Task1 Ans

History: APT34 has been active since at least 2014. They are believed to be involved in a long-term cyber espionage campaign focused on reconnaissance for Iranian national interests .

Nation/State: APT34 is associated with Iran. Evidence for this includes infrastructure details referencing Iran, use of Iranian infrastructure, and targeting aligning with Iranian interests

Targeted Industries: APT34 primarily targets organizations in the Middle East, including government agencies,critical infrastructure, telecommunications, and financial institutions [APT34 Deploys Phishing Attack With New Malware | Trend Micro].

Motives: Their motives are believed to be cyberespionage, collecting sensitive intelligence for the Iranian government.

Tactics, Techniques, and Procedures (TTPs):

- Spear phishing: APT34 uses targeted phishing emails to gain initial access to victim networks. They may leverage social media platforms like LinkedIn for these attacks.
- Exploiting vulnerabilities: They exploit software vulnerabilities to deploy malware and maintain access within networks].
- Custom Malware: APT34 develops and uses custom malware like POWRUNER, BONDUPDATER, and SideTwist for various malicious activities.

Security Measures: Here are some security measures to defend against APT34 attacks:

- Security awareness training: Train employees to identify phishing attempts and suspicious emails.
- Up-to-date software: Regularly update software and patch vulnerabilities promptly.
- Multi-factor authentication (MFA): Implement MFA to add an extra layer of security beyond passwords.
- Endpoint security: Use endpoint detection and response (EDR) solutions to monitor systems for malicious activity.
- Network segmentation: Segment your network to limit the impact of a breach.
- Security monitoring: Continuously monitor your network for suspicious activity.