All About LAPSUS$: What We Know About the Extortionist Group [Updated]

By Flashpoint Intel Team

Published: 2022-03-23 · Archived: 2026-04-05 22:09:29 UTC

Understanding the Rise and Fall of LAPSUS$

LAPSUS$ is an extortionist threat group that became active on December 10, 2021. 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.

What Made LAPSUS$ Tactics So Effective?

Unlike traditional ransomware groups, they did not always encrypt their victims' data. Instead, they focused on data extortion. They would steal sensitive source code or customer data and then demand a ransom to keep it private.

Using Social Engineering to Bypass MFA

One of the group's most famous tactics was bypassing multi-factor authentication (MFA). They did not use technical exploits to do this. Instead, they used "MFA fatigue" attacks. They would send a flood of login requests to an employee's phone at night. Eventually, the tired employee might approve just to stop the noise.

They also used simple social engineering to trick help desks. They would call an IT support line and pretend to be an employee who lost their phone. By using basic personal info found online, they convinced help desks to reset passwords or add new devices. These human errors provided the group with initial access.

Notable LAPSUS$ targets

LAPSUS$ is different from ransomware collectives in that the group is not encrypting the files of their victims, but rather gaining access to important files and threatening to leak if an extortion is not paid.

Brazil's Ministry of Health

LAPSUS$ claimed its first victim, Brazil's Ministry of Health, on December 10, 2021. Since then, the group has claimed an additional 19 victims, the first 15 of which were all Latin American and Portuguese targets.

Localiza

LAPSUS$ gained additional notoriety on when, on January 11, it began redirecting users of the official website for Localiza, one of the largest car rental conglomerates in Latin America, to a pornography site.

Vodafone Portugal

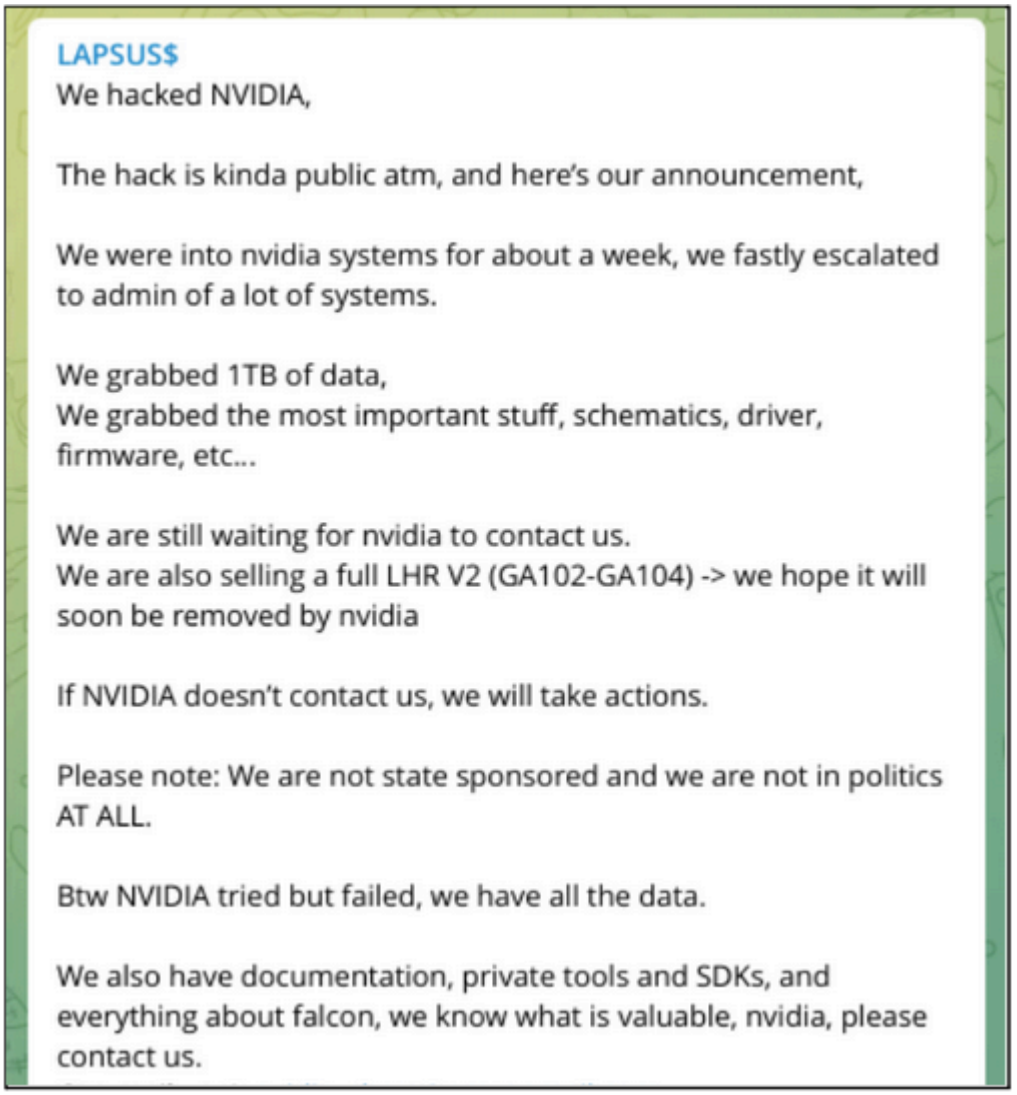
On February 8, Vodafone Portugal suffered a cyberattack impacting its 4G and 5G services. Initially, no group claimed responsibility, which was speculated to be either a distributed denial-of-service (DDoS) or ransomware attack. But on February 24, LAPSUS$ admitted responsibility for the Vodafone Portugal attack on its Telegram channel.

