NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

ENTERPRISE THREAT BULLETIN

Conference Tracking Tags: Risk Considerations

ETD Bulletin 2024-10; April 2024

This Bulletin is from NCSC's Enterprise Threat-Mitigation Directorate (ETD) and the National Operations Security Program (NOP)

Attending conventions, trade shows, and symposiums are important elements of any U.S. government (USG) agency's strategy for conducting outreach and staying connected. However, the benefits of such participation also come with Counterintelligence (CI) and Operations Security (OPSEC) risks. The latest concerning trend involves the expanded use of tracking tags by conference organizers which, if not properly mitigated, can place attending USG officers, their home agencies, and sensitive national security information at risk.

Landscape

Tracking tags are relatively simple devices that utilize Bluetooth Low Energy technology to help users locate personal belongings or track movement. Prevalent commercial products include Apple's AirTag and Samsung's SmartTag. Conference hosts increasingly use this technology by attaching tracking tags to event lanyards, access keycards, and informational binders. This capability brings tremendous value to organizers by gathering metrics on session participation, capturing visits to exhibitor booths, and monitoring the movement of people around a convention facility.

Potential Threat Concerns

Unaware Conference affiliates, or third parties (to include threat actors), who are able to hack into the Bluetooth connections of these devices can collect location data on USG personnel and track in real-time their movements, who they engage with, topics of interest, and where they stay. In addition to these concerns about privacy violations, foreign intelligence entities can use such information to target USG officers for elicitation or coercion. And since these devices can be technically manipulated, a tag embedded in a lanyard or folder that is ultimately brought into a USG facility by a returning attendee could provide critical data to an adversary.

OPSEC Recommendations

- **Be Aware:** Check all items given to you. Be mindful of your surroundings. Remain vigilant.
- **Disable Tracking Tags:** If you receive an item containing a tracking tag, consider disabling it immediately by removing the battery or following the manufacturer's instructions for disabling.
- **Review Privacy Settings:** While at the conference, familiarize yourself with your phone's Bluetooth settings and adjust as needed to manage interactions with tracking devices and cellular networks.
- **Report Concerns:** If you believe you've been targeted by the use of a suspicious tracking tag, please consult with your organization's CI or security officials.
- **Do NOT bring affected items into your Sensitive Compartmented Information Facility or USG facility without proper coordination**.

For additional information on OPSEC and Insider Threats, please visit the **NCSC website.**