The Adblocking Tug-of-War

HAMED HADDADI, RISHAB NITHYANAND, SHEHARBANO KHATTAK, MOBIN JAVED, NARSEO VALLINA-RODRIGUEZ, MARJAN FALAHRASTEGAR, JULIA E. POWLES, EMILIANO DE CRISTOFARO, AND STEVEN J. MURDOCH.

Hamed Haddadi is a Senior Lecturer in Digital Media at the School of Electronic Engineering and Computer Science, Queen Mary University of London. hamed.haddadi@qmul.ac.uk

Rishab Nithyanand is a PhD student at Stony Brook University. He is currently an OTF Senior Emerging Technology Fellow and a visitor at the International Computer Science Institute at Berkeley. rnithyanand@cs.stonybrook.edu

Sheharbano Khattak is a PhD student and Research Assistant in the Security and Networks and Operating Systems Groups at Computer Laboratory, University of Cambridge. Sheharbano. Khattak@cl.cam.ac.uk

Mobin Javed is a final year PhD student in computer science at UC Berkeley. Her research interests are in the areas of network security, privacy, and Internet measurement. mobin@cs.berkeley.edu

Narseo Vallina-Rodriguez is an Assistant Professor at IMDEA Networks, Madrid, and a Principal Investigator at the International Computer Science Institute in Berkeley, CA. narseo@icsi.berkeley.edu

Online advertising subsidizes a majority of the "free" services on the Web. Yet many find this approach intrusive and annoying, resorting to adblockers to get rid of ads chasing them all over the Web. A majority of those using an adblocker tool are familiar with messages asking them to either disable their adblocker or to consider supporting the host Web site via a donation or subscription. This is a recent development in the ongoing adblocking arms race which we have explored in our recent report, "Adblocking and Counter Blocking: A Slice of the Arms Race" [1]. For our study, we used popular adblockers, trawled the Web and analyzed some of the most popular sites to uncover how many are using anti-adblockers. Our preliminary analysis found that anti-adblockers come from a small number of providers, are widely used, and that adblockers also often block anti-adblockers.

The Perils of Targeted Advertising

The Internet economy today is largely driven by targeted advertising. Most "free" apps and Web services are bundled with third-party Web tracking [2] scripts and at times malicious code running at the user end, collecting and transmitting browsing history and personal data. Consumers often have no negotiating power in this ecosystem, despite clear evidence that such aggressive tracking and advertising often jeopardizes individuals' privacy, security, energy, and bandwidth [3]. This is particularly the case in the mobile advertising domain, where earnings are usually paid on ad impressions by the thousand, so ad brokers aim to maximize the number of ads and the frequency with which they get clicked on.

Adblockers vs. Anti-Adblockers—The Arms Race

Adblockers represent one of the ways in which consumers have retaliated against the targeted advertising industry. The main task of an adblocking software is to remove ads from users' Web pages, but some may even curb online tracking (also referred to as anti-trackers). The reasons for the rising popularity of adblockers include improved browsing experience, better privacy, and protection against malvertising. As a result, online advertising revenue is gravely threatened by adblockers, prompting publishers to actively detect adblock users, and subsequently block them or otherwise coerce the user to disable the adblocker—practices referred to as anti-adblocking (see Figure 1).

Example of Anti-Adblocking

Anti-adblocker detects adblockers by one of the following two approaches:

1. The anti-adblocker injects a bait advertisement container element (e.g., DIV), and then compares the values of properties representing dimensions (height and width) and/or visual status (display) of the container element with the expected values when properly loaded.

Marjan Falahrastegar is a PhD student at Computer Networks Group of Queen Mary University of London. marjan.falahrastegar@qmul.ac.uk

Julia Powles is a Postdoctoral Researcher in the Faculty of Law and Computer Laboratory at the University of Cambridge. jep50@cam.ac.uk

Emiliano De Cristofaro is a Senior Lecturer in the Information Security Group at University College London. e.decristofaro@ucl.ac.uk

Steven Murdoch is a Royal Society University Research Fellow in the Computer Science Department of University College London. s.murdoch@ucl.ac.uk

Figure 1: An example of an anti-adblocking message. You very likely have seen pages like this from popular new sites. These are served to users when an anti-adblocking script has determined that the user has an adblocker installed.

2. The anti-adblocker loads a bait script that modifies the value of a variable, and then checks the value of this variable in the main anti-adblocking script to verify that the bait script was properly loaded. If the bait object is determined to be absent, the anti-adblocking script concludes that an adblocker is present.

To track whether the user has turned off the adblocker after being prompted to do so, the anti-adblocker periodically runs the adblock check and stores the last recorded status in the user's browser using a cookie or local storage.

While incidents of anti-adblocking, and the legality of such practices, have received increasing attention, our current understanding is limited to online forums and user-generated reports. As a result, we lack quantifiable insights into the scale, mechanism, and dynamics of anti-adblocking. We have started to address these issues in our current research study, presented recently at USENIX FOCI '16 [1]. We did so by leveraging a novel approach for identifying third-party services shared across multiple Web sites to present a first characterization of anti-adblocking across the Alexa Top-5000 Web sites. Using a Web crawler to capture screenshots, HTML source code, and responses to all requests generated, we uncovered how anti-adblocking operates and mapped Web sites that perform anti-adblocking as well as the entities that provide anti-adblocking scripts.

