Online Trust Alliance

Voluntary Anti-Malvertising Guidelines & Best Practices

Helping to Preserve Trust in Interactive Advertising & Content Publishing

Introduction

The Online Trust Alliance (OTA) formed the Anti-Malvertising Working Task Force in 2010 which is now expanded to become the Advertising & Content Integrity Working Group to facilitate a multi-stakeholder response to the rising tide of compromised and malicious online advertising and syndicated content. OTA staff conducted research, interviewing advertisers, publishers and trade organizations to better understand malvertising. In addition, input was obtained through interviews with law enforcement and individuals and who have had first-hand experience infiltrating the ad ecosystem.

OTA's goal is two-fold; 1) Aid in the reduction of threats to consumers, businesses and employee's privacy, identity and personal computers, 2) help protect the critical infrastructure of web sites and the advertising ecosystem. The following guidelines reflect a collaborative effort and will be updated based the evolution of the threat landscape and online fraud battlefield.

Malware perpetrators attempt to infiltrate online advertising networks, including the creation of fraudulent advertisers or advertising agencies that appear to represent legitimate brands. Known as malvertising, the cybercriminal typically masks malicious code with seemingly harmless advertisements. The victims include not only the consumer, but also the entire advertising ecosystem and the web site's reputation. The advertisements may lead to harmful or deceptive content or may directly infect a victim's computer with malicious software. Cybercriminals exploit the ability to easily "push" their attacks by exploiting the reputation of the website and the allegedly advertised brands. The rise in malvertisements reflects a change is cybercriminals modus operandi, moving towards softer targets with great reach and efficiency.

The taskforce's goals include but are not limited to:

- Develop and promote voluntary best practices and guidelines
- Develop standardized reporting and data sharing with industry and law enforcement
- Advance technical solutions to help detect, mitigate and block threats

As these and other threats continue to grow and the regulatory landscape evolves, companies need to establish an ongoing review for evolving threats. Our recommendations are meant to be a foundation to aid in the development of more comprehensive operational, security and compliance processes. The business community has a shared responsibility for the protection of consumers, by helping secure the advertising ecosystems from abuse. At the same time consumers need to insure their computer, applications and add-ins are patched and they practice safe computing.

Executive Summary

Web 2.0 provides significant value to consumers through dynamic content, contextual and relevant advertising. Users realize today tremendous value from content rich sites, free email and photo storage and other services which are directly and indirectly funded from search and display advertising. Unfortunately, as these very same services have grown, they also become the targets of exploits. Not unlike malicious email which emerged in early 2000, we are seeing a shift of malicious activity focusing on web sites, ad networks and exchanges who may be unknowingly serving malicious content and advertising.

According to the IAB, it is estimated over 1 million sites carry advertising, served by upwards of 300+ ad networks and ad exchanges. Web page content can change constantly and dynamically. The cybercriminals are taking advantage of the open system which relies on multiple parties including advertisers, ad networks, ad exchanges, ad services and site publishers. The very structure of the ad ecosystem which provides flexibility and dynamic ad serving has proven itself ripe for exploits. Not unlike the early threats of email, in the absence of integrated controls, standards and end-to-end accountability, we can only expect these attacks to persist.

The cybercriminals are increasingly gravitating to the advertising ecosystem as an efficient distribution channel, offering an increased ability to remain anonymous without any of the costs and efforts of setting up email campaigns, creating phishing sites or setting up malicious sites. Based on data reported to OTA, incidents of malvertising increased over 250% from Q1 2010 to Q2 2010, with over 100 advertising networks serving compromised display advertising.

The cybercriminals have been able to exploit the advertising ecosystems primarily through two methods. An increasing trend has been to create a fictitious identity and "front" purporting to be a legitimate advertiser or advertising agency. They provide upfront payment and often approach unsuspecting partners with the urgency of a breaking ad campaign. They simply provide the ad creative which appear legitimate on the surface. The ad is embedded with malicious code or JavaScript, often obfuscated to hide the actual code being executed or server calls being made.

The second and more traditional approach has been to breach or hack into an unprotected server, obtain an employee's log on credentials and then compromise legitimate ads. Such compromises are typically undetected to the networks and web sites that the ads are served on.

