Subject: **Prevention Against Cyber Espionage - (Advisory No 16) March, 2018**

1. **Introduction.** A new MAC based malware has been discovered named **"Coldroot",** the malware is a remote access Trojan (RAT) that remains undetected by major antivirus programs.

2. **Technical analysis**

a. The RAT is cross-platform and capable of planting a keylogger on MacOS systems prior to the OS High Sierra.

b. Coldroot masqueraded as the Apple audio driver "com.apple.audio .driver2.app" and when clicked displayed an authentication prompt asking the victim to provide his MacOS credentials.

c. The malware is capable of capturing screenshots, initiate and end processes, search for and upload new files, start a remote desktop session and shut down the operating system remotely.

d. The malware retains its persistence by installing itself as launch daemon to remain functional even after reboot.

3. **Infection Method.** It infects using a pop-up message, once the user clicks on it, a message that seems like a regular authentication message appears. It requests for user's MacOS credentials. When credentials are provided, Coldroot modifies the TCC.db privacy database allowing malware the required accessibility to perform system-wide key logging.

4. **Affected Product Versions.** The malware effects on **"MacOS Version (10.0 - 10.12)"** versions of MAC Operating System.

5. **Mitigation Measures.** Following best practices are suggested in this regard:-

a. It is advisable to clear cache of web browsers regularly, and also empty the download folder.

b. It is strongly advised reinstall macOS *and* update *it* to latest version i.emacOS 10.13 (High Sierra).

c. Install apps/ softwares only from official stores. It's wise to disable installation of apps from third-party sources.

d. If in doubt, don't download. Pay attention to misspelled app names, small numbers of downloads, Or dubious requests for permissions - any of these things should raise flags.

e. Install a reliable security solution ,for example, Kaspersky Internet Security for MAC. This will protect your device from most malicious apps and files, suspicious websites, and dangerous links.

f. Be careful while using social media groups/ pages and don't *click download any file or image.

g. Don't open any document received via email or any unknown resource:

h. Keep all the software's, browser and operating system up-to-date: