# Rookie Of The Year - Lapsus$ Group

March 2022

Cyberint

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

2022 saw several significant and historical cases in the ransomware industry, new players were introduced and some already have caused major damage to top-of-the-line organizations around the world.

Although LAPSUS$ commenced its operations in December 2021, they have made its greatest impact in 2022, compromising major organizations such as NVIDIA, Vodafone, Samsung Microsoft, LG and Okta.

The Latin American group keeps things simple and has some unique characteristics, whether it's their leak channel, the way to choose the victims, and due to the lack of knowledge sharing from the victim's perspective - their TTPs and initial infection methods.

In addition, the big question is, is the group's operation might come to an end anytime soon and can we compare them to the big game hunters?

# INCIDENTS

While most dominant and talented groups are based in Asia and Eastern Europe, the relatively new group that is in charge of some big enterprises breaches shows that Latin America threat groups are not far behind.

# FIRST MAJOR-LEAGUE VICTIM – NVIDIA

On February 28, LAPSUS$ shared an announcement on their Telegram group that **NVIDIA was hacked**, the official announcement shared that the group gained access to NVIDIA's infrastructure for a week; initially performed privilege escalation (i.e. admin permissions) to gain access to the most sensitive data, right after that the group exfiltrated 1TB of information including schematics, drivers, firmware, SDKs, documentation and Fast Logic Controller (Falcon).

**At this point, there is no evidence of ransomware activity being deployed on NVIDIA's systems.**

After the data exfiltration, LAPSUS$ left instructions note for NVIDIA to contact them back, which they did.

## TIME TO GAIN SOME REPUTATION

A couple of hours after the first announcement, the group's reputation started to take off, NVIDIA was just the beginning.

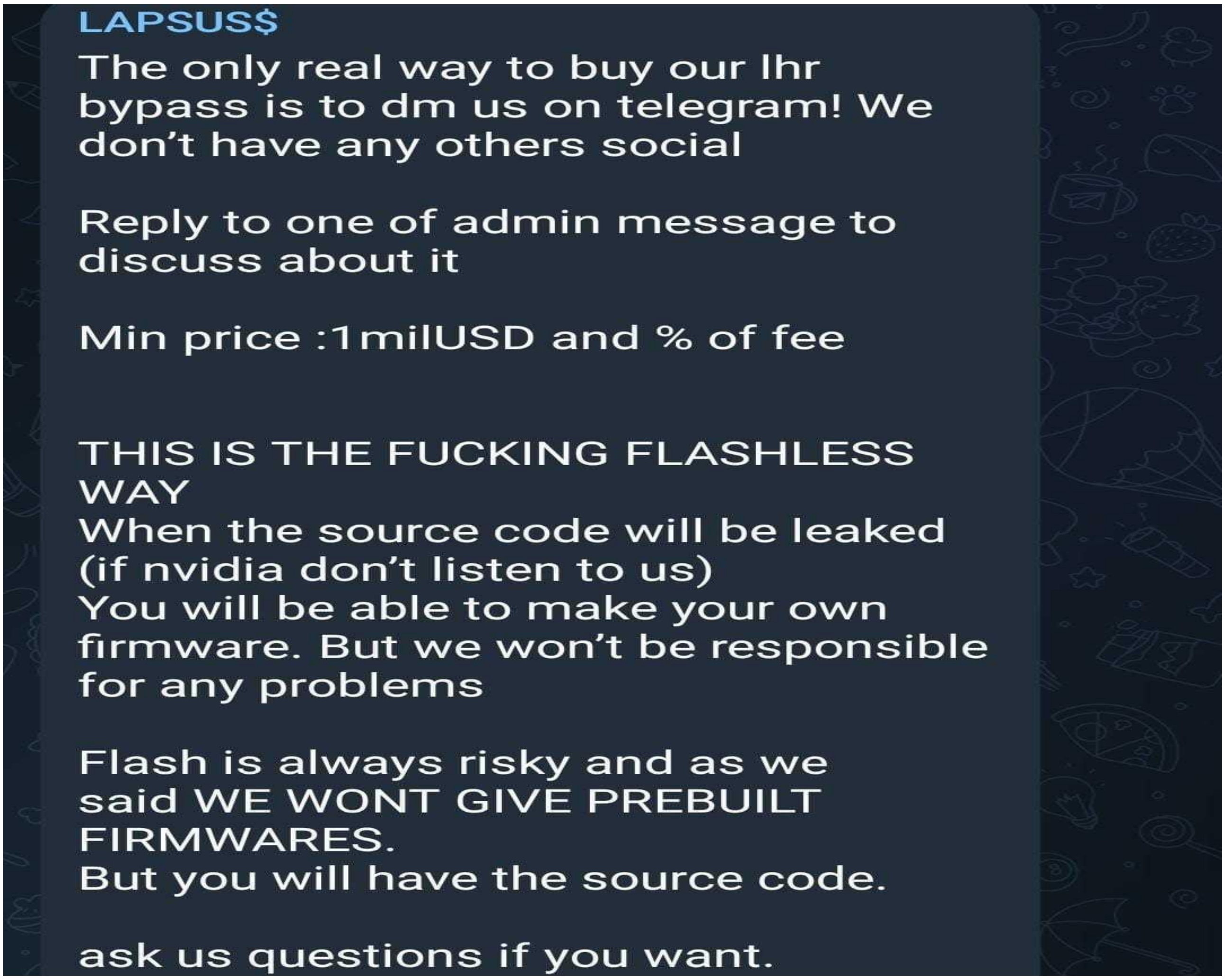
One hour after the announcement, LASPSUS$ started to release the first part (18.9GB) of the internal source code, silicon designs, driver certificates, infrastructure of Falcon and the LHR (Lite Hash Rate technology that put strict limits on the mining performance of select GPUs), which later, the group uploaded to an AWS server, that later on was taken down.

However, it did not stop there, the group's unique way of delivering the leakage and communicating with the subscribers, helped with the distribution process - subscribers uploaded the leaks to multiple sources and shared the links along the thread, the files are not going to disappear anytime soon.

Two hours after the announcement, additional demand from LAPSUS$ posted on their telegram channel.

LAPSUS$ demanded to remove all limitations on "30 series" (i.e. GeForce 30 series), otherwise- they will leak the NVIDIA Hardware repository with the excuse of helping the **gaming and mining** community.

The subscribers noticed that something is missing - the LHR bypass and they asked for clarifications from the gang, which announced that they will not share the bypass anytime soon due to the fact that it might harm the GPU. However, on March 2, LAPSUS$ offered the LHR bypass data for sale - the price? 1M$ and a fee (Figure 1). Money comes first.



LAPSUS$

The only real way to buy our lhr bypass is to dm us on telegram! We don't have any others social

Reply to one of admin message to discuss about it

Min price :1milUSD and % of fee

THIS IS THE FUCKING FLASHLESS WAY
When the source code will be leaked (if nvidia don't listen to us)
You will be able to make your own firmware. But we won't be responsible for any problems

Flash is always risky and as we said WE WONT GIVE PREBUILT FIRMWARES.
But you will have the source code.

ask us questions if you want.

Figure 1: LAPSUS$ Willing to Sell LHR Bypass

On March 1, the group announced the fourth demand, and perhaps the major one:

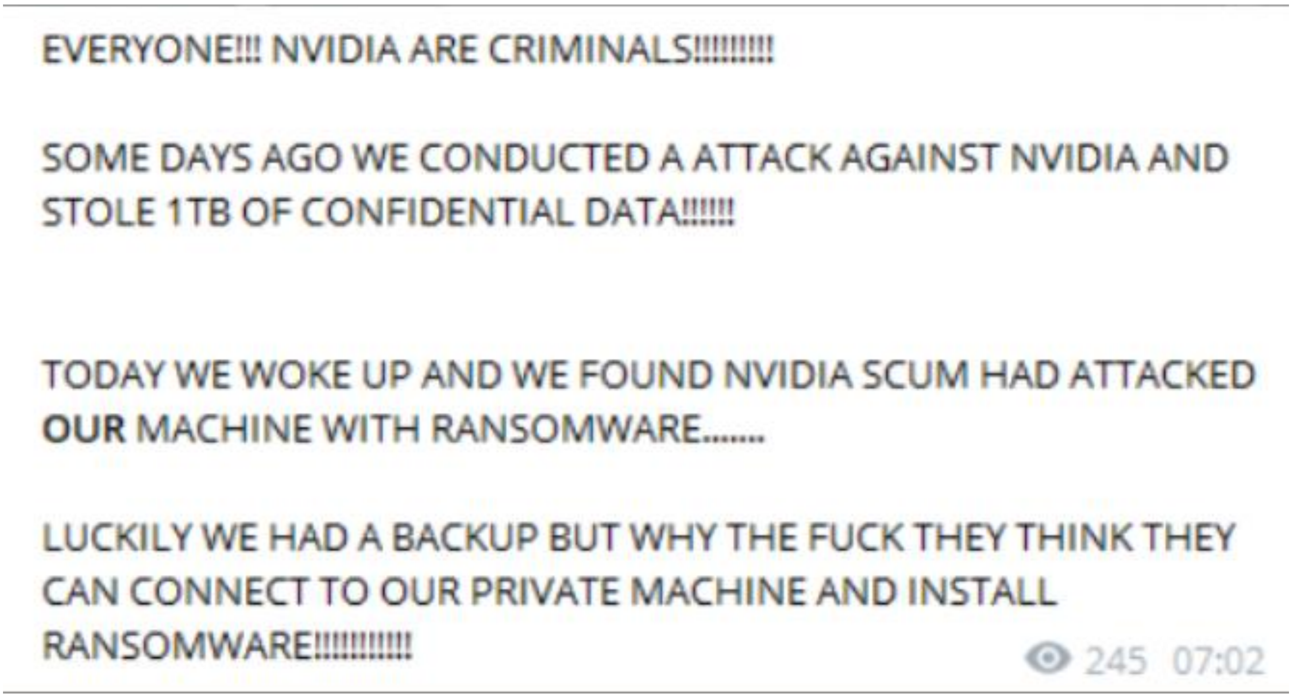
NVIDIA should commit to fully open-source their GPU Drivers for Windows, MacOS and Linux, which Nvidia did not follow and initiated a move of their own.

## NVIDIA STRIKES BACK

Aware of the breach from February 23th, Nvidia didn't confirm if it was LAPSUS$ who breached their networks and exfiltrated data but approved that the threat actor took employee credentials and some Nvidia proprietary information from their systems and begun leaking it online.

A few days later, LAPSUS$ shared an uncommon message, which they claim to be targeted back by ironically, a ransomware attack, possibly to mitigate the damage that can be done by the leaked data. Apparently, LAPSUS$ created a backup with the stolen data which disrupted Nvidia's efforts.

It's currently unclear if NVIDIA succeeded to encrypt their own data. Regardless of the result, taking this kind of significant action may introduce us to new tactics when handling ransomware or data leakage attack.



EVERYONE!!! NVIDIA ARE CRIMINALS!!!!!!!!!

SOME DAYS AGO WE CONDUCTED A ATTACK AGAINST NVIDIA AND STOLE 1TB OF CONFIDENTIAL DATA!!!!!!

TODAY WE WOKE UP AND WE FOUND NVIDIA SCUM HAD ATTACKED OUR MACHINE WITH RANSOMWARE.......

LUCKILY WE HAD A BACKUP BUT WHY THE FUCK THEY THINK THEY CAN CONNECT TO OUR PRIVATE MACHINE AND INSTALL RANSOMWARE!!!!!!!!!!!

245 07:02

Figure 2:LAPSUS$ Reaction After NVIDIAs Counter-Attack

Given that, one month passed from the first NVIDIA leak and still no sign of whether the remaining data will see daylight, It is still possible that Nvidia's counterattack was successful.

Meanwhile, other large-scale corporations' data has been exfiltrated and exposed by LAPSUS$ team.

### STOLEN NVIDIA CERTIFICATE

To date, Cyberint detected a minimum of 130 instances of malicious files signed by the leaked NVIDIA certificate, in several cases we have witnessed known stealers, such as Agent Tesla, taking advantage using this attribute.

The certificate infringing method seems to be spreading as more and more malicious executables are signed with NVIDIA's certificate.

## SAMSUNG

Shortly after leaking NVIDIA's data, another major announcement was published by the group in their Telegram channel. On March 4th, an additional international company was introduced to the victims' list — this time releasing data purportedly stolen from Samsung Electronics.

The leaked files size was 401GB and available via torrent. The leak is divided into two main sections - Samsung Online Services and Samsung Devices/Hardware data.

### DEVICES/HARDWARE AND ONLINE SERVICES

The sensitive Device/Hardware leaked data contains the source code for every trusted applet - including DRM modules and Keymaster/Gatekeeper, algorithms for all biometric unlock operation, including low-level sensor code, bootloader source code for all recent Samsung devices (including Knox), and confidential source code from Qualcomm.

In the Online Services section, LAPSUS$ shared Samsung activation server source code in addition to Samsung Accounts Full Source code - including Authentication, Identity, API, Services etc.

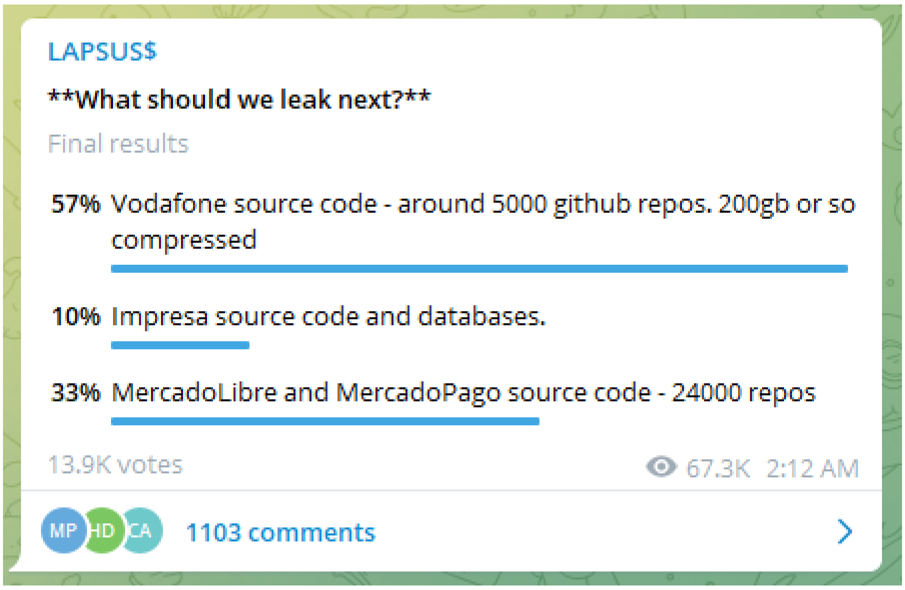
### POTENTIAL IMPACT - TRUSTZONE

Samsung TrustZone (Knox) is the secure premise of Samsung devices, if the TrustZone is compromised, a threat actor could access the TrustZone environment and into the device's sensitive data.

## VODAFONE, IMPERSA AND MERCADO LIBRE

As the Telegram channel continues to grow and add subscribers, the group seems to be in-love with the PR they are getting and concurrently continue working on the upcoming victims data.

On March 7th, LAPSUS$ posted a poll in their Telegram channel followed by the topic - "What should we leak next?" (Figure 3), more compromised victims is now in the pipeline as Vodafone, Impersa (attacked by the group on January 2022) and MercadoLibre ("unauthorized access" was identified on the company's source code potentially impacting approximately 300,000 company's users) are up next.



