Malvertising - A Rising Threat To The Online Ecosystem

Catherine Dwyer
cdwyer@pace.edu

Ameet Kanguri
ak23433n@pace.edu

Seidenberg School of Computer Science & Information Systems
Pace University
New York, New York, USA

Abstract

Online advertising is a multi-billion dollar industry that supports web content providers around the globe. A sophisticated technology known as real time bidding (RTB) dominates the advertising landscape, connecting advertisers with specific online customers of interest. With RTB, when web visitors connect to a site, advertising networks are notified of space available on that site along with what can be gleaned about the visitor. These combinations of space and visitor are auctioned, and the winning bid's ad content is served to the web visitor. The entire process, from a visitor landing on a publisher's page to ads being auctioned, selected and served, takes 200 milliseconds, the time needed to snap your fingers. This tightly choreographed interaction is a technical marvel, but one with built in risks. The just-in-time collaboration between ever changing technology providers gives an opening to malicious actors, who through devious means, use ad networks to deliver malware rather than ads. Delivering malware as an ad is called malvertising, and its presence on otherwise credible sites is dangerous, undermining the business models of trustworthy publishers and legitimate online advertisers. The purpose of this paper is to introduce malvertising, describe its relationship with online advertising, and identify the risks RTB and malvertising bring to the online ecosystem.

Keywords: malware detection, malvertising, online advertising, ad blockers, real time bidding (RTB).

1. INTRODUCTION

The web as we know is it funded in large part by advertising revenue. Google and Facebook derive most of their funding from online advertising in one form or another (Gjorgievska, 2016).

Google introduced bidding for ads associated with specific search terms with the introduction of AdWords in 2000 (Mehta, Saberi, Vazirani, & Vazirani, 2007). With AdWords, advertisings compete with each other to serve ads to users based on search terms and cookie data. Companies such as RightMedia and DoubleClick expanded the bidding process beyond search advertising. By 2011 RTB had become the dominant mechanism for online advertising (Chen, Berkhin, Anderson, & Devanur, 2011).

The online advertising ecosystem is an multifaceted technical network matching buyers and sellers of ad space on pages currently under view by web visitors who match specific profiles of interests. Given this happens on millions of web pages seen by millions of web visitors, all within a window of 200 milliseconds (Lederer, 2014), online advertising can be considered one of the most technologically advanced information systems ever developed.

As of 2016, 23 different sub-categories of companies have been identified that participate

in the market for online display advertising (Kawaja, 2016). For the purposes of this paper, we will focus on these players:

1) Publisher - Companies or individuals that generate content for the consumption of consumers. Publishers monetize their content by putting up ads besides their content. Examples of publishers include NYTimes.com and Forbes.com.

2) Supply Side Platform (SSP) - A supply-side platform or sell-side platform (SSP) is a technology platform hired by publishers to manage their online advertising space inventory, fill it with ads, and receive revenue. Examples of SSPs include Rubicon and Pubmatic.

3) Demand Side Platform/Ad network (DSP) - A demand side platform hired by advertisers to manage their bids for online ad space. Examples of DSPs include MediaMath and InviteMedia.

4) Ad exchange – Like a stock exchange, it brings together buyers and sellers of online ad space. Examples of ad exchanges include DoubleClick (owned by Google) and OpenEx.

5) Digital marketer - Advertising agencies representing large companies wanting to post advertisements online. Examples include OmniconGroup and WPP (Ju, 2013).

The interaction that takes place in online advertising is diagrammed in Figure 1 (Kneen, 2015). When a web visitor lands on a web page (labeled as step 1), it is loaded along with an ad tag embedded in the page (step 2). This tag triggers a further call to an SSP, passing along the ad dimensions and the identity of the publisher (step 3 and 4). From there the SSP reads the SSP cookie (step 5) from the user's machine (most users already have a SSP cookie which is created while visiting an earlier site). Major SSPs claim to have cookie coverage of 80% across US users (Ad Ops Insider, 2010).

