Case Study on Uber Data Breach

Uber:

- Uber Technologies, Inc. (Uber), based in San Francisco, provides mobility as a service, ride-hailing (allowing users to book a car and driver to transport them in a way similar to a taxi), food delivery (Uber Eats and Postmates), package delivery, couriers, and freight transportation. Via partnerships with other operators such as Thames Clippers (boats) and Lime (electric bicycles and motorized scooters), users are also able to book other modes of transport through the Uber platform in some locations. Uber sets fares, which vary using a dynamic pricing model based on local supply and demand at the time of the booking and are quoted to the customer in advance, and receives a commission from each booking. It had operations in approximately 72 countries and 10,500 cities as of December 31, 2021.

What happened at Uber?

- On September 15, 2022, Uber employees were surprised to find an unauthorized user posting in their company's slack channel. They had hacked their way into the account and left a message that read, "I announce I am a hacker and Uber has suffered a data breach." Uber employees, who did not reveal their identities, admitted that it appeared as if the hacker breached multiple internal applications and accessed sensitive data.
- Although the suspected hacker, who is allegedly only 18 years old, has been arrested, the damage was done.
- The hacker left an explicit image within Uber's internal systems and exposed how they had hacked the company using social engineering.
- Uber is now having to launch their own internal investigation into the incident, and will more than likely to enact a costly remediation plan.

How did the hacker gain access to Uber's internal systems?

- The Uber cybersecurity protocols would have probably been enough to prevent the data breach - if it weren't for the use of social engineering*. The hacker admitted on Twitter that they gained access to the company's internal VPN by tricking an employee into handing it over.
- The threat actor also had access to credentials that allowed them to breach Uber's AWS and G Suite accounts.

    - Social engineering* or the practice of using human emotion to get the victim to perform an action or give the threat actor needed information – is not uncommon in the cybersecurity world.
    - Untrained employees are your biggest area of vulnerability.
    - The threat actor responsible for the Uber breach has also claimed to have used social engineering when launching an attack against Rockstar Games.

Wikipedia had to say this regarding the Uber data breach:

- On September 15, 2022, Uber discovered a security breach of its internal network.[84] A hacker, who identified himself as an 18-year-old, utilized social engineering to obtain an employee's credentials and gain access to the company's VPN and intranet.[85] From there, the individual found powershell scripts which contained administrative credentials which gave them access to Uber's services such as Amazon Web Services and Google Cloud.[86] The individual announced the hack on an internal Slack channel, where many employees thought it was a joke.[87] In a statement on September 16, Uber indicated that there was no evidence that user data was compromised, all services were operational and law enforcement had been notified.[88][89] Additionally, Uber uses services of HackerOne, a Californian bug bounty platform that employs ethical hackers to help identify bugs and protect the systems of many big companies.[90]

Related malicious activity

- Sigma rules developed by SOC Prime developers help security professionals to ensure that their systems can withstand attacks involving MFA- related failures.
- (SIGMA is another tool for the open sharing of detection, except focused on SIEM instead of files or network traffic. SIGMA allows defenders to share detections in a common language.)
- Okta Possible MFS/2FA Flooding/Spamming/Phishing (via user_auth)
    - This identifies failed MFA due to user; a large grouping of these events may indicate mfa/2fa flooding/spamming/phishing.
- Azure Possible MFA/2FA Flooding/Spamming/Phishing (via azuread)
    - This identifies failed MFA due to user; a large grouping of these events may indicate mfa/2fa flooding/spamming/phishing.

Uber Breach 2022 Analysis [SOC Prime]

- The attacker manipulated one of the company's employees into sharing their password, which allowed for the initial access of the target. The criminal hacker then proceeded with launching MFA fatigued* attacks and compromising a worker's Slack account to send out a message announcing to other employees that their company had suffered a data breach, In response Uber has restricted access to Slack for internal communication. Among other compromised services are Google Cloud Platform, OneLogin, SentinelOne incident response portal, and AWS.
    - MFA fatigued*: MFA Fatigue attacks are when a threat actor has access to corporate login credentials but is blocked from access to the account by multi-factor authentication. They then issue repeated MFA requests to the target until the victims become tired of seeing them and finally accept the notification.
- Prior to the incident, logs gathered from infostealers were put up for sale in the underground market. The infostealers that were used in these attacks against Uber employees were Racoon* and Vidar**. The evidence suggests that the attacker used the acquired data to move laterally inside the Uber's network.
    - **Racoon***: Racoon stealer was earlier distributed under the Malware-as-a-Service (MaaS) model.

