Subject: **Advisory - Prevention Against Cyber Espionage (Advisory No.18)**

1. **Context.** Recently, a malware has been found spreading **through spoofed emails** that is targeting **Army / Defense / Intelligence Organizations** as well as **Defence Attaches** abroad in a well-planned targeted manner. These emails portray a legitimate looking **Ministry of Foreign Affairs document informing the recipient about his involvement in ongoing investigation regarding a Military Coup**. Downloading and clicking on fake document executes a malware in background which will compromise victim's machine.

2. **Summary of Malicious Email.**

   a. **Email Subject.** CIRCULAR 209/1312/BC/1011411

   b. **Spoofed Email address**. compliance-helpdesk@mofa.digital

   c. **Download File.** CIRCULAR 2091312BC1011411.doc

   d. **Antivirus Detection Rate.** Low

   e. **File Size.** 83 bytes

   f. **File Extension**. MS-word (**.doc**)

   g. **C&C Servers.**

Ser	URL Address	IP address	Country
(1)	https://world-dnld.com	109.235.65.11	Lithunia

3. **Capabilities of Malware**

   a. The malware is specially designed for targeted attacks and **steal files** and **keystrokes** (along with stored usernames / passwords) from windows system.

   b. The attacker can **gain remote access** of the system and can execute additional payload from it. .

4. **Recommendations**.

   a. Install well reputed antivirus (AV) on the system such as kaspersky, Avira, Avast etc. Regularly update AV and scan the system.

   b. Update all software including Windows OS, Microsoft office and all other regular basis.

   c. Uninstall all software / applications from systems which are not in use.

   d. **Do not download attachments from emails unless you are sure about the source.**