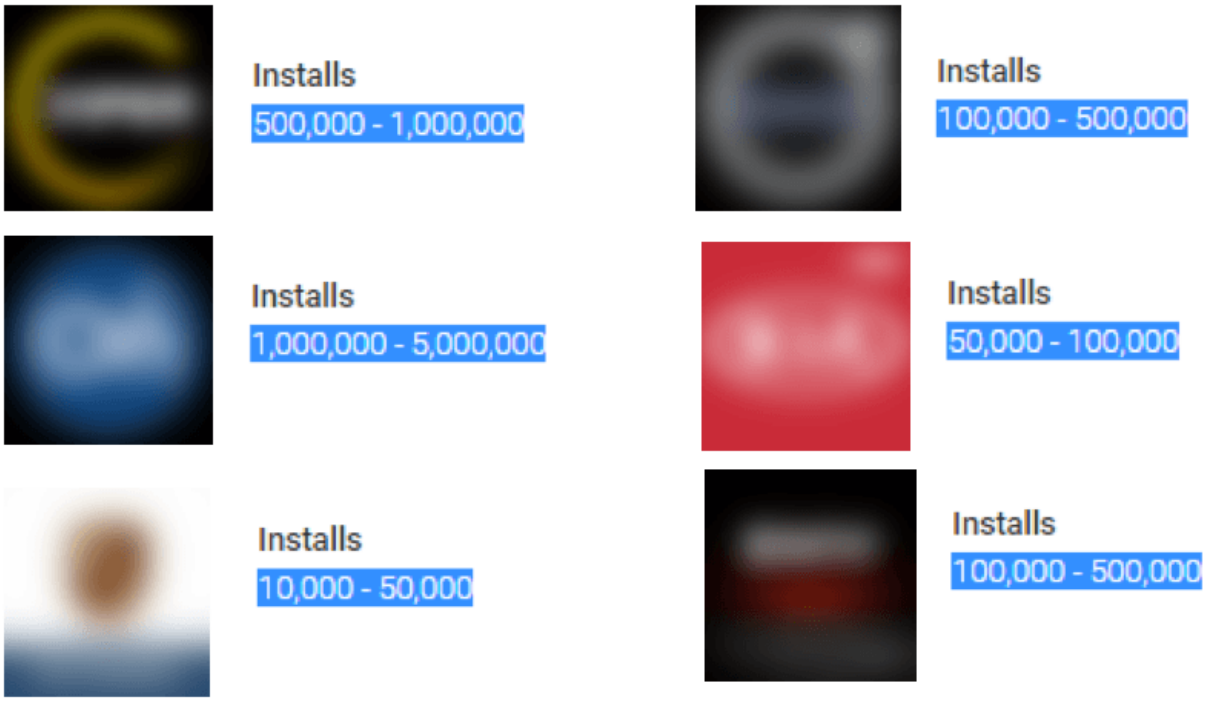
Kaspersky Lab researchers pick apart risky nature of some mobile apps for connected cars

February 20 2017, by Nancy Owano



Credit: Kaspersky Lab

(Tech Xplore)—A mobile device app shown as vulnerable to hack story. Yawn. But what if the hacks are being used to steal your car? Wake up call.

Imagine the scenario. Hey what is happening with my car? Better question, where are the security features your car application should have had?

Jeffrey Esposito, Kaspersky Lab, wrote earlier this month about a mixed bag. On the upside, the connected car concept has continued to evolve.

Certain apps that have come along can make users' lives easier by linking the devices to their automobiles. Andy Greenberg in *Wired*: "In the era of the connected car, automakers and third-party developers compete to turn smartphones into vehicular remote controls, allowing drivers to locate, lock, and unlock their rides with a screen tap."

The problem is that they can be exploited by attackers. The mischief makers could make use of functions to open doors and more.

"Upon successful exploitation, an attacker can gain control over the car, unlock the doors, turn off the security alarm and, theoretically, even steal the vehicle," Esposito wrote.

The underbelly of convenience is security risks. Certain safety mechanisms seem to be ignored when it comes to the apps that the researchers explored. Esposito said, "as with many IoT connected devices, the answer is, security needs to become more of a priority for developers and manufacturers."

Anti-malware researchers Victor Chebyshev and Mikhail Kuzin made that point clear when they presented research conducted on some of the popular apps for vehicles. They found that the apps were fairly ripe for exploitation.

The researchers disclosed their findings to the developers, but they did not disclose names of the apps publicly. No actual exploitations had been

seen in the wild, they said.

"At this point," said the two researchers in Securelist from Kaspersky Lab, "it should be noted that we have not witnessed a single attack on an app that controls cars, and none of the thousands of instances of our malware detection contain a code for downloading the configuration files of such apps."

The apps, said *Wired*, lacked some basic software defenses that drivers might expect to protect one of their most valuable possessions.

In the Kaspersky Lab report from Esposito, Chebyshev stated that "Applications for connected cars are not ready to withstand malware attacks. We expect that car manufacturers will have to go down the same road that banks have already taken with their applications…After multiple cases of attacks against banking apps, many banks have improved the security of their products."

Attacks against car applications have not yet been detected—and that, he added, means that "car vendors still have time to do things right."

Doing things right does not involve having to address security bugs. The problem here is sheer lack of safeguards.

Such as? Encrypting or hashing credentials stored on the device, adding two-factor authentication or fingerprint authentication, or creating integrity checks to see if alterations were made to include malicious code.

Ars Technica's Sean Gallagher, IT editor, provided a summary of their findings. Gallagher's discussion included the note that all seven of the applications allowed a user to remotely unlock a car. None of these seven were found to have performed an integrity check.

He also noted that "Two of the seven apps used unencrypted user logins and passwords, making theft of credentials much easier."

IDG News Service Lucian Constantin shared his thoughts on the findings: None of the apps checked if the devices they're running on are rooted.

"While manufacturers are rushing to add smart features to cars that are meant to improve the experience for car owners, they tend to focus more on securing the back-end infrastructure and the communications channels. However, the Kaspersky researchers warn, that client-side code, such as the accompanying mobile apps, should not be ignored..."

More information: blog.kaspersky.com/rsa-connected-cars/14060/