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 19-221 **October 2019, Issue #10**

BusinesSafe Highlight: Information Technology

Criminal Activity
Businesses are increasingly dependent on the information technology (IT) sector for normal operations. The IT sector often provides hardware, software, application services, and internet connectivity within critical infrastructure facilities. The heavy reliance of business on the IT sector may present challenges in fully securing assets.

1. **Cryptocurrency Mining on Company Equipment** – Cryptocurrency mining uses computer processing power to verify cryptocurrency transactions and to produce new cryptocurrency. The equipment needed to effectively mine cryptocurrency can be expensive, and may use large amounts of electrical and processing power. Due to the profitable nature of cryptocurrency mining, individuals may attempt to use company resources for this process.
   - Florida State Employee Arrested for Allegedly Mining Crypto at Work
   - Rogue Employees Mine Cryptocurrency Using Company Hardware

2. **Insider Threat** - An insider threat is an individual, usually an employee, who may use their authorized access, wittingly or unwittingly, to do harm. Insiders may be difficult to detect and can cause severe damage. To mitigate insider threat, organizations can monitor system activity, implement least privilege access, and promptly remove users who no longer require access.
   - Man Sentenced to Prison for Cyber Sabotage
   - Programmer Uses "Logic Bomb" to Trick Company Into Rehiring Him

   The mishandling of personally identifiable information (PII) is an example of insider threat with potentially costly and damaging consequences. Mishandling of PII occurs when sensitive personal information (e.g. names, passwords, identification numbers, medical records, etc.) stored within a database or network lacks necessary protections. Disclosure of this information can result in private information being accessed by unauthorized individuals.
   - Database Exposes Medical Info, PII of 137K People in U.S.
   - Number of U.S. Data Breaches Dip in 2018, But PII Exposure Jumps 126%

3. **Spearphishing Campaigns** – Spearphishing is the act of sending a targeted phishing email in an attempt to steal credentials from a certain industry or group within an

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, HSEC-7, FSIN 1.1, FSIN 1.6, FSIN 1.9, FSIN 1.10

industry. IT professionals are heavily targeted in spearphishing campaigns due to the high level of access they generally have to an organization's network. One successful spearphishing attempt can potentially give threat actors access to an entire network.

- Phishing and Spearphishing: A Cheat Sheet for Business Professionals

Foreign Adversary Activity

Foreign adversaries continue to target the U.S. IT sector to gain information on technology and assets. Although implementing of standard IT best practices may help in guarding against foreign adversary cyber intrusions, the IT sector may face other cyber espionage challenges.

1. **Advanced Persistent Threats** - In December 2018, two alleged members of Advanced Persistent Threat 10 (APT10), a Chinese cyber espionage group, were charged with allegations of computer intrusion in multiple countries between 2006 and 2018. APT 10 has targeted engineering, aerospace, and telecom firms in alleged support of Chinese national security goals. The two individuals allegedly conducted computer intrusion campaigns that targeted intellectual property and confidential business information.
   - Two Chinese Hackers Associated with Ministry of State Security Charged with Global Computer Intrusion Campaigns
   - Advanced Persistent Threat Groups: Who's Who of Cyber Threat Actors

In May 2019, President Trump signed Executive Order 13873 addressing foreign adversary exploitation of the information and communications technology (ICT) supply chain. The order prohibits the acquisition and installation of ICT equipment which is subject to the jurisdiction of a foreign adversary or which poses an undue risk to the security of U.S. critical infrastructure.

- Executive Order on Securing the Information and Communications Technology and Services Supply Chain

Resources

The National Counterintelligence and Security Center (NCSC) within the Office of the Director of National Intelligence (ODNI) provides a variety of content and guidance for protecting sensitive information, assets, and technology from foreign adversaries.
NCSC Awareness Materials

The link below provides Secure Florida's 10 Best Practices for Office Information Security.
Secure Florida Online Safety for Office Information Security (PDF)

The following document provides information on identifying suspicious activity and potential indicators or pre-attack mobilization related to IT.
BusinesSafe Fact Sheet: Information Technology – Cyber Security (PDF)

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, HSEC-7, FSIN 1.1, FSIN 1.6, FSIN 1.9, FSIN 1.10