Subject: Cybercriminals perpetrating Eavesdropping attack to steal sensitive data

Threat Summary

Eavesdropping attacks happen when cyber criminals intercept, delete, or modify network traffic traveling over computers, servers, mobile devices and Internet of Things (IoT) devices. Network eavesdropping, also known as network snooping or sniffing, occurs when malicious actors exploit insecure or vulnerable networks to read or steal data as it travels between two devices. Eavesdropping is most common for wireless communication. Eavesdropping attacks can often be difficult to spot.

Fig. 01 – Eavesdropping attack

Modus Operandi

- Cybercriminals target connections between two endpoints (a client and server) which are not secure for Eavesdropping attacks.
- Insecure network connections exist when encryption isn't used, when applications or devices aren't up to date, or when malware is present.
- With an insecure network connection (typically a Wi-Fi hotspot or websites not running the HTTPS protocol) data packets (web, email or messaging traffic) traveling across the network are intercepted by cybercriminals.
- Many sniffer programs created for network monitoring and vulnerability management are exploited for nefarious purposes of eavesdropping by cyber criminals.
- Cybercriminals gain unauthorized access of user accounts with weak passwords, which gives them a route into sensitive data, corporate systems or networks and steal sensitive & valuable data.
- The cybercriminals are after sensitive financial and business information that can be sold for criminal purposes. The eavesdropping attacks result in major financial losses and Identity theft.

Suggestions

- Ensure operating systems and applications are updated to the most current versions.
- Personal Firewall & Virtual Private Networks (VPN) may be used to prevent eavesdropping attacks.
- Avoid Public Wi-Fi networks, especially for sensitive transactions.
- Ensure passwords are strong and the password may be changed frequently.
- Update anti-malware and anti-virus software and conduct regular network scans.
- Report any such incidents on the ***cybercrime.gov.in*** portal and follow ***@CyberDost*** on Twitter, YouTube, Facebook, Instagram, Public, Koo and LinkedIn to know more about safety tips.

Regards,

Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23438207