Issued 8/9/17

Another Popular Chrome Extension Hijacked through Phishing

Chris Pederick, the creator and maintainer of the Web Developer for Chrome extension, is the latest victim of attackers who hijack popular Chrome add-ons in order to push ads onto users. The method the attackers used to compromise the extension's account is the same one that was so successful a few days ago against the developers of the Copyfish Chrome extension: a phishing email impersonating the Chrome Web Store team, with a link that points to a site mimicking Google's customer support system.

After getting their hands on Pederick's Google account login credentials, the attackers used them to hijack his account and push out a newer version of the add-on (v0.4.9) that performs ad injection (but apparently not all the time). Unlike the Copyfish creators, Pederick noticed that something was wrong rather quickly, and managed to disable the extension and push out a fixed version (v0.5) of it in less than six hours.

The quick reaction is probably what made it impossible for the attackers to transfer control of the add-on to their own developer

account, as they did with the Copyfish extension. Pederick is urging the million or so users of Web Developer for Chrome to uninstall and reinstall the extension, and to run adware detection on their machine, just in case. He says that there is no evidence that the malicious extension stole passwords, but it might be a good idea for users to change any password they entered in the browser while using it.

This hijacking is just the latest instance of compromised Chrome extensions made to spew ads. Among previous victims are the developers of other popular add-ons: User-Agent Switcher, Block Site, Infinity New Tab, and Live HTTP Headers.