2016

Gone in 200 Milliseconds: The Challenge of Blocking Malvertising

Catherine Dwyer
Seidenberg School of CSIS, Pace University

Ameet Kanguri
Pace University

Gone in 200 Milliseconds: The Challenge of Blocking Malvertising

by
Catherine Dwyer
Ameet Kanguri
Pace University
cdwyer@pace.edu
ak23433n@pace.edu

Abstract

Online advertising is a multi-billion dollar global industry that lets advertisers serve ads to specific customers of interest as they browse the web. Using real time bidding (RTB), as web visitors land on a site, advertising networks are alerted of space available and whatever profile information can be gleaned about the visitor. Ad networks then auction this combination of space and profile through ad exchanges, and the winning bid's ad content is then 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. Operating in such a short time frame requires efficiency and speed, so ad networks typically do not host ad content, and rely on servers optimized to quickly deliver content. 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 can hire a digital marketer, purchase online advertising space, and through devious means, use ad networks to deliver malware rather than ads. The practice of delivering malware as an ad has been termed malvertising, and its incidence is increasing at an alarming rate. This article will present examples of malvertising, describe its relationship with online advertising, and discuss ways to reduce the incidence of malvertising attacks.

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

Introduction

The online advertising ecosystem is an extremely complex, 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, online advertising can be considered one of the most technologically advanced systems ever developed. The infographic in Figure 1 shows the current state of the online advertising ecosystem, one that continues to change and evolve, requiring updates to this infographic on a regular basis (Kawaja 2016).

The companies that participate in the market for online display advertising are grouped into 23 different sub-categories. The specific players in the online ad ecosystem relevant to this paper are:

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 to enable web publishers to manage their 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 enables digital advertisers to effectively bid for ad space on publisher's website. Utilizing a DSP, marketers can manage their bids. Examples of DSPs include MediaMath and InviteMedia.

4) Ad exchange (RTB enabled)- It is similar to a stock exchange. It provides a platform for bidding ads and connects a SSP to multiple DSPs. 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)

