PRESS RELEASE

Stockholm, Sweden
July 22, 2021

AdaptiveMobile Security Highlights the Need to Protect Mobile Subscribers Against Spyware

This week the findings from the “Pegasus Project” revealed widespread abuse of mobile phone hacking spyware from a company identified as NSO Group. The implications are far reaching and severe, impacting the integrity of personal communication and national telecommunication infrastructure: the mobile phone spyware is capable of extracting stored data and spying on individual mobile devices. The revelations highlight the need for solutions from specialists like AdaptiveMobile Security to protect against mobile cyber threats.

Cyber-attacks and cyber surveillance are growing at a fast pace and have evolved to use a combination of different techniques to achieve their goals. In particular, surveillance platforms are powerful tools capable of manipulating mobile network signalling protocols, modifying service profiles, and introducing malware onto mobile devices. As an example, AdaptiveMobile Security previously developed effective protection against the Simjacker “zeroday” vulnerability which left more than one billion mobile phones exposed worldwide.

“This latest revelation is a stark reminder that mobile network security has never been more critical to ensure the integrity of personal communication and national telecom infrastructure,” says Brian Collins, Senior Vice President of AdaptiveMobile Security, an Enea company. “We remain committed to relentlessly securing mobile operators, governments and regulators against these cyber threats.”

The AdaptiveMobile Security Signalling Protection Platform and Signalling Intelligence Services have been deployed by mobile network providers and governments to protect subscribers from surveillance and service fraud by providing real-time protection from many of the techniques used by spying platforms.

More information about Pegasus spyware: https://en.wikipedia.org/wiki/Pegasus_(spyware)

More information about Simjacker: https://simjacker.com/

More information about NSO Pegasus and HLR Lookups: https://blog.adaptivemobile.com/nso-pegasus-and-hlr-lookups.

Enea AB, P.O. Box 1033
164 21 Kista

Phone: +46 8 507 140 00
Fax: +46 8 507 140 40

E-mail: info@enea.com
Website: www.enea.com

PRESS RELEASE

Contact

Erik Larsson, Senior Vice President Marketing
E-mail: erik.larsson@enea.com

About AdaptiveMobile Security

AdaptiveMobile Security, an Enea company, is a world leader in mobile network security, protecting more than 2.2 billion subscribers worldwide. With deep expertise and a unique focus on network security, AdaptiveMobile Security award-winning innovative security solutions and services provide its customers with advanced threat detection, response, and actionable intelligence, combined with the most comprehensive security product-set in the market today, predicting and protecting against multiprotocol mobile security attacks.

AdaptiveMobile Security provides its customers with the unique combination of technology, analyst input and intelligence to ensure their subscribers, data and networks remain protected from cyber warfare.

AdaptiveMobile Security was founded in 2006 and counts some of the world's largest carriers, Governments and Regulators as customers. The Company is headquartered in Dublin with offices in North America, Europe, South Africa, the Middle East, and Asia Pacific region.

About Enea

Enea is one of the world's leading specialists in software for telecommunications and cybersecurity. The company's cloud-native products are used to enable services for mobile subscribers, enterprise customers, and the Internet of Things. More than 3 billion people rely on Enea technologies in their daily lives.

Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm.

For more information: www.enea.com