Hackers Likely Stole FBI Call Logs From AT&T That Could Compromise Informants

Lily Hay Newman ⋮ 4-5 minutes ⋮ 1/16/2025

The United States telecom giant AT&T disclosed a breach in July involving call and text messaging logs from six months in 2022 of “nearly all” its more than 100 million customers. In addition to exposing personal communication details for a slew of individual Americans, though, the FBI has been on alert that its agents’ call and text records were also included in the breach. A document seen and first reported by Bloomberg indicates that the bureau has been scrambling to mitigate any potential fallout that could lead to revelations about the identities of anonymous sources connected to investigations.

The breached data didn't include the content of calls and texts, but Bloomberg reports that it would have shown communication logs for agents' mobile numbers and other phone numbers they used during the six months period. It is unclear how widely the stolen data has spread, if at all. WIRED reported in July that after the hackers attempted to extort AT&T, the company paid $370,000 in an attempt to have the data trove deleted. In December, US investigators charged and arrested a suspect who reportedly was behind the entity that threatened to leak the stolen data.

The FBI tells WIRED in a statement: “The FBI continually adapts our operational and security practices as physical and digital threats evolve. The FBI has a solemn responsibility to protect the identity and safety of confidential human sources, who provide information every day that keeps the American people safe, often at risk to themselves.”

AT&T spokesperson Alex Byers says in a statement that the company “worked closely with law enforcement to mitigate impact to government operations” and appreciates the “thorough investigation” they conducted. “Given the increasing threat from cybercriminals and nation-state actors, we continue to increase investments in security as well as monitor and remediate our networks,” Byers adds.

The situation is surfacing amid ongoing revelations about a different hacking campaign perpetrated by China's Salt Typhoon espionage group, which compromised a slew of US telecoms, including AT&T. This separate situation exposed call and text logs for a smaller group of specific high-profile targets, and in some cases included recordings as well as information like location data.

As the US government has scrambled to respond, one recommendation from the FBI and the Cybersecurity and Infrastructure Security Agency has been for Americans to use end-to-end encrypted platforms—like Signal or WhatsApp—to communicate. Signal in particular stores almost no metadata about its customers and would not reveal which accounts have communicated with each other if it were breached. The suggestion was sound advice from a privacy perspective, but was very surprising given the US Justice Department's historic opposition to the use of end-to-end encryption. If the FBI has been grappling with the possibility that its own informants may have been exposed by a recent telecom breach, though, the about-face makes more sense.

If agents were following protocol for investigative communications strictly, though, the stolen AT&T call and text logs shouldn't pose a big threat, says former NSA hacker and Hunter Strategy vice president of research Jake Williams. Standard operating procedure should be designed to account for the possibility that call logs could be compromised, he says, and should require agents to communicate with sensitive sources using phone numbers that have never been linked to them or the US government. The FBI could be warning about the AT&T breach out of an abundance of caution, Williams says, or it may have discovered that agents' mistakes and protocol errors were captured in the stolen data. “This wouldn't be a counterintelligence issue unless someone was not following procedure,” he says.

Williams adds, too, that while the Salt Typhoon campaigns are only known to have impacted a relatively small group of people, they affected many telecoms, and the full impact of those breaches still may not be known.

“I worry about the FBI sources who might have been affected by this AT&T exposure, but more broadly the public still doesn't have a full understanding of the fallout of the Salt Typhoon campaigns,” Williams says. “And it seems that the US government is still working on getting a grasp of that as well.”