Uber Hack 2022- A devastating social engineering attack

Varad Magare[1], Satyam Shinde[2], and Priyanka More[3]
[1]*Varad Magare, VIT, Pune*
[2]*Satyam Shinde, Suma soft, Pune*
[3]*Priyanka More, MMCOE, Pune*

***Abstract*—We live in the 21st century, An era of digitalization. In the last decade, we have seen an enormous amount of growth in the use of internet-connected devices which include mobile phones, laptops, computers, smart watches, tablets, smart televisions, etc. People are using the internet like never in the history. Some popular websites are getting a billion hits a day. But with increased features comes the increased risk of cyber-attacks. Recently, an 18 years old young attacker breached the security of Uber and released pictures of gaining access to Uber's internal infrastructure. This paper covers the technical aspects of this cyber-attack and explains the whole timeline.**

***Index Terms*—Cyber-Attacks, Digitalization, Internet, Uber, Websites.**

I. INTRODUCTION

Nowadays, the Use of the World Wide Web is at its peak. People use websites for different purposes such as buying stuff online, Entertainment, Researching and collecting information, Learning, Trading, Video conferencing, and Chatting. Usage of the internet and websites is included in day-to-day activities. And almost every sector is using web applications, and mobile applications for different purposes nowadays.

Daily new websites are getting created and hosted on the world wide web. Due to skill gaps in the cyber security field and unawareness of security vulnerabilities, websites are often vulnerable to serious bugs which can cost a ton to businesses and their customers. There have been many incidents of data breaches where the company has suffered huge losses due to cyber-attacks.

In January 2018, Records of over a billion Indian citizens were leaked from the government's ID database. In February 2021, CD Projekt RED suffered a ransomware attack that breached the source code of their popular games. The data was open publically on the dark web. So, no matter how strong security measures companies take, they have to be extra cautious when it comes to security. No matter how well-protected companies are, no system is totally immune to attack. The same happened with Uber. Despite best efforts, in a well-protected environment, Uber got hacked.

They say, Weakest link in cyber security which we can't eliminate totally is a victim of social engineering. On September 16th, 2022 an 18-Years-Old hacker claimed to breach Uber and shared screenshots of accessible internal systems. The hack involved different stages but it initiated with social engineering which is considered as the most powerful weapon in the cybersecurity field.

II. WHAT IS SOCIAL ENGINEERING?

Fig: An image describing social engineering

Social engineering is a technique used by cybercriminals to reveal specific sensitive information or perform sensitive actions from victim unknowingly leading to malicious activity. Social engineering got popular with famous American security consultant & hacker Kevin Mitnick. He has written a book named "The Art of Deception" in 2001, which covers the art

of social engineering and tells us how easy it is to manipulate a human to reveal the information we are interested in.

Nowadays, Scams related to social engineering are happening more often. Many times people are getting scammed by hackers disguised as bank's employee trying to steal their credit card information.

III. STAGES OF THE UBER ATTACK 2022

A. Social Engineering

An Attack began with a hacker running social engineering campaign on Uber employees. One of them fell victim to this trick which granted access to a virtual private network which is very essential for sending requests in the intranet.

B. MFA Spamming

Spamming is a technique in which malicious hacker sends repetitive messages/phishing links to multiple users to gain sensitive information. One of the Uber employees was targeted by a hacker for this attack. The attacker pretended to be a support engineer from the IT & Support department of Uber company and tricked the victim to give Multi-Factor Authentication(MFA) code.

C. VPN Access

After getting the MFA code, Attacker got initial access to the network via VPN and shared code.

D. Discovery

Then, the Attacker did reconnaissance over Uber's internal infrastructure and network and gathered information that can be used in the later stages of the attack.

E. Hardcoded Credential in Scripts

During the reconnaissance phase, the Attacker discovered hardcoded credentials of Thycotic in one of the PowerShell scripts.

F. Access to internal services

The attacker used this PowerShell script to login into the domain administrator account of Thycotic which is Uber's privileged access management system. It further led to extracting secret passwords of all of Uber's important services.

IV. SEVERITY

The severity of this attack was very critical. It can be determined by services got breached due to the attack. The attacker got access to Thycotic which led to disclosing passwords of different services such as,

A. Amazon Web Services-Critical

Uber uses AWS for their cloud infrastructure. Getting access to AWS means attacker can potentially get access to sensitive information, shut down services, and delete-modify data according to will.

B. VMware vSphere-Critical

VMware vSphere is used for the virtualization of cloud platforms. Access to VMware vSphere can give more controls and privileges to attackers.

C. GSuite-Critical

Many companies use GSuite for managing users, managing administrative controls. With access to this attacker can delete, and add user accounts. Also, It may lead to sensitive information disclosure as employees' data may be stored on GSuite.

D. Slack-High

Slack is used as an official medium of communication for daily activities by many companies. Access to Slack may lead to sensitive information disclosure about the company's current product, future product, and source of the same.

V. CONCLUSION

The risk of cyber intrusions looms over all enterprises, irrespective of their scale. Organizations must comprehend the sheer potency of social engineering and fortify their workforce with resolute defenses against it. Additionally, a diligent effort must be made to consistently scrutinize and eradicate hardcoded passwords. Employing these collective methodologies cannot ensure complete immunity for your establishment, but they will unquestionably diminish the probability of succumbing to cyberattacks in this era dominated by the internet.

VI. REFERENCES

[1] Ravie Lakshmanan. “The Hacker News Article.” 2022.
[2] Pieter Arntz. “Uber hacked by Malwarebytes” 2022.
[3] TUSHAR P. PARIKH, DR. ASHOK R. PATEL, “Cybersecurity: Study on Attack, Threat, Vulnerability” (IJRMEET) 2017.
[4] Mackenzie Jackson “Uber Breach 2022 – Everything You Need to Know.” 2022
[5] VeenooUpadhyay, Dr.SuryakantYadav, “Study of Cyber Security Challenges Its Emerging Trends: Current Technologies”5 IJERM 2349-2058 (2018).