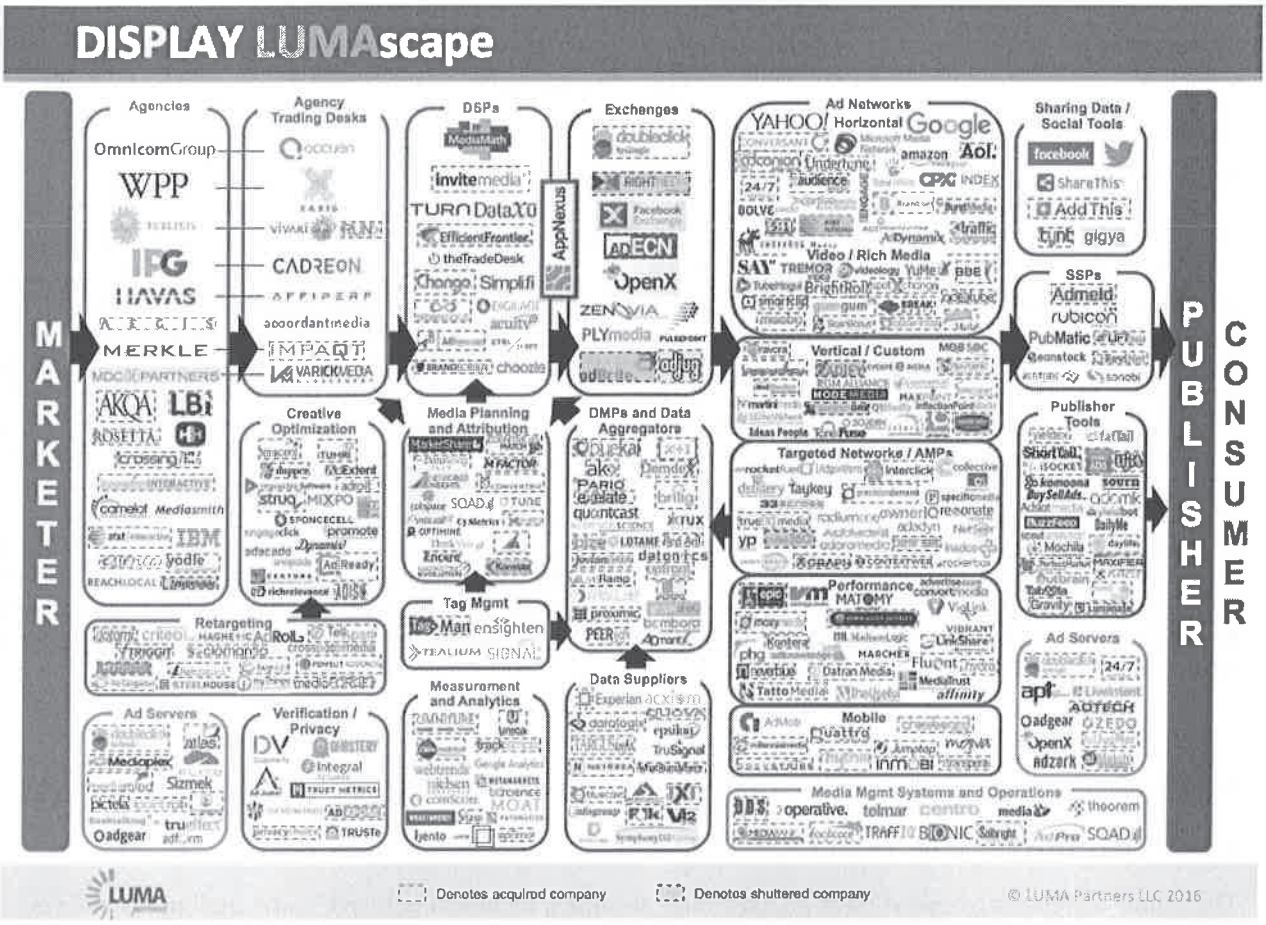

Figure 1. Advertising Landscape: LUMAscape

The interaction that takes place in online advertising is presented in Figure 2. When a web visitor lands on a web page, it is loaded along with an ad tag embedded in the page. This tag triggers a further call to an RTB enabled SSP, passing along the ad dimensions and the publisher site id. From there the SSP reads the SSP cookie from the user's machine (most users already have a SSP cookie which is created while visiting an earlier site). If the cookie is missing on the end user the bidding price of the ad comes down significantly as there is no prior information of the user and the ad becomes more generic. Most major SSPs claim to have cookie coverage of 80% across US users.

The SSP starts the bidding by requesting bids from a host of DSPs. The SSP cookie is passed on to the DSP and this helps the DSPs value the impression. The DSP matches the cookie data to their own cookie data 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.

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 that calls the marketer's server to

display the ad. The RTB ad serving process is complete. The entire process is completed in under 200 milliseconds. (Kneen 2015)

The complexity 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), and 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).

