

 FLASH**UBER BREACH****ZEROFOX INTELLIGENCE**

F-2022-09-16a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: PII & Fraud

September 16, 2022



Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 11:00 AM (EDT) on September 16, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Uber Breach

Key Findings

- Initial access to a breach disclosed by Uber on September 15, 2022, was gained through social engineering.
- Administrative credentials stored in a network-accessible script allowed the additional discovery of even more sensitive credentials.
- While the depth and breadth of the breach is yet to be determined, screenshots posted on social media indicate that the attacker may have had access to over 1 Petabyte of data.

Analyst Commentary

Uber notified the public of an ongoing cybersecurity incident late on September 15, 2022, via Twitter.¹ While Uber itself has not provided much detail, the alleged attacker appeared to share details and screenshots with those who reached out through Telegram.

According to the attacker, they began the attack by repeatedly sending multi-factor authentication (MFA) push requests to an employee's phone. The attacker then pretended to be someone from Uber's IT department and told the employee that, in order for the requests to stop, the employee needed to accept the request.

(I was spamming employee with push auth for over a hour) i then contacted him on WhatsApp and claimed to be from Uber IT, told him if he wants it to stop he must accept it

6:47 PM

And well, he accepted and I added my device

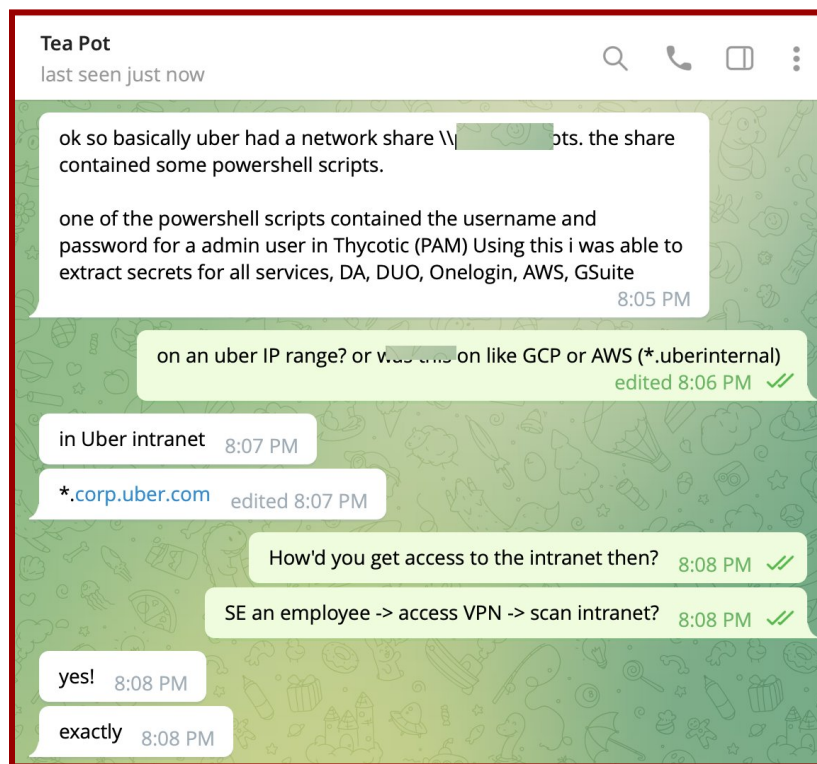
6:47 PM

Source: [hXXps://twitter\[.\]com/GossiTheDog/status/1570717994397073410](https://twitter.com/GossiTheDog/status/1570717994397073410)

¹ [hXXps://twitter\[.\]com/Uber_Comms/status/1570584747071639552](https://twitter.com/Uber_Comms/status/1570584747071639552)

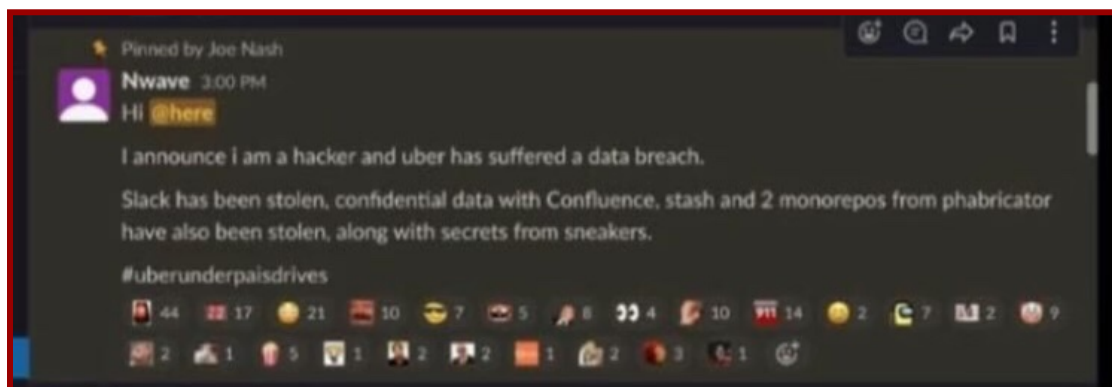


Once the attacker had access to MFA, they were able to log into Uber's corporate VPN and begin scanning the internal network. This led to the discovery of a network share with PowerShell scripts that contained admin-level credentials. These credentials were then used to access Thycotic, a Privileged Account Management (PAM) solution, to extract credentials for Uber domain administrator accounts and several services such as AWS, Duo, Google Workspace, Onelogin, and VMware vSphere.



