



DATA CENTRE

SOFTWARE

SECURITY

TRANSFORMATION

DEVOPS

BUSINESS

PERSONAL TECH

SCIENCE

EMERGENT TECH

BOOTNOTES



Security

40

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

O2 confirms online thefts using stolen 2FA SMS codes

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 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

Most read



Oracle: You've got such strong arms, Mr Pai. Oh, hello, Donald! We didn't see you there



Amazing new boffinry breakthrough: Robots are eating our brains



Russian RATs bite Handbrake OSX download mirror



Dell patches AMT-vulnerable systems



IBM: Remote working is great! (for everyone except us)

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. ®

Sponsored: [Continuous lifecycle London 2017 event](#). [DevOps, continuous delivery and containerisation](#). [Register now](#)

Tips and corrections

40 Comments

Sign up to our Newsletter

Get IT in your inbox daily

[Subscribe](#)

More from The Register



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



Dormant Linux kernel vulnerability finally slayed

Just, er, eight years later

43 Comments



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



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



'Amnesia' IoT botnet feasts on year-old unpatched vulnerability

New variant of 'Tsunami' is a disaster waiting to happen

12 Comments



WhatsApp blind-sided by booby-trapped photo vulnerability

Same issue in Telegram, says researcher

14 Comments



CIA hacking dossier leak reignites debate over vulnerability disclosure

Spy agencies more interested in stockpiling bugs than closing the gaps

21 Comments



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?

Whitepapers



Critical security and compliance considerations for hybrid cloud deployments

The need for greater business agility and overall cost-containment pressures are the twin-turbo drivers behind the growing adoption of hybrid cloud.

The Register uses cookies. [Find out more](#) [Close](#)



Emerging technologies and an evolving, digitally-reliant consumer base have left retailers scrambling to maintain a competitive edge.



Harness the Power of the Cloud

With NICE WFM in the Cloud, you can leave the infrastructure, management and maintenance of your workforce management solution to them.



Veracode Secure Development Survey

As developers and development managers, you're seeing this paradigm shift in real time.



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



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

Sponsored links

[Call for contributions: the only UK conference for cyber security & functional safety engineers](#)

[Advanced Threat Prevention. Visit The Register's Endpoint Security Hub](#)

[Get The Register's Headlines in your inbox daily - quick signup!](#)

[Continuous lifecycle London 2017. DevOps, continuous delivery and containerisation. Register now](#)

[M3: Minds Mastering Machines. The ML & AI conference. Register now](#)

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



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