LAPSUS$

**What should we leak next?**

Final results

57% Vodafone source code - around 5000 github repos. 200gb or so compressed

10% Impresa source code and databases.

33% MercadoLibre and MercadoPago source code - 24000 repos

13.9K votes

67.3K 2:12 AM

1103 comments

Figure 3: LAPSUS$ Telegram Polls

The poll was available for six days and gained almost 14k votes, 57% of the votes pointed to the next victim - Vodafone.

whilst the notorious team claims to have stolen approximately 200 GB of source code files, allegedly contained in 5,000 GitHub repositories, Vodafone announced on launching an investigation.

Recap to Mid-February, Vodafone Portugal suffered a major cyberattack that caused service outages in the country, media reported the temporary disruption of 4G/5G communications and television services. While the identification of the threat actors responsible for the Vodafone attack is unclear, it is possible that due to the time frame of all three incidents, this was the initial foothold of LAPSUS$.

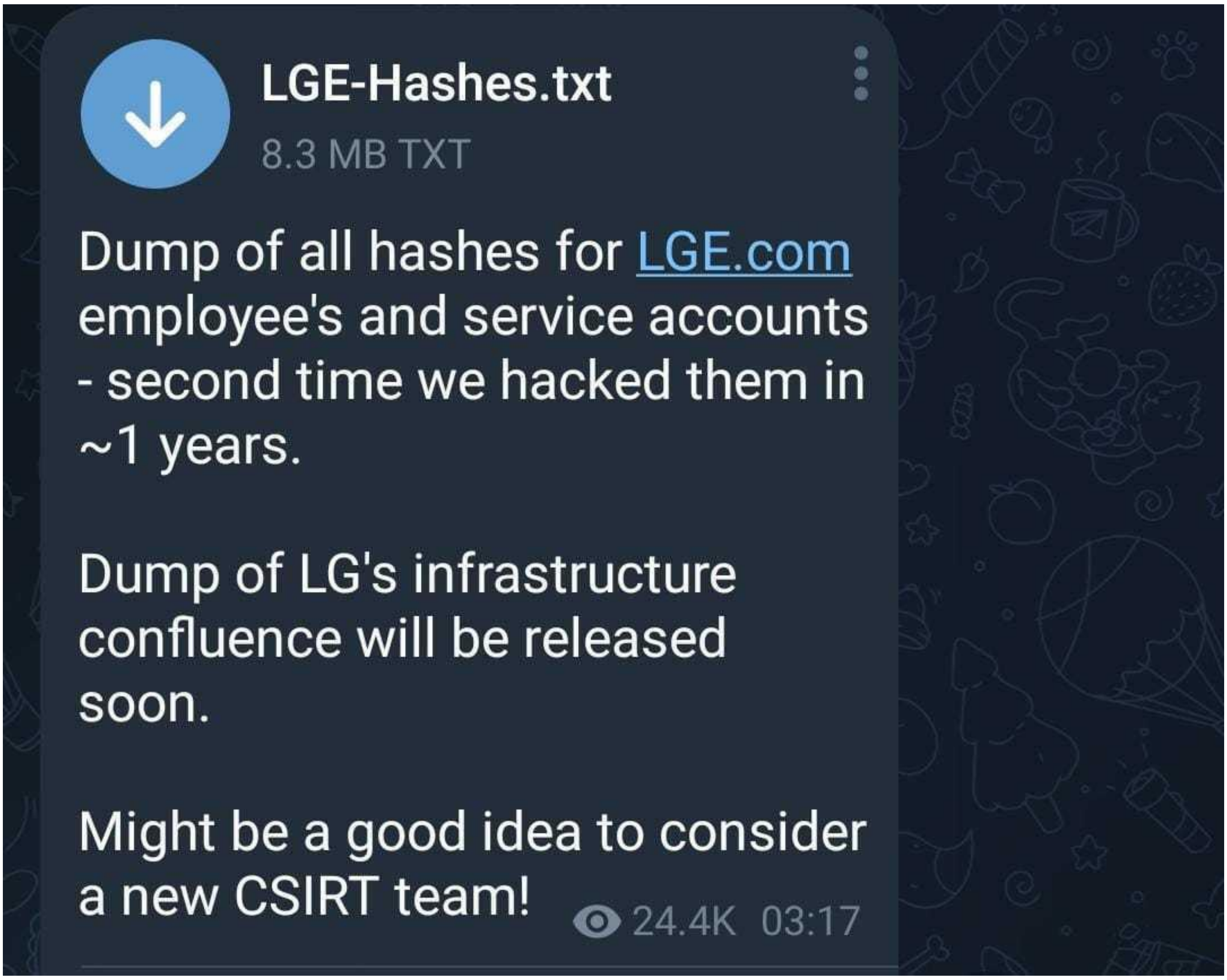
# MARCH 22ND - CREDENTIALS, AI, AND MAPS

On March 22nd, the group continued their quest to astonish the cyber security world, announcing three major corporations suffering new breaches.

## LGE

The first major leak is LGE - the group claims to have dumps of employee's and services account hashes, admittingly, for the second time this year.

The group attached a 8.3MB TXT file which includes all of the data. If that wasn't severe enough - the group shared that they got LG's infrastructure confluence and it will be released soon.



LGE-Hashes.txt

8.3 MB TXT

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.

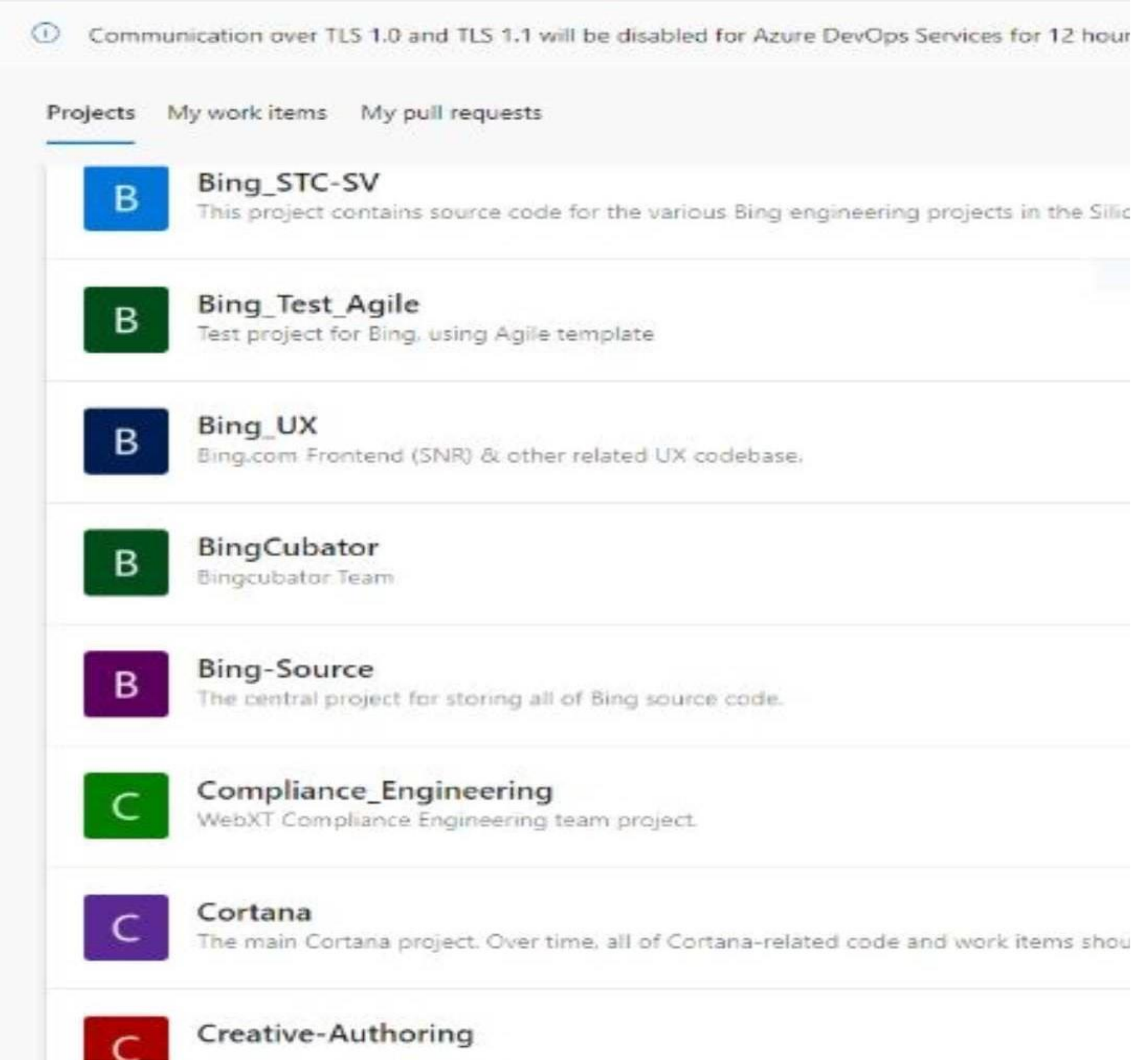
Might be a good idea to consider a new CSIRT team!

