# LAPSUS and the Terrible, Horrible, No Good, Very Bad Ransom Day 1 (UPDATED) - DataBreaches.Net

Published: 2022-02-27 · Archived: 2026-04-09 02:14:51 UTC

***First they thought their victim hacked them back. Then they appeared to be trolled by a "negotiator" who wasn't. I don't know if the Brazilian threat actors who call themselves LAPSUS felt like moving to Australia after a bad day at the ransom office yesterday, but their attack on Nvidia and the aftermath seemed somewhat… unusual, to say the least.***

On February 26, word of the attack on chip giant Nvidia gained attention on Twitter after LAPSUS used their Telegram channel to leak what they claimed was employee data. They also threatened to leak 1TB of Nvidia's data.  @DarkTracer_int tweeted some screencaps:

At that point, it seemed to be a fairly standard situation — threat actors claim to have compromised victim, leak some data as proof of claim, and make threats, while the victim entity says it is investigating the claims.

But what happened next started to derail this one.

LAPSUS, typing in always-ridiculed all uppercase capitals with tons of exclamation points, claimed that Nvidia were criminals because they hacked them back.

*LAPSUS claimed that Nvidia had hacked back.*

> LAPSUS$, [2/26/2022 1:02 AM] EVERYONE!!! NVIDIA ARE CRIMINALS!!!!!!!!!
>
> SOME DAYS AGO A ATTACK AGAINST NVIDIA AND STOLE 1TB OF CONFIDENTIAL DATA!!!!!!
>
> TODAY WOKE UP AND FOUND NVIDIA SCUM HAD ATTACKED **THE** MACHINE WITH RANSOMWARE…….
>
> LUCKILY IT HAD A BACKUP BUT WHY THE FUCK THEY THINK THEY CAN CONNECT TO THE PRIVATE MACHINE AND INSTALL RANSOMWARE!!!!!!!!!!

> LAPSUS$, [2/26/2022 1:03 AM] (100% DISK USAGE) from nvidia ENCRYPTING **THE** DRIVES!!!!!!!!!!

LAPSUS later offered an explanation as to how Nvidia allegedly hacked them and encrypted their drives:

> To address all the rumours about how nvidia hacked us.
>
> Its simple.

> Access to nvidia employee VPN requires the PC to be enrolled in MDM (Mobile Device Management)
>
> With this they were able to connect to a VM we use.
>
> Yes they successfully encrypted the data. However we have a backup and it's safe from scum!!!
>
> We were not hacked by a competitors group or any sorts.

Marcus Hutchins (@malwaretechblog) offered a somewhat different explanation:

> To me this sounds a lot like LAPSUS$ installed Nvidia's corporate agent on their own machine then triggered a data loss prevention policy, which they mistook for ransomware because they're morons. https://t.co/NNF27yidE6
>
> — Marcus Hutchins (@MalwareTechBlog) February 27, 2022

> To me this sounds a lot like LAPSUS$ installed Nvidia's corporate agent on their own machine then triggered a data loss prevention policy, which they mistook for ransomware because they're morons. — Marcus Hutchins (@MalwareTechBlog) February 27, 2022

In less than 24 hours, LAPSUS had gone from appearing to be a threat to rapidly losing credibility. And their day wasn't over yet…..

**The Negotiations That Weren't**

While DataBreaches.net continued to try to get a response from Nvidia about the claimed hack-back, this site was contacted by a Russian threat actor who has communicated with this site in the past. "Tokyo" (one of his aliases) informed this site that he wanted to expose LAPSUS as frauds and to make a point to victims that you can't trust amateur groups. To make that point, it seems that Tokyo posed as a negotiator for Nvidia.

"No one should trust this shitty group who didnt even confirm that i was genuine," Tokyo told this site.

DataBreaches.net was shown the chat log between Tokyo and "SigmA" from Lapsus. This site was also provided with some of the email chain for the negotiations, one of which included a URL provided by Lapsus for the sample data. The archived sample, which was still available on the URL as of today, contained almost 20 GB of source code and other non-personal information. It also contained a SpyEye trojan.

The following is a screencap of the folders in the sample archive:

*Directory of files in the archived sample provided by Lapsus. Image: DataBreaches.net*

According to the email chain and statements to this site by “Tokyo,” LAPSUS asked $750,000 to delete all the data they had exfiltrated.

*Part of email negotiations thread between Lapsus and someone posing as Nvidia negotiator. Lapsus had been told to email the amount demanded to specific employees, who had no knowledge of the ruse or troll at all. Image: Provided. URL redacted by DataBreaches.net.*

The “negotiator” counteroffered $560,000 – an offer that Lapsus appeared to accept, providing their BTC wallet where payment could be made.

*Lapsus accepts the offer of $560k and provides their BTC wallet. The employee named in the chat had no participation or knowledge of any of this.*

But as you might have guessed by now, no, that wasn't the end of it, because the "negotiator" waited a while, and then sent another message, saying that he had made a mistake and the offer was $56,000 and not $560,000.

And of course, that wasn't real anyway.

At some point last night, LAPSUS removed Nvidia screencaps and data from their Telegram channel, which might have indicated that they thought they were getting paid. But according to their email to this site in response to inquiries, that's not what happened.

When asked about being trolled, a spokesperson replied:

> I suspected he was a fraud from the start. So I decided not to send him the most important data.
>
> I sent him some old GPU driver or something, not the important information about GV10* chips or 30** GPU's

The posts were removed, the spokesperson wrote, "due to the fact we are going to make a better announcement in some time."

In follow-up email, they indicated that they would be leaking about 100 GB of data soon after the time of their email.

In response to their explanation of their responses to him, Tokyo claims that they are just making excuses and had been completely cooperative, raising concerns about why they didn't actually verify him as a negotiator. And as to the posts being removed, he wrote, "This is bullshit. I [the negotiator] told them to take the posts down and they did."

As to Nvidia, well, DataBreaches.net had sent inquiries to Nvidia beginning early yesterday about the claimed hack-back but got no response. Nvidia finally responded late last night that they would be issuing a statement today. So far, that hasn't happened yet, and it is not clear to me that when they do issue a statement if they will address the questions this site put to them. This post will be updated if their statement contains any new information about the scope of the breach and their incident response.

**Update:** LAPSUS did post another announcement of the breach. In their statement, they claimed they were in Nvidia systems "for about a week," and they "grabbed the most important stuff, schematics, driver, firmware, etc… "

They also leaked some data, noting that "This leak contains source code and highly confidential/secret data from various parts of NVIDIA gpu driver. Falcon, LHR, and such." DataBreaches.net did not download it to determine if it was identical to the sample data this site had previously acquired and that included a trojan.

Less than two hours later, however, LAPSUS seemed to have changed their mind about leaking data, writing:

> We decided to help mining and gaming community, we want nvidia to push an update for all 30 series firmware that remove every lhr limitations otherwise we will leak hw folder.
>
> If they remove the lhr we will forget about hw folder (it's a big folder)
> We both know lhr impact mining and gaming.
>
> Thanks.

As to Nvidia's promised statement: they never sent this site any statement after more than 24 hours. In combination with LAPSUS's revised announcement, the breach may be worse than they were willing to acknowledge initially.

---

[1] *With apologies to Judith Viorst, the author of the classic children's book, Alexander and the Terrible, Horrible, No Good, Very Bad Day*

---

Source: https://www.databreaches.net/lapsus-and-the-terrible-horrible-no-good-very-bad-ransom-day1/