Subject: **Prevention Against Cyber Espionage - Advisory No.06 February, 2018**

1. **Introduction.** A malicious email titled as **MOST IMMEDIATE"** impersonating officers of GHQ is being sent to officers and staff of Government departments. The email contains a malware hidden in a **PDF** and **Word** file. Downloading and running the file, executes malware in background that results in hacking of the computer.

2. **Summary of Malicious Email**

   a. **Subject.** MOST IMMEDIATE.

   b. **Name of Attachments.** Appendix-A-4-001.exe.

   c. **Malware Type.** Malware.Binary.exe.

   d. **Antivirus Detection Rate.** 4/55 (7.27%).

   e. **C&C Servers**

Ser	URL	IP	Hosting Country	Registrant Country
(1)	ems.kosikslev.com	93.113.131.155	Norway	-

3. **Indicators of Compromise.** The malware makes following files on the infected system:-

   a. Parent name: C:\WINDOWS\explorer.exe.

   b. Start: C:\Users\<admin>\AppData\Local\Temp\RESTD.exe.

   c. Reg Read: C/Documents and Settings\\admin\\Application Data\\ATI\ \Diagnostics\\comhost.exe.

4. **Capabilities of Malware**

   a. The malware carries executable file, once clicked on file, the malware detonates and steal the system's username/ password and continuously capture screen shots and send to Command and control server.

   b. The malware is persistent in nature, once executed on target system, a malware try to hide and achieve persistence on the exploited machine, in order to continue to act even after system reboot.

5. **Recommendations**

   a. **Install and update well reputed antiviruses** such as Kaspersky, Avira, Avast etc.

   b. Block C&C Servers at para 2e in firewalls of own networks.

   c. In case if indicators of compromise (para 3) are found in the system, please disconnect the computer from Internet and reinstall Windows.

   d. Update all softwares including Windows OS, Microsoft Office and all other softwares.

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