COOK COUNTY HOMELAND SECURITY & EMERGENCY MANAGEMENT

SAU SITUATIONAL AWARENESS UPDATE

COOK COUNTY DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT
69 West Washington - Suite 2600 Chicago, IL 60602 V. (312) 603-8180

TONI PRECKWINKLE, *President - Cook County Board of Commissioners*
MICHAEL G. MASTERS, *Executive Director*

Date: 07 August 2015
No. 01
RESTRICTED

Please report relevant information and direct all media inquiries to the DHSEM DUTYDESK via e-mail: duty.desk@cookcountyil.gov or phone: (312) 603-8185 or (312) 603 - 8180.

The attached information is being passed through as a courtesy to the originating agency. DHSEM had no part in developing this information and has not verified the contents to be factual. If you have any questions reference this information please contact the originating agency. Please ensure the Data Security designation on this document is adhered to. Persons or organizations violating distribution restrictions will be prohibited from receiving future documents and will be removed from distribution lists. NO REPORT OR SEGMENT THEREOF MAY BE RELEASED TO ANY MEDIA SOURCES. Please contact DHSEM at 312-603-8185 if you have any questions or need additional information.

Android flaw lets hackers spy on you with your own phone

ByAmanda SchupakCBS NewsAugust 6, 2015, 4:46 PM

Researchers at Check Point Software Technologies have identified a vulnerability in Android phones that could let hackers take over devices remotely, steal personal data and even turn phones into spying devices. The "Certifi-gate" vulnerability takes advantage of preloaded apps that allow mobile carriers and manufacturers to remotely access your phone to troubleshoot problems. Certifi-gate affects hundreds of millions of devices by top manufacturers running most versions of Android, including Lollipop, the latest and most secure.

"It potentially allows cybercriminals to take complete control of any of these Android devices, enabling them to steal information from contact lists, calendars, location, anything that you have on your device," Check Point VP of product management Gabi Reish, told CBS News. "More than that, it can turn a victim's mobile device into a spy phone. That means bad guys can activate the microphone at any time they want. I can record anything I want to, in any meeting, any conference room. It's quite problematic."

The vulnerability is based on so-called mobile remote support tools, apps that allow manufacturers or service providers to access phones to fix problems remotely. (Ironic, huh?) If you call customer service because you can't get an app to work, or your calendar won't sync, reps use these tools to take over, fix what's wrong and get you on your way. They work by accessing small components that come baked into the operating system when you buy your phone. Certifi-gate makes it possible for any app to potentially access those same plug-ins, giving hackers a way in.

If you unwittingly download a malicious app that targets the weakness -- an innocuous-looking flashlight app, say -- whoever made it can now connect to the innards of your phone without your knowledge. Reish said his company disclosed the vulnerability to a number of manufacturers months ago and that "as far as we know they are taking steps to solve this." CBS News reached out to several manufacturers to confirm whether patches were in the works. In a statement, HTC said, "Working with Google, HTC has already begun rolling the fix into our software, and we will deliver these updates first to the HTC One M9 and the newest HTC Desire products." Reish thinks it could be "a while" before security updates are released across all device makers. The best protection in the meantime is to avoid downloading apps from third-party app stores that don't verify the products they sell. But Reish cautioned that theoretically even apps sold on the official Google Play store could be malicious.

His company is offering a free app on Google Play that scans your phone for apps that are exploiting or attempting to exploit the Certifi-gate vulnerability. This is not the first dangerous Android flaw revealed in recent days. In the lead up to Black Hat, the cybersecurity conference taking place this week in Las Vegas where Check Point made its big reveal (Certifi-gate-*gate*?) Thursday, another security firm exposed what they called "the mother of all Android vulnerabilities." The Stagefright vulnerability is a set of bugs that could let hackers take over your phone with a picture message.

Information labeled FOUO should be safeguarded, and withheld from public release until approved for release by the originating agency. Dissemination of FOUO is restricted to persons with "need-to-know." Need-to-know is defined as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in the lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Typical FOUO requirements include:

1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.

2. The holder of the information will comply with access and dissemination restrictions.

3. Ensure the recipient of FOUO has valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

0700	0740