in focus:
UBER HACK

Uber Technologies, Inc. [Uber] is a US-based mobility-as-a-service provider

incident

On September 15, 2022, the ride-hailing company Uber was breached by a hacker thought to be linked to the Lapsus$ group, who gained initial access by socially engineering an Uber contractor. The attacker had apparently acquired the corporate password of this contractor on the dark web after it had been exposed through malware on the contractor's personal device. The attacker then repeatedly tried to login to the contractor's Uber account, which sent multiple two-factor login approval requests to the contractor's phone. Finally, the hacker posed as Uber IT and sent a message asking the contractor to approve the sign-in. After successfully exhausting the contractor, the approval was granted, and this provided the hacker with the valid credentials needed to gain access to Uber's VPN. Once inside, the hacker found a network share that had PowerShell scripts. One of these scripts contained admin credentials for Thycotic [a privileged access management solution]. Once the hacker had access to this, he was able to get access to all other internal systems by using their passwords.

key takeaways

OSINT information [contractor mobile number] was used to socially engineer an Uber contractor via a smishing attack

Using the contractor's credentials, the hacker gained access to Uber's VPN and compromised all of Uber's internal systems

Future compromises are probable as the hacker gained access to all Uber vulnerability disclosure reports

remediations

- Increase employee-based protections against social engineering by minimizing the relevant public data that hackers use to target employees, including job titles that attract hackers.
- Identify and neutralize any breached employee credentials, especially those associated with personal email accounts.
- Utilize physical [FIDO] MFA token.
- Harden internal environment through monitoring, securing PAM effectively, not hard coding credentials, and using the principle of least privilege for all employees.

actor & motivation

Claimed by the NY Times to be an 18-year-old unidentified hacker that attacked Uber because its security was weak [motivation: Script kiddie behavior]. Potentially British based on language used.

sources

- https://www.uber.com/newsroom/security-update/
- https://twitter.com/Uber_Comms/status/1570584747071639552?ref_src=twsrc%5Etfw
- https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html
- https://www.forbes.com/sites/daveywinder/2022/09/15/has-uber-been-hacked-company-investigates-cybersecurity-incident-as-law-enforcement-alerted/
- https://www.bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/
- https://twitter.com/BillDemirkapi/status/1570602097640607744?t=wUuqf6wA_gKjxFcY7ALM5Q&s=19

This is an ongoing story, and more information is likely to be shared in the coming days.
Similar stories involving social engineering include the 2022 Twilio and 2020 Twitter attacks.

PICNIC™