Researcher to talk at Black Hat on 'scary' area in Android

July 28 2015, by Nancy Owano

Does that cute little green robotic creature with two ear-sticks call up feelings of an open, friendly mobile operating system, aka Android? Wow, Monday stories were not about how cute and adorable is that little green creature. Wow, these are no small numbers.

Malicious booby-trapped multimedia messages (MMS) can hijack 950 million Android phones. Let's put it another way. Almost 1 billion phones can be hacked. The findings are from mobile security firm Zimperium. Security researchers there discovered the vulnerability. Attackers can take control if they send a malware-laden MMS video.

The vulnerability is with "Stagefright," an Android code library that processes several media formats, which are widely used, said Security Editor Dan Goodin in *Ars Technica*.

Stagefright "may be one of the worst Android security holes discovered to date," said Robert Hackett in *Fortune*.

"This is Heartbleed for mobile," said Chris Wysopal, chief tech and information security officer at the application security firm Veracode, in *Fortune*.

"Since media processing is often time-sensitive, the library is implemented in native code (C++) that is more prone to memory corruption than memory-safe languages like Java," said the blog about the findings at Zimperium.

A message from Hackett in *Fortune*: Think twice before giving away your cell phone number, especially if you happen to own a phone that runs on Android.

Aarti Shahani, tech reporter for NPR, explained how this exploitation could work. "The bad guy creates a short video, hides the malware inside it and texts it to your number. As soon as it's received by the phone, Drake says, "it does its initial processing, which triggers the vulnerability." [Drake refers to Joshua Drake, Zimperium zLabs VP of platform research and exploitation.]

"The kicker is that you may not even need to do anything to trigger the payload, depending on your text messaging app of choice. While the stock Messenger app won't do anything until you see the message, Hangouts' pre-processing for media attachments could put you at risk before you're even aware that there's a message waiting," said Jon Fingas in *Engadget*.

NPR's Shahani explained this too: "The messaging app Hangouts instantly processes videos, to keep them ready in the phone's gallery. That way the user doesn't have to waste time looking. But, Drake says, this setup invites the malware right in."

If using the phone's default messaging app, it's a bit less dangerous, he said, according to NPR. "You would have to view the text message before it processes the attachment. But, to be clear, 'it does not require in either case for the targeted user to have to play back the media at all,' Drake says."

The Zimperium blog commented that "Devices running Android versions prior to Jelly Bean (roughly 11% of devices) are at the worst risk due to inadequate exploit mitigations."

Issues in Stagefright code critically expose 95 percent of Android devices, an estimated 950 million devices, said the Zimperium blog.

"Attackers only need your mobile number, using which they can remotely execute code via a specially crafted media file delivered via MMS. A fully weaponized successful attack could even delete the message before you see it. You will only see the notification."

Does Google know about this? Yes. Drake reported the vulnerabilities, said *Fortune*, and Google acted promptly. It now remains for various device manufacturers to push the updates out.

Jamie Lendino, managing editor of *ExtremeTech*, told how Drake originally informed Google about the exploit in April and patches were sent. "The problem is," said *ExtremeTech*, "Android OS is notoriously difficult to update unless your carrier and phone vendor both play ball and coordinate a patch rollout."

Fortune noted Google's response: "We thank Joshua Drake for his contributions. The security of Android users is extremely important to us and so we responded quickly and patches have already been provided to partners that can be applied to any device."

Lendino further reported that Adrian Ludwig, Android Security's lead engineer at Google, told NPR that they notified partners and already sent a fix to the smartphone makers who use Android.

Lendino pointed out that "there are hundreds and hundreds of different models out there, each with their own custom code on top of Android and woven into it in various fashions. Patching it will be a nightmare, and will depend entirely on how each manufacturer and carrier approach and resolve the problem individually."

Associate Editor Mark Bergen in *Re/code* commented that "Openness is Android's greatest strength—a flexibility that has enabled it to spread to now power four of every five smartphones on the planet. But openness can be, at times, its greatest weakness."

Fingas in *Engadget* similarly pointed out that "Google is already on top of the flaw, and has pushed out a fix to its hardware partners. However, whether or not you'll get that fix will depend on your phone's manufacturer."

Drake, co-author of *Android Hacker's Handbook*, plans to present his research at the Black Hat security conference next month. His talk is

titled "Stagefright: Scary Code in the Heart of Android."

In briefings about the upcoming event, Black Hat said, "With over a billion activated devices, Android holds strong as the market leading smartphone operating system. Underneath the hood, it is primarily built on the tens of gigabytes of source code from the Android Open Source Project (AOSP)."

Drake's presentation "centers around the speaker's experience researching a particularly scary area of Android, the Stagefright multimedia framework. By limiting his focus to a relatively small area of code that's critically exposed on 95% of devices, Joshua discovered a multitude of implementation issues with impacts ranging from unassisted remote code execution down to simple denial of service. "

The site page added, "Joshua will show you why this particular code is so scary, what has been done to help improve the overall security of the Android operating system, and what challenges lie ahead."