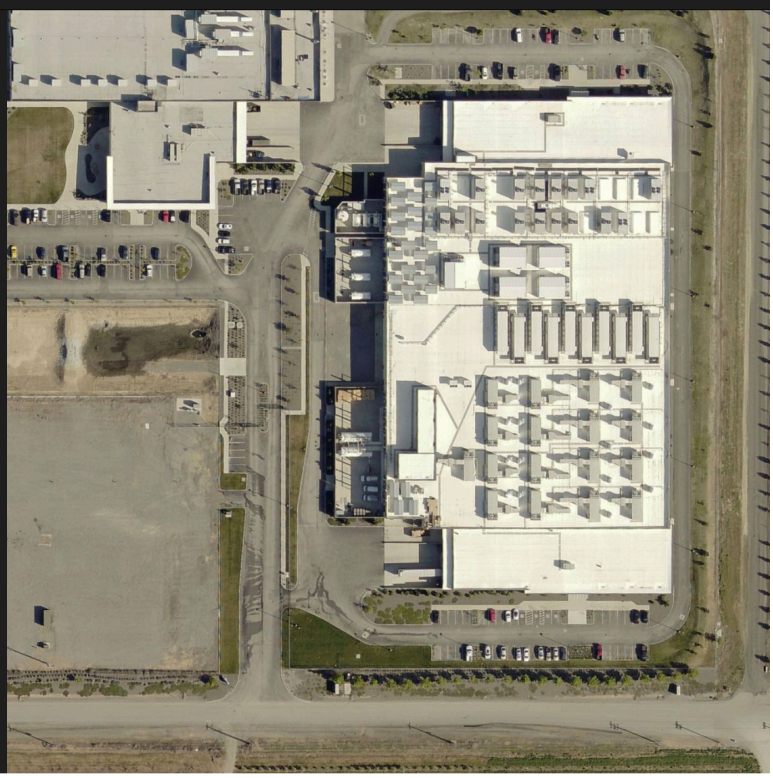
THE WALL STREET JOURNAL.

WSJ NEWS EXCLUSIVE

T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security Is Awful'

A 21-year-old American said he used an unprotected router to access millions of customer records in the mobile carrier's latest breach



John Binns was able to hack into T-Mobile's data center near East Wenatchee, Wash., where stored credentials allowed him access to more than 100 servers. PICTOMETRY

By Drew FitzGerald and Robert McMillan
Updated Aug. 27, 2021 6:36 pm ET

The hacker who is taking responsibility for breaking into T-Mobile US Inc.'s TMUS 0.58% ▲ systems said the wireless company's lax security eased his path into a cache of records with personal details on more than 50 million people and counting.

John Binns, a 21-year-old American who moved to Turkey a few years ago, told The Wall Street Journal he was behind the security breach. Mr. Binns, who since 2017 has used several online aliases, communicated with the Journal in Telegram messages from an account that discussed details of the hack before they were widely known.

The August intrusion was the latest in a string of high-profile breaches at U.S. companies that have allowed thieves to walk away with troves of personal details on consumers. A booming industry of cybersecurity consultants, software suppliers and incident-response teams have so far failed to turn the tide against hackers and identity thieves who fuel their businesses by tapping these deep reservoirs of stolen corporate data.

DATA BREACHES AND YOU

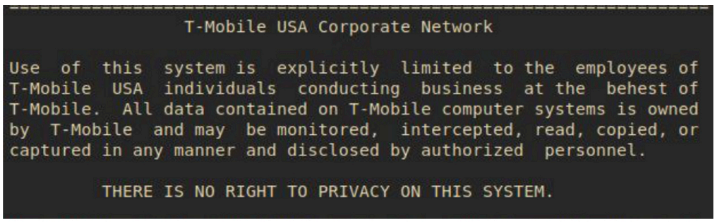
- T-Mobile Data Hack: What We Know and What You Need to Do

The breach is the third major customer data leak that T-Mobile has disclosed in the past two years. The Bellevue, Wash., company is the second-largest U.S. mobile carrier with roughly 90 million cellphones connecting to its networks.

