BUSINESSAFE

BusinesSafe is designed to aid businesses in protecting the safety and well-being of Florida's residents and visitors from threats. BusinesSafe provides private sector partners with open source information, analysis and resources to help protect their businesses and communities.

Florida Fusion Center 20-026 **January 2020, Issue #18**

BusinesSafe Highlight: Communications

Criminal Activity

The Communications sector provides individuals and businesses with reliable interconnected systems to exchange information. The sector includes wired wireless, satellite, cable, and broadcasting communication services. Protecting the sensitive information transmitted via this sector's infrastructure continues to be a priority for both private and public sector entities.

1. **Insider Threat** – An insider threat is an individual, usually an employee, who may use his or her authorized access, wittingly or unwittingly, to do harm to the security of an agency or department. Insiders may be current or former employees, partners, consultants, or contractors. Malicious actors continue to attempt to gain access to the customer and company data of internet and communications service providers through insiders.

   - Microsoft Exposes 250 Million Call Center Records in Privacy Snafu
   - Telecom Industry "Top Target" for Cyberattacks by Hackers Luring Insiders to Gain Access to Systems

2. **Copper Wire Theft** – Telecommunications companies typically use copper wiring for grounding and transmission lines. Criminal actors may steal this copper wire from cell phone towers to sell at pawn shops, recycling facilities, and scrap metal centers. The theft of this material from communications infrastructure interferes with proper operation of cell towers and can cause service disruptions.
   - Trio Charged with 25 Counts of Grand Theft for Stealing AT&T Wire
   - Suspected Copper Thieves Cut Down 250 Feet of AT&T Wire

3. **Supply Chain Compromise** – The Communications sector depends on a robust supply chain network to operate effectively. Supply chains face a number of risks due to their multi-layered structure and can be vulnerable to disruption. Communication sector entities may be at risk of inadvertently inheriting vulnerabilities from compromised suppliers without proper vetting and inspection of equipment and suppliers.

   - 4 Elements in Security the Telecommunications Supply Chain
   - Supply Chain Risks for Information and Communication Technology (PDF)

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1.10

Foreign Adversary Activity
Foreign adversaries continue to target the Communications sector for theft of personal information and disruptive cyber-attacks. These adversaries may exploit vulnerabilities within this sector's infrastructure to gain access to this sensitive information.

1. **Advanced Persistent Threats** – Foreign adversary Advanced Persistent Threat (APT) groups have a continued interest in gaining access to and exploiting information housed within the U.S. telecommunications sector. Many of these actors appear to have varied interests in gaining access to this information including surveillance, intellectual property theft, and espionage.

- APT39: An Iranian Cyber Espionage Group Focused on Personal Information
- Messagetap: Who's Reading Your Text Messages?

Resources
The Department of Homeland Security provides houses the National Cybersecurity and Communications Integration Center, which is responsible for coordination between government, private sector, and international entities on matters related to cybersecurity and communications.
National Cybersecurity and Communications Integration Center

The Federal Bureau of Investigation provides recommended best practices for developing a supply chain risk assessment and neutralizing risks.
Best Practices in Supply Chain Risk Management for the U.S. Government

To sign up to receive BusinesSafe directly to your email, visit our website.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1.10