kindred

Security Newsletter

22 Aug 2022

Subscribe to this newsletter

How a Third-Party SMS Service Was Used to Take Over Signal Accounts

Last week, hackers broke into the systems of Twilio, a cloud communications company that provides infrastructure to other companies to automate sending text messages to their users. By breaking into Twilio systems hackers could read victims' text messages. This potentially gave the hackers a chance to take over any victim's accounts that were tied to their phone number on services that use Twilio.

Crucially, Twilio provides text verification services for the encrypted messaging app Signal. When a user registers their phone number with Signal, Twilio sends them an SMS containing a verification code, which they then input to Signal. On Monday, Signal, which uses Twilio for delivering text messages with verification codes, disclosed that it was one of the targets of this attack. In particular, Signal said that hackers targeted around 1,900 of its users. This means that for those users, the hackers could have registered their numbers on their own device and essentially impersonated them, or intercepted the SMS verification code that Signal uses to register users.

The good news: because of the way Signal is designed, even if a hacker registers their account with a victim's phone number, they don't get access to a lot of information.

Read More on Vice

More #News

- CISA adds 7 vulnerabilities to list of bugs exploited by hackers
- Russian APT29 hackers abuse Azure services to hack Microsoft 365 users
- Google blocks largest HTTPS DDoS attack 'reported to date'
- When Efforts to Contain a Data Breach Backfire
- Hyundai Uses Example Keys for Encryption System

#Breach Log

- LockBit claims ransomware attack on security giant Entrust, leaks data
- New MailChimp breach exposed DigitalOcean customer email addresses

#Patch Time!

- Apple releases Safari 15.6.1 to fix zero-day bug used in attacks
- Apple security updates fix 2 zero-days used to hack iPhones, Macs
- Google fixes fifth Chrome zero-day bug exploited this year
- Exploit out for critical Realtek flaw affecting many networking devices

#Tech and #Tools

- An encrypted ZIP file can have two correct passwords — here's why
- Back in Black: Unlocking a LockBit 3.0 Ransomware Attack
- Microsoft Sysmon can now block malicious EXEs from being created
- Wheel of Fortune Outcome Prediction – Taking the Luck out of Gambling
- "As Nasty as Dirty Pipe" — 8 Year Old Linux Kernel Vulnerability Uncovered
- iOS Privacy: Announcing InAppBrowser.com
- GraphQL Security Testing Without a Schema
- Cookie stealing: the new perimeter bypass

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