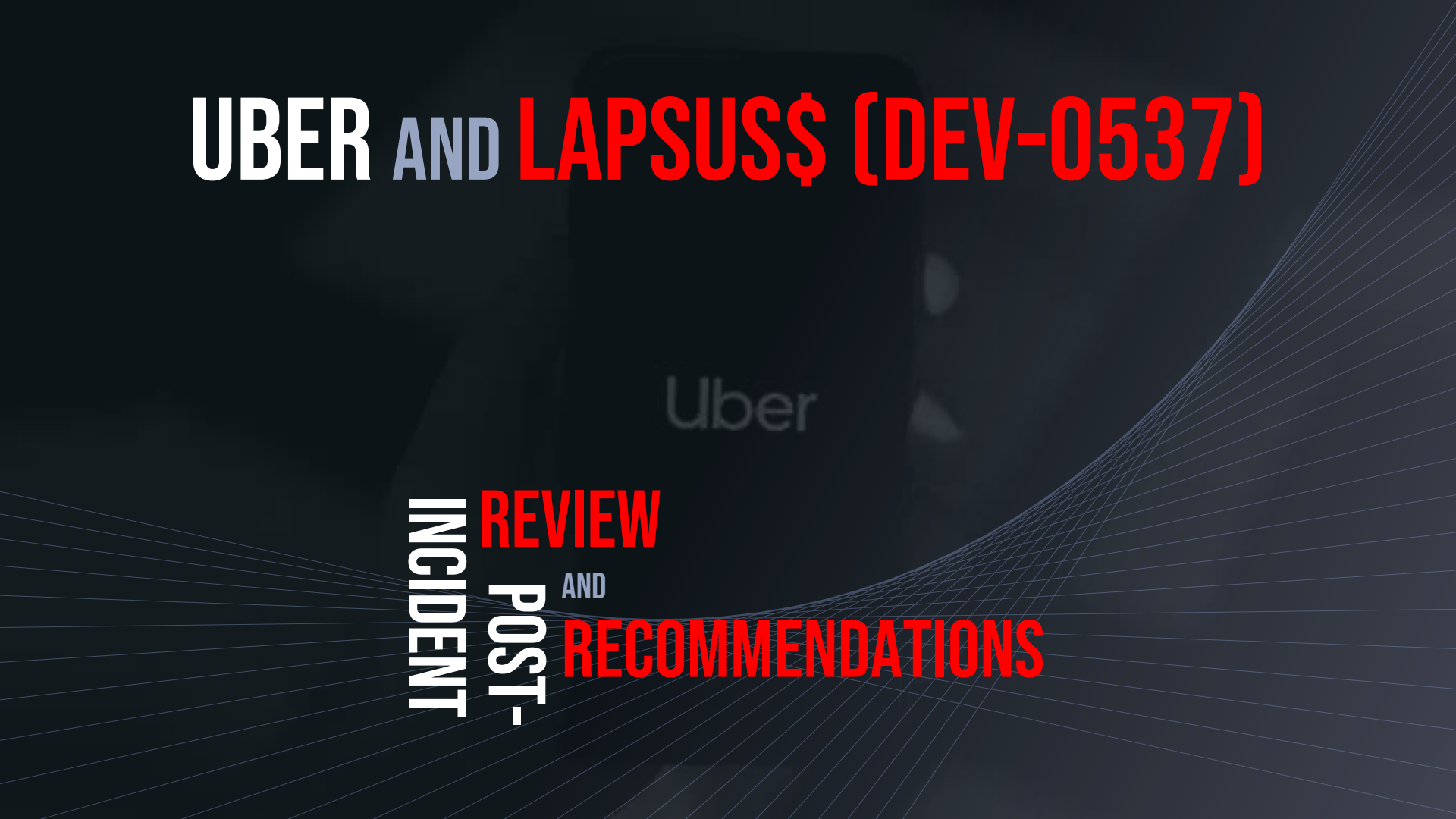
UBER AND LAPSUS$ (DEV-0537)



POST-INCIDENT REVIEW AND RECOMMENDATIONS

BIT 5134 ASSIGNMENT 2 GROUP 3

Equan Hotson
Cybersecurity Architecture Engineer

Simon Mere-Mere
Cybersecurity Analyst

Shae Smith
Quality Documentation and Training Specialist

SUMMARY

Uber was hacked by a teenager using an Uber employee work number (multi-factor authorization) MFA fatigue attack. The hacker pretended to be IT support and nudged the employee to respond to the spam (social engineering).

