



| Flash |

Lapsus\$ Group Announces Resurgence

F-2026-09-18a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Threat Actor, Data Breach, Dark Web

September 18, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were *identified prior to 10:00 AM (EDT) on September 17, 2026*; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Lapsus\$ Group Announces Resurgence

| Key Findings

- On September 10, 2026, threat collective Lapsus\$ Group posted a message on its leak site declaring a "Chapter II" return from retirement and stating an intent to directly target the Federal Bureau of Investigation (FBI).
- The group's Chapter II announcement likely serves as an official declaration of its reactivated operations and likely indicates that fresh cyber offensive actions are already taking place.
- The leak site's "Upcoming Target" listing describes a global company generating more than USD 50 billion in annual revenue, with a countdown clock that showed roughly 10 days remaining as of the writing of this report.
- The Chapter II announcement very likely marks a genuine, ongoing resumption of Lapsus\$ Group's offensive operations and will likely garner substantial near-term media coverage given the collective's name reputation and recognition among security teams and the general public.

| Details

On September 10, 2026, threat collective Lapsus\$ Group posted a message on its leak site declaring a "Chapter II" return from retirement and stating an intent to directly target the FBI. This statement is paired with a leak site countdown clock referencing a new, as-yet-unnamed victim company the group describes as generating more than USB 50 billion in annual revenue.

- The message was PGP-signed by the group, which is typically done by threat collectives to dispel authenticity concerns. It is the same authenticity marker Lapsus\$ Group has used historically to validate its claims.¹ Despite this, there is a roughly even chance that the message is from a reorganized successor or an unrelated actor using a high-profile name.
- Lapsus\$ Group was part of the Scattered Lapsus\$ Hunters (SLH) alliance responsible for several prominent ransomware and digital extortion (R&DE) attacks and doxing campaigns targeting law enforcement last year. The group announced a temporary dissolution in October 2025 following law enforcement operations.

¹ [hXXps://lapsus\[.\]ar\[.\]io/](https://lapsus[.]ar[.]io/)

LAPSUS\$ GROUP

CHAPTER II

STATEMENT

DISCLOSED TARGETS & RECORDS

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

When we completed our first operations, we demonstrated the triviality of modern enterprise defense systems. To TeamPCP, we send our sincere gratitude: your sacrifice provided us with the exact coverage we needed. We owe you all our gratitude for falling and taking on the acts of our cooperation.

Retirement was only a temporary diversion born of pure boredom. Yet, driven by our enduring passion for the craft, we return not out of necessity, but to reclaim our dominance and for the love of the game. Our primary goal today is explicit: to openly challenge the FBI and the federal apparatus, proving once and for all that we operate completely above the law on this network. Corporate violations, corporate extortion and the generation of countless millions of dollars will continue unhindered, without any risk to ourselves, completely free.

Prepare your incident response units and alert your federal managers. The clock is active.
-----BEGIN PGP SIGNATURE-----

iJEEARYKADkWiQR9D6LIEuOYV2x5cQITHE/zjE2TawUCapgzNBsUgAAA
AAAEAASt
YW51MiwylJUrMS4xMiwylLDEACgkQEExP84xNk2tEswEAjB1VlcKyz6iDga
0jhtVY
bs+m5HaAgdlXFP6s9Ety0sBAJ1UO4S29mnj73OBh/0N926ON3KBq0fey
Psko/0
pKcE
=nNsE
-----END PGP SIGNATURE-----

VirtaHealth

DATA PUBLISHED

Virta Health is a digital health company focused on reversing type 2 diabetes and improving metabolic health through personalized nutrition and remote clinical care.

ACCESS ARCHIVE REPOSITORY

Upcoming Target

PENDING RELEASE

A global company generating over \$50 billion in annual revenue, with operations and a strong presence worldwide.

