



ANTI- MALWARE

CERTIFIED AGAINST MALWARE

TAG Malvertising Taxonomy

Version 2.0

Release: April 2024



The mission of the TAG Certified Against Malware Program is to prevent, mitigate and remediate malware events using the digital advertising supply chain as an attack vector.

Since 2014, the TAG (the Trustworthy Accountability Group) has partnered with industry leaders to design and strengthen the Certified Against Malware Program, providing companies with a roadmap for taking on the complicated issue of malvertising.

A survey of U.S. consumers conducted by the Brand Safety Institute (BSI) found that 93% of respondents would reduce their spending on an advertised product if the ad had infected their computers or mobile devices with malware – and 73% would stop buying that product altogether. Additionally, the Federal Trade Commission¹ indicated that consumers lost \$5.8 billion to online scams in 2021, up more than 70% over losses reported in 2022, and malvertising is understood to be a common threat vector for these crimes.

The digital advertising industry has reacted to that consumer attention with greater vigilance and a strengthening of anti-malware practices, and the number of companies holding the Certified Against Malware Seal grew by more than 44% in the past year alone, making it TAG's fastest growing certification program.

About TAG

TAG (the Trustworthy Accountability Group) is the leading global initiative fighting criminal activity and increasing trust in the digital advertising industry. TAG advances its mission of eliminating fraudulent traffic, facilitating the sharing of threat intelligence, promoting brand safety and enabling transparency by connecting industry leaders, analyzing threats, and sharing best practices worldwide. The global TAG community include the world's largest and most influential brands, agencies, publishers, and ad tech providers.

To learn more about TAG, please visit www.tagtoday.net.

¹ <https://www.ftc.gov/new-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0>



1. Executive Summary	4
2. Principles	6
4. Malvertising Taxonomy and Examples	8
3.1. Defining malvertising	9
3.2. Scope	9
3.3. Examples	9
5. Conclusion	14
6. Appendix A: Glossary of Digital Advertising Terms	16
7. Appendix B: Related Malicious Threats Outside the Advertising Supply	18



The page features decorative red geometric shapes in the corners. In the top-left corner, there are overlapping triangles in various shades of red. In the bottom-right corner, there are overlapping triangles and a large red arrow pointing towards the center. The text is centered in the white space between these shapes.

EXECUTIVE **SUMMARY**

While the concept of malvertising is relatively novel to businesses and consumers, criminal interest in using ads as a vector for malware attacks has grown steadily for more than a decade now. With malvertising now a problem at scale, the need for the digital advertising industry to collaborate and build momentum in the fight against malvertising, as demonstrated by initiatives such as TAG's Threat Exchange and Certified Against Malware program, has never been greater.

Part of that momentum fosters the increasing need to ensure discussions and information exchange about malvertising, especially across the Certified Against Malware program and TAG's Threat Exchange, are consistent and specific. With this in mind, *TAG's Malvertising Taxonomy* is created to address this growing need with a high-level, but actionable framework, not only across the digital advertising ecosystem but for the broader cybersecurity and law enforcement sectors as well. TAG's Malvertising Taxonomy is intended to complement and not replace existing industry documentation such as MITRE's ATT&CK Framework and Confiant's Malvertising Attack Matrix, among others. With this Taxonomy, TAG strives to improve identification, analysis and resolution of malvertising events and threat vectors and provide a consistent framework to structure further specific reporting and initiatives around combatting malvertising.



PRINCIPLES

The TAG Malvertising Taxonomy was created in support of the following principles:

- Build trust throughout the digital advertising ecosystem.
- Provide sufficient granularity in terminology to help partners in the digital advertising supply chain troubleshoot issues for the purposes of identifying and reducing malvertising.
- Improve the process of resolving malvertising reporting discrepancies between different parties in the digital advertising supply chain.
- Facilitate threat intelligence sharing within and between organizations combating malvertising.
- Act as a resource across the cybersecurity industry to provide common language around the definition of malvertising and examples of malvertising events

MALVERTISING TAXONOMY **AND EXAMPLES**



3.1. DEFINING MALVERTISING

Malvertising is the exploitation of digital advertising to enable bad actors to spread malware and circumvent systems in a way that harms end users, publishers, and platforms. These cyber-attack activities rely on digital ads that are designed to deploy payloads with explicitly malicious intent or enable systems to be compromised by bad actors.

There are many different forms of malvertising categorized by various actions triggered when the ad is served to a user. But the common element is the use of the ad creative (including pixels, code, intended landing pages, and/or other aspects of creative assets), or any other vulnerable points along the advertising supply and/or demand chain, to harm the end user.

Bad actors may also incorporate obfuscation or cloaking techniques to evade detection. Ultimately, malvertising entails identifying the traits/behaviors and segmenting around two significant components: what has been deployed (e.g. payload) and how they are being deployed (e.g. circumventions taken).

Malvertising can occur through (but is not limited to) the injection of unwanted or malicious code into ads. Malicious actors may pay digital advertising networks to display the infected ads on various websites, exposing every user visiting these sites to the potential risk of infection, while advertising networks and websites may remain unaware that they are serving such content.

3.2. SCOPE

The TAG Threat Exchange and Certified Against Malware programs consider all monetizable transactions, which includes impressions, clicks, conversions, etc. that a company handles as defined within the *Certified Against Malware Guidelines*, to be considered within scope for purposes of TAG's *Malvertising Taxonomy*.

Events considered in-scope as malvertising include, but are not limited to scam ads, auto-redirecting, deceptive or drive-by-downloads, etc. A more comprehensive list of in-scope event types is included in Section 3.3.

Events considered out of scope for this malvertising taxonomy include, but are not limited to:

- **Platform-specific Policy Violations** – examples include political, pharmaceutical, gambling, and dating services policies, as well as sale of illegal products or services. Note that these examples can still be in scope of this Taxonomy with regards to scams, but platform-specific policy violations under these categories are considered out-of-scope.
- **Content Analysis Outside Malvertising** (including language, location, demographic, and/or contextual categorizations). This category includes content taxonomies or floors (avoidance categories).
- **Ad Quality issues** – examples include 'unwanted' ads, not universally shared/banned across all platforms, broken creatives or landing page links.

In general, events considered out-of-scope should only include events determined not to demonstrate malicious intent, once a full investigation and analysis is completed.

3.3. EXAMPLES

Three different components are critical to better understand malvertising and ensure effective sharing of threat intelligence and communications:

1. Glossary of terms commonly used within digital advertising for reporting purposes, as referenced in Appendix A
2. Observable behaviors and/or artifacts. These would be equivalent to flags or indicators of compromise across cybersecurity sectors but are specifically tailored for digital advertising. Examples include:
 - a. Parked domains
 - b. Atomic indicators such as URLs, suspect domains, IP addresses
 - c. App identifiers (re: patterns of app spoofing, etc)
3. Types of malvertising events / activities

The chart below explains the different types of malvertising with corresponding examples. These examples are meant to be illustrative to help represent the differences between categories and represent only a subset of possible malicious behaviors & tactics. Note that an advertisement may be classified into one or more categories listed below; these categories are not exclusive of each other.

MALVERTISING EVENTS		
TECHNIQUE/ TACTIC	DEFINITION	SUB-CATEGORY (EXAMPLES) (at least one)
Scam Ads	Sophisticated schemes in which a threat actor uses social engineering or other forms of deception to gain access to sensitive user information, misrepresenting the product, business or service, phishing or financial harm to the user.	Scam ads fall across a number of sub-categories, including the following: <ul style="list-style-type: none"> ● <u>Retail</u> - Scamming users by concealing or misstating information about the advertiser's business, product, or service, and/or impersonating brands or businesses by referencing or modifying the brand content in the ads, URL, destinations or misrepresenting yourself as the brand or business in user interactions ● <u>Services</u> - False advertising of services that could endanger a user's health, life, or safety. Pretending to provide critical services that result in a delay to the user receiving treatment or medical help ● <u>Financial</u> - Enticing users to part with money or information through a fraudulent organization that lacks the accredited qualifications or verifiable capacity to provide the advertised products or services. ● <u>Phishing / Credential or PII 'theft'</u> - Ad destinations that use "phishing" techniques to gather user information. This includes sites that trick users into revealing their personal information by mimicking a trusted entity such as a browser or bank. This includes, but is not exclusive to, fake anti-virus/software and/or VPN activity



