Subject:- **Equation Group; The Crown Creator of Cyber Espionage (Advisory No. 04) March, 2015**

Introduction A report published by Kaspersky Lab on 16-Feb-2015 uncovers a highly sophisticated threat actor that has been engaged in multiple Cyber-attacks since 2001. Report suggests that Equation Group which is probably NSA uses multiple malware platforms, some of which surpass the well-known Regin malware in terms of complexity and sophistication.

2. **Modus Operandi**. Malware designed by Equation Group is capable of reprogramming the hard drive firmware of more than dozen popular brands. This is the most powerful tool as no malware till date is found to have such capability. This capability serves following purposes:-

a. Malware can't be removed by formatting hard disk or OS installation as it creates an invisible, persistent area hidden inside the hard drive.

b. Capable of removing itself once it is deemed that host is no longer important or interesting.

c. Cover air gap by spreading and extracting data through USB.

d. Most of security products don't detect the malware.

3. **Indications of Infection.** Some of the indicators are given below. Details of the new indicators will be shared in due course of time.

a. Fanny.bmp file is found in USB or Hard drive.

b. Various shortcut (.Lnk) files found in USB or Hard drive.

c. Malware installs following files:-

(1) %windir%\system32\comhost.dll

(2) %windir%\system32\mscorwin.dll

4. **Recommendations** It is strongly recommended that all under command and concerned personnel be specifically informed regarding the threat and feedback be sought for any indicators of infection so that remedial measures can be suggested. Following measures be ensured:-

a. Strict control and segregation of official USBs / system from personal and internet connected USBs / system.

b. Install latest anti-virus and update it regularly.

c. Install software firewall to control incoming and outgoing connections.

d. If indications mentioned in para 3 are found, immediately turn off computer and consult Cyber Security / IT department for its removal.