Subject: **Prevention Against Cyber Espionage (Advisory No 25)**

1. **Introduction.** Recently, a critical vulnerability regarding Microsoft Outlook has been disclosed by the security researchers that could allow attackers to steal sensitive information including login credentials from windows system.

2. **Technical Details**

   a. This vulnerability resides in Microsoft Outlook that it automatically initiates an SMB connection whenever remotely hosted RTF based email message is previewed.

   b. A remote attacker can exploit this vulnerability by sending an RTF email to a target.

   c. Microsoft Outlook will automatically execute the attacker's malicious content handling over the victim's credentials and allowing the hackers to take control of the victim's system.

3. **Affected Products.** All outdated versions of windows that utilize Microsoft Outlook are compromised.

4. **Recommendations**

   a. Update windows immediately.

   b. Block specific ports 445, 127 and 139 used for incoming and outgoing SMB connections.

   c. Make use of complex passwords.

   d. Block NT LAN Manager (NTLM) Single Sign-on (SSO) authentication.

   e. Don't click on links from un-trusted sources.