Lapsus$ Group - an emerging dark net threat actor leveraging insider threats-or was it?

By Silent Push Threat Team

Published: 2022-03-17 · Archived: 2026-04-05 15:49:30 UTC

Research by the Silent Push Labs team.

Introduction:

Lapsus$ Group is an extortion group that gained public recognition in the last few weeks due to its attacks to **NVIDIA** and **Samsung** where they stole and leaked critical information from the companies.

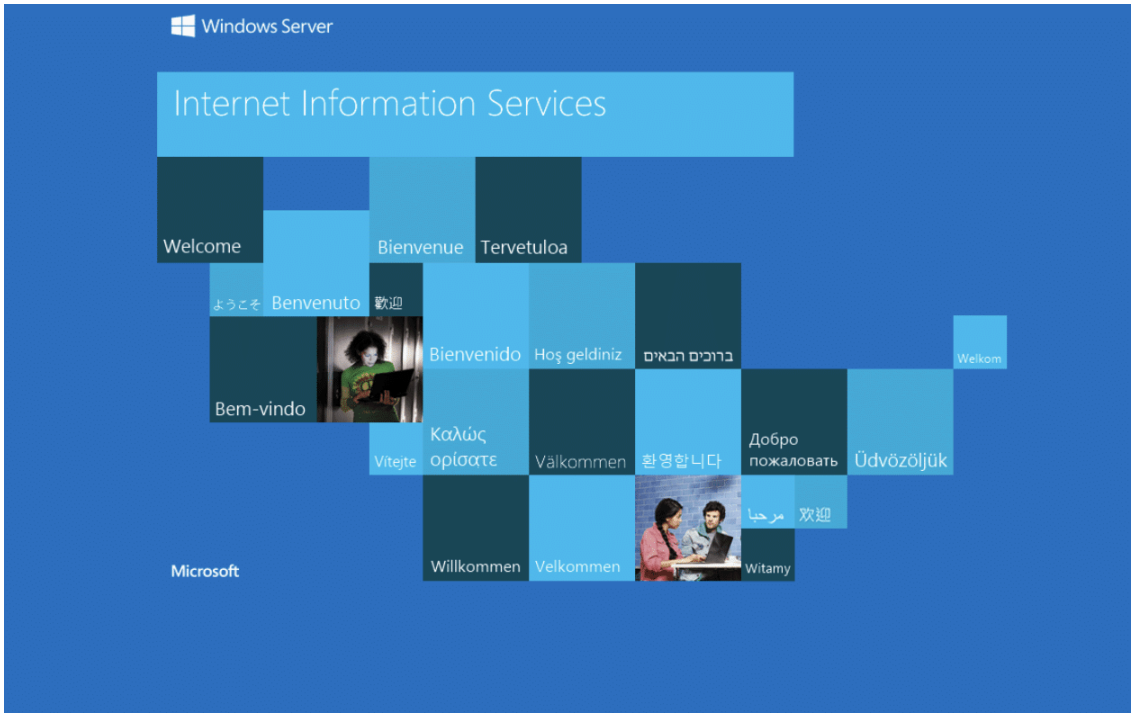
Previously they had conducted:

– a ransomware attack to the **Ministry of Health of Brazil** back in December 2021;
– DNS spoofing attacks to Portuguese speaking companies such as **Localiza**, **Submarino** and **Americanas** during the months of January and February of the current year 2022;
– cyber attacks where they stole confidential information from a Portuguese media and information company- **Impresa**– and a Brazilian TV and Telecommunications company- **Claro** and **Embratel**.

This latter type of attack, where critical data is accessed and stolen without being encrypted or deleted, is the most common procedure of the group and it is the reason why to this date, this threat actor does not fall under the category of a *ransomware group*.

Nevertheless, this threat actor is responsible for **leaking important data and confidential information** that compromises services and companies.

`lapsus-group[.]com` as of December 2021:



`lapsus-group[.]com` as of January 2022:

Methods

But how exactly does this threat actor infiltrate into its target systems?

The groups initial step appears to be to c**ollect authentic credentials** either by conducting phishing attacks or by advertising on the internet that they are looking to buy verified passwords from employees. However recent

updates may suggest they had access through the customer’s OKTA accounts. More on the updated timeline below.


LAPSUS$
31,724 subscribers
Pinned Message
SAMSUNG LEAK IS HERE! Now leaki...
LAPSUS$
We recruit employees/insider at the following!!!!
- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)
TO NOTE: WE ARE NOT
Join

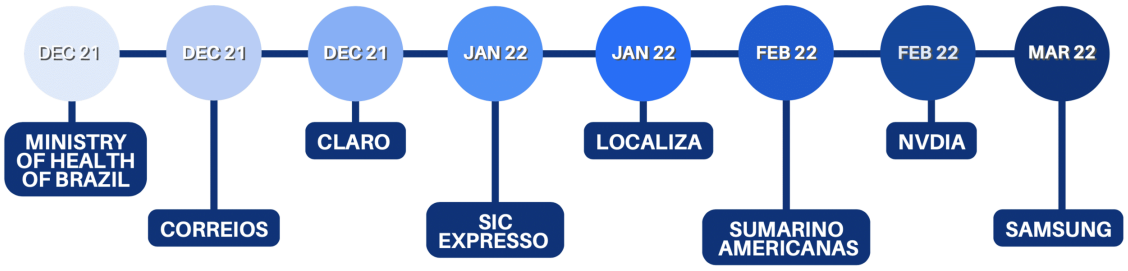
Lapsus recruit insiders

In this way, they can access the IT infrastructures with minimal detection, sometimes being in the system for weeks.
After either successfully having stolen enough data or being discovered, the subsequent step of the group is to **actively advertise their actions** on their public Telegram channel or by leaving a note on the compromised websites.
At last, the story unfolds as predicted: the gang **threatens the victim to either contact them or the crucial information will be leaked.**

Often, some bitcoin payment is demanded, but the requests vary. This backs up the hypothesis that this threat actor is not sponsored or politically motivated but **purely looking for money and recognition.**

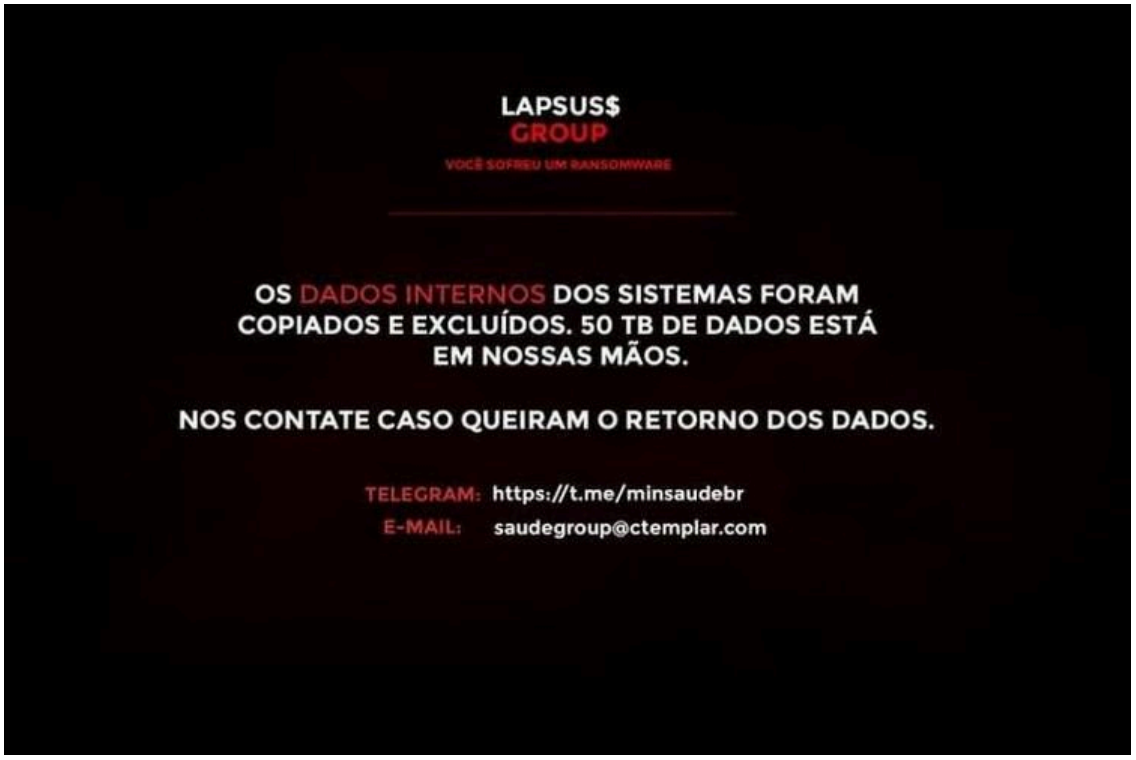
We have reasons to believe that the attacks from this extortion group will continue and become more frequent, possibly targeting international companies and infrastructures.

For that reason, we'll continuously monitor the activity of this threat actor, collecting information and Indicators of Compromise which will be available to the Silent Push customers under the tag **'lapsus$'.**



Confirmed Lapsus$ attacks

Ministry of Health of Brazil

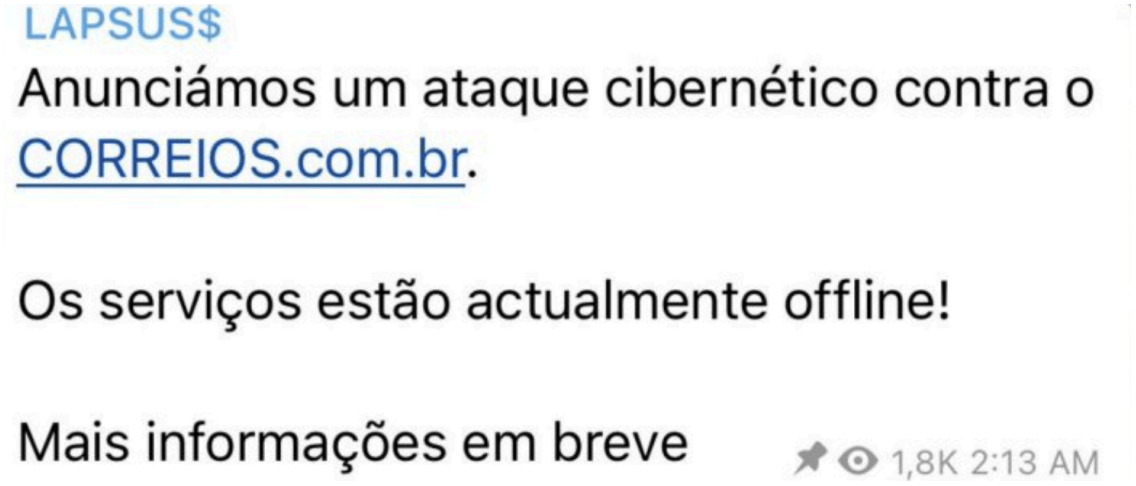


On December 10th 2021, the threat actor conducted a ransomware attack on the websites of the Ministry of Health of Brazil, blocking access to **COVID-19 vaccination certificates** and other vital information of the **public healthcare system.**

A Portuguese written message was left on the compromised websites where the group claimed to have stolen and erased **50 TB of data.**

Their contacts were also provided in order for negotiating the restoration of the stolen information.