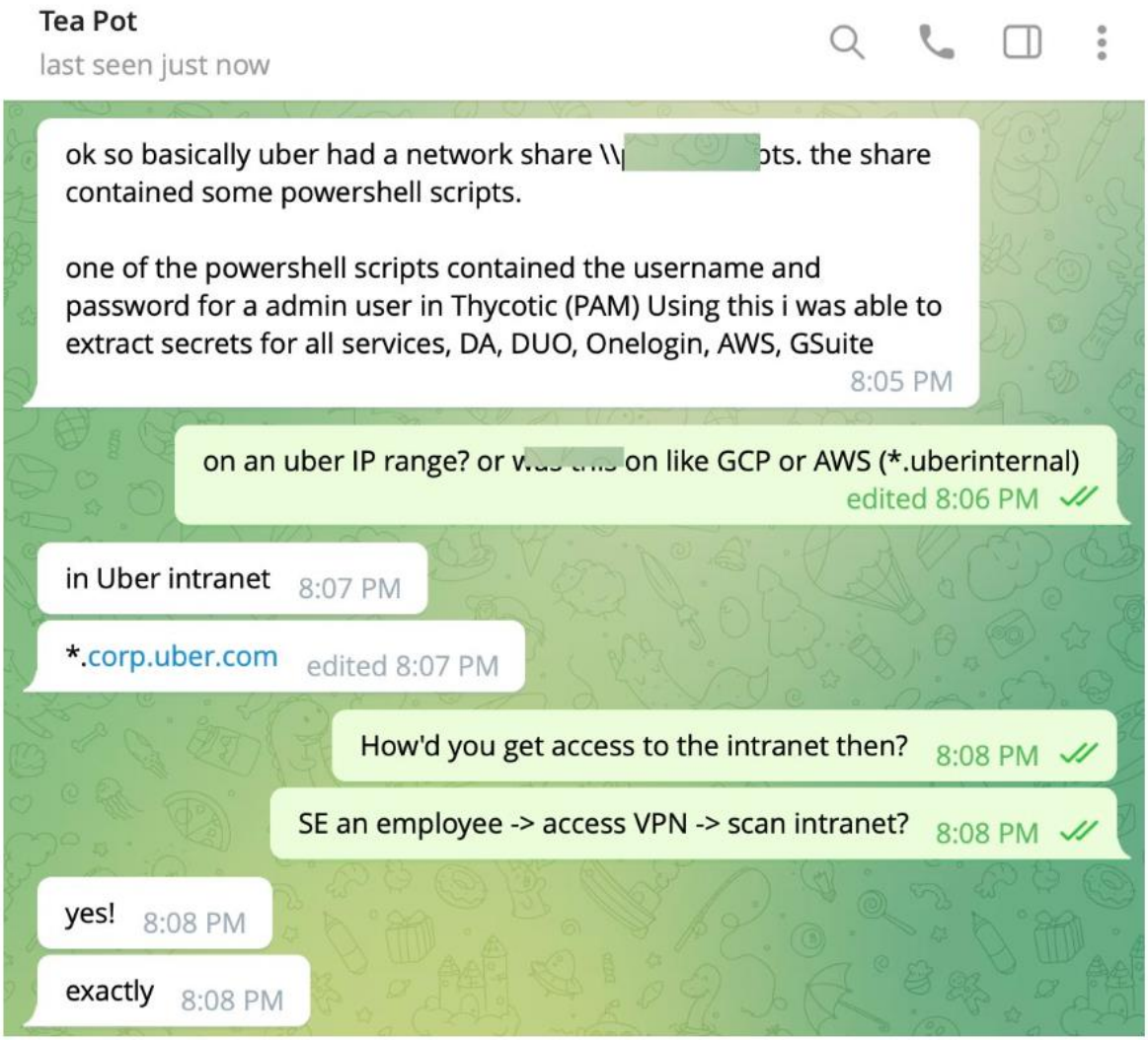
- Racoon Stealer malware was previously reported to have been replaced with Dridex Trojan by the RIG exploit kit as part of an ongoing campaign that resulted in the temporary suspension of the malware operations in March 2022.
- Racoon Stealer 2.0 A.K.A RecordBreaker, is capable of stealing system fingerprints, browser data, crypto wallets, web browser extensions, individuals' files located on all disks, etc.
- Also, the new strain can also take screenshots and grab installed app lists.

