The Register®
Biting the hand that feeds IT

Security

10

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

O2 in Germany confirms online thefts from sour krauts□

3 May 2017 at 20:02, Iain Thomson

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.

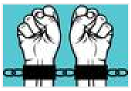
The hackers first spammed out malware to victims' computers, which collected the bank□ account balance, login details and passwords for their accounts, along with their mobile

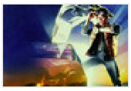
Most read

Windows 10 S: Good, bad, and how this could get ugly for PC makers

Microsoft sparks new war with Google with, er, $999+ lappies for kids

Forgetful ZX Spectrum reboot firm loses control□ of its web domains


Welsh Linux Mint terror nerd jailed for 8 years


Post Unity 8 Ubuntu shock? Relax, Linux has been here before

Spotlight

3D printing and drones are the tech del día at Spanish startup fiesta□

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. ®

Tips and corrections

10 Comments

Sign up to our Newsletter

Get IT in your inbox daily

Subscribe

More from The Register

Hey FCC, when you're not busy screwing our privacy, how about those SS7 cell network security flaws, huh?□

No one else seems to care, sniff politicians

8 Comments

Why are creepy SS7 cellphone spying flaws□ still unfixed after years,□ ask Congresscritters

And why won't the NSA open up about Section 702 spying?

25 Comments

Oracle patches Solaris 10 hole exploited by NSA spyware tool – and 298 other security bugs

Mega load of updates lands for tons of Big Red gear

13 Comments

Mac OS IM tool Adium lagging on library security vulnerability

`libpurple` is a 'binary blob of unknown provenance' says researcher

3 Comments

SS7 spookery on the cheap allows hackers to impersonate mobile chat subscribers

WhatsApp, Telegram secure - but the transport isn't

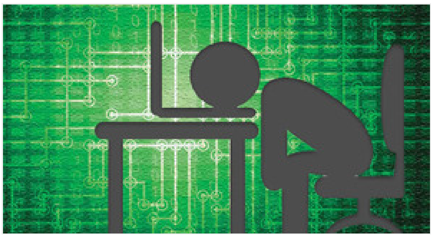
11 Comments

Dormant Linux kernel vulnerability finally□ slayed

Just, er, eight years later

43 Comments

Speaking in Tech: Hacking Microsoft Windows? That's cute



Machine vs. machine battle has begun to de-fraud the internet of lies

Security co-operation unlikely to change post Brexit, despite threats

More fun in the sandbox: Experts praise security improvements to Edge

UK vuln 'fessing pilot's great but who's going to give a FoI?

MAC randomization: A massive failure that leaves iPhones, Android mobes open to tracking

Next Generation Security: No, Dorothy, there is no magic wand

Whitepapers

Sponsored links

About us

- Who we are
- Under the hood
- Contact us
- Advertise with us

More content

- Week’s headlines
- Top 20 stories
- Alerts
- Whitepapers

Situation Publishing

- The Next Platform
- Continuous Lifecycle London
- M-cubed
- Webinars

Sign up to our Newsletters

Join our daily or weekly newsletters, subscribe to a specific section or set□
News alerts

Subscribe

SITUATION PUBLISHING

The Register - Independent news, views and opinion for the tech sector. Part of Situation Publishing

Mobile website

Cookies Privacy Ts&Cs