Correios



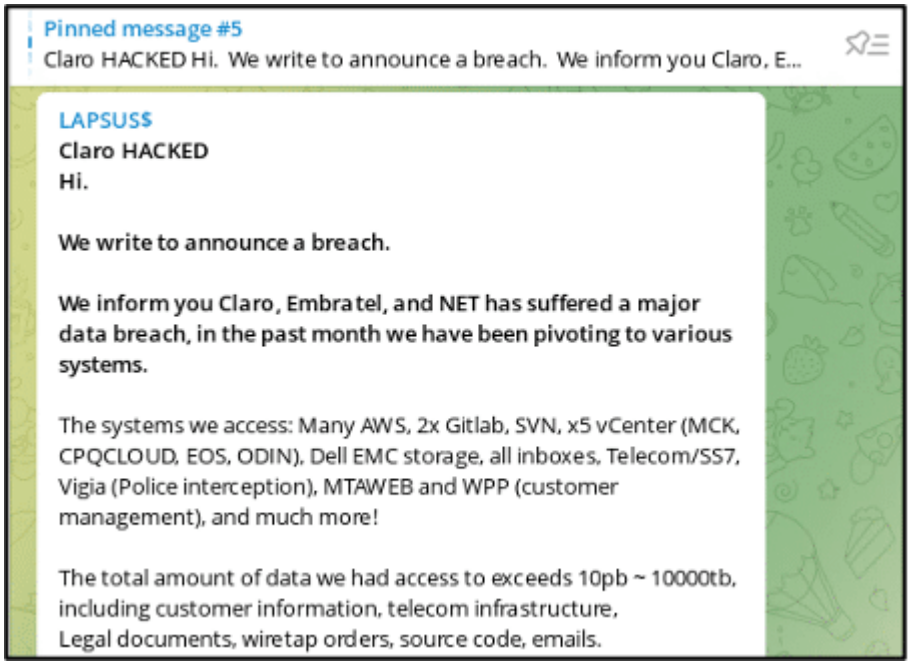
Lapsus$ announcement of attack on Correios

On December 23rd 2021, the post office company Correios **website** was taken down.

The group immediately utilized their Telegram channel to take responsibility for the attack.

Unlike the attack conducted to the Ministry of Health of Brazil, no message was left on the compromised website and there is no evidence that any data was accessed or stolen.

Claro and Embratel Telecommunications



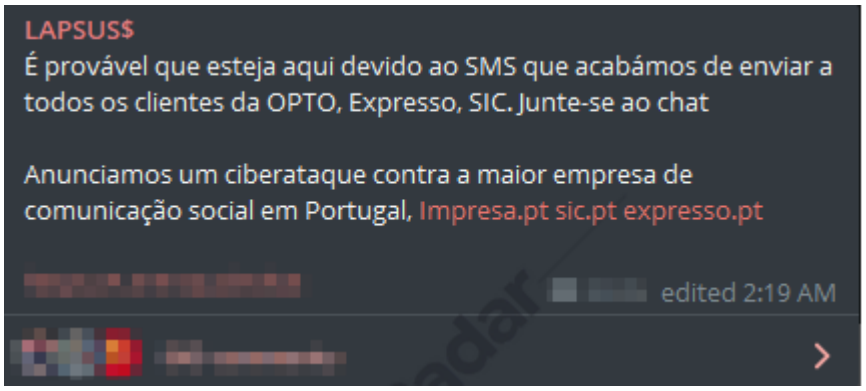
Lapsus$ announcing they have hacked Claro

On December 30th 2021 , the group posted a message on their Telegram claiming to having accessed Claro IT infrastructure and stolen almost **10000TB of confidential data.**

A previous post on their channel shows that the group was looking to buy the access credentials of a Claro employee. This suggests it is possible that they were on the system for brief period since many users reported

issues in the weeks prior to the attack.
With access to the cloud IT infrastructure and apparently undetected, the group claims to have collected sensitive data including **customer information**, **legal documents**, **emails**, **source codes**, **confidential court orders** and **wiretapping recordings**, and requested a monetary payment in order to stop the leakage of the information obtained.

Impresa



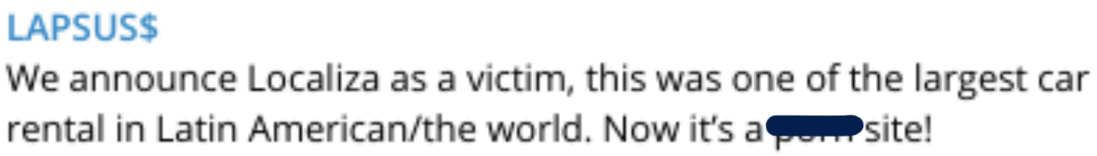
On January 2nd, a cyber attack conducted by this gang, **took down several websites** of Impresa, a Portuguese media and information company, for a brief number of days.
Additionally, the group accessed the **twitter and email accounts of Expresso** which they used to send tweets and emails sharing their Telegram account.
On the compromised websites, the group left their signature message, claiming to have gained access to the **AWS** servers of the company and requesting a monetary payment in order to stop the leakage of the information

obtained.

It is believed that the group obtained valid credentials obtained via a **fraudulent phishing campaign.**

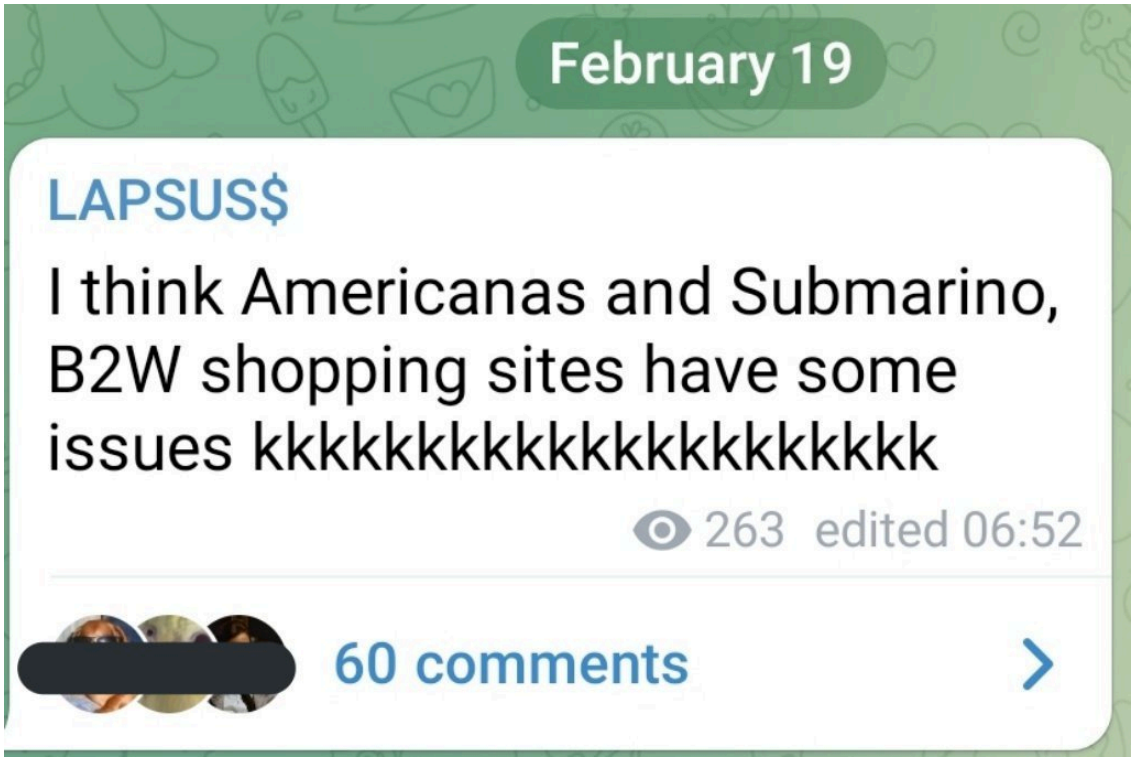
Big claims by Lapsus$

Localiza



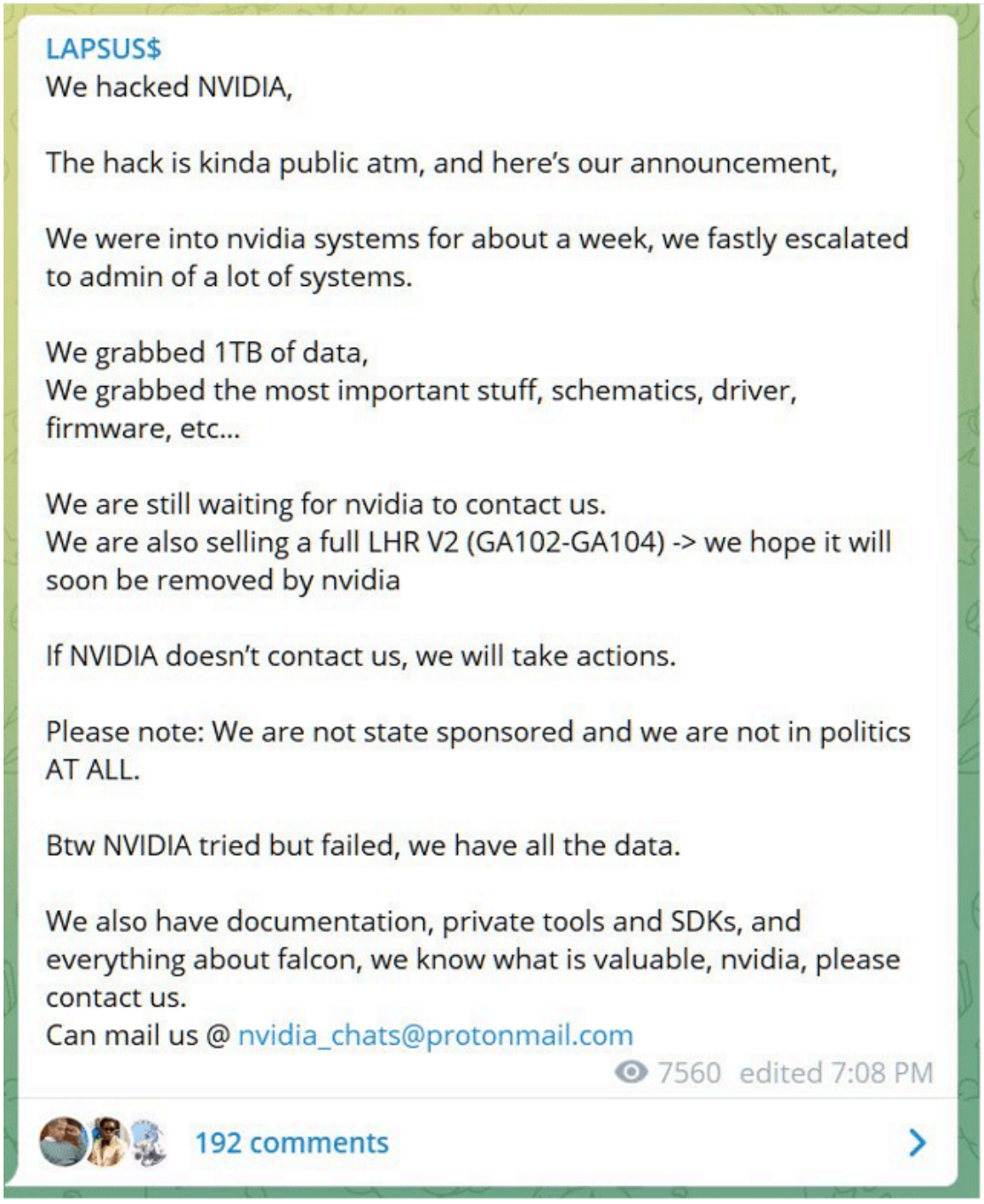
On January 11th lapsus$ performed a **DNS spoofing attack** on Localiza, a Brazilian rent-a-car, redirecting their website to an adult media one.

