Subject: **Prevention Against Cyber Espionage (Advisory No 03 Feb 2016)**

1. **Summary of Cyber Attack**

File:	Tax Payment Challan.scr	**Subject:**	Your Tax PaymentHas been Deducted from your netbanking
Purpose: To steal information from users of sensitive organizations			

2. **Indicators of Compromise.** Following are the indicators of attack:-

a. Opening the file drops the following malicious file:-

(1) C: \ Documents and Settings \ admin \ Start Menu \ Programs \ Startup\ subbro.exe

(2) C:\Documents and Settings \ admin \ local \ Settings \ Temp \ bitty.bmp

b. **C&C Server. Domain:** dororachy. com **IP:** 91.223.82.82 **Location:** Netherland

3. **Method of Operation.** A target receives an email with an attachment of this file. It drops and executes the malicious dropper (C:\Documents and Settings\admin\Start Menu\Programs\Startup\subbro.exe) which hooks the system processes to steal information and sends to C&C server.

4. **Recommendation**

a. Avoid spoofed emails/subjects and mark them as spam.

b. Change password of online account immediately.

c. Enable 'Two Factor Authentication" in email accounts.

d. Install well reputed antivirus/firewall software that block known malwares:-

(1) Bitdefender total security.

(2) Kaspersky internet security.

(3) Eset NOD32 internet security.