Uber hacked, internal systems breached and vulnerability reports stolen

bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/

Lawrence Abrams

By
Lawrence Abrams

- September 16, 2022
- 12:30 AM
- 0

Uber suffered a cyberattack Thursday afternoon with an allegedly 18-year-old hacker downloading HackerOne vulnerability reports and sharing screenshots of the company's internal systems, email dashboard, and Slack server.

The screenshots shared by the hacker and seen by BleepingComputer show what appears to be full access to many critical Uber IT systems, including the company's security software and Windows domain.

Other systems accessed by the hacker include the company's Amazon Web Services console, VMware vSphere/ESXi virtual machines, and the Google Workspace admin dashboard for managing the Uber email accounts.

The threat actor also breached the Uber Slack server, which he used to post messages to employees stating that the company was hacked. However, screenshots from Uber's slack indicate that these announcements were first met with memes and jokes as employees had not realized an actual cyberattack was taking place.

Uber has since confirmed the attack, tweeting that they are in touch with law enforcement and will post additional information as it becomes available.

"We are currently responding to a cybersecurity incident. We are in touch with law enforcement and will post additional updates here as they become available," tweeted the Uber Communications account.

The New York Times, which first reported on the breach, said they spoke to the threat actor, who said they breached Uber after performing a social engineering attack on an employee and stealing their password.

The threat actor then gained access to the company's internal systems using the stolen credentials.

On Friday afternoon, Uber posted an additional update stating that the investigation is still ongoing but could sharing these additional details:

> - We have no evidence that the incident involved access to sensitive user data (like trip history).
> - All of our services including Uber, Uber Eats, Uber Freight, and the Uber Driver app are operational.
> - As we shared yesterday, we have notified law enforcement.
> - Internal software tools that we took down as a precaution yesterday are coming back online this morning.

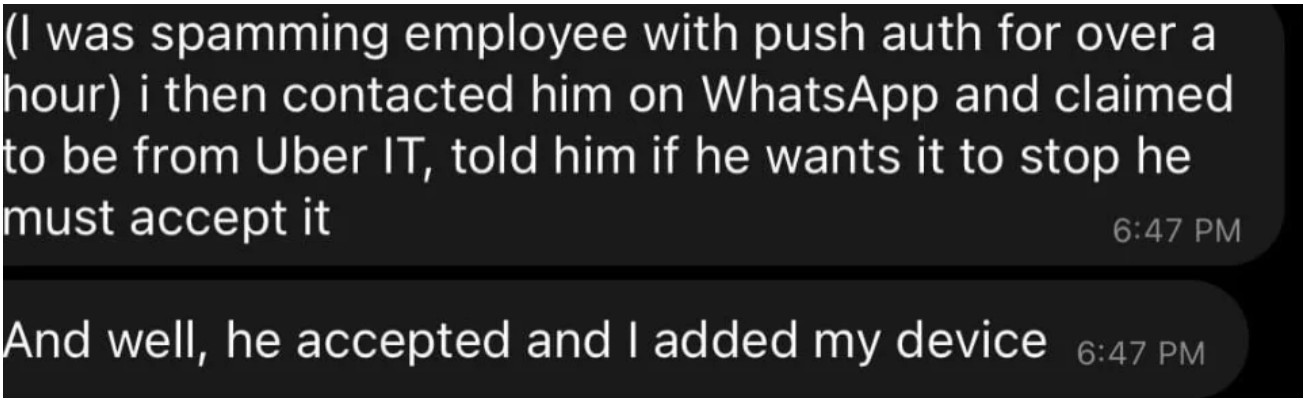
More details emerge

After the attacker loudly announced that they breached Uber's systems on the company's Slack server and in comments to submission on the HackerOne bug bounty program, security researchers reached out to the threat actor to learn more about the attack.

In a conversation between the threat actor and security researcher Corben Leo, the hacker said they were able to gain access to Uber's Intranet after conducting a social engineering attack on an employee.

According to the threat actor, they attempted to log in as an Uber employee but did not provide details on how they gained access to the credentials.

As the Uber account was protected with multi-factor authentication, the attacker allegedly used an MFA Fatigue attack and pretended to be Uber IT support to convince the employee to accept the MFA request.



Hackers claim to have used an MFA Fatigue attack

Source: Kevin Beaumont

MFA Fatigue attacks are when a threat actor has access to corporate login credentials but is blocked from access to the account by multi-factor authentication. They then issue repeated MFA requests to the target until the victims become tired of seeing them and finally accept the notification.

