CASE_STUDY.docx

by Madhur MAHAJAN

Submission date: 24-Oct-2024 01:34AM (UTC+0530)
Submission ID: 2495054813
File name: CASE_STUDY.docx (238.52K)
Word count: 3517
Character count: 19364

Project ID: 41

॥वसुधैव कुटुम्बकम्॥

SYMBIOSIS INSTITUTE OF TECHNOLOGY, PUNE

Cyber Security Project

"A Case Study on Uber Data Breach"

CA-3

Course Coordinator
Dr. Pooja Bajane

Group Members

Madhur Mahajan	22070122508
Aanchal Mehta	22070122509
Shivam Rajput	22070122513
Ratan Singh Madrecha	22070122516

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

INTRODUCTION

Overview of Uber Technologies Inc.

Uber Technologies which has their base in the US is a global provider of mobility services and operates in four business segments, namely, ride-hailing “Uber”, food sanitation and delivery under Uber Eats business, package delivery and freight transport. The company applies various pricing models which offer flexible fares depending on the current influx and flow of clients which in turn puts them in the lead of other companies operating in this field. By 2021, Uber had got registered operations in over 72 countries and cities more than ten thousand.

The Incident: What Happened at Uber?

Uber's internal communications were disrupted on September 15, 2022, when an insider entered the systems and began sending messages in the organization's Slack channel without authorization. The intruder openly proclaimed, 'I proclaim I am a hacker and Uber was hacked in respect to its databanks.' It was discovered that the hack did not need much cleverness; actually, he had successfully executed social engineering on Uber's critical infrastructure where he successfully breached into their internal VPN, AWS, and even G Suite accounts.

ABSTRACT

In September of 2022, the Uber Technologies Inc., which is a multinational transportation network company and also specializes in ride sharing around the globe, suffered a loss as its great internal systems were recently hacked. The hacker used social engineering approaches, taking advantage of Uber's inflexible security structure that relied heavily on poor employee education and weak MFA (Multi Dual-factor Authentication). This report elaborates the incidence; from how the breach occurred, to the security weaknesses it exposed, and what other strategies would have lessened the breach, if any. Such breaches form the bulk of worst case scenarios worth considering at the time when corporate firms are almost entirely digitalized.

LITERATURE REVIEW

Cybersecurity has turned out to be one of the most necessary evils for the 21st century organizations since they have to keep up with the demands of technology. Citing Ponemon Institute's cyber security reports, it has been established that human mistakes, like clicking on phishing emails, account for a large number of data breach cases. In the same spirit, GitGuardian asserts that organizations are doing a very poor job of ensuring that their employees, who are the primary targets of social engineering campaigns, are well versed on how to deal with these attacks.

METHODOLOGY

The analysis of Uber's data breach is based on public sources such as incident reports from cybersecurity firms, statements from Uber, and other verified reports. The data was gathered through a thorough review of documentation related to the incident, focusing on the techniques used in the attack, vulnerabilities exposed, and recommendations for prevention. Additionally, reports from Uber's cybersecurity partners and experts in the field were reviewed to provide insights into the company's internal response mechanisms and security gaps.

RESULTS & DISCUSSIONS

The evaluation of the Uber data breach has been carried out with the help of reliable information sources consisting of incident descriptions from cybersecurity companies, Uber's statements, and other trustworthy reports. The information was collected via analyzing documents connected to the event, aimed at the methods of the attack, issues revealed, and measures for averting recurrence of such breaches. Enterprises dealing with cybersecurity and experts about the Uber Company were also consulted to understand the internal mechanisms employed by the Company in dealing with the situation and its weaknesses.

UBER:

- Uber Technologies, Inc. (Uber) is headquartered in San Francisco. Uber is the ride-hailing app that enables users to book a car and driver that will take them to the post or packages like couriers, and Deliver food (Uber Eats and Postmates). Uber Technologies Inc. partners with various transportation service providers, including Thames Clippers (boats) and Lime (electric bikes and motorized scooters) to allow their users to book for other transportation services within some geographic locations through the Uber platform. Uber determines all fares which differ as there is a dynamic pricing structure dependent on the where and when a transaction was made. It then takes a steady cut from every booking made. As of December, it had been active in about 72 countries across 10,500 cities

- In this regard, Wikipedia was obliged to discuss the Uber data breach.

