


What is going on with Lapsus\$?

 cyfirma.com/blogs/what-is-going-on-with-lapsus/

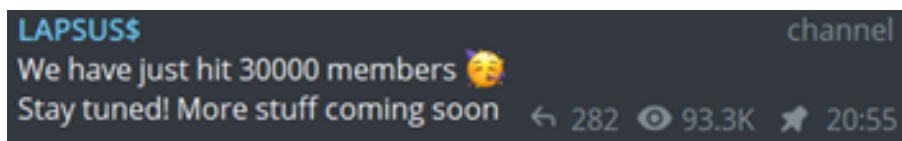
April 13, 2022

2022-04-13



What's going on with Lapsus\$

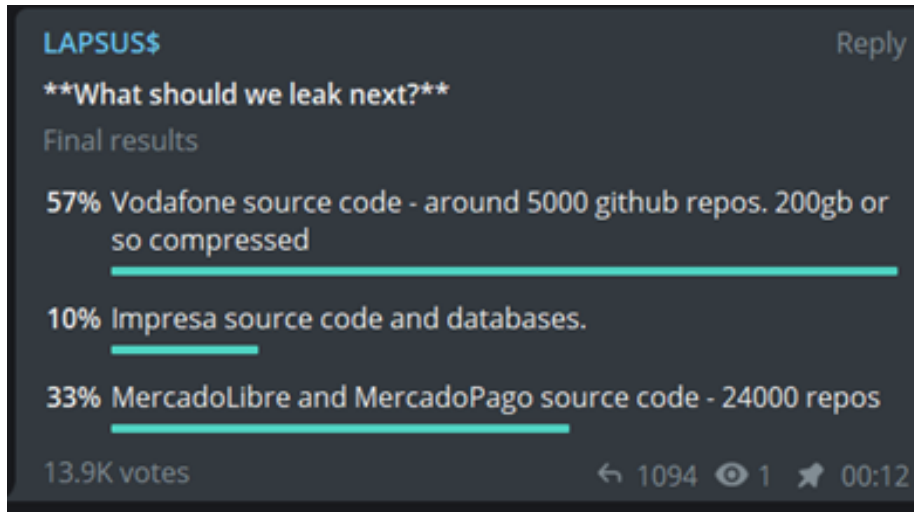
By Adam Parsons, CYFIRMA Cyber Threat Intelligence



Lapsus\$ has hit the headlines recently partly due to the mega-corporations that they appear to have successfully hacked and partly due to the claims that they are or were led by a 16-year-old.

Indeed, there have been a number of arrests, most recently a 16-year-old and a 17-year-old appeared in court in the UK charged with a number of cyber offenses. However, as the above post on their telegram chat group shows they have no intention of stopping.

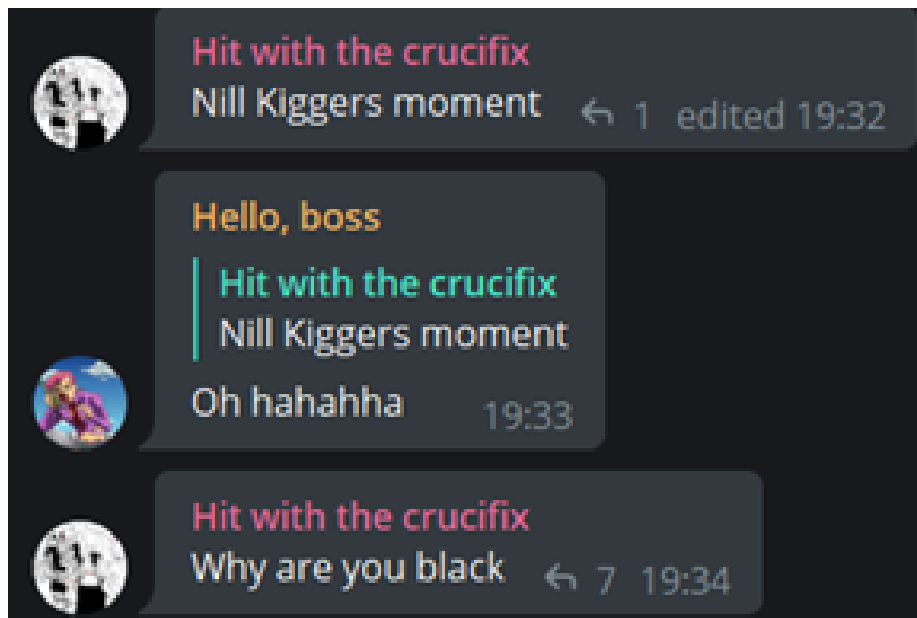
The telegram channel was their only official communication method where they have published stolen data, and in at least one instance, held a vote on who to attack next.