Submarino and Americanas



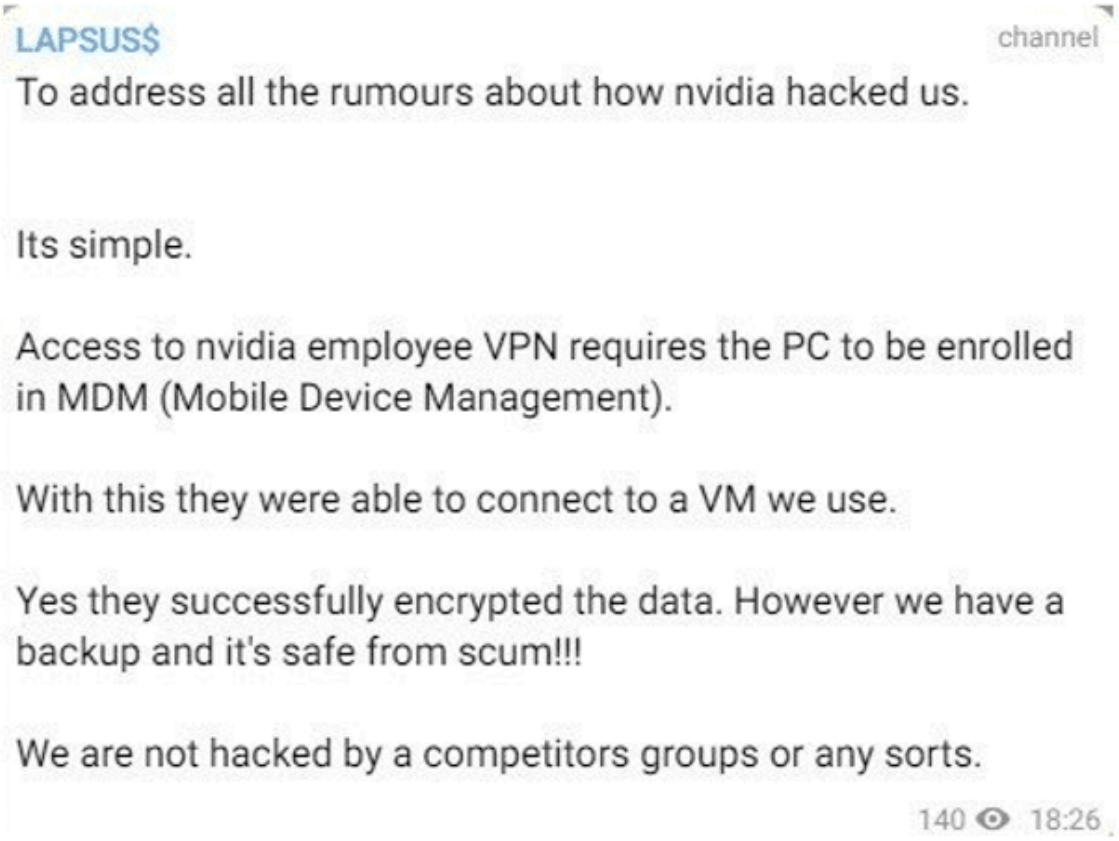
More announcements from Lapsus$

NVIDIA



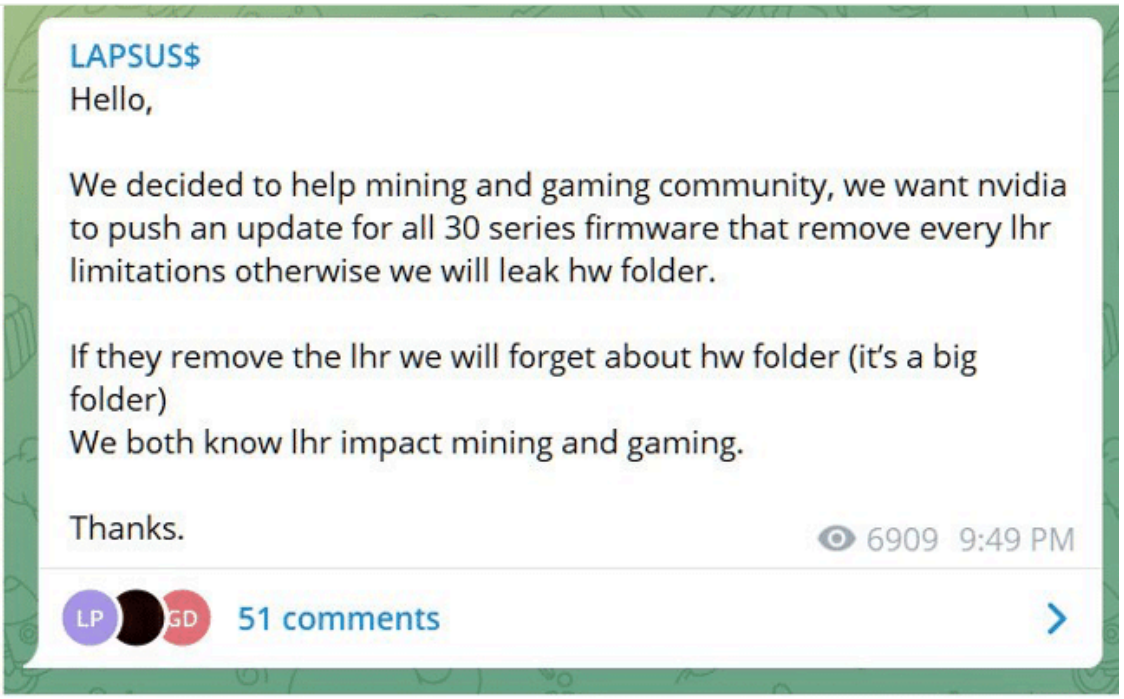
On march 1st 2022, NVIDIA confirmed they had suffered a cyber attack where **employee credentials and confidential data** had been stolen from their systems.
Shortly after this, the group posted a message on their telegram claiming responsibility and demanding a response from NVIDIA threatening to expose the data they had collected.
It appears that negotiations either did not occur or the results were not the expected by the gang, since they ended up leaking **20GB of the data** they had stolen, which contained information about the components of the **NVIDIA GPU Driver namely Falcon and LHR.**

On another message, the gang claimed that NVIDIA was able to connect to their virtual machine and **encrypted back** the information. This affirmation has not been confirmed by NVIDIA.

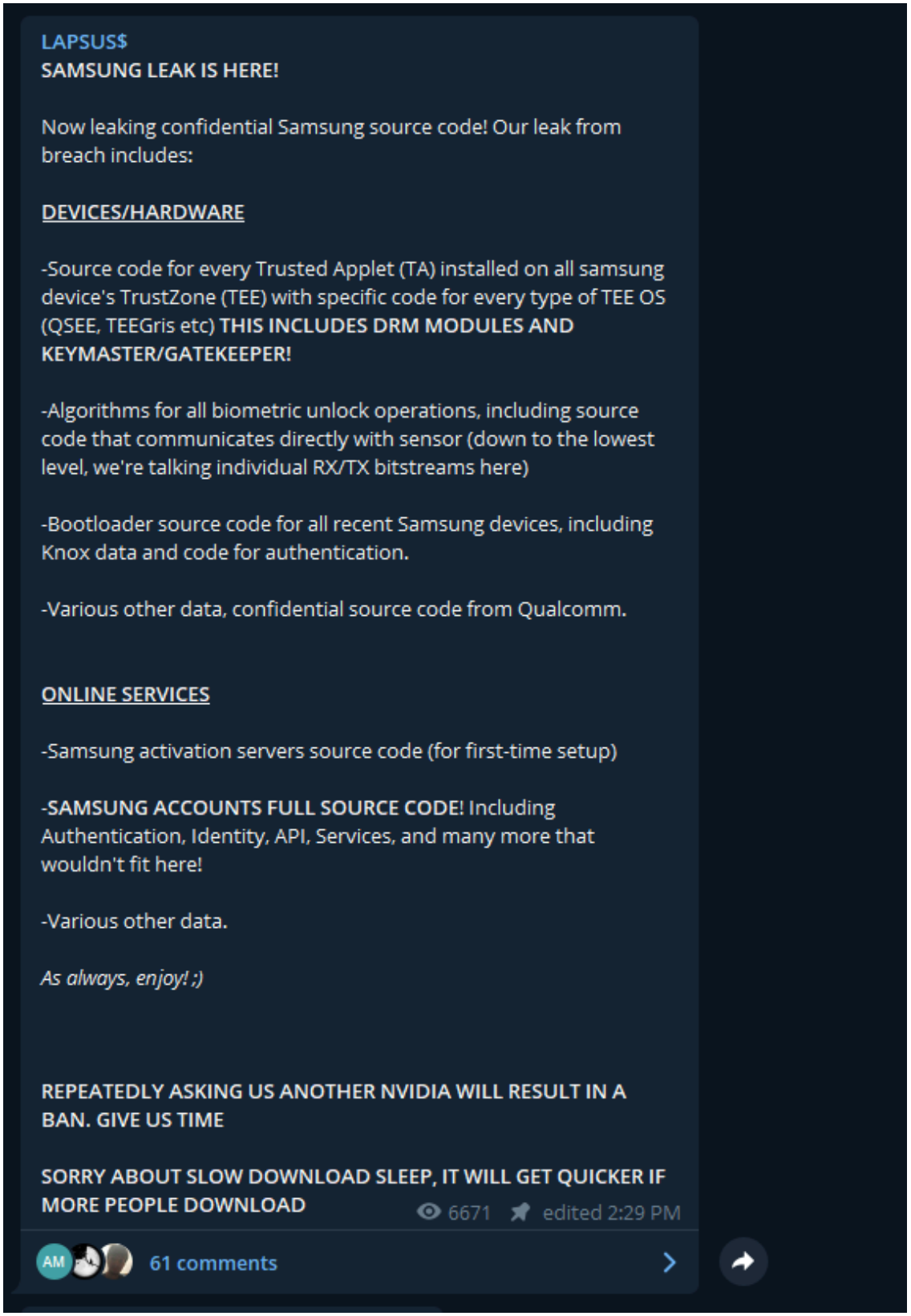


Unfortunately, the group declared that they had made copies from the information stolen and keep threatening to release all the sensitive data obtained if their demands are not met. One of these demands that were recently made public by the gang concern the **NVIDIA LHR limitations.**

The group is asking for the company to **remove all LHR limitations** which would profit **Bitcoin mining.**


LAPSUS$
Hello,
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.
6909 9:49 PM
LP
GD
51 comments

Samsung

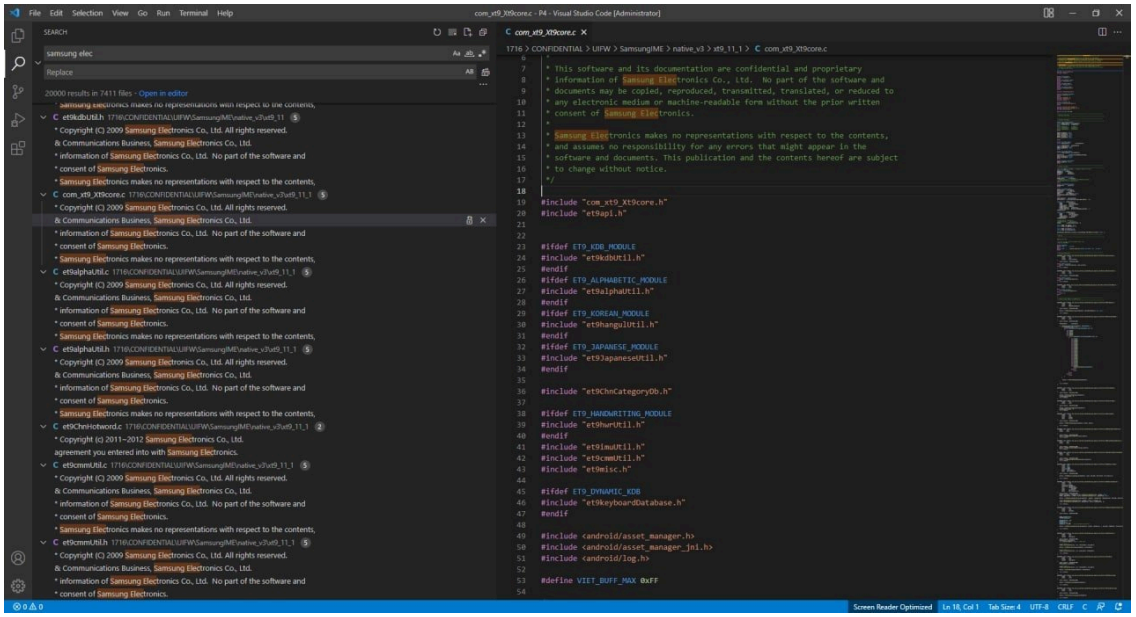


On march 4th, the group leaked **190G** of Samsung confidential data including:
– source code from every **Trusted Applet** installed on Samsung devices's TrustZone;
– algorithms for all **biometric unlock** operations;
– **Bootloader** source code for all recent Samsung devices;
– **Samsung activation servers** source code;

– **Samsung accounts** full source code;

– among other highly sensitive data, what they claim to be source code from **Qualcomm.**

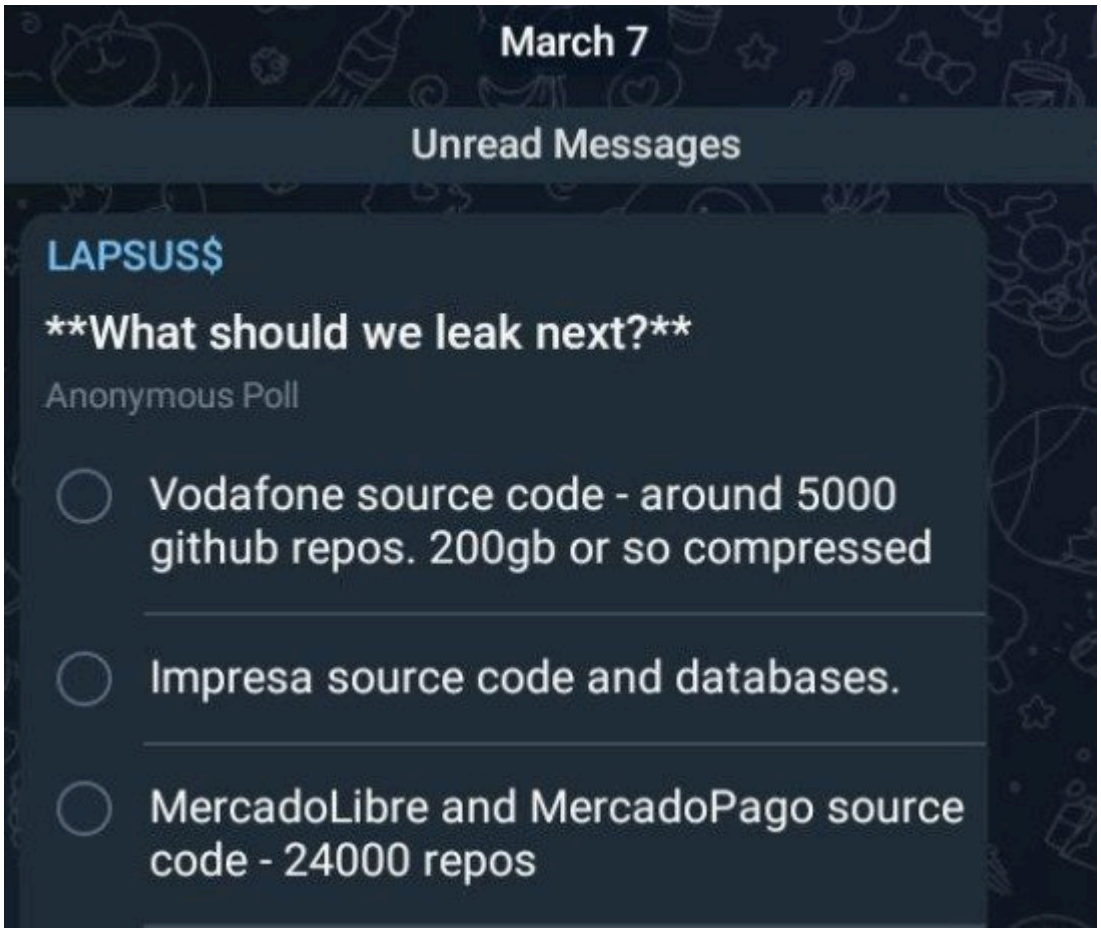
It is unclear if Samsung was contacted by the group before the leak or if some attempted extortion occurred. The company has already confirmed the breach.



Suspected Lapsus$ attacks:Vodafone Portugal, Mercado Livre and Ubisoft

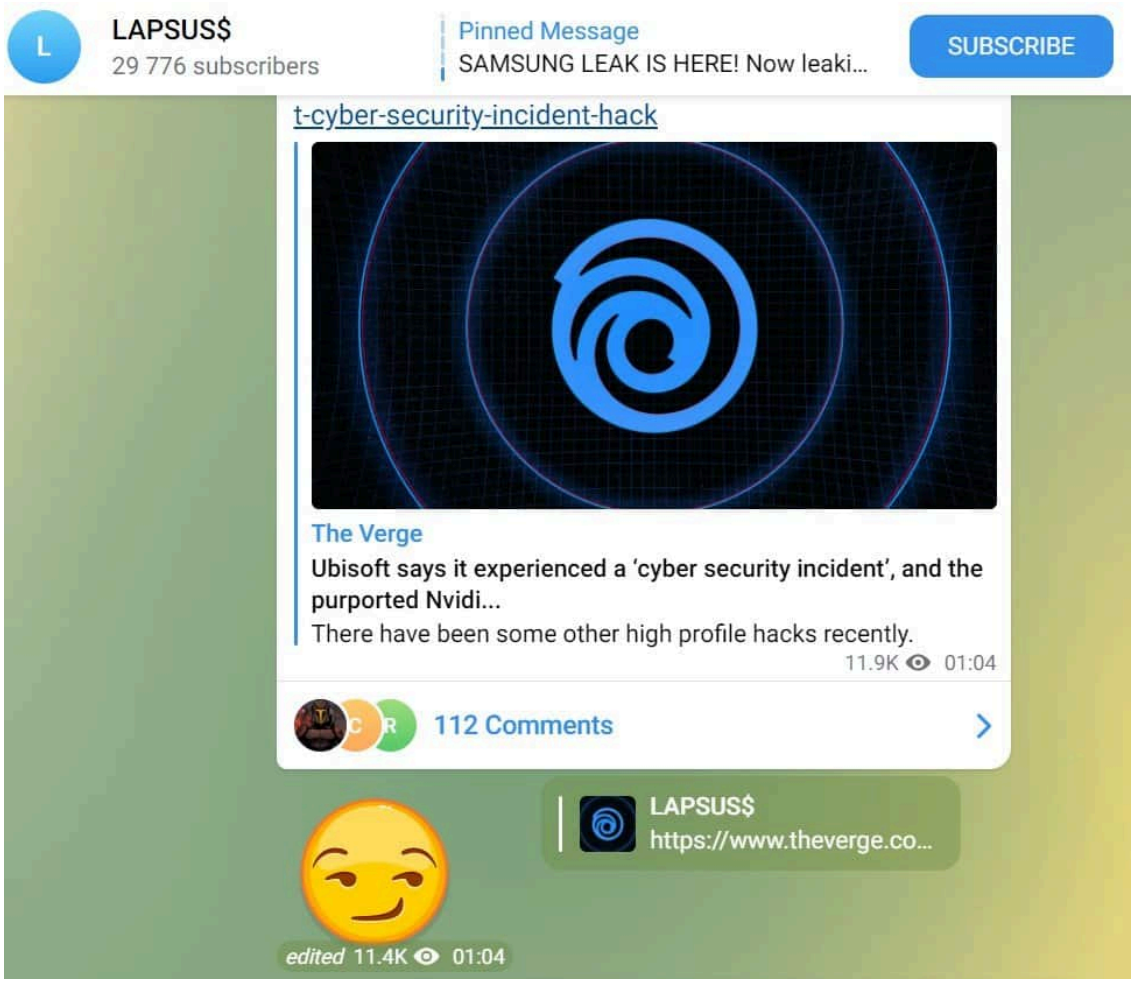
Recently the group created a **poll** on their Telegram channel where they requested their followers to choose the content of the next **data leak.**

One of the companies in this list was **Impresa**, which the group had attacked in January and requested money in order to stop the leakage of the information obtained.
At the time, there was no evidence that the requested amount was payed but this recent publication suggests it was not.