While outside the scope of the Anti-Malvertising Taskforce scope, many of these guidelines can be applied to other forms of online abuse including 1) malicious search advertising, 2) third party content publishing exploits and 3) deceptive advertising, including brand infringement, Pharma and Click Fraud.

The business community, industry, as well as users have important roles and a shared responsibility in increasing protection from these threats. Infrastructure must be hardened and business processes re-examined. Business, infrastructure providers, ISPs, web publishers and the interactive advertising supply chain need to work to help counter this abuse.

Concurrently, consumers need to practice safe computing and follow the recommendations of the recently announced efforts of the National Cyber Security Alliance and their campaign "Stop, Think and Click".[1] Users need to exercise caution when downloading documents, video and file sharing from unknown publishers and sources. Unfortunately by the nature of malvertising drive-by-downloads, occur by simply landing on a trusted site. Not unlike having to drive defensively and maintain a safe vehicle on the highway, users need to take reasonable steps in patching vulnerabilities and using anti-virus and malware services to help protect their computer from related threats. While there is no silver bullet, working together we can harden the attack surface and increase the "cost" to the cybercriminal.

Resources - Updates to this document and resources including a glossary are posted at https://otalliance.org/3Pintegrity.html . Combating these threats a list of industry solutions are available and posted at: https://otalliance.org/resources/malvertising.html#Resources. To submit comments or to suggest resources, please email OTA at admin @otalliance.org

[1] National Cybersecurity Consumer Awareness Campaign, www.onguardonline.gov

	Advertiser	Ad Agency	Ad Exchange	Ad Network	Ad Servers	Site Publisher
OPERATIONAL 1. **Create an accreditation/authentication process for new clients and agencies.** Perform fact checking to verify the credentials of the advertiser or agency. Consider the following to include but not be limited to: a) Conduct searches on the company including fact checking their contact information with their Who Is information. b) Was the domain registered recently (e.g. within the past 30/60 days)? c) Is the site hosted in different country than where the company is based? d) Is the registrant's contact info hidden behind a privacy company or uses a false address? e) Validate the email address of the advertiser. Is it authenticated?[2] f) Does the registrant have an unexpectedly high number of domain registrations (eg. there are 5 domains at the same IP but the registrant's email address has been used for 20, 30, or more domains) g) Complete a reverse-IP-lookup. Are suspicious-looking domains hosted on the same IP address? h) Can they provide reputable trade and bank references that you can verify independently? i) Verify their corporate information with the State or Province they operate out of. Does everything check out? j) Can the company provide reputable third parties who can attest to their legitimacy?		✓	✓	✓	✓	✓
2. Educate your team. Be wary of new clients or agencies that place last minute orders or have urgent campaigns to hit on weekend or holidays.		✓	✓	✓	✓	✓
3. **Validate third party ad servers**. Store tag templates and use them in your QA/review process. If a tag deviates from the standard template that you typically see from a third party ad server, escalate them for review.[3]			✓	✓		✓

[2] https://otalliance.org/resources/authentication/index.html

	Advertiser	Ad Agency	Ad Exchange	Ad Network	Ad Servers	Site Publisher
4. **Do not accept ads or creative hosted by clients who have <u>not</u> been validated or adhere to security best practices.** Upon receiving an ad, scan the ad and its click redirects for malware. Then, host the ad on your servers to retain as much proactive control as possible, and re-scan the click redirects regularly (especially closer to weekends) as the destinations may change or result in further redirections. Consider regularly scanning third-party hosted ads with an anti-malvertising monitoring tool or service.[3]		✓	✓	✓	✓	✓
5. **Create an incident response plan to notify** affected clients and partners upon the discovery of compromised or fraudulent advertising.[4] Notify ad networks providing the URL and referrer trace. OTA recommends emailing malvertising@domain.com for reporting, (*domain being the ad network or web site domain).* Sites and networks are encouraged to create a mailbox or redirect such mail for immediate review and escalation to both the ad operations and security teams to facilitate the removal or take down of the ads and retain data for potential forensics.	✓	✓	✓	✓	✓	✓
6. **Report bad actors** to law enforcement and industry groups for analysis. Include host and URL of payloads. Where possible, include a URL trace that includes referrers, a network-layer trace and contents including hashes of malicious files downloaded. OTA recommends emailing malvertising@domain.com for reporting, (*domain being the domain of the organization).* Law enforcement agencies are recommended to create a mailbox or redirect such mail for immediate review and escalation.	✓	✓	✓	✓	✓	✓

