
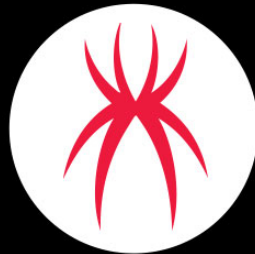


# Trustwave's Action Response: The Lapsus\$ Hacker Group Shows Us the Importance of Securing the Digital Supply Chain

 [trustwave.com/en-us/resources/blogs/spiderlabs-blog/trustwaves-action-response-the-lapsus-hacker-group-shows-us-the-importance-of-securing-the-digital-supply-chain](https://trustwave.com/en-us/resources/blogs/spiderlabs-blog/trustwaves-action-response-the-lapsus-hacker-group-shows-us-the-importance-of-securing-the-digital-supply-chain)



## SpiderLabs Blog

*Update March 24: This blog has been updated to reflect the new information provided by vendors attacked by Lapsus\$ and the reported arrests.*

***Trustwave is actively tracking the threat of Lapsus\$ for our clients. We encourage all organizations, especially those part of the digital supply chain, to remain vigilant and ensure that cyber best practices are implemented.***

***We are actively investigating all unusual login behaviors for clients that use Okta. For more information on the Okta incident, please visit [their blog](#). Trustwave does not use Okta.***

***Actionable security recommendations for organizations can be found below. [Join our threat briefing on Monday, March 28 for additional insights and recommendations from Trustwave SpiderLabs.](#)***

Lapsus\$ is the breakout cybercriminal gang making government entities and organizations in manufacturing, higher education, energy, retailers, and healthcare around the world question whether they could be the victim of a cyberattack.

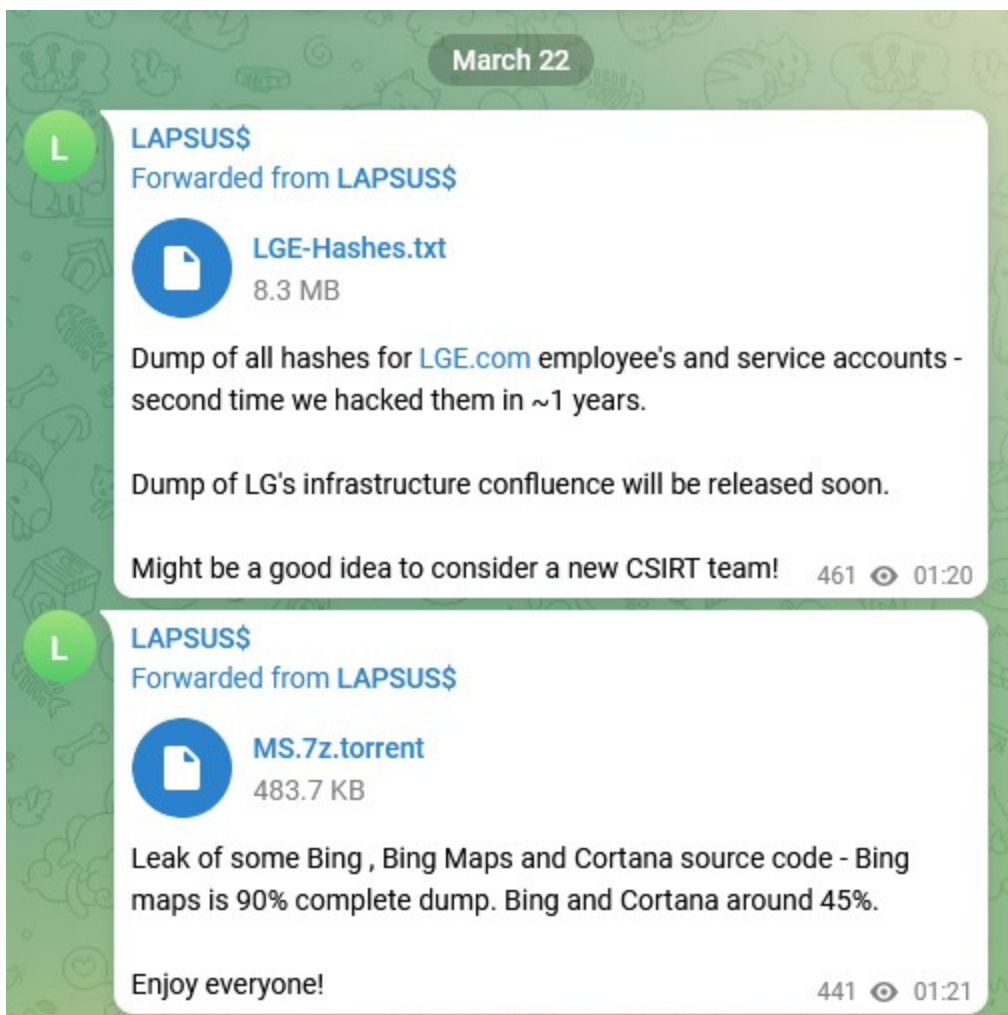
The new and unique Lapsus\$ cyber gang (or DEV-0537 as they are tracked by Microsoft) appears to be following a very different path – from the group’s communications to its tactics and techniques – compared to well-known groups like Conti, REvil and DarkSide.

