Data Breach

T-Mobile

Security Data Breach

On August 17, 2021, T-Mobile learned that a bad actor illegally accessed and/or acquired personal data. The bad actor first gained access to T-Mobile systems on or before July 19, 2021. Our investigation is ongoing, but we have verified that a subset of T-Mobile data had been accessed and/or acquired by unauthorized individuals and the data stolen from our systems did include some personal information. The latest details about the affected data are available here.

The mobile service provider said in a statement that it had been investigating the data breach since last week, when it was "informed of claims made in an online forum that a bad actor had compromised T-Mobile systems."
The company said the stolen files included information from approximately 7.8 million current T-Mobile accounts, as well as records of more than 40 million former or prospective customers who had applied for credit with the company.

Some of the exposed data included customers' first and last names, social security numbers, driver's license and other information, T-Mobile said. It also included the PINs of about 850,000 active prepaid customers.

Timeline

T-Mobile Attack

1 **A cyberattack on T-Mobile exposed the information of more than 40 million people.**

2 Then located and immediately closed the access point that we believe was used to illegally gain entry to our servers.

3 Offering two years of free identity protection services with McAfee's ID Theft Protection Service to any person who believes they may be affected

4 Recommending that all eligible T-Mobile customers sign up for free scam-blocking protection through Scam Shield

5 Offering an extra step to protect your mobile account with our Account Takeover Protection capabilities for postpaid customers, which makes it harder for customer accounts to be fraudulently ported out and stolen.

6 Approximately 850,000 active T-Mobile prepaid customer names, phone numbers and account PINs were exposed. W

Vulnerabilities

The mobile operator revealed that the compromised data included full names, dates of birth, SSNs and driver's license/ID information for 7.8 million current T-Mobile postpaid customers as well as over 40 million former or prospective customers who had applied for credit with T-Mobile. No phone numbers, account numbers, PINs, passwords, or financial information were exposed for these users. However, names, phone numbers, and account PINs were exposed for 850,000 active T-Mobile prepaid customers.

SMS phishing
phishing attacks could be launched over SMS messages, impersonating the mobile operator. At first glance, in the case of the 48 million current, former, and prospective T-Mobile customers whose personal details were exposed.

SIM swapping
Another type of attack that is specific to phone users is SIM swapping. This is when an attacker manages to convince a mobile operator to associate a victim's phone number with a SIM card under their control to receive all their phone calls and text messages.

Victim profiles

The more breaches occur, the easier it is for attackers to build complete victim profiles and launch attacks that are increasingly hard to detect by both companies and users.

Costs

- The data breach could turn out to be a costly one for the mobile operator, as new research shows the average cost of a data breach has risen to more than $4.7m.
- T-Mobile US said 7.8 million postpaid service customer records were lifted by hackers. The data of about 850,000 prepaid customers was also hacked, as well as more than 40 million records of former or prospective customers.

Prevention

- T-Mobile is offering all impacted customers a free two-year subscription for McAfee's ID Theft Protection Service, which includes credit monitoring, full-service identity restoration, identity insurance, dark web monitoring, and more
- Business and postpaid customers can also enable T-Mobile's Account Takeover Protection service for free and all T-Mobile users can use the company's Scam Shield app that enables caller ID and automatically blocks calls flagged as scams.