The SSP then requests bids through the ad exchange from a host of DSPs (step 6 and 7). The SSP cookie is passed on to each DSP and this helps the DSPs value the impression. The DSP matches the cookie data to their own cookie data (step 8, 9 and 10), which in-turn is tied to a huge cache of marketer data and third party data. In a nutshell this data is a detailed browsing history of the user that marketers and data brokers have collected. The richer the data available about the user, the higher the bids from DSPs (Ad Ops Insider, 2010).

Using this information the DSPs place bids and send an ad redirect link to the SSP in case it wins the bid. The SSP selects the winning bid, and sends the DSP link to the user, whose browser then calls the marketer's server to display the ad (steps 11 and 12). The RTB ad serving process is complete. The entire process takes about 200 milliseconds (Kneen, 2015).

The nature of the online advertising ecosystem and the rapidly changing collection of companies participating in online advertising has creating an opportunity for malicious actors to masquerade as advertisers (Zarras et al., 2014), who can use the existing real time bidding advertising ecosystem to quite effectively deliver malware (Segura, 2015), and even specifically target individuals of interest, such as those that work in defense industries (Invincea, 2015a). Cyphort Labs, a provider of anti-malware services, issued a report that noted an increase in documented malvertising campaigns of 325% (2015). MalwareBytes has documented the presence of malvertising on msn.com (Segura, 2016).

2. WHAT IS MALVERTISING?

Malvertising is the seeding of malicious code in online advertisements and delivering these to unsuspecting users visiting common and trusted websites, such as huffingtonpost.com, twitter.com, and cnn.com (Mimoso, 2015).

Online malware is a serious problem, one that affects individuals and organizations. An important element of safe internet use is avoiding suspicious, criminal, or inappropriate websites ("Safe Internet Use," 2016). Another important practice is vigilance with email, and staying away from links that seem suspicious in any way ("Spam & Phishing," 2016).

It certainly is a safer practice to only visit legitimate sites, those whose authenticity can be independently verified. While this is excellent advice, the use of online advertising networks by malicious actors to distribute malware on legitimate sites means that more rigorous methods must be developed to control the distribution of malware on the Internet.

Most sites and publishers rely heavily on online advertisements to monetize visits to their sites. According to the Interactive Advertising Bureau (IAB), online advertising in the USA reached $27.5 billion in the first half of 2015, a 19% rise over first half of 2014 ("Digital Ad Revenues Surge 19%, Climbing to $27.5 Billion in First Half Of 2015," 2015). It is expected to continue to grow at a similar pace over the next few years.

RTB is a sophisticated technological interchange that has created a marketplace where many technology companies exchange bids and serve ads. The multi-party nature of this highly automated bidding exchange has introduced a risk in the form of malvertising.

Publishers are connected with advertisers by a network of companies, and the entire process is opaque to the end user. Ads are sold via a bidding process, and apart from the type of ad displayed, the publisher does not control which advertiser wins the bid and post ads. This allows not just legitimate parties but also miscreants to bid for ads (Invincea, 2015a).

Attack methods used in malvertising include deceptive downloads, link hijacking, and drive by downloads. Deceptive downloads lure their victims to download malicious software components disguised as browser plugins and other software add ons. This happens by having the user believe that to access some desirable content they need to install a particular software component.

In link hijacking the user is automatically redirected away from safe websites to sites with exploits. This is done by inserting malicious code in the ads that causes the redirect.

The most dangerous method is called a "drive-by-downloads". The risk from drive by downloads is that the user may infect his or her computer by merely visiting the website, even without directly interacting with malicious part of the page. In this scenario the malicious exploit is originates from the ad network server and probes for browser vulnerabilities. The most common targets among attackers are machines with outdated plugins for Java and Flash (Zarras et al., 2014).

Malvertising is the use of online advertising as a vector to deliver malware. It involves the injection of malicious or malware laden advertisements into legitimate, recognized web sites such as Yahoo.com (Grandoni, 2015), MSN.com (Segura, 2016), and dictionary.com (Invincea, 2015b). By injecting malware via advertising into high profile web sites, users not typically vulnerable to malware can be targeted. This infection can take place "silently," through techniques such as drive by downloads that do not require any action by the web site visitor other than opening the page in a browser.

A report by the IAB and Ernst and Young included this sobering comment about malvertising: "the need to click on the malware to be infected is a common misconception of the public," ("What Is An Untrustworthy Supply Chain Costing The U.S. Digital Advertising Industry?," 2015). Through malvertising, the profiling capabilities of online advertising can be re-purposed to target individuals and organizations of interest, for the distribution of ransomware, and theft of intellectual property.

The security firm Invincea has documented dozens of these attacks taking place on sites such as cbssports.com, match.com, answers.com, and realtor.com (Invincea, 2015b).

3. MALVERTISING AND AD BLOCKERS

If malware can be delivered through advertising networks, then it has been suggested that using an ad blocker will also block malvertising. In 2015 Edward Snowden endorsed the use of ad blockers to protect against attacks through malvertising, saying "as long as service providers are serving ads with active content that require the use of Javascript to display, that have some kind of active content like Flash embedded in it, anything that can be a vector for attack in your web browser — you should be actively trying to block these," (Lee, 2015). While many claim that ad blockers can protect you, no empirical studies have been published to date that prove that ad blockers protect against malvertising.

Ad blockers have been at the center of a dispute between publishers and the developers of ad blocking software. The head of the IAB has criticized ad blockers, and the organization has begun a public campaign against them, arguing they "are stealing from publishers, subverting freedom of the press, operating a business model predicated on censorship of content and ultimately forcing consumers to pay more money for less—and less diverse—information." (Heine, 2016). Some publishers prevent web visitors using ad blockers from viewing content, including wired.com and forbes.com (Schneier, 2016).

The use of ad blockers by online users has been criticized by publishers. Ad blockers are found on 15% of all US internet browsers ("The 2015 Ad Blocking Report," 2015). Most ad blockers are installed as browser plugins, with the two most popular versions being AdBlock and Adblock plus. Irrespective of the ad blocker used, most ad blockers rely on a collaborative database called EasyList ("Ad Blockers a guidebook for publishers, advertisers and Internet users," 2014) . EasyList gathers a list of regular expressions that recognize an ad versus other content. These are sequences of code written to

spot keywords or frameworks inside a webpage. Contributors submit any new sequences to the community who then reviews and approves it. Having more than 80,000 expressions it is largest reference database for all ad blockers.

Ad blockers do not differentiate between legitimate ads and malvertising, they block both. If the expression of code pattern is found on the web page the ad is blocked. This acts like a double edged sword. While on one side with an updated database and a vibrant community adblockers block most malware, they also block legitimate ad content that is displayed on websites. But with advertisements hurting earnings of publishers, a few of them have resorted to not displaying their content (or charging a fee) if they detect an ad blocker installed on the user browser. Forbes (Patrizio, 2016) and Wired (Zorabedian, 2016) are more recent publishers who do not allow those using an ad blocker to view content for free on their site.

4. RISKS TO THE ONLINE ECOSYSTEM

The more automated online advertising is, the greater the efficiencies built into the system, the greater the opportunity for a malicious actor to exploit RTB.

There are challenges for publishers and online advertisers that make it more difficult to address the risks of malvertising and RTB. For one, publishers do not make as much money from online content as they made with print versions in the past and are vulnerable to any disruption in online revenue.

Secondly, online advertising depends on speed. One technique to disrupt malvertising is to place stricter controls over what files can be served as ads, however this can only slow the process down. The actual ad content does not come from either the publisher or the ad exchange, it comes from a separate technology company that optimizes its delivery. So there is a security supply chain problem in place. Checking the validity of ad content will only make the process less efficient and more time consuming.

The proliferation of malvertising on trusted sites has led businesses to turn to security solutions such Blue Coat that maintains a blacklist of known malware sites, including a number of ad networks. This acts like a super ad blocker, blocking any ad delivery to a corporate environment (Mimoso, 2015).

For high income consumers visiting trusted sites like Forbes.com, they are attractive bait for exploits such as ransomware delivered through advertising. The success of these exploits are directly related to RTB, says Pat Belcher, director of malware analysis at the security company Invincea. "RTB has made it easier for malware authors to target individuals. Before RTB, you had to compromise the ad delivery network. Now, you not only win bids and place ads, you can use the same platform to pinpoint and target anyone you want" (Mimoso, 2015).