## The Rise to Infamy

The Lapsus\$ hacker group began operations in late 2021 when the gang began targeting organizations in the Western hemisphere. These targets included Brazil’s health ministry, South American telecom companies, and Brazilian car rental services.

While Lapsus\$ is reportedly loosely formed, the gang was able to effectively attack additional South American organizations before graduating to hacking telecom giant Vodafone, video game developer Ubisoft, tech icon Samsung, and chipmaker NVIDIA.

Lapsus\$ most recently made headlines for allegedly exfiltrating source code data from LG Electronics and Microsoft – while most notably claiming to have had access to a ‘super user’ account of identity access management provider Okta.



Microsoft confirmed no customer code or data was involved in the observed activities of Lapsus\$. Their investigation found a single account had been compromised, granting limited access.

Okta has stated the access Lapsus\$ claimed was part of a January 2022 security incident that has since been resolved. The hacker group has responded – sharing how it believed the attack was a success and alleging Okta has downplayed the effectiveness of the breach.

On March 24, the BBC reported that City of London Police arrested seven people between the ages of 16 and 21 in connection with an investigation into a hacking group. According to the BBC, the police did not name the group, but the news agency cited cybersecurity researchers and fellow hackers who say at least one of those arrested is associated with Lapsus\$.

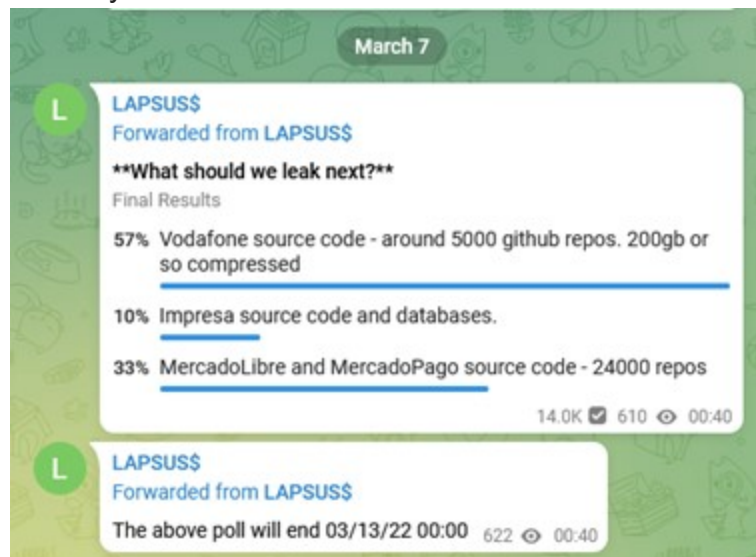
## Lapsus\$ Communication Behavior: Constant Contact With Their Community

---

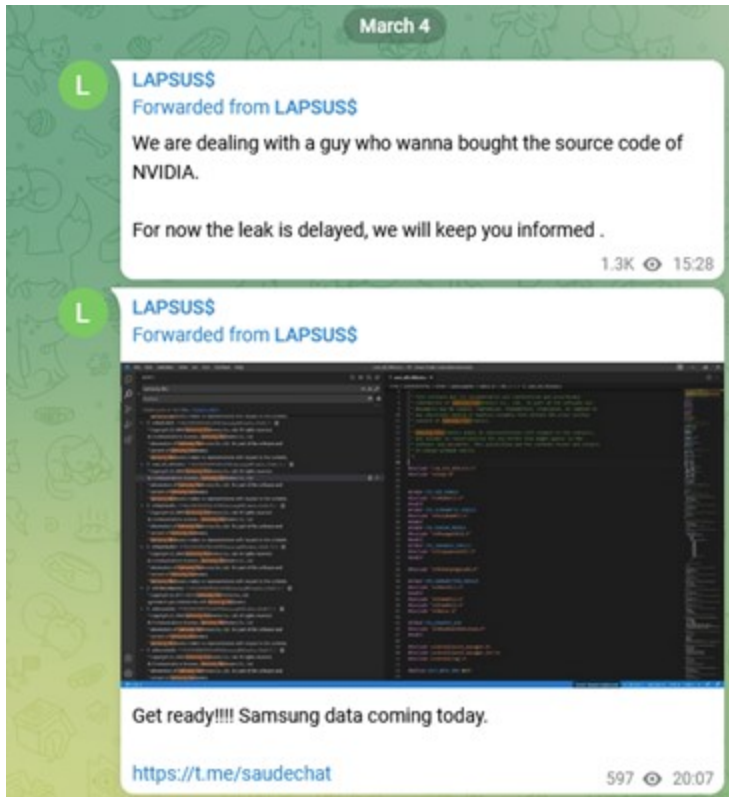
Lapsus\$ is communicating with its ‘audience’ mainly via Telegram Channel and a chat room. The main channel names spotted are "minsaude," "minsaudebr," "minsaudebrnews," and "saudechat." The word “Saude” translates from Portuguese as “Health!”

The group frequently looks to engage with members of its Telegram channel – even putting their next data leak up for a member poll. They also like to ‘tease’ information out – “Get

ready!!! Samsung data coming today.”



Lapsus\$ also likes to let people know when it has interested buyers. However, confirming this type of information is not always possible.



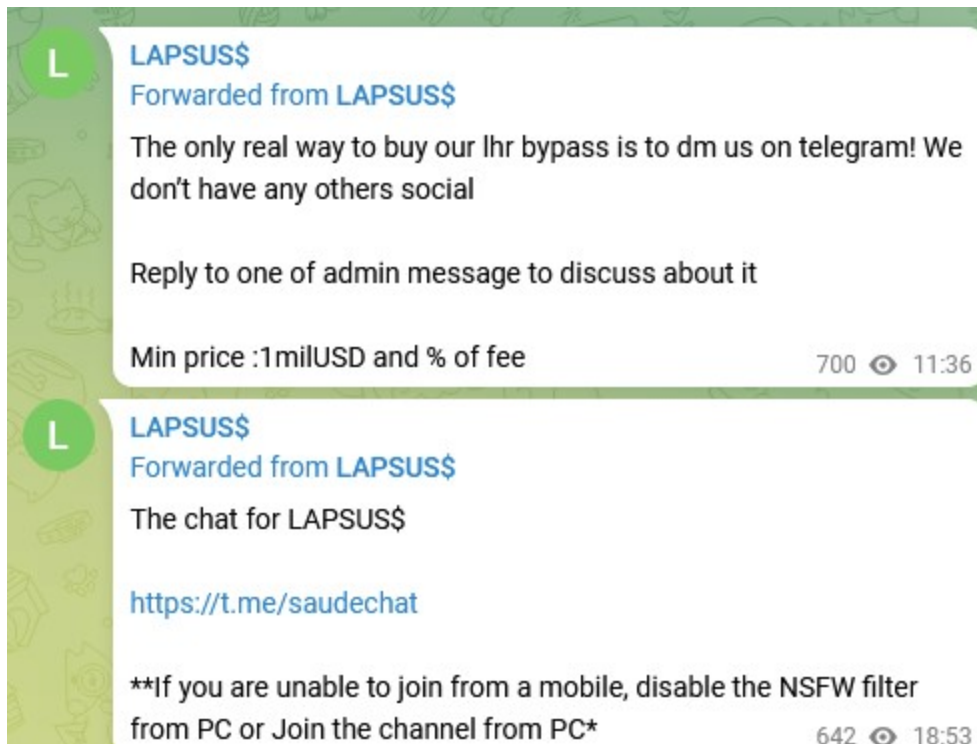
## Motivations: If Not Money, Hacker Clout?

At this time, it is not known whether Lapsus\$ has successfully monetized any of the attacks it has executed. There is a strong indication that money isn't the group's primary goal. Instead, it appears more preoccupied with being in the spotlight for its extortion tactics, and the group feels more like a modern incarnation of LulzSec than REvil.

However, some of the group's posts do imply that financial gain is a desired outcome, but at the same time it is not using the tactics of a traditional ransomware gang. The group does leverage extortion tactics in an effort to get what it wants. In one post, Lapsus\$ threatened to publicly release some of the data it claims to have exfiltrated from NVIDIA unless the company removed a feature known as LHR, short for "Lite Hash Rate," from its graphics cards – which blocks crypto mining on graphics cards – according to ARS Technica.

Lapsus\$'s demand for NVIDIA to remove mining restrictions from its hardware is likely more of an attempt to ingratiate themselves with the run-of-the-mill hacker and crypto community. Many in those communities see NVIDIA's restrictions as improperly leveraging its power to halt crypto-mining.