		<ul style="list-style-type: none"> • <u>Gift card / giveaway scams</u>– can fall under multiple categories such as Retail, Service, Financial and/or Phishing. When a user goes to a landing page that tells them that they received a gift card or won a giveaway and to receive it, they must fill out their personal information. The personal information given is used for malicious intent
Auto-Redirecting	Without intentional interaction, an advertisement or script automatically redirects users to a website, app or app store.	<ul style="list-style-type: none"> • Without the user interacting with an ad, it automatically clicks and the user is taken to another website or app store (e.g. click-jacking) • Forced Redirects: When a bad actor redirects victims without any user action to a malicious landing page through alteration of the user's systems or code
Compromised Landing Site/Pages	Upon ad click, user is taken to a landing page that has been unknowingly compromised for malicious intent by threat actors outside of the advertising supply chain. Absent this compromise, the site would be benign and acceptable. Website operator is not complicit, and an unknowing victim.	<ul style="list-style-type: none"> • Landing page of ad loads adversely modified Javascript libraries (e.g. jQuery) or hacked resources (e.g. Wordpress plugins) leading to additional redirecting of user, injected authorized ads, or stealing of personal information. • Injected ads not authorized by the site owner, commonly including pop-unders • Credit card skimming / credential theft • A user views a creative hosted on a publisher's ad server that has been compromised.
Compromised Ads (Assets)	Ad is unknowingly compromised for malicious intent by threat actors outside of the advertising supply chain, resulting in unexpected and negative changes in creative upon delivery. Advertiser and partners are not complicit, and an unknowing victim.	<ul style="list-style-type: none"> • A user views a creative hosted on a publisher's ad server that has been compromised. • A publisher's ad server has been compromised to inject cryptocurrency mining code into the ad slot. • System (e.g. ad server) compromise or hack that demonstrates malicious intent and/or causes harm. • Creatives that unintentionally manipulate behavior such as incorporating/removing back button, or otherwise messing up user interactions.
Cloaking (Ads)	Attempts to mask or misrepresent the ad creative to evade detection.	<ul style="list-style-type: none"> • An ad network auditor views a creative and it appears to be for furniture. When viewed by targeted users, it instead has material promoting an investment scheme which violates the "Scam Ads" section at top. • <u>Steganography</u>: Hiding secret information inside of a non-secret message. This is

		usually performed in malvertising through payload smuggling
Cloaking (Landing Pages)	Attempts to mask or misrepresent the landing page so as to evade detection.	<ul style="list-style-type: none"> An ad network auditor views a landing page and it appears to be for furniture. When viewed by targeted users, the page instead has material promoting an investment scheme which violates the "Scam Ads" section at top. Landing pages that are benign when non targeted users visit; but under proper conditions, targeted users are redirected to malicious destinations <u>Steganography</u>: Hiding secret information inside of a non-secret message. This is usually performed in malvertising through payload smuggling
Drive-by-Download (Software)	A drive-by download attack utilizing software refers to the unintentional download of malicious or non-malicious code without user consent and usually without user-initiated ad interaction, such as ad expansion or clicks. Malvertisers creates a vector for malware delivery via ads or legitimate program downloads that in turns download malware without the user's consent.	<p>A user visits a publisher page and without the user interacting with the ad slot, an executable file (e.g. .exe, .apk, .dmg) is downloaded to their device.</p> <ul style="list-style-type: none"> <u>Browser extension/hijacker</u>: Software add-ons that can contain malware to infect a user by stealing personal information or redirecting a user to malicious ads. A browser hijacker is malware that can modify or change a browser's settings without the user's knowledge <u>Click-jacking</u>: When a bad actor disguises an element to trick a user into clicking it. This will hijack their click and unknowingly download malware, visit malicious web pages, or steal personal information
Drive-by-Download (Files)	A drive-by download attack using files refers to the unintentional download of files and/or disclosures. Please note that certain companies may be legally required to have users download disclosures (e.g. pharma) and do not demonstrate malicious intent – these should not be characterized in-scope.	<p>Malicious vs non-malicious downloads – particularly from within ad slots, are considered abusive, regardless of whether the binary file (e.g. font file such as OTF, TTF) itself is bad</p> <ul style="list-style-type: none"> <u>Cookie Stuffing</u>: When a bad actor drops affiliate cookies on a user's browser so that they can claim commission on the sales made from that browser
Fake Landing Site/Pages	Upon ad click, user is taken to a fake landing page, that was created to make a decoy ad seem convincing even though it might be malicious. Absent this compromise, the site	<ul style="list-style-type: none"> Typosquatting Fake updates

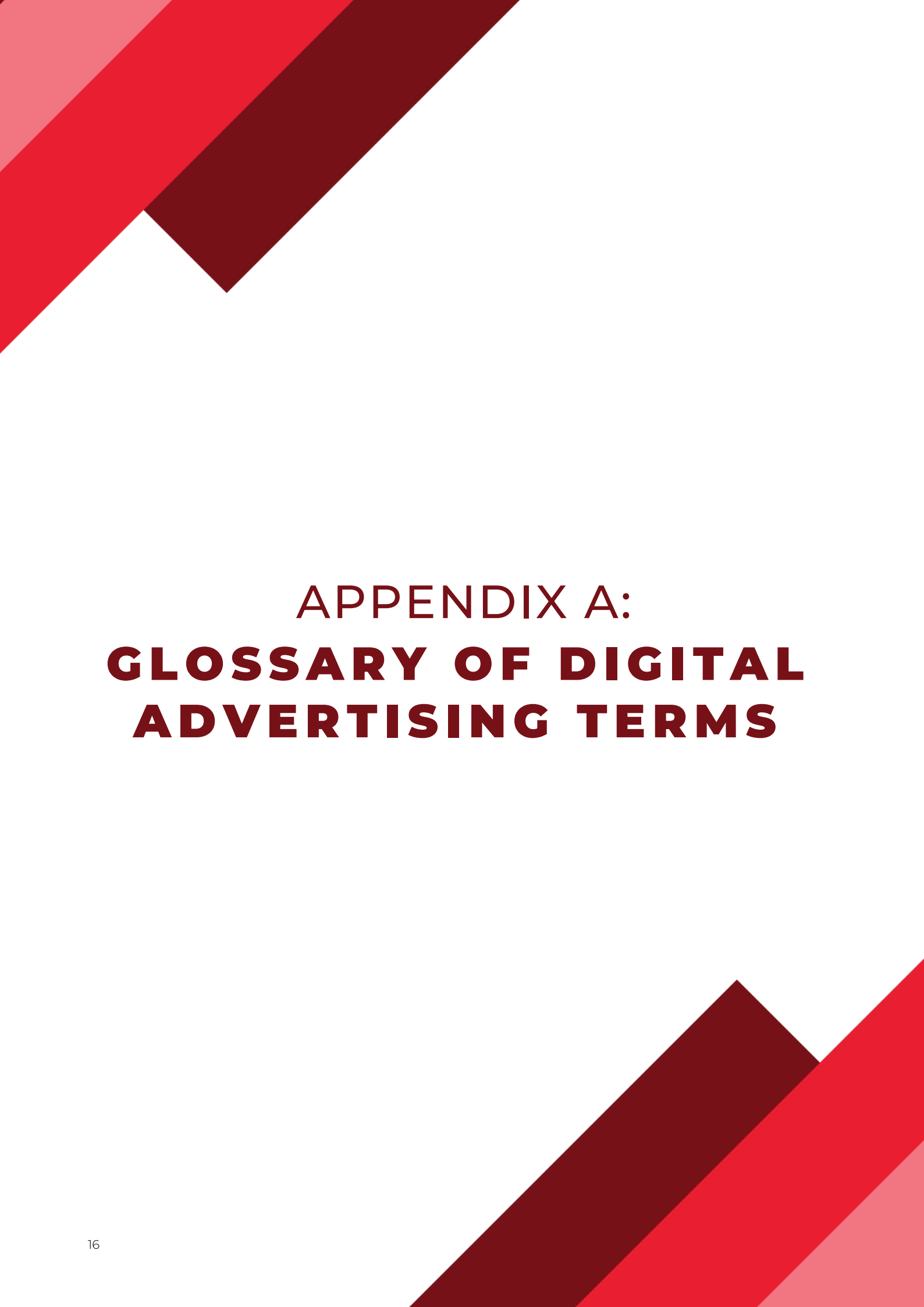
	would be benign and acceptable.	
Other Malicious & Malware Activity	User's devices may be vulnerable to malicious activity outside above defined categories which imply malicious intent.	<ul style="list-style-type: none"> • Injection of in-creative crypto currency mining • Advertisements pointing to binary malware downloads which delivers a payload like ransomware, cookie theft for account hijacking • Includes demonstration of deceptive/malicious behavior, including "gross" policy violations and/or platform-specific rules • <u>Exploit Kit</u>: Type of malicious toolkit that bad actors use to attack vulnerabilities in code or systems • <u>Ransomware</u>: A type of malicious software that will add or adversely affect systems until a requested amount of money is paid to the bad actor • <u>Trojan Malware</u>: Disguises itself as legitimate code or software and once it is inside of the network and on an individual's computer, it can take control of a user's computer • Homoglyphs • <u>SEO Poisoning</u>: When bad actors create malicious advertisement links and use search engine optimization tactics to make the malicious links show up at the top of search results