- – On September 15, 2022, Uber confirmed that its internal network had been compromised. An 18-year-old self-identified hacker was able to gain access to the company’s VPN and intranet after he used social engineering to convince one of its employees to provide him with their credentials. As a result, that person found powershell scripts that were saved alongside administrative credentials that provided access to services such as Amazon Web Services and Google Cloud which were also used by Uber. The hacker claimed for the breach on the firm’s internal Slack channel and most employees took it to be an internal joke. In Uber’s Statement issued the following day, however, it stressed that there was no damage to the data of any users and there was no compromise of any services provided to users. They confirmed that nobody has been arrested but the police have been informed of the act of crime. Furthermore, Uber has engaged the services of HackerOne, a California based bug bounty site that uses a pool of ethical hackers to seek out bugs in an attempt to secure numerous organizations.

- Similar illicit works

- – Based on this, another writer in the field, this time from the SOC Prime company that developed the security rules known as Sigma from which the developers employed by SOC are able to enforce tighter security into the systems targeted against attacks involving MFA devices or even their encounters.

RELATED MALICIOUS ACTIVITY

- To counter related malicious activity that seeks MFA failures, SOC Prime developers have come up with Sigma which most security practitioners may find useful.
- (SIGMA is another tool for the open sharing of detection, except focused on SIEM instead of files or network traffic. SIGMA makes it possible to share the detections among defenders in one common language.)

- Okta Possible MFS/2FA Flooding/Spamming/Phishing (via user_auth)

This identifies failed MFA because of user; accumulation of these events would suggest mfa/2fa flooding or spamming within that user base.

- Azure Possible MFA/2FA Flooding/Spamming/Phishing (via azuread)

This identifies failed MFA because of user; since these are considerable number of events, it would appear as mfa/2fa flooding or spamming within that user base.

ANALYSIS OF THE UBER BREACH 2022

- There is evidence that one of the employees was social engineered into sharing their password which granted the initial access of the target. The criminal hacker then goes on to initiate more multi-factor authentication fatigue* attacks, and there is an instance where the employees' Slack account is hacked to send out a data breach announcement to the entire company. In its reaction, Uber has now limited access to the internal communication platform - Slack. Other effected systems include GCP, OneLogin, SentinelOne incident response portal, AWS cloud storage among others.

MLA Factors*: MFA Fatigue attacks are when a threat actor has access to corporate login information but has been restricted from accessing the account by multi-factor authentication. A threat actor uses this strategy among others to wear down the targeted account to the point of ubiquity where the victim would succumb and click override.

- Prior to the incident, logs gathered online from infostealers were being shopped in the underground market. The infostealers that were used in these attacks against Uber employees were Racoon and Vidar. So, these people obtained the data for the purpose of lateral movement to Uber's site.

Racoon*: the patented Racoon stealer was earlier circulated in the fashion of malware as a service model.

It has been found that the RIG exploit kit has replaced the Ever evolving Racoon Stealer malware and changed it to the Dridex Trojan which resulted in a temporary break in the operations of the malware in March of 2022.

Record Breaker 2.0 A.K.A Racoon Stealer, is able to steal system fingerprints, crypto wallets, browser history, browser extensions, files located around all available disks and more.

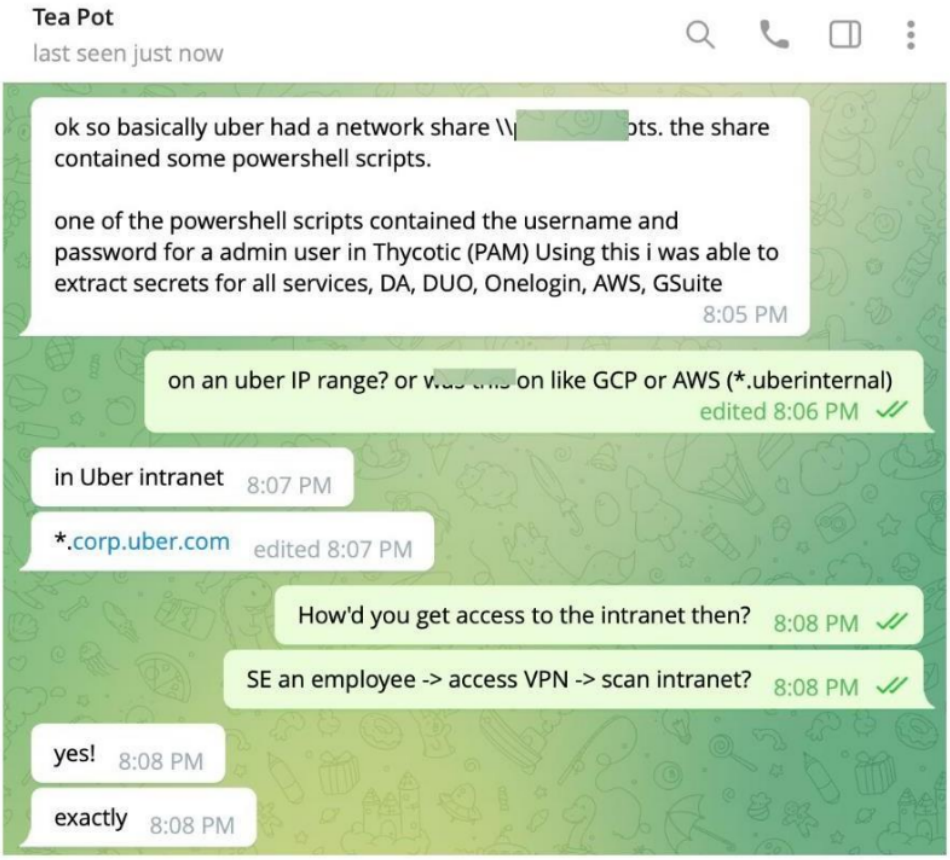
Keyboard's shortcuts CTRL+Z and CTRL+Y are other common terms used by the newer strain to take screenshots and grab the lists of the installed applications.

Microsoft's Help files contain images and code embedded within Microsoft Help files which contains Vidar.

The single click operation's functionality includes the possibility for advertisers to select their area of thievery.

- The hacker group which was once known for stealing crypto assets and financial credentials, has now transitioned to stealing multi-factor Authentication (MFA) data, history of browsers, documents, and cookie files.
- Apparently there existed a demand for better payment rates for the drivers which is most probably the cause of the heist.
- The heist started gaining traction in Germany with social engineering of Uber employees hence bingo a VPN was obtained and gave internal access to the internal network *.corp.uber.com of Uber.
- While still in the network, the attacker sighted some Powershell Scripts and was able to focus on a script that was storing domain admin accounts to Thycotic which is the Privileged Access Management solution for Uber.
- Using admin rights, the attacker was able to gain access

- From a logged-in perspective, the hacker with administrative privileges was able to lead a multitude of Ubers key services and tools including AWS, GCP, Google Drive, Slack workspace, SentinelOne, the admin console for HackerOne, Uber's internal dashboards for employees, and some code repositories.



Screenshot from a private message with the hacker on Telegram

- The critical weakness which enabled the attacker to login into administrator's areas was hard-coded passwords in PowerShell scripts. These credentials allowed obtaining administrator privileges in the PAM system Thycotic. Such a tool carries regard privileges. Even so, the PAM is a single point of failure. PAM encompasses employee endorsements for internal services access and external applications usage, as well as software development coding secrets. This is the most catastrophic scenario. PAM governs access to several systems. Therefore with authority over such an account one can create, obtain or provide himself with all resources in relation to all other interlinked

systems. Therefore this appears to have enabled the attacker access to the entire Uber systems.

- On this occasion, it is not the first Uber leak that we have witnessed, in 2014 civilian hackers breached an AWS S3 bucket once developers bothered to leave some secrets on 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?

- VMware vSphere – Severity = Critical

While VMware vSphere is a cloud computing virtualization platform. This one is critical as it connects with both the cloud environment and on-premise servers allowing attack accessibility through the controlled on-premise server plus a myriad of administrative functions that could allow the attacker to a deeper penetration of the systems.

- SentinelOne – Severity = High

SentinelOne is an XDR (extended detection and response) platform. To put it simply, this platform links with your key systems and notifies you of any security breaches. An attacker that gains access to high privileges on this system can disguise their activities and further extend their attacks. XDRs have the capability to embed "back doors" even for Responders for Incidence Response (IR) teams for instances to allow ER teams to shell into employees devices hence lettings the attacker gain more access.

- Slack workspace – Severity = Medium

The internal communication tool of Slack can serve a wonderful medium for attacking phishing campaigns as the attacker has the instant trust of other users and the ability to send malicious links and or tries to persuade administrators to enhance their privileges to sensitive information.