Impresa and Confina

LAPSUS$ breached two of Portugal's largest media companies: Impresa, on January 3 and Confina on February 6.

NVIDIA

In perhaps its most publicized attack to-date, LAPSUS$ claimed it carried out an attack against US-based graphics and computing chip manufacturer NVIDIA, successfully exfiltrated 1 TB of data from the company's networks, including proprietary information related to NVIDIA's GPUs, which is not set to be publicly launched for sale until March 29. Overall, LAPSUS$ has thus far released 150GB of stolen data as of this publishing.



Screenshot of LAPSUS$'s Nvidia Hack Announcement (Image: Flashpoint).

The group also offered to separately sell a bypass for Nvidia's Lite Hash Rate (LHR) limit imposed on Nvidia GPUs to make them more ineffective for crypto mining purposes in an effort to address the global chip shortage. The group stated the minimum offer they would entertain for the LHR bypass was US$1 million.

Samsung

On March 4, LAPSUS$ posted a message in its official Telegram channel informing subscribers that it had carried out an attack against the South Korean electronics conglomerate, Samsung. The group later leaked 189 GB of stolen Samsung data and instructed Samsung to contact the group directly to prevent further leaks.s.

On March 7, Samsung revealed that it had suffered a data breach in which source code for Samsung Galaxy mobile devices had been stolen. However, the company stated that no personal customer or employee information was compromised as part of the breach. Samsung did not name a threat group responsible for the hack.

