Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:00:17 UTC

Other threat group: Lapsus$

Names	Lapsus$ *(self given)* DEV-0537 *(Microsoft)* Strawberry Tempest *(Microsoft)* Slippy Spider *(CrowdStrike)* G1004 *(MITRE)*	
Country	Brazil	
Motivation	Financial gain	
First seen	2021	
Description	(Flashpoint) LAPSUS$ is an extortionist threat group that became active on December 10, 2921. Unlike the majority of extortionist groups that typically rely on a combination of ransomware and data leaks, LAPSUS$ is focused on monetizing their operations exclusively through data leaks advertised on Telegram without the use of ransomware. Initially, the group focused on data breaches against Latin American and Portuguese targets but in late February 2022, LAPSUS$ began widening the scope of its targeting by announcing it had successfully breached US-based graphics and computing chip manufacturer Nvidia. Since then, LAPSUS$ has continued to focus on large-scale international technology companies, including Microsoft, Okta, and Samsung, as the financial incentive for stealing source code and extorting companies for sensitive proprietary technical data is high. Around July 2025, ShinyHunters teamed up or merged with Subgroup: Scattered Spider. They share their Telegram channel also with Lapsus$, so they may all work together now – see the DataBreaches.net references in the Information section under ShinyHunters.	
Observed	Countries: Argentina, Brazil, Portugal, USA.	
Tools used		
Operations performed	Dec 2021	Brazil health ministry website hit by hackers, vaccination data targeted <https://www.reuters.com/technology/brazils-health-ministry-website-

	hit-by-hacker-attack-systems-down-2021-12-10/>
Dec 2021	The Lapsus$ ransomware gang has hacked and is currently extorting Impresa, the largest media conglomerate in Portugal and the owner of SIC and Expresso, the country's largest TV channel and weekly newspaper, respectively. <https://therecord.media/lapsus-ransomware-gang-hits-sic-portugals-largest-tv-channel/>
Jan 2022	Lapsus$ Attacks Localiza, Redirects Users to Porn Site <https://www.databreachtoday.com/lapsus-attacks-localiza-redirects-users-to-porn-site-a-18286>
Jan 2022	Okta confirms 2.5% customers impacted by hack in January <https://www.bleepingcomputer.com/news/security/okta-confirms-25-percent-customers-impacted-by-hack-in-january/> <https://thehackernews.com/2022/03/new-report-on-okta-hack-reveals-entire.html>
Feb 2022	In the wake of the attack last month on the Impresa group, the latest victims – Correio da Manhã (the country's most widely-read tabloid), Sábado, Jornal de Negócios and CMTV – belong to the Cofina media group. <https://www.portugalresident.com/hackers-bring-down-new-media-sites-pj-cybercrime-unit-investigating/>
Feb 2022	Cyberattack brings down Vodafone Portugal mobile, voice, and TV services <https://therecord.media/cyberattack-brings-down-vodafone-portugal-mobile-voice-and-tv-services/> <https://www.securityweek.com/vodafone-investigating-source-code-theft-claims>
Feb 2022	GPU giant NVIDIA is investigating a potential cyberattack <https://www.bleepingcomputer.com/news/security/gpu-giant-nvidia-is-investigating-a-potential-cyberattack/> <https://www.databreaches.net/lapsus-and-the-terrible-horrible-no-good-very-bad-ransom-day1/>
Mar 2022	Hackers leak 190GB of alleged Samsung data, source code <https://www.bleepingcomputer.com/news/security/hackers-leak-190gb-of-alleged-samsung-data-source-code/>

