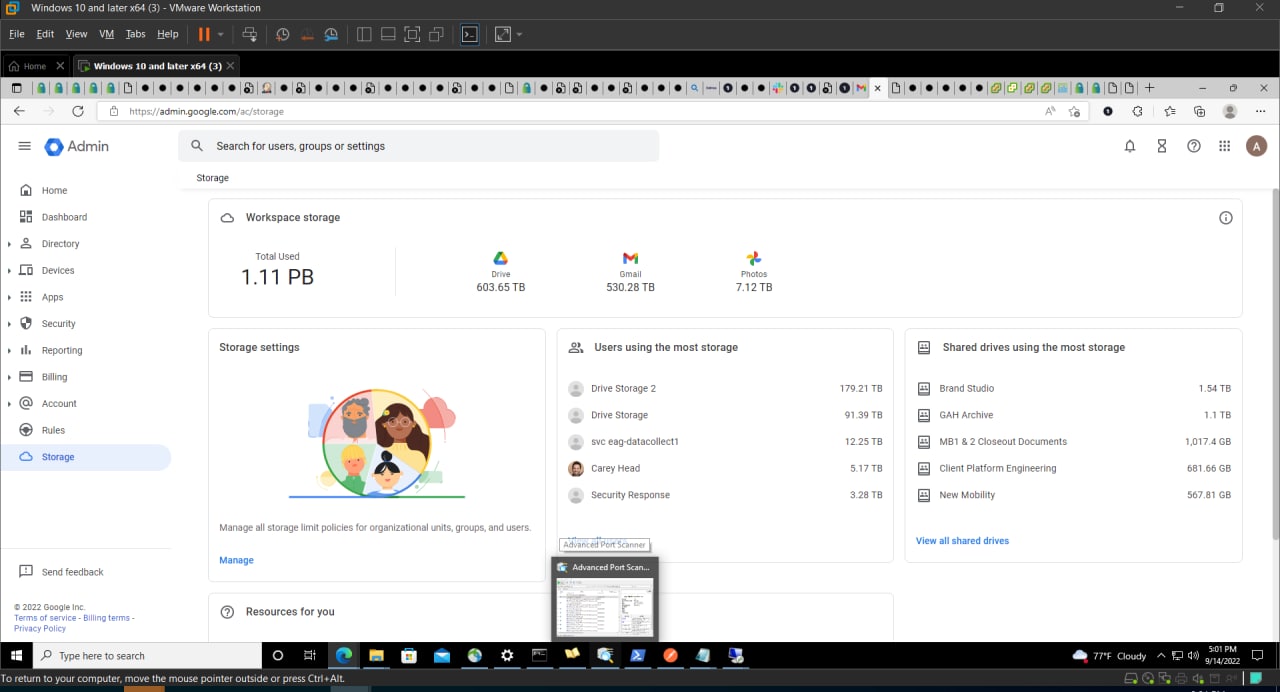


(vx-underground, 2022)

### Google workplace data

The hacker accessed an admin console of google workplace and work email of a believed Uber employee.





(vx-underground, 2022)

## Assets at risk

In an official update provided by Uber, they said “We have no evidence that the incident involved access to sensitive user data (like trip history).”-“All of our services including Uber, Uber Eats, Uber Freight, and the Uber Driver app are operational.” (Uber Team, 2022)

### Employee Data

Whilst Uber confirmed the hacker did not get access to any sensitive user data, the hacker did get access to the Thycotic Privileged access management system where employee’s access data could be at risk as the hacker has access to all privileged accounts of various services that were stored on the PAM.

### External Services Used by Uber

External services such as slack, GSuite, AWS, and more are all at risk because of the attack due to their confidentiality being breached by the hacker when the hacker got access to a privileged admin account on the Thycotic PAM system.

## Affected Stakeholders

### Uber Shareholders

Due to the Uber breach, Uber has suffered a drop in their share’s value down to 5.2%, so any shareholder of Uber has experienced a massive drop in the value of the shares.

### Customers

The trust of Uber’s customers is likely to have been affected as a compromise of this magnitude means that Uber failed to properly handle its corporate data security and while uber has confirmed no sensitive user data was affected or breached, it may always bring up the question of data trust again.

### Employees

Employees have also been affected by the breach as the company may choose to let go of employees for failing to keep the company secure.

# Overview of Techniques and Tools

## Nmap

Nmap is an open-source tool for scanning networks and open ports, and it is believed that the hacker had used this tool to scan the internal network and find the open Windows Share domains that had the PowerShell scripts with leaked admin credentials.

## SMBmap

SMBmap is an open-source tool used for scanning SMB shares and windows shares, it is assumed that the hacker may have used a tool like SMBmap to enumerate the contents of the Windows Shares.

## Active Directory explorer

The hacker certainly used Active Directory explorer to enumerate the active directories

# Impact of the breach on the CIA triad properties

CIA Triad is a widely used cybersecurity model detailing the 3 main pillars of cybersecurity, Confidentiality, Integrity, and Availability. A cyberattack is considered to have generally occurred when one of the 3 pillars has fallen.

Confidentiality was breached throughout the whole company as this was a full company-wide data breach, whilst the integrity was not changed or modified for any of the assets or services, it could have meant that, if the attacker wanted to, they would be able to amend or modify any of the details, so while not directly breaching Integrity, it was still a possibility.

Availability was not directly breached, the company had to take down some of its services temporarily, but it was not directly a result of the attack, more of a result of responding to the attack, by running an investigation first, responding to the incident and then bringing back up their services after the investigation.

# Countermeasures to prevent a future breach

* **Stop hardcoding credentials**
  + This will stop the hacker from being able to escalate privileges and widen the scope of the attack.
* **Add more than one layer of authentication for a privileged access management solution**
  + adding more than one layer will ensure that it is much harder to authenticate into a critical service such as Thycotic PAM.
* **Using methods such as hashing, salting, and stretching to protect credentials**
  + It will be very hard to return the hash from cipher text to plain text and is more secure than storing admin credentials in plain text.

# References

Browne, R. (2022, September 16). *CNBC*. Retrieved from Consumer News and Buisness Channel: https://www.cnbc.com/2022/09/16/uber-investigates-cybersecurity-incident-after-reports-of-a-hack.html

Jackson, M. (2022, September 16). *Uber Breach 2022 – Everything You Need to Know*. Retrieved from GitGuardian: https://blog.gitguardian.com/uber-breach-2022/

Sjouwerman, S. (2022, September 16). *Uber security breach 'looks bad', caused by social engineering*. Retrieved from KnowBe4: https://blog.knowbe4.com/

Uber Team. (2022, September 16). *Security Update*. Retrieved from Uber Newsroom: https://www.uber.com/newsroom/security-update/

M. Qasim Munir [Savitar0x01]. (2022, Sep 22). Something fishy [Tweet]. Twitter. https://twitter.com/Savitar0x01/status/1570580235716014081/photo/1  
vx-underground [vxunderground]. (2022, Sep 16). They disclosed Uber's financial data [Tweet]. Twitter. https://twitter.com/vxunderground/status/1570598055560482817