In some ways this dilemma resembles the troubles advertisers and publishers have encountered with the collection of web browsing data. It is the use of these vast troves of data to serve carefully targeted ads that raises privacy concerns, and in trying to make a perfect match instantly, millions of times a day, has created an opening for malvertising that could undermine the trust that is the foundation of ecommerce and the online market.

In addition to the risk of malvertising, because ad bids are higher if more can be discovered about the digital profile of a web visitor (Ad Ops Insider, 2010), there is a perverse incentive for publishers to collect and share as much information as possible with ad networks. And ad networks then collaborate through cookie sharing to precisely identify who is the online viewer, whether that person is at work, at home using a tablet, or on the go using their smart phone (Schiff, 2016).

5. CONCLUSIONS

Computer security best practices encourage end users to deploy strong passwords and avoid suspicious links. These however do not protect against drive-by downloads delivered by malvertising. If you do have a strong password and do avoid suspicious links, what else do you need to do to avoid malvertising? It is critically important to keep browsers and all plug-ins updated. It has also been suggested that ad-blockers can also protect the end user from infection by malware, since the online ad is the vector of delivery for the malware, since the ad-blocker blocks the ad, in theory it also blocks the malware.

Right now the web depends on advertising for most of its financial support. However, that business model has opened the door to malware attacks using online ads as a vector. While publishers can say that the use of ad blockers does hurt their revenue, is also means publishers have an obligation to protect their site from malvertising. Given that RTB depends on a window of 200 milliseconds to deliver an ad

(Lederer, 2014), there needs to be another control mechanism to ensure that bad actors cannot exploit this bidding process to serve malware.

Online advertising has grown into a multi-billion dollar industry by allowing advertisers to serve ads based on individual profiles, geolocation, client machine, and even a specific range of IP addresses. These precise targeting capabilities also make malvertising an attractive option for malicious actors. The customized delivery of ads also allows malvertising to hide from detection by employing stealthy targeting schemes that alternate the placement benign advertising with the sporadic placement of malware (Cyphort, 2015).

Combatting malvertising will require an intricate multi-platform effort. It will require vigilance and adoption of best practices by multiple actors, including publishers/web hosting sites, ad networks, and web surfers. Publishers must require ad networks to develop an active prevention plan in place against malvertising. And ad networks will need to be more vigilant about the content of the ads they serve. As online ads take on more dynamic properties, including embedded scripts that customize the ad's content and appearance, then ad networks will need strict controls to ensure those scripts do not inject malware. Web surfers must protect themselves by keeping their browsers up to date, and where possible, disabling vulnerable plugins such as Java and Flash. So it is up to publishers, online advertisers, and the people who use those sites to work together to ensure the security of the web.

6. REFERENCES

The 2015 Ad Blocking Report. (2015). Retrieved from https://blog.pagefair.com/2015/ad-blocking-report/

Ad Blockers a guidebook for publishers, advertisers and Internet users. (2014). Retrieved from http://www.secretmedia.com/whitepaper/adblocker_whitepaper.php

Chen, Y., Berkhin, P., Anderson, B., & Devanur, N. R. (2011). Real-time bidding algorithms for performance-based display ad allocation. Paper presented at the Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining.

Cyphort. (2015, February 26, 2016). The Rise of Malvertising. Retrieved from http://go.cyphort.com/Malvertising-Report-15-Page.html

Digital Ad Revenues Surge 19%, Climbing to $27.5 Billion in First Half Of 2015. (2015). Retrieved from http://www.iab.com/news/digital-ad-revenues-surge-19-climbing-to-27-5-billion-in-first-half-of-2015-according-to-iab-internet-advertising-revenue-report/

Gjorgievska, Aleksandra (2016), Google and Facebook Lead Digital Ad Industry to Revenue Record. Retrieved from http://www.bloomberg.com/news/articles/2016-04-22/google-and-facebook-lead-digital-ad-industry-to-revenue-record

Grandoni, D. (2015). Hackers Exploit 'Flash' Vulnerability in Yahoo Ads. Retrieved from http://bits.blogs.nytimes.com/2015/08/03/hackers-exploit-flash-vulnerability-in-yahoo-ads/?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=0

