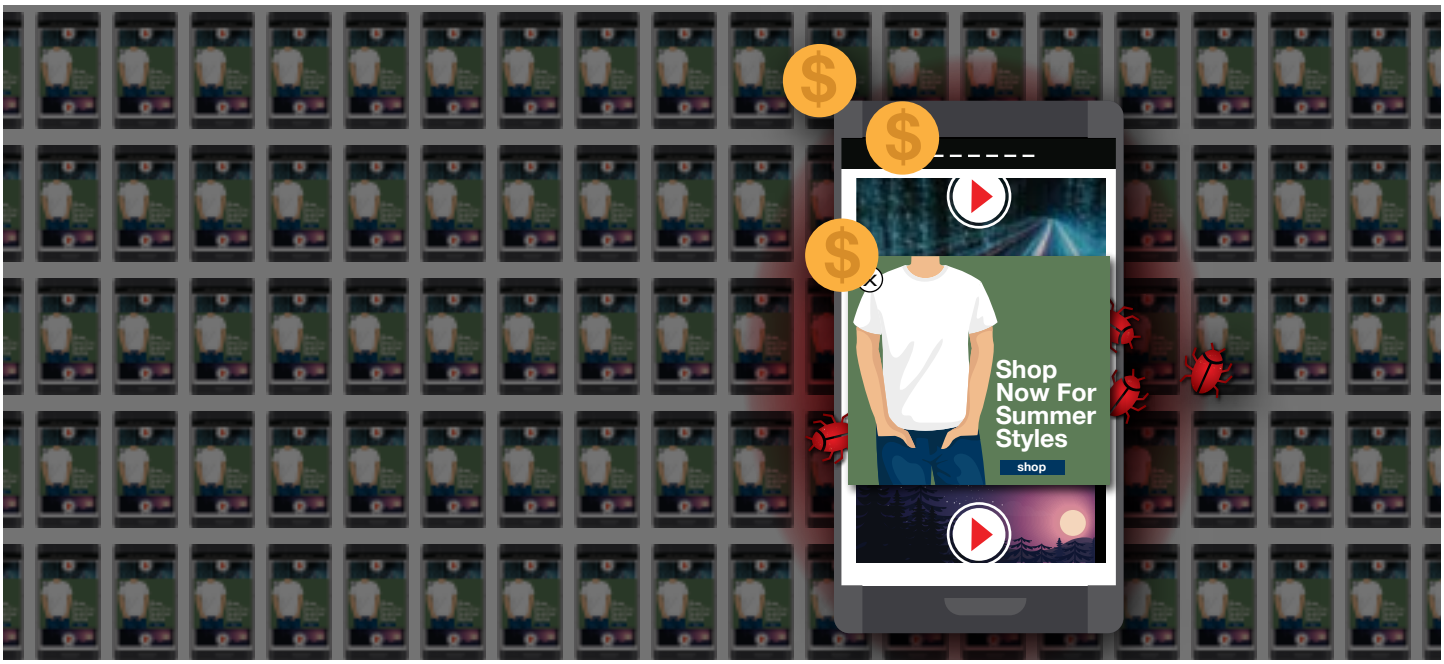
tag
TRUSTWORTHY ACCOUNTABILITY GROUP

CHANGING THE CRIMINAL CALCULUS:

BEST PRACTICES IN THE FIGHT AGAINST MALVERTISING

AUGUST 2020



Executive Summary

The dangers of malware are nearly as old as computers themselves, but the concept of malvertising is a relatively new one to businesses and consumers alike. While the term malware can mean malicious software of any sort delivered by any means, "malvertising" refers to the use of digital advertisements – including creative, tags and landing pages – specifically to distribute malware, often for financial gain.

The first known instance of malvertising dates to 2007, and criminal interest in using ads as a vector for malware attacks has grown slowly over more than a decade now. Malvertising is now a problem at scale, and the scope of that problem has doubled since 2017. Recent research suggests that nearly 1 in every 100 ad impressions are impacted by a malicious or disruptive ad – meaning that more than 20% of user sessions may be impacted by malvertising.

Malvertising degrades consumer trust in the digital advertising industry, and brands face significant financial risk if their ads are found to be "malvertising." A recent survey of U.S. consumers conducted by the Brand Safety Institute (BSI) and the Trustworthy Accountability Group (TAG) 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.

Because each participant in the ecosystem has visibility into only their subset of the problem, preventing the delivery of infected ads can be challenging without industry coordination. The digital advertising industry has taken significant action to combat the problem of malvertising in recent years, and those efforts are beginning to show dividends.

Keeping ads clean of malicious code is a serious brand safety concern, but the fight against malvertising does not have to be a painful one. By instituting best practices, tightening our collective defenses against malware threats and building a threat-sharing culture throughout digital advertising, the digital advertising ecosystem can change the criminal equation and put an end to the malvertising attacks plaguing our industry today.

The State of the Fight

What is Malvertising?

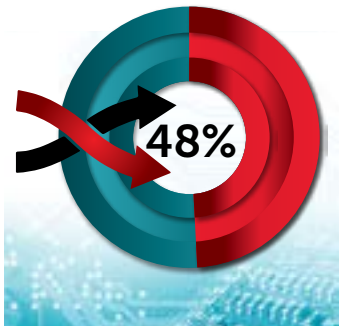
The dangers of malware are nearly as old as computers themselves, but the concept of malvertising is a relatively new one to businesses and consumers alike. While the term malware can mean malicious software of any sort delivered by any means, "malvertising" refers to the use of digital advertisements – including creative, tags and landing pages – specifically to distribute malware, often for financial gain.

Malvertising comes in a variety of forms. A legitimate ad can become malvertising – it can be corrupted once it has been placed on a publisher website, when it passes through an ad tech intermediary, or before a campaign even begins. In other cases, criminals create fake advertisers or advertising agencies, pretending to represent legitimate clients in an ad buy while in reality distributing fake ad creative infected with malware. Sometimes, rather than focusing on ads directly, criminals simply compromise third-party scripts or pieces of code that are delivered with an ad or page content for measurement or viewability purposes.

Here are just a handful of the types of malvertising attacks plaguing the digital ad ecosystem today.

In a **deceptive download** attack, consumers are lured by a fake ad to a fake landing page by criminals seeking to infect consumer devices with malware, or to steal consumers' money or personal information. Consumers may think that they are downloading programs or content that they desire, while those downloads are in fact malware in disguise.

Other types of malvertising attacks occur without the user experiencing anything suspicious. For example, in the case of **redirects** when users click on an infected ad it automatically sends them from



Redirects are the most prevalent form of malware in the digital advertising supply chain, accounting for 48% of all malvertising events

the website or app where the ad was placed to a fake website or app that they did not intend to visit, where malware is then delivered to users' devices without their knowledge. While consumers may be aware that they have ended up somewhere other than they intended, they are unlikely to have any idea that their devices have been infected. Redirects are the most prevalent form of malware in the digital advertising supply chain, accounting for 48% of all malvertising events.[1]

Drive-by-download attacks don't require a user to take any action – such as clicking – to be redirected, as infected ads on a website or in an app automatically initiate the download of malware when the consumer visits, without giving the user any sign that something has gone wrong.

Similar to a drive-by-download, a **watering hole** attack targets a specific audience by taking advantage of a legitimate site or app, or setting up fake ones likely to be of interest to a particular category of end users. Users visit the "watering hole," where an infected ad initiates the download of malware onto their devices without their knowledge.

Regardless of how a malicious payload is attached to an ad, once infected ads enter the digital adverting supply chain, they are well-positioned to deliver malware onto consumer devices.

[1] "Preventing Malware With Safe Frame: Pros & Cons," GeoEdge, July 2020.

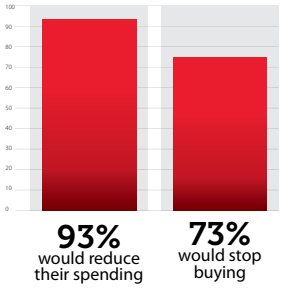
A Problem at Scale

The first known instance of malvertising dates to 2007, and criminal interest in using ads as a vector for malware attacks has grown slowly over more than a decade now. Focusing first on infecting ads placed on major publisher sites, criminal entities expanded their targets to include major ad networks by 2013, when Symantec posited that the one-third rise in drive-by attacks seen that year was largely due to malvertising.[2]

Malvertising is now a problem at scale, and the scope of that problem has doubled since 2017.[3] Recent research suggests that despite improvements in the malvertising landscape, nearly 1 in every 100 ad impressions were still impacted by a malicious or disruptive ad, suggesting that more than 20% of user sessions may be impacted by malvertising.[4]

Recent research suggests that nearly 1 in every 100 ad impressions were still impacted by a malicious or disruptive ad, suggesting that more than 20% of user sessions may be impacted by malvertising

