Cyber Vulnerabilities in the Air Domain

Emergence of 5G

Numerous U.S. government agencies collaborated in identifying and assessing potential threats with the emergence of 5G.

Resource : www.cisa.gov

Malware

Malware is a term for any type of malicious software meant to damage or exploit other networks. According to McAfee.com, "malware can be spread through email attachments, malicious advertisements on popular sites (malvertising), fake software installations, infected USB drives, infected apps, phishing email and even text messages."

To report Malware or suspicious activity please visit: www.malware.us-cert.gov

Ransomware

Ransomware is an evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.

Resource: www.cisa.gov

Exfiltration of Proprietary Data

Data exfiltration is a type of security breach that occurs when an individual's or company's data is copied, transferred, or retrieved from a computer or server without authorization.

Example: www.gao.gov

Destructive & Disruptive Attack

Cyberattacks cause much disruption in network operation and can cause catastrophic damage to economies and governments if undermined.

Example: www.justice.gov

Business Email Compromise (BEC)

In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request.

Resource: www.fbi.gov