The Seattle office of the Federal Bureau of Investigation is investigating the T-Mobile hack, according to a person familiar with the matter. "The FBI is aware of the incident and does not have any additional information at this time," the Seattle office said in a statement Wednesday.

In messages with the Journal, Mr. Binns said he managed to pierce T-Mobile's defenses after discovering in July an unprotected router exposed on the internet. He said he had been scanning T-Mobile's known internet addresses for weak spots using a simple tool available to the public.

The young hacker said he did it to gain attention. "Generating noise was one goal," he wrote. He declined to say whether he had sold any of the stolen data or whether he was paid to breach T-Mobile.



The 21-year-old hacker shared a screenshot of internal T-Mobile servers with warnings against unauthorized access.

Several cybersecurity experts said the public details of the hack and reports of previous T-Mobile breaches show the carrier's defenses need improvement. Many of the records reported stolen were from prospective clients or former customers long gone. "That to me does not sound like good data management practices," said Glenn Gerstell, a former general counsel for the National Security Agency.

Mr. Binns said he used that entry point to hack into the cellphone carrier's data center outside East Wenatchee, Wash., where stored credentials allowed him to access more than 100 servers.

"I was panicking because I had access to something big," he wrote. "Their security is awful."

He said it took about a week to burrow into the servers that contained personal data about the carrier's tens of millions of former and current customers, adding that the hack lifted troves of data around Aug. 4.

John Binns, who attended high school in northern Virginia, moved to Izmir, Turkey, with his Turkish mother when he was 18, a person familiar with the matter said.
PHOTO: UYGAR OZEL/ZUMA PRESS

On Aug. 13, the security research firm Unit221B LLC reported to T-Mobile that an account was attempting to sell T-Mobile customer data, according to the security firm. Two days later, T-Mobile publicly acknowledged it was investigating a potential breach.

T-Mobile confirmed that more than 50 million customer records have been stolen. The wireless carrier said it had repaired the security hole that enabled the breach. "We are confident that we have closed off the access and egress points the bad actor used in the attack," it said in a statement.

A T-Mobile spokeswoman declined to comment on specific claims by Mr. Binns or by cybersecurity experts.

On Friday, the day after this article was originally published, T-Mobile CEO Mike Sievert apologized to customers for the breach and said the wireless company was working to

strengthen its cyber defenses. “We didn’t live up to the expectations we have for ourselves to protect our customers,” Mr. Sievert wrote in a public letter.

For Mr. Binns, who uses the online names IRDev and v0rtex, among others, the T-Mobile hack represents a major development in a track record that has featured various exploits and—four years ago—peripheral involvement in the creation of a massive network of hacked devices that was used for online attacks.

Mr. Binns showed the Journal that he could access accounts linked to the IRDev online personality, which shared screenshots depicting access into T-Mobile’s network. He declined to be photographed but answered personal questions to confirm his identity as John Binns.

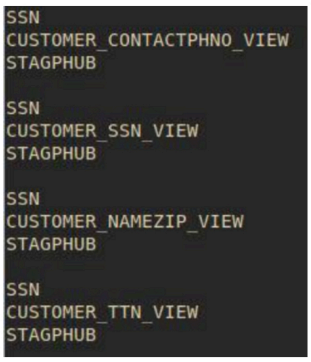
SHARE YOUR THOUGHTS

What will be the long-term impact of the T-Mobile hack? Join the conversation below.

In a statement, Unit221B said it believed the individual behind the IRDev alias was responsible for the T-Mobile hack because someone using this handle was reaching out to online criminals trying to sell the T-Mobile data before the hack had been made public.

It is unclear whether Mr. Binns worked alone. At one point in his communications with the Journal, he described a collaborative effort to find the login credentials needed to crack T-Mobile’s internal databases. Another online personality also offered in online forums to sell some of the stolen T-Mobile data.

Mr. Binns said he grew up in northern Virginia with his Turkish mother. His father died in 2002. when Mr. Binns was two years old, according to a newspaper article and a published obituary. He attended McLean High School in 2015 and 2016, according to the school’s yearbooks. He was estranged from his father’s family and moved with his mother to Izmir, Turkey, shortly after his 18th birthday, according to a person familiar with the matter.



John Binns shared tables of personal information that he said he found in the company’s internal systems.