The financial impact of malvertising has grown apace as well. In 2015, research from the Interactive Advertising Bureau (IAB) and Ernest & Young suggested that the digital advertising industry had lost $1.1 billion in the previous year due to malvertising, including revenue lost from black-listing and malware-related ad-blocking, as well as the cost of fighting and remediating malvertising attacks.[5] By 2018, it was estimated that the industry lost $210 million annually to auto-redirects, and another $920 million from the ads auto-redirects facilitated with click fraud.[6]



While the direct costs of malvertising is significant, malvertising attacks make it possible for criminals to steal even greater revenue through ad fraud. The Bot Baseline study by White Ops and the Association of National Advertisers (ANA) projected that the digital advertising industry would lose $5.8 billion to ad fraud globally in 2019.[7]

There are also intangible costs associated with malvertising, with consumer trust at the top of that list. A recent survey of U.S. consumers conducted by the Brand Safety Institute (BSI) and the Trustworthy Accountability Group (TAG) 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.[8] These findings highlight the significant financial risk that brands face if their ads are found to be "malvertising," carrying malware payloads that can harm the very consumers their ad campaigns seek to engage.

Industry Action

Malvertising degrades consumer trust in the digital advertising industry, and stymies industry growth by feeding ad revenue to criminals. Because each participant in the ecosystem has visibility into only their subset of the problem, preventing the delivery of infected ads can be challenging without industry coordination. The digital advertising industry has taken significant action to combat the problem of malvertising in recent years, and those efforts are beginning to show dividends.

Setting Standards

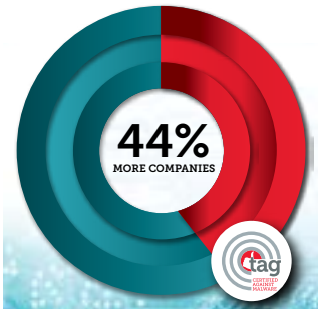
The TAG Certified Against Malware Program

Adoption of industry best practices is one important means of ensuring that malvertising attacks are prevented whenever possible, and properly remediated when they do occur. Since 2014, the Trustworthy Accountability Group (TAG) has partnered with industry leaders to design and strengthen a robust anti-malware program for the digital ad supply chain.

TAG launched its Certified Against Malware Program in 2016, providing companies with a roadmap for taking on the complicated issue of malvertising. Companies that obtain the Certified Against Malware Seal can use the seal to publicly communicate their commitment to combatting malvertising in the digital advertising supply chain.

---

[2] "2013 Symantec Internet Security Threat Report," Symantec, April 2013.
[3] "The Media Trust Cements Malware Certification for Record Fourth Year in a Row," The Media Trust, March 2020.
[4] "Confiant Data Quality Report Q1 2019," Confiant, January 2020.
[5] "What is an Untrustworthy supply chain costing the US Digital Advertising Industry?" IAB US benchmarking study, provided by Ernst and Young, November 2015.
[6] "Auto-Redirects: A Security Paper by GeoEdge," GeoEdge, January 2018.
[7] "Bot Baseline Report: Fraud in Digital Advertising," ANA and White Ops, May 2019.
[8] "Consumer Perceptions Around Brand Safe Advertising," Trustworthy Accountability Group, August 2019.



As the BSI/TAG survey highlighted, there is a growing awareness of malvertising threats among consumers. The digital advertising industry has reacted to that consumer attention with greater vigilance and a strengthening of anti-malware practices, including increased participation in the TAG's Certified Against Malware Program. The number of companies holding the Certified Against Malware Seal grew by more than 44% in the past year, and Confiant has posited that participation in the program was one of several factors underlying continued improvement in the rate of malicious impressions seen in the digital ad supply chain, along with greater industry-wide awareness of malvertising and better overall collaboration between industry partners.[12] This growth and recognition only reinforces that the Certified Against Malware Seal is an important way that companies communicate their commitment to protecting consumers and their clients – and a powerful symbol that brands seek when choosing partners.

Fighting Back…Together
Coordinated Response to Criminal Threats

TAG has facilitated threat-sharing across the digital ad industry since its inception in 2015, and the suite of threat-sharing tools available to the TAG Community has grown and evolved significantly over time to include all-hands briefings on major malvertising and ad fraud attacks to coordinate industry response; the Data Center IP List to help companies remove non-human traffic that should not be monetized; and the Pirate Mobile App List to aid marketers in keeping their ads from association with apps hosting pirated or counterfeit content.

While these types of monthly, quarterly or periodic threat-sharing efforts have been key in reducing criminal activity within the digital advertising supply chain, real-time threat-sharing throughout the industry remains very limited. Understandably, companies have been reticent to share intelligence directly with competitors, even if doing so would better protect their own assets.

Recognizing that companies needed a trusted third-party to facilitate that type of threat-sharing, TAG was designated as the sole Information Sharing and Analysis Organization (ISAO) for the digital advertising industry in 2017. With this Department of Homeland Security (DHS) designation, TAG serves as a hub for the industry to gather and analyze information related to threats affecting the digital advertising supply chain, and as a conduit for partnership with government agencies and law enforcement bodies in the fight against such criminal activity.

TAG serves as a hub for the industry to gather and analyze information related to threats affecting the digital advertising supply chain

While the concept of sharing threat intelligence is fairly new to the digital advertising ecosystem, the industry has already enjoyed several huge wins against malvertisers thanks to companies sharing information about the threats they uncover with one another and partnering with law enforcement to take down the criminal rings responsible. One of the most successful examples of industry collaboration to date was in the case of the Methbot and 3ve attacks, which ultimately resulted in coordinated takedown.

Methbot was first identified in December of 2016 and brought to the attention of the TAG Community by White Ops. TAG quickly activated the information-sharing infrastructure it had built and organized an emergency briefing on the fraud operation for hundreds of executives at leading companies across the industry, enabling companies to learn about the threat directly from White Ops, and to evaluate and respond to it in real time.

[9] "Confiant Data Quality Report Q1 2019," Confiant, January 2020.

While quick and concerted action by the TAG Community stopped the monetization of Methbot in its tracks, the criminals behind the attack did not give up on defrauding the digital ad supply chain. Instead, they simply changed techniques, this time using malvertising to launch the 3ve attack.

3ve was one of the most complex and sophisticated ad fraud operations seen to date, operating on a massive scale. At its peak, the criminals behind 3ve took control of over 1 million IPs through residential botnet infections and attacks on corporate IP spaces. 3ve was designed in such a way that several sub-operations allowed the massive fraud infrastructure to continue operating even when one part of it was disrupted. At its peak, 3ve generated billions of fraudulent ad bid requests.

Having first identified 3ve in 2017, Google and White Ops engaged companies from across the digital ad supply chain – including Adobe, Amazon Advertising, CenturyLink, Facebook, Microsoft, Oath and The Trade Desk – in a coordinated takedown of 3ve's operational infrastructure, rendering its bots unable to continue driving fraudulent ad traffic.[10] The case was also referred to law enforcement, and in November 2018, the U.S. Attorney's Office for the Eastern District of New York announced criminal charges against those associated with both the Methbot and 3ve operations.[11]

Real-Time Threat-Sharing
The TAG Threat Exchange

In their white paper describing the 3ve takedown, Google and White Ops described the importance of industry collaboration in fighting this and future threats to the industry, and noted the vital role of TAG and other industry bodies "as agents of change and collaboration across our industry."[12] In fact, at the same time that the Federal Bureau of Investigation (FBI) and DOJ were working with digital advertising companies to affect the takedown of Methbot and 3ve, TAG was working with many of those same companies to stand up the TAG Threat Exchange, a robust platform to facilitate real-time threat-sharing within the trusted TAG Community.

After working closely with experts from the TAG Anti-Malware Working Group to clearly define the industry's needs in this area throughout 2018, Team TAG stood up the TAG Threat Exchange – powered by TruSTAR technology – to provide the TAG Community with the ability to:

- Leverage a centralized intelligence platform to collaborate within your company, with other companies working to combat the same threat, or with the TAG Community as a whole;

- Share and receive timely, actionable and highly relevant threat intelligence between trusted parties in the TAG Community;

- Enrich, enhance, and shorten your own investigations with high-fidelity intel.

Early adopters of the TAG Threat Exchange included a handful of TAG's largest ad tech member companies with sophisticated capabilities to detect, analyze, mitigate and share intelligence about malvertising threats facing the digital advertising ecosystem. Intel-sharing among those "super users" has focused on malicious redirect attacks, which has substantially reduced time-to-live (TTL) for these attacks.[13]

Continued expansion of the TAG Threat Exchange will focus on operations that serve new aspects of TAG's crime-fighting mission, new types of intelligence, and more of the TAG Community.

[10] "The Hunt for 3ve: Taking down a major ad fraud operation through industry collaboration," Google and White Ops, November 2018.
[11] "Two International Cybercriminal Rings Dismantled and Eight Defendants Indicted for Causing Tens of Millions of Dollars in Losses in Digital Advertising Fraud," US Department of Justice, November 2018.
[12] "The Hunt for 3ve: Taking down a major ad fraud operation through industry collaboration," Google and White Ops, November 2018.
[13] "Malware Attack Bypasses Blockers to Target Consumers," The Media Trust, July 2020.

