

T-Mobile denies new data breach rumors, points to authorized retailer

By [Lawrence Abrams](#)



September 22, 2023



11:05 AM



0



T-Mobile has denied suffering another data breach following Thursday night reports that a threat actor leaked a large database allegedly containing T-Mobile employees' data.

The mobile carrier told BleepingComputer that the leaked data is believed to belong to an authorized retailer, which was breached earlier this year.

"There has not been a T-Mobile data breach. The data being referred to online is believed to be related to an independently owned authorized retailer from their incident earlier this year. T-Mobile employee data was not exposed," T-Mobile told BleepingComputer.

Last night, someone under the alias 'emo' shared an 89 GB ZIP archive allegedly containing T-Mobile data on the BreachForums hacking forum for free.

While emo states in the post title that the breach is related to T-Mobile and Connectivity Source (a third-party T-Mobile authorized retailer), the post indicates that it was stolen from the cellular company.

"In April 2023 T-Mobile suffered a data breach exposing sales data/ analytics, T-Mobile support calls with customers, employee credentials, partial SSNs, email addresses and customer data," reads the forum post.

The screenshot shows a forum post on a dark-themed website. The post title is "(2023) T-Mobile | Connectivity Source" by user "emo" (profile picture of an anime girl), posted on Thursday, September 21, 2023, at 06:21 PM. The post content features a large pink T-Mobile logo, a credit to "doubl" for the breach, and a text-based sample of a CSV file containing employee data. The user's profile sidebar on the left shows 174 posts, 79 threads, joined in June 2023, and a reputation of 993.

(2023) T-Mobile | Connectivity Source
by emo - Thursday September 21, 2023 at 06:21 PM

5 hours ago

emo

boss

GOD

Posts: 174
Threads: 79
Joined: Jun 2023
Reputation: 993

Credit to doubl for this breach

In April 2023 T-Mobile suffered a data breach exposing sales data/ analytics, T-Mobile support calls with customers, employee credentials, partial SSNs, email addresses and customer data

Sample

```
head Paylocity/old/Paylocity_User_List_07032022.csv
"Row Level","Employee Id","Employee Status - Current","Hire Date - Current","Termination
Date - Current","Rehire Date","Job Title - Code - Current","Job Title - Name -
Current","Department - Code - Current","Department - Name - Current","E-mail","NT ID -
Text","Paycom ID - Text","Last Name","First Name","Middle Name","Name &
ID","SSN4","District","Region","Area"
0,"100004","T",07/06/2001,05/13/2022,, "OPSMGR", "REGIONAL OPERATIONS
```

Forum post claiming to share T-Mobile data

Source: *BleepingComputer*

The archive posted to the hacking forum contains a large amount of data, including employee IDs, employment status, hire dates, termination dates, rehire dates, job titles, department, names, last four digits of social security number, and email addresses.

The data also appears to contain information about customer orders and their plans.

Malware repository VX-Underground was first to share info on the data leak in tweets [1, 2] describing it as being the result of a T-Mobile breach.

"T-Mobile has been breached (again). Data has been exfiltrated and it is being shared online (again) This is T-Mobile's 8th breach since 2018," reads tweets from VX-Underground.

As T-Mobile is known in the cybersecurity community for its repeated data breaches, [suffering nine since 2018](#), with two already in 2023, it was easy to assume that it suffered another.

Likely linked to Connectivity Source breach

However, this data breach is believed to be related to Amtel, LLC, an authorized T-Mobile retailer doing business as the Connectivity Source brand, who warned of a breach earlier this year.

In May 2023, Amtel warned that they suffered a data breach on April 19th that allowed the attackers to steal data for current or former employees of the company.

"On April 19, 2023, Amtel was notified of suspicious activity in its network environment. Upon discovery of this incident, Amtel promptly engaged a specialized cybersecurity firm to secure its environment and to determine the nature and scope of the incident," reads the Amtel/Connectivity Source [data breach notification](#).

"While the investigation is ongoing, Amtel determined the incident involved limited personally identifiable information ("PII") the same day."

While it has not been confirmed if the data released on BreachForums is the same data breach disclosed by Amtel, the dates align, making it highly likely.

BleepingComputer contacted Connectivity Source about the publishing of its stolen data last night but did not receive a response to our email.

The good news is that this data does not contain customer data, and Amtel claims that only 17,835 current and former employees were impacted by the breach.

However, this data is still valuable for threat actors, who could send targeted phishing emails to Connectivity Source employees to gain access to support systems or perform SIM Swapping attacks.

Therefore, all Connectivity Source employees should be on the lookout for suspicious emails and confirm that they are legitimate before acting upon any of them.

BREACHFORUMS

CONNECTIVITY SOURCE

CYBERSECURITY

DATA BREACH

HACKING FORUM

T-MOBILE





LAWRENCE ABRAMS

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

[< PREVIOUS ARTICLE](#)

[NEXT ARTICLE >](#)