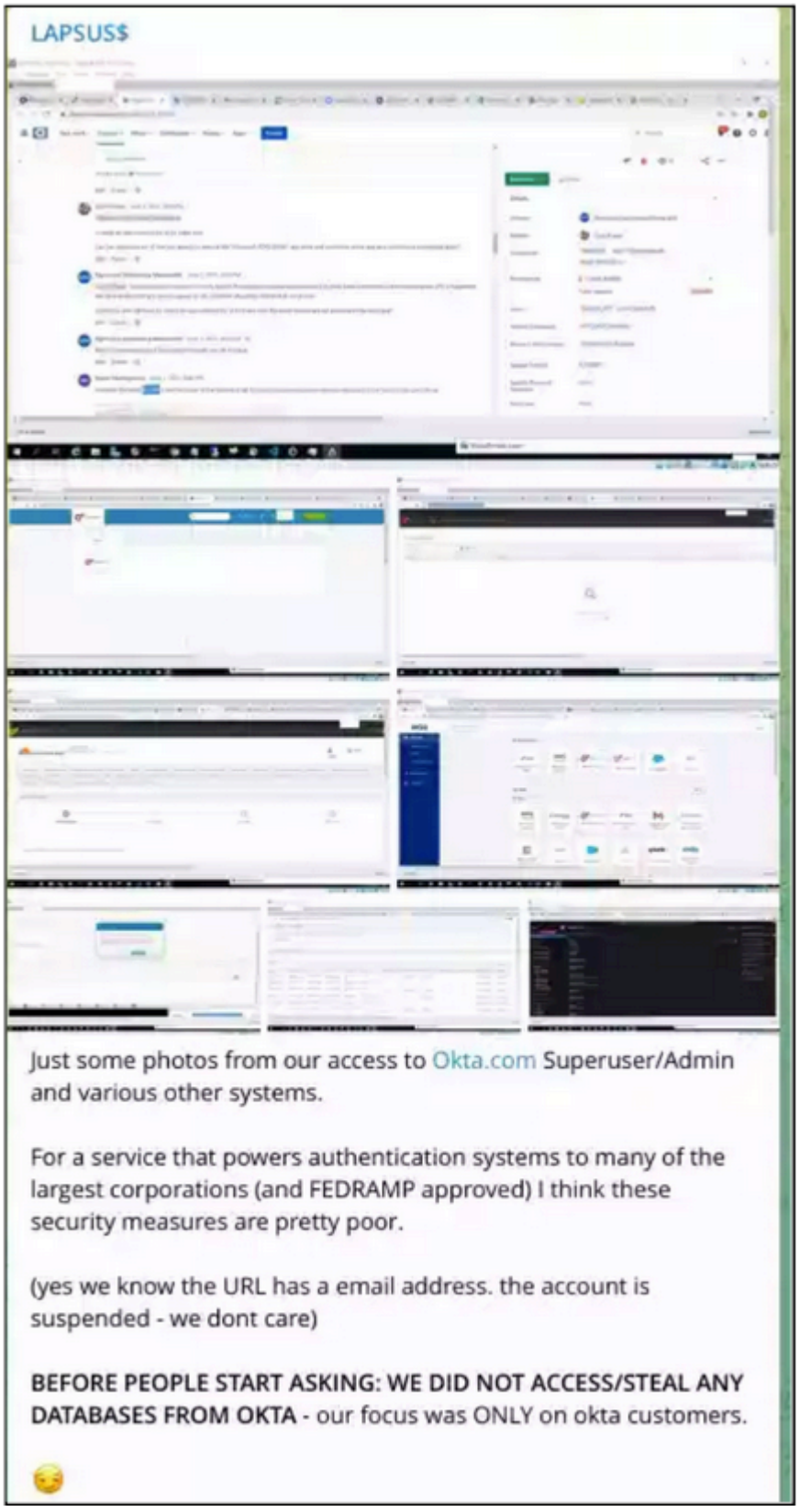
Microsoft

On March 20, 2022, LAPSUS$ claimed to have breached one of Microsoft's Azure DevOps accounts. Later, on March 22, LAPSUS$ leaked 37 GB of stolen data which allegedly included partial source code for Bing, Bing Maps, and Cortana.

On March 22, Microsoft released a blog post detailing LAPSUS$ and confirmed that a single account had been compromised and source code was stolen as a result. However, Microsoft stated that customer data and code theft had not been witnessed and incident responders were able to halt the malicious activity. Microsoft also stated that confidentiality of source code was not one of their security methods as access to it does not increase risk.

Okta

On March 22, LAPSUS$ claimed to have remote access and superuser and admin privileges on multiple Okta systems. LAPSUS$ stated that it did not steal data from Okta and the group's focus was rather on Okta customers.



Screenshot of LAPSUS$'s Okta Hack Announcement (Image: Flashpoint).

In response to LAPSUS$'s claims, Okta issued an official statement on March 22 in which the company revealed that in late January 2022, it had detected an attempt to compromise an account belonging to a third-party customer support engineer. Okta stated that it investigated the incident and was able to contain it. The company stated that

the screenshots shared by LAPSUS$ appeared to be related to this late January incident and that the company's investigations have not identified additional evidence of current malicious activity.

