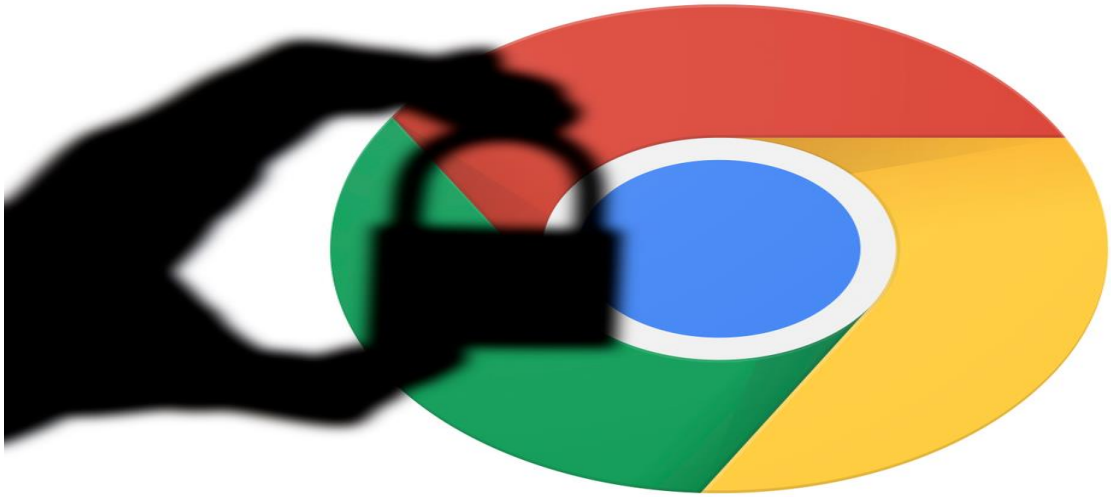
Google’s Face-off with Harmful Extensions on Its Web Store



For more than a decade, Google has been setting security benchmarks. But its Chrome browser, which attracts the major share of users (around 64%), has been keeping its security team on toes with scores of fake and malware-loaded chrome extensions infiltrating the platform almost every day.

What happened recently?

Fake crypto-wallet extensions have surfaced again on the Chrome Web Store, siphoning off victims' passwords. Security experts have identified and reported 11 more knavish add-ons masked as legit crypto-wallet software such as KeyKeep, Jaxx, Ledger, and MetaMask.

How grave the situation looks?

According to Google, there are nearly 200,000 browser extensions on its Web Store. Piracy and fake reviews have been misleading genuine users into installing malicious add-ons.

- Just three weeks earlier, after receiving several complaints from the crypto-wallet users, Google removed 49 Chrome extensions impersonating crypto players like Ledger, Trezor, and MyEtherWallet.
- Around mid-Feb, Google abruptly culled over 500 Chrome extensions that researchers found leaking browsing data and executing click fraud and malvertising on millions of computers.

Depending on how you want to look at it, this is either a good outcome or a bad example of how handy it is for adversaries to sneak past the Chrome Web Store's automated defences.

The current development in the landscape

A week ago, Google elevated the restrictions on its Web Store for developer's community to ensure a clear and informative path for users to discover an extension on its platform. The new policy must be adopted and implemented by developers by August 27th, 2020. Extensions not complying with the policy would be taken down and disabled, the tech giant has warned.

How to parry off fake extension threats?

While working with chrome extensions offer flexibility, we must follow the right steps to avoid falling into the traps of cybercriminals.

- To begin with, install and work with only the most needed extension/s.
- Carefully read the latest reviews and feedback about the add-ons left by users.
- Observe the responsiveness of the developer group toward the questions, and concerns posted on the forums.

Learn about the various permissions add-ons ask for (in Chrome, Settings > Extensions > Details) and ensure they're in line with the extension's features.

References:

- https://cyware.com/news/googles-face-off-with-harmful-extensions-on-its-web-store-ed3befe8
- https://nakedsecurity.sophos.com/2020/02/17/google-pulls-500-malicious-chrome-extensions-after-researcher-tip-off/
- https://www.tomsguide.com/news/google-chrome-malicious-extensions
- https://www.zdnet.com/article/google-threatens-to-delist-chrome-extensions-installed-by-deceptive-tactics/