After latest iPhone hack, Charlie Miller kicked out of iOS dev program

Written by Ryan Naraine, Contributor Nov. 7, 2011 at 6:30 p.m. PT ⋮ 2-3 minutes

Charlie Miller gets a kick of out defeating Apple's security mechanisms, using his hacking skills to break into Macbooks and iPhones. Now, Apple has kicked the security researcher out of its iOS developer program after word got out that he built a proof-of-concept iPhone app to showcase a bypass of the code signing mechanism.

Charlie Miller gets a kick of out defeating Apple's security mechanisms, using his hacking skills to break into Macbooks and iPhones. Now, Apple has kicked the security researcher out of its iOS developer program after word got out that he built a proof-of-concept iPhone app to showcase a bypass of the code signing mechanism.

According to Forbes's Andy Greenberg, Miller found a way to sneak an evil app into the iPhone/iPad app store and will demonstrate the vulnerability at the upcoming SysCan conference in Taiwan.

Miller plans to present a method that exploits a flaw in Apple's restrictions on code signing on iOS devices, the security measure that allows only Apple-approved commands to run in an iPhone or iPad's memory. Using his method–and Miller has already planted a sleeper app in Apple's App Store to demonstrate the trick–an app can phone home to a remote computer that downloads new unapproved commands onto the device and executes them at will, including stealing the user's photos, reading contacts, making the phone vibrate or play sounds, or otherwise repurposing normal iOS app functions for malicious ends.

Miller has created a video demonstrating the attack, which gave him enough control over the hijacked iPhone to control the device vibration or read files off the iPhone.

Greenberg writes that Miller effectively created a proof-of-concept app called Instastock that appears to merely list stock tickers, but also communicates with a server controlled by Miller, "pulling down and executing whatever new commands he wants."

Details on the actual vulnerability being exploited is being kept under wraps until Apple issues a fix.

Just hours after word of his Miller's app -- which was approved by Apple -- was publicized by Greenberg, Apple nuked Miller from the iOS dev program "effective immediately."