The group chat is used to share stolen data (not linked to Lapsus\$), tools and requests for hacking help. However, the channel is not quite a wild west...there are rules:

1. No porn
2. Not too much trolling
3. No spam

But outside of these rules anything goes...



The channel is not just for English speakers, there are a significant number of users communicating in Portuguese. This is potentially a throwback to the first few public victims of Lapsus\$ being the Ministério da Saúde do Brasil (Ministry of Health of Brazil) and latterly Portugal's Impresa media group.

Given that the rise of Lapsus\$ has coincided with the downfall of Raidforums, a popular entry-level hacking forum, it appears that the Lapsus\$ chat has attracted a significant number of like-minded individuals.

The telegram group still bears the name of its initial victim (<https://t.me/saudechat>), we can assume that it was initially set up to share the stolen data from the Ministério da Saúde do Brasil. That has long since passed, but still, the attacks keep coming even after what many thought would be arrested that would bring about their downfall. Likewise, the doxing of one of the supposed main members of the group has also not stopped their progress.

Given the naming of the telegram channel, we can assume that their ongoing activity was not planned. One would expect that they are making it up as they go along, thinking barely one step ahead. This may be one reason law enforcement is having such problems shutting them down. There is no plan, victims are targets of opportunity and profit is not the main motivation.

It has been reported that members of the group originate from the Sim Swapping world, a relatively small sub-section of the hacking community that is specifically focused on illegally obtaining control of phone numbers and subsequently control of their linked social media accounts. These social media accounts have then been used in several high-profile scams often involving crypto. Alternatively, sim swaps have been used to gain control of specific users' social media accounts due to a unique Twitter or Instagram handle that can then be sold in online forums. Much like Lapsus\$, individuals arrested in sim swapping are largely of a similar youthful age.

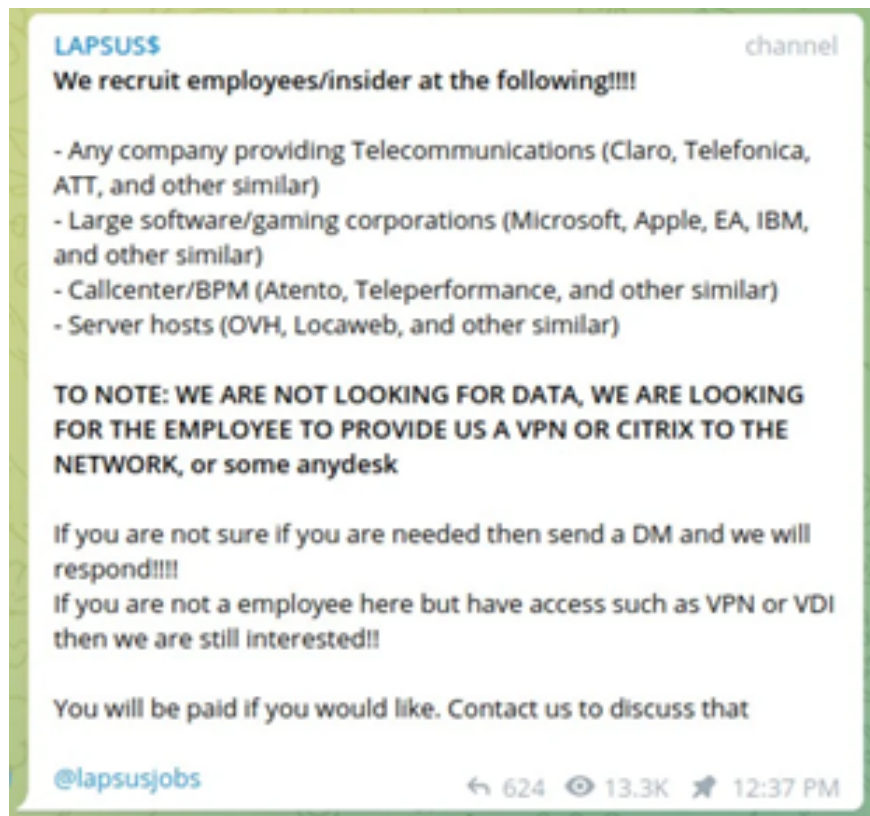
This might explain the brazen attacks against mega-corporations and so far their lack of interest in regularly using these attacks for financial gain or at least it does not appear to be their main motive. Hacks of Okta and Microsoft are by far more valuable than even the most high-profile Twitter handle. The reasons for these attacks are quite bizarre. The hack of Nvidia was followed by a demand to remove all Lite Hash Rate (LHR) limitations to its Graphics Processing Unit (GPU) hash rate that prevents faster crypto mining activities. It also wanted Nvidia to publish the base codes of its GPU drivers as open-source, making them publicly accessible and openly modifiable forever. Neither of these demands would directly benefit Lapsus\$ and seem more targeted at pleasing their fans and enhancing their reputation amongst the community.

