

Brazil arrests suspect believed to be a Lapsus\$ gang member

By Sergiu Gatlan

Published: 2022-10-19 · Archived: 2026-04-05 12:57:21 UTC



Today, the Brazilian Federal Police arrested a Brazilian suspect in Feira de Santana, Bahia, believed to be part of the Lapsus\$ extortion gang.

The suspect was detained following an investigation started in December 2021 after last year's breach of the Brazilian Ministry of Health.

During the incident, the attackers deleted files and defaced the Ministry of Health website to display a message where the Lapsus\$ hacking group claimed the attack and said it had stolen data from the ministry's network.



Visit Advertiser website [GO TO PAGE](#)

The investigations that led to the arrest are a result of Operation Dark Cloud, launched in August and aiming to collect information on the activity of a possible criminal organization behind multiple cyberattacks targeting Brazilian government agencies since the end of last year.

Besides the Ministry of Health, the group also targeted dozens of other Brazilian Federal Government bodies and entities, including the Ministry of Economy, the Comptroller General of the Union, and the Federal Highway Police.

"The crimes determined in the police investigation are those of criminal organization, invasion of a computer device, interruption or disturbance of telegraphic, radiotelegraphic or telephone service, preventing or hindering its restoration," the Brazilian Federal Police [said](#) (automated translation).

"It was also found the practice of corruption of minors, a crime provided for in the Statute of Children and Adolescents, and money laundering, according to Law No. 9,613/1998."

Lapsus\$ member arrests

The City of London Police also [arrested seven individuals](#) from the UK in late March under suspicions that they were connected with the Lapsus\$ gang.

Two of them [were charged](#) on April 2nd with helping the Lapsus\$ extortion gang. They were both released on bail after appearing in the Highbury Corner Magistrates Court.

Last month, UK Police also detained a 17-year-old teen believed to be behind the [Uber](#) hack, [attributed to the Lapsus\\$ extortion group](#).

The Lapsus\$ gang has made the news this year after attacking high-profile tech companies worldwide, including [Microsoft](#), [Nvidia](#), [Samsung](#), [Ubisoft](#), [Okta](#), telecom company Vodafone, and e-commerce giant [Mercado](#).

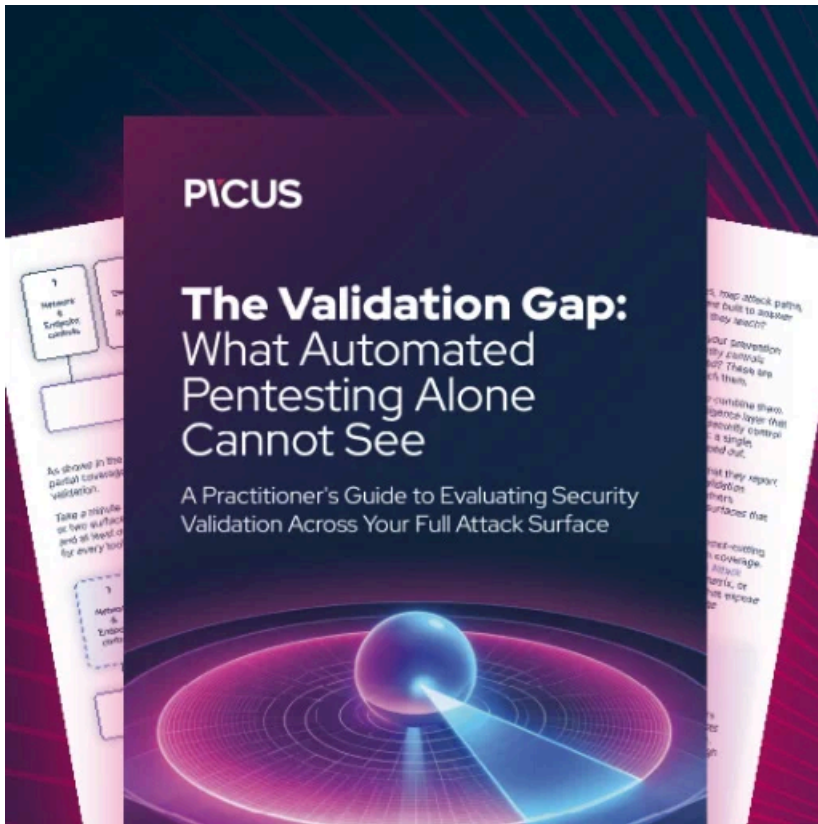
In many cases, the extortion group also leaked closed source code and proprietary data stolen from their victims, leading to massive data leaks.

Most Lapsus\$ members are believed to be teenagers driven not by financial motivation but mainly by their goal of making a name on the hacking scene.

The FBI is also looking into Lapsus\$'s illegal activities and seeking info concerning those group members who were involved in the compromise of computer networks belonging to US-based companies.

"These unidentified individuals took credit for both the theft and dissemination of proprietary data that they claim to have illegally obtained," the US law enforcement agency [says](#). "The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions."

Although it's still unclear how many active members the gang still has, it is believed that Lapsus\$ has affiliates worldwide and, based on [Telegram chats seemingly suggesting](#), they speak multiple languages, including English, Russian, Turkish, German, and Portuguese.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/brazil-arrests-suspect-believed-to-be-a-lapsus-gang-member/>