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 19-170 **July 2019, Issue #3**

BusinesSafe Threat Topic: Ransomware

This Threat Topic is published in partnership with SecureFlorida, Visit secureflorida.org to learn more about cyber safety.

Ransomware is a type of malicious software (malware) that encrypts digital files until the victim pays a ransom. It generally functions in one of two ways.

The first way simply locks the user out of their device and attempts to manipulate the user into paying the ransom. Sometimes, the hacker may claim to represent a law enforcement agency that declares the user has broken one or more of several (usually bogus) laws. This ransomware type (also called locker ransomware) can usually be removed from the computer, without any payment, using a good antivirus program or professional technical assistance.

The second way is known as *encryption ransomware*, and it encodes the user's files, making them indecipherable without the decryption key. The hacker then demands payment for the key. There are tools that will remove the ransomware, but the only way to unlock the files is with the decryption key. Paying the thieves for the decryption key is risky as they may not provide it.

- In May 2019, the Federal Bureau of Investigation identified over 100 cases of businesses targeted by *Ryuk* ransomware since August 2018. The FBI report indicates that while the attacks are indiscriminate, logistics and technology companies, as well as small municipalities, have been disproportionately impacted.
  FBI Cyber Division: Indicators of Compromise Associated with Ryuk Ransomware
- Since May 2019, Riviera Beach, Lake City, and Key Biscayne, Florida, have all reported ransomware attacks which have disrupted city government functions. These attacks disabled city computer systems that often left city employees and officials without access to email and many other necessary systems. Riviera Beach and Lake City have reportedly paid ransomware attackers in order to gain access to infected computer systems.
  Another Hacked Florida City Pays a Ransom, This Time for $460,000
- In October 2018, a manufacturing company's networks were infected with *Ryuk* ransomware after an employee clicked a URL in a phishing email forcing the company to operate without

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, FSIN 1.1.4

computers. Since the attack, the company has increased cyber-security and is instituting new cloud-based storage.
How a Manufacturing Firm Recovered from a Devastating Ransomware Attack

Experts predict that ransomware usage is unlikely to decrease anytime soon. Businesses and organizations are encouraged to institute practices that better protect them from this threat.

Ways to protect yourself and your company from ransomware include:

1. **Backup files.** Ensure your backed up files do not have continuous connection to network computers to ensure that they don't become infected with the ransomware or encrypted as well.
2. **Make sure backup files can be successfully restored.** Verify the quality and integrity of backups regularly.
3. **Install security patches.** Ransomware will take advantage of vulnerabilities in operating systems which can stem from gaps in security.
4. **Disable Remote Desktop Services if not needed.** This is a common method of intrusion.
5. **Keep your security software up to date.** Updated antivirus and antispyware will help protect against ransomware.
6. **Encourage security awareness.** Train network users to use best practices, including:
    - Never click on links in emails from unknown sources.
    - Never download files from untrusted sites.
    - Be cautious of suspicious emails from trusted sources.
    - Research any files before you install them.
    - Never release confidential information to unverified individuals.

Visit secureflorida.org to learn more about cyber safety.

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 1.1.4