Subject: Cybercriminals using malicious browser extensions to perpetrate Cyber Crime.

Threat Summary

It has been observed that a large number of users have started installing browser extensions, and many such extensions are malicious, and use adware to target users with advertisements.

The most common payloads carried by these malicious web browser extensions belong to adware families, which carry out snooping on browsing activity and promoting affiliate links.

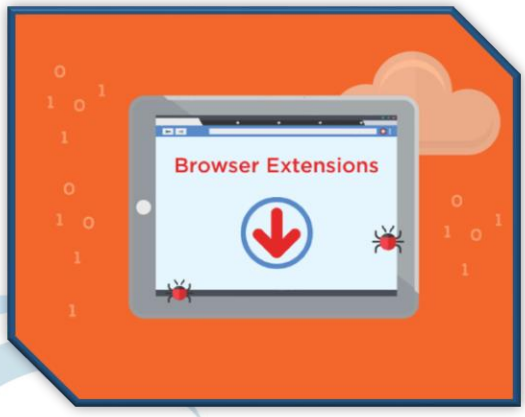

Fig. 01 – Malicious browser extensions

Modus Operandi

- Cybercriminals use adware extensions to target users by mimicking productivity tools such as DOC to PDF converters, document merging utilities, etc.
- These malicious extensions monitor users' browsing activity to profile them based on their interests and then promote links on the browser from affiliated marketing programs that help monetize the infection.
- These malicious extensions also download & execute pirated software from peer-to-peer networks and dubious sites.
- New registry keys are inserted in the systems to add persistence, so if the user removes the extension, it is re-downloaded and installed on the browser.
- These malicious extensions change the browser's home page to promote affiliate sites that match the user's search queries.
- The cybercriminals leverage the stolen sensitive personal/financial information to perpetrate further financial cyber crimes.

Suggestions

- Avoid downloading browser extensions from unofficial and unknown sources. Browser's official web store is a reliable source to download extensions.
- Scrutinize user comments and reviews, and run a background check on the developer/publisher of the extension.
- Review the privacy policy and data collection practices carefully before agreeing to them, as some extensions require permissions.
- Periodically review the installed add-ons and extensions, remove any that you are unsure of how they were installed.
- Report any such incidents on the *cybercrime.gov.in* portal and follow *@CyberDost* on Twitter, YouTube, Facebook, Instagram, Public, Koo and LinkedIn to know more about safety tips.

Regards,

Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23438207