September 19, 10:45am PT

While our investigation is still ongoing, we are providing an update on our response to last week’s security incident.

What happened?

An Uber EXT contractor had their account compromised by an attacker. It is likely that the attacker purchased the contractor’s Uber corporate password on the dark web, after the contractor’s personal device had been infected with malware, exposing those credentials. The attacker then repeatedly tried to log in to the contractor’s Uber account. Each time, the contractor received a two-factor login approval request, which initially blocked access. Eventually, however, the contractor accepted one, and the attacker successfully logged in.

From there, the attacker accessed several other employee accounts which ultimately gave the attacker elevated permissions to a number of tools, including G-Suite and Slack. The attacker then posted a message to a company-wide Slack channel, which many of you saw, and reconfigured Uber’s OpenDNS to display a graphic image to employees on some internal sites.

How did we respond?

Our existing security monitoring processes allowed our teams to quickly identify the issue and move to respond. Our top priorities were to make sure the attacker no longer had access to our systems; to ensure user data was secure and that Uber services were not affected; and then to investigate the scope and impact of the incident.

Here are some of the key actions we took, and continue to take:

* We identified any employee accounts that were compromised or potentially compromised and either blocked their access to Uber systems or required a password reset.
* We disabled many affected or potentially affected internal tools.
* We rotated keys (effectively resetting access) to many of our internal services.
* We locked down our codebase, preventing any new code changes.
* When restoring access to internal tools, we required employees to re-authenticate. We are also further strengthening our multi-factor authentication (MFA) policies.
* We added additional monitoring of our internal environment to keep an even closer eye on any further suspicious activity.

What was the impact?

The attacker accessed several internal systems, and our investigation has focused on determining whether there was any material impact. While the investigation is still ongoing, we do have some details of our current findings that we can share.

First and foremost, we’ve not seen that the attacker accessed the production (i.e. public-facing) systems that power our apps; any user accounts; or the databases we use to store sensitive user information, like credit card numbers, user bank account info, or trip history. We also encrypt credit card information and personal health data, offering a further layer of protection.

We reviewed our codebase and have not found that the attacker made any changes. We also have not found that the attacker accessed any customer or user data stored by our cloud providers (e.g. AWS S3). It does appear that the attacker downloaded some internal Slack messages, as well as accessed or downloaded information from an internal tool our finance team uses to manage some invoices. We are currently analyzing those downloads.

The attacker was able to access our dashboard at HackerOne, where security researchers report bugs and vulnerabilities. However, any bug reports the attacker was able to access have been remediated.

Throughout, we were able to keep all of our public-facing Uber, Uber Eats, and Uber Freight services operational and running smoothly. Because we took down some internal tools, customer support operations were minimally impacted and are now back to normal.