Issued 1/18/18

Google Chrome Extensions with 500,000 Downloads Found to be Malicious

Researchers have uncovered four malicious extensions with more than 500,000 combined downloads from the Google Chrome Web Store, a finding that highlights a key weakness in what's widely considered to be the Internet's most secure browser. Google has since removed the extensions. Researchers from security firm ICEBRG stumbled on the find after detecting a suspicious spike in outbound network traffic coming from a customer workstation. They soon discovered it was generated by a Chrome extension called HTTP Request Header as it used the infected machine to surreptitiously visit advertising-related Web links. The researchers later discovered three other Chrome extensions—Nyoogle, Stickies, and Lite Bookmarks—that did much the same thing. ICEBRG suspects the extensions were part of a click-fraud scam that generated revenue from per-click rewards. But the researchers warned that the malicious add-ons could just as easily have been used to spy on the people or organizations who installed them. "In this case, the inherent trust of third-party Google extensions, and accepted risk of user control over these extensions, allowed an expansive fraud campaign to succeed," ICEBRG researchers wrote in a report published Friday [link]. "In the hands of a sophisticated threat actor, the same tool and technique could have enabled a beachhead into

target networks." Google removed the extensions from its Chrome Web Store after ICEBRG privately reported its findings. ICEBRG also alerted the National Cyber Security Centre of the Netherlands and the US CERT. In its public report, ICEBRG went on to explain how the malicious extensions worked: "By design, Chrome's JavaScript engine evaluates (executes) JavaScript code contained within JSON. Due to security concerns, Chrome prevents the ability to retrieve JSON from an external source by extensions, which must explicitly request its use via the Content Security Policy (CSP). When an extension does enable the 'unsafe-eval' permission to perform such actions, it may retrieve and process JSON from an externally controlled server. This creates a scenario in which the extension author could inject and execute arbitrary JavaScript code anytime the update server receives a request."