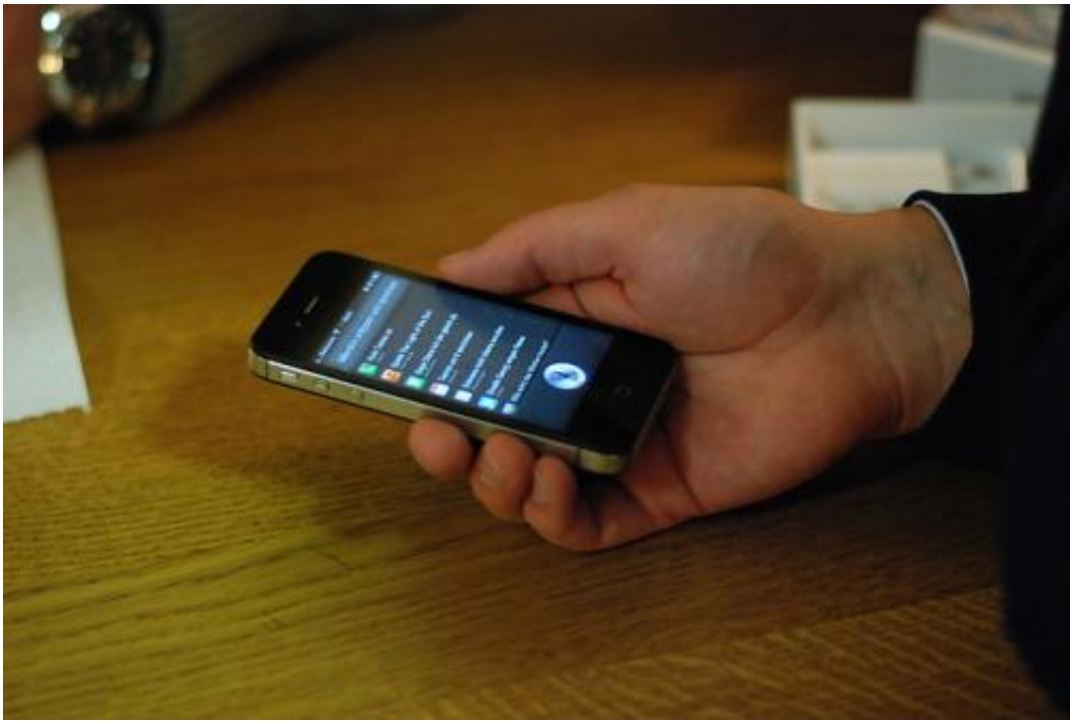
Is your iPhone at risk after the Oleg Pliss hack?

May 29 2014, by Andrew Smith



Bad news for iPhone users. Credit: Vasile Cotovanu, CC BY

iPhone users in Australia were greeted with an alarming message this week when they tried to use their devices. They were told that a hacker or group of hackers going by the name Oleg Pliss had taken control of their phone and will lock it permanently unless a $100 ransom is paid.

It's not yet clear whether the attack is likely to affect iPhone users

outside Australia but even if it doesn't, the attack has raised questions about the security of the iPhone. Apple products have a reputation for being more secure than others and this is the first major attack of its kind.

I recently said the iPhone is one of the most secure smartphones and that is still true. This attack is a very clever compromise but it does not actually hack into your phone.

Instead, Oleg Pliss seems to have found a way of attacking the remote server that supports an iPhone user's iCloud account. It is through this account that the user has cloud data storage for their phone as well as the opportunity to access the Find My iPhone service.

We don't know the exact detail of what has actually happened. Apple has issued a short statement saying that the iCloud was not compromised, but that users should change their passwords as soon as possible and has not given much more away.

It seems the hackers have identified a vulnerability by harvesting compromised data from other sources. That has allowed them to gain access to a large number of iCloud accounts. By identifying whether someone has an email @icloud.com or @me.com, the attackers have worked on an assumption that there are people who have used the same password for their iCloud account as well as for the other compromised service.

So instead of attacking the castle, they have compromised one of the supply pipes connecting the castle to the outside world.

Designed as a post-theft tool, as well as a fallback for those of us who regularly misplace our phones, the Find My iPhone app allows you to locate your lost device, lock it or send a message with a contact number

that will let anyone who finds it know how to reach you without giving them full access to your information. The app comes as an automatic addition to the latest iPhone.

Find My iPhone is recommended by police and there have been tales of police and citizens using this service to locate stolen phones.

After accessing the system, these hackers are sending remote warnings to iCloud users, threatening to wipe their devices unless they pay up. This suggests they are taking advantage of a feature of the app that allows you to wipe your device remotely if it falls into the wrong hands.

iPads and Mac computers also use this service so while the initial concern has been for iPhones, there is the potential for others to fall victim too. The chances are the cybercriminals could use their advantage in other ways.

What to do now

We don't know all the facts in this case but it would be prudent to change the password for your iCloud account. The possibility of this compromise not being an issue local to Australia is worrying. It is worth picking a password that has never been used on any other service.

The attackers may exploiting weaknesses caused by the Heartbleed bug or another vulnerability like the one recently discovered at eBay to gain access to iCloud accounts.

While Apple services were not affected, they may have been able to discover your @icloud email address if you've you've used it on other sites and services. If you're one of the many people who use the same password for different sites, your iPhone will be more vulnerable.

It's important to note that this is not a weakness in the iPhone or the services provided by Apple. Whoever these cybercriminals are, they have been very clever in their exploitation of other systems and are now putting this data to good use.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation