FORK ME! Uber hauls GitHub into court to find who hacked database of 50,000 drivers

By Kieren McCarthy

Published: 2015-02-28 · Archived: 2026-04-05 18:04:51 UTC

Uber has subpoenaed GitHub to unmask netizens suspected of hacking its database of thousands of taxi drivers.

The ride-booking app vendor is trying to force GitHub [PDF] to hand over the IP addresses of anyone who visited a particular gist post between March and September 2014.

That gist is believed to have contained a login key used by a hacker to access an internal Uber database of 50,000 drivers. Github declined to voluntarily hand over its gist access logs, leading to Friday's subpoena filing.

Uber has also launched a John Doe lawsuit [PDF] in the district court of northern California against the mystery hacker. Uber and GitHub are both headquartered in San Francisco, California.

"On or around May 12, 2014, from an IP address not associated with an Uber employee and otherwise unknown to Uber, John Doe used the unique security key to download Uber database files containing confidential and proprietary information from Uber’s protected computers," the lawsuit's paperwork reads.

In a blog post on Friday, Uber admitted the database of driver names and license plates was accessed by the hacker way back in May, but the startup only spotted it in September.

Uber's security team knows the public IP address used by the database invader, and wants to link that number against the IP addresses and usernames of anyone who looked at the GitHub-hosted gist in question – ID 9556255 – which we note today no longer exists.

It's possible the gist contained a leaked login key, or internal source code that contained a key that should not have been made public. We won't speculate further. Uber's also on a hiding to nothing if the IP address it's tracking down is a proxy, Tor exit relay, or similar – but again, we'd hate to speculate.

Uber wants GitHub to provide ...

> all records, including but not limited to transactional or other logs, from March 14, 2014 to September 17, 2014, identifying the IP addresses or subscribers that viewed, accessed, or modified these posts and the date/time of access, viewing, or modification, as well as any records or metadata relating to the browser (i.e., logged HTTP headers, including cookies) or device that viewed, accessed, or modified the posts.

In other words, Uber hopes it will find an online breadcrumb trail from the gist to whoever hacked its systems. Quite why Uber has waited more than five months to subpoena GitHub is unclear, and the taxi-booking biz has refused to explain the delay.

In its statement, Uber's Managing Counsel of Data Privacy Katherine Tassi said the breach covered "current and former Uber driver partner names and driver’s license numbers," and is offering a year of credit monitoring for free to those whose details were leaked.

In keeping with its image as a gas tank of ethics running on empty, Uber does not provide an explanation for why it did not inform its drivers their details had been swiped until it decided to file a lawsuit five months later.

The post noted that the company had "not received any reports of actual misuse of information as a result of this incident." ®