Trustwave SpiderLabs observed a post where Lapsus\$ advertised the sale of an LHR bypass for \$1 million. The unusually high price reflects the potential financial opportunities that an LHR bypass could provide to hackers who purchase the bypass, at least according to the group's statement.



The essentially public communication efforts made by Lapsus\$ are gaining the group headlines, but as we've seen with many similar groups in the past, a high profile also means a big target on your back.

But the threat of cyberattack from Russia could be the perfect diversion for groups like Lapsus\$ to continue to grow and execute successful attacks.

### **Lapsus\$ Offers to Pay Insiders for Access to Digital Supply Chain Leaders**

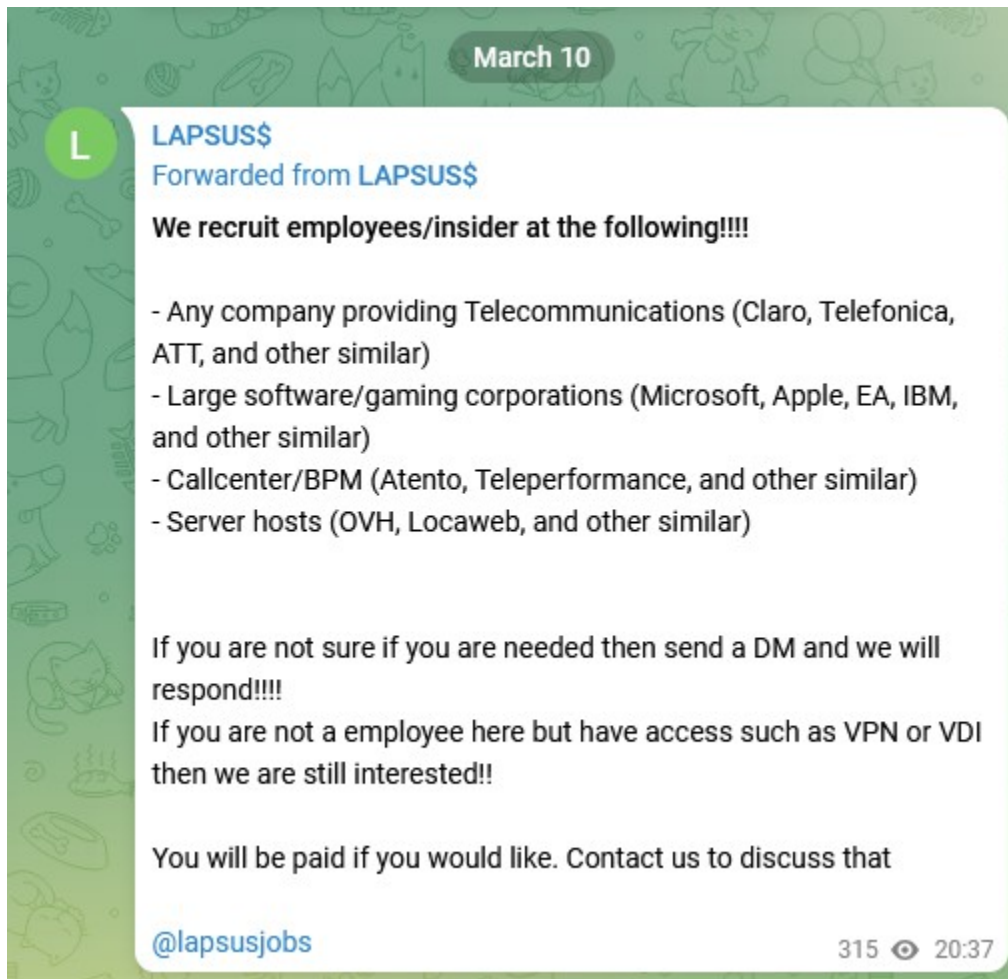
---

Another interesting tactic from Lapsus\$ is its very public call for insider assistance. To shortcut the process of obtaining VPN (virtual private network) and virtual desktop infrastructure (VDI) information needed to gain entry to its victims, the threat group simply posted a request on its Telegram channel stating it is willing to pay for access. The advertisement also indicated which organizations it may be targeting in the future.

Paying for insider information is a tried and trusted hacker tactic, and threat actors are often able to pay someone several times their usual salary for access.

In its advertisement Lapsus\$ said it was looking for employees from major technology organizations like Microsoft, Apple, IBM and Electronic Arts, alongside telcos such as Claro, Telefonica and AT&T, call centers and server hosts.

