Is Your Cloud Provider Using Encrypted Communications Between Their Data Centers? *How Would You Know?*

From Wired: "Satellites Are Leaking the World's Secrets: Calls, Texts, Military and Corporate Data"

URL: https://archive.ph/2025.10.14-100340/https://www.wired.com/story/satellites-are-leaking-the-worlds-secrets-calls-texts-military-and-corporate-data/)

Published: October 13, 2025

Situation

The adoption of satellite communications by governments, corporations, and data centers comes with a significant data security vulnerability. Geostationary satellites constantly beam proprietary data, including consumer calls, texts, corporate information, and military communications. An October 13th, 2025, article in **Wired** magazine by Andy Greenbuer and Matt Bergess points out that many signals lack encryption, making them vulnerable to interception. Researchers from UC San Diego and the University of Maryland highlighted this issue after discovering that roughly half of the over 1500 geostationary satellites they scanned (about 15% of the total satellites in service) transmitted unencrypted data, which could be easily intercepted with low-cost, readily available equipment.

Task: The researcher's goal was to determine if they could use affordable and straightforward commercial hardware to access the data and ascertain whether it was proprietary or sensitive data for the military, government, or corporations. They planned to examine a large set of satellite feeds to determine if sensitive military and industrial communications could be easily intercepted, thereby uncovering encryption gaps in critical infrastructure and highly sensitive data.

Action

Their plan involved a 36-month study using an $800 satellite receiver system on a rooftop in San Diego. To reveal the data, they used demodulation tools with software-defined radio. Plus, their home-brewed testing equipment scanned signals from hundreds of satellites, focusing on plain text transmissions. When the researchers found sensitive unencrypted data, they alerted the parties whose data was being transmitted. They did not publicize the data vulnerabilities.

Result

The researchers found that almost 50% of the unencrypted signals they intercepted contained Sensitive Military and Corporate data.

Conclusion

This report on satellite and data encryption vulnerabilities should concern any organization that cannot identify all the links its sensitive data takes as it travels from source to recipient. Most carriers and other organizations use encryption for their signals but there are still gaps in protection. This study helped locate and identify these weaknesses for further mitigation.

Zerowait's engineering team works with our customers to protect their organization's handling of critical and proprietary data, including their FileMaker databases. Our customers recognize that they must prioritize secure, on-premises storage to mitigate risks from external data stores and data transmissions. Zerowait's SimplStor-NVMe solutions offer a robust alternative, providing high-performance, encrypted storage arrays designed for on-premises environments.

Zerowait Corporation
707 Kirkwood Hwy, Wilmington DE 19805
TEL: 302-996-9408

Unlike off-premises Cloud solutions, Zerowait SimplStor ensures data remains under direct control, with features like end-to-end encryption and redundant failover. Zerowait's Solutions mitigate the risk of unencrypted data interception. The Zerowait approach enhances compliance with regulations like GDPR or HIPAA and provides reliable, cost-effective scalability while safeguarding sensitive information from leaks and providing low-latency access for mission-critical operations.

Zerowait Corporation
707 Kirkwood Hwy, Wilmington DE 19805
TEL: 302-996-9408