Lapsus$ suspects arrested for Microsoft, Nvidia, Okta hacks

By Ionut Ilascu

Published: 2022-03-24 · Archived: 2026-04-05 14:00:13 UTC

As Lapsus$ data extortion gang announced that several of its members are taking a vacation, the City of London Police say they have arrested seven individuals connected to the gang.

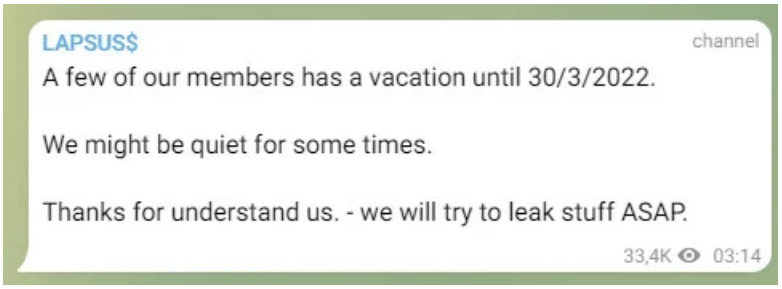
A minor in Oxford, England, is believed to be among the leaders of the group that leaked closed source code and proprietary data from high-profile companies like Nvidia, Samsung, Microsoft, and Okta.

Lapsus$ has also claimed attacks on game developer Ubisoft, telecom company Vodafone, and e-commerce giant Mercado.


DIE LINKE.
0:00

Some members may take a longer break

The latest public message from the group on Wednesday announced that some of its members were taking a vacation until March 30.



It is unclear how many members are in Lapsus$ but clues from their Telegram chats seem to suggest that there are members who speak English, Russian, Turkish, German, and Portuguese.

In a statement to the BBC, the City of London Police said that it had arrested seven people aged 16 to 21 “in connection with an investigation into a hacking group” and that all of them are under investigation.

No names have been released but the real identities of some Lapsus$ members have been known for a while as they had been doxed by rival hackers.

One of them is a teenager using the aliases White/Breachbase, a 17-year-old known from Oxford, England, who is believed to have accumulated over 300 BTC - around $13 million at today’s value, from hacking activities, SIM swapping being one of them.

Allegedly, White lost a good part of this fortune gambling and by leaving their system unprotected, allowing it to get hacked, twice.

The aliases above are just a few of more than a dozen the teenager used online, along with a couple of pseudonyms used on various platforms and hacker forums

Along with identifying information that included the real name, home address, date of birth, and education, rival hackers also published private photos of White with their family.

This was possible because of the long string of poor opsec decisions that left behind an identification trail, which appears to be a flaw that extends to other members of the Lapsus$ group as well.

A sample of this is exemplified by Bill Demirkapi, senior security engineer at Zoom, who noticed that Lapsus$ bragged about breaching Microsoft while stealing the source code:

While this is not a crtitical mistake in revealing the identity of the group, it shows that their operational security skills are incredibly lacking, allowing security researchers and rivals alike to link email accounts and usernames to their real identity.

These operational security mistakes are likely what allowed law enforcement to identify and arrest many of the cybercrime gang's members.

Source: https://www.bleepingcomputer.com/news/security/lapsus-suspects-arrested-for-microsoft-nvidia-okta-hacks/