Lapsus$ teen hackers convicted of high-profile cyberattacks

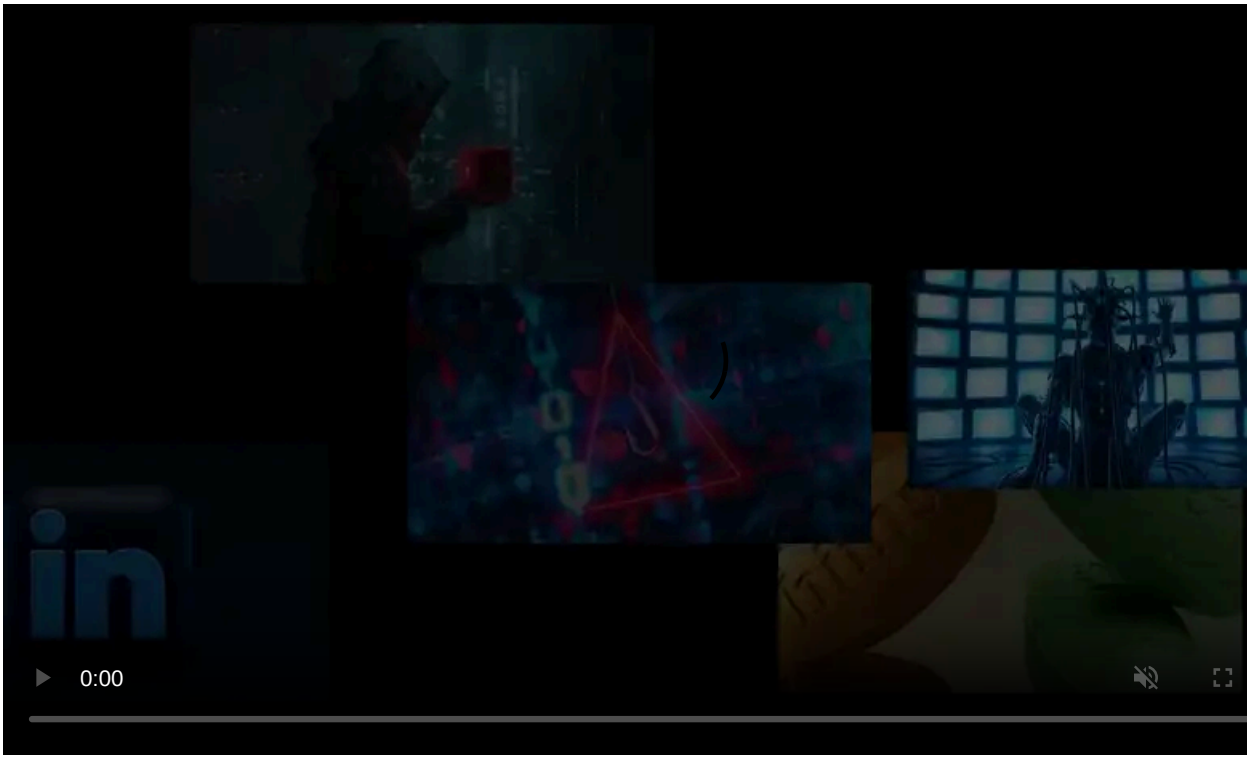
By Ionut Ilascu

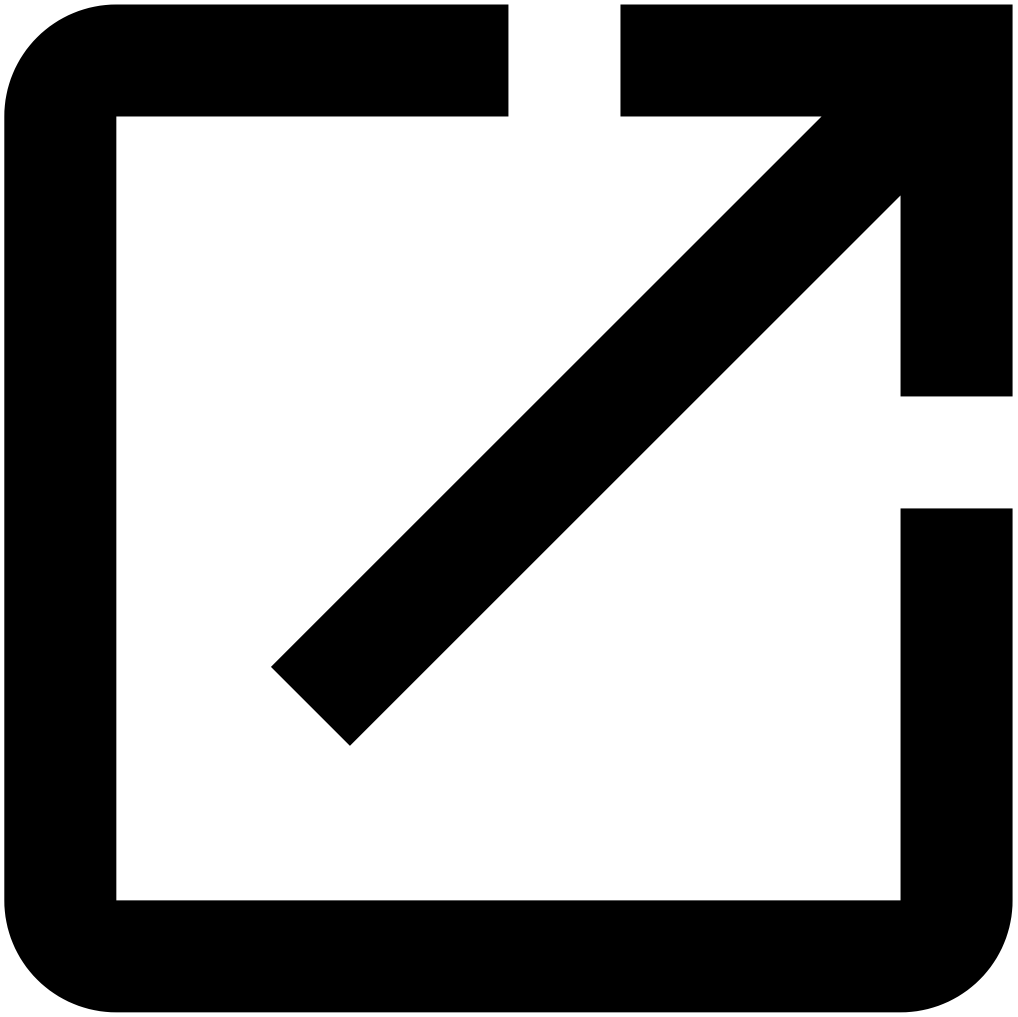
Published: 2023-08-23 · Archived: 2026-04-05 18:05:18 UTC

A London jury has found that an 18-year-old member of the Lapsus$ data extortion gang helped hack multiple high-profile companies, stole data from them, and demanded a ransom threatening to leak the information.

Believed to be one of the leaders of the group, Arion Kurtaj, from Oxford, England, was arrested twice in 2022, first in January and then again in March, in connection with Lapsus$ hacking activity.

He is on trial for breaching fintech company Revolut, ride-sharing service Uber, and game developer Rockstar Games.


0:00



High-profile organizations impacted by Lapsus$ also include Microsoft, Cisco, Okta, Nvidia, T-Mobile, Samsung, Vodafone, Ubisoft, 2K, and Globant.

Leaking data while on bail

Kurtaj is autistic and was not deemed fit to be in court. However, a jury was asked to determine if he was responsible for the alleged hacking activity, disregarding criminal intent.

The teenager is believed to have breached the City of London Police cloud storage after he was arrested in connection with the attack on mobile operator EE.

