US recommends encrypted messaging as Chinese hackers linger in telecom networks

An unnamed FBI official was quoted in the same report as saying that phone users “would benefit from considering using a cellphone that automatically receives timely operating system updates, responsibly managed encryption, and phishing-resistant” multifactor authentication for email accounts, social media, and collaboration tools.

The FBI official reportedly said the hackers obtained metadata showing the numbers that phones called and when, the live phone calls of some specific targets, and information from systems that telcos use for court-ordered surveillance.

Despite recognizing the security benefits of encryption, US officials have for many years sought backdoors that would give the government access to encrypted communications. Supporters of end-to-end encryption have pointed out that backdoors can also be used by criminal hackers and other nation-states.

“For years, the security community has pushed back against these backdoors, pointing out that the technical capability cannot differentiate between good guys and bad guys,” cryptographer Bruce Schneier wrote after the Chinese hacking of telecom networks was reported in October.

Noting the apparent hacking of systems for court-ordered wiretap requests, Schneier called it “one more example of a backdoor access mechanism being targeted by the ‘wrong’ eavesdroppers.”

1994 surveillance law in focus

CISA issued a statement on the Chinese hacking campaign in mid-November. It said:

> *The US government's continued investigation into the People's Republic of China (PRC) targeting of commercial telecommunications infrastructure has revealed a broad and significant cyber espionage campaign.*
>
> *Specifically, we have identified that PRC-affiliated actors have compromised networks at multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain information that was subject to US law enforcement requests pursuant to court orders.*

The hacks raise concerns about surveillance capabilities required by a 1994 law, the Communications Assistance for Law Enforcement Act (CALEA), which requires "telecommunications carriers and manufacturers of telecommunications equipment design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for information."

https://arstechnica.com/tech-policy/2024/12/us-recommends-encrypted-messaging-as-chinese-hackers-linger-in-telecom-networks/