TIME REMAINING BEFORE PUBLIC RELEASE

10 11 59 21
DAYS HOURS MINUTES SECONDS

Lapsus\$ Group's statement on its leak site

Source: ZeroFox Intelligence

The group's Chapter II announcement likely serves as an official declaration of reactivated operations and likely indicates that fresh cyber offensive actions are already taking place. The statement frames the prior hiatus as a deliberate pause rather than a retreat forced by law enforcement pressure, while explicitly identifying U.S. federal law enforcement as a target of Lapsus\$ Group's renewed campaign.

The explicit focus on the FBI likely functions as a reputational and recruitment signal and increases the likelihood of retaliatory harassment or doxing campaigns directed at law enforcement personnel and their families. The tactic is a continuation of an observed pattern in which the collective's members and affiliated groups have used public taunting of investigators—very likely to draw attention and elevate their standing among their cybercriminal peers. Prior enforcement actions against individuals connected to Lapsus\$ Group have not ended the brand's activity, and its own framing treats those losses as the cost of doing business rather than a deterrent.

- Lapsus\$ Group's statement closes by addressing incident response teams and federal managers directly, extending its intended audience beyond a single victim organization.²
- Law enforcement in the United States, United Kingdom, and Brazil have previously arrested individuals tied to the collective, and the group's own post treats those losses as an acceptable operating cost.³
- The collective's public taunting of federal agencies mirrors tactics used by its affiliate groups since at least 2022, when members openly mocked corporate security teams during earlier campaigns.⁴

The Chapter II declaration demonstrates the group's persistence, as observed in the March 2026 claimed breach of French luxury retailer Lacoste SA by actors using the Lapsus\$ name, which compromised employee records and internal business systems roughly three years after the group's original wave of high-profile intrusions. That incident, and the broader history of extortion brands surviving arrests through splintering or the reactivation of dormant members, likely indicates that prior law enforcement action degraded the group's visibility, not its capability.

- The Lacoste breach, published March 1, 2026, compromised employee databases, CRM platforms, and SAP enterprise systems, though the full scope of affected records has not been publicly quantified to date.
- The Lacoste incident very likely indicates that the 2022–2023 arrests of several Lapsus\$ Group members were insufficient to permanently neutralize the operation, a conclusion the Chapter II announcement now reinforces directly.⁵

The collective paired its Chapter II statement with an active countdown clock toward a new disclosure, likely indicating the announcement reflects an operational restart already in progress. The pairing of a public statement with a live countdown clock mirrors a promotional pattern Lapsus\$ Group has used in the past to build anticipation ahead of a release.

² [hXXps://lapsus\[.\]ar\[.\]io/](https://lapsus[.]ar[.]io/)

³ [hXXps://www.gblock\[.\]app/articles/lapsus-return-lacoste-luxury-brand-ransomware](https://www.gblock[.]app/articles/lapsus-return-lacoste-luxury-brand-ransomware)

⁴ *Ibid.*

⁵ [hXXps://www.gblock\[.\]app/articles/lapsus-return-lacoste-luxury-brand-ransomware](https://www.gblock[.]app/articles/lapsus-return-lacoste-luxury-brand-ransomware)

- The site's "Upcoming Target" listing describes a global company generating more than USD 50 billion in annual revenue, with a countdown clock that showed roughly 10 days remaining as of the writing of this report.

The Chapter II announcement very likely marks a genuine, ongoing resumption of Lapsus\$ Group's offensive operations and will likely garner substantial near-term media coverage given the collective's name reputation and recognition among security teams and the general public. This likelihood is heightened by the group's established record of high-impact intrusions spanning the technology, telecommunications, and financial sectors. Furthermore, Lapsus\$ Group's explicitly stated plan to target the FBI significantly increases the likelihood of secondary campaigns by its affiliated groups or other cybercriminals targeting law enforcement.

Organizations in the sectors Lapsus\$ Group has previously targeted, along with any entities whose personnel could be impacted in law-enforcement-directed campaigns, should treat the collective's Chapter II announcement and countdown clock as an active rather than hypothetical threat. Heightened media traction is likely and consistent with Lapsus\$ Group's public profile, which is likely to amplify pressure on the collective's named or teased victims independent of the technical severity of any single intrusion.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	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.	Sources may use 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.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	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.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%