Research on Ad Blockers and Facebook "Like Farms" Takes Aim at Web Security

By Kasra Zarei
kasra-zarei@uiowa.edu

A UI researcher has been working to make the internet more secure through developing stealthy ad blockers and identifying fake accounts on social media.

Online advertisements are very targeted. Cookies, computer programs that collect information about which users visit websites, are inserted into a user's web browser when a site is visited.

This information is aggregated and used to profile every user. Then by analyzing someone's browser's habits, targeted advertisements can be made.

While it looks relatively benign, Edward Snowden revealed that the National Security Agency has been using information traditionally used by advertisers, to profile users worldwide.

There is a prevalent concern that besides showing relevant ads, online advertising and profiling can fall into the wrong hands.

This is one of many Internet security issues being studied by Zubair Shafiq, University of Iowa assistant professor of Computer Science.

Shafiq's group, who has recently been awarded a Data Transparency Lab grant, has been trying to develop tools that can be used to mitigate tracking and surveillance that happens on the Internet, since online advertisements have become nefarious.

"A lot of websites have had their ad systems exploited to install malware on users. For instance, Forbes was once surveying malware to users," Shafiq said.

One common tool that people use to avoid tracking through online advertisements is ad blockers.

However, recently websites have been able to detect ad blockers, and essentially force users into disabling their ad blockers.

The overarching goal of Shafiq's recent study focused on developing a stealthy ad blocker, one that would not be detectable by websites.

"It's kind of like an arms race – websites try to detect an ad blocker while you try to develop an ad blocker that websites cannot detect," Shafiq said.

As part of his study, Shafiq and his collaborators had to understand how websites actually detect ad blockers in the first place.

The team did a measurement study to understand how the top 100,000 websites actually detect ad blockers.

“One of the main findings in our study was that websites often rely on third party services that provide ad block detection capabilities, and the use of these third party services is increasing,” Shafiq said.

Unless the advertisement industry tightens their security standards, users need ad blockers for protection against potential threats.

“The way forward is [online] advertising has to be strictly regulated. Ad blockers must be used to force the hands of the higher-up authorities and protect users,” Shafiq said.

Shafiq’s work does not stop at ad blockers. He is developing algorithms to detect fake accounts in social networks including Facebook.

“There are a lot of ‘like farms’ that rely on exploitation of Facebook applications. Fraudsters have created third party applications that they can exploit to do fake activity on pages, or worse, put personal information in the hands of unscrupulous marketers and help spread dangerous computer viruses and other forms of malware,” Shafiq said.

Shafiq and his team recently did an extensive study in collaboration with Facebook, with the goal of taking down these “like farms” that are used for reputation manipulation.

“We identified more than a million Facebook users collaborating to exchange fake likes and comments - we call them collusion networks,” said Shehroze Farooqi, University of Iowa graduate student in computer science.

“Our analysis aims at providing effective countermeasures for mitigating such networks,” Farooqi said.

Security is still an arms race.

“This is a cat and mouse game makes working in this area exciting and challenging,” Farooqi said.

“A while ago Facebook devised algorithms for detection of reputation fraud. Afterwards, fraudsters developed new methodologies to circumvent these algorithms,” Farooqi said.

Alberto Segre, University of Iowa DEO of the Computer Science Department, spoke positively about Shafiq’s work and his impact on the department.

"His [Safiq] expertise in networking and security has noticeably broadened the scope of the Department's growing research program,” Segre said.

For Shafiq and his group, the main motivation of the research is the impact of the problems that are being looked at.

“We hope that our work will shed light on these important problems and help people browse the web in a more secure way,” Shafiq said.