Ubisoft confirms 'cyber security incident', resets staff passwords

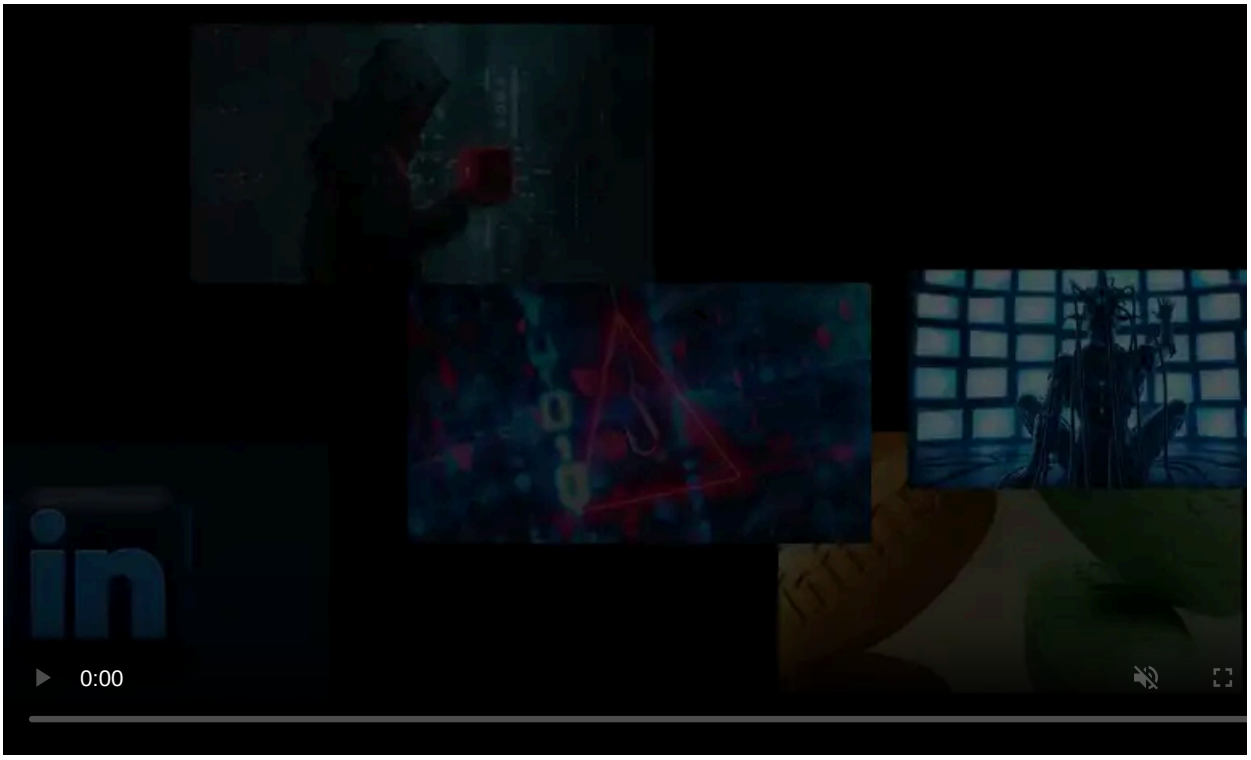
By Ax Sharma

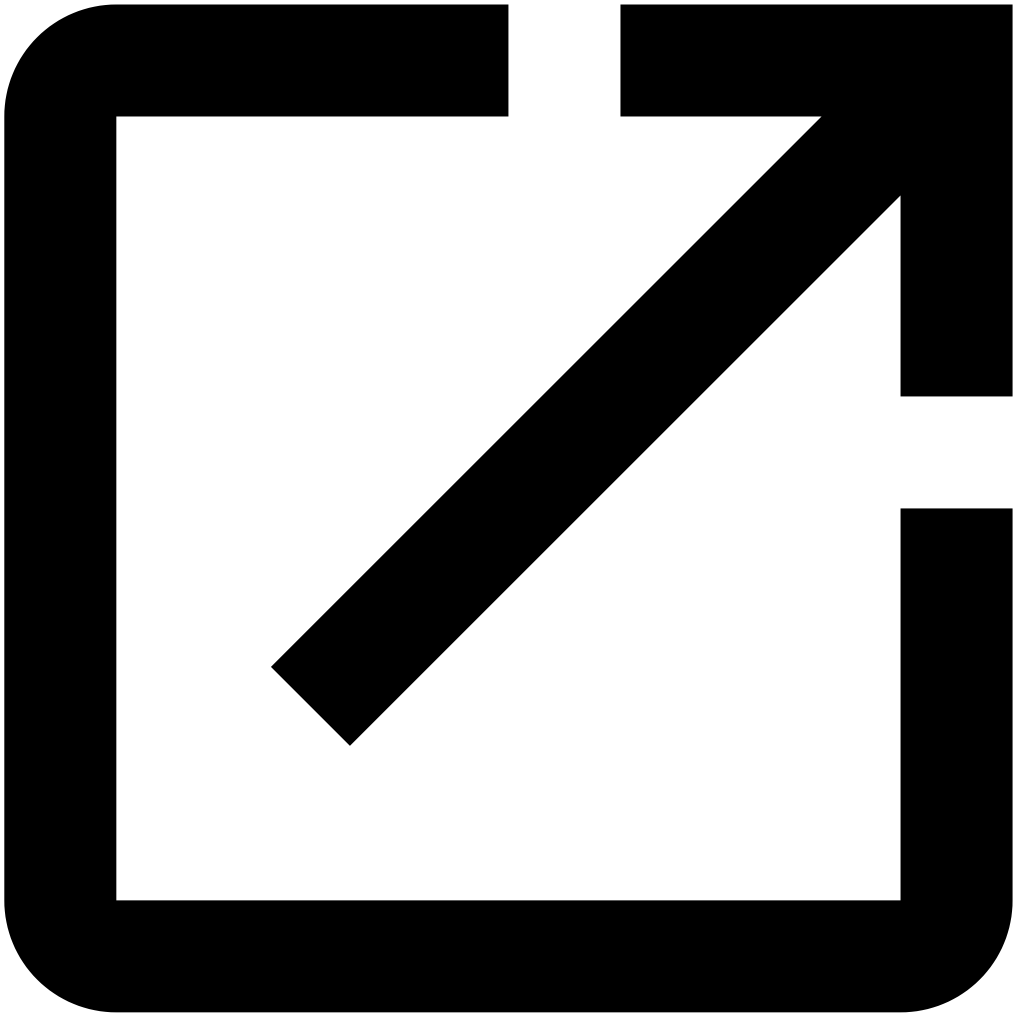
Published: 2022-03-12 · Archived: 2026-04-05 16:31:06 UTC