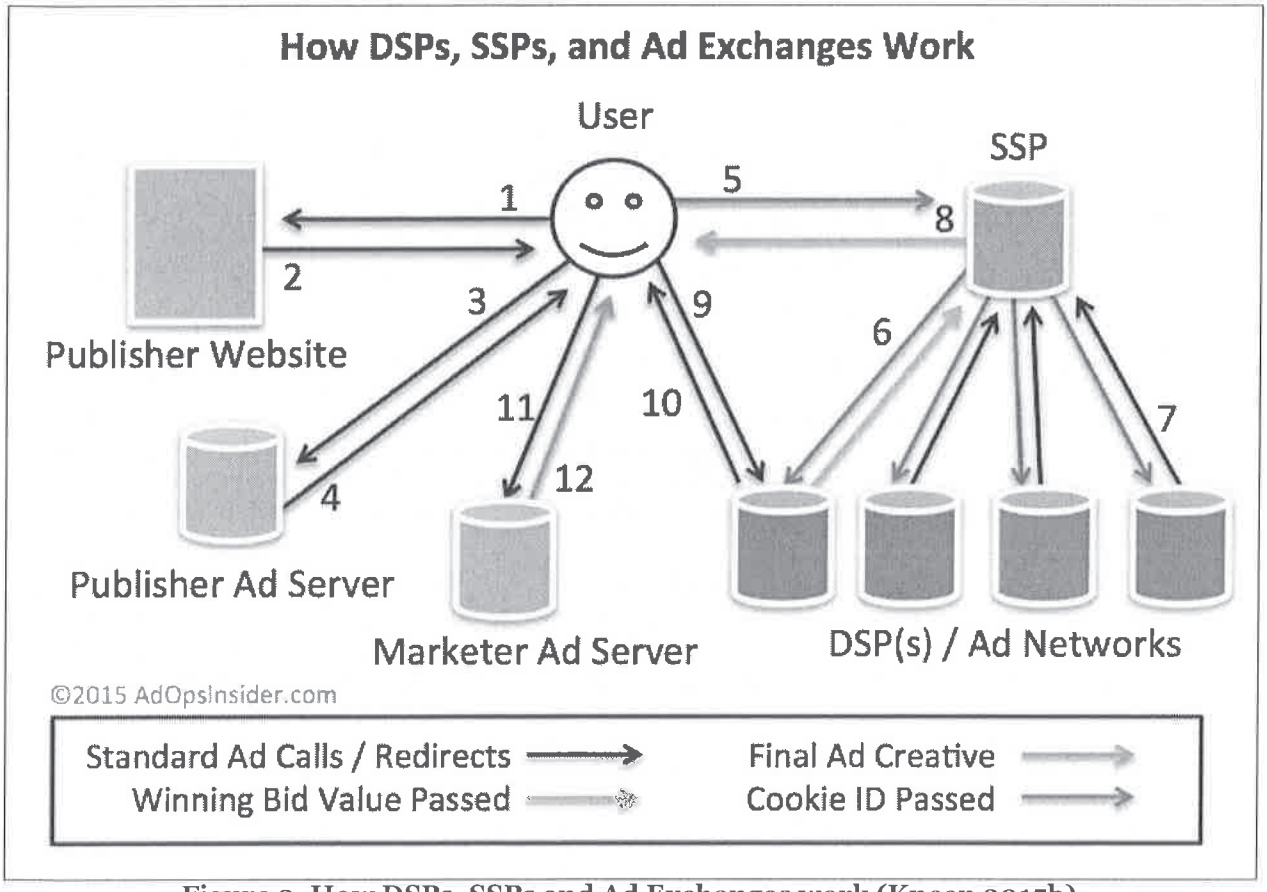

Figure 2. How DSPs, SSPs and Ad Exchanges work (Kneen 2015b)

What is Malvertising?

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 (2016a). Another important practice is vigilance with email, and staying away from links that seem suspicious in any way (2016b).

It 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 (2015a). It is expected to continue to grow at a similar pace over the next few years.

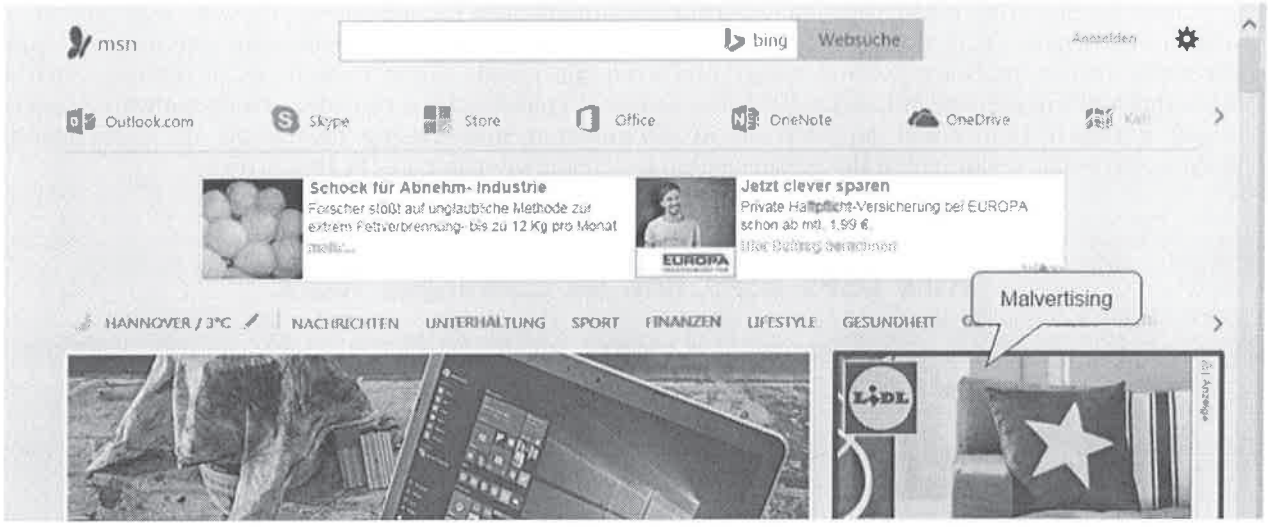

Figure 3. Malvertising on msn.com

Publishers are put in contact with advertisers by a complex network of companies and the entire process is not very transparent to the end user. The ads are sold via a bidding process and the publisher does not control which advertiser will win the bid and post ads (apart from the kind of content that should be displayed). This allows not just legitimate parties but also miscreants to bid for ads (Invincea 2015a). Malvertising is seeding 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).

