New research gives users another reason to hate unwanted ads

November 11 2022

Credit: Pixabay/CC0 Public Domain

New research released this week reveals the process used by third party advertisers to target online users can be viewed or manipulated by online adversaries using only their target's email address.

A four-person team of researchers from the Georgia Institute of Technology, University of Illinois Chicago (UIC), and New York

University (NYU) presented their findings Wednesday at the ACM Conference on Computer and Communications Security (CCS), a premier security venue.

Today, much of the advertising that appears online is specifically tailored to individuals based on their browsing history, location, and a variety of other factors that have been collected by third party advertising networks.

This data is collected by tracking cookies, which are sent out by third party ad networks and correlated with unique identifiers like email addresses. These cookies allow advertisers to create extensive profiles of internet users, however as the researchers found, this system can be influenced by bad actors.

Once an attacker knows a user's email address, they can tap into the information being collected by any third-party advertiser observing a specific user's targeted ad stream. This could allow bad actors insight into to an individual's detailed browsing history, such as online retailers and travel websites.

"Third party ad networks have no direct relationship with users. Thus, if they want to track user activity across devices, they must rely on identity information, such as email addresses, given to them from other various websites," said Paul Pearce, assistant professor in the School of Cybersecurity and Privacy (SCP) at Georgia Tech. "Our work shows the way that information is passed to the ad networks is both insecure and hard to verify. If an attacker knows a victim's email address, they can lie to the ad network pretending to be a user, leading to very real privacy problems."

The researchers describe this susceptibility as advertising identity entanglement and it happens when attackers confuse ad networks into

correlating the attacker's tracking cookies with a targeted person's email address, looping them into the data being gathered by third parties. As Pearce and his colleagues state in their paper, adversaries can also leverage the process to send ads of any kind to their targets.

"When I use the Internet on my own private device, like a phone or a laptop, I don't expect that anyone who knows my personal email could manipulate what I see," said Chris Kanich, associate professor at UIC. "This attack is particularly disturbing, and I am relieved that I use ad and tracking blockers in my web browsers."

To test the scale of this problem, researchers created an artificial users and profile for their experiment, at no time was a real person targeted. By knowing only, the experimental user's email address, the team was able to Identify specific items and websites the victim interacted with.

Along with shopping habits, the test also showed retargeted advertisements can contain sensitive location information. For example, if a victim interacted with some hotel and travel websites, the attacker could then receive retargeted ads for the specific hotel the victim viewed.

"An ad network potentially leaking travel plans to anyone with a target's email address is a significant privacy threat and potentially dangerous to people being stalked," said Damon McCoy, associate professor at NYU.

The researchers indicate that combatting this problem without the support of ad networks is challenging, but ad blockers provide a reasonable initial option to limit exposing a user's private data. Mitigation of this threat shouldn't just fall on the users, however. The team also suggests that if third party ad networks encrypted the process of exchanging identity information and ensured the data was verified and correct it would help mitigate the threat.

The research was presented at ACM CCS 22. The paper, "Cart-ology: Intercepting Targeted Advertising via Ad Network Identity Entanglement," is co-authored by SCP Ph.D. student ChangSeok Oh, Kanich, McCoy, and Pearce. In accordance with ethical research guidelines, the threat was disclosed to Criteo, one of the largest third-party ad networks on the market, as well as Yahoo.

More information: Conference: www.sigsac.org/ccs/CCS2022/

Provided by Georgia Institute of Technology