Video game developer Ubisoft has confirmed that it suffered a 'cyber security incident' that caused disruption to its games, systems, and services.

The announcement comes after multiple Ubisoft users had reported issues last week accessing their Ubisoft service.

Data extortion group LAPSUS$, who has claimed responsibility for hacking Samsung, NVIDIA, and Mercado Libre thus far, appears to be behind this incident.


0:00



Ubisoft initiates 'company-wide password reset'

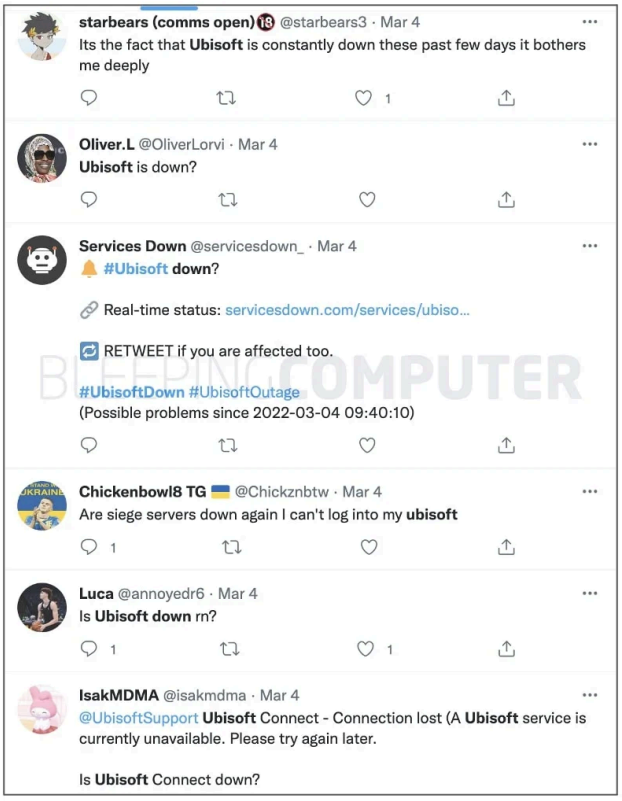
Video game production giant Ubisoft states it experienced a cyber security incident sometime last week.

"Last week, Ubisoft experienced a cyber security incident that caused temporary disruption to some of our games, systems, and services," says the company in a succinct news release.

"Our IT teams are working with leading external experts to investigate the issue. As a precautionary measure we initiated a company-wide password reset."

Headquartered in Montreuil with its studios around the world, the game maker has repeatedly produced hit titles including Assassin's Creed, Far Cry, For Honor, Just Dance, Prince of Persia, Rabbids, Rayman, Tom Clancy's, and Watch Dogs.

