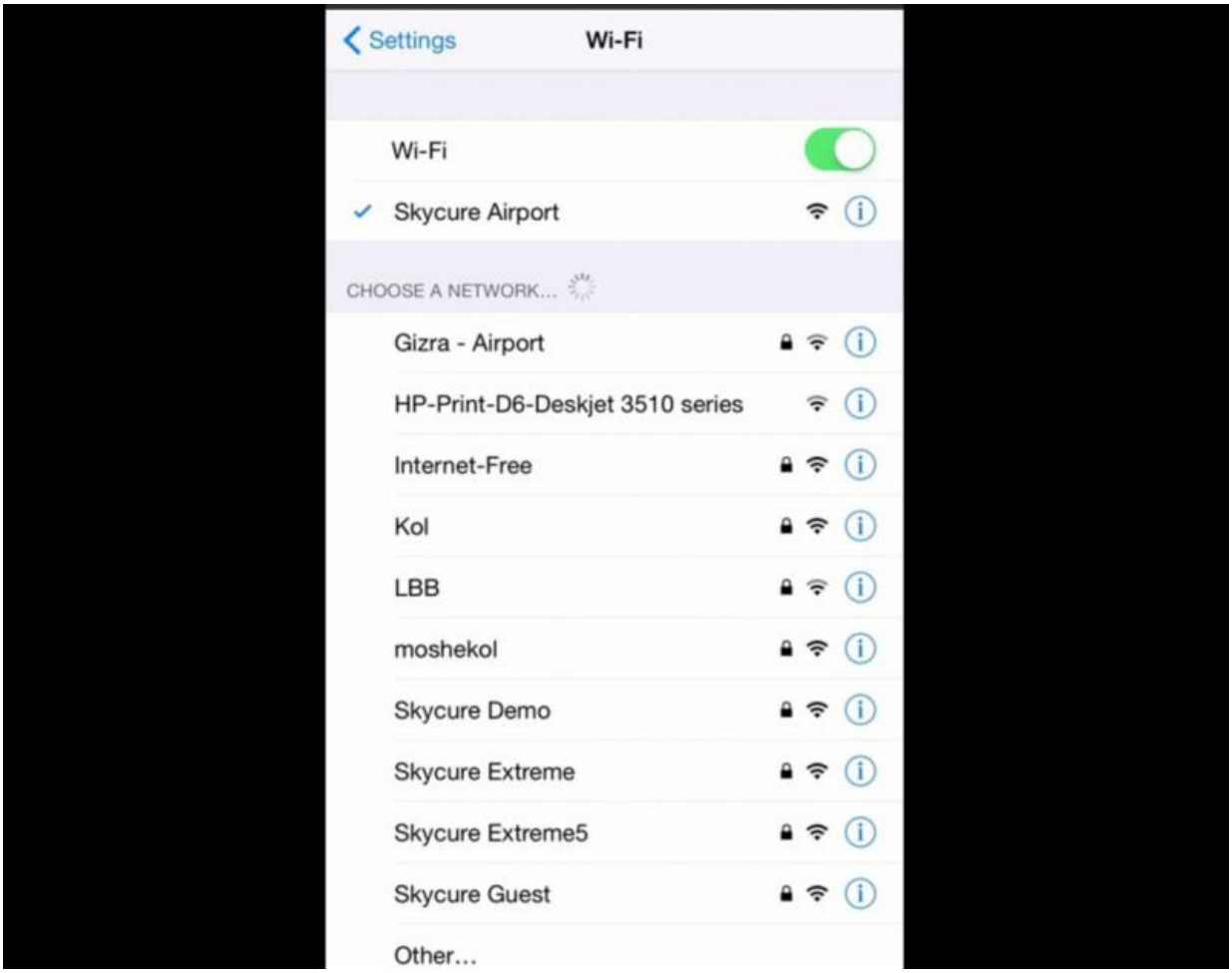
Security meet hears about "No iOS Zone" vulnerability

April 22 2015, by Nancy Owano



At the RSA security conference in San Francisco. a security firm's researchers presented what they said was a vulnerability allowing attackers to crash iOS devices in range of a WiFi hotspot. Chris Mills in *Gizmodo* reacted to the news and said "Gulp." The attack can occur whether or not the victim deliberately connects.

The security company, Skycure, calls the vulnerability the "No iOS Zone," described as allowing DoS attacks on iOS devices. Yair Amit, CTO and co-founder along with colleague Ari Sharabani, CEO, shared comments about the vulnerability—identified in iOS 8.

Darren Pauli in *The Register* reported on Sharabani's bracing remarks at the conference: "Anyone can take any router and create a Wi-Fi hotspot that forces you to connect to their network, and then manipulate the traffic to cause apps and the operating system to crash," said Sharabani. "There is nothing you can do about it other than physically running away from the attackers. This is not a denial-of-service where you can't use your Wi-Fi – this is a denial-of-service so you can't use your device even in offline mode."

By manipulating SSL certificates sent to iOS devices over a network, said Mills in *Gizmodo*, the researchers could make the devices crash, and in the worst-case scenario, he added, putting them in a constant boot-loop. Amit said in his Wednesday blog that, "under certain conditions, we managed to get devices into a repeatable reboot cycle, rendering them useless."

What makes Skycure think this is a vulnerability? Amit said, "our research team frequently performs experiments to check how mobile devices behave in various scenarios. One day, during preparation for a demonstration of a network-based attack, we bought a new router. After setting the router in a specific configuration and connecting devices to it, our team witnessed the sudden crash of an iOS app. After a few

moments, other people started to notice crashes. Pretty quickly, we realized that only iOS users were suffering from crashes."

Two more members of their research team analyzed the crashes. Their finding: "Basically, by generating a specially crafted SSL certificate, attackers can regenerate a bug and cause apps that perform SSL communication to crash at will." The team created a script that exploits the bug over a network interface. Amit said SSL, a security best practice, is utilized in almost all apps in the Apple app store, so the attack surface is wide.

The team is working with Apple on a fix, said Mills. In his Wednesday blog, Amit thanked Apple's security team for their cooperation. Amit said that the team reported the issue to Apple per the Skycure responsible-disclosure process. "As the vulnerability has not been confirmed as fully fixed yet, we've decided to refrain from providing additional technical details, in order to make sure iOS users are not exposed to the exploit caused by this vulnerability."

Skycure, with offices in Palo Alto and Tel Aviv, is in the business of unearthing mobile vulnerabilities and offering solutions.

Remarked Mills: "Consider this your monthly reminder to stay the hell away from dodgy Wi-Fi networks."

Amit offered three suggestions, meanwhile, for users: Disconnect from the bad Wi-Fi network or change location in case of experiencing continuous crashing or rebooting; the latest iOS 8.3 update might have fixed a few of the mentioned threats, and users are highly advised to upgrade to the latest version; in general, avoid connecting to any suspicious "free" Wi-Fi network.

More information: — www.skycure.com/blog/ios-shiel … acks-on-

ios-devices/

— www.rsaconference.com/events/u … a-breach-to-complete

© 2015 Tech Xplore

Citation: Security meet hears about "No iOS Zone" vulnerability (2015, April 22) retrieved 18 April 2024 from https://techxplore.com/news/2015-04-ios-zone-vulnerability.html

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.