Hacker claims responsibility for T-Mobile attack, bashes the carrier's security

A person claiming to be behind the T-Mobile data breach that exposed almost 50 million people's info has come forward to reveal his identity and to criticize T-Mobile's security, according to a report by *The Wall Street Journal*. John Binns told the *WSJ* that he was behind the attack and provided evidence that he could access accounts associated with it, and he went into detail about how he was able to pull it off and why he did it.

According to Binns, he was able to get customer (and former customer) data from T-Mobile by scanning for unprotected routers. He found one, he told the *Journal*, which allowed him to access a Washington state data center that stored credentials for over 100 servers. He called the carrier's security "awful" and said that realizing how much data he had access to made him panic. According to the *WSJ*, it's unclear whether Binns was working alone, though he implied that he collaborated with others for at least part of the hack.

Binns called T-Mobile's security "awful"
The information the hacker gained access to includes sensitive personal data, like names, birthdates, and Social Security numbers, as well as important cellular data like identification numbers for cellphones and SIM cards. T-Mobile has said in a statement that it's "confident" that it's "closed off the access and egress points the bad actor used in the attack."

The *WSJ*'s report goes in depth into Binns' history as a

hacker. He claims that he got his start making cheats for popular video games and that he discovered the flaw that ended up being used in a botnet that attacked IoT devices (though he denies actually working on the code).

Binns describes a troubled relationship with US intelligence services

According to Binns, his relationship with US intelligence services is troubled, to say the least. A lawsuit that appears to have been filed by Binns in 2020 demands that the CIA, FBI, DOJ, and other agencies tell him what information they have on him. The lawsuit also accuses the government of, among other things, having an informant try to convince Binns to buy Stinger missiles on an FBI-owned website, attacking Binns with psychic and energy weapons, and even with being involved in his alleged kidnapping and torture. An FBI response to his lawsuit denied he was being investigated by the bureau for the botnet or having information related to the alleged surveillance, and abduction, and torture.

Binns told the *WSJ* that one of his goals behind the attack was to "generate noise," saying that he hopes someone in the FBI will leak information related to his alleged kidnapping. It's not likely that Binns' situation will be improved now that he's shone a spotlight on himself as the person who hacked one of the US's major carriers. However, if his reports about how he gained access to a vast trove of T-Mobile data are true, it paints a concerning picture of the carrier's security practices.

https://www.theverge.com/2021/8/26/22643277/t-mobile-hacker-data-leak-claims-responsibility-criticizes-security