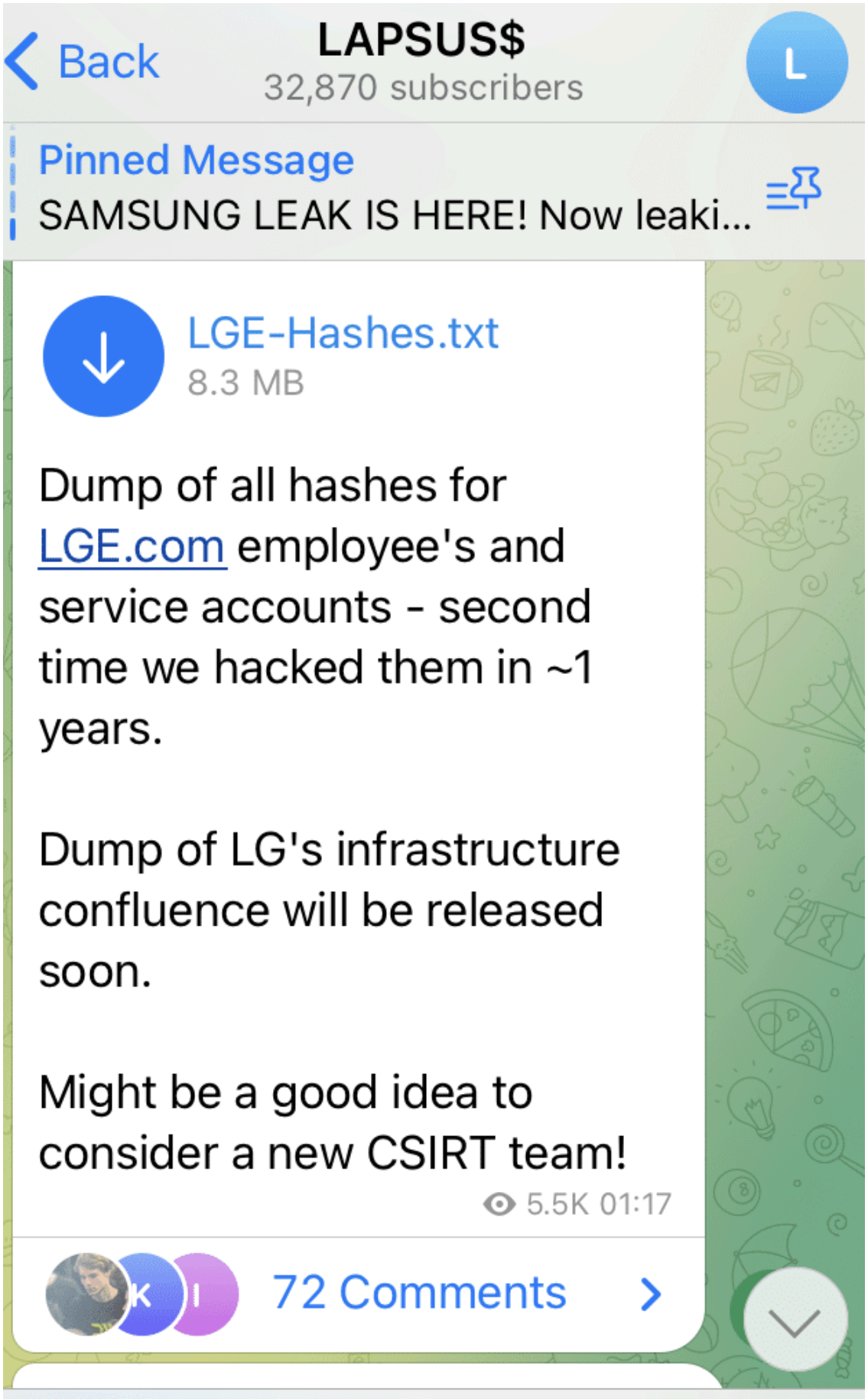


Is this the official claim that Lapsus$ did attack Vodafone Portugal?

On the other hand, the group never confirmed their responsibility for the cyber attacks of **Vodafone Portugal** and **MercadoLibre** at the time of the events.
Is this publication an admission of their actions?
Moreover, a recent publication on their Telegram suggests that they could be behind the recent cyber attack to Ubisoft.

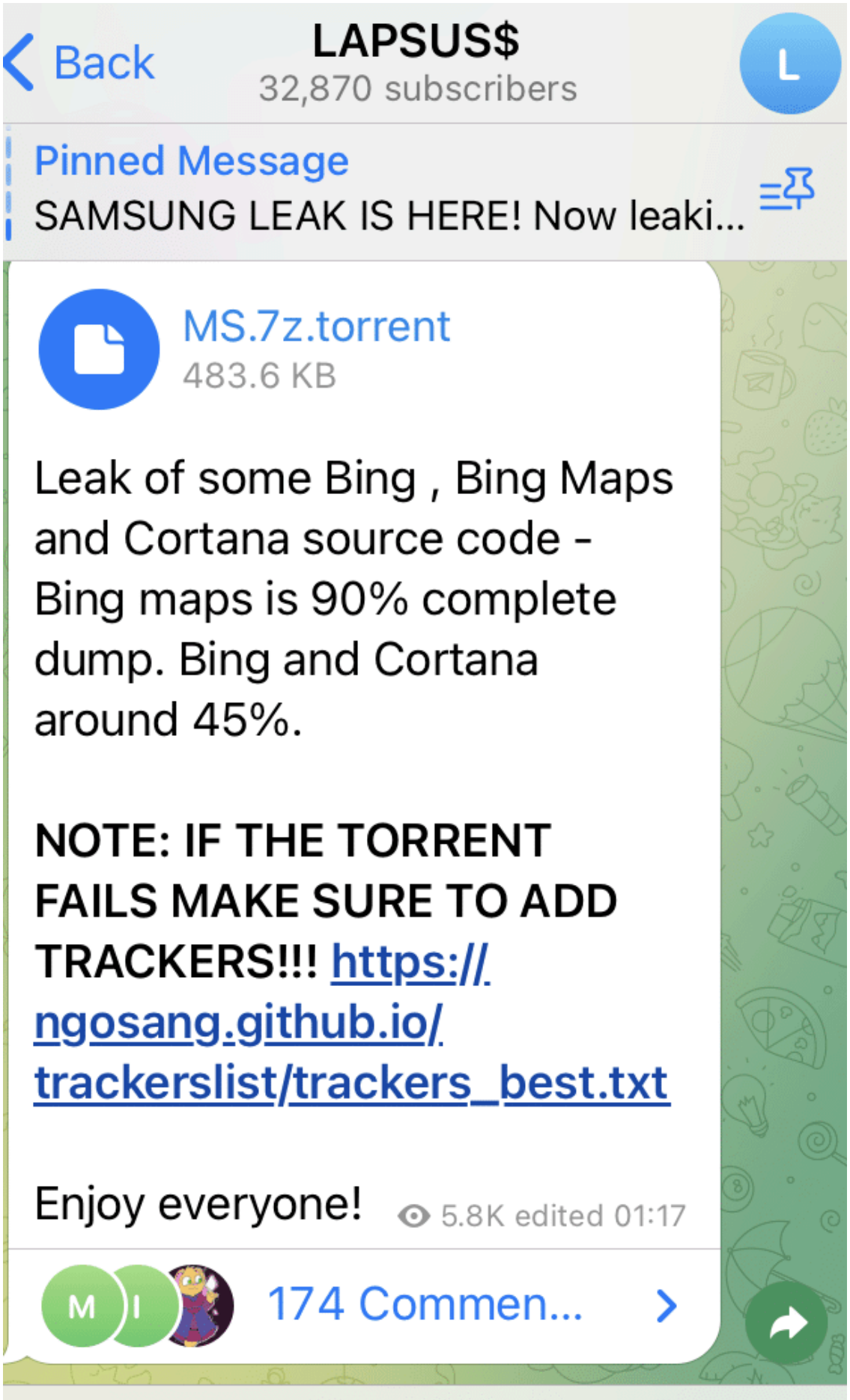

LAPSUS$
29 776 subscribers
Pinned Message
SAMSUNG LEAK IS HERE! Now leaki...
SUBSCRIBE
t-cyber-security-incident-hack
The Verge
Ubisoft says it experienced a 'cyber security incident', and the purported Nvidi...
There have been some other high profile hacks recently.
11.9K 01:04
112 Comments
LAPSUS$
https://www.theverge.co...
edited 11.4K 01:04

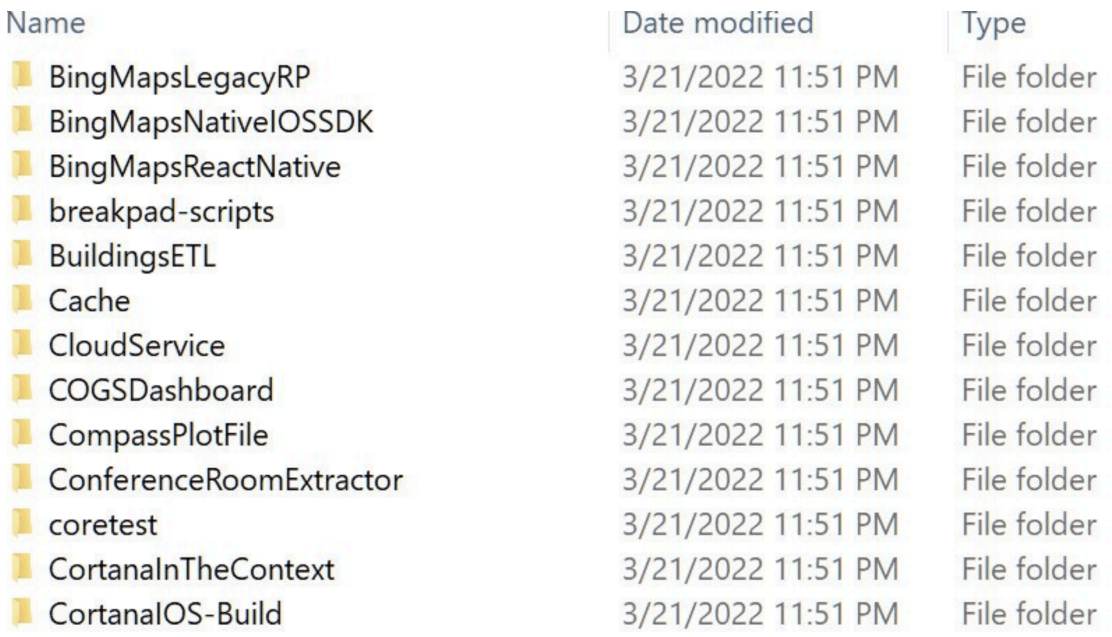
LG Data Dump


Back
LAPSUS$
32,870 subscribers
L
Pinned Message
SAMSUNG LEAK IS HERE! Now leaki...
LGE-Hashes.txt
8.3 MB
Dump of all hashes for LGE.com employee's and service accounts - second time we hacked them in ~1 years.
Dump of LG's infrastructure confluence will be released soon.
Might be a good idea to consider a new CSIRT team!
5.5K 01:17
72 Comments

In a last minute rush of data dumps Lapsus$ on 22nd March 2022 suddenly dropped a lot of information quickly beginning with this dump of LG data from an alleged breach and claiming to have infrastructure information from their confluence which will be released soon. However, this was almost lost compared to what was to come.

Bing, Bing Maps and Cortana


Back
LAPSUS$
32,870 subscribers
L
Pinned Message
SAMSUNG LEAK IS HERE! Now leaki...
MS.7z.torrent
483.6 KB
Leak of some Bing , Bing Maps and Cortana source code - Bing maps is 90% complete dump. Bing and Cortana around 45%.
NOTE: IF THE TORRENT FAILS MAKE SURE TO ADD TRACKERS!!! https://ngosang.github.io/trackerslist/trackers_best.txt
Enjoy everyone!
5.8K edited 01:17
M
I
174 Commen...