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 to websites they had not decided to visit. This is done by inserting malicious code in the ads which are included in iframes that facilitates in the page redirect. The most stealthiest of them is "drive-by-downloads". In this scenario the malicious exploit is setup on the ad network server and tries to attack browser vulnerabilities. The most common targets among attackers are machines with outdated plugins for Java and Flash (Zarras et al. 2014). 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.

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 Interactive Advertising Bureau (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" (2015b). 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.

Table 1 is a list of known malvertising attacks, as identified by the security firm Invincea that were carried out from October 2014 to February 2015 (Invincea 2015b).

Date	Source	Malvertised on:
Oct 17, 2014	216.157.99.23	webmail.nc.rr.com
Oct 22, 2014	216.157.99.25	Lucianne.com
Oct 29, 2014	216.151.221.212	Vyped.com
Nov 2-11, 2014	chebroom.com	Mail.twc.com, lucianne.com huffingtonpost.com, Photobucket.com, DNSrsearch.com, RT.com, answers.com,
Nov 12-14, 2014	Kenthopm.org	Hrtwarming.com, thesaurus.com
Nov 19, 2014	vectallies.org	Mail.twc.com
Nov 21-24, 2014	hevpazana.org	Answers.com, dictionary.reference.com, techeblog.com
Dec 10-11, 2014	labutinra.org	Dictionary.reference.com POF.com mail.twc.com webmail.nc.rr.com Windstream.net
Dec 12, 2014		Sailinganarchy.com mjsbigblog.com
Dec 21, 2014	pinkavuz.org	Worthly.com
Dec 25-26, 2014	beatrinko.org	Thehulltruth.com answers.com Windstream.net
Dec 27, 2014	vemisaio.org	Sailinganarchy.com nydailynews.com dictionary.reference.com answers.com
Dec 28, 2014	zhonte.org	News.com.au match.com mail.twc.com
Dec 29, 2014	binachio.org	Answers.com realtor.com opposingviews.com dailysanctuary.com uticaod.com
Dec 31, 2014-Jan 1, 2015	zarafint.org	Answers.com webmail.nc.rr.com mail.twc.com
Jan 3, 2015	landors.org	Photobucket.com
Jan 4, 2015	tesuin.org	Pof.com nj.com
Jan 5, 2015	rliner.org	Search.aol.com realtor.com photobucket.com
Jan 8, 2015	litpou.org	Cinemablend.com popularmechanics.com
Jan 9, 2015	fersob.org	Webmail.windstream.net
Jan 11, 2015	estuty.com	Huffingtonpost.com
Jan 12, 2015	ontiq.com	Thehouseofsmiths.com webmail.earthlink.net mail.twc.com
Jan 13, 2015	deinq.com	Mapquest.com
Jan 14, 2015	ermuz.com	Dictionary.reference.com
Jan 20-21, 2015	azurf.org	Webmail.nc.rr.com pof.com webmail.windstream.net
Jan 27, 2015	relom.org	Noodlenuke.com
Jan 28, 2015	retilio.com	Worthly.com webmail.nc.rr.com chowhound.chow.com 100gateswalkthrough.com
Jan 29, 2015	uvreno.com	Sailinganarchy.com

Feb 2, 2015	64.34.127.86	Theblaze.com realtor.com webmail.nc.rr.com thesaurus.com
Feb 3, 2015	64.34.127.134	answers.com
Feb 3, 2015	tunim.net	Thebrofessional.net

Table 1. Malvertising attacks from October 2014 to February 2015

Malvertising and Ad Blockers

If malware can be delivered through advertising networks, then it has been suggested that by using an ad blocker you can 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 you against malvertising.

Ad blockers have been at the center of a separate 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 are beginning to prevent web visitors using ad blockers from viewing content, including wired.com and forbes.com (Schneier 2016).

It has been suggested that the use of ad blockers can protect against malware infection through advertising. However, the authors have not been able to find any empirical data to support this claim. This paper then describes an experimental design that will test the hypothesis as to whether the use of ad blockers does indeed protect against infection through malvertising.

