Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

14 February 2020

PIN Number
20200214-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released **TLP:WHITE**: The information in this product may be distributed without restriction, subject to copyright controls.

VSAT Signals Vulnerable to Low-Cost Device Exploitation

Summary

The FBI has identified a potential increased risk to data transmitted by Very Small Aperture Terminals (VSAT). Previously, the cost of the satellite equipment needed to intercept the data from these terminals served as a barrier for threat actors. However, recently conducted research discovered man-in-the-middle attacks against maritime VSAT signals can be conducted with less than $400 of widely available television equipment,[a] presenting opportunities to a wider range of threat actors to potentially gain visibility into sensitive information. VSATs are commonly used within the maritime and aerospace industries, predominantly seen in airplanes, cargo shipping, cruise ships, and offshore oil drilling platforms for a variety of services as well as point of sale systems in the retail sector. VSAT networks generally utilize Transmission Control Protocol (TCP), Internet Protocol (IP), and radio frequency (RF) channels to transmit data.

Threat Overview

The FBI continues to monitor the potential for cyber threat actors to target maritime and aerospace critical infrastructure. Maritime, aerospace, and retail industry stakeholders should be aware of the

[a] The materials used in the researchers experiment included a TBS-6903 DVB-S2X PCI card, Selfsat H30D satellite dish, and 3 meter coaxial cable.

risks posed by VSAT signal interception, and how information collected could be leveraged to identify targets of interest and conduct cyber intrusions. Using readily available hardware and software, a researcher gained access to the following information via VSAT signal interception, which could also be leveraged by a broad spectrum of cyber criminals:

- Cargo management, vessel routing, and navigation updates.
- Voice communication, email or file transfers (including complete credit card, passport information, and other personally identifying information), video conferencing, and port regulations communication.
- Operating systems, devices, and software, which can be used to identify existing vulnerabilities prior to an on-board intrusion.

Recommended Mitigations

- Secure data being transmitted over VSAT using end-to-end encryption for all customer, vessel, and aircraft communications.
- Ensure implementation of security policies across the entire fleet, including non-US flagged vessels.
- Monitor log files for suspicious Internet connections and audit networks and systems for unauthorized remote connections.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey