After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

By Iain Thomson

Published: 2017-05-03 · Archived: 2026-04-06 01:11:33 UTC

Experts have been warning for years about security blunders in the Signaling System 7 protocol – the magic glue used by cellphone networks to communicate with each other.

These shortcomings can be potentially abused to, for example, redirect people's calls and text messages to miscreants' devices. Now we've seen the first case of crooks exploiting the design flaws to line their pockets with victims' cash.

O2-Telefonica in Germany has confirmed to Süddeutsche Zeitung that some of its customers have had their bank accounts drained using a two-stage attack that exploits SS7.

In other words, thieves exploited SS7 to intercept two-factor authentication codes sent to online banking customers, allowing them to empty their accounts. The thefts occurred over the past few months, according to multiple sources.

In 2014, researchers demonstrated that SS7, which was created in the 1980s by telcos to allow cellular and some landline networks to interconnect and exchange data, is fundamentally flawed. Someone with internal access to a telco – such as a hacker or a corrupt employee – can get access to any other carrier's backend in the world, via SS7, to track a phone's location, read or redirect messages, and even listen to calls.

In this case, the attackers exploited a two-factor authentication system of transaction authentication numbers used by German banks. Online banking customers need to get a code sent to their phone before funds are transferred between accounts.

The hackers first spammed out malware to victims' computers, which collected the bank account balance, login details and passwords for their accounts, along with their mobile number. Then they purchased access to a rogue telecommunications provider and set up a redirect for the victim's mobile phone number to a handset controlled by the attackers.

Next, usually in the middle of the night when the mark was asleep, the attackers logged into their online bank accounts and transferred money out. When the transaction numbers were sent they were routed to the criminals, who then finalized the transaction.

While security experts have been warning about just this kind of attack – and politicians have increasingly been making noise about it – the telcos have been glacial at getting to grips with the problem. The prevailing view has been that you'd need a telco to pull off an assault, and what kind of dastardly firm would let itself be used in that way.

That may have worked in the 1980s, but these days almost anyone can set themselves up as a telco, or buy access to the backend of one. To make matters worse the proposed replacement for SS7 on 5G networks, dubbed the Diameter protocol, also has security holes, according to the Communications Security, Reliability and Interoperability Council at America's comms watchdog, the FCC.

This first publicly confirmed attack will hopefully ginger up efforts to fix issues with SS7, at least in Europe, where Germany has a leadership position. As for the US, it might take a series of SS7 assaults before the telcos get their backsides into gear. ®

PS: *A US Department of Homeland Security report this month admitted SS7 "can be exploited by criminals, terrorists, and nation-state actors/foreign intelligence organizations" to hijack messages and calls.*

Basically, it's time to stop using SMS for two-factor authentication for sensitive stuff.