CONCLUSION

While industry efforts, including widespread adoption of the TAG Certified Against Malware Program and participation in the TAG Malvertising Threat Exchange, have brought awareness of malvertising to the forefront of digital advertising, varying definitions and misrepresentation of malvertising-related terminology continues to result in miscommunication between partners sharing the same goal of fighting malvertising. In releasing an updated and better tailored TAG Malvertising Taxonomy, TAG strives to improve analysis and resolution of malvertising reporting discrepancies and provide a consistent framework to structure specific reporting and initiatives around combatting malvertising and improving threat intelligence sharing overall.



APPENDIX A:
**GLOSSARY OF DIGITAL
ADVERTISING TERMS**

Advertiser Domain - The URL of the brand represented in the creative. (please be mindful if there is a potential domain redirect). The advertiser domain, or adomain, is passed through bid responses.

Associated Domains – Typically lower-level domains separate but associated with top level domains.

Buyer (Seat) ID – The Buyer ID is associated directly to the entity, most likely an agency, that represents advertisers buying ad inventory. This is also sometimes called “Seat ID” and one or more Seat IDs may be associated to a single Buyer. Seat is the generally used term for any “account” on a DSP.

Buyer (Seat) Name – The Buyer or Seat name is the name of the entity with an account on a DSP that aligns with a specific Buyer ID.

Creative ID / crid – An ID (identification) number assigned to the creative typically by a DSP or SSP that can be used as a unique identifier during a malvertising incident. While a DSP or SSP may use an internal-only version of the creative ID, it is preferable to use an external version, as returned in the bid response, for the purpose of sharing.

Creative Image – Data file of an image for the creative, usually shared in a malvertising incident in the form of a screenshot or web scrape.

Bidder (DSP) Name – The name of the legal entity that pays for inventory bought on behalf of Buyer ID. In most cases, a Bidder ID should represent only a single legal entity, but an entity may also be a managed service desk or similar operation servicing a variety of buyers. Any individual Bidder ID that aggregates demand from multiple legal entities should consider itself a DSP and be identified as well.

Image URL – URL called to retrieve the image attached to the creative.

Malicious Landing Page Domain – Domain where the malware was found/active. The landing page is typically a standalone web page that potential customers can “land” on when they click through from an email, ad, or other digital location. A landing page aims to capture information from contacts in exchange for something of value. They serve a specific purpose in a specific moment of an advertising campaign to a target audience.

Malicious URL – A URL which contains code which performs a Malvertising Event, as defined in Section 3.3. This includes code to collect signals for cloaking purposes, even if the cloaking occurs in a subsequent event. The domain may or may not be controlled by the party causing the Malvertising Event, e.g. the URL may point to JavaScript hosted on a major cloud platform’s object storage product.

Threat Actor - Commonly referenced in cybersecurity, a threat actor is anyone, or any entity, who is either a key driver of, or participates in, a malicious action, such as malvertising, that can target an entity or user group’s IT security, platform, ecosystem or end users.



APPENDIX B:
**RELATED MALICIOUS
THREATS OUTSIDE THE
ADVERTISING SUPPLY**

Malicious Browser Extension - User has been compromised by something they previously downloaded and installed browser extension. User is unaware the malicious actions such as a redirect, are caused by the extension, not by malvertising.



tag

tagtoday.net