Subject:- **Summary of Cyber Attack (Advisory No 02 January, 2016**

1. **Summary of Cyber Attack**

File. Hidden Truth 1971 Bangladesh Fiasco.doc	**Subject.** Hidden Truth 1971 Bangladesh Fiasco.
Purpose. To gain and steal information from users of sensitive Organization	

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

a. Folder created at "C:\Win\drv\ifxc".

b. Communication with following server:-

(1) Scholars90.website

(2) www.sportszone71.com

3. **Method of Operation.** The target receives an email with an attachment of this file. It drops and executes malicious payload in background and opens a fake file in foreground to trick the user. Effected version of MS office are MS office 2003, 2007 and 2010.

4. **Recommendation**

a. Use updated and patched version of MS Office.

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

c. Change password of account immediately, if the file were opened.

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

e. Use Protected View and block ActiveX controls in Office documents.

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

(1) Bit defender total security.

(2) Kaspersky internet security.

(3) Eset N0D32 internet security.