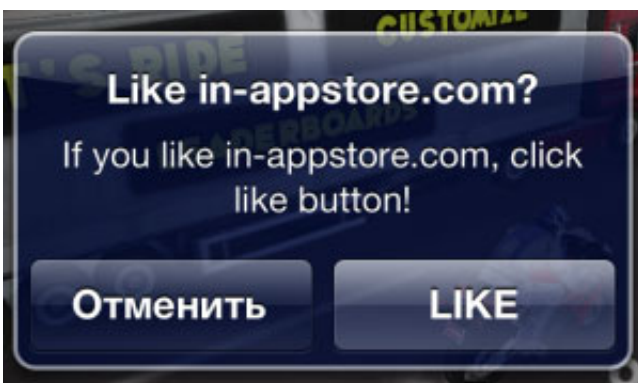


Hacker tricks Apple app pay system, posts YouTube how-to

July 14 2012, by Nancy Owano



(Phys.org) -- Apple's 2012 Friday the Thirteenth turned memorable for the company yesterday with news outside Apple traveling fast and furious that a hacker [was offering instructions](#) on a [YouTube video](#), telling iOS users how to wrest free access to paid iOS app content. The exploit was first posted earlier in the week, but achieved wide attention early Friday, with postings on numerous websites. A Russian hacker found a way to get hold of in-app purchasing power. Using the name ZonD80, he was also, it was learned, running a website In-AppStore.com with everything needed for the hack to work. He said donations were being accepted to support the project and help to keep servers up and running.

The most interesting, and troubling to some developers, feature of the new exploit was that it was so easy; no jailbreak was needed. Software developer Alexey V. Borodin aka ZonD80 showed a simple three-step technique for beating [Apple's](#) payment systems by installing a few certificates (CA and appstore.com) and changing the DNS in Wi-Fi settings—basically a matter of installing system certificates and doing a certain Wi-Fi tweak.

The technique included a fake in-[app](#) purchase server as well as a custom DNS server. The exploit worked on devices running iOS 3.0 to 6. According to reports, however, the hack did not work in specific regions around the world. The reason suggested is that developers there were using enhanced ways to protect their apps.

The exploit for circumventing Apple's in-app purchasing system was first flagged by a Russian blog i-ekb.ru. Reacting to their tips, news of the exploit tutorial was soon after reported on the Apple-watching site, *9to5 Mac*. The comments were that, since the published instructions were already getting attention, the site decided to carry the story too “as a warning to the Apple developer community.”

By 3 pm yesterday, the hack was getting so popular that the server enabling it bucked under the high demand. Apple, meanwhile, issued a statement.

“The security of the App Store is incredibly important to us and the developer community,” Apple representative Natalie Harrison, said. “We take reports of fraudulent activity very seriously and we are investigating.”

Since Apple's App Store is such a popular storefront for buying mobile apps, the store has also been the most desirable platform for developers trying to make money. The news of such an easy and successful exploit

has not gone down well with some developers who would prefer better news, such as how Apple's purchase system is adequately secure.

Developer Marco Tabini told *Macworld* that Apple's approach to receipt validation is flawed.

"The whole point of the [in-app purchase] system and the App Store is that you shouldn't have to worry about the system," Tabini said.

"Otherwise, what are you giving Apple its 30 percent for?"

© 2012 Phys.org

Citation: Hacker tricks Apple app pay system, posts YouTube how-to (2012, July 14) retrieved 2 May 2024 from <https://phys.org/news/2012-07-hacker-apple-app-youtube-how-to.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