How are they doing....what they do!

There have been a number of in-depth reports on how Lapsus\$ has evaded the defenses of their victims. Researching the group, we discovered how incredibly simple some of their methods were.

The technical skills and social engineering techniques bear resemblance to those used in the sim swapping world, which is after all where they first got started.

Lapsus\$ group put out a call on their telegram channel to employees at potential victim companies, as seen below:



Whilst this was widely mocked in cybercriminal communities for the lack of hacking prowess it takes to recruit insiders to simply give you access, it has been reported that this was in fact the reason Microsoft fell prey to the attack. Lapsus\$'s approach may seem less sophisticated compared with advanced threats groups, but as we have witnessed, they are a force to be reckoned with. Given that Lapsus\$ appears to have used this technique as early as November 2021, we can easily assume that it has been more successful than reported.

Aside from this, Lapsus\$ techniques are a throwback to their sim swapping days and revolve around social engineering techniques.

Lapsus\$'s methods – they seem so easy



Sim swapping involves obtaining control of a victim's phone number by tricking the phone service provider to transfer the phone number and therefore control to another device as per the above illustration. This method requires a significant level of knowledge of potential questions posed by the phone service provider and their requisite and often personal answers. Lapsus\$ likely makes use of openly available data through social media and previously breached data to answer these questions.

Once the number has been transferred, threat actors can then get access to most if not all the victim's linked accounts through password resetting via the transferred phone number where the phone number is used as a method of recovery. Email accounts often hold valuable information, including account details, passwords and answers to security questions. Lapsus\$ has also been reported to deploy Redline malware, a password and session token stealer.

There is another avenue much like sim swapping where it requires the threat actor to make a call impersonating the victim. The hacker will call the employee's IT department and attempt to have their password reset. Depending on the security stance of the organization, this often requires answering numerous questions which are personal to the victim.

Once the victim's password has been obtained, there is another line of defense.

Multifactor Authentication (MFA) or 2-factor authentication (2FA) comes in many forms as it is an additional security measure should a password be leaked or otherwise obtained by an unauthorized party. MFA requires the approval or authentication on an additional device to grant access.

Once an employee password is known, the group would need to pass MFA. Should they have access to the victim phone number and MFA is linked to the compromised number, access can be obtained. If this is not the case, then there are a number of other methods that can be used.

Spamming employees with push requests and automated calls to get MFA approval is one such method. Lapsus\$ even brag about this technique on their channel “Call the employee 100 times at 1 AM while he is trying to sleep, and he will more likely to accept it. Once the employee accepts the call, you can access the MFA enrolment portal and enroll another device”

Whilst bombarding an employee with MFA requests creates a lot of noise and could potentially alert the victim, there are other stealthy methods at play. One such method involves sending MFA push requests a few times a day, hoping the employee’s guard drops momentarily.

Opting for more advanced MFA such as FIDO2 provides a higher degree of security. FIDO2 requires the authentication to be performed on the device that is used to log in, making remote logging in on any other device ineffective.

Of course, awareness by employees of these techniques is key. Suspicion should immediately be raised if an unrequested MFA notification is received. Likewise, IT staff must remain vigilant to suspicious password resets requests. Staying updated on what is shared online on social media and awareness of any personal data that has been leaked will help avoid becoming a victim.

So what’s next from Lapsus\$?

As we have seen, law enforcement coming down on Lapsus\$ has not stopped the group’s activities. We can assume a leadership group is controlling the telegram channel rather than an individual. One would expect that it is a point of pride that the channel stays up despite law enforcement action. The group has a plan to use Element.io instant messaging platform as a backup should their Telegram channel shut down.

In the meantime, the channel continues to grow, as Lapsus\$ have triumphantly noted that their telegram chat group now has over 30,000 members. Should the leadership group be taken down, it would not be out of the question for one of these members to form their own Lapsus\$ franchise if they have not already done so. The added humiliation of a multinational corporation being hacked by a group most associated with teenagers doing it for the ‘Lolz’ would make the Lapsus\$ name an attractive brand.

APTS have imaginative animals as their mascot, Hacktivists have Guido Fawkes masks, will malicious teenagers use the Lapsus\$ name as their logo?

If we were to illustrate a picture of the Lapsus\$ group based on their history and current trajectory, we should draw a multi-headed hydra, each head laughing as Law Enforcement arrests teenager after teenager, and the regrown heads hack their way through the sophisticated defenses of company after company.....just for the Lolz.

[Back to Listing](#)