On March 4th, users on Twitter and Downdetector did report issues accessing some of the Ubisoft services, that appear to be linked to this incident:



Ubisoft users reported issues last week (Twitter)

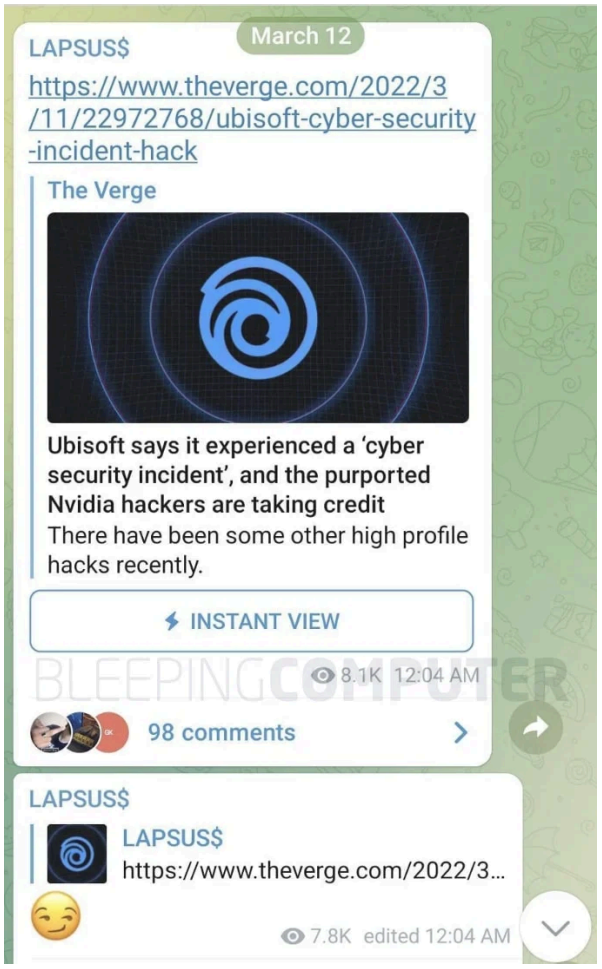
At this time, there is no evidence indicating any personal information of players was exposed during the incident.

The company confirms that all Ubisoft games and services are now functioning normally.

LAPSUS$ group reacts to the disclosure

News of Ubisoft confirming the cyber security incident was first reported by The Verge.

Moments later, admins of what is believed to be Lapsus$' Telegram group reacted to The Verge's initial report with a smirk emoji, insinuating that Lapsus$ is behind the hack:



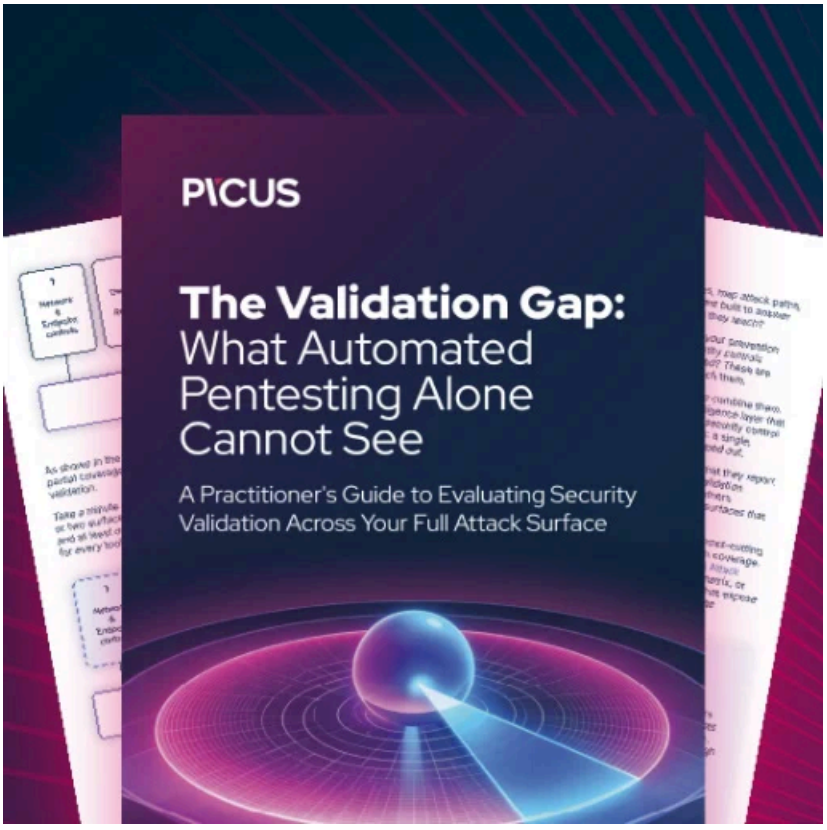
Lapsus$ group appears to claim responsibility on Telegram (BleepingComputer)

Lapsus$ has previously leaked gigabytes of proprietary data purportedly stolen from leading companies as Samsung, NVIDIA, and Mercado Libre confirmed this month they had suffered a breach.

Data extortion groups like Lapsus$ breach victims but as opposed to encrypting confidential files like a ransomware operator would, these actors steal and hold on to victims' proprietary data, and publish it should their extortion demands not be met.

In 2020, Egregor ransomware had hit game developer Crytek and leaked what they claim were files stolen from Ubisoft's network. Although, at the time, Ubisoft did not confirm the authenticity of the claim.

In this case, however, it does not seem that Lapsus$ or any other threat actor was able to obtain Ubisoft's proprietary data, and the investigation continues.



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/ubisoft-confirms-cyber-security-incident-resets-staff-passwords/