Uber attributes hack to Lapsus$, working with FBI and DOJ on investigation

By Jonathan Greig

Published: 2023-01-10 · Archived: 2026-04-05 21:21:37 UTC

Ride-share giant Uber said on Monday that the headline-grabbing cyberattack on their systems was traced back to the compromised account credentials of a contractor exploited by hackers connected to the notorious extortion group Lapsus$.

The company said in a statement that it is working with the FBI, Department of Justice and several leading digital forensics firms on the investigation but noted that the hacker has been involved in several other breaches of large companies.

“We believe that this attacker (or attackers) are affiliated with a hacking group called Lapsus$, which has been increasingly active over the last year or so,” the company said. “This group typically uses similar techniques to target technology companies, and in 2022 alone has breached Microsoft, Cisco, Samsung, Nvidia and Okta, among others. There are also reports over the weekend that this same actor breached video game maker Rockstar Games.”

The hacker downloaded internal messages from the company’s Slack and accessed information from an internal tool the company’s finance team uses to manage invoices. Uber said the attacker was also able to access the company’s dashboard for vulnerability reporting platform HackerOne.

Uber said that the hacker was not able to access public-facing systems that power their apps, user accounts, or the databases used to store credit card numbers and bank account information. Their investigation found that the attacker did not change their codebase and did not access any customer or user data stored by their cloud providers.

Uber said it is still investigating the incident but believes that an “Uber EXT contractor” had their account compromised by someone who likely 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 ride-share company confirmed earlier reports that the attacker repeatedly tried to log in to the contractor’s Uber account.

The contractor blocked access each time they received a two-factor login approval request but eventually accepted it, giving the attacker access.

“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,” Uber said. “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.”

Uber said that once its security team discovered the issue, they first wanted to get the hacker out of their system, ensure user data was safe and limit any potential damage done to Uber services.

They did this by blocking the compromised employee accounts or forcing through password resets.

The company went so far as to disable some of the affected internal tools that had been accessed during the incident and subsequently reset access to the internal services.

“Because we took down some internal tools, customer support operations were minimally impacted and are now back to normal,” Uber explained.

Uber’s security team also said it prevented changes to its code by “locking it down.” The company did not respond to requests for clarification about these steps.

Employees were forced to re-authenticate after the company restored access to the internal tools that had been hacked.

According to the statement, Uber instituted more stringent multi-factor authentication policies and added additional tools allowing security officials to monitor internal environments more closely.

A person claiming to have broken into the ride-hailing company’s network contacted The New York Times last week with evidence of the breach, including “images of email, cloud storage and code repositories.”

They also contacted several security researchers claiming to have obtained log-in credentials for some of the company’s most sensitive business accounts.

> Uber was hacked.
>
> The hacker social engineered an employee -> logged into the VPN and scanned their intranet.
>
> — Corben Leo (@hacker_) September 16, 2022

The hacker claimed he was male, 18 years old, and “had broken into Uber’s systems because the company had weak security.” Over the weekend, the same alleged hacker claimed to have broken into Rockstar Games and stolen information related to the next installment of the Grand Theft Auto series.

If accurate, the attack would be yet another feather in the cap of Lapsus$, a group that made waves earlier this year with several brazen attacks on the world's biggest tech companies.

Last month, Brazil’s Federal Police carried out eight search and seizure warrants as part of an investigation into attacks claimed by the Lapsus$ Group that disrupted the country’s Ministry of Health last December.

Some alleged members of the group were reported to be teenagers — including one in Oxford who was doxxed in an episode of hacker drama, according to Bloomberg. U.K. law enforcement arrested seven people, ages ranging from 16 to 21, in March for alleged involvement in Lapsus$.

The group continued to post for several days after the arrests, including about a data breach at the software company Globant, but its public Telegram channel has been silent since late March.

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