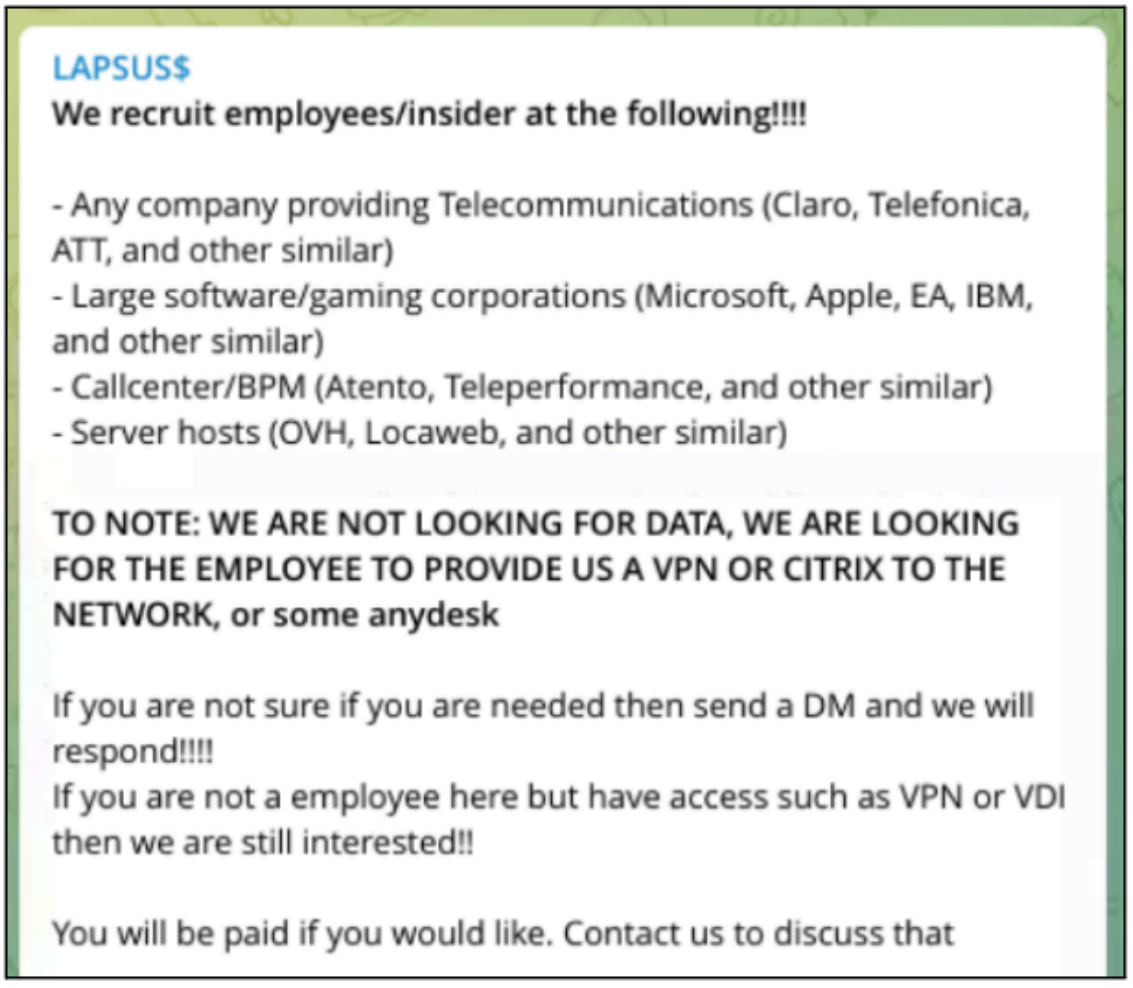
LAPSUS$ and Insider Threats

Since LAPSUS$ became active in December 2021, they have actively sought out corporate and government insiders which could provide the group with remote internal network access.

LAPSUS$ has emphasized that it is not interested in corporate data stolen from insiders but was specifically interested in network access, listing VPNs, Citrix, and AnyDesk as network access type examples.

On March 10, 2022, LAPSUS$ posted a advertisement (below) seeking to recruit insiders employed who could provide remote corporate network access through VPN or virtual desktop infrastructure (VDI) credentials within the following sectors:

- Telecommunications companies
- Large software and/or gaming companies
- Call centers and business process management (BPM) providers
- Server hosting providers



Screenshot of LAPSUS$ insider recruitment ad (Screenshot: Flashpoint).

Even prior to this latest insider recruitment advertisement, Flashpoint has observed multiple instances of LAPSUS$ insider recruitment attempts in the LAPSUS$ Telegram group going back to the group's founding in December 2021. For example, on December 12, 2021, the group offered to pay potential Brazilian Federal Police insiders within their Telegram group chat $15,000 for internal network access to Brazil's Federal Police network.

Although Flashpoint has not observed an example of an insider providing LAPSUS$ with access which later led to a real world attack, it's likely that if an insider has provided access to LAPSUS$ that has enabled an attack, these conversations likely would have taken place via private direct messages.