KEY FACTORS

- *No safeguards against 2FA spam on the authenticator's end.*
- *Hardcoding admin credentials in a PowerShell script.*
- *Failed network segmentation (highly privileged users can scan a network and find file shares).*

OUTCOMES

- *Significant share drop.*
- *Possible litigation by FTC or class-action lawsuits (shareholders / customers).*

SYSTEMS COMPROMISED

MFA Prompt Bomb	Thycotic (PAM)	AWS	VMWare vSphere	SentinelOne	HackerOne	GSuite Admin	Slack Workspaces
MFA prompt bombing and social engineering of an EXT employee granted Lapsus$ access to the Uber network via VPN	Lapsus$ then obtained hardcoded credentials in Powershell scripts for a domain admin account for Thycotic, Uber's Privileged Access Management solution	Gained admin access to shut down services, abuse computing resources, access, sensitive user data, delete or ransom data, change user access.	Gained admin access to cloud computing, on-premise servers, and admin functions granting deeper dive into systems	Gained admin access to XDR platform which allowed the attackers to conceal activity and prolong attacks	Gained admin access to detailed info on (likely unpatched) vulnerabilities in other areas of Uber's IT systems	Gained admin access to create and delete accounts, access to employee data and other sensitive Uber data	Potential to elevate privilege, access sensitive info, and send malicious links. A message from the attacker is what made Uber aware of the attack (Kedrosky)

ORGANIZATIONAL CHANGES

CREATE A CYBER CULTURE THAT PROMOTES PRACTICAL APPLICATION VS. ANNUAL TRAINING

- *Annual training should remain enforced to ensure employees are compliant with mandated requirements. Though, this should not be the only training received.*
- *This could be implementing blind and staged scenario-based events that allow employees to be tested in a controlled environment.*
- *Utilize Threat-Based planning to ensure the cybersecurity department is trained on specific possible incidents.*

BOOSTER AN ENVIRONMENT WHERE EMPLOYEES ARE NOT AFRAID TO CONTACT CYBERSECURITY FOR SUSPECTED INCIDENTS

- *If end users are afraid to reach out to cybersecurity, incidents can go unnoticed, and attackers can gain escalated privileges. Thus, bringing down the company.*

CONTINUE TO IMPLEMENT INFORMATION SECURITY ACROSS ALL BUSINESS PROCESSES

- *Business processes are where the wheels meet the road for Uber. Ensuring that information security best practices are implemented can ensure the business thrives.*
- *"In integrating information security practices, it is extremely important to understand information security issues in the context of business processes. From a process perspective, information flows between activities, people, functions, and organizations as a process component." (Andress et al.)*

PREVENTION

IDENTITY, AUTHENTICATION, AND ACCESS MANAGEMENT (IAAM)

- *Least privilege*
  - *If the organization were to implement least privilege, one employee's credentials would not be able to be utilized outside of their granted access.*
  - *Access should be limited to "need to know" privileges. This will assist in preventing an intruder using an employee's credentials from escalating their privileges and pivoting deeper into the network.*

DATA-AT-REST ENCRYPTION AND CRYPTOGRAPHY

- *The credentials that the intruder discovered in PowerShell should have been encrypted. By leaving these credentials in plaintext, Uber was left exposed and vulnerable.*
- *If these credentials were stored in ciphertext, the intruder would have at least been delayed in pivoting and escalating their access.*

APPLICATION SECURITY

- *Since the intruder utilized multi-factor authentication fatigue, the company could have utilized a timeout on request sent. If there was a limit on how many requests could be sent per a set time frame, the attacker could have been locked out for a long enough time that cybersecurity may have detected the intruder.*

