Bank Account Hack and SS7 Exploits get Real

The Inevitable Finally Happened: Bank Account Hack and SS7 Exploits get Real

Hackers have finally found a way to get into consumers' pockets by exploiting the SS7 network and stealing two-factor authentication (2FA) SMS codes to empty people's bank accounts.

Engineers spoke out with a warning to possible risks of the security of Signaling System Number Seven, or SS7 as far back as 2008. This widely-used protocol, that allows networks to interconnect and exchange data has loopholes, that, if left unprotected, can be wide open to the unrelenting hacks of cyber-criminals including listening in on conversations, monitoring messages, hijacking subscriber locations and stealing money!

Back in 2014, when German researchers first publicly reported that SS7 was vulnerable to exploitation and that it had been used for surveillance purposes, this was a more abstract problem that only seemed to affect those who were on government security watch lists, but now the threat is close to us all.

Mavenir leaders - Mark Windle and Ilia Abramov shared the following insights with the media:

1. SS7 is Vulnerable: What Next?

Mark Windle, Director at Mavenir, commented to CyberScoop that, "This latest attack serves as a warning to the mobile community about what is at stake if these loopholes aren't closed, and provides a rallying-cry to mobile carriers to act fast and work with vendors to protect their customers and their networks."

Windle also told eSecurity Planet's Jeff Goldman, "Operators are already collaborating to better understand the ways in which vulnerabilities can be exploited, and mitigate them." This critical collaboration must be done rapidly and in an organized manner, because legacy SS7 technology will be replaced by Diameter or SIP in the next ten years."

And that, "Furthermore, as long as there is national and international interconnect access, the window for hacking will still be there. In the meantime, by continuing to address security flaws in signaling protocols by using an optimal, multi-layer solution, operators can increase subscriber trust levels, decrease churn rates and, most importantly, protect mobile devices." Windle expanded on his commentary in a byline for Wireless Week entitled, "SS7 Vulnerability Allows Hackers to Drain Bank Accounts – What Next?"

2. What Should CSPs Do?

Ilia Abramov, Mavenir Product Director, advised Help Net Security that "CSPs and those involved in authentication should increase their investment in this security method by upgrading existing systems with further measures."

He continued, "If mobile operators want to defend their role in enterprise Application to Person (A2P) communications, it is imperative that action is taken now to secure the SMS channel, (and the network more generally) before lucrative A2P messaging is put at risk."

For CSPs looking to take precautions against SS7 hacks, Abramov recommends a dual-step approach: first, installing a signaling firewall as a first step and conducting regular audits to analyze networks for gaps. The second step is the key to defending against a dynamic threat landscape.

For more information on how to protect networks and customers' information, read more about our solutions here.