Technical Best Practices Against Malware

Best practices for combatting malware in the digital advertising supply chain

DRAFT

Version 2.1
Release July 2019

About the TAG Certified Against Malware Program

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.

In order to guide companies in fighting malware using the digital advertising supply chain as an attack vector effectively, the TAG Anti-Malware Working Group developed and maintains the *Certified Against Malware Guidelines*, as well as a suite of anti-malware tools to aid in compliance with those guidelines.

Companies that are shown to abide by the *Certified Against Malware Guidelines* can achieve the Certified Against Malware Seal and use the seal to publicly communicate their commitment to combatting malware using the digital advertising supply chain as an attack vector.

DRAFT

About the Trustworthy Accountability Group

The Trustworthy Accountability Group (TAG) is the leading global certification program fighting criminal activity and increasing trust in the digital advertising industry. Created by the industry's top trade organizations, TAG's mission is to:

- Eliminate fraudulent traffic,
- Combat malware,
- Prevent Internet piracy, and
- Promote greater transparency in digital advertising.

TAG advances those initiatives by bringing companies across the digital advertising supply chain together to set the highest standards.

TAG is the first and only registered Information Sharing and Analysis Organization (ISAO) for the digital advertising industry.

To learn more about the Trustworthy Accountability Group, please visit www.tagtoday.net.

Table of Contents

DRAFT

1. Executive Summary

Malware delivered through the advertising ecosystem degrades overall trust in the system by generating a poor consumer experience. Additionally, malware infected machines attack the advertising ecosystem to generate money for fraudsters. Because each participant in the ecosystem has limited visibility into their subset of the problem, preventing the delivery of malware overall is challenging, resulting in continued attacks on consumers through various uncoordinated parts of the system.

TAG's *Technical Best Practices Against Malware* offers best practices for documenting scanning responsibilities with partners in the digital ad transaction, receiving ad tags and ad creative, scanning this content for malware, and handling and resolving malware events upon occurrence of malware threats in digital advertising.

The document is intended to aid companies in complying with the requirements outlined in the *Certified Against Malware Guidelines*, and provides additional best practices to facilitate prevention, mitigation and remediation of malware events using the digital advertising supply chain as an attack vector.

TAG encourages companies to consider and implement these best practices in order to further strengthen industry efforts in combatting malware effectively.

DRAFT

2. Best Practices for Documenting Scanning Responsibilities

A company's ability to scan varies depending on whether an entity has access to some or all of the advertising campaign assets. Participants in the supply chain pass along and modify ad tags while not necessarily handling ad creatives. As such, different scanning responsibilities are recommended.

- For all entities with access to the creative or tags, all intermediate calls should be screened for malware – including bid requests and bid responses, along with landing pages – as specified in Section 3.
- To ensure that all revenue generating assets are scanned up and down the ecosystem, each participant in the ecosystem should know their partners' scanning responsibilities.
- If malware is detected in a particular creative, it should be categorizes as having a higher risk profile. That creative and landing page should also be scanned AND rescanned at a higher frequency. Evidence should be provided to address that particular threat.
- Buy-side Intermediaries bear great responsibility in scanning for malware, as they are often responsible for the injection of ads into a direct or programmatic transaction. Thus, special attention should be paid to their specific scanning and rescanning responsibilities.
- Buy-side Intermediaries (DSPs) should enforce their scanning rules on their Direct Buyers and require disclosures of scanning practices as part of their legal agreements with partners.
- Upon a Direct Seller's request, Scanning Companies should confirm that a Direct Buyer or Intermediary with whom it is working is using a scanning company's services. Scanning Companies may opt to reject clients that don't send 100% of their inventory for scanning.
- Scanning Companies should provide the following information to its clients upon request:
    - Does a particular entity use your scanning service?
    - Specifically, what is that entity scanning for?
    - What percentage of inventory is your company scanning?
    - Is your company rescanning actively serving creatives daily?
    - A complete list of products/service offerings, along with a level of scanning service for each offering.

- To maximize quality and accuracy of scans of all ad tags and creatives, all parties should provide the following information to scanning companies or have this information available for in-house scanning:

    - Specific geo-targeting parameters
    - Specific channel targeting parameters (e.g. video/mobile)
    - Targeted operating system (OS) markups (refreshed regularly)
    - Bid request information, including all data within the bid, such as domain passed through bid response, buyer ID, buyer name, creative ID (ecrid), etc.
    - Referring domain(s)
    - Landing page(s)
    - Expected formats for scanning

DRAFT

- Creative URL for third parties
- Ad markup for delivery

DRAFT

3. Best Practices for Scanning and Rescanning

Beyond scanning requirements called out in the *Certified Against Malware Guidelines*, the following best practices should be adhered to when scanning advertising campaign assets and/or corresponding landing page URLs:

- Any company hosting and/or creating advertising campaign assets, which include physical files such as images and scripts associated with a campaign, should scan 100% of all advertising campaign assets with the exception of first-party generated, controlled and hosted assets, preceding initial delivery.
- Any company hosting and/or creating advertising campaign assets should also scan 100% of landing page click-through URLs, preceding initial delivery.
- Direct Buyers and buy-side Intermediaries who host and/or create advertising campaign assets should ideally scan and rescan all non-first party created, generated and hosted assets at least twice daily using multiple scanning types.
- Scanning should incorporate updated safe browsing blacklists that account for new threats.
- Scanning should strive to detect and recognize threats that are at times hidden but still exposes users to malware (i.e. cloaking).
- Scanning of advertising campaign assets and landing page click-through URLs may be performed asynchronously, but it is recommended to precede a landing page scan with an appropriate ad request.
- Scanning should strive to detect and recognize threats embedded within deep link notations, or use of hyperlinks that links to a specific, generally searchable or indexed, piece of web content on a website (e.g., "http://example.com/path/page"), rather than the website's home page (e.g., "http://example.com/")

DRAFT

Ads, as well as landing pages click-through URLs, should be re-scanned with appropriate resources in proportion to the user exposure, technologies, and partner confidence.

- All active advertising campaigns should have assets rescanned at least once every 24 hours or less, depending on a company's rescanning methodolog(ies) used. Varying frequency or randomizer cadences using deduping and/or relevancy logic for rescanning can be used to optimize resourcing, based on the factors called out in Section 3.1.
- All active advertising campaigns with one or more known asset change(s) should be rescanned before commencing delivery.
- No active advertising campaign should be run for more than seven (7) days without being rescanned.
- Intermediaries using an RTB platform should scan prior to initial delivery and rescan landing page click-through URLs at least twice daily.
- Depending on the type of assets entailed in specific advertising campaigns (e.g. rotating tags, header bidding, content/widget ads, etc.), sell-side Intermediaries and Direct Sellers should consider increasing and randomizing their rescan frequencies to account for multiple asset formats and threat scenarios.
- All active advertising campaigns' click-through landing page URLs should be rescanned at least once every 24 hours or less, depending on a company's rescanning methodolog(ies) used.

- Publishers should consider supplementing their rescanning methodologies with website and app scans to boost their ability to detect threats and ensure scanning is occurring across multiple “hops” within the digital advertising supply chain.
- Reach a high confidence that malware is not present by scanning a mathematically appropriate amount, adjusted based on factors outlined in this document. For example, ads with millions of impressions per day may need hourly scanning, while ads with a hundred impressions per day may need daily scanning.
- All participants should use commercially reasonable and best efforts to provide acceptable coverage.

3.1. Scanning and Rescanning Factors

A variety of factors influence the best cadence of scanning and rescanning to achieve effective malware detection. It is recommended that a risk-based approach be utilized to determine the best cadence for scanning and rescanning. The following factors should inform the development of specific scanning practices by an individual company.

The most Direct Buyer is an advertiser – a brand company represented in the advertisements that it wants to place in the publisher’s inventory.

However, many brands hire an advertising agency to manage their advertising campaigns. A brand-appointed agency is also a Direct Buyer, except in cases it operates as an Intermediary. To qualify as a direct buyer, the agency must directly represent the advertiser.

DRAFT

3.1.a. Partner Confidence

The current length of partnerships with Direct Buyers should be considered in rescanning cadence, as well as the assertions made by and track record of the Direct Buyer with regards to scanning and detecting malware themselves. Factors to consider include:

- Companies should scan 100% of assets coming from new Direct Buyer partners while periodically scanning assets from trustworthy advertisers (i.e., Direct Buyers that have proven over time that they are good actors)
- A thorough risk assessment of a partner’s scanning practices should be performed as part of the onboarding of new Direct Buyer partnerships (less than 90 days).

For new Direct Buyer partnerships or partnerships with Direct Buyers who are undergoing management or other significant changes, more frequent rescanning or signal sharing protocols should take place to mitigate higher risk of malware delivery.

3.1.b. Demand Type

The breadth of clients to which an ad may be delivered to will affect scan frequency. When ads may be delivered across multiple types of connections to a variety of devices, scans should be increased to reflect this diversity. Factors to consider include:

- Whether malware may deliver to specific ranges of IPs that represent public Wi-Fi or cellular connections.
- Whether malware may deliver to specific cookie data.
- Whether malware may deliver only over HTTPS or non-HTTPS connections.

- Whether malware may deliver only to certain geo-locations.
- Whether malware may deliver only to a subset of User Agents: Browser/OS and App/Mobile Web (mobile/tablet, iOS/Android) combinations.

3.1.c. Frequency

The number of ad impressions and ad click data should affect scan frequency. Multiple scans should be performed when an ad is being delivered more often. Other factors to consider include:

- **Absolute number of impressions or other common KPIs.** This describes a general exposure risk.
- **Acceleration of impressions or spend.** While mid-campaign changes are often innocuous, they may reflect a malware activation.
- **Changes in impression targeting.** Fine tuning a campaign's targeting can be a normal part of the effort, but also might represent the activation of malware delivery.
- **Changes in Technology.** A shift from static creative to dynamic creative with external resources, introduction of a redirect or number of redirects in a chain may all indicate an increased need of scanning.

3.1.d. Rescan Factors

Scanning ad creative and ad tags directly is an ongoing cost. In order to achieve an effective and commercially reasonable scanning cadence, additional data points can be used to inform the rescanning interval:

DRAFT

- **Initial scan results.** The complexity of the ad encountered during the initial scan, as evaluated by the number of URLs, number and size of reference JavaScript files, can influence the frequency of follow-up scans.
- **Sub-element errors.** If there are technical issues in making requests during a scan, (like 404 errors, DNS errors, server timeouts, and so on), the rescanning cadence should be increased.
- **Domain location.** The physical location of the domains referenced in the ad tag should be considered. Hosting at a well-known co-location facility presents a different risk profile than resources hosted by fast fluxing DNS on residential or proxy IPs.
- **Domain and IP ownership information.** The ownership information about domains and their associated IPs referenced in the ad tag should be considered. Domain WHOIS data from ICANN accredited registrars, and IP WHOIS data from ARIN, RIPE, APNIC, and so on should be considered here.
- **Technology.** Some technologies are intrinsically higher risk since they contain an increased potential for delivering malware (like SWF files), or because they are different for each delivery (like rotating tags).
- **Campaign targeting.** Depending on the targeting criteria of the campaign, such as highly selective target segments or multiple permutations of targeting criteria, more frequent rescanning is warranted to mitigate risk of malware being injected into those ads.
- **Dynamic, rotating and/or changed creatives.** Since any of these types of creative may not have been initially scanned upon injection into the supply chain and/or may have been changed after initial execution, changes in creatives increase the risk of malicious payload being delivered through the creative and/or ad tag.
- **Impression / delivery acceleration.** For campaigns that need to accelerate impression delivery due to deadlines and/or other changes in campaign parameters, rescanning

cadence should be increased in these cases.

3.1.e. Cost / Value

Not all scans are equal cost. Frequency of higher cost scans can be reserved for the coverage commensurate with the value gained (and insuring that other serving metrics are not impacted).

The order of costs should be considered as follows:

- **Simple Rescoring.** Analysis of previously collected scan information against updated database of threats.
- **Static Analysis of Creative.** Analysis of previously collected creative against updated database of threats.
- **Low- to Full-feature scans**. Actual scanning, from simple requests for the ad tags to scans made from emulated browsers that interact with ads and request landing pages.
- **Scans from consumer IP spaces**. Actual scanning, but instead of from a datacenter, the scans originate from known consumer IP addresses.
- **Scans from various mobile networks**. Actual scanning, but instead of from a datacenter, the scans originate from known mobile network IP addresses.

DRAFT

3.2. Best Practices for Scanning based on Risk Tolerance and Creative Hosting Type

Best practices for scanning and rescanning are linked to the level of risk associated with a particular creative hosting type. These recommended best practices should be considered minimally acceptable standards for injection into the digital advertising supply chain and are prioritized by risk. Buy-side Intermediaries (e.g. DSPs) should structure their buys such that the majority of their inventory fits into the lowest risk categories, when possible.

3.2.a. Creative Risk Levels

The creative types listed below are shown in accordance with level of risk in introducing malware into the digital advertising supply chain, sorted from high to low risk. As third-party hosting enables the opportunity for potential attackers, such as malicious Direct Buyers, to inject malicious content into the digital advertising supply chain, it is recommended to treat any third-party resource as a potential threat.

Active creative hosted remotely

- A Direct Buyer could subvert the supply chain at multiple levels and is difficult to detect or interdict.

Static creative hosted remotely

- A Direct Buyer could subvert the supply chain at multiple levels and is easier to detect than active content (type/MIME mismatch), but still difficult to interdict.

Active creative hosted locally

- A Direct Buyer could still potentially make remote calls out to other remote resources, if buyer's own processes are insufficient.
- Improper scrubbing on the part of the Direct Buyer could easily put this in the same risk category as active content hosted remotely.

Static creative hosted locally

- A Direct Buyer likely has only one chance to get its payload into the system.
- Scanning static creatives for "bad things" is easier than scanning active creatives.

3.2.b. Best Practices for Scanning Active Content Hosted Remotely

Active content hosted remotely carries the highest risk for introducing potential malware into the digital advertising supply chain, given the fact that active content can deliver JavaScript to ad code or creative assets from systems for which a company has no ability to control. The following scanning practices listed below are recommended:

DRAFT

- Scan ad tags with robust malware scanning.
    - A well-supported scanning system with a reputation for success is recommended.
    - Reputation will impact the long-term viability of any homegrown scanning technology.
    - Rescan more frequently since this is active content.
- On initial creative ingest, fetch all remote resources, and do the following:
    - Block creative that involves eval().
    - Block creative that has remote resources within remote resources.
    - Block creative that appears to have excessive base-encoded data and also contains a call to a decoder function.
    - Determine if a checksum or other digital signature can help speed subsequent rescans, since these will be frequent.
- Ingest verifiable proof of scanning by the hosting party.
    - If the hosting party is able to provide verifiable and trusted proof of their own malware scanning, you may be able to reduce your scanning interval.

3.2.c. Best Practices for Scanning Static Content Hosted Remotely

While less risky than active content hosted remotely, static content hosted remotely still carries high risk for introducing potential malware into the digital advertising supply chain from systems

that a company has no ability to control. The following scanning practices listed below are recommended:

- Scan creative with robust malware scanning.
    - Homegrown or third-party malware scanning tools are acceptable.
    - Reputation will impact the long-term viability of any homegrown scanning technology.
    - Rescan at a reasonable interval since the static content can be changed (i.e. HTTP 302, etc.).
        - Deep scan on creative change. Use checksum or full bit comparison.
- Ingest verifiable proof of scanning by the hosting party.
    - If the hosting party is able to provide verifiable and trusted proof of their own malware scanning, you may be able to reduce your scanning interval.
- On initial creative ingest, attempt to check the following:
    - Minimum and maximum file size.
    - Ability to correctly resize the image without throwing an exception.

