

Subject: **Prevention Against Cyber Espionage (Advisory No 26)**

1. **Introduction.** Chrome extension is a built-in feature of chrome browser to install feature based applications like Calculator, Adblock, and VPN etc. Recently, popular chrome extensions are found to be infected with malware which are being used by approximately 20 million users. Downloading and enabling these extensions in chrome can steal sensitive information from the browser.

2. **Affected Extensions.** Following is the list of compromised Chrome browser extensions along with the number of people that have installed it:-

- a. AdRemover for Google Chrome™ (10 million+ users).
- b. uBlock Plus (8 million+ users).
- c. [Fake] Adblock Pro (2 million+ users).
- d. HD for YouTube™ (400,000+ users).
- e. Webutation (30,000+ users).

3. **Technical Details**

- a. The above mentioned malicious browser extensions can access all online activities of user, incl passwords, web history and credit card details.
- b. These malicious extension can receive commands from the remote server, which are executed in the extension 'background page' and can manipulate browser's behavior in any way.

4. **Recommendations**

- a. Install extension from trusted sources only.
- b. Install and update well reputed antiviruses such as Kaspersky, Avira, Avast etc.
- c. Update all softwares including Windows OS, Windows Browser, Microsoft Office regularly.
- d. Remove any unwanted extension from Google Chrome by going to **Customize and Control > More Tools > Extensions**
- e. Don't download attachments from emails unless you are sure about the source.