Source: [hXXps://twitter\[.\]com/hacker_/status/1570582547415068672](https://twitter.com/hacker_/status/1570582547415068672)

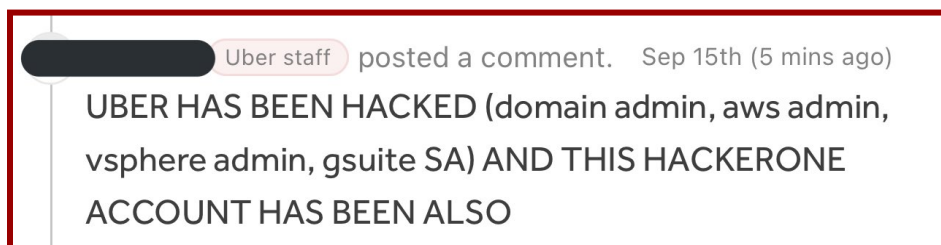
After gaining access to company services, the attacker posted a message to Uber employees via Slack.



Source: [hXXps://twitter\[.\]com/ColtonSeal/status/1570596125924794368](https://twitter.com/ColtonSeal/status/1570596125924794368)

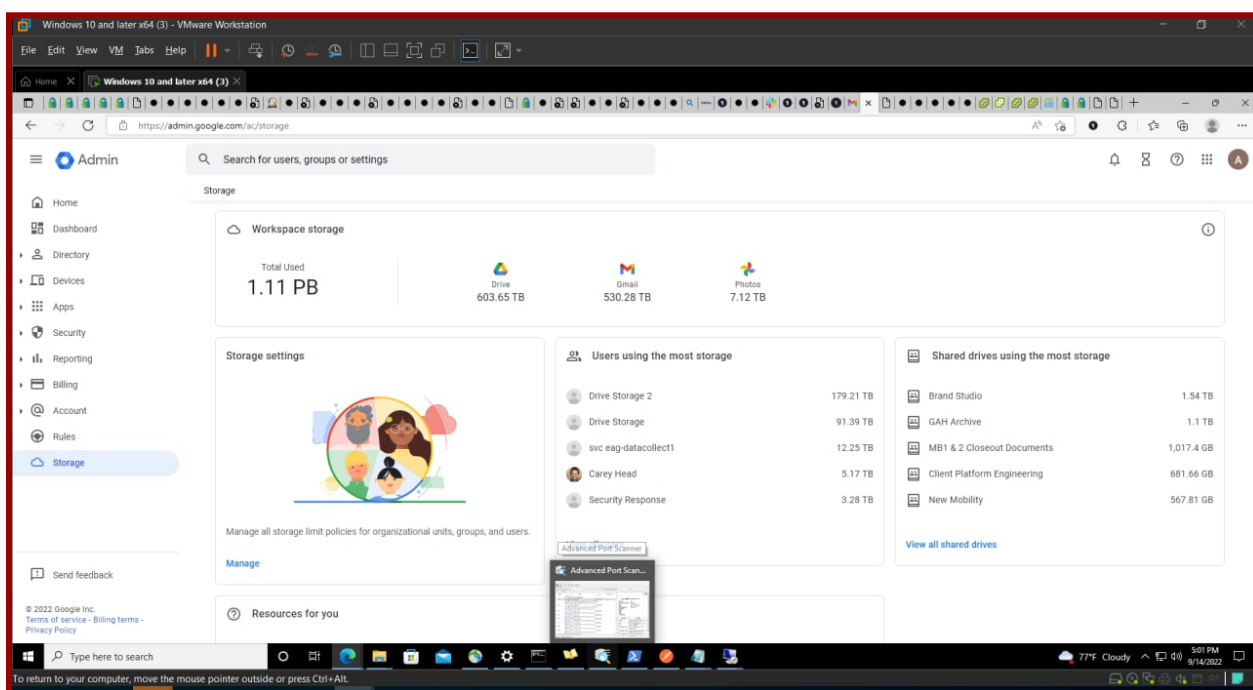


Comments announcing the compromise were also posted using Uber's official HackerOne account. Although a message on Uber's HackerOne profile says that the account is currently disabled, there is still a chance that vulnerability reports have already been accessed.



Source: [hXXps://twitter\[.\]com/samwcyo/status/1570577801790783493](https://twitter.com/samwcyo/status/1570577801790783493)

Several screenshots of the alleged access have begun circulating online showing administration panels for services like AWS, Google Workspace, SentinelOne, VMware vSphere, and even internal sites displaying financial data. If the screenshots are legitimate, the attacker may have had access to over 1 Petabyte of data.



Source: [hXXps://twitter\[.\]com/vxunderground/status/1570611979169202179](https://twitter.com/vxunderground/status/1570611979169202179)



Recommendations

Although the alleged attacker states that they repeatedly sent MFA requests to the Uber employee for over an hour, it was not until they reached out to the employee directly via WhatsApp posing as someone from IT that the request was finally accepted. ZeroFox recommends staying vigilant and denying MFA requests you did not specifically trigger through logging in or requesting device enrollment. These requests are typically immediate and should not randomly appear throughout the day.

In addition, ZeroFox recommends taking similar precautions to mitigate the risk of phishing attacks when contacted outside official channels. Ask yourself:

- Would IT usually reach out in this manner?
- Is this request outside of typical working hours?
- Is the request asking me to give my credentials or perform some sensitive action?
- If anything seems suspicious, contact your IT department directly instead of responding to the message received.



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.