24.4K 03:17

Figure 5: LG Leaked Files on LAPSUS$ Channel

## MICROSOFT - BING THE HASH

The second major leak of the day is Microsoft's leak - it all started on March 20th as the group shared a screenshot of multiple repositories which includes Bing and Cortana Projects alongside additional internal projects (Figure 6). shortly after, the post was removed by the admins and a message *"Deleted for now will repost later"* appeared instead. PR machine works once again.



Communication over TLS 1.0 and TLS 1.1 will be disabled for Azure DevOps Services for 12 hour

B Bing_STC-SV
This project contains source code for the various Bing engineering projects in the Silic

B Bing_Test_Agile
Test project for Bing, using Agile template

B Bing_UX
Bing.com Frontend (SNR) & other related UX codebase.

B BingCubator
Bingcubator Team

B Bing-Source
The central project for storing all of Bing source code.

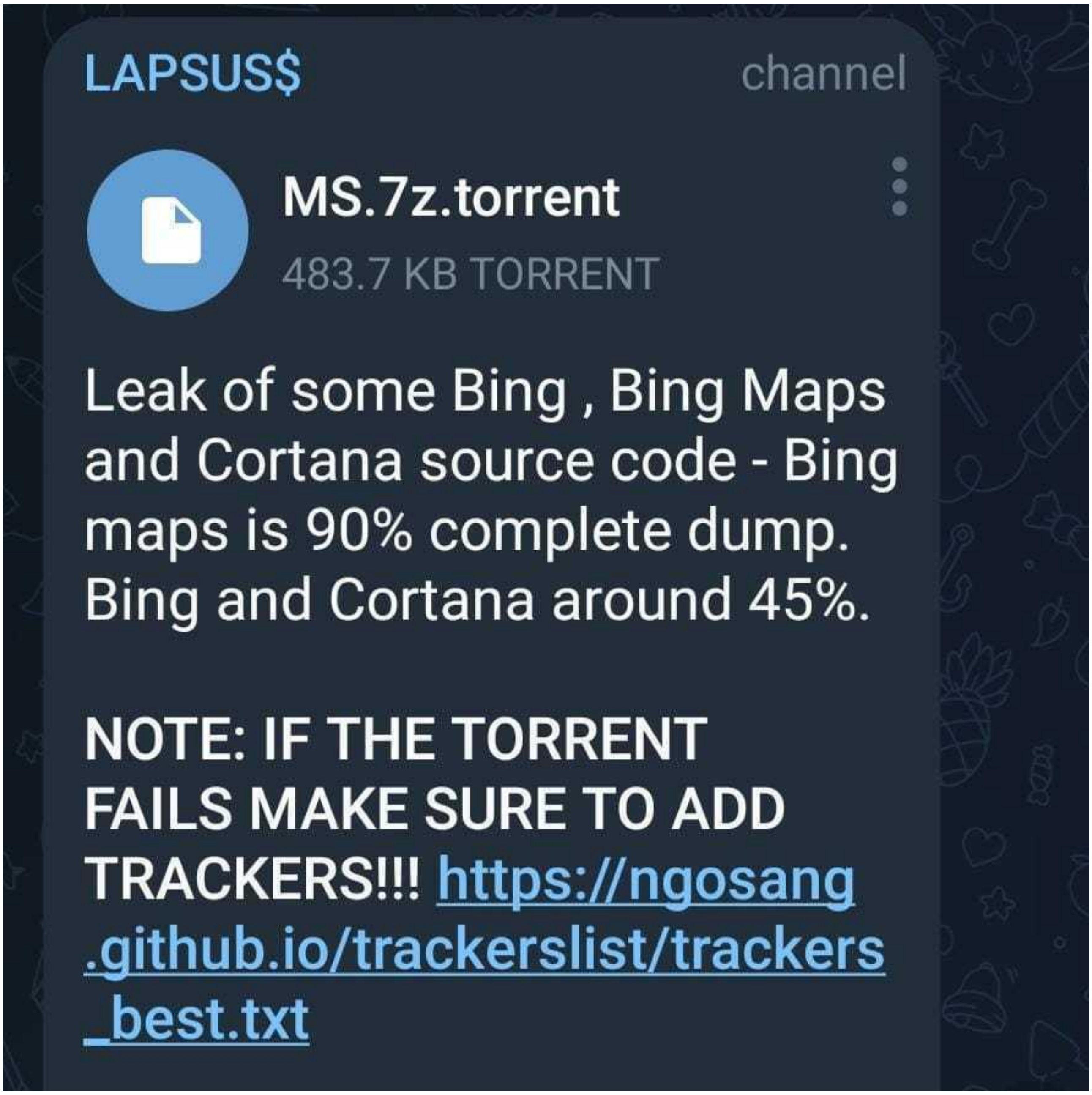
C Compliance_Engineering
WebXT Compliance Engineering team project

C Cortana
The main Cortana project. Over time, all of Cortana-related code and work items shou

C Creative-Authoring

Figure 6: Microsoft's Leak as Published on LAPSUS$ Channel

As mentioned, the group officially shared a torrent download with a description that the file contains 90% of Bing Maps and 45% of Cortana and Bing (Figure 7).



LAPSUS$ channel

MS.7z.torrent

483.7 KB TORRENT

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

Figure 7: Microsoft's Leak as Published on LAPSUS$ Channel

## OKTA - CUSTOMER FACING BREACH

A new message appeared on the group's Telegram channel, indicating, what appears to be the "biggest" most influencing breach yet. Why breach single companies, never mind their size, such as Nvidia and Samsung when we can reach them all?

While Identity and access management services and Single-Sign-On (SSO) are both highly common these days, breaching the "center" of it, could lead to more than just one single victim.

The Okta breach, indicates a new level of thinking, allowing the group to access all of Okta's customer list.

Looking at the screenshots published, we see that the dates on these go back two months (Figure 8), indicating the information and havoc LAPSUS$ could have already made.

