Blog Post: Uber 2022 Breach

Investigating the Cyber Attack Against Uber in 2022

Kendal E. Taylor

Cybersecurity Fundamentals, Old Dominion University

CS 462: Cybersecurity Fundamentals

Susan Zehra

April 14th, 2024

Blog Post: Uber 2022 Breach

Investigating the Cyber Attack Against Uber in 2022

On September 15th, 2022, Uber confirmed reports of their organization-wide cybersecurity breach. The attacker, going by the alias of "Tea Pot," was affiliated with a hacking group named Lapsus$. This same group has breached Samsung, Microsoft, and NVIDIA early in 2022. It is speculated that the attacker targeted an external contractor whose credentials were purchased on the dark web. This was done via a social engineering campaign on Uber employees, in which the embedded file yielded access to a VPN, granting access to Uber's internal network. The attacker then retrieved hardcoded administrative credentials via some PowerShell scripts. This gave the attack total access to the Access Management software. The attacker was then able to login and take over several services that Uber utilized, including AWS, Sentinel One, Cloud Solutions, and even internal employee dashboard. In this blog post, we will look at how the breach worked, including the protocols, applications and devices that can be attacked. We will also observe how this breach affects today's society as well.

Technologies Used to Perpetuate the Attack

One of the first steps in this hacker's operations was establishing an initial access to Uber's systems. This was done via a social engineering campaign on Uber employees, which was a text message posing as corporate IT personnel. The message persuaded the victim to hand over a password, which allowed access to the company. Upon logging in, the attacker also yielded access to a VPN, granting access to all of Uber's internal network. The attacker then retrieved hardcoded administrative credentials via some PowerShell scripts. This gave the attack total access to the Access Management software. The attacker was then able to login and take

over several services that Uber utilized, including AWS, Sentinel One, Cloud Solutions, and even internal employee dashboards (2022, CyberArk).

To fully understand how this attack works, we must deconstruct it into a series of phases. During phase 1, initial access, the attacker gained initial access to Uber's infrastructure by gaining access to credentials through social engineering. During phase 2, the discovery phase, the intranet was scanned, likely to find administrative accounts to utilize. During this discovery phase, the attacker was able to find a PowerShell script that contained hard-coded privileged credentials to Uber's PAM (privileged access management) solution. This PowerShell script was used to automate authentication for daily tasks. These hard-coded credentials granted admin access to the management solution. Following that was phase 3, privilege escalation. From the hard-coded credentials obtained in the last phase, the attacker was able to move laterally and further escalate privileges. One of the ways that this lateral movement occurred was the hacker's use of tools called Raccoon and Vidar, which are info stealers that were used to acquire data from Uber employees. The information compromised by these tools helped the attack move laterally.

During phase 4, accessing secrets, the attacker was able to access several tools. This included the SSO service and several cloud management consoles as well, where sensitive customer and financial data were stored. This was also the phase where the attacker had complete access to internal systems such as Amazon Web Service (AWS), Google Cloud Platform (GCP), Google Drive, Sentinel One, Slack workspace and much more. Finally, there is phase 5, the data exfiltration phase. The attacker downloaded several pieces of customer information from an internal tool used by the finance department to manage invoices. These pieces. information included internal Slack messages containing sensitive Uber employee

information, along with several critical financial operations details from the invoice management tool.

How the Attack Works

After examining the various phases of the Uber cybersecurity breach, we can comprehensively understand how the breach worked. The hacking group Lapsus$ targeted an external contractor, where they then obtained credentials from the dark web. After that, the initial breach occurred. This is where the attacker found the critical vulnerability of hardcoded credentials in an automation PowerShell script, granting admin access to the Uber's Privilege Access Management system.

After delivering the exploit, the attackers then gained full access to Thycotic. According to Mitnick Security, Thycotic is a privileged access management provider that employs services such as secret servers, account risk mitigation, connection management, DevOps secrets vaults, and much more (2023, Mitnick). This is how the attackers were able to access absolutely everything, including cloud infrastructure, Slack, Sentinel One and VM platforms.