- **Vidar**:** Hides within Microsoft Help files.
- Its functionality includes the ability for advertisers to set up preferences regarding type of information they want to steal.
- Previously Vidar was associated with stealing crypto assets, financial credentials, along with multi-factor Authentication (MFA) data, browser history, documents and cookies.

- Motive: Apparently demanded for better pay for drivers.

Timeline

- The attack started with a social engineering campaign on Uber employees, which yielded access to a VPN, in turn granting access to Uber's internal network *.corp.uber.com.
- Once on the network, the attacker found some PowerShell Scripts, one of which contained hardcoded-credentials for a domain admin account for Thycotic, Uber's Privileged Access Management (PAM) solution.
- Using admin access, the attacker was able to log in and take over multiple services and internal tools used at Uber: AWS, GCP, Google Drive, Slack workspace, SentinelOne, HackerOne admin console, Uber's internal employee dashboards, and a few code repositories.



Screenshot from a private message with the hacker on Telegram

- The critical vulnerability that granted the attacker such high levels of access was **hardcoded credentials in a PowerShell script**. These

credentials gave admin access to a Privileged Access Management (PAM) system: Thycotic. This tool carries huge amounts of privilege, making it a single point of failure; it stores both end-user credentials for employee access to internal services and third-party apps as well as DevOps secrets used in the context of software development. **This is a worst-case scenario**. The PAM system controls access to multiple systems, and having admin access means you can give yourself or extract secrets to all connected systems. This has appeared to give the attacker complete access to all of Uber's internal systems.

- This isn’t the first time we’ve seen an Uber data breach: In 2014 hackers gained access to an AWS S3 bucket after developers leaked secrets to a public git repository.
- Two years later, a similar incident happened when attackers exploited poor password hygiene by some developers to gain access to private repositories which contained multiple access credentials.

How bad is it? [GitGuardian]

- **Thycotic – Severity = Critical**
  - The attacker gained admin access to the Thycotic PAM system. PAM systems can be a single full-featured software console or a collection of multiple tools; in the case of Thycotic, it is a single tool with many features. It can control access to different services and also has a secrets manager where credentials and passwords are stored.
- **AWS instance – Severity = Critical**
  - The AWS instance controls the cloud infrastructure of Uber's applications. Depending on configuration, privileges, and architecture, the attacker can potentially shut down services, abuse computing resources, access sensitive user data, delete or ransom data, change user access, and many more things.
- **VMware vSphere – Severity = Critical**
  - VMware vSphere is a cloud computing virtualization platform. This is a critical platform as it interfaces with both cloud computing and on-premise servers which can give attack access to controlled on-premise servers as well as many administrative functions that would help an attacker move deeper into systems.
- **SentinelOne – Severity = High**
  - SentinelOne is an XDR (eXtended Detection and Response) platform. Simply put, this platform connects to your mission-critical systems and lets you know if there are security issues. Any attacker that can obtain privileged access to this system can obfuscate their activity and prolong their attacks. XDRs can bake in "backdoors" for Incident Response (IR) teams, such as allowing IR teams to "shell into" employee machines and potentially widening the attacker's access.
- **Slack workspace – Severity = Medium**
  - The internal messaging system of Slack can be used to great effect as an attacker to launch phishing campaigns. As the attacker has the instant trust of other users, they can send malicious links, try and get admins to elevate their privilege, and access sensitive information.
- **GSuite Admin – Severity = Medium**
  - GSuite is a tool used by many companies to manage their users, store data, and many other administrative tasks. With admin access, the attacker can create and delete accounts, but would also

likely have access to employee data and other sensitive company data.