This social engineering tactic has become very popular in recent attacks against well-known companies, including Twitter, MailChimp, Robinhood, and Okta.

After gaining access to the credentials, the threat actor told Leo that they logged into the Internal network through the corporate VPN and began scanning the company's Intranet for sensitive information.

As part of these scans, the hacker says they found a PowerShell script containing admin credentials for the company's Thycotic privileged access management (PAM) platform, which was used to access the login secrets for the company's other internal services.

> "ok so basically uber had a network share \\[redacted]pts. the share contained some powershell scripts.
>
> one of the powershell scripts contained the username and password for a admin user in Thycotic (PAM) Using this i was able to extract secrets for all services, DA, DUO, Onelogin, AWS, Gsuite"

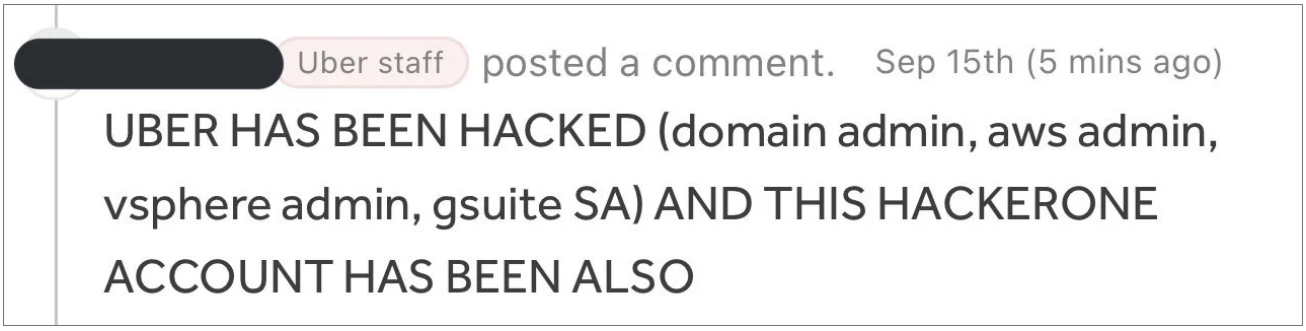
The New York Times reports that the attacker claimed to have accessed Uber databases and source code as part of the attack.

To be clear, this information is from the threat actors and has not been verified by Uber, which has not responded to our requests for more information.

HackerOne vulnerability reports exposed

While it's possible that the threat actor stole data and source code from Uber during this attack, they also had access to what could be an even more valuable asset.

According to Yuga Labs security engineer Sam Curry, the hacker also had access to the company's HackerOne bug bounty program, where they commented on all of the company's bug bounty tickets.



Comment left by the hacker on HackerOne submissions
Source: Curry

Curry told BleepingComputer that he first learned of the breach after the attacker left the above comment on a vulnerability report he submitted to Uber two years ago.

Uber runs a HackerOne bug bounty program that allows security researchers to privately disclose vulnerabilities in their systems and apps in exchange for a monetary bug bounty reward. These vulnerability reports are meant to be kept confidential until a fix can be released to prevent attackers from exploiting them in attacks.

Curry further shared that an Uber employee said the threat actor had access to all of the company's private vulnerability submissions on HackerOne.

BleepingComputer was also told by a source that the attacker downloaded all vulnerability reports before they lost access to Uber's bug bounty program. This likely includes vulnerability reports that have not been fixed, presenting a severe security risk to Uber.

HackerOne has since disabled the Uber bug bounty program, cutting off access to the disclosed vulnerabilities.

However, it would not be surprising if the threat actor had already downloaded the vulnerability reports and would likely sell them to other threat actors to cash out on the attack quickly.

Update 9/16/22:

Added more details provided by the hacker about how the attack took place.
Added statement from Uber.

Related Articles:

MFA Fatigue: Hackers' new favorite tactic in high-profile breaches

Hackers steal crypto from Bitcoin ATMs by exploiting zero-day bug

CISA adds 7 vulnerabilities to list of bugs exploited by hackers

Hackers are actively exploiting password-stealing flaw in Zimbra

CISA: Hackers exploit critical Bitbucket Server flaw in attacks

- Credentials
- Cyberattack
- HackerOne
- Social Engineering
- Uber
- Vulnerability

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: