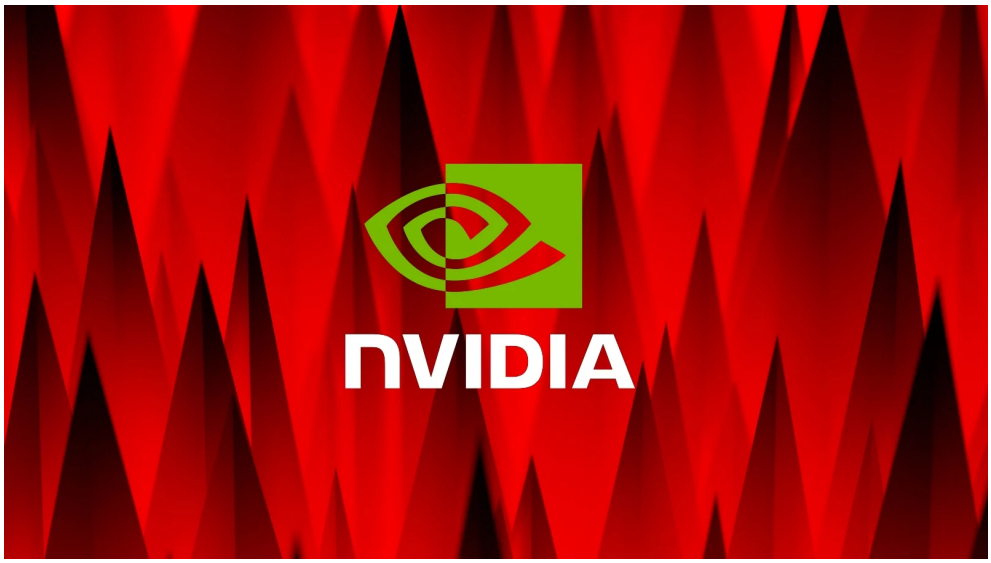
NVIDIA data breach exposed credentials of over 71,000 employees

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** March 3, 2022 04:59 PM **0**



More than 71,000 employee credentials were stolen and leaked online following a data breach suffered by US chipmaker giant Nvidia last month.

The Have I Been Pwned data breach notification service has added data belonging to 71,335 compromised accounts to its database on Wednesday.

Have I Been Pwned says the stolen data contains "email addresses and NTLM password hashes, many of which were subsequently cracked and circulated within the hacking community."

Nvidia confirmed on March 1st that its network was breached last month (https://www.bleepingcomputer.com/news/security/nvidia-confirms-data-was-stolen-in-recent-cyberattack/), with the attackers gaining access to employees' login data and proprietary information.

Attack claimed by the Lapsus$ extortion gang

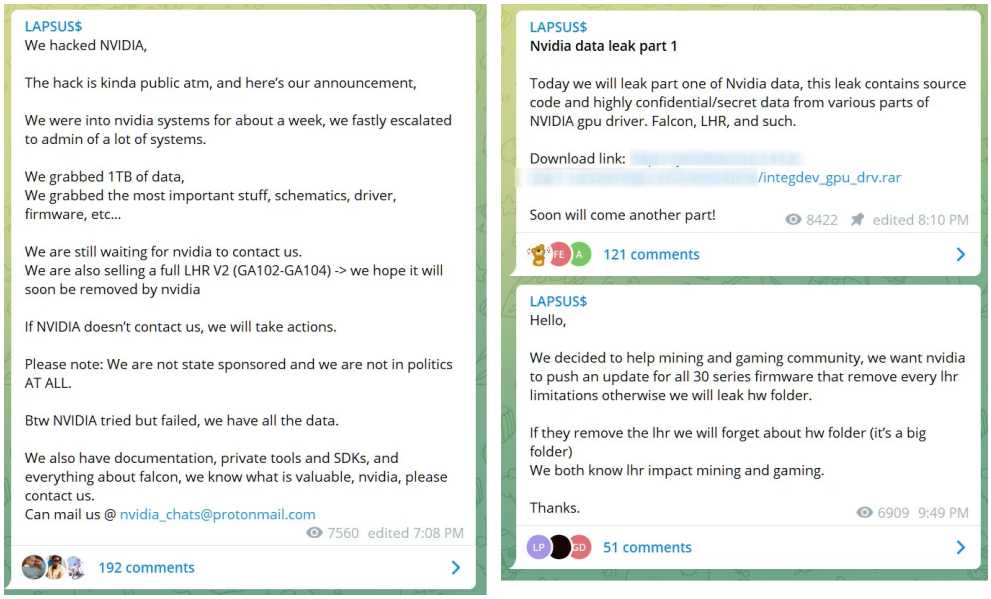
Nvidia said it was investigating an "incident" (https://www.bleepingcomputer.com/news/security/gpu-giant-nvidia-is-investigating-a-potential-cyberattack/) that had reportedly impacted some of its systems, causing a two-day outage after news of the incident first came to light almost a week ago (https://www.bleepingcomputer.com/news/security/gpu-giant-nvidia-is-investigating-a-potential-cyberattack/).

The same day, a data extortion group dubbed Lapsus$ claimed the attack and provided details regarding the incident, including that they stole 1TB of data from Nvidia's network.

Over the weekend, Lapsus$ shared even more details about the intrusion (https://www.bleepingcomputer.com/news/security/hackers-to-nvidia-remove-mining-cap-or-we-leak-hardware-data/) and leaking a 20GB archive containing data stolen from Nvidia's systems, as well as company employees' password hashes,

The group threatened to leak hardware specifications info (https://www.bleepingcomputer.com/news/security/hackers-to-nvidia-remove-mining-cap-or-we-leak-hardware-data/) unless lite hash rate (LHR) limitations from GeForce RTX 30 Series firmware were not removed.

Lapsus$ also asked Nvidia to commit to open-sourcing their GPU drivers (https://twitter.com/serghei/status/1498779322450169859) for Windows, macOS, and Linux devices until Friday, March 4th, to avoid having stolen information on all recent GPUs, including the RTX 3090Ti, leaked online.



Lapsus$ claiming the attack on Nvidia (BleepingComputer)

After refusing to confirm the extortionists' claims, Nvidia told BleepingComputer Tuesday that it detected "a cybersecurity incident which impacted IT resources" on February 23rd.

The company added that it found no evidence of a ransomware attack, although the threat actor still managed to steal employee credentials and proprietary data, confirming Lapsus$'s claims.

"However, we are aware that the threat actor took employee credentials and some NVIDIA proprietary information from our systems and has begun leaking it online. Our team is working to analyze that information," Nvidia told BleepingComputer.

"We do not anticipate any disruption to our business or our ability to serve our customers as a result of the incident."