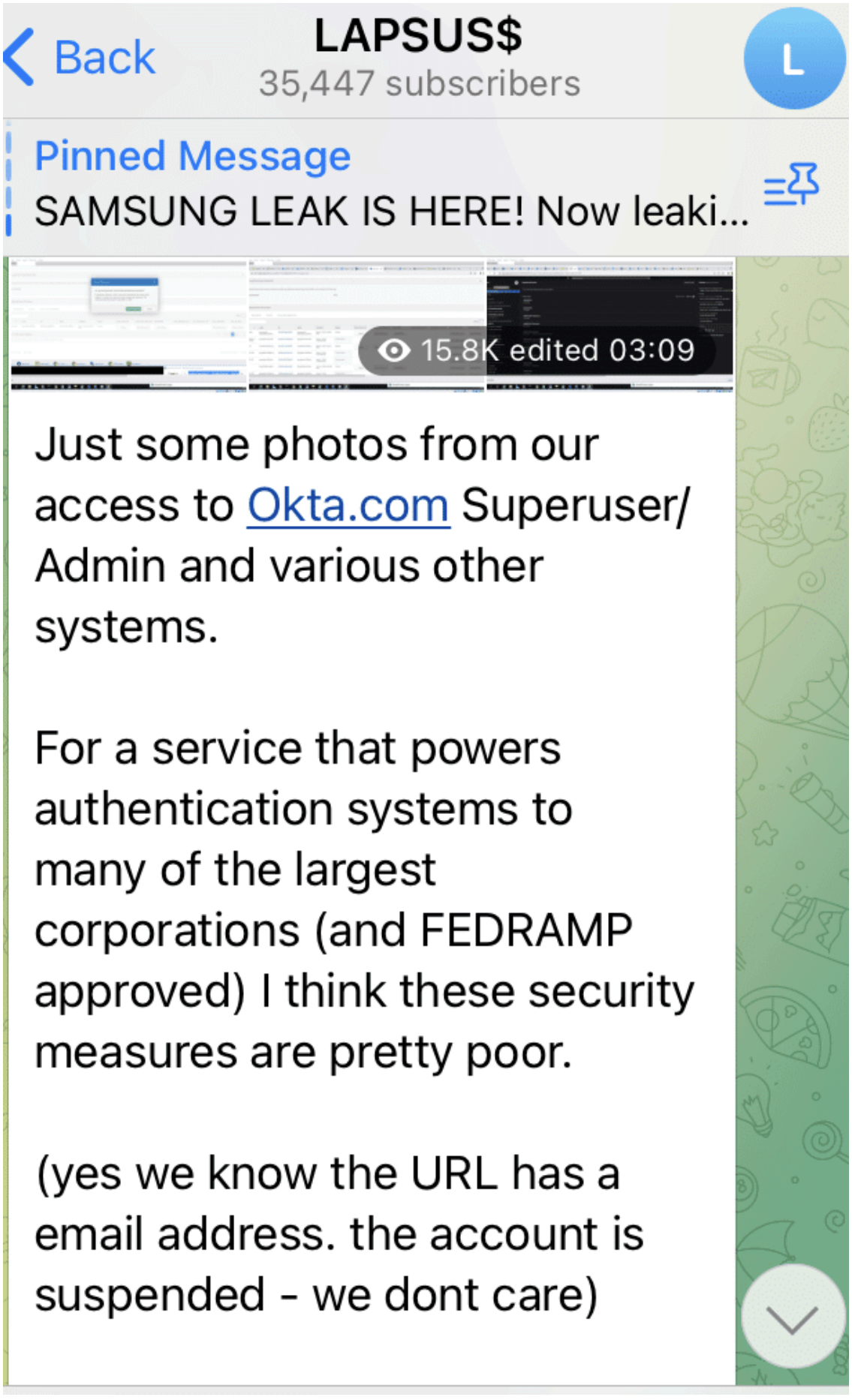


Name	Date modified	Type
BingMapsLegacyRP	3/21/2022 11:51 PM	File folder
BingMapsNativeIOSSDK	3/21/2022 11:51 PM	File folder
BingMapsReactNative	3/21/2022 11:51 PM	File folder
breakpad-scripts	3/21/2022 11:51 PM	File folder
BuildingsETL	3/21/2022 11:51 PM	File folder
Cache	3/21/2022 11:51 PM	File folder
CloudService	3/21/2022 11:51 PM	File folder
COGSDashboard	3/21/2022 11:51 PM	File folder
CompassPlotFile	3/21/2022 11:51 PM	File folder
ConferenceRoomExtractor	3/21/2022 11:51 PM	File folder
coretest	3/21/2022 11:51 PM	File folder
CortanaInTheContext	3/21/2022 11:51 PM	File folder
CortanaIOS-Build	3/21/2022 11:51 PM	File folder

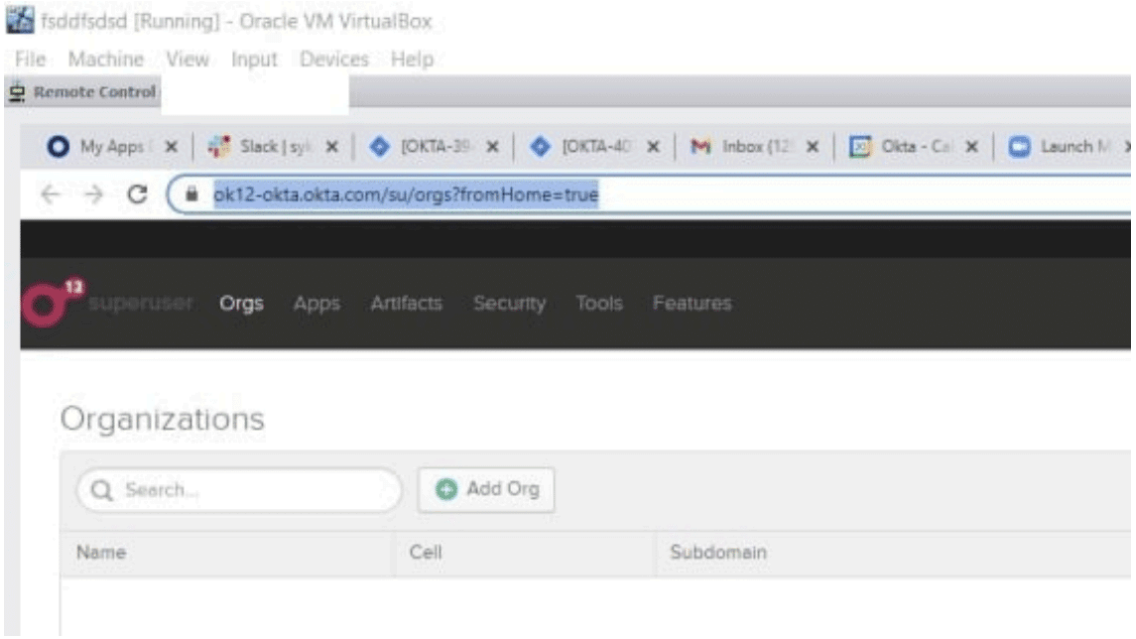
This had been hinted at in previous days but the Telegram message was deleted. So at this point everyone is wondering how this group is getting access to all of these big brands. The previous posts looking for insiders makes it look like that could be the weakness across all of these organizations. However, what happens next changes the picture.

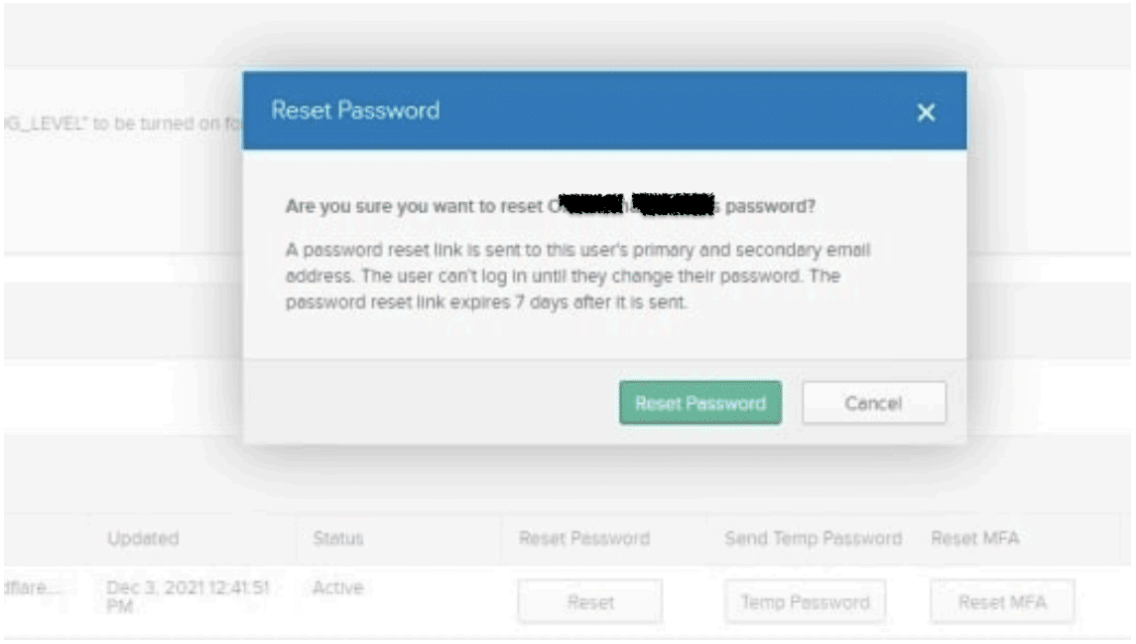
OKTA

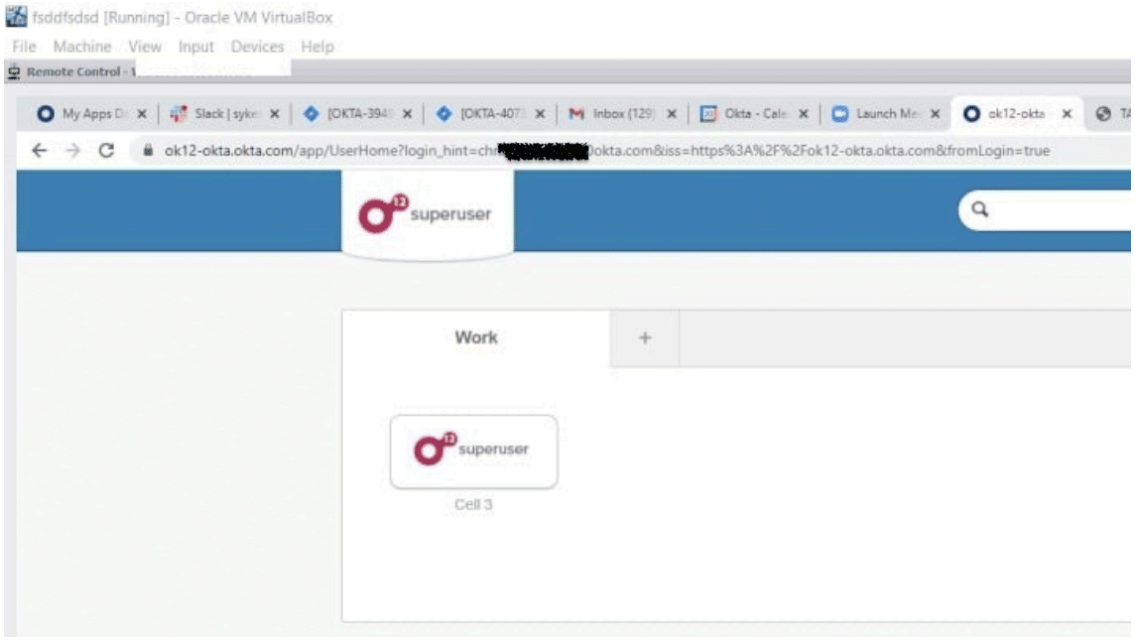
One of the most well used tools across the security industry is OKTA. It completely changes the access management capabilities of a large organization. Instead of managing each users access to each corporate application they are all done through OKTA. The user logs in to OKTA and from there they just have to click on the application tile. It significantly reduces the password management risks from each individual user as well as many other benefits. But what if OKTA becomes the entry point for the attacker. Well that appears to be what happens next.