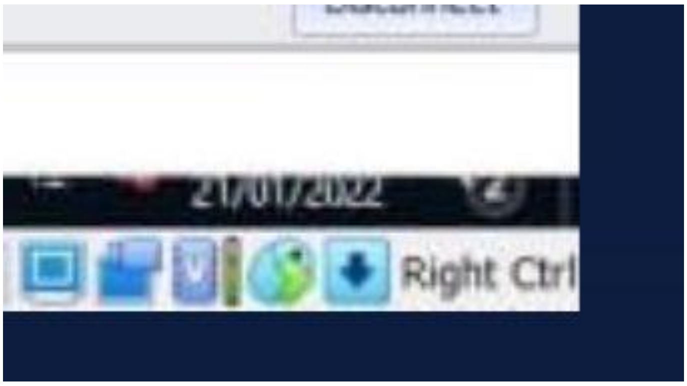
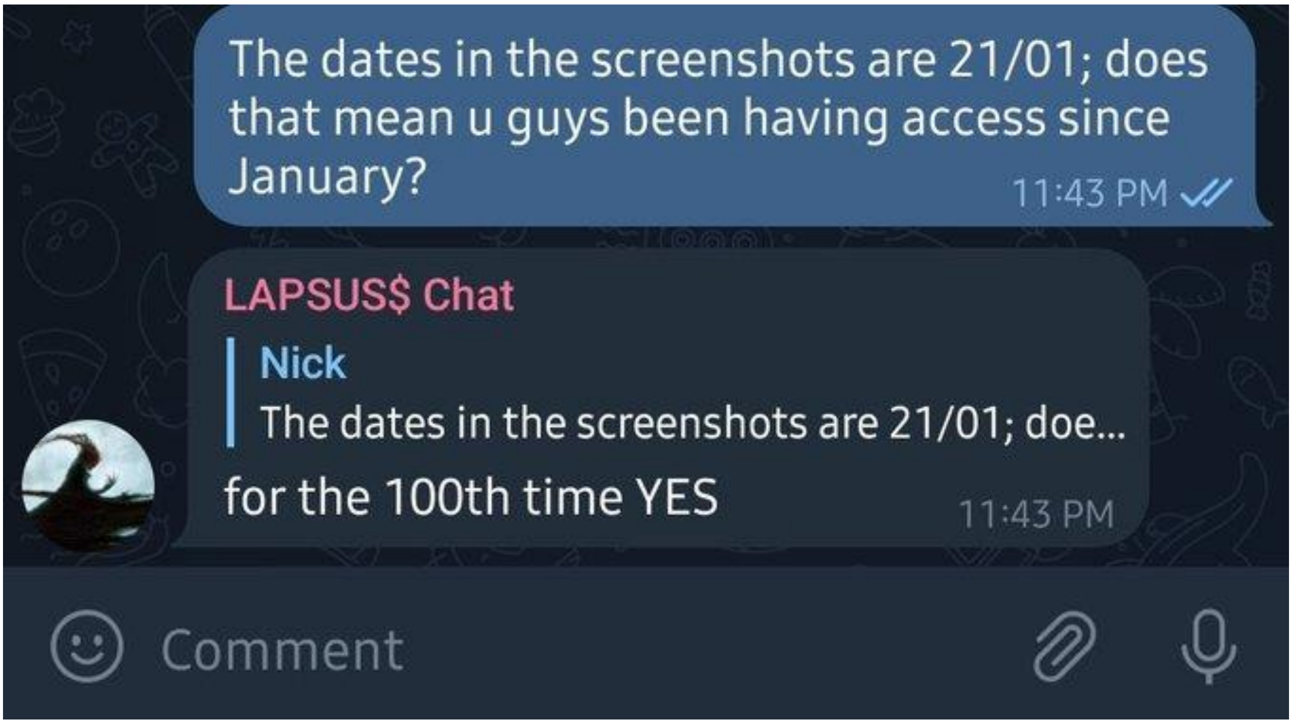


Figure 8: Okta's leaked screenshot date

LAPSUS$ openly answer and acknowledge this, as seen in figure 9.



The dates in the screenshots are 21/01; does that mean u guys been having access since January? 11:43 PM

LAPSUS$ Chat

Nick
The dates in the screenshots are 21/01; doe...

for the 100th time YES 11:43 PM

Figure 9: LAPSUS$ confirm they have access to Okta for over 2 months

The initial message claims that *"BEFORE PEOPLE START ASKING: WE DID NOT ACCESS/STEAL ANY DATABASES FROM OKTA - our focus was ONLY on okta customers."*, which shows that Okta is not the target here, only a means to an end.

This breach can also shed some light on the recent (and future) leaks LAPSUS$ publish. This might be the "way in", in most, if not all, of the recent breaches.

The immediate question here, is why burn down their bridge? Given that this is such a strategic breach, why publish the Okta breach? One assumption is that the breach got fixed, and LAPSUS$ lost their access, which led them to brag about the breach two months after the initial access.

## OKTA'S STATEMENT

On March 23rd, Okta's Chief Security Officer, David Bradbury, shared two following statements:

In the first statement, Bradbury shared an unsuccessful attempt to compromise an account of a customer support engineer working for a third-party provider.

On top of that, Bradbury sheds light on the incident, revealing that there was a five-day window between January 16th-21st, where an attacker had access to a support engineer's laptop.

Bradbury approved that the leaked screenshots provided by LAPSUS$ are related to this incident and elaborates on the limited access of support engineers who are unable to create or delete users or download customer databases. In addition, support engineers do have access to limited data - for example, Jira tickets and lists of users - that were seen in the screenshots.

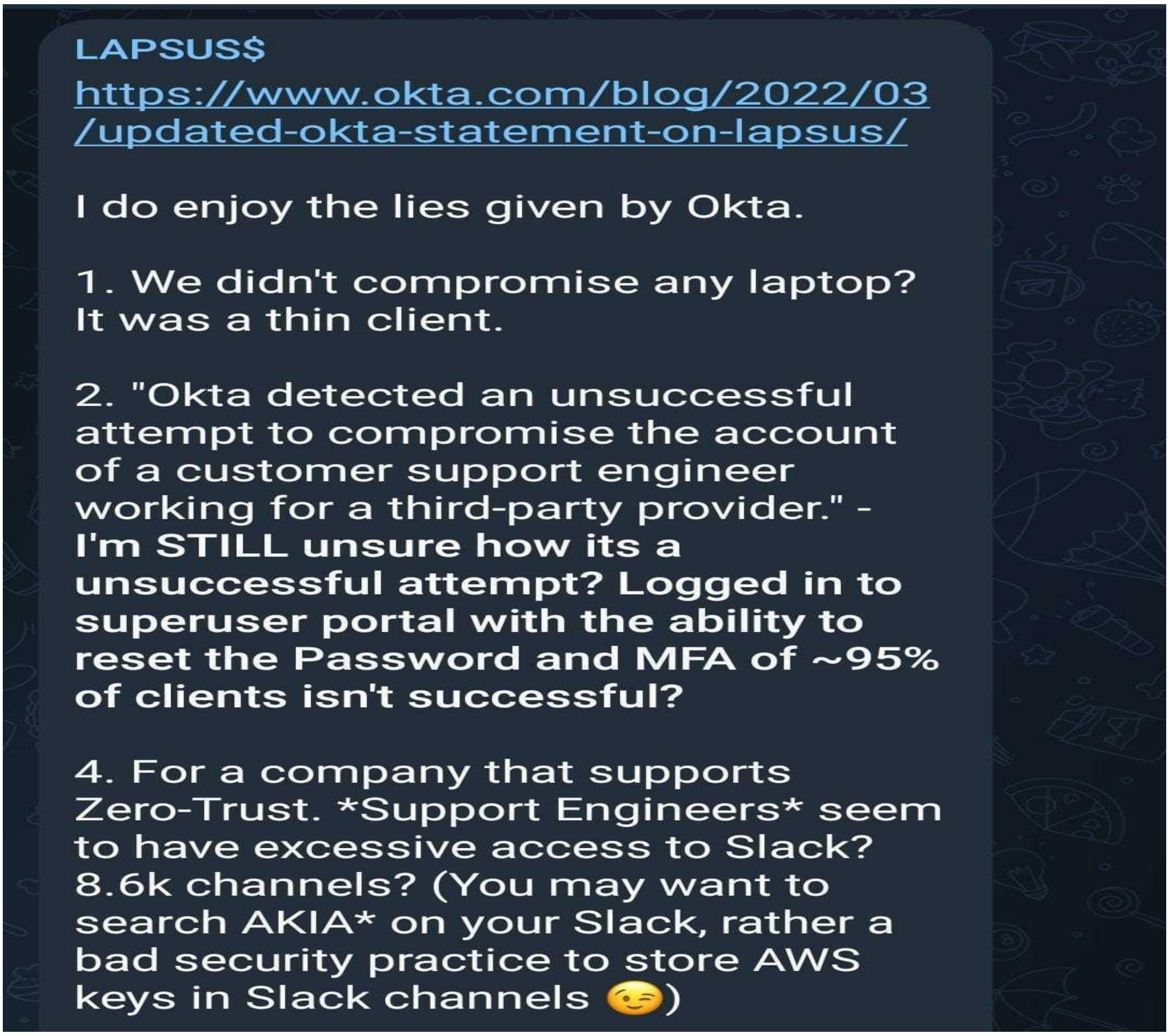
At the moment, Okta continues its investigation and contacts all the allegedly affected customers and claims that the service is fully operational while announcing that only 2.5% of Okta's customers were impacted by this breach, and already contacted by the company.