	Mar 2022	E-commerce giant Mercado Libre confirms source code data breach <https://www.bleepingcomputer.com/news/security/e-commerce-giant-mercado-libre-confirms-source-code-data-breach/>
	Mar 2022	Lapsus$ Ransomware Group is hiring, it announced recruitment of insiders <https://securityaffairs.co/wordpress/128912/cyber-crime/lapsus-ransomware-is-hiring.html>
	Mar 2022	Ubisoft confirms 'cyber security incident', resets staff passwords <https://www.bleepingcomputer.com/news/security/ubisoft-confirms-cyber-security-incident-resets-staff-passwords/>
	Mar 2022	Lapsus$ hackers leak 37GB of Microsoft's alleged source code <https://www.bleepingcomputer.com/news/microsoft/lapsus-hackers-leak-37gb-of-microsofts-alleged-source-code/>
	Mar 2022	Globant confirms hack after Lapsus$ leaks 70GB of stolen data <https://www.bleepingcomputer.com/news/security/globant-confirms-hack-after-lapsus-leaks-70gb-of-stolen-data/>
	Mar 2022	Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code <https://krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code/>
	Sep 2022	Uber attributes hack to Lapsus$, working with FBI and DOJ on investigation <https://therecord.media/uber-attributes-hack-to-lapsus-working-with-fbi-and-doj-on-investigation/>
	Sep 2022	2K Games says hacked help desk targeted players with malware <https://www.bleepingcomputer.com/news/security/2k-games-says-hacked-help-desk-targeted-players-with-malware/>
	Sep 2022	Rockstar confirms cyberattack, leak of confidential data including GTA 6 footage <https://therecord.media/rockstar-confirms-cyberattack-leak-of-confidential-data-including-gta-6-footage/>
Counter operations	Mar 2022	Lapsus$ suspects arrested for Microsoft, Nvidia, Okta hacks <https://www.bleepingcomputer.com/news/security/lapsus-suspects-arrested-for-microsoft-nvidia-okta-hacks/>
	Apr 2022	Two teenagers charged in connection with investigation into hacking group <https://www.cityoflondon.police.uk/news/city-of-

		london/news/2022/march/two-teenagers-charged-in-connection-with-investigation-into-hacking-group/>
	Aug 2022	Brazilian police launch investigation targeting Lapsus$ group <https://therecord.media/brazilian-police-launch-investigation-targeting-lapsus-group/>
	Sep 2022	UK Police arrests teen believed to be behind Uber, Rockstar hacks <https://www.bleepingcomputer.com/news/security/uk-police-arrests-teen-believed-to-be-behind-uber-rockstar-hacks/>
	Oct 2022	Brazil arrests suspect believed to be a Lapsus$ gang member <https://www.bleepingcomputer.com/news/security/brazil-arrests-suspect-believed-to-be-a-lapsus-gang-member/>
	Jul 2023	British prosecutors say teen Lapsus$ member was behind hacks on Uber, Rockstar <https://therecord.media/british-prosecutors-accuse-teen-lapsus-member-of-uber-revolut-rockstar-hacks>
	Aug 2023	Lapsus$ teen hackers convicted of high-profile cyberattacks <https://www.bleepingcomputer.com/news/security/lapsus-teen-hackers-convicted-of-high-profile-cyberattacks/>
	Dec 2023	Lapsus$ hacker behind GTA 6 leak gets indefinite hospital sentence <https://www.bleepingcomputer.com/news/security/lapsus-hacker-behind-gta-6-leak-gets-indefinite-hospital-sentence/>
Information	<https://www.flashpoint-intel.com/blog/lapsus/> <https://www.silentpush.com/blog/lapsus-group-an-emerging-dark-net-threat-actor> <https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/> <https://unit42.paloaltonetworks.com/lapsus-group/> <https://www.cybereason.com/blog/lapsus-activity-betrays-nation-state-motivation> <https://research.nccgroup.com/2022/04/28/lapsus-recent-techniques-tactics-and-procedures/> <https://thehackernews.com/2022/05/everything-we-learned-from-lapsus.html> <https://www.tenable.com/blog/brazen-unsophisticated-and-illogical-understanding-the-lapsus-extortion-group> <https://www.bleepingcomputer.com/news/security/dhs-cyber-safety-board-to-review-lapsus-gang-s-hacking-tactics/> <https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G1004/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
