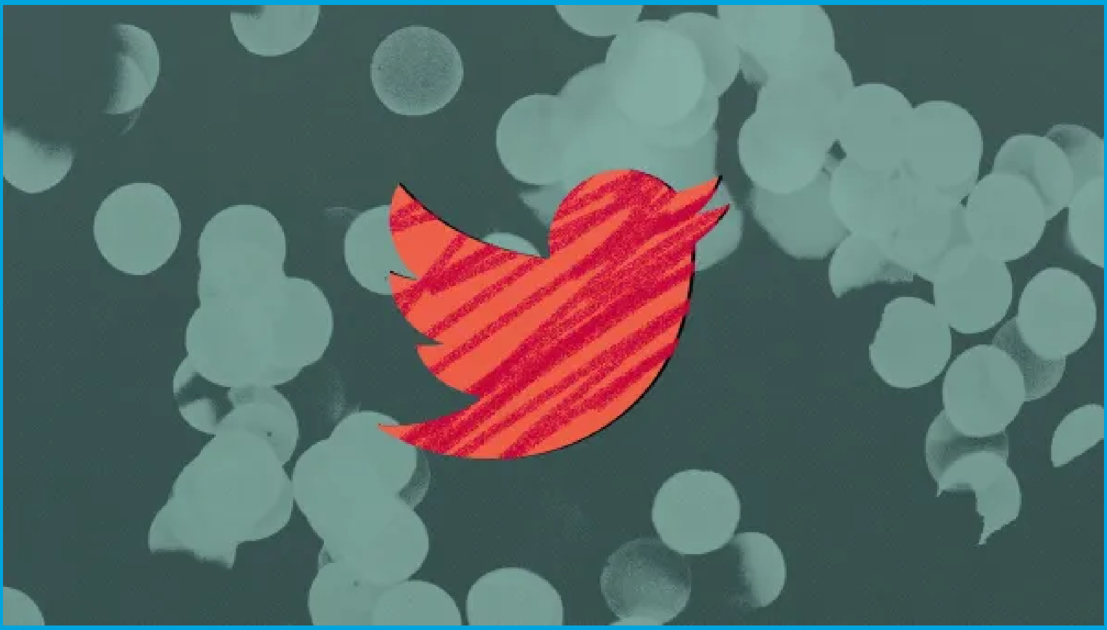
Security Newsletter

9 Jan 2023

Subscribe to this newsletter

What Twitter's 200 Million-User Email Leak Actually Means



AFTER REPORTS AT the end of 2022 that hackers were selling data stolen from 400 million Twitter users, researchers now say that a widely circulated trove of email addresses linked to about 200 million users is likely a refined version of the larger trove with duplicate entries removed. The social network has not yet commented on the massive exposure, but the cache of data clarifies the severity of the leak and who may be most at risk as a result of it.

From June 2021 until January 2022, there was a bug in a Twitter application programming interface, or API, that allowed attackers to submit contact information like email addresses and receive the associated Twitter account, if any, in return. Before it was patched, attackers exploited the flaw to "scrape" data from the social network. And while the bug didn't allow hackers to access passwords or other sensitive information like DMs, it did expose the connection between Twitter accounts, which are often pseudonymous, and the email addresses and phone numbers linked to them, potentially identifying users.

Read More

More #News

- Don’t Panic, but Slack’s GitHub Got Hacked
- Malicious PyPi packages create CloudFlare Tunnels to bypass firewalls
- Microsoft ends Windows 7 extended security updates on Tuesday
- Hackers push fake Pokemon NFT game to take over Windows devices

#Breach Log

- Air France and KLM notify customers of account hacks
- Malicious PyPi packages create CloudFlare Tunnels to bypass firewalls
- Devs urged to rotate secrets after CircleCI suffers breach

#Patch Time!

- Update Android Right Now to Fix a Scary Remote-Execution Flaw
- Microsoft ends Windows 7 extended security updates on Tuesday
- Zoom Whiteboard patches XSS bug
- Exploit drops for RCE bug in Control Web Panel

#Tech and #Tools

- WhatsApp Launches a Tool to Fight Internet Censorship
- Millions of Vehicles at Risk: API Vulnerabilities Uncovered in 16 Major Car Brands
- Hackers Can Abuse Visual Studio Marketplace to Target Developers with Malicious Extensions
- CORS for concern Tesla tackles misconfigurations that left internal networks vulnerable

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 more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 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