Due to the limited information provided in the screenshots, we assume that the access and valuable data LAPSUS$ obtained was limited, as the group's mentality is to shame and blame and if they were possessing any valuable information they would sell or brag about it.

## LAPSUS$ RESPONSE TO OKTA'S STATEMENT

It didn't take too long for LAPSUS$ to respond. A few hours after the first announcement, they wrote an elaborated message, opened with "I do enjoy the lies given by Okta" (Figure 10).

In their response, the group mainly tries to contradict Okta's announcement, with no great success.



LAPSUS$

https://www.okta.com/blog/2022/03/updated-okta-statement-on-lapsus/

I do enjoy the lies given by Okta.

1. We didn't compromise any laptop? It was a thin client.

2. "Okta detected an unsuccessful attempt to compromise the account of a customer support engineer working for a third-party provider." - I'm STILL unsure how its a unsuccessful attempt? Logged in to superuser portal with the ability to reset the Password and MFA of ~95% of clients isn't successful?

4. For a company that supports Zero-Trust. *Support Engineers* seem to have excessive access to Slack? 8.6k channels? (You may want to search AKIA* on your Slack, rather a bad security practice to store AWS keys in Slack channels 😉)

Figure 10: LAPSUS$ reply on Okta's announcement

Regarding the support engineers' limited access, the group commented that those limited access engineers had excessive access to Slack (about 8.6k channels) and those channels contained plaintext AWS keys. As AWS keys value depends on the permissions they grant, and since LAPSUS$ describes these as "excessive", we can only guess the magnitude of these. Obviously, LAPSUS$ gang members should poses AWS knowledge to take advantage of these. Since Okta's statement does not mention any AWS keys rotation, this makes us wonder if we will continue hearing about Okta in the next upcoming weeks.

It is quite notable that LAPSUS$ didn't achieve their main goal via Oktas' breach, through defensive-posture shaming posts without any clear evidence or goal. Also, the way they embedded internal insights into Okta's team, perhaps reflects the potential impact of the breach.

Once again, the need to brag and to answer for every announcement Okta's have made indicates of the immaturity of the leaders and their will to "show off" and to have legitimization in the cyber security community.

## LEVEL OF SOPHISTICATION

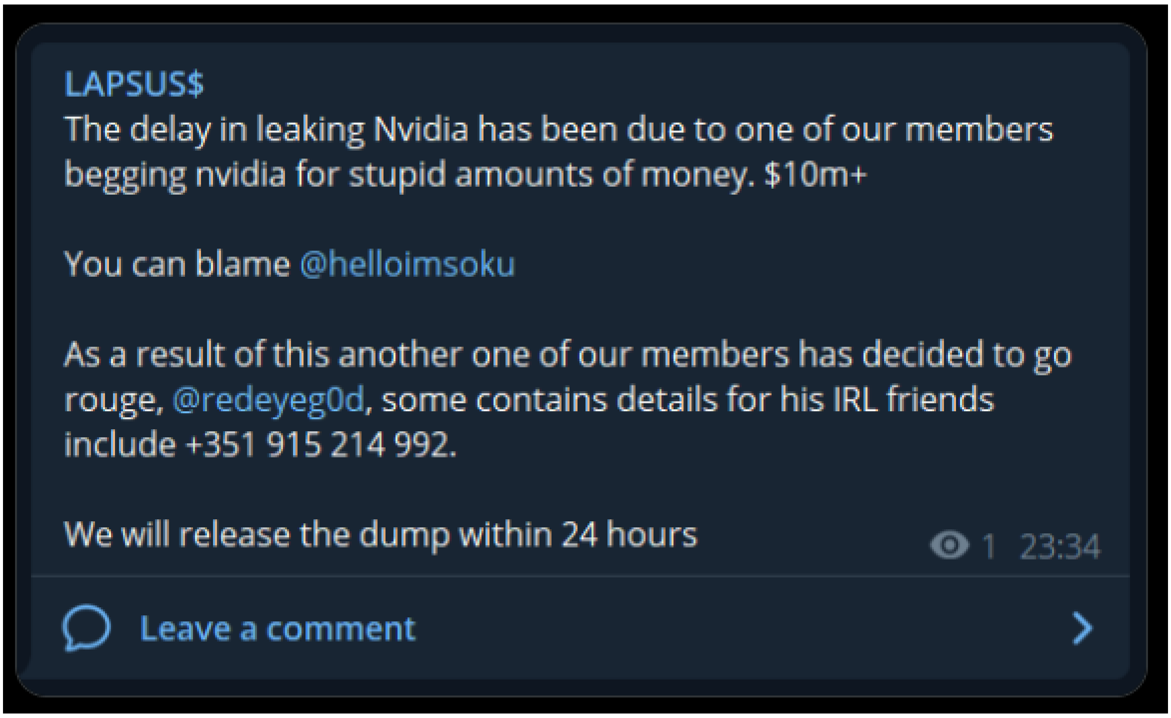
When it comes to the technical sophistication and professional maturity of the group, it seems that the group has gained a massive amount of followers due to their success, but they haven't worked to expand the group itself.

Most of their campaigns are based on insider threats and no evidence of recruiting vulnerability researchers, reverses, and top-of-the-line developers were found. once they gain an employee creds, they still need some level of understanding of how to move and what to look for once they are inside the network.

The only adjustment the group made as a result of the growth of followers, was the migration of announcements to English from Portuguese.

LAPSUS$ keeps its methods simple at the moment and most of their work is done manually, including analyzing their findings and publishing the leaked data. We have witnessed several cases in which the group delayed publications of leaked data and chose almost amateur working methods.

The group's lack of sophistication and maturity is also seen in their temper the take-backs of their announcements, changing their demands and blaming each other in their Telegram channel for mistakes (Figure 11).



LAPSUS$
The delay in leaking Nvidia has been due to one of our members begging nvidia for stupid amounts of money. $10m+

You can blame @helloimsoku

As a result of this another one of our members has decided to go rouge, @redeyeg0d, some contains details for his IRL friends include +351 915 214 992.

We will release the dump within 24 hours

Figure 11: LAPSUS$ admin blame members for failure in Nvidia negotiation and revealed rogue member's information

## LEAK CHANNELS

As most ransomware groups are using Onion-based blogs to upload the extorted data, LAPSUS$ mainly uses Torrent and AWS services to share the data and users re-upload the data into other storage services creating a distribution of the data on multiple sources.