- **HackerOne – Severity = Medium**
    - HackerOne is the platform used to pay and communicate with security researchers that find vulnerabilities within systems for rewards. Given the level of detail bounty hunters usually provide, anyone with access to the HackerOne tenant has detailed how-tos on how to exploit (likely unpatched) vulnerabilities in other areas of their IT systems. This means persistence is highly likely.

Vulnerabilities

- Uber's system vulnerability came to the fore when its native Privileged Access Management (PAM) platform admin credentials were compromised.
- Predefined parameters in a PowerShell script are a significant weakness that gives the attacker such extensive access.
- First, they failed to monitor login attempts properly. Uber doesn't receive notifications if third-party tries to log into a business account but fails to enter the network. These failed entry attempts don't trigger Uber's security system networks, which shows an apparent lag in the system.
- Second, Uber failed to restrict the available data to third-party apps. Such easy availability allows hackers to access sensitive information from other linked third-party apps.
- Thirdly, there is a possibility this attack was a result of phishing. In phishing, hackers pose as a trustworthy person or entity to gain access to sensitive information. This breach is notable as there have been multiple breaches in Uber's history. Such multiple violations are unusual, as most breaches only happen once or twice.

Cost of the data breach

- The recent hack of September 2022 is under investigation and it's too early to know the full extent of this data breach.
- A hack in 2016 compromised the personally identifiable information (PII) of some 57 million Uber customers and drivers, including 600,000 drivers' licenses. To date, Uber has settled multiple claims for $148 million with the 50 states, and several class action suits are pending along with a settlement with the Department of Justice.
- The hack of 2014 compromised the data of more than 100,000 Uber drivers, in some cases including PII, which can lead to identity theft.

Prevention

- **How can phishing attacks be avoided?** Companies should be aware that the "human factor" is one of the largest contributors to cyber-attacks and network breaches.
- **Security training** – Help employees identify suspicious emails and avoid falling victim to their schemes.
- **Secure Web Gateway** (SWG) – A SWG processes all user Internet requests and can identify phishing sites and block corporate user attempts to reach them.

- **Corporate network infiltration**– Enabling inadequately secure and unrestricted access to corporate networks makes hackers' lives easy and potential damage much more devastating.
- **How can VPN access be more secure?** Obtaining user credentials shouldn't be enough to gain access to corporate networks, and even when they are, they shouldn't enable unrestricted lateral movement within the network. This can be avoided by:
- **Multi-factor authentication (MFA)** – By implementing an MFA solution, users must provide additional proof of who they are (i.e. token, code, fingerprint, etc.). Even if hackers can compromise a user's credentials, they will likely not be able to supply the additional required proof–though MFA is vulnerable to social engineering if precautions aren't taken.
- **Zero Trust Network Access (ZTNA)** – A secure access mechanism such as ZTNA limits any specific users' access to network resources. By implementing a least privilege approach, ZTNA limits access only to those systems explicitly allowed to said user. This greatly limits the capacity of lateral movement and the ability to compromise sensitive resources outside the scope of the user's granted access.
- **Device Posture Checks (DPC)** – Adding a mechanism that continuously monitors all corporate endpoints to make sure they are meeting the defined requirements and comply with geo and time-based restrictions goes a long way in preventing non-corporate devices from accessing and breaching the corporate network. It also can be used to enforce access only from pre-approved managed devices of the organization.

- **Admin credential exploitation** – In the event additional credentials are obtained, especially ones of higher privilege, additional access restrictions should be put in place. The best practice to help prevent this is, once again, the implementation of a Multi-Factor Authentication (MFA) mechanism. The greater the privileges a user has, the stricter this restriction should be, possibly requiring additional verification forms beyond those required from other users.

References

- mitnicksecurity
- SOC Prime
- GitGuardian
- Wikipedia
- Ponemon Institute report
- Perimeter81

Gathered and Compiled by –

Indrajith S B

04 December, 2022

As part of IBM Cybersecurity Analyst Capstone Project.