Of note, most of these organizations are deeply rooted in the digital supply chain.



In the end, it's hard to get a handle on how widespread the true insider threat is. Although having someone "on the inside" makes the process of gaining an initial foothold and performing reconnaissance easier, finding an insider that has the access you need, is IT savvy, and whom they can trust to risk it all to commit a crime could prove to be difficult.

## Tactics and Techniques Reportedly Used by Lapsus\$

Per Microsoft, the threat actors gain initial access using the following methods:

- Deploying the malicious Redline password stealer to obtain passwords and session tokens.
- Purchasing credentials and session tokens on underground criminal forums.
- Paying employees at targeted organizations (or suppliers/business partners) for access to credentials and MFA approval.
- Searching public code repositories for exposed credentials.

From that foothold, the group expands its access via virtual private network (VPN), remote desktop protocol (RDP), Virtual Desktop Infrastructure (VDI) including Citrix, or Identity providers (including Azure Active Directory and Okta) and collect high-valued data to use for extortion.

Microsoft has observed instances where the group successfully gained access to organizations through recruited employees.

According to Microsoft, once Lapsus\$ obtained access to the target network using the compromised account, it used multiple tactics to discover additional credentials or intrusion points to extend their access including:

- Exploiting unpatched vulnerabilities on internally accessible servers including JIRA, Gitlab, and Confluence
- Searching code repositories and collaboration platforms for exposed credentials and secrets.

Lapsus\$ has also been reported to use social engineering techniques via phone – reaching out to support centers at organizations in an attempt to reset a privileged account’s login credentials. They’ve reportedly answered common recovery prompts such as “first street you lived on” or “mother’s maiden name” to convince helpdesk personnel of authenticity.

Because helpdesks are frequently outsourced, this can be a weak point in supply chain security.

Overall, Lapsus\$ appears to be following a path that differs from conventional cyber gangs – opting for exfiltration, destruction and extortion techniques over ransomware.

As more organizations comment on their breaches, we likely will obtain more information.

## **Defend and Protect Against Lapsus\$ - Hardening the Digital Supply Chain**

---

If you’re an organization that provides software that is used at scale by numerous other organizations, you are part of the digital supply chain. These types of organizations need to remain extra vigilant during this time. The cyber fundamentals are especially critical during this time of Lapsus\$ and the threat of nation-state hackers.

Trustwave will continue to monitor the threat Lapsus\$ poses as more intel becomes available and respond accordingly for its clients.

Remember, threat actors – whether a hacker group or a nation-state affiliated – are always looking for the path of least resistance and companies that are susceptible to breach due to not executing the cyber basics.

## **Ensure your organization is executing these cyber fundamentals:**

---

- Operate under an assume-breach mindset.
- Ensure that cybersecurity/IT personnel focus on identifying, detecting, assessing and responding to any unexpected or unusual network behavior.

- Conduct proactive threat hunting to ensure unknown threats are not lurking within your environment.
- Conduct an asset audit focusing on assets that have external access; eliminate stale accounts and check privileged access.
- Conduct a third-party vendor / supply chain assessment. Focus on those places where third parties have access to your environment. Ensure no old entry points are left open.
- Institute multi-factor authentication (MFA) for internal and external users. Check that passwords are strong.
- Bring your workers to a higher state of alert, tell them to triple check links and attachments in emails before clicking to guard against phishing attacks.
- Deploy an effective endpoint detection and response (EDR) solution.
- Conduct crisis simulations to ensure all parts of your organization are prepared to respond to a major cyber event, not just IT staff.
- Reward employees for reporting if a suspicious contact reaches out asking for access

### **Tips to harden your defenses against potential insider threats:**

---

- Institute strong authentication and passwords measures; practice least-privileged access.
- Implement specific insider threat solutions: data loss prevention (DLP), user and entity behavior analysis (UEBA).
- Limit employee access to the minimum necessary and routinely review this access and make updates as roles change or people leave the company.
- Practice good encryption hygiene.
- Don't forget about physical security at the office (key cards, ID badges, unattended equipment, etc.).
- Ensure you have strong data access, use, and exfiltration policies in place.
- Routinely review software that is installed on employees' computers and look for unauthorized installations of software such as AnyDesk.
- Utilize an IDS or IPS (intrusion detection system, or intrusion prevention system) with anomaly detection features to detect if your employee is connecting remotely (or behaving oddly).
- Utilize database protection and monitoring tools to detect anomalies and flag suspicious activities or requests that violate policies.
- Work closely with your HR department to ensure there are culture policies in place that employee satisfaction doesn't deteriorate.