[3] See OTA site for a list of third party services and solutions https://otalliance.org/resources/malvertising.html#Resources

[4] See OTA Best Practices https://otalliance.org/resources/Incident.html

	Advertiser	Ad Agency	Ad Exchange	Ad Network	Ad Servers	Site Publisher
7. Evaluate and test all creative using an isolated and sandboxed system or third party service. *Consider scanning the creative using anti-malvertising scanner, in addition to the "static" checks below:* a) Investigate the URL's domain via WHOIS b) Open all creative including .swf files c) Inspect iframes and redirects against the freely available blacklists d) Scan Flash, PDFs and JavaScript with third party tools and resources posted at https://otalliance.org/malvertising.html e) Test creative and all files the creative's code invokes. Use a SWF-to-XML converter to detect references made from each SWF file. f) Treat creative that contains obfuscated or encrypted code with suspicion. g) Consider limiting the use of rotating or dynamic tags to known networks / advertisers *(Note when rotating tags are used, the ad network domain in the tag may be irrelevant as arbitrary levels of syndication and/or sub-syndication can occur)*.[5]	✓	✓	✓	✓	✓	✓
8. **Re-evaluate and re-test "high risk" creatives on a regular basis.** "High risk" creative may be ads which were created within the past week or two, or contain rotating tags. *Re-evaluation and re-testing of high risk creative should be done more frequently as weekends near, when malvertisers are more likely to attack.* [3]		✓	✓	✓	✓	✓
9. Thoroughly examine and vet any creative which includes obfuscated script. Threat with suspicion until verified. Use of obfuscated script is a known tactic for attempting to bypass pop blockers and distribute malware. *Attempted use should be reported (see #5 above). Note is it recognized they may be some limited legitimate uses for obfuscated script; e.g., intellection property protection for ad creatives and should only be accepted by known advertisers who can assert the integrity and security of their creative being free of malware.*	✓	✓	✓	✓	✓	✓

[5] Each point in the advertising supply chain needs regular testing to detect malvertisements. As ad servers call other ad servers via chains of ad tags, each of these are potential insertion points for malware in an ad. See OTA site for resources and tools. https://otalliance.org/malvertising.html

	Advertiser	Ad Agency	Ad Exchange	Ad Network	Ad Servers	Site Publisher
10. Configure all PCs and devices for automatic updates	Highly recommended for all internal systems & devices					
11. Install anti-malware and virus protection.	✓	✓	✓	✓	✓	✓
12. **Update all employees' systems to the current browser version.**	Highly recommended for all internal systems & devices.					
13. **Scan applications and browser add-ons.** To minimize threats, uninstall unused and end of life software. Consider third party desktop tools to provide-real-time monitoring and patching of applications.	Highly recommended for all internal systems & devices					
14. **Launch a "patch" policy for all computers/devices used by employees who manage ad campaigns and have access to ad infrastructure.** Ensure systems have updated/patched operating systems, and have the latest application patches installed.	✓	✓	✓	✓	✓	✓
15. **Leverage best practices for authentication/ log-in credentials to help prevent account takeovers.** To include but not be limited to frequent password resets and automatic account disable after a pre-set number of log on attempts, two-factor authentication and challenge response questions.	✓	✓	✓	✓	✓	✓
16. Implement email authentication for all inbound and outbound servers. Cybercriminals and fraudulent business often forge or spoof their email address purporting to represent legitimate businesses. Email authentication through the use of SPF/Sender ID and DKIM are proven industry standards to counter email forgery often used in phishing and to capture log on credentials.[6] *Email from a free email account or not from the same domain as the company domain should be considered highly suspicious even if they can be authenticated.*	✓	✓	✓	✓	✓	✓

[6] https://otalliance.org/resources/authentication/index.html