DETECTION

IDENTITY, AUTHENTICATION, AND ACCESS MANAGEMENT

- *IAAM-03 & IAAM-04: Multi-Factor Authentication (MFA) & Privilege Management and Access Control*
  - *Uber was reportedly relying on Duo Security for Multi-Factor Authentication at the time of its breach. Implement monitoring and warning mechanisms to detect suspicious activity, such as MFA prompt bombing.*
  - *To counter future threats, include number matching with MFA to boost sign-in security or switch to Phishing-Resistant MFA, which relies on cryptographic techniques, biometrics, and the FIDO2 standard (Kapko).*

NETWORK SECURITY

- *NS-11: Network Access Control (NAC)*
  - *NAC works with the VPN to inventory users, devices, and level of access and can detect unusual network activity, such as an unauthorized computer trying to access the network. NACs can be configured to immediately respond to a threat detected, isolating the device from the network.*

ENDPOINT, SERVER, AND DEVICE SECURITY

- *ESDS-02: Computer Security and Logging Policies*
  - *Establish and monitor baseline activity of users and IP-connected devices to identify trends and detect suspicious activity, like having more than one active session or accessing systems they don't typically use. Set up real-time alerts for suspicious changes to system configurations, and limit the number of users that can modify logs so attackers can't cover their tracks.*

MONITORING, VULNERABILITY, AND PATCH MANAGEMENT

- *MVPM-03 & MVPM-07: System Configuration Change Detection & Security Information and Event Management (SIEM)*
  - *Lapsus$ reconfigured OpenDNS for the sole purpose of loading a graphic image on internal systems. Set up OpenDNS to notify of any configuration changes.*
  - *Utilize SIEM advanced analytics and event correlation to gain full observability of Uber infrastructure and to flag unauthorized access events for early detection of system hijacking.*

RECOMMENDATIONS

INCIDENT RESPONSE

- *IR-03 / IR-04: Forensic Tools / Computer Imaging*
  - *Necessary to collect and analyze the evidence, see the logs, and analyze IP addresses (location, provider, OS type, and type of attack). Making an image of a compromised computer and the phone might be advisable. Additionally, implement IR-05: Indicators of Compromise (IOCs) to see how many compromised computers were on the network and which one provided admin credentials that were in Powershell script.*

SYSTEM ADMINISTRATION

- *SA-08: Administrator Audit Trail(s)*
  - *Check admin logs and document all the activities the system and administrators performed to see what exactly allowed the unauthorized access. Analyze the audit trail to determine what machine was responsible for allowing the access and suggest necessary changes. Use data collected for e-discovery preparation as well so law enforcement can hold the attacker responsible.*

POLICY, AUDIT, E-DISCOVERY, AND TRAINING

- *PAET-03: Audit Frameworks*
  - *At the end of the forensic investigation, suggest necessary changes: reevaluate MFA effectiveness and maybe provide agency training to show the employees how to avoid MFA fatigue in the future. Decide on what other deficiencies could be critical in the future and buy necessary preventive, detective, and forensic software to ensure timely response to hacker attacks.*

IMPLEMENTATION CHALLENGES

INCIDENT RESPONSE

- *IR-03 / IR-04: Forensic Tools / Computer Imaging*
  - *Technical challenges of using Forensic Tools include the time required to find and sort the data, as some files might be encrypted or "hidden" by the attacker. Other differences in data types, such as real-time data versus multi-layered data, cause different levels of complexity which could result in significant delays in analysis. It may also be required to duplicate the data so that multiple people can inspect it, which increases the risk of the data being altered or deleted.*

SYSTEM ADMINISTRATION

- *SA-08: Administrator Audit Trail(s)*
  - *Issues with audit trails begin with the cost and expertise required in the analysis. Other problems lie in the number of audit logs that need to be sorted through and troubleshooting problems with log maintenance and storage.*

POLICY, AUDIT, E-DISCOVERY, AND TRAINING

- *PAET-03: Audit Frameworks*
  - *It could be challenging to implement and guarantee compliance training with Uber since so many of their employees, specifically "driver-partners," use BYOD devices linked to their network. Issues can also arise due to budget or staffing constraints. For instance, Uber may hesitate to implement changes to its current SOC due to the financial cost involved.*

REFERENCES

Andress, Jason, et al. Building a Practical Information Security Program. 1st Edition, Syngress, 2016.