- GSuite Admin – Severity = Medium

GSuite is a tool that is employed in many organizations to perform user management, data storage and many other administrative activities. As an admin, the intruder would not only be able to delete or create accounts but would also have employee and other sensitive organizational data.

- HackerOne – Severity = Medium

HackerOne is the service where vulnerabilities with a system are located and rewarded by a security researcher and is used to pay and interact with them. Bounty hunters are generally very detailed in their reports and people with access to the HackerOne tenant have very detailed reports on how to perform exploits on other unpatched parts of their IT systems. This means persistence is more likely.

VULNERABILITIES

- Uber self-reported an insecurity within its system that occurred due to a compromise in the native credentials of the Privileged Access Management (PAM) platform administrators.
- One of the notable weaknesses is that empty variables inside a PowerShell script broaden the attacker's access.
- To begin with, there were no due processes in place to track the number of times an attempt was made to log into the system. At present, Uber does not receive alerts whenever a user fails to successfully log into a business account owned by Uber. These unsuccessful network entries do not cause Uber's security networks to engage which is an indication of a system with delays.
- Second, Uber did not seek to limit the data to be accessed by the third – party applications. There is serious concern since many are able to gain access to sensitive data from other linked third-party apps.
- Thirdly, it may also be the case that this particular attack came as a result of executing a phishing scheme. Phishing is a kind of computer fraud where a hacker impersonates someone trustworthy to obtain sensitive information for malicious reasons. This intrusion is particularly significant due to the fact that it is when taken together with its context in past events in Uber's history. The number of breaches in this case may be considered high as breaches in majority are losit one or two.

COST OF THE DATA BREACH

- Handling: There has been a reported breach in the recent months, specifically in September 2019 when it appears a cyber attack took place. The details surrounding that breach are still being investigated and it is too soon to understand how many accounts in total were breached along with other details which are pertinent to the topic.

- A hack in 2016 comprised PII of 57 million Uber customers and drivers including the license of approximately 600,000 drivers. An agreement or settlement of 148 Million US dollars have been reported through various state jurisdictions with additional ten settlements pending pertaining to class action suits filed alongside the Justice Department.

- In somewhere around 2014 a hack was performed that lead to an unauthorized breach of data containing information on drivers associated with Uber. To some extent, the information may contain the PII which puts the owners at risk of total exposure and identity theft.

PREVENTION

- How can phishing attacks be managed? The employers should keep in mind that the 'human element' is one of the greatest sources of cyber-attacks as well as breaches of the network.

- **Security training** – Order employees to be able to spot suspicious emails and avoid being duped by the emails.

- **Secure Web Gateway (SWG)** – A secure web gateway allows the worker to send the internet request and distinguish phishing attacks and prevent the employees from attempting to access the phishing sites.

- **Ingress into a corporate network** – Allowing weak and open access to corporate networks only makes it convenient for the hackers and mitigating the impact can be extremely difficult.

- **What's the best way to enhance VPN access?** Perhaps the most basic requirement is that merely having user log in credentials should not be sufficient to grant access to corporate networks however in the actual scenario they still allow free lateral access to the entire network. This can be avoided by:

- **Multi-Factor Authentication (MFA)** – With the use of an MFA solution, users are required to authenticate more than just their passwords. This extra proof could be a token, a code, or a thumbprint for example. Even if hackers manage to steal the credentials of a user, they will most likely not produce the additional verification needed. However, MFA is also easily targeted through social engineering attack unless steps are taken to prevent this.

- **Zero Trust Network Access (ZTNA)** – ZTNA allows an authorative figure to impose policies that limit how much system/network resources a specific user can access. By adopting a least privilege methodology, ZTNA access is limited only to particular systems that have been defined as permissible to that user. This significantly minimizes the extent of lateral movement and the potential to compromise invaluable assets that lie outside the user's accessibility privileges.

- **Device Posture Checks (DPC)** – Implementing a feature that constantly tracks all corporate endpoints to ensure that these devices satisfy the set standards, are within the geographical location and the time frames usually greatly minimizes the percentage chances of uncontrolled devices penetrating the corporate network. It can equally be employed to limit access to only selected managed devices approved by the organization.