Ad blockers have recently been a topic of debate among online users and online publishers. Ad blockers are enabled on 15% of all US internet browsers (pagefair 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 (media 2014) . EasyList gathers a list of regular expressions, 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 currently do not differentiate between legitimate ads and malvertising, they will 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 the adblockers block most malwares, 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.

Can Ad Blockers Block Malvertising? Experimental Design

The purpose of this experimental design is to test the hypothesis that browsing while using an ad blocker can protect you from infection via malvertising. In order to test this hypothesis, browsing will be conducted both with and without ad blockers, and the machines will then be compared for any evidence of infection through malvertising.

One of the challenges of designing this type of experiment is the intent to get infected, i.e. get malware on a machine. This requires precautions to protect malware from causing damage or spreading on other networks. The use of virtual machines is a common way that computer security researchers investigate viruses and malware. The virtual machine serves as a protective container between malware and specific hardware.

This plan is to use a cloud provider such as Amazon Web Services, and create instances of machines both with and without ad blockers. Each machine will browse through a set list of web sites, and after visiting a significant number of sites, the machines with the ad blocker will be compared to the machines without the ad blocker. By controlling as much as possible for other variables such as browser used, web site visited, and time of visits, then the design of the experiment will provide evidence that can be used to determine if ad blockers have a protective benefit.

Conclusion

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 internet as we know it 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 a complex and 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 will need to require that the ad networks they use have an active prevention plan in place against malvertising. 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.

REFERENCES

□

2015a. "Digital Ad Revenues Surge 19%, Climbing to $27.5 Billion in First Half of 2015." Interactive Advertising Bureau (IAB).

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

2016a. "Safe Internet Use." Retrieved February 26, 2016, from https://www.getsafeonline.org/protecting-your-computer/safe-internet-use/

2016b. "Spam & Phishing." Retrieved February 26, 2016, from https://staysafeonline.org/stay-safe-online/keep-a-clean-machine/spam-and-phishing
Cyphort. 2015. "The Rise of Malvertising." from http://go.cyphort.com/Malvertising-Report-15-Page.html
Grandoni, D. 2015. "Hackers Exploit 'Flash' Vulnerability in Yahoo Ads." The New York Times.
Heine, C. 2016. "Iab Chief Blasts Adblock Plus as an 'Immoral, Mendacious Coven of Techie Wannabes'," in: *adweek*.
Invincea. 2015a. "A Case Study in Successfully Defeating Malvertising Attacks." http://www.invincea.com: Invincea.
Invincea. 2015b. "Fessleak: The Zero-Day Driven Advanced Ransomware Malvertising Campaign."
Ju, R. 2013. "Online Advertising Explained: Dmps, Ssps, Dsps and Rtb." kBridge.
Kawaja, T. 2016. "Display Lumascape." LUMA Partners.
Kneen, B. 2015. "How Real Time Bidding, Dsps, Ssps, and Ad Exchanges Work." Ad Ops Insider.
Lederer, B. 2014. "200 Milliseconds: Life of a Programmatic Rtb Ad Impression," in: *Programmatic Insider*. MediaPost.
Lee, M. 2015. "Edward Snowden Explains How to Reclaim Your Privacy." The Intercept.
media, S. 2014. "Ad Blockers a Guidebook for Publishers, Advertisers and Internet Users." Secret Media.
Mimoso, M. 2015. "Ad Networks Ripe for Abuse Via Malvertising." http://www.threatpost.com.
pagefair. 2015. "The 2015 Ad Blocking Report."
Patrizio, A. 2016. "How Forbes Inadvertently Proved the Anti-Malware Value of Ad Blockers." networkworld.com.
Schneier, B. 2016. "The Ads Versus Ad Blockers Arms Race," in: *Schneier on Security*.
Segura, J. 2015. "Real-Time Bidding and Malvertising: A Case Study." Malwarebytes Labs.
Segura, J. 2016. "Msn Home Page Drops More Malware Via Malvertising," in: *MalwareBytes Blog*.
Zarras, A., Kapravelos, A., Stringhini, G., Holz, T., Kruegel, C., and Vigna, G. 2014. "The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements," in: *Proceedings of the 2014 Conference on Internet Measurement Conference*. Vancouver, BC, Canada: ACM, pp. 373-380.
Zorabedian, J. 2016. "Wired to Ad Blocker Users: Pay up for Ad-Free Site or You Get Nothing." nakedsecurity.sophos.com.