Subject: **Prevention Against Cyber Espionage -Advisory No. 21, Nov 2017)**

1. **Introduction.** A critical vulnerability of TOR browser has been identified by Italian security researcher Filippo Cavallarin. This vulnerability can leak real IF addresses of users to potential attackers, upon visiting certain types of web page.

2. **Affected Software.**

   a. The vulnerability affects Tor browser for mac OS and Linux. However it doesn't affect Windows users apparently.

   b. This vulnerability would affect the privacy and security of Tor users.

3. **Mode of operation.** Mode of operation is as under:-

   a. The vulnerability resides in Firefox that also affects Tor Browser, as the privacy-aware service that allows users to surf the web anonymously uses FireFox at its core.

   b. **TorMoil** bug, the vulnerability affects Tor browser. TorMoil is triggered when users click on links that begin with file:// addresses, instead of the more common https:// and http:// addresses.

   c. Once an affected user [running macOS or Linux system] navigates to a specially crafted web page, the operating system may directly connect to the remote host, bypassing Tor Browser

4. **Recommendations.** Following is suggested in this regard:-

   a. The Tor Project has currently issued a temporary workaround to prevent the real IP leakage.

   b. MacOS and Linux users may found the updated versions of the Tor anonymity browser that will not behave properly while navigating to file:// addresses, until a permanent patch becomes available.

   c. Regularly update the system with latest anti-virus.

   d. Update TOR to version 7.0.8

   e. **Install and UPDATE well reputed antiviruses** such as Kaspersky, Bitdefender, Nod 32, Avast etc.

   f. Update all softwares including Windows OS, Internet browser (Mozilla,firfox) and microsoft office.

   g. Install and regularly update software firewall such as Comodo Firewall or Zonealarm.

   h. Don't click on any suspicious website popup during the Internet surfing.

j. Don't download attachments from emails unless you are sure about the source.