Subject: **Prevention Against Cyber Espionage - Advisory 10 March, 2018**

1. **Introduction.** A malware named **"Zyklon"** has been spreading which is exploiting recently discovered vulnerabilities in Microsoft office. Malware is capable of executing additional plug-in, including secretly using infected systems for DDoS attacks and crypt° currency mining.

2. **Technical analysis**

   a. Zyklon malware communicates with its Command and control server over TOR network and allow attackers to steals key logs, sensitive data, like passwords stored in web browser.

   b. The malware can download several plugins ,some of which include features such as crypto currency mining and password recovery.

   c. Vulnerabilities in Microsoft Office that execute a PowerShell script on the targeted computers to download the final payload from its C&C server, Detail as under:-

      (1) .NET **Framework RCE Vulnerability** (CVE-2017-8759).

      (2) **Microsoft Office RCE Vulnerability** (CVE-2017-11882).

      (3) **Dynamic Data Exchange Protocol** (DDE Exploit).

3. **Mitigation Measures.** Following best practices are suggested in this regard:-

   a. Don't open any word document received via **email** or any **unknown resource.**

   b. Don't click on any link appear during internet surfing unless adequately verifying the source.

   c. Use **latest** and **updated** version of **Microsoft office.**

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

   e. Keep all the softwares and operating system up-to-date.

4. **Recommendations**

   a. Strictly follow all mitigation measures discussed at para 3.

   b. Regularly check the Microsoft website for updates and release of security patch.