Data Breach Case Study

T-Mobile

T-Mobile Security Breach

John Binns, a 21-year-old American attacked T-Mobile network on Aug 17, 2021 and stole their sensitive data. The evidence indicates that the bad actor first gained unauthorized access to a T-Mobile system on March 18, 2021. They had also verified that a subset of T-Mobile data had been accessed and/or acquired by unauthorized individuals and the data stolen from their systems did include some personal information.

Reference:

https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105

https://www.t-mobile.com/brand/data-breach-2021

T-Mobile US, Inc. (doing business under the global brand name T-Mobile) is an American wireless network operator partly owned by German telecommunications company Deutsche Telekom (DT), which has a 43.2% share. Its headquarters are located in Bellevue, Washington, in the Seattle metropolitan area, and Overland Park, Kansas, in the Kansas City metropolitan area. T-Mobile is the second-largest wireless carrier in the United States, with 106.9 million subscribers as of the end of Q3 2021.

The exact personal information impacted varies by individual. The types of impacted information include names, drivers' licenses, government identification numbers, Social Security numbers, dates of birth, T-Mobile prepaid PINs (which have already been reset to protect you), addresses and phone number(s). Social Security numbers and government identification numbers are collected in connection with prospective and current customers' application for services and eligibility determinations.

Timeline

T-Mobile Security Data Breach

1. **Sunday, August 15: Hackers claim to be selling 100 million stolen T-Mobile records on cybercrime forum**
2. Monday, August 16: T-Mobile confirms data breach and begins technical review of the incident
3. Tuesday, August 17: T-Mobile says data breach affected approximately 7.8 million current customers and 40 million records of former or prospective customers. Company takes steps to help protect individuals at risk from cyberattack
4. Wednesday, August 18: Security researcher Brian Krebs advises customers to follow T-Mobile advice and warns of follow-on phishing attacks
5. Friday, August 20: T-Mobile says another 5.3 million existing customers and 667,000 former customers affected by breach
6. Sunday, August 22: T-Mobile faces pair of lawsuits in wake of data breach
7. Thursday, August 26: 21-year-old American claims to be behind T-Mobile hack, criticizes "awful" security

Vulnerabilities

News broke on Vice.com of hackers claiming to have accessed data relating to over 100 million people, which they were offering sale. While the underground forum post did not mention T-Mobile specifically, a message to Motherboard confirmed that the information came from T-Mobile servers and included SSNs, phone numbers, names, physical addresses, IMEI numbers, and driver's license information. Motherboard confirmed this to be accurate.

Vulnerability #1

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.

Vulnerability #2

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.

Vulnerability #3

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 of T-Mobile turned out to be a costly one for the mobile operator up to $4.7m.
- A new research shows the average cost of a data breach can rise 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
- More than 40 million records of former or prospective customers.

Prevention

- Monitor your accounts for fraudulent activity. Most Americans don't keep close tabs on their checking and saving balance and don't examine every item on their credit card bill—and hackers count on that.
- Set up credit monitoring to ensure no one is using your personal information. T-Mobile has not yet offered any credit monitoring subscriptions to users. There are several third-party companies that will watch out for you, though, which don't charge an exorbitant amount.
- If you're especially worried about identity theft, consider a credit freeze, which prevents new credit from being issued without your direct permission.
- Keep an eye on other accounts, especially if you use a shared password for those and you've been the victim of a previous data breach.
- It's time to change your passwords again. Yes, it's a pain, but it's a critical step, especially if you're using the same password on multiple sites.