Comeau, Zachary. “What IT and Security Teams Should Take Away From the Uber Hack.” *My TechDecisions*, 21 Sept. 2022, https://mytechdecisions.com/network-security/what-it-and-security-teams-should-take-away-from-the-uber-hack/.

De Simone, Sergio. “Multi-Factor Authentication Fatigue Key Factor in Uber Breach.” *InfoQ*, 24 Sept. 2022, https://www.infoq.com/news/2022/09/Uber-breach-mfa-fatigue/.

Donaldson, Scott, et al. Enterprise Cybersecurity. Apress, 2015.

Geronimo, Adelle. “Uber Data Breach Spotlights Need for Enterprises to ‘Get the Basics Right’, Say Experts.” *ITP.Net*, 19 Sept. 2022, https://www.itp.net/security/uber-data-breach-prompts-cybersecurity-experts-to-urge-enterprises-to-get-the-basics-right.

Hutchins, Marcus. “Tea Pot.” *Twitter*, @MalwareTechBlog, 15 Sept. 2022, https://twitter.com/MalwareTechBlog/status/1570600059909345280.

Jackson, Mackenzie. “Uber Breach 2022 – Everything You Need to Know.” GitGuardian Blog - Automated Secrets Detection, 16 Sept. 2022, https://blog.gitguardian.com/uber-breach-2022/.

Kapko, Matt. “What Is Phishing-Resistant Multifactor Authentication? It’s Complicated.” Cybersecurity Dive, 10 Oct. 2022, https://www.cybersecuritydive.com/news/phishing-resistant-mfa/633703/#:~:text=In%20practice%2C%20phishing%2Dresistant%20MFA,better%20than%20single%2Dfactor%20authentication.

Kedrosky, Eric. “Uber Data Breach Is Worst Case Scenario .” Security Boulevard, 17 Sept. 2022, https://securityboulevard.com/2022/09/uber-data-breach-is-worst-case-scenario/.

REFERENCES

Security, Microsoft. “6 Ways to Protect Your Organization Against the Threat Group DEV-0537.” *CSO Online*, 16 June 2022, https://www.csoonline.com/article/3664050/6-ways-to-protect-your-organization-against-the-threat-group-dev-0537.html.

“Security Update.” *Uber Newsroom*, 16 Sept. 2022, https://www.uber.com/newsroom/security-update/.

Seytonic. “Uber Completely Pwned By Teenager.” *YouTube*, 17 Sept. 2022, https://www.youtube.com/watch?v=d1XpwSR2BLo.

Strom, David. “How Uber Was Hacked — Again.” *Avast Blog*, 20 Sept. 2022, https://blog.avast.com/uber-hack.

The CyberWire Staff. “Preliminary Lessons from the Uber Breach.” The CyberWire, 19 Sept. 2022, https://thecyberwire.com/stories/ff7ea32e10874b3dafd49209d1af26a8/preliminary-lessons-from-the-uber-breach.

“Thread by @GroupIB_GIB.” *Thread Reader App*, https://threadreaderapp.com/thread/1570821174736850945.html.

Turner, Rich. “Meaningful Learnings from the Uber Breach.” *Infosecurity Magazine*, 27 Sept. 2022, https://www.infosecurity-magazine.com/opinions/learnings-uber-breach/.

“Uber Shares.” *Google*, https://www.google.com/search?q=uber+shares&oq=uber+shares+&aqs=chrome..69i57j0i512l2j0i457i512j0i512l6.3561j0j4&sourceid=chrome&ie=UTF-8.

Whittaker, Zack. “How Do You Stop Another Uber Hack? .” TechCrunch, 19 Sept. 2022, https://techcrunch.com/2022/09/19/how-to-fix-another-uber-breach/.