- **Admin credential exploitation** – In the occurrence that extra credentials are received, particularly of a higher rank, these obligate the need for more additional access restrictions. The ideal position for this management process best preventive measure is, again, through the enforcement of Multi-Factor Authentication (MFA) mechanism. The user with high privileges has a greater number of restrictions and generally, more sophisticated controls are placed them above the rest of the employees.

THE UBER DATA BREACH HAD SEVERE CONSEQUENCES:

1. Vulnerabilities of the Systems: The attack resulted in the compromise of sensitive systems such as the Uber AWS and GCP along with other internal comms, which had significant implications to the operational aspect of the business.

2. Brand Crisis: Uber lost some of its business image because it was not the first time this company was hacked. This mattered to investors as Uber's previous lapse in cyber practices, this was not going unnoticed.

3. Economic Violence and Legal Cost: Despite the loss from the 2022 data breach not being fully quantified, earlier occurrences have seen Uber pay in the millions as part of their settlement.

CONCLUSION

The Uber data breach of 2022 exposed critical weaknesses in the company's cybersecurity infrastructure, particularly in its human element and multi-factor authentication protocols. The attack illustrates how social engineering, coupled with technical vulnerabilities like hardcoded credentials, can lead to catastrophic breaches. Moving forward, Uber and other organizations must prioritize employee training, implement more robust MFA mechanisms, and adopt a Zero Trust approach to network security. By addressing these vulnerabilities, companies can significantly reduce the likelihood of future breaches.

REFERENCE

1. SOC Prime - Sigma rules for MFA-related failures.
2. GitGuardian - Privileged Access Management (PAM) vulnerabilities.
3. Ponemon Institute - Cybersecurity insights and data breach statistics.
4. Mitnicksecurity - Social engineering methods and defenses.
5. Perimeter81 - VPN and Zero Trust Network Access (ZTNA) security measures.
6. Verizon Data Breach Investigations Report (DBIR) 2023 - Overview of data breaches across various sectors.
7. CrowdStrike Global Threat Report - Understanding social engineering tactics used in modern cyberattacks.
8. HackerOne - Bug bounty platform and how ethical hacking is used to prevent vulnerabilities.
9. Microsoft Security Intelligence Report - Best practices for defending against phishing and social engineering attacks.
10. Cybersecurity and Infrastructure Security Agency (CISA) - Guidance on multi-factor authentication and threat mitigation.
11. OWASP (Open Web Application Security Project) - Guidelines for protecting against social engineering and phishing.
12. NIST (National Institute of Standards and Technology) - Guidelines on cybersecurity frameworks.
13. IBM X-Force Threat Intelligence Index - Analysis of cyber threats, with a focus on phishing and social engineering.
14. FireEye (Mandiant) - Incident response reports on social engineering breaches.
15. MITRE ATT&CK Framework - Techniques related to social engineering and privilege escalation.
16. Thycotic - Privileged Access Management (PAM) and securing administrative credentials.
17. Fortinet - Multi-factor authentication (MFA) fatigue and strategies for mitigation.
18. Sophos Labs - Analysis of ransomware and social engineering attack vectors.
19. Kaspersky - Research on phishing and its evolution in targeted attacks.
20. Rapid7 - Security analysis of enterprise systems vulnerable to social engineering.
21. Palo Alto Networks - Overview of advanced persistent threats (APTs) and how social engineering plays a role.
22. Check Point Research - Data breach prevention methods and cybersecurity strategies.
23. Trend Micro - An in-depth analysis of the rise in cyberattacks using social engineering techniques.
24. Cisco Security - How organizations can defend against network infiltration and lateral movement post-breach.
25. Gartner - Best practices for implementing Zero Trust Network Access (ZTNA) in corporate environments.
26. McAfee - Security challenges related to cloud systems (AWS, GCP) and privileged access breaches.
27. Dark Reading - Lessons from high-profile data breaches, including the Uber case.
28. SANS Institute - Case studies on the importance of employee training in preventing cyber breaches.
29. Symantec - Threat intelligence on phishing and social engineering tactics.
30. Wired - Investigation reports on the Uber data breach and hacker tactics used.

CASE_STUDY.docx

ORIGINALITY REPORT

8%	8%	0%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	cherrypatel.blogspot.com Internet Source	6%
2	socfortress.medium.com Internet Source	1%
3	blog.gitguardian.com Internet Source	1%
4	www.bleepingcomputer.com Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	Off		