FBI CYBER DIVISION

Private Industry Notification

DATE: 2 October 2014

PIN #: 141002-001

(U) Cargo Thieves use GPS Jammers to Mask GPS Trackers

(U) This Private Industry Notification (PIN) highlights the use of Global Positioning Systems (GPS) jammers by criminals to thwart law enforcement response and investigation into cargo thefts in the United States. Since at least February 2012, various law enforcement and private sector partners have reported that GPS tracking devices have been jammed by criminals engaged in nefarious activity including cargo theft and illicit shipping of goods. Although banned by federal law, the jammers are readily available over the Internet and easy to employ.

(U) GPS Jammers are Small and Unobtrusive

(U) GPS jammers are transmitters that block tracking devices from acquiring GPS broadcast signals by transmitting electromagnetic interference[a] (noise) on the same frequency[b]. They come in many shapes and sizes, with varying capabilities. Plugged into a standard cigarette lighter jack, a small jammer (pictured right) operating in the vehicle will disrupt GPS logging or GPS tracking systems for a radius of up to five yards. Mid-sized and larger jammers typically block a combination of GPS, cellphone, Wi-Fi, and other signals and thus also prevent the tracker from wirelessly reporting any location or status data. In a test conducted by a federal law enforcement agency, GPS jamming devices were determined to be effective to approximately 65 feet. A large GPS jammer can disrupt any tracking device or receiver within a radius of several hundred yards.

UNCLASSIFIED

(U) An example of a GPS Jammer

(U) Source: Los Angeles Sheriff's

Cargo Theft Groups Employ Jammers to Mask GPS Tracking Devices

(U) Auto thieves shipping vehicles to China used GPS jammers placed in shipping containers in an attempt to thwart tracking of the containers, according to July 2014 information from the National Insurance Crime Bureau. In 46 reported incidents, the thieves placed one or more GPS jammers in cargo

[a] (U) Electromagnetic Interference (EMI) is any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment. (JP-02 Department of Defense Dictionary of Military and Associated Terms)

[b] (U) Jamming technology generally does not discriminate between desirable and undesirable communications. A jammer can block all radio communications on any device that operates on radio frequencies within its range (*i.e.*, within a certain radius of the jammer) by emitting radio frequency waves that prevent the targeted device from establishing or maintaining a connection.

containers with stolen automobiles. The devices were made in China and could be bought for approximately $14.00 over the internet. The use of the GPS jammers was an apparent attempt by thieves to thwart the tracking of the shipping containers.

(U) Cargo thieves in North Florida used GPS jammers with a stolen refrigerated trailer containing a temperature controlled shipment, according to a July 2014 report from the Pharmaceutical Cargo Security Coalition. In this incident, the hauling tractors were swapped out by the cargo thieves. The Miami based suspects were ultimately stopped and apprehended by the Florida Highway Patrol in mid-Florida on a routine vehicle stop; the shipment was recovered intact. Discovered, hidden inside of the trailer's refrigerator unit, were portable GPS jamming devices hooked unobtrusively to a battery located inside the unit. The trailer, although not equipped with a visible GPS tracking device, was treated by the thieves as if there were a device on or in the trailer. It is reasonable to believe that the individuals who planted the jammer felt that there may have been a tracking device secreted somewhere inside the shipment and used the GPS jammer to thwart the tracking of the shipment.

(U) Sales and Use of Jamming Devices is Illegal in the United States

(U) Federal law prohibits the marketing, sale, importation, or use of a transmitter (*e.g.*, a jammer) designed to block, jam, or interfere with wireless communications. The Federal Communications Commission (FCC) has issued Enforcement Advisories and has also ordered numerous online retailers to stop selling signal jamming devices. A retailer that receives a second warning could face a fine of up to $16,000 for each day on which a jammer was illegally marketed, up to a maximum of $122,500. The FCC has also issued actions with substantial fines against individuals caught operating these devices within U.S. territory. Jammers, which are sometimes used to avoid cell phone distractions or evade surveillance, could produce ***"disastrous consequences by precluding the use of cell phones to reach life-saving 9-1-1 services provided by police, ambulance, and fire departments,"*** according to the FCC. Though a limited exception exists for use by authorized federal agencies, jammers have no lawful consumer use. Accordingly, mere possession of a jammer with intent to violate federal law may subject the device to seizure.

UNCLASSIFIED

(U) Communications Act of 1934

Section 333 of the Communications Act: "No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under [the Communications] Act or operated by the United States Government."

Source: 47 U.S.C. § 333.

(U) Industry Observations of GPS Jammers

UNCLASSIFIED

Observations from Industry

- *The vast majority of successful jamming events in a cargo theft incident have taken place after the thieves have taken control of the truck.*
- *A layered security program, utilizing multiple tracking devices (to include covertly placed units within a shipment) provides the best mitigation against jamming.*
- *Jammers have limited range and successful jamming, particularly if a covert device is placed inside the load, and has proven difficult to maintain for extended periods of time. Active monitoring of GPS tracking in areas of high risk for jamming activity can be the best, earliest detection of that illegal activity – which can ultimately lead to successful law enforcement intervention.*

Source: Pharmaceutical Cargo Security Coalition

(U) Reporting Notice

(U) The FBI encourages recipients to report information concerning suspicious activity to the local FBI field office, www.fbi.gov/contact/fo/fo.htm , or contact the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or cywatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, identification of cargo containers, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) The FBI's Criminal Division investigates cargo theft in the United States. If you are notified of cargo theft involving the supply chain, contact your local FBI field office. FBIHQ has a Cargo Theft initiative and is tracking these incidents and will provide additional guidance.

(U) If you have questions about the Federal Communications Commission's (FCC) enforcement of the jamming prohibition, you can email the Enforcement Bureau at jammerinfo@fcc.gov. To file a jammer-related complaint with the Enforcement Bureau, you should use the FCC's online complaint form at www.fcc.gov/complaints.

(U) Cargo Theft and Organized Retail Theft task forces exist in many state and local jurisdictions. Incidents of cargo theft should be reported to appropriate state and local law enforcement agencies, regional intelligence centers. Additionally, the private sector has a number of organizations, such as FreightWatch, CargoNet, the Pharmaceutical Cargo Security Coalition and the National Insurance Crime Bureau (NICB) that monitor cargo theft issues and can provide situational awareness information to their members.

(U) Administrative Note: Law Enforcement Response

(U) In addition to federal, state and local law enforcement agencies, the information contained in this product is authorized for release to the Surface Transportation Information Sharing and Analysis Center (ISAC), Supply Chain-ISAC and Maritime ISAC for distribution to container terminal operators, freight forwarders, shipping lines/agents, cargo brokers, intermodal cargo facilities, railroad operators, drayage/trucking companies, and last mile couriers. These companies are the likely targets for criminal actors engaged in cargo and organized retail theft.

(U) This product is marked TLP: GREEN. The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels. No portion of this product should be released to the media, posted to public-facing Internet Web sites, or transmitted over non-secure, external communications channels.

(U) For comments or questions related to the content or dissemination of this document, please contact the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or cywatch@ic.fbi.gov

Appendix A: (U) Jamming devices

UNCLASSIFIED