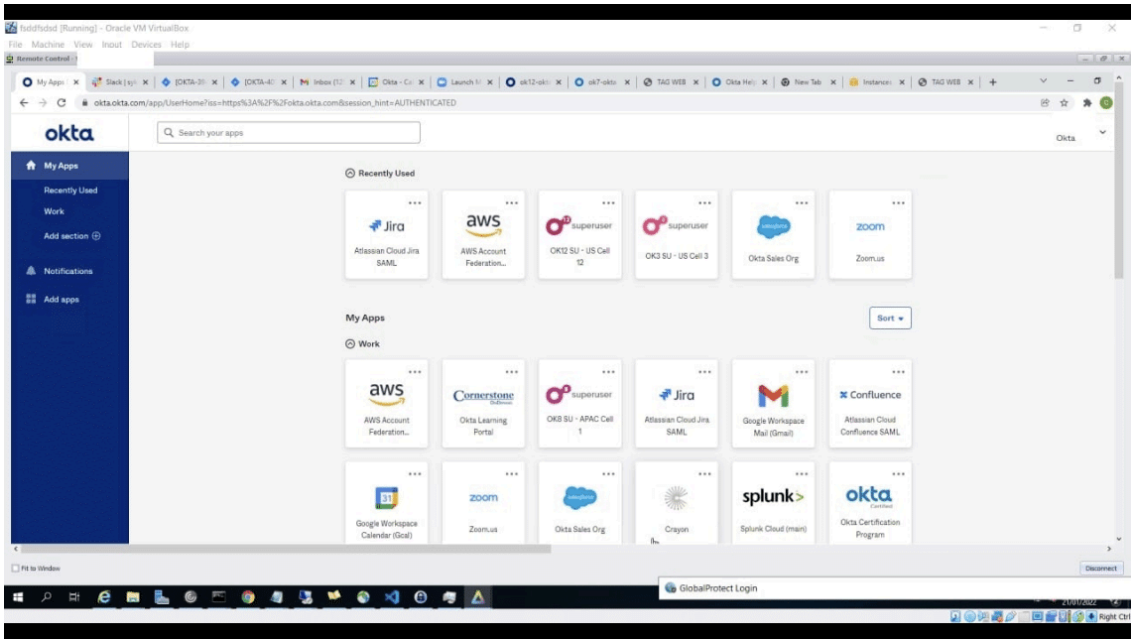

Back
LAPSUS$
35,447 subscribers
L
Pinned Message
SAMSUNG LEAK IS HERE! Now leaki...
15.8K edited 03:09
Just some photos from our access to Okta.com Superuser/ Admin and various other systems.
For a service that powers authentication systems to many of the largest corporations (and FEDRAMP approved) I think these security measures are pretty poor.
(yes we know the URL has a email address. the account is suspended - we dont care)

This is followed by many images backing up their claims including the user names of OKTA employees who appear to be Software Engineers in OKTA.

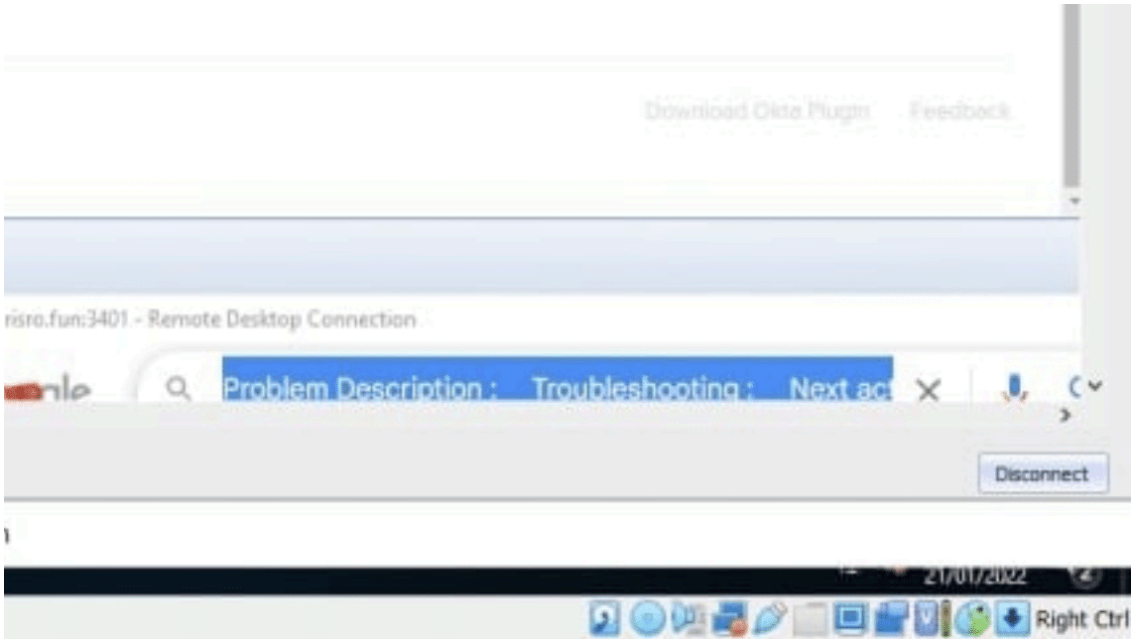




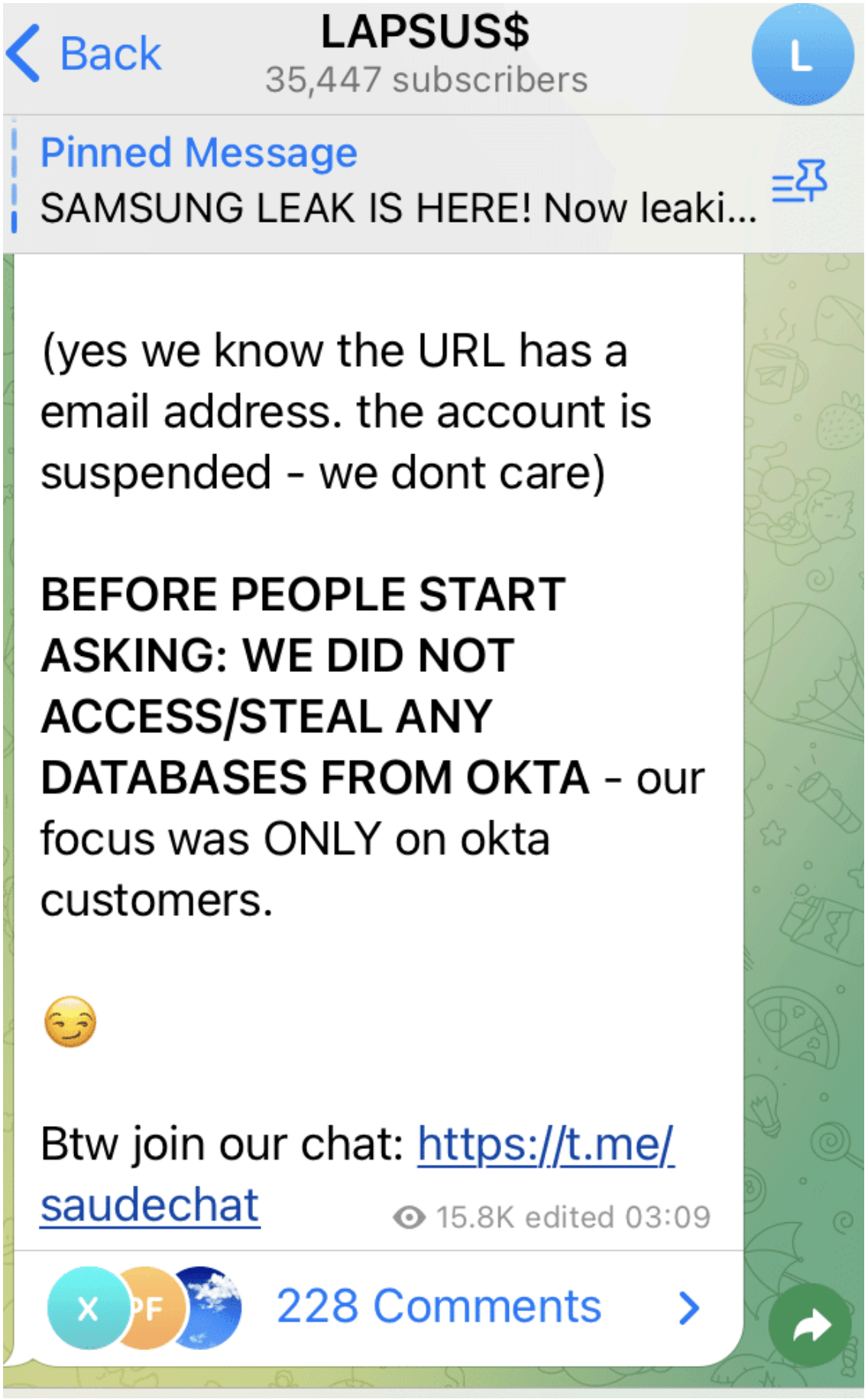




The date of these screenshots is visible as 21st January 2022

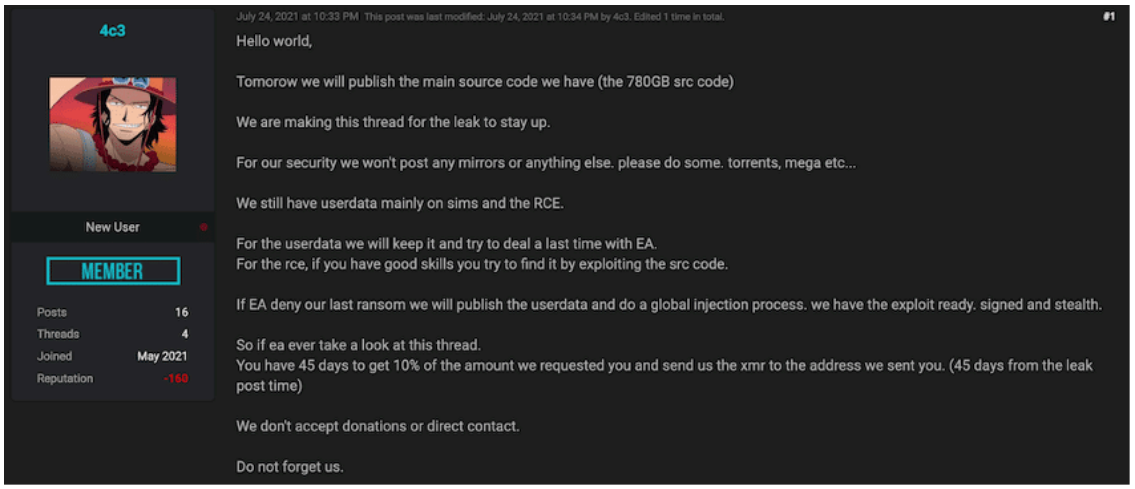


The next claim is strange, Lapsus$ then take pains to point out that they haven’t accessed any databases belonging to OKTA, they just are targeting their customers.


Back
LAPSUS$
35,447 subscribers
L
Pinned Message
SAMSUNG LEAK IS HERE! Now leaki...
(yes we know the URL has a email address. the account is suspended - we dont care)
BEFORE PEOPLE START ASKING: WE DID NOT ACCESS/STEAL ANY DATABASES FROM OKTA - our focus was ONLY on okta customers.
Btw join our chat: https://t.me/saudechat
15.8K edited 03:09
228 Comments

And that is the timeline so far. We'll continue to update if there are any more developments. This group appears to be a young and inexperienced group who are struggling to actually receive any payments for all of this extortion work. We don't know how they obtained this access to a Superuser(if there is such a thing) account in OKTA and it may never be revealed. It definitely reinforces the message that security is always about people. This group have gained a lot of notoriety and a following on social media, which may be an important factor for them. I imagine the lives of people working in the organizations that have been victims have been badly effected. Particularly for the employees mentioned in the images that were released.

