KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Lessons to learn from the Uber security breach

Tracker ID: TN0924 **Date:** 27/Sept/2022 **Category:** Incident **Industry:** All **Region**: All

Background

Uber Newsroom issued a Security Update on September 15, reporting that they had encountered a cybersecurity incident and were coordinating with law enforcement to contain the breach. They announced a day later that their investigation and response activities are underway, and that they have no evidence that the attacker acquired access to sensitive user data. They claim that all services are operating, including Uber, Uber Eats, Uber Freight, and the Uber Driver app. Meanwhile, the internet was swamped with screenshots of several critical Uber portals and systems revealed by the attacker, including AWS, OneLogin, Google Cloud Platform, SentinelOne's incident response portal, Slack and even the bug bounty portal HackerOne. These accesses were obtained by leveraging an internal network share that had PowerShell scripts with privileged admin credentials, mocking the giant organization's security mechanisms.

Uber issued an update on September 19 that linked its current intrusion to an attacker associated with the notorious LAPSUS$ threat group, which has breached Microsoft, Cisco, Samsung, Nvidia, and Okta this year. The attacker used a stolen Uber EXT contractor's credentials in an MFA fatigue attack, in which the contractor was flooded with two-factor authentication (2FA) login requests until one of them was granted. The attacker then gained access to numerous other employee accounts, granting the attacker increased capabilities on a variety of platforms, including G-Suite and Slack. Uber, on the other hand, asserted that no unauthorized code changes had been performed and that there was no evidence that the hacker had access to the production systems that underpin its customer-facing apps.

As the attack unfolds, it appears that the attacker targeted an Uber Incident Response Team employee using a combination of social engineering and phishing. According to the Group-IB, an "EXT contractor's" personal device was earlier infected with a malware and company account credentials were stolen and sold on the dark web. Also, at least two Uber employees in Brazil and Indonesia had been infected by Raccoon and Vidar information stealers. The attacker utilized the stolen credentials to gain access and evaded the MFA again using a basic social engineering approach. The attacker overwhelmed the victim with multiple MFA "Push" requests in a single hour while simultaneously contacting him via WhatsApp, telling him that the attacker was from the Uber IT team and that the employee needed to accept the MFA "Push" to stop receiving multiple MFA prompts.

Once inside the Uber network, the attacker merely browsed the Intranet and obtained PowerShell scripts with admin user credentials to the privileged access management tool "Thycotic“, from which it was most likely able to "extract" passwords for various services, including DA, DUO, OneLogin, AWS, and GSuite. Furthermore, the hacker got access to the company's HackerOne bug bounty program during an internal investigation and is accused of accessing and downloading every bug report submitted to the company by white-hat hackers. This access was also used by the attacker to modify a policy that ensured he was notified whenever HackerOne received a submission.

The hacker is accused of gaining access to various critical internal systems and apps, forcing the firm to disable its internal communications and engineering systems to contain the damage. This same perpetrator was also alleged to have penetrated the security of video game developer Rockstar Games.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Lessons to learn from the Uber security breach

Tracker ID: TN0924 **Date:** 27/Sept/2022 **Category:** Incident **Industry:** All **Region**: All

On September 23, the City of London Police detained a 17-year-old student from Oxfordshire on suspicion of hacking in connection with the recent wave of high-profile breaches directed at Uber and Rockstar Games. Both intrusions are said to have been committed by the same threat actor, aka Tea Pot (aka teapotuberhacker). The administrator of an illegal internet forum claimed that the teapotuberhacker was the same person who supposedly hacked Microsoft and 'owned' Doxbin. It is also known as White, Breachbase, and WhiteDoxbin, and is thought to be "LAPSUS$'s apparent ringleader". Uber, working in coordination with the FBI and US Department of Justice, is yet to share an update regarding this arrest.

MITRE ATT&CK Tactics

Reconnaissance, Initial Access, Credential Access, Discovery, Defense Evasion, Impact, Privilege Escalation and Lateral Movement.

Recommendations

- Regular phishing awareness and training should be implemented throughout the workplace. Make sure employees are aware of any active phishing threats.
- Employees should be trained to recognize and report suspicious emails and messages as soon as possible. Ensure that only authorized platforms are used for work-related communication.
- As a precaution, enable automatic (temporary) account lockouts via the MFA provider when multiple prompts are sent in a short period of time.
- Disable Okta's "send push notification" feature and switch to more secure MFA approval techniques, such as number matching, to limit the possibility of a user accepting an authentication verification prompt blindly.
- Identify and replace compromised users' credentials. Make sure credentials are complex, unique, and not reused on another platform.
- Enforce periodic password changes and key rotation to limit the likelihood of credential stuffing attacks.
- Enforce strict non-compliance with the usage of hard-coded credentials in any scripts or code.
- Identify critical resources in your environment and review their access on a regular basis.
- Apply the principle of least privilege and provide the bare minimum of access or permissions required to complete a task.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Lessons to learn from the Uber security breach

Tracker ID: TN0924 **Date:** 27/Sept/2022 **Category:** Incident **Industry:** All **Region**: All

References

- Uber Team, Security update, Uber Newsroom, 16th September 2022, External Link (www.uber.com).
- Tara Seals, Hacker Pwns Uber Via Compromised VPN Account, Dark Reading, 16th September 2022, External Link (www.darkreading.com).
- Sergiu Gatlan, Uber links breach to Lapsus$ group, blames contractor for hack, Bleeping Computer, 19th September 2022, External Link (www.bleepingcomputer.com).
- Ravie Lakshmanan, Uber Blames LAPSUS$ Hacking Group for Recent Security Breach, The Hacker News, 20th September 2022, External Link (thehackernews.com).
- Ravie Lakshmanan, London Police Arrested 17-Year-Old Hacker Suspected of Uber and GTA 6 Breaches, The Hacker News, 24th September 2022, External Link (thehackernews.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia