kindred

Security Newsletter

23 Aug 2021

Subscribe to this newsletter

T-Mobile Faces Class Action Lawsuit Over Massive Data Breach

T-Mobile is facing a class action lawsuit for its most recent data breach, in which hackers stole data on at least 47 million current, former, and prospective customers, including Social Security Numbers, according to a copy of the class action complaint filed in a Washington court.

The move comes after Motherboard broke news of the breach on Sunday. At the time, a hacker was advertising 30 million SSNs from an unnamed source. Motherboard verified the data was sourced from T-Mobile; T-Mobile itself later confirmed the contours of the breach.

Beyond granting the plaintiffs an unspecified amount of damages, the class action asks the court to prohibit T-Mobile from keeping "personal identifying information on a cloud-based database."

Read More on Vice.com

T-Mobile's press release

More #News

- How 5 Years of DEF CON's Voting Village Has Shaped Election Security
- Chase bank accidentally leaked customer info to other customers
- Half of APAC firms bypass processes to accommodate remote work
- Secret terrorist watchlist with 2 million records exposed online
- Apple is bringing client-side scanning mainstream and the genie is out of the bottle
- World Bank Launches Global Cybersecurity Fund
- Malware campaign uses clever 'captcha' to bypass browser warning
- CISA shares guidance on how to prevent ransomware data breaches
- Social account thief goes to prison for stealing, trading nude photos
- Microsoft shares guidance on securing Windows 365 Cloud PCs
- Wanted: Disgruntled Employees to Deploy Ransomware

#Breach Log

- Hive ransomware attacks Memorial Health System, steals patient data
- Brazilian government discloses National Treasury ransomware attack
- Japanese insurer Tokio Marine discloses ransomware attack
- US Census Bureau hacked in January 2020 using Citrix exploit
- Microsoft Exchange servers being hacked by new LockFile ransomware

#Patch Time!

- Cisco won't fix zero-day RCE vulnerability in end-of-life VPN routers
- New unofficial Windows patch fixes more PetitPotam attack vectors
- CISA: BadAlloc impacts critical infrastructure using BlackBerry QNX

#Tech and #Tools

- Cloudflare thwarts 17.2M rps DDoS attack — the largest ever reported
- SNIcat: Circumventing the guardians
- Mandiant Discloses Critical Vulnerability Affecting Millions of IoT Devices
- macOS 11's hidden security improvements
- ShadowPad | A Masterpiece of Privately Sold Malware in Chinese Espionage
- Malicious PDF Generator
- Anti-Debug JS/WASM by Hand

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us