He contacted a U.S. relative last year, claiming by telephone that he was a computer expert who had been kidnapped and taken to a hospital against his will, this person said. “He gushed about how he could do anything with a computer,” this person said.

In Telegram messages with the Journal, Mr. Binns repeated similar claims. He said he wanted to draw attention to his perceived persecution by U.S. government authorities. He described an alleged incident in which he claims he was abducted in Germany and put into a fake mental hospital.

“I have no reason to make up a fake kidnapping story and I’m hoping that someone within the FBI leaks information about that,” he wrote, explaining his reason for publicly discussing the hack.

Mr. Binns’s mother didn’t respond to phone calls and messages seeking comment. After the Journal reached out to her for comment, she took down her public Facebook page.

In 2020, Mr. Binns sued the Central Intelligence Agency, Federal Bureau of Investigation and other federal agencies to compel them to fulfill a federal records request he made for information about FBI investigations of botnet attacks. He didn’t use an attorney to file the complaint in the case, which is still active in the U.S. District Court for the District of Columbia. The agencies have denied his allegations in past court filings.

Security researchers said several online profiles tied to Mr. Binns were associated with groups of young gamers who have infected swarms of devices around the world. These botnets, as the infected device clusters are called, are often used by other gamers to knock people and websites offline.

T-Mobile's most recent breach is the third major customer-data leak that the company has disclosed in the past two years. A T-Mobile retail store in Arlington, Va.

PHOTO: CHIP SOMODEVILLA/GETTY IMAGES

Mike Benjamin, vice president of security for network operator Lumen Technologies Inc., said U.S. prosecutions in past years have limited the threat from these botnets, though network attacks have started growing in recent months. He said many young people, especially in the U.S. and Europe, first learn basic hacking techniques by sharing tricks and tactics with fellow gamers online.

"Online videogaming drives a natural competitiveness," Mr. Benjamin said. "Everybody's looking for that edge. That can reach into this area of outside of the videogame," where tactics end up "breaking the internet instead of just inside the rules of the game."

Mr. Binns told the Journal he first learned to find zero-days—previously undisclosed software flaws—by figuring out cheats for videogames such as "Minecraft," "Arma" and "DayZ." He said he found the zero-day that other hackers used to create Satori, a botnet-building virus that infects unprotected home routers, but denied writing any of the Satori code. "There are people who are way more skilled than I am," he wrote.

The August hack of T-Mobile stole an array of personal details from more than 54 million customers, according to the company's latest tally. Some customers had their names, Social Security numbers and birth dates exposed. Another batch of data included IMEI and IMSI numbers tied to users' phones, which other attackers could use as a starting point to take control of victims' phone lines.

T-Mobile last week started notifying affected customers. The company offered two years of identity-protection services and reminded customers to regularly update passwords and PIN codes as a standard precaution.

The carrier has suffered other data breaches before. The company notified customers of two separate breaches in 2020 that affected smaller sets of records. The company this year hired McDonald's Corp. executive Timothy Youngblood to oversee its cybersecurity measures. He succeeded longtime information security chief Bill Boni, who retired in June.

The Federal Communications Commission said it has launched a probe into the latest failure.

Past data-breach penalties have reached into the hundreds of millions of dollars. Equifax Inc. in 2019 reached a settlement with U.S. officials to resolve several investigations and lawsuits for $700 million. The credit-data provider generated $3.5 billion of revenue that year. T-Mobile had $68.4 billion of revenue in 2020.

A 2020 merger with Sprint Corp. made T-Mobile the U.S.'s second-largest mobile service provider, trailing only Verizon Communications Inc. T-Mobile executives have said they intend to keep growing by luring subscribers away from the competition.

"The upside for them from here is moving upmarket," said New Street Research analyst Jonathan Chaplin. "For the high-end customers that might've thought about moving over, this might be a signal that 'Hey, T-Mobile isn't Verizon yet.' This is totally unquantifiable, but to the extent that there's brand damage, that's where it will be felt."

Write to Drew FitzGerald at andrew.fitzgerald@wsj.com and Robert McMillan at Robert.Mcmillan@wsj.com

Appeared in the August 27, 2021, print edition as 'T-Mobile Hacker Found Weakness.'