Shoplifters hit up Chrome Store for Facebook data

28 March 2012, by Nancy Owano

(PhysOrg.com) -- A cash-for-Facebook's-"likes" hustle hanging out in Google Chrome Web Store has been discovered by Kaspersky Lab. The researchers first discovered extensions leading to the wave of hijackings under an umbrella of assorted themes that were targeting users of Chrome and Facebook. They were rolling out malicious extensions for use to nab Facebook profile data. The lure was in the form of invitations for users to make changes on their profile or to see who was visiting their profile or to remove a virus from their Facebook profile.

Then Kaspersky's Fabio Assolini, a lab expert, said one bit of malware especially caught his team's attention because the malicious extension was hosted on Google's own Chrome Web Store. "At this time," Assolini said in a March 23 blog, "the malicious app has 923 users."

The extension presented itself as Adobe Flash Player. After installation, the extension could gain complete control of the victim's profile first by downloading a script file. The script file had instructions to send commands to the victim's Facebook profile. The result was the eventual spread of a malicious message, inviting more users to install the fake extension.

So what's in such a scheme for the malware makers? Profit, in the form of selling Facebook "likes" to businesses looking for (ironically) a reputation boost and may be willing to pay the $27 charged for 1,000 "likes."

According to reports, Google personnel removed the malicious extension after Kaspersky informed them of the hustle - titled Trojan.JS.Agent.bxo- which the Kaspersky experts had discovered on March 6 in a previous similar attack.

According to *Ars Technica*, a Google response was, "When we detect items containing malware or learn of them through reports, we remove them from the Chrome Web Store and from active Chrome instances. We've already removed several of these extensions, and we are improving our automated systems to help detect them even faster."

Beyond the Store, one security plus for Google was the launch, earlier this year, of Bouncer, which scans the Android Market for malicious apps. The scan happens when developers first upload an app to the Market and then periodically after that.

The Bouncer safeguard does not, however, seem to console observers over thieves who find ways to outsmart Facebook and Google.

Those behind the cash-for-likes scheme "are uploading new extensions regularly, in a cat and mouse game," said Kaspersky's Assolini.

Kaspersky Lab noticed a "huge wave" of attacks in Brazil. Without naming the miscreants, Assolini's column warning users to "think twice" before installing Chrome extensions simply referred to "Brazil's bad guys" turning their attention to Chrome and Facebook, which are now Brazil's two key go-to places on the Internet. Recent statistics show that Google Chrome has become the most popular browser in Brazil with more than 45 percent of

market share. Facebook is the most popular social network in Brazil, with 42 million users, displacing Orkut.

More information:
www.securelist.com/en/blog/208 …
ng_Chrome_extensions

APA citation: Shoplifters hit up Chrome Store for Facebook data (2012, March 28) retrieved 13 April 2021 from https://phys.org/news/2012-03-shoplifters-chrome-facebook.html