DRAFT

3.2.d. Best Practices for Scanning Active Content Hosted Locally

Active content hosted locally carries moderate risk for injecting malware into the digital advertising supply chain through active content inserting JavaScript within the ad code or creative asset. However, this is less likely as this content is coming from systems that a company can control. The following scanning practices listed below are recommended:

- On initial creative ingest:
    - Ensure creative is well formed. How this is performed technically will depend on the format of the creative:
        - Flash presents a small technical hurdle.
        - Java applets should be immediately suspect, given their high power over the local system, and relative rarity of their appearance.
        - Block calls to eval()
        - Potentially block any heavily encoded payloads, especially double and triple encoded.
    - Determine if there are any remote systems called inside this creative
        - If there are, assess reputation of those endpoints.
- Subject creative to long-term remote scanning (connecting as a client would), whether by a 3rd party or by a homegrown solution.

- Consider creating verifiable proof of scanning.
    - As the hosting party, provide verifiable and trusted proof of your own malware scanning, to reduce the scanning interval or partners from which you are buying.

3.2.e. Best Practices for Scanning Static Content Hosted Locally

Static content hosted locally carries the lowest risk for injecting malware into the digital advertising supply chain. Also known as “directly hosted static content”, this refers to creative delivered through systems that a company can control. The following scanning practices listed below are recommended:

- On initial creative ingest, check the following:
    - Ensure creative is well formed. How this is performed technically is dependent on the format of the creative.
- Monitor the local file for changes on a routine basis, and re-scan when changes occur, such as
    - New content uploads that occur while a campaign is running
    - Potentially compromised system changing the creative outside the application.

DRAFT

3.3. Best Practices for Scanning for Auto-Redirects

There has been an increasing number of malware threats where malicious code on ad creative executes auto-redirects on users’ machines. Scanning companies are preparing to combat ever-evolving malware tactics from bad actors. Recommendations for specific variables to scan for suspected auto-redirects include the following:

- The mWeb variable should be targeted as part of the scanning and testing to combat auto-redirects. This can also be a source for potential obfuscations as well.
- Companies should also scan and test to identify potential drive-by-downloads.
- Scanning for auto-redirects should occur for mobile and desktop platforms.

4. Best Practices for Generating Campaign Assets

As ad code and tags have been known to inject malware into the digital advertising supply chain, Creative Agencies responsible for creative development/generation should also be responsible for scanning creatives for malware before delivering ads to Direct Buyers and/or Intermediaries.

The following recommendations should be implemented by Creative Agencies and their partners to prevent injection of malware into the digital advertising supply chain:

- In-depth vetting of ad code, along with scanning of creatives and landing pages, should be executed prior to delivery to their clients.
- Encoding of the creative asset should be limited to reduce the potential of malware injection, though there may be a limited number of scenarios where encoding is required.
- Any calls or assets delivered via the ad tag should be viewable and compliant in all environments (including https) and should be verified by creative agencies as well.
- In-depth scanning is recommended when JavaScript insertion occurs within the ad code or creative asset. Clean ad delivery is essential to mitigate risk of malware in the digital advertising supply chain.
- Rich media assets should also be scanned in-depth and rescanned more frequently due to its susceptibility to malicious code insertion.

DRAFT

5. Best Practices for Malware Event Handling and Resolution

5.1. Information Sharing for Direct Sellers

Data sharing may be restricted, depending on legal agreements with partner companies, whether this pertains to business-to-business contract language, Terms of Service, Site-Level Agreements, public policies or other places that a business expectation is set with a partner. However, best attempts should be made to ensure transparency and facilitate resolution of malware events as expediently as possible.

For an identified malicious auto-redirect, Direct Sellers should collect the following info before reaching out to their partners:

- Direct Sellers should identify the scope of any malware event, including threshold criteria revenue/user experience/sophistication.
- End point: Direct Sellers should detect the end point in order to block the malicious domain. That said, Direct Sellers may not necessarily be able to track chain of redirects resulting from the malware incident

Direct Sellers should share as much data regarding the event as possible, including:

- Screenshots, redirected domains, HAR, HTTP watch log, Charles logs.
- If unable to capture the ad call, provide specifics of the redirect incident needed for replication efforts (desktop/mobile web/ mobile app redirects, network provider (AT&T, Verizon, etc.), browser, IP, frequency of redirects etc.

DRAFT

Expectations related to resolution timing, severity of the event reported, and requests for increased scanning (possibly cloaked) should be communicated with buy-side partners. It is understood that additional investigations may also be warranted, depending on the severity of the event reported and availability of information upon initial reporting.

5.2. Malware Event Resolution for Direct Sellers and Intermediaries

The following requirements, as called out in Section 4.11 of the *Certified Against Malware Guidelines*, must be implemented by Direct Sellers and Intermediaries to facilitate malware event resolution for all parties in the digital advertising supply chain.

To achieve the Certified Against Malware Seal, any participating company acting as a Direct Buyer, Direct Seller or Intermediary must employ Seat ID object attributes to troubleshoot and handle Red Flag events, as defined in Section 4.10. Additionally, any participating company acting as a Direct Seller or Intermediary must build or set up the capability to turn off Seat IDs or a

company's direct partner to whom the Seat ID belongs, should a Red Flag event occur.

As stated within IAB Tech Lab's OpenRTB API specifications, a seat is defined as "an advertising entity (e.g., advertiser, agency) that wishes to obtain impressions and uses bidders to act on their behalf; a customer of a bidder and usually the owner of the advertising budget."[1] Seat ID attributes are defined for the bid response model as follows:

Object: SeatBid
A bid response can contain multiple SeatBid objects, each on behalf of a different bidder seat and each containing one or more individual bids.

Attribute	Type	Description
Seat	String	ID of the buyer seat (e.g., advertiser, agency) on whose behalf this bid is made.

A participating company's path to complying with this requirement will vary, depending on the covered party categories (see Section 3.0) into which it falls and its role in the digital advertising supply chain. As a minimum, companies must ensure that all programmatic buying disclosures fully comply with OpenRTB specifications v.2.2 or higher[2] and include the SeatBid object and Seat (ID) attribute information when making and honoring bid responses.

The following recommended best practices should be implemented by Direct Sellers and Intermediaries to facilitate malware event resolution for all parties in the digital advertising supply chain:

- Direct Sellers should require that their demand-side Intermediary partners scan and shut off malicious demand sources. Direct Sellers should consider requesting and accepting ads based on whitelists of acceptable demand sources based on anti-malware ad quality.

- Direct Sellers should validate that partners are scanning by asking the partner which vendor they use. Alternatively, Direct Sellers should confirm with TAG whether their partners are currently holding TAG's Certified Against Malware Seal.

- Prior to turning off Seat IDs, Direct Sellers and Intermediaries should employ policies and processes to provide advance notice to all points of contact for the affected partner(s), as outlined in Section 4.6 of the *Certified Against Malware Guidelines,* when such actions negatively and significantly impact the financial performance of partners on their platform. The entity should ensure that any feedback and remediation policies and procedures be communicated to partners prior to executing this capability.

- To enable transparency in resolving malware events, Intermediaries should disclose URLs along with creatives to share advertiser details with their partners. Intermediaries should also share Seat ID mappings to help inform sell-side partners working towards resolution of malware events.

[1] https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API-Specification-Version-2-5-FINAL.pdf

[2] http://www.iab.com/guidelines/real-time-bidding-rtb-project/

DRAFT

- The following fields should also be shared by sell-side Intermediaries to facilitate malware event resolution:
    - Domains passed through bid responses
    - Buyerid
    - Direct Buyer name
    - Creativeid (ecrid)

- For an identified malicious auto-redirect, Direct Sellers should collect the following info before reaching out to their partners:
    - Direct Sellers should identify the scope of any malware event, including threshold criteria revenue/user experience/sophistication.
    - End point: Direct Sellers should detect the end point in order to block the malicious domain. That said, Direct Sellers may not necessarily be able to track chain of redirects resulting from the malware incident

- Direct Sellers should share as much data regarding the event as possible, including:
    - Screenshots, redirected domains, HAR, HTTP watch log, Charles logs.
    - If unable to capture the ad call, provide specifics of the redirect incident needed for replication efforts (desktop/mobile web/ mobile app redirects, network provider (AT&T, Verizon, etc.), browser, IP, frequency of redirects etc.

DRAFT

5.3. Malware Event Resolution for Direct Buyers

The following requirements, as called out in Section 4.11 of the *Certified Against Malware Guidelines*, must be implemented by Direct Buyers to facilitate malware event resolution for all parties in the digital advertising supply chain:

To achieve the Certified Against Malware Seal, any participating company acting as a Direct Buyer, Direct Seller or Intermediary must employ Seat ID object attributes to troubleshoot and handle Red Flag events, as defined in Section 4.10 of the *Certified Against Malware Guidelines.*

As stated within IAB Tech Lab's OpenRTB API specifications, a seat is defined as "an advertising entity (e.g. advertiser, agency) that wishes to obtain impressions and uses bidders to act on their behalf; a customer of a bidder and usually the owner of the advertising budget."[3] Seat ID attributes are defined for the bid response model as follows:

Object: SeatBid
A bid response can contain multiple SeatBid objects, each on behalf of a different bidder seat and each containing one or more individual bids.

Attribute	Type	Description
Seat	String	ID of the buyer seat (e.g. advertiser, agency) on whose behalf this bid is made.

[3] https://www.iab.com/wp-content/uploads/2016/03/OpenRTB-API-Specification-Version-2-5-FINAL.pdf

A participating company's path to complying with this requirement will vary, depending on the covered party categories (see Section 3.0) into which it falls and its role in the digital advertising supply chain. As a minimum, companies must ensure that all programmatic buying disclosures fully comply with OpenRTB specifications v.2.2 or higher[4] and include the SeatBid object and Seat (ID) attribute information when making and honoring bid responses.

The following recommended best practices should be implemented by Direct Buyers to facilitate malware event resolution for all parties in the digital advertising supply chain:

- A Direct Buyer should share Seat ID mapping to their direct partners where they buy inventory or run ads. Seat ID mapping should be transparent to its partners to help facilitate malware event resolution and handling. Additionally, any changes to seat ID mapping should be provided to partners in a timely fashion prior to executing transactions with updated Seat IDs. Seat ID mappings should include the following:
    - Advertiser legal entity name
    - Advertiser's business domains (if available)
    - Account identifier (if applicable)
    - Advertiser address
    - Billing information
    - Advertiser identifier (TAG recommends the use of TAG-ID, if the advertiser has one. Ad-IDs, DigiTrust IDs, Dun and Bradstreet business identifiers or other standardized IDs may be used in lieu of TAG-IDs)

- Transparency should be provided through ad serving paths. Obfuscated ad serving limits potential malware analysis and event resolution.

DRAFT

[4] http://www.iab.com/guidelines/real-time-bidding-rtb-project/

6. Glossary

Ad - The superset of both creatives and tags. Different participants in the supply chain may have access to only creatives or only tags, so this is shorthand for both.

Creative - The actual payload that, when delivered to a web browser or other client, displays a message to the consumer.

Landing Page - After the consumer interacts (i.e. a “click through”), this is the final site or app destination.

Malware - Any malicious software impacting a computer or device (e.g. phone, tablet, connected device, or router) without user consent. This can include (but not limited to) spyware, worms, bots, viruses, adware, phishing, auto-subscription, or unwanted changes to system configurations. Examples of malware events can include:

DRAFT

- Auto-Redirecting - Without interaction, an advertisement or script automatically redirects users to a website or app (typically an app store). The site or app can deliver malicious software to the user.
- Drive-by-Download - Users unintentionally download malicious software to their device, without their knowledge. This may occur via an ad impression.
- Deceptive Download - Users authorize a download. However malicious software is downloaded either instead or in addition to the authorized download. This may occur via an ad click, a deceptive ad posing as other content, or via a link on a landing page.

Scan - Analysis by means of static examination, virtual execution/emulation, or manual rendering of a creative or tag. This can and should also include any actions caused from user interaction, such as a click, and should also include malware detection on the landing page.

Scan Frequency - The regularity of which an ad is evaluated, scanned, or rendered for the purpose of compliance checks.

Tag - JavaScript or HTML code that indicates to the web browser or other client the location of the creative. Tags may also indicate the location of other tags.