Heine, C. (2016). IAB Chief Blasts Adblock Plus as an 'Immoral, Mendacious Coven of Techie Wannabes'. adweek. Retrieved from http://www.adweek.com/news/technology/iab-chief-blasts-adblock-plus-immoral-mendacious-coven-techie-wannabes-169194

How RTB ad serving works (2010). Retrieved from http://www.adopsinsider.com/ad-serving/diagramming-the-ssp-dsp-and-rtb-redirect-path/

Invincea. (2015a). A case study in successfully defeating malvertising attacks. Retrieved from https://www.invincea.com/2015/09/white-paper-a-case-study-in-successfully-defeating-malvertising-attacks/

Invincea. (2015b). Fessleak: The Zero-Day Driven Advanced RansomWare Malvertising Campaign. Retrieved from https://www.invincea.com/2015/02/fessleak-the-zero-day-driven-advanced-ransomware-malvertising-campaign/

Ju, R. (2013). Online Advertising Explained: DMPs, SSPs, DSPs and RTB. Retrieved from http://www.kbridge.org/en/online-advertising-explained-dmps-ssps-dsps-and-rtb/

Kawaja, T. (2016). Display LUMAscape. Retrieved from http://www.lumapartners.com/lumascapes/display-ad-tech-lumascape/

Kneen, B. (2015). HOW REAL TIME BIDDING, DSPS, SSPS, AND AD EXCHANGES WORK. Retrieved from http://www.adopsinsider.com/ad-serving/how-dsps-ssps-and-ad-exchanges-work/

Lederer, B. (2014). 200 Milliseconds: Life of a Programmatic RTB Ad Impression. Programmatic Insider. Retrieved from http://www.mediapost.com/publications/article/225808/200-milliseconds-life-of-a-programmatic-rtb-ad-im.html

Lee, M. (2015). Edward Snowden Explains How to Reclaim Your Privacy. Retrieved from https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/

Mehta, A., Saberi, A., Vazirani, U., & Vazirani, V. (2007). Adwords and generalized online matching. Journal of the ACM (JACM), 54(5), 22.

Mimoso, M. (2015). Ad networks ripe for abuse via malvertising. Retrieved from https://threatpost.com/ad-networks-ripe-for-abuse-via-malvertising/111840/

Patrizio, A. (2016). How Forbes inadvertently proved the anti-malware value of ad blockers. Retrieved from http://www.networkworld.com/article/3021113/security/forbes-malware-ad-blocker-advertisements.html

Safe Internet Use. (2016). Retrieved from https://www.getsafeonline.org/protecting-your-computer/safe-internet-use/

Schiff, A. (2016). A Marketer's Guide To Cross-Device Identity. Retrieved from http://adexchanger.com/data-exchanges/2016-edition-marketers-guide-cross-device-identity/.

Schneier, B. (2016, February 23). The Ads Versus Ad Blockers Arms Race. Retrieved from https://www.schneier.com/blog/archives/2016/02/the_ads_vs_ad_b.html

Segura, J. (2015). Real-time Bidding and Malvertising: A case study. Retrieved from https://blog.malwarebytes.org/malvertising-2/2015/04/real-time-bidding-and-malvertising-a-case-study/

Segura, J. (2016). MSN Home Page Drops More Malware Via Malvertising. MalwareBytes Blog. Retrieved from https://blog.malwarebytes.org/malvertising-2/2016/01/msn-home-page-drops-more-malware-via-malvertising/

Spam & Phishing. (2016). Retrieved from https://staysafeonline.org/stay-safe-online/keep-a-clean-machine/spam-and-phishing

What Is An Untrustworthy Supply Chain Costing The U.S. Digital Advertising Industry? (2015, February 26, 2016). Retrieved from http://www.iab.com/insights/what-is-an-untrustworthy-supply-chain-costing-the-u-s-digital-advertising-industry/

Zarras, A., Kapravelos, A., Stringhini, G., Holz, T., Kruegel, C., & Vigna, G. (2014). The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements. Paper presented at the Proceedings of the 2014 Conference on Internet Measurement Conference, Vancouver, BC, Canada.

