Study uncovers invisible mobile app ads gumming up the works

26 July 2015, by Nancy Owano

Credit: Peter Griffin/Public Domain

Sobering news for ad industry players on Friday: "Invisible ads could be defrauding advertisers out of nearly $1B a year," said the *Silicon Valley Business Journal*. They along with numerous other sites were referring to a new study that revealed invisible ads on some mobile apps.

One percent of all devices in the U.S. and two to three percent of devices in Europe and Asia are running at least one app that commits ad fraud, according to the findings.

The company behind the study, New York-based Forensiq, said that the secretly loaded ads affect both advertisers and smartphone users.

Fundamentally, users of the mobile apps are affected because those invisible ads are burning though gigabytes of their data plan every day. The smartphone is slowed down; the ads eat away at batteries too. Performance issues are almost certainly caused by the extra load resulting from the apps' secondary functions, said Forensiq in *Bloomberg Business*.

Forensiq carried out a ten-day study exploring instances of unseen ads. "About 1% of mobile devices that Forensiq observed in the U.S. and 2% to 3% in Europe and Asia were seen running 'infected' apps, including those operating Google Android and Apple iOS operating systems, as well as Microsoft's Windows Mobile," said Jack Marshall, who covers marketing and the media for *The Wall Street Journal*. He also quoted Forensiq founder and CEO David Sendroff: "Users may see one ad on their screen, but there might be 5 or 10 in the background that were never viewable."

Joshua Brustein in *Bloomberg Business* noted that "Surreptitiously running advertisements is a violation of the rules governing all apps available in Apple and Android stores." However, it is tricky to identify what is happening. How does the code for generating fraudulent ads land in the mobile apps? Brustein commented on the problem: "Fraud is endemic in the online advertising world, and the victims—the brands paying for the ads—often lose track of where their ads end up once they are traded through several automated layers of middlemen."

Mashable said the apps themselves tend to come from smaller lesser known publishers.

"It's not Angry Birds or Candy Crush, but these are apps that people play and enjoy and some real effort went into developing," Sendroff told *Bloomberg Business*.

"We wanted to show the public how blatant and obvious and hurtful all this fraud is—not just to advertisers who pay for ads that no one sees but also people using these apps on these tiny devices that are bandwidth-limited and power-limited," Forensiq Chief Scientist, Mike Andrews, told *Mashable*.

The authors had built algorithms to look for instances when certain ads showed suspiciously

non-human behavior. (*Silicon Valley Business Journal* referred to the report: "Malicious apps often request suspicious permissions, which include being able to prevent the device from sleeping, run at start-up, modify and delete content on the SD card, and access location services while running in the background.") Forensiq said analysis tools which they used for the study allowed them to uncover that many apps launch on reboot without the user loading the application.

Andrews said in *Mashable* that they can slip in like Trojan horses, disguising intentions until they make it through the door.

Mobile advertisers are losing 13% of their ad spend to mobile device hijacking, said Forensiq, and the company projects in-app ad fraud will surpass the $1 billion mark globally in 2015. "With mobile ad spending expected to overtake desktop spending in 2016, tracking fraudulent behavior and raising awareness to new threats such as mobile device hijacking is essential to building a more sustainable and overall safe advertising ecosystem," said Sendroff, in a company release.. "We hope this study will open a discussion and bring all stakeholders together around the issue."

Patrick Kulp in *Mashable* shared this advice: "Researchers say users can take relatively simple steps to protect them from running up their phone bills and draining their batteries. One is scanning app review sections for accounts of excessive data or power usage that may indicate fraud is at play. Another is switching off access to cell data for apps that don't absolutely need it."

More information:
forensiq.com/mobile-app-fraud-study/

APA citation: Study uncovers invisible mobile app ads gumming up the works (2015, July 26) retrieved 27 September 2022 from https://techxplore.com/news/2015-07-uncovers-invisible-mobile-app-ads.html