Subway Puts a LockBit Investigation on the Menu

By Tara Seals

Published: 2024-01-23 · Archived: 2026-04-06 00:07:56 UTC

Tara Seals,Managing Editor, News,Dark Reading

January 23, 2024

2 Min Read

Source: graham jepson via Alamy Stock Photo

The Subway restaurant chain, creator of the Sweet Onion Teriyaki combo and slinger of sports-themed fast-casual sandwich deals, is investigating claims that the LockBit 3.0 ransomware gang was able to toast up its infrastructure.

Last week, the infamous ransomware group claimed on its Tor leak site that it "exfiltrated [Subway's] SBS internal system, which includes hundreds of gigabytes of data and all financial aspects of the franchise, including employee salaries, franchise royalty payments, master franchise commission payments, restaurant turnovers etc."

LockBit claims that it will put the information up for sale on Feb. 2 unless the ransom is paid (the amount that the group is demanding is unknown).

For its part, Subway didn't unwrap what it thought about the claims until this week, when the company issued private statements to media that it's actively investigating LockBit's claims, but it has not yet provided any assessments or findings.

LockBit Hacks Fresh?

One thing's certain — going after such a big hoagie of a target is out of character for the LockBit gang, so, if true, the Subway hit could signal a change in its modus operandi.

"LockBit's recent claim of breaching Subway has raised eyebrows, but what's most interesting is that it's not their typical gig," says Ferhat Dikbiyik, head of research at the Black Kite cybersecurity firm. "Their average prey consists of companies with about $100 million in revenue, signaling that while they've taken a bite out of a billion-dollar brand [now], the majority of their targets are midsize or small."

The reason for the pivot could be the presentation of sheer opportunity, he adds: "An analysis of Subway with Black Kite's platform confirms issues similar to other major enterprises with large attack surfaces. Many are slow to patch and, as a result, face vulnerability exploitation, a tactic of ransomware groups like LockBit. We've seen this before with incidents like the Boeing breach via CitrixBleed."

Black Kite estimates that LockBit enjoyed about a fifth (21%) of global ransomware market share last year, claiming more than 1,000 victims. That's a number that dovetails with other estimates; a ransomware stats report this week from ZeroFox, for example, found that LockBit accounted for more than 35% of total extortion attacks in early 2023 — peaking at almost 50% last February and 20% in the fourth quarter.

ZeroFox recommends a range of best practices as a good LockBit defense as the gang potentially expands its menu of targets:

- Implement secure password policies and multifactor authentication.
- Configure ongoing monitoring for compromised account credentials.
- Proactively monitor for compromised accounts being brokered in deep and Dark Web forums.
- Back up critical, proprietary, or sensitive data to secure, off-site, or cloud servers.
- Implement network segmentation.
- Develop a comprehensive incident response playbook.
- Implement email protections like DMARC.
- Keep versions and patching up-to-date.

About the Author

Managing Editor, News, Dark Reading

Tara Seals has 20+ years of experience as a journalist, analyst and editor in the cybersecurity, communications and technology space. Prior to Dark Reading, Tara was Editor in Chief at Threatpost, and prior to that, the North American news lead for Infosecurity Magazine. She also spent 13 years working for Informa (formerly Virgo Publishing), as executive editor and editor-in-chief at publications focused on both the service provider and the enterprise arenas. A Texas native, she holds a B.A. from Columbia University, lives in Western Massachusetts with her family and is on a never-ending quest for good Mexican food in the Northeast.
