Blog Post (Sinch)

Protecting your network from Simjacker with Sinch

You may have heard of "Simjacker". It's a software exploit capable of hacking cell phone SIM cards. AdaptiveMobile Security discovered and named the exploit last week, highlighting a vulnerability that's been a growing threat to telecom network security for some time now.

Simjacker attacks take place via text messages that contain hidden SMS toolkit (STK) instructions. STK instructions are an old technology once used by operators to push updates and trigger value added services, but Simjacker ups the ante by instructing a victim's device to secretly share its location and sensitive data. And because they are SIM-based, these attacks can affect more than just phones – they can cause widespread disruption by compromising billions of SIM-enabled IoT devices.

What's interesting – if a bit unnerving – about Simjacker is that it represents a more complex attack on telecom network security than those already defined by the GSMA. That explains why you've seen headlines where Simjacker is coupled with words like "state surveillance" and "espionage", but it doesn't mean we aren't prepared for it. Simjacker is exactly the type of attack we watch for at Sinch and we work alongside the community of researchers and security experts like AdaptiveMobile to tackle state-of-the-art signaling threats.

It can be alarming to see bad actors exploiting network vulnerabilities outside of test environments, especially when allegations extend to state players and private companies, but one silver lining is that these types of attacks are now getting the attention they deserve. More and more operators are being spurred into action to provide safer networks for their customers.

How to safeguard your network against Simjacker (and other threats)

The good news is that there are solutions available to protect your network against Simjacker and other next generation threats. The best defense against attacks on your network and subscribers is to put up both a Signaling Firewall and an SMS Firewall with deep filtering capability. Read our white paper Signaling Threats: SS7 and Beyond to learn more about the risks that exist in mobile networks and how the global mobile network can be made safer for everyone.

Related Social Media Posts (Sample)

Twitter
We've been reading up on Simjacker, a new software exploit that targets SIM cards. Sinch helps protect networks and people from this type of threat. More here: [link]

LinkedIn
We're grateful to see AdaptiveMobile Security bringing Simjacker out of the shadows. Sinch works hard to ensure that networks and cell phones are protected from software exploits of all types, and we keep up by developing cutting-edge solutions. Jump to our blog to learn more about Simjacker and how you can safeguard your network and those who use it every day.