Best Practices for Fighting Malvertising

Keeping ads clean of malicious code is a serious brand safety concern, but the fight against malvertising does not have to be a painful one. The actions that best-in-class buyers and sellers take today to prevent and remediate malvertising threats provide a roadmap of best practices that can ensure success on this important aspect of overall brand safety. Everyone in the digital advertising industry can benefit from following simple and proven effective best practices.

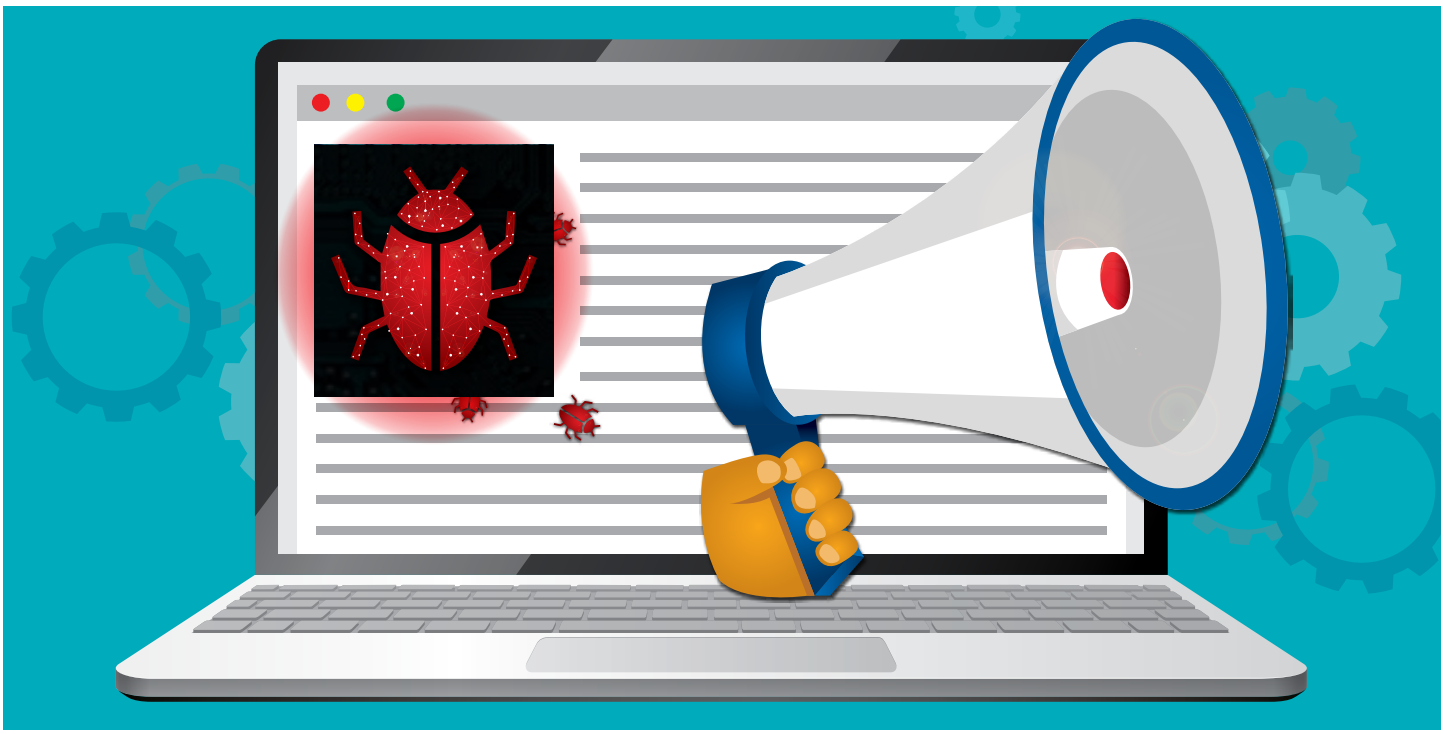
Responsibility
Take Responsibility and Communicate Your Commitment

The fight against malvertising starts at home. Brands that want to ensure their ads are not inadvertently infecting consumer devices with malware focus resources on achieving that goal. Brands also need to be aware of the risk of unauthorized use of their creative assets and place pressure on the industry to clean up abuses.

Create – and sustain – an internal focus on keeping your ads free from malware. Consider creating a brand safety team, or resources within such a team with particular expertise relating to malvertