



'Ohshit' - Sophos Recovers Password to New iPhone Virus

The first iPhone virus, known as Ikee, appeared about two weeks ago, written by an Australian to target Australians.

Most people remained relaxed about Ikee. It only infected unsecured, jailbroken iPhones, and it didn't do terribly much harm. Sure, it used up your bandwidth -- which can be expensive on 3G networks -- and it Rickrolled your phone, but it didn't have any secondary cybercriminal intentions. Ikee was an old-school "bragging rights" virus.

But at the end of last week, a new iPhone virus appeared in The Netherlands. Informally known as 'Duh', it is doubly criminal. Not only does it invade without permission, but it also hooks up your iPhone to a botnet command server in Lithuania. Your iPhone is turned into a zombie, ready to download and to perform any commands the cybercrooks might want in the future.

'Duh' also changes the password on your iPhone. It breaks in using Apple's feeble default root password ('alpine'), and immediately changes it. This change is made by directly editing the encrypted value of the password in the master password file, so that the new password is never revealed.

The password-changing of 'Duh' thus represents both a challenge and a risk, since THEY know what it is, so they can log back into your phone later, but YOU don't, so you can't login and neutralise the virus.

But Paul Ducklin, Head of Technology, Asia Pacific at

Sophos in Sydney, has recovered the password and offers this advice: "If you're infected with this new iPhone virus, you really ought to say 'Duh', since you could so easily have prevented it by changing your password. You may also think 'ohshit' -- and if you do, the virus writers are having the last laugh, because that's the new root password.'

So, if you have a jailbroken iPhone and you are able to login as root with the 'ohshit' password, you are almost certainly infected. Seek help from an iPhone geek or a malware expert at once!

For further information, try these links:

<http://www.sophos.com/blogs/duck/g/2009/11/23/iphone-worm-password/>

<http://www.sophos.com/blogs/gc/g/2009/11/23/lightning-strikes-iphone-malware-malicious/>

<http://www.sophos.com/blogs/chetw/g/2009/11/21/malicious-iphone-worm-loose/>

<mailto:duck@sophos.com>