DHS Cyber Safety Board to review Lapsus$ gang’s hacking tactics

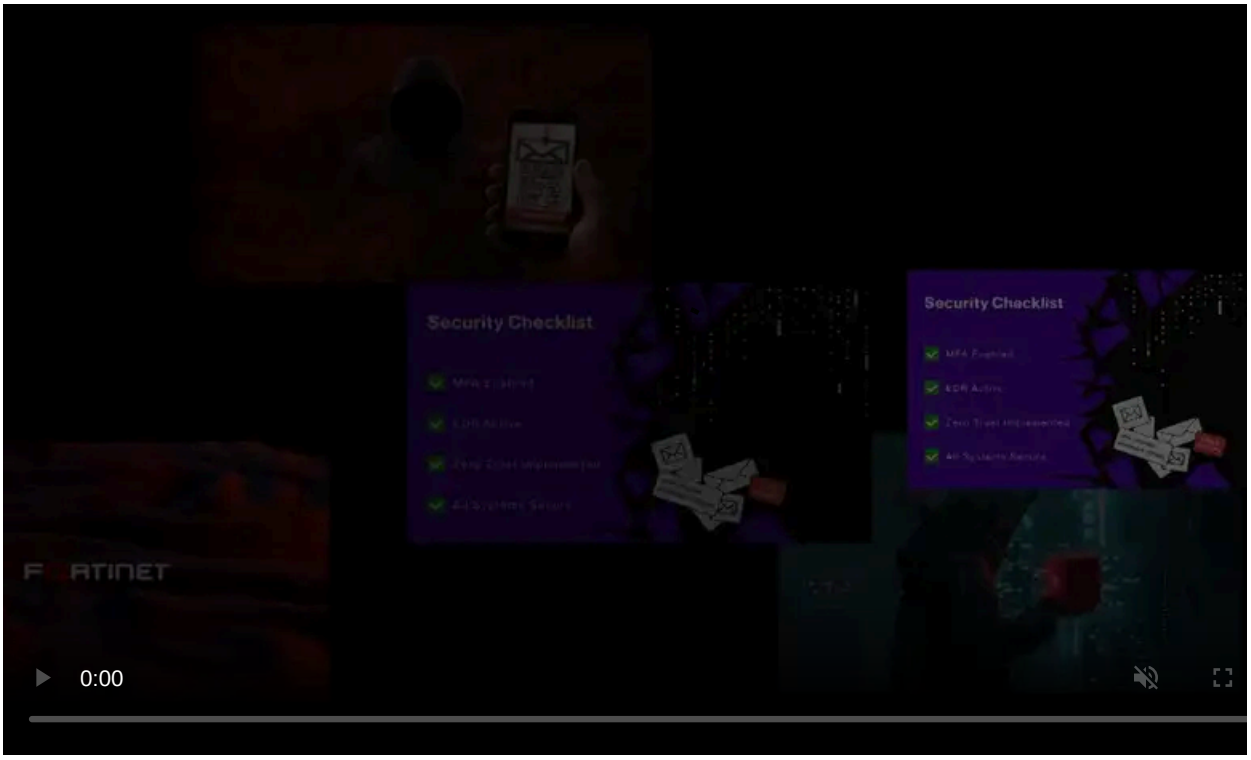
By Sergiu Gatlan

Published: 2022-12-02 · Archived: 2026-04-06 15:32:17 UTC

The Department of Homeland Security (DHS) Cyber Safety Review Board will review attacks linked to an extortion gang known as Lapsus$, which breached multiple high-profile companies in recent incidents.

The Lapsus$ hacker group made the news earlier this year after hacking Microsoft, Nvidia, T-Mobile, Samsung, Uber, Vodafone, Ubisoft, Okta, and e-commerce giant Mercado Libre.

Following many incidents they were linked to, the extortion group also leaked proprietary data and source code stolen from their victims' networks, leading to massive data breaches and leaks.


Security Checklist
Security Checklist
F ATINET
0:00

As announced on Friday, the goal behind CSRB's review of the gang's hacking activities is to provide advice on defending against Lapsus$ attacks.

"With its review into Lapsus$, the Board will build on the lessons learned from its first review and share actionable recommendations to help the private and public sectors strengthen their cyber resilience," DHS Secretary Alejandro N. Mayorkas said.

"As cyber threats continue to evolve, it is imperative that all organizations recognize that they are not invincible. The CSRB will review the cyber activity of Lapsus$ in order to analyze their tactics and help organizations of all sizes protect themselves," CSRB Deputy Chair Heather Adkins added.

The Cyber Safety Review Board is a public-private initiative composed out of 15 cybersecurity experts from private sector organizations and federal government entities.

It was established by President Biden via executive order in May 2021 to assess attacks leading to "significant cyber incident," provide defense recommendations, and share any relevant confidential information with law enforcement.

While the CSRB doesn't have enforcement authority or regulatory powers, it reports directly to the Secretary of Homeland Security and the President to ensure that relevant lessons are noted and its recommendations are implemented and addressed.

Some Lapsus$ members arrested by law enforcement

Earlier this year, the FBI said it's also looking into Lapsus$'s illegal activities and is seeking info regarding group members involved in the compromise of computer networks belonging to US-based organizations.

Some suspected Lapsus$ members have already been arrested and charged for involvement in some of the gang's attacks by the City of London Police, the U.K. Police, and the Brazilian Federal Police.

Most of this group's members are believed to be teenagers driven not by financial motivation but by their aim of making a name for themselves on the hacking scene.

"Lapsus$ actors have perpetrated damaging intrusions against multiple critical infrastructure sectors, including healthcare, government facilities, and critical manufacturing," CISA Director Jen Easterly said.

"The range of victims and diversity of tactics used demand that we understand how Lapsus$ actors executed their malicious cyber activities so we can mitigate risk to potential future victims. We applaud the CSRB for taking on this review to help advance our collective cyber defense."
