



PROFILE

Lapsus\$

ZEROFOX INTELLIGENCE

P-2022-03-22a

Classification: TLP - Amber

Intelligence Requirements: Internet Infrastructure, Malware, Vulnerabilities

March 22, 2022



Created on: March 15, 2022

Last Updated: March 22, 2022

Intelligence Cut-off: 1:00 PM (EDT) on March 22, 2022

First Seen: December 2021

Origin: South America

Aliases: N/A

Motivation: Likely financial

Targeted Industries: Telecommunications; Media and Entertainment; Technology; Retail; Public Sector

Targeted Nations: Brazil; Nepal; Portugal; South Korea; United States

Background

Lapsus\$ is an extortion collective. After compromising a network, Lapsus\$ typically, though not exclusively, exfiltrates data that can be leveraged in ransom demands. The group was identified operating in its current form as early as December 2021 following an attack on websites owned by Brazil's Ministry of Health; however, there is some evidence to suggest entities within the collective may have been operating since as early as July 2021.¹ The group appears to be financially motivated.

ZeroFox assesses that Lapsus\$ likely originates in South America—specifically, Brazil—given the plethora of attacks it has claimed against South American organizations and Brazilian and Portuguese-speaking companies more broadly. This is also supported by the Portuguese-language ransom notes Lapsus\$ sends to victims, though the group has shown proficient use of different languages within its Telegram channel. It is likely the collective has operatives based in other countries.

The collective has conducted multiple intrusions in the year to date and appears to have expanded its scope of targets. In February and March 2022, Lapsus\$ began targeting a host of large tech firms in other regions, including Microsoft, NVIDIA, and Samsung, with confirmation of data stolen by the group in many cases. Lapsus\$ is likely attempting to rapidly make a name for itself, emboldened by the success of previous operations. Most recently, Lapsus\$ claimed to have breached South Korean electronics firm LG and Okta, the access-management company servicing over 15,000 companies worldwide; unconfirmed reports indicate a third-party contractor may have been leveraged as part of the intrusion.² At the time of writing, Lapsus\$ has not yet made this data available or offered it for sale to the wider market. Customers should contact ZeroFox with any specific questions on the alleged Okta breach.

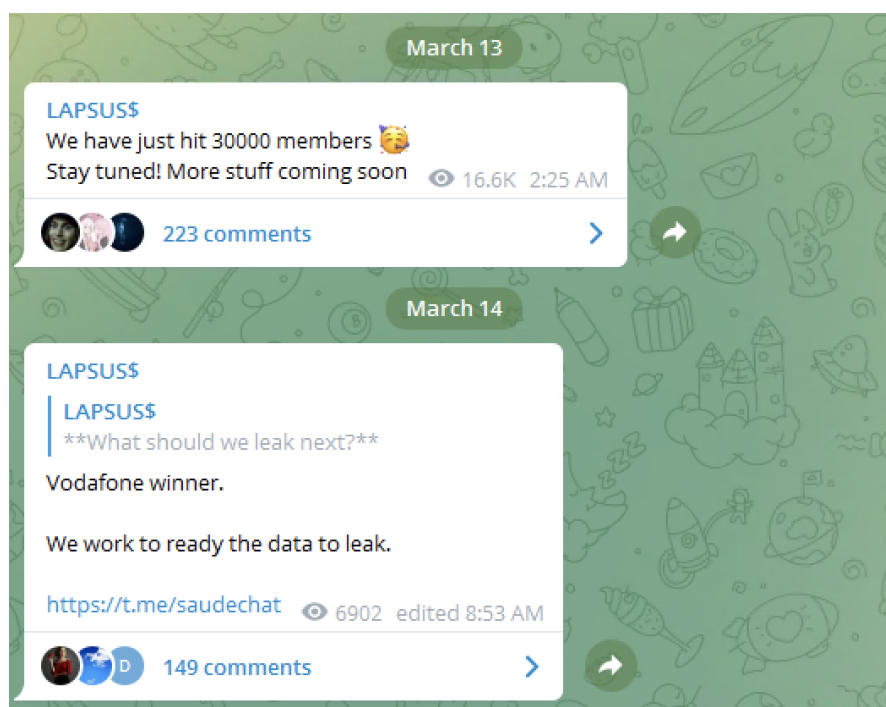
¹ <https://community.ee.co.uk/t5/Online-safety/Lapsus-Text/td-p/1067036>

² https://twitter.com/declx0_/status/1506148323056488450?s=20&t=hkRJlhiQe5ey2s0JM3l2CA