To date, the dedicated LAPSUS$ Telegram group contains 43K subscribers.

While most groups communicate with their communities often in a one-sided relationship in which the group decides who is the next victim, LAPSUS$ chose a way for their audience to participate in the group's strategy and in the decision making.

The first way is another Telegram channel in which their followers can talk to the group's members and give them ideas, tips and talk to each other. The second, and more interesting way, is the group's polls. The group chooses three compromised victims and give the followers the ability to choose which one will be leaked.

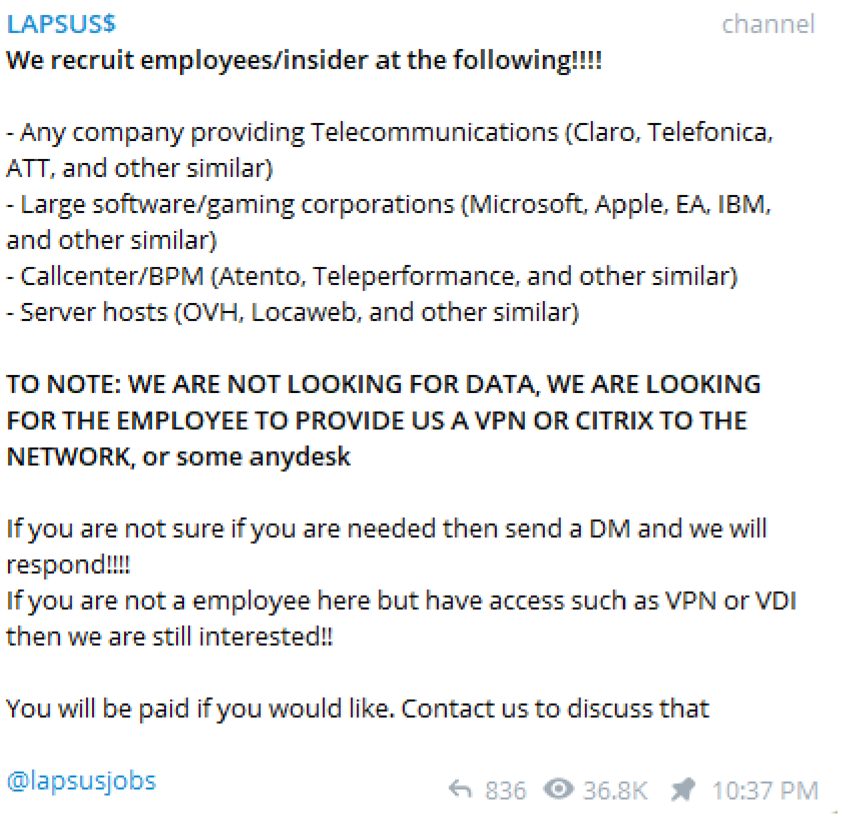
# RECRUITMENT OF INSIDE THREAT

Currently, LAPSUS$ is not known for having very sophisticated techniques they implement when it comes to initial infection and gaining a foothold within the victim's network. As the group is not well funded nor fully organized at the moment and lacks talented people that have the ability to exploit vulnerabilities and research for zero-days, they address the easiest way to gain a foothold, which is the insider threat.

The most simple yet lethal technique involves bribing and recruiting employees of potential victims that will intentionally compromise their credentials and help LAPSUS$ gain a foothold.

Although this technique is not new or unique to LAPSUS$, as Lockbit2.0 is also known for doing so, it is very efficient as we saw in their last campaigns.

LAPSUS$ has published a recruitment message in their Telegram channel calling all employees that can provide them remote access to join the group (Figure 12).



LAPSUS$ channel

**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 LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk**

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

@lapsusjobs

Figure 12: LAPSUS$ recruitment announcement on Telegram

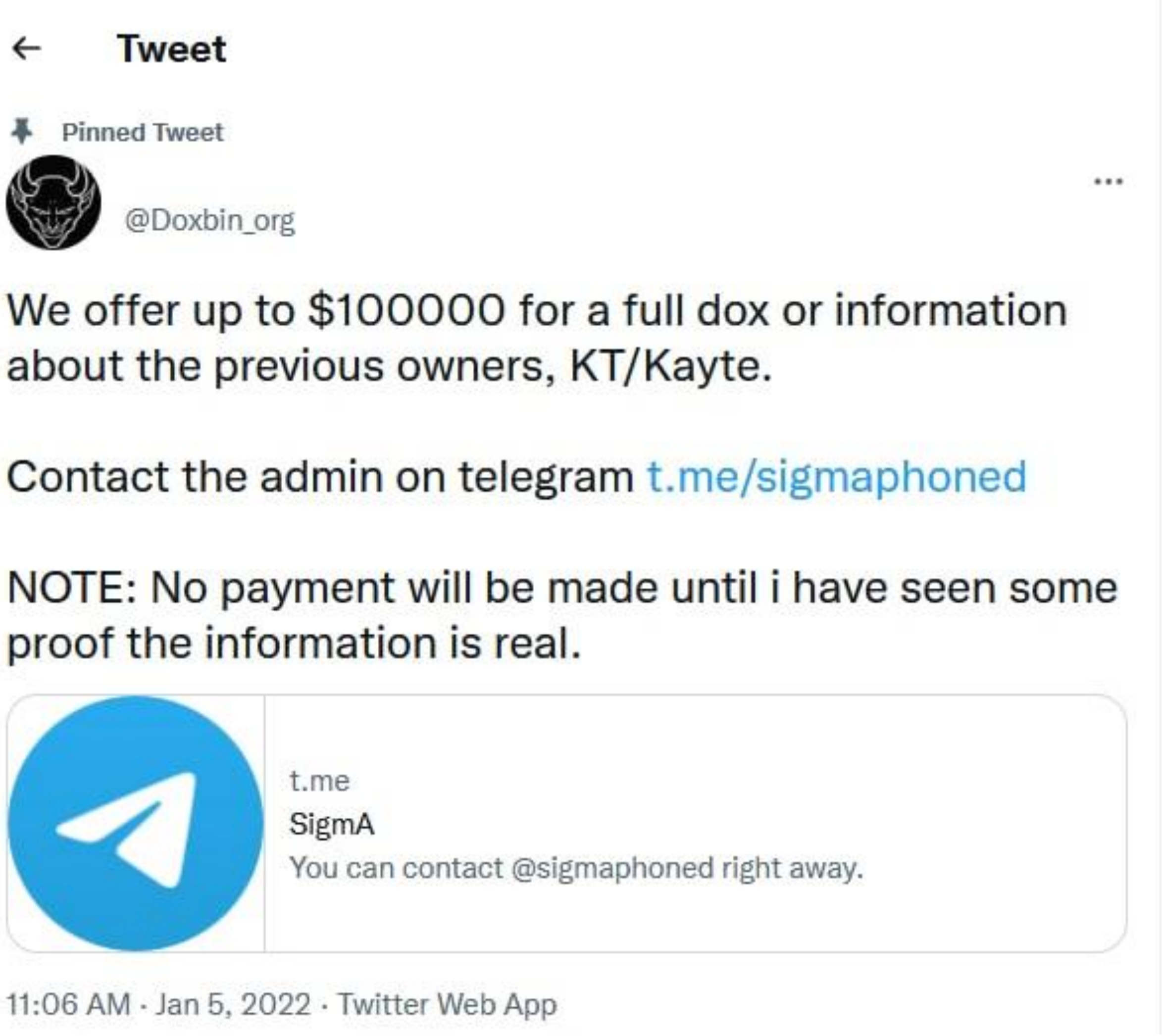
Cyberint's Research team actively monitors the gang's activity and Telegram channel, LAPSUS$ is mainly targeting Telecommunication and large software/gaming companies.

# HUNTING THE GROUP

As the group gained popularity, it also draw the attention of the cyber security community and in the process to understand the group better, some crucial details might have been compromised that affects the team's activity.