Research Findings

Overall, we found that at least around 7% of Alexa Top-5000 Web sites employ anti-adblocking, with the practices finding adoption across a diverse mix o-f publishers, particularly publishers in the categories "general news," "blogs/wiki," and "entertainment." It turns out that these Web sites owe their anti-adblocking capabilities to 14 unique scripts pulled from 12 different domains. Surprisingly, anti-adblockers operate on a simple premise: if a bait object (i.e., an object that is expected to be blocked by ad-blockers—e.g., a JavaScript or DIV element named ads) on the publisher's Web site is missing when the page loads, the script concludes that the user has an adblocker installed. Figure 2 shows a summary of the types of Web sites deploying an anti-adblocking strategy.

Unsurprisingly, the most popular domains are those that have skin in the game—Google, Taboola, Outbrain, Ensighten, and Pagefair—the latter being a company that specializes in anti-adblocking services. Then there are in-house anti-adblocking solutions that are distributed by a domain to client Web sites belonging to the same organization: TripAdvisor distributes an anti-adblocking script to its eight Web sites with different country code top-level domains, while adult Web sites (all hosted by MindGeek) turn to DoublePimp. As a further element of the research, we visited a sample Web site for each anti-adblocking script

%	Category	%	Category
19.5%	General News	2.5%	Pornography
9.3%	Blogs/Wiki	2.5%	Forum/Bulletin Boards
8.5%	Entertainment	2.2%	Technical/Business Forums
4.3%	Internet Services	2.2%	Potential Illegal Software
3.7%	Sports	2.0%	Online Shopping
3.7%	Games	1.7%	Portal Sites
3.2%	Travel	1.7%	Humor/Comics
3.2%	Education/Reference	1.2%	Social Networking
2.7%	Business	1.2%	Provocative Attire
2.5%	Software/Hardware	1.2%	Marketing/Merchandising

Figure 2: Distribution of anti-adblocking Web sites by category according to McAfee's URL categorization

via AdBlock Plus, Ghostery, and Privacy Badger, and discovered that half of the 12 anti-adblocking suppliers are counter-blocked by at least one adblocker—suggesting that the arms race has already entered the next level.

Implications, Legality, and Ethics

The implications of the findings are manifold and complicated due to the involvement of a plethora of players: publishers, consumers, and a jostling array of intermediaries that compete to deliver ads, mostly supported by business models that involve taking a cut of the resultant advertising revenue. Advertising creates overhead for the users and telcos. In an extreme example, a mobile operator recently started to *block mobile ads altogether*. If such a steps were to be widely adopted, they would severely limit the degree to which app developers could continue to innovate and create while maintaining the illusion of "free" apps and content for users. Arguably, handing control of the Web ecosystem to telecom companies or small yet powerful adblocking businesses that allow advertisers to *whitelist their ads* so that they are still seen by users, is also an undesirable outcome for the freedom of the Web and Net Neutrality, and their effectiveness is debatable as this merely shifts control of which ads are displayed to users from one entity to another. Alternatively, efforts such as Brave (blog.brave.com) allow individuals to directly pay for the content of their favorite Web sites without being tracked.

The legality of adblocking is also potentially contestable under laws about anti-competitive business conduct and copyright infringement. To date, only Germany has tested these arguments in court, with adblockers winning most but not all of the cases. By contrast, anti-adblocking in the EU might in turn breach Article 5(3) of the Privacy and Electronic Communications Directive 2002/58/EC, as it involves interrogating an end-user's terminal equipment without consent.

Conclusion

Many consider adblocking to be an ethical choice for consumers and publishers to consider from both an individual and societal perspective. In reality, however, both sides have resorted to radical measures to achieve their goals. The Web has empowered publishers and advertisers to track, profile, and target users in a way that is unprecedented in the physical realm. In addition, publishers are inadvertently and increasingly serving up malicious ads. This has resulted in the rise of adblocking, which in turn has led publishers to employ anti-adblocking. The core issue is to get the balance right between ads and information: publishers turn to anti-adblocking to force consumers to reconsider the default blocking of ads for earnest publishers. But defaults are difficult to shift at scale. And, in any event, even worthy ad-supported publishers will fail if they do not redress in a fundamental way the reasons that brought consumers to adblockers in the first place. Regulation and proposals such as privacy-friendly advertising or mechanisms to give users more control over ads and trackers may provide a compromise in this space.

References

[1] R. Nithyanand, S. Khattak, M. Javed, N. Vallina-Rodriguez, M. Falahrastegar, J. E. Powles, E. De Cristofaro, H. Haddadi, and S. J. Murdoch, "Adblocking and Counter Blocking: A Slice of the Arms Race," 6th USENIX Workshop on Free and Open Communications on the Internet (FOCI 16), 2016: https://www.usenix.org/conference/foci16/workshop-program/presentation/nithyanand.

[2] M. Falahrastegar, H. Haddadi, S. Uhlig, R. Mortier, "Tracking Personal Identifiers Across the Web," Passive and Active Measurement Conference (PAM 2016), in *Lecture Notes in Computer Science*, vol. 9631, pp. 30–41: http://link.springer.com/chapter/10.1007%2F978-3-319-30505-9_3.

[3] N. Vallina-Rodriguez, J. Shah, A. Finamore, Y. Grunenberger, K. Papagiannaki, H. Haddadi, J. Crowcroft, "Breaking for Commercials: Characterizing Mobile Advertising," in *Proceedings of the 2012 ACM Internet Measurement Conference*, pp. 343–356: http://dl.acm.org/citation.cfm?id=2398812.

[4] I. Thomson, "Ad-Blocker Blocking Web Sites Face Legal Peril at Hands of Privacy Bods": http://www.theregister.co.uk/2016/04/23/anti_ad_blockers_face_legal_challenges/.