Lapsus$ history:



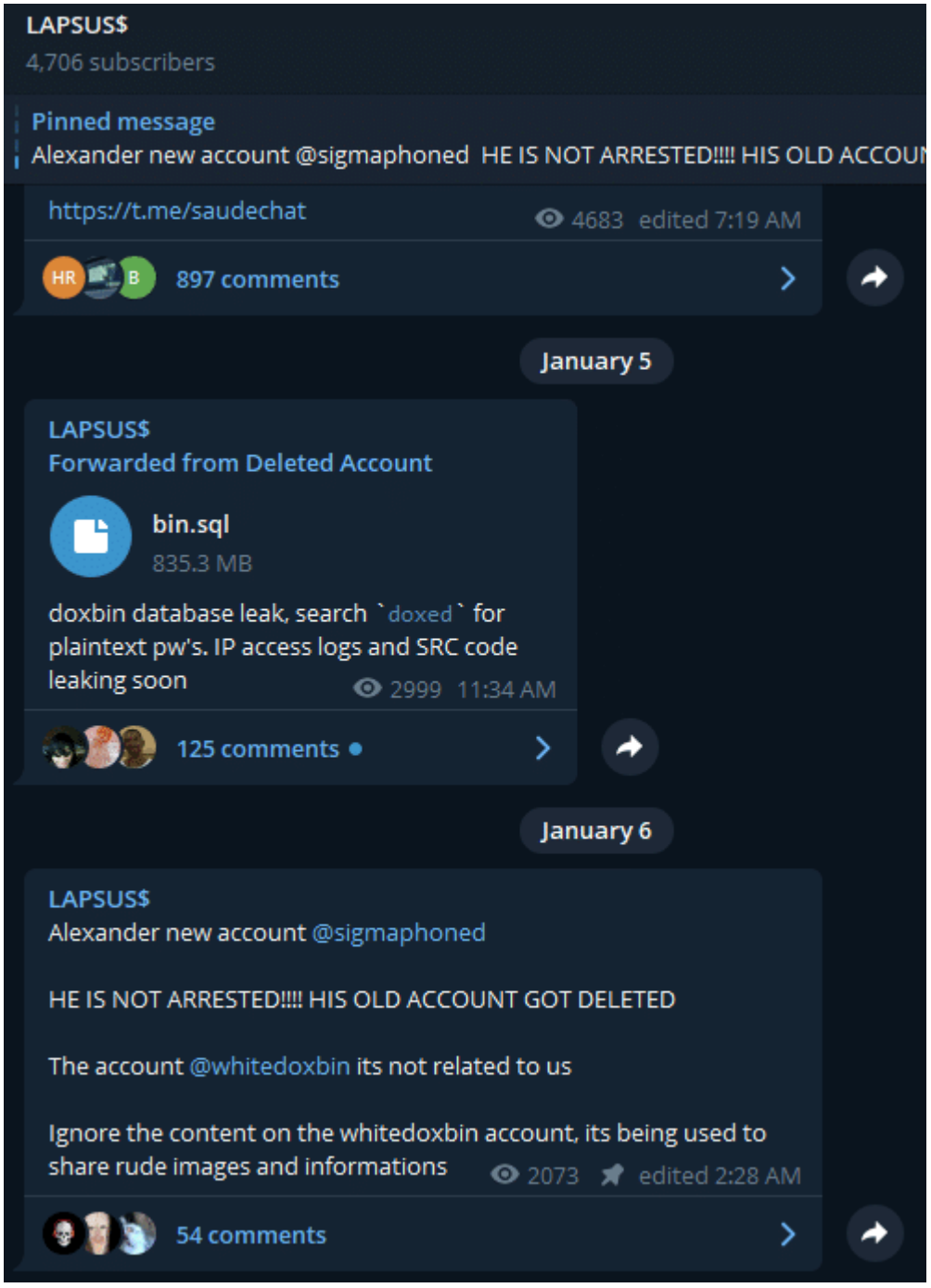
It is difficult to pinpoint a date when this threat actor began its activity.
There is a clear severity and frequency increase of their attacks since **December 2021.**
Prior to this date, there can be found a few English written posts on web forums of what appears to be their first attack as group.
In this attack which took place in **June 2021**, the group claims to have stolen the source code from **FIFA 21** from the **Electronic Arts** company.
The company acknowledged this event but failed to fulfill the requests from the group and the source code ended up being leaked on the dark web.

Query	Answer	Count	First Seen	Last Seen	Type
seed.bitcoin.wiz.biz	185.56.83.70	1	2022-03-15 05:09:26	2022-03-15 05:09:26	A
mta-sts.box.binance-help-desk.com	185.56.83.208	1	2022-02-27 05:04:11	2022-02-27 05:04:11	A
box.binance-help-desk.com	185.56.83.208	2	2022-02-27 05:04:11	2022-02-27 05:04:11	A
autodiscover.binance-help-desk.com	185.56.83.208	1	2022-02-27 05:01:55	2022-02-27 05:01:55	A
autoconfig.binance-help-desk.com	185.56.83.208	1	2022-02-27 05:01:55	2022-02-27 05:01:55	A
mta-sts.binance-help-desk.com	185.56.83.208	1	2022-02-27 05:01:55	2022-02-27 05:01:55	A
www.binance-help-desk.com	185.56.83.208	1	2022-02-27 05:01:55	2022-02-27 05:01:55	A
binance-help-desk.com	185.56.83.208	3	2022-02-26 14:39:59	2022-02-27 12:03:34	A
mx.www.doxbin.net	185.56.83.150	3	2021-12-21 12:39:38	2021-12-30 03:05:58	A
mx.doxbin.net	185.56.83.150	2	2021-12-21 10:56:20	2021-12-30 02:58:22	A
mail.doxbin.net	185.56.83.150	3	2021-12-21 08:09:59	2021-12-30 00:04:47	A
www.lapsus-group.com	185.56.83.40	13	2021-12-12 02:50:29	2022-03-10 08:08:53	A
lapsus-group.com	185.56.83.40	86	2021-12-12 02:43:39	2022-03-15 12:30:25	A
www.doxbin.net	185.56.83.150	8	2021-11-20 04:19:42	2022-01-04 04:30:17	A
doxbin.net	185.56.83.150	49	2021-11-16 13:27:46	2022-01-03 11:43:02	A
amigos.deals	185.56.83.203	1	2021-10-13 17:03:47	2021-10-13 17:03:47	A
x1.dnsseed.bluematt.me	185.56.83.70	1	2021-07-07 14:49:10	2021-07-07 14:49:10	A

Doxbin link to Lapsus$

For the next few months there were some minor attacks that could be traced back to the group but these are irrelevant in comparison to their current spike of malicious activity.
The group also changed their communication channels by retracting from web forums and twitter to exclusively use **Telegram.**
Despite that they speak both **Brazilian-Portuguese and English**, little is known about the members of the gang. Recently, a dox was leaked where it claimed that the head of this group was a 16 year old boy who lives in the United Kingdom and suffers from severe autism. He is known on the dark web as as **SigmA (most recent)**, **wh1te**, **Breachbase** or **Alexander Pavlov (Also an aliase).**

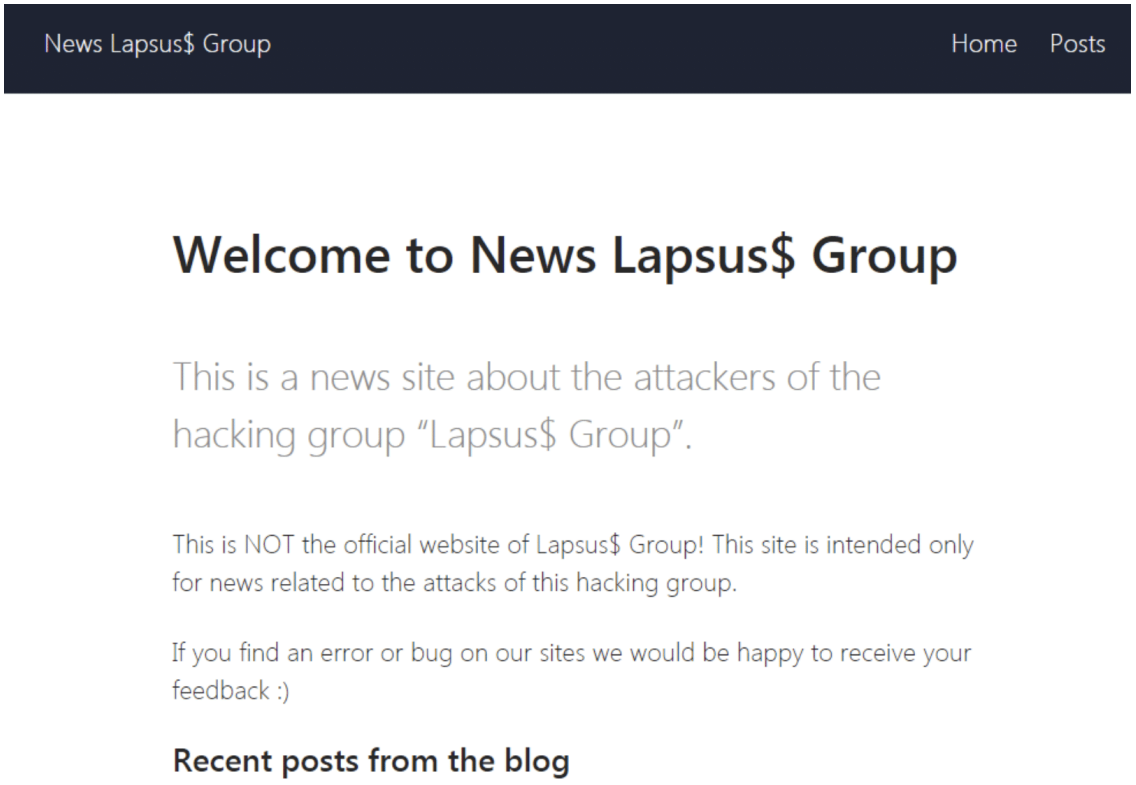
This came to light after some disputes that took place when **SigmA** bought the website `doxbin.com` and tried to sell it back to previous owner afterward. It appears that negotiations didn't go as planed and he ended up being exposed as **Lapsus$ chief** on the website that he once owned.



By using the PADNS features on the Silent Push app, we found some information that could back up this hypothesis: during the period that **SigmA** supposedly owned `doxbin.com`, this website was hosted on the same subnet as the main **Lapsus$** website at the time.
Another thing that supports this claim are the messages posted by the group on their Telegram where they deny that **SigmA** was arrested and share his new Telegram account.

SilentPush IoC research:

Using the PADNS feature on the silent push app, we found domains that fitted the `*lapsus*group*.*` pattern and the IP addresses that hosted them.
Their **registar** is unavailable and they use `*.cloudflare.com` **nameservers.**



→ IoC:

`lapsus-group[.]com`

`lapsusgroup[.]tk`

`185.56.83[.]40`

`185.56.83[.]150`

Source: https://www.silentpush.com/blog/lapsus-group-an-emerging-dark-net-threat-actor