Data Breach Case Study

Uber Technologies, Inc.

Attack Type: Data Breach

Social Engineering combined with phishing

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.

Uber provides mobility as a service, ride-hailing, food delivery, package delivery, couriers, and freight transportation. The Uber business model is also known as a multisided platform business model, as it connects drivers (offer) and passengers (demand), in order to offer cheaper transportation and an additional source of income.

Company Description: Uber Technologies, Inc. (Uber), based in San Francisco, provides mobility as a service, and other services 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.

Incident Summary: On September 15, 2022, Uber discovered a security breach of its internal network. 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. 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. The individual announced the hack on an internal Slack channel, where many employees thought it was a joke. 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. 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.

Timeline

Uber Data Breach

Social Engineering

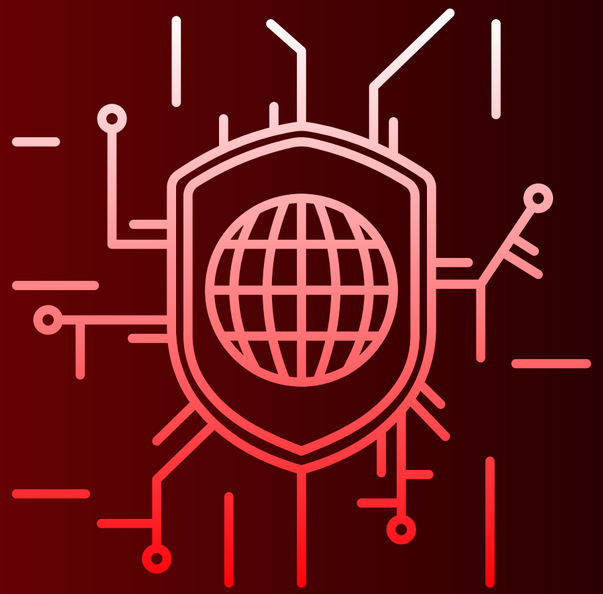
- The attack started with a social engineering campaign on Uber employees, which yielded access to a VPN, in turn granting access to Uber's internal network *.corp.uber.com.

PowerShell Scripts Discovery

- 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.

Admin Access

- 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.



Workspace Defecation

- The hacker left an explicit image within Uber’s internal systems and exposed how they had hacked the company using social engineering.

Internal Investigation Launched

- Uber is now having to launch their own internal investigation into the incident, and will more than likely to enact a costly remediation plan.

Hacker Arrested

- Although the suspected hacker, who is allegedly only 18 years old, has been arrested, the damage was done.

Vulnerabilities

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.

Privileged Access Management (PAM)

- Uber's system vulnerability came to the fore when its native Privileged Access Management (PAM) platform admin credentials were compromised.

Phishing

- 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.

Monitor login attempts

- 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.

Third-party data exposure

- 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

Cost

- 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.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.

- 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.

Done By-

Indrajith S B