It is alleged that after that with the help of some Lapsus$ members, Kurtaj targeted Revolut, Uber, and Rockstar Games, demanding millions of U.S. dollars in ransoms.

Using the handle 'teapotuberhacker' and while on bail at a hotel, Kurtaj leaked gameplay videos from the unreleased Grand Theft Auto 6, obtained after breaching the game developer's Slack server and Confluence wiki.

Kurtaj used more than a dozen online names, White and Breachbase among them, and is believed to have made more than 300 BTC from his hacking activity, SIM-swapping included.

Most of the money was lost to gambling or hackers that breached White's computer, allegedly twice.

Kurtaj is not the only teenager on trial for Lapsus$-related hacking activity. Another member of the gang, a 17-year-old also suffering from autism, has been convicted for breaching companies as well.

Despite being a loosely organized group of mostly teenagers, Lapsus$ managed to breach organizations with a strong sense of security.

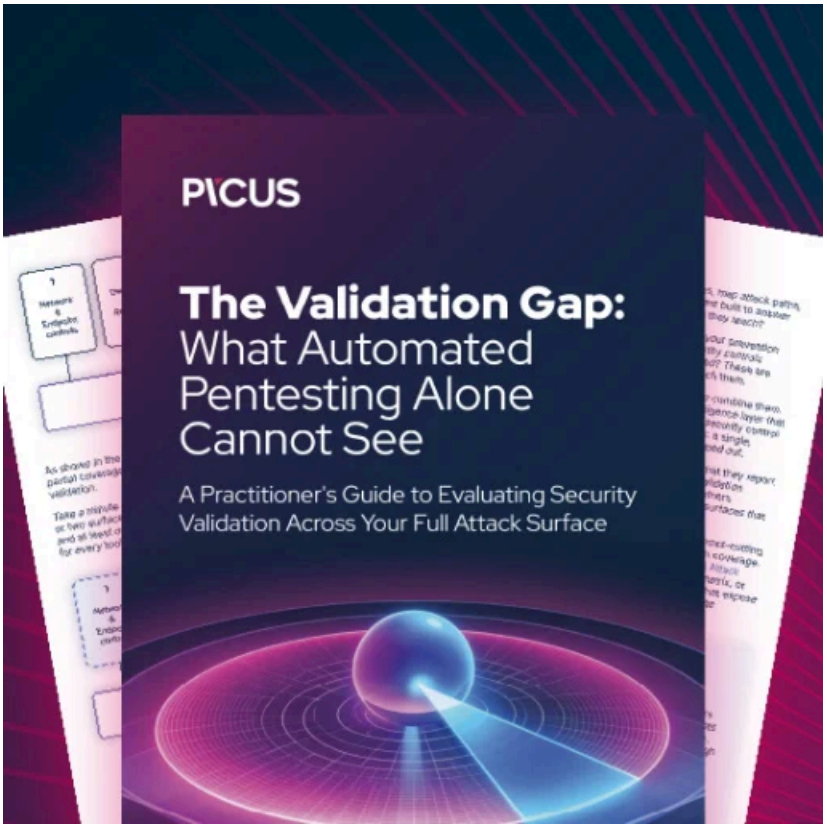
Skilled actors still get caught

A recent report from the U.S. government notes that the gang used low-cost techniques to reveal "weak points in our cyber infrastructure."

The members of the group took SIM-swapping to the next level by paying $20,000 a week for access to a telecommunication provider's platform, which allowed them to hijack targeted phone numbers and obtain one-time passcodes to various accounts.

Lapsus$ activity spread from 2021 to 2022 and involved individuals from the U.K. and Brazil who used social engineering and hacking techniques of various complexity to breach companies for fame, financial game, and fun.

Last year in September Lapsus$ activity died, as law enforcement started arresting multiple members of the group: multiple individuals in the U.K. [1, 2] and another one in Brazil.



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/lapsus-teen-hackers-convicted-of-high-profile-cyberattacks/