Infrastructure

Lapsus\$ communicates externally via its Telegram channel, which was created in December 2021 and has in excess of 37,800 subscribers as of March 22, 2022.³ Multiple channels with “Lapsus\$” in their titles have been created in the last seven days, likely indicative of copycat activity. The group may leverage other means of communication during operational activity. Lapsus\$ regularly posts statements on its Telegram channel about past and planned attacks and has conducted polls on which organizations should be targeted in the future. Lapsus\$ conducted an anonymous poll in early March on which organization’s data should be leaked next. On March 14, 2022, the group declared Vodafone the “winner” and indicated they are working on the data leak.⁴ The group also typically leverages its Telegram channel as the platform for publishing victims’ data. Reporting suggests Lapsus\$ has previously claimed not to use dark web forums for communication.⁵



Lapsus\$ declaring Vodafone the “winner” of its Twitter poll

Source: Lapsus\$ Telegram channel

³ <https://twitter.com/ZeroLogon/status/1503223605257191428>

⁴ <https://cloud.zerofox.com/intelligence/search?sources=telegram&q=%22Vodafone%20winner%22>

⁵

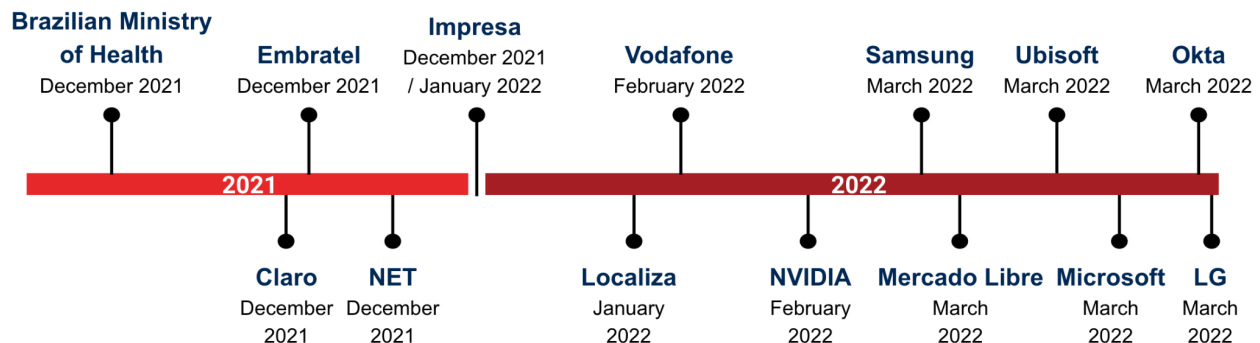
<https://www.forbes.com/sites/daveywinder/2022/03/12/threat-intel-report-who-is-behind-staggering-190gb-samsung-galaxy-hack/?ss=consumertech&sh=12e49c185723>



Intrusion Vectors

Lapsus\$ leverages phishing campaigns and vulnerabilities in internet-facing applications as a method of intrusion. In its early January 2022 compromise of Impresa, Lapsus\$ deployed phishing emails to subscribers of the Espresso newsletter using the lure that the President of Portugal had been murdered.⁶ Reporting also indicates that Lapsus\$ has leveraged Microsoft Exchange Server, FortiGate Firewall, and public AWS infrastructure vulnerabilities. While very little is known about the specific tactics, techniques, and procedures used by Lapsus\$, the group is understood to lay dormant for a period of time while maintaining persistence, moving laterally and escalating privileges.⁷ To date, no victims or security researchers have published verifiable technical information about the attacks, such as indicators of compromise (IoCs).

In March 2022, Lapsus\$ leveraged Telegram in a bid to drive recruitment, issuing a statement that the group was willing to pay “insiders” (current or former employees) from several companies to provide them access to VPN or VDI credentials. The list of companies that the group sought to recruit from included AT&T, Microsoft, EA, IBM, and Apple. Such tactics have previously been deployed by threat actors; LockBit ransomware operators announced their intention to recruit insiders in August 2021.⁸ ZeroFox has identified no credible evidence to suggest Lapsus\$ has been successful in its attempts.



Alleged Lapsus\$ attacks December 2021 - March 2022

Source: ZeroFox internal collections

⁶

<https://www.euronews.com/2022/01/06/hackers-send-fake-news-alert-about-portugal-president-s-re-moval>

⁷ <https://blog.vairav.net/2022/02/07/lapsus-group-targets-nepal/>

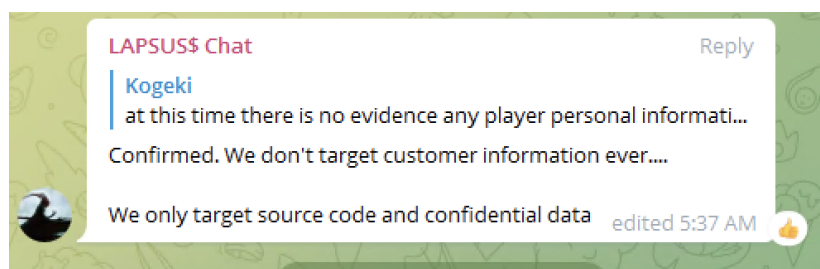
⁸

<https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breac-h-corporate-networks/>