Devices, Protocols, or Applications That Can Be Attacked.

Based on the details of this attack, there were several devices, protocol and applications that were attacked. One of these was PowerShell. The hard coded credentials were found here, as a user had automated hard-coded admin credentials to automatically complete a task that required admin access. Though the specific details of this script were not in the breach details, it is likely that the hardcoded credentials were related to the third-party Privileged Access Management needing administrative credentials to access Thycotic (2022, Jackson M.).

In addition to these, another application that can be exploited is the Extended Detection and Response (XDR) platforms. These are designed to alert analysts of security issues or

intrusions, which is a significant reason that they are often attacked. They provide security services to emails, software, cloud services, access management and identities, endpoints, and much more. Attackers work to compromise these systems to cover their tracks so their infiltration cannot be monitored. Slack is also an example of something that can easily be compromised during a breach. Slack is a platform that can accomplish several tasks including automation, several tools, and services, and enables several communication channels. With the amount of information automation needs and the data that is communicated between channels, this can serve as a valuable piece of information for attackers. They can learn the structure of a system this way, which can also be used to construct phishing and social engineering attacks. Cloud infrastructure is another potentially valuable target to attackers. Infiltrating the cloud can allow access to virtual machines, servers, database, storage, and access control policies.

How This Affects Today's Society

This attack affects today's society by reinstating the importance of avoiding hard-coded credentials. Thanks to this one fatal security vulnerability, the attackers were able to compromise millions of customer's data, several critical pieces of Uber information, cloud infrastructure, access control mechanisms, and much more given they had total access to everything. Uber suffered several consequences for this breach, including the loss of consumer trust, remediation and investigation costs, legal fees, reputation damage, data leaks and more. It is also speculated that thanks to the slew of information harvested during the attack, Uber still suffers social engineering threats and attempted attacks.

In response to this successful attack, society today can learn and understand the importance of proper authentication methods, instead of hardcoded credentials. Some alternatives include secret management tools like a secret server. Utilizing Kerberos tokens,

configuration files, cloud configurations, and hashing values are all more secure options. With the compromise of several third-party security systems, this aspect of the breach can also affect society's stance on vendor security, third-party contract security, and evaluating service-level agreements between third parties. This breach impacted society by learning from Uber's mistakes. It is a common practice now to avoid hardcoding credentials, and the several details of this attack has helped develop threat intelligence to avoid a situation like this from ever occurring again.

Conclusion

In conclusion, the Uber breach of 2022 serves as an additional demonstration of the importance of effective cybersecurity measures within organizations. The hacking group Lapsus$ made the breach possible through a social engineering campaign that targeted Uber employees, resulting in the compromise of the company's internal network. Once infiltrated, the attacker then exploited hardcoded administrative credentials, gaining total access to Uber's Access Management software. The group was able to find these vulnerabilities through an external contractor on the dark web; they were then exploited after the social engineering campaign. In a worst-case scenario situation, this allowed the hacker to gain full access to Uber's Privilege Access Management system Thycotic. Some of the devices, protocols and applications exploited include PowerShell, XDR platforms, Slack, and cloud infrastructure. Society can learn about the dangers of hardcoded credentials thanks to this attack, as well as the importance of user training regarding social engineering. Though Uber was able to successfully recover from this attack, the costs of their reputation, legal fees, investigation fees, and the loss of consumer trust were still some of the consequences of this breach.

References

CyberArk Blog Team. (2022, September 20). Unpacking the Uber Breach. https://www.cyberark.com/resources/blog/unpacking-the-uber-breach

Jackson, M. (2022, September 16). Uber Breach 2022 – Everything You Need to Know. https://blog.gitguardian.com/uber-breach-2022/

Mitnick Security. (2022, October 3). Uber Data Breach: What To Know About the 2022 Cybersecurity Attack. https://www.mitnicksecurity.com/blog/uber-data-breach