Evidence shows a relationship between the Doxbin website and LAPSUS$. It seems that one of Doxbin's former admin is currently one of LAPSUS$ leaders.

Doxbin is a document-sharing website that suffered a major breach in January. While the active admin has blamed the former one, an official Tweet was released with contacting information to the user sigmaphoned on Telegram (Figure 13).



Tweet

Pinned Tweet

@Doxbin_org

We offer up to $100000 for a full dox or information about the previous owners, KT/Kayte.

Contact the admin on telegram t.me/sigmaphoned

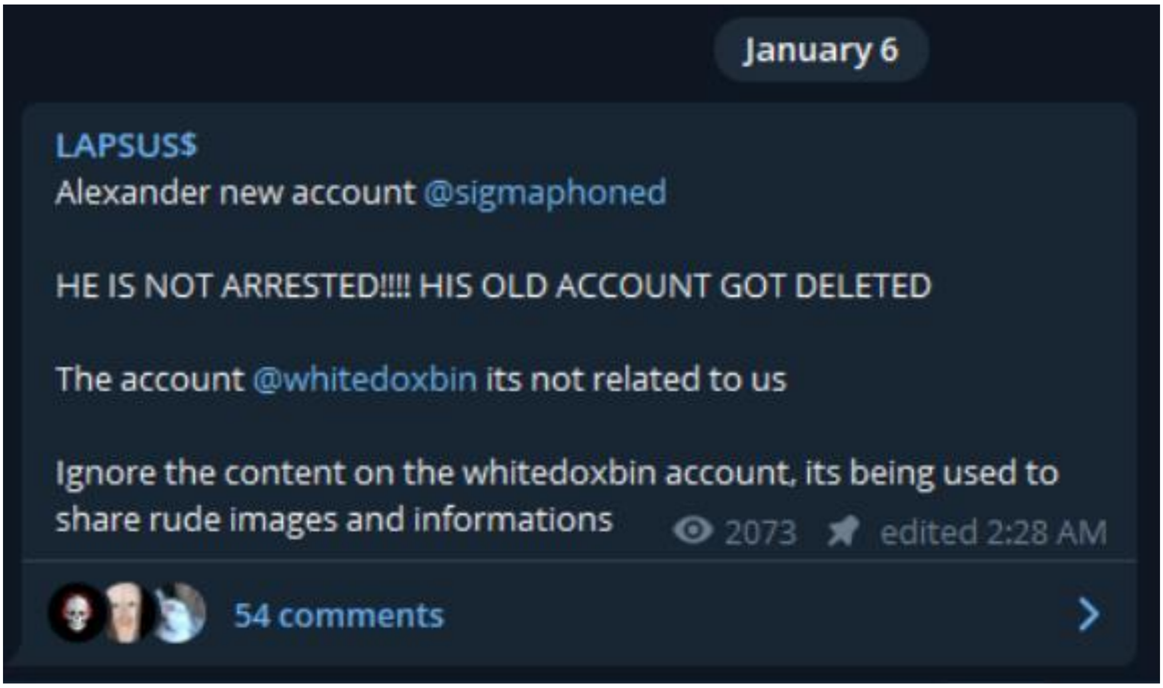
NOTE: No payment will be made until i have seen some proof the information is real.

t.me
SigmA
You can contact @sigmaphoned right away.

11:06 AM · Jan 5, 2022 · Twitter Web App

Figure 13: Doxbin's admin blaming the former one for the breach and looking to buy information

Looking at the Telegram channel of the group following this event, a new account was added as the admin's new account - sigmaphoned (Figure 14).



January 6

LAPSUS$

Alexander new account @sigmaphoned

HE IS NOT ARRESTED!!!! HIS OLD ACCOUNT GOT DELETED

The account @whitedoxbin its not related to us

Ignore the content on the whitedoxbin account, its being used to share rude images and informations

Figure 14: sigmaphoned account revealed as LAPSUS$ admin.

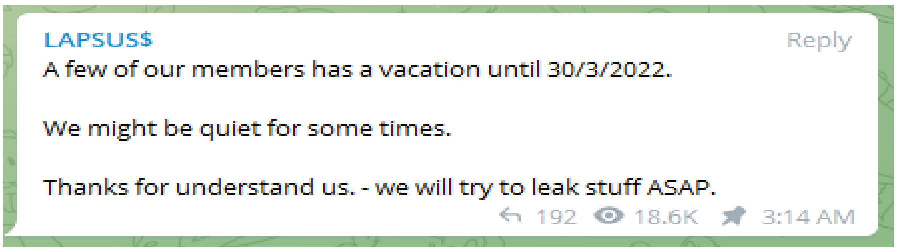
While the group suspiciously insists the other account, `@whitedoxbin`, is not related to them, also draw attention to this account. When looking at the Doxbin leaks for the relevant account, we are able to find the information of a certain individual in his teenage years, based in London, UK, that is suspected to be LAPSUS$ leader.

Chatters found regarding this individual indicate that law enforcements are currently on the pursuit of this individual that fled the UK, and at the moment is off-grid.

The claim that LAPSUS$ is but a group of teenagers or young adults aligns with many behavior patterns we have seen of the group.

## GOING OFF-GRID

After Okta's incident, it seems that LAPSUS$ has drawn a lot of heat. Some speculations suggest that several Law enforcements entities including the FBI are currently in pursuit of the leaders. One of LAPSUS$'s last announcements is that some of the members are going to take a vacation of a week and that they might be "quiet for some times" (Figure 14).



LAPSUS$

A few of our members has a vacation until 30/3/2022.

We might be quiet for some times.

Thanks for understand us. - we will try to leak stuff ASAP.

Figure 14: LAPSUS$ announcement that they are going on a vacation

# CONCLUSION

LAPSUS$ is a unique group for many reasons and although they are responsible for several big-scale campaigns such as Nvidia, Ubisoft, Samsung, and more, their methods are not too sophisticated and their management techniques and logistics of the group is done very poorly.

There is a big question mark regarding if the group continues to exist, given the allegedly leaked identity of the leader which will make things very hard to improve and expand the group's activities and personal.

As mentioned, although the most successful ransomware group based in Asia and Eastern Europe, LAPSUS$ was able to make a convincing tribute with the mentioned campaigns and put Latin America on the cybercrime map.

LAPSUS$ success in these major organizations leads us to understand that given basic knowledge in security, with a single insider threat, any organization, specifically supply chain organizations, regardless of its security measures, is vulnerable.

Also, we can learn that attacking these targets might be easier for threat actors given the massive amount of employees they hire - more employees, more inside threat potential, more strategic damage for the organization.

# RECOMMENDATIONS

Although Okta's announcement doesn't leave a lot of room to worry, Given the gravity of the Okta case, we would like to suggest additional security measures that might help mitigate and identify any potentially compromised accounts within Okta's customers.

- The impact of compromising an Okta account will be followed by a mechanism of resetting password or modifying Multi-Factor Authentication (MFA). In order for an organization to find these changes, we would recommend any Okta client that would like to identify accounts that might be compromised to look for the following event types in the past three months:
  - user.account.reset_password
  - user.mfa.factor.update
  - system.mfa.factor.deactivate
  - user.mfa.attempt_bypass
  - user.session.impersonation.initiate
- Any potentially compromised accounts should be immediately suspended until identity check will be verified in the following methods:
  - Verify identify through a video or audio call
  - Verify identify through security question
- Forced a password reset for all suspected accounts.
- Using MFA for all user accounts - These days, passwords alone does not provide full protection on our accounts.
- Usage of hard keys - Although MFA adds another layer of needed protection, it still can be vulnerable to phishing and smishing attacks.

# CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

## USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

## ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

## UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

## SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

## LATAM

Tel: +507-395-1553
Panama City