Extortion

Though it is clear Lapsus\$ is an extortion outfit, ZeroFox has been unable to verify the widespread assertion that Lapsus\$ is a ransomware operation. After successfully compromising a network, threat actors have been observed exfiltrating sensitive corporate data, including source code and intellectual property; following a recent alleged intrusion into Ubisoft, the group claimed that it does not target customer information. However, no evidence has been identified that malware has been deployed or files encrypted in its attacks to date. ZeroFox assesses it is more likely that the group is leveraging “hack-and-leak” tactics under the guise of a ransomware operation. While the ransoms demanded are sometimes monetary, this is not always the case.



Lapsus\$ stating it targets source code and confidential data, not customer information

Source: Lapsus\$ Telegram channel

Lapsus\$ often attempts to disrupt business processes and cause reputational damage. The group’s January 2022 attack on the Brazilian car rental company Localiza saw the collective redirect the victim’s website to a pornography website via a DNS spoofing exploit. The attack was followed by an announcement from Lapsus\$ highlighting its actions. Notably, evidence suggests this attack did not involve data exfiltration or a ransom demand. Lapsus\$ also attacked the Portuguese media conglomerate Impresa by defacing its website and then uploading a ransom notice stating the group had control over Impresa’s AWS account. The Expresso Twitter account was hijacked, and a tweet was posted stating “Lapsus\$ is officially the new president of Portugal.”⁹ It is likely these attacks were conducted by Lapsus\$ for bragging rights and to enhance its own reputation and demonstrate capability before pivoting to larger targets, such as Microsoft, NVIDIA, and Samsung.

Following Lapsus\$’s breach of NVIDIA, researchers reported that they had collected samples of suspicious software payloads using at least two of NVIDIA’s digital certificates that were compromised in the breach.¹⁰ Both certificates are expired, but they remain valid for Windows systems—meaning that threat actors can use the certificate to make their malware payloads seem like valid NVIDIA software updates.

⁹ <https://twitter.com/campuscodi/status/1478002854128500743>

¹⁰

<https://www.bleepingcomputer.com/news/security/malware-now-using-nvidias-stolen-code-signing-certificates/>



NVIDIA (February 2022)

- After compromising U.S.-based computer chip maker NVIDIA, Lapsus\$ claimed to have exfiltrated one TB of data.¹¹ The stolen data consisted of proprietary information and more than 85,000 employee credentials, including email addresses and New Technology LAN Manager (NTLM) password hashes— which the group began publishing.
- The leak also included two stolen code-signing certificates used by NVIDIA developers to sign their drivers and executables.¹² In March 2022, threat actors were identified using the stolen certificates to sign malware and tools to enable malicious drivers to be loaded in Windows. These included Cobalt Strike beacons, Mimikatz, backdoors, and remote access trojans.
- It is not clear if a financial ransom was initially demanded. However, Lapsus\$ threatened to leak hardware specifications information if lite hash rate (LHR) limitations were not removed from NVIDIA's GeForce RTX 30 Series firmware. Lapsus\$ also demanded that NVIDIA commit to open-sourcing its GPU drivers for Windows, macOS, and Linux devices.
- NVIDIA claimed that it had found no evidence of a ransomware attack but did confirm that data had been exfiltrated.
- During negotiations, Lapsus\$ claimed NVIDIA had attempted to encrypt the threat actor's virtual machine that contained the data in a "hacking back" attempt but failed. ZeroFox cannot confirm the veracity of the claims made.

Recommendations

- Critical data should be backed up regularly, including password-protected backup copies kept offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, or the cloud).
- Ensure proper network segmentation.
- Never download email attachments from unknown senders or click links from untrusted sources. Provide user-training programs to fight against phishing or social engineering attacks used to obtain critical information that can lead to attacks.
- Enable multi-factor authentication wherever possible.
- Patch disclosed vulnerabilities with updated software versions as quickly as practical.
- Disable PowerShell wherever possible to limit the possibility of operators employing lateral movement modules.

¹¹

<https://www.bleepingcomputer.com/news/security/hackers-to-nvidia-remove-mining-cap-or-we-leak-hardware-data/>

¹²

https://twitter.com/BillDemirkapi/status/1499437244830175236?s=20&t=_EUUVs3s9yR8tsuA8auYOw



Appendix: Traffic-Light Protocol for Information Dissemination

Color	When Should It Be Used?	How May It Be Shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use the TLP: AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.