Zorabedian, J. (2016). Wired to ad blocker users: pay up for ad-free site or you get nothing. Retrieved from https://nakedsecurity.sophos.com/2016/02/10/wired-to-ad-blocker-users-pay-up-for-ad-free-site-or-you-get-nothing/

ISSN: 2167-1508
v9 n4266

Appendix

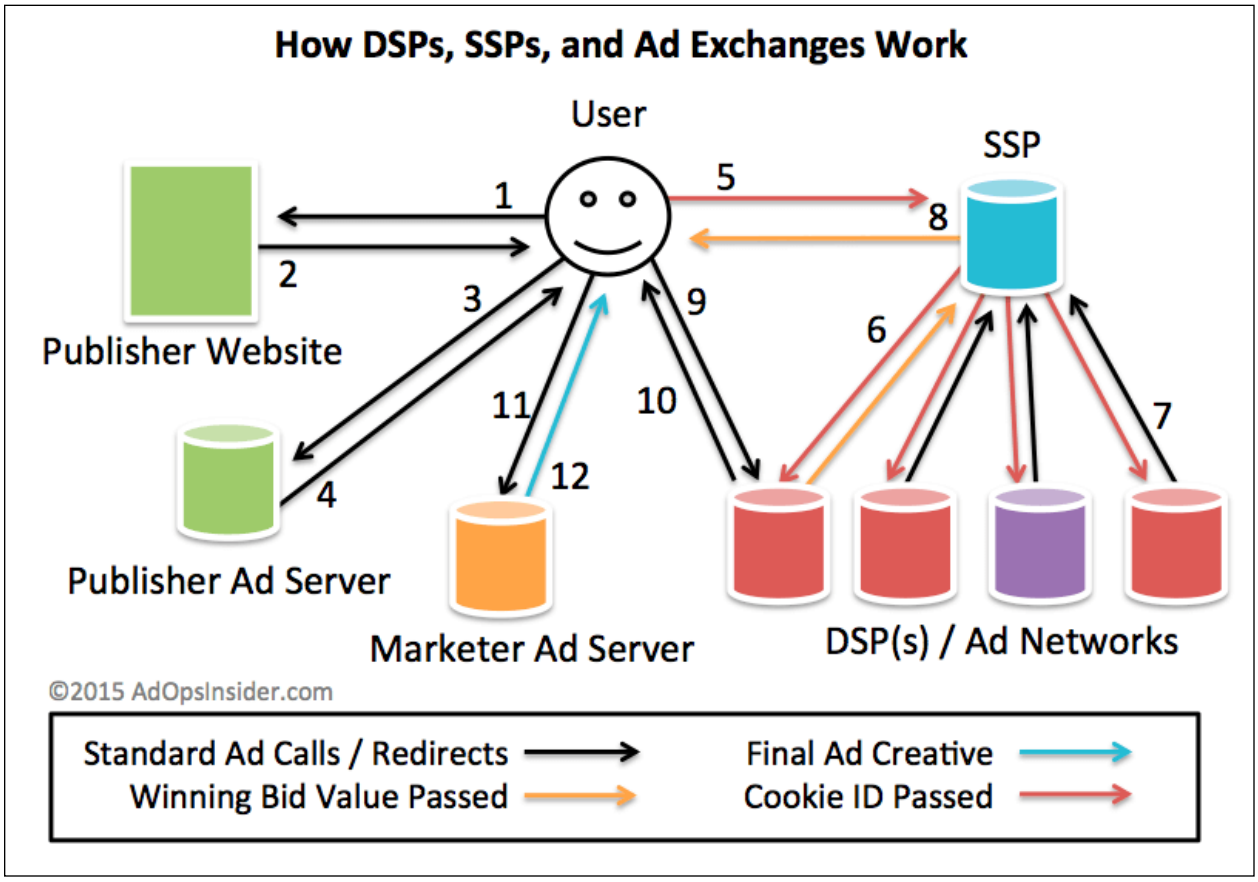

Figure 1: How DSPs, SSPs and Ad Exchanges work