Based on LAPSUS$'s history of openly soliciting for corporate network accesses, Flashpoint assesses with moderate confidence that this is at least one if not the primary method the group is gaining initial access to victim organizations. As the group has also demonstrated a preference in login credentials for remote network gateways, it's also possible that the group could be procuring a portion of these accesses through dark web purchases such as browser stealer malware logs which are readily available for purchase on several dark web account shops and marketplaces.

Major LAPSUS$ Arrests

The City of London Police arrested seven individuals today, March 24, in connection with the extortionist group LAPSUS$, allegedly responsible for carrying out several high-profile attacks in recent weeks. Police revealed that all of the individuals arrested were between the ages of 16 and 21; no names are yet to be released. One of the threat actors arrested is said to have accumulated $14M as the fruits of their malicious cyber activities, according to the BBC.

On March 23, Bloomberg released an article tying the group's ringleader to the online aliases "white" and "breachbase," which belong to a 16-year-old UK minor. This individual was further tied to the aliases "WhiteDoxbin" and "Oklaqq" according to a KrebsOnSecurity article, also released yesterday. London Police did not reveal whether this individual was included in these arrests.

This minor was previously doxed by a rival threat actor on January 9. The doxxer purported that the alleged LAPSUS$ mastermind had purchased Doxbin, an illicit leak and dox site, which has had its issues ever since. This dox also contained personally identifiable information (PII) for the individual, but due to their underage status, Flashpoint will not be sharing this information.

The Bloomberg article also alluded to another LAPSUS$ member likely residing in Brazil, but did not provide an alias for this individual, suggesting perhaps this LAPSUS$ member may still be at large.

After the arrests, LAPSUS$ made reference to a vacation being taken by some of the groups members in their Telegram channel—a probable reference to the arrests announced.

Get Flashpoint Intelligence on Your Team

Any organization's security capabilities are only as good as its threat and vulnerability intelligence partner. Flashpoint's suite of tools offer you a comprehensive overview of your threat landscape, providing you with the

ability to proactively manage risks and protect your assets, infrastructure, and personnel. To unlock the power of great threat intelligence, **sign up for a demo** or get started with a **free trial** today.

LAPSUS$ Frequently Asked Questions (FAQs)

What is LAPSUS$ and how does Flashpoint Ignite track their activity?

LAPSUS$ is a high-profile extortion group within Flashpoint Ignite's monitoring scope that gained notoriety for targeting major global tech firms. Flashpoint Ignite tracks this group by monitoring their public and private Telegram channels where they announce new victims and poll their followers on which data to leak next. This provides Flashpoint users with immediate awareness of the group's targets and the specific TTPs they are using to bypass modern security stacks.

Group Characteristic	Flashpoint Ignite Strategic Benefit
Extortion Focus	Alerts users to data leaks even when no ransomware is present.
Telegram Presence	Captures real-time chatter and recruitment ads from the group.
Target Diversity	Tracks shifts in their focus across different industries and regions.

How does Flashpoint help prevent the MFA fatigue attacks used by LAPSUS$?

Flashpoint helps prevent MFA fatigue attacks by providing intelligence on the "initial access" methods that lead to these requests. Before LAPSUS$ can spam an employee with MFA prompts, they must first obtain a valid username and password. Flashpoint monitors for your organization's leaked credentials on the dark web, allowing you to reset compromised accounts before the group can ever initiate a malicious login or social engineering attempt.

- **Credential Monitoring:** Identifies stolen logins that are the prerequisite for MFA bypass.
- **TTP Intelligence:** Details how the group uses "MFA bombing" to overwhelm targets.
- **Help Desk Protection:** Provides training context for staff on how LAPSUS$ manipulates support calls.

Why is Flashpoint's visibility into "insider recruitment" vital for corporate defense?

Flashpoint's visibility into insider recruitment is vital because it allows organizations to detect when their own employees are being targeted by groups like LAPSUS$. Flashpoint monitors illicit forums and encrypted apps for posts specifically soliciting "access for hire" from within your domain. This allows security and HR teams to identify high-risk areas and take proactive measures to secure privileged accounts before an insider can facilitate a breach.

Insider Risk Factor	Flashpoint Integrated Response
Direct Recruitment	Alerts you when actors post ads for insiders at your company.
Credential Sales	Identifies if internal access tokens are being sold in illicit markets.
Behavioral Context	Provides a clear view of the rewards and incentives actors use to lure insiders.
