PRESS RELEASE

Stockholm, Sweden
February 14, 2024

A2P Messaging Under Threat: Joint Report By Enea and Mobilesquared Reveals 20 Billion Fraudulent Messages Sent In 2023

Investigation into Artificial Inflation of Traffic (AIT) confirms 4.8% of global messaging traffic is fraudulent, putting strain on the widely used application-to-person (A2P) messaging ecosystem

A new report co-authored by Enea and messaging intelligence specialist Mobilesquared has revealed that Artificial Inflation of Traffic (AIT) is now so pervasive in the messaging ecosystem that between 19.8 billion and 35.7 billion fraudulent messages were sent in 2023. The study also underscores the substantial financial toll of AIT, with brands incurring costs of $1.16 billion due to fraudulent messages.

Artificial Inflation of Traffic (AIT) represents a critical challenge within the messaging ecosystem. AIT involves the generation of fraudulent A2P (Application-to-Person) SMS traffic through various deceptive methods, such as bots and counterfeit messaging. This practice not only leads to financial losses for many of those in the message ecosystem it also undermines the integrity of mobile messaging for brands' communication with their customers. AIT fraudulent messages now account for a notable portion of total international traffic (4.8%), eroding trust and reliability in SMS services. This family of fraud types is prompting major brands to shift away from SMS to alternative communication channels, thereby threatening the viability and profitability of the entire messaging ecosystem.

Despite the significant impact that AIT is having on the A2P SMS industry, there is still no consistent or comprehensive definition for AIT or detailed descriptions of the various methods that threat actors deploy. This is a major obstacle to understanding and combating AIT. Based on its own threat intelligence in combination with industry sources, Enea has identified a taxonomy of six different AIT abuses, covering AIT injected into the message path at brands, CPaaS providers, and aggregators. These six AIT types and their estimated market impacts are detailed in this report.

In an effort to quantify the problem, Enea has worked with Mobilesquared to highlight the full impact AIT is having across the industry. According to the report, the three AIT attack types having the greatest impact on the market are:

- **Counterfeit Fabrication AIT:** traffic injected in transit by aggregators.
- **Amplification bot Generation of AIT:** traffic created by triggering one-time-passwords and other message-generating triggers at brand websites and services.

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

- **Masquerade Parasite Generation of AIT:** traffic injected through accounts created at CPaaS providers.

The report argues that understanding the various types of AIT is crucial for developing effective strategies to combat this threat in the messaging ecosystem.

“Understanding the profound impact of AIT on A2P messaging is essential for safeguarding the integrity of our A2P communication ecosystems," said Simeon Coney, VP of Business Development at Enea. "AIT not only inflicts significant financial damage but also erodes trust in A2P messaging platforms, a cornerstone for brand-consumer interactions. Our report highlights the urgent need for a unified industry response to accurately define and tackle these deceptive practices.”

Coney continued, “It's imperative that all stakeholders in the messaging ecosystem — from mobile operators to CPaaS and aggregators — collaborate closely to measure the impact of these AIT frauds, develop and deploy robust solutions that can effectively identify sources and mitigate AIT threats. At Enea, we contribute to this work by offering a range of effective countermeasures to AIT in the Enea Adaptive Messaging Firewall, and we continue to invest in our capabilities to protect our customers in the A2P path.”

Nick Lane, chief messaging officer at Mobilesquared said: "The Pandemic accelerated brand adoption of SMS, but the rise of AIT, and the abuse of brand-spend relating to authentication and one-time passwords in particular, will set the A2P SMS industry back years, if indeed it will ever recover from the turbulence it has experienced over the last 12 months. This should not be the case as brands continually tell us that SMS remains the best channel. As an industry, we just need to find improved and enhanced methods of protecting it."

To download the full report and learn more, please visit info.enea.com/ait.

Contact

Stephanie Huf, Chief Marketing Officer
E-mail: stephanie.huf@enea.com

About Enea

Enea is a world-leading specialist in software for telecom and cybersecurity. The company's cloud-native solutions connect, optimize, and secure services for fixed and mobile subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day.

PRESS RELEASE

Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security.

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

For more information: www.enea.com

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