Lapsus$ gang claims new hack with data from Apple Health partner

After a short “vacation,” the Lapsus$ hacking gang is back. In a post shared through the group’s Telegram channel on Wednesday, Lapsus$ claimed to have stolen 70GB of data from Globant — an international software development firm headquartered in Luxembourg, which boasts some of the world’s largest companies as clients.

Screenshots of the hacked data, originally posted by Lapsus$ and shared on Twitter by security researcher Dominic Alvieri, appeared to show folders bearing the names of a range of global businesses: among them were delivery and logistics company DHL, US cable network C-Span, and French bank BNP Paribas.

Also in the list were tech giants Facebook and Apple, with the latter referred to in a folder titled “apple-health-app.” The data appears to be development material for Globant’s BeHealthy app, described in a prior press release as software developed in partnership with Apple to track employee health behaviors using features of the Apple Watch. Neither Apple not Globant responded to a request for comment at time of publication.

On Telegram, Lapsus$ shared a torrent link to the allegedly stolen data with a message announcing, “We are officially back from a vacation.”

If confirmed, the leak would show a swift return to activity after seven suspected members of Lapsus$ were arrested by

British police less than a week ago.

The arrests, first reported on March 24th by BBC News, were carried out by City of London Police after a yearlong investigation into the alleged ringleader of the gang, who is believed to be a teenager living with his parents in Oxford. On the other side of the Atlantic, the FBI is also seeking information on Lapsus$ related to the breach of US companies.

The Lapsus$ gang has been remarkably prolific in the range and scale of companies it has breached, having previously extracted data from a number of well-known technology companies, including Nvidia, Samsung, Microsoft, and Vodafone.

Most recently, Lapsus$ was in the spotlight for a hack affecting the authentication platform Okta, which put thousands of businesses on high alert against subsequent breaches. The latter hack has been an embarrassment for a company that provides security services to other businesses and led to criticism of Okta for a slow disclosure.

Correction, 1:38PM ET: *A previous version of this post overstated the connection between the breached data and Apple. The data labelled as "apple-health" was not data from Apple itself, but from an app developed in partnership with Apple. The Verge regrets the error.*

https://www.theverge.com/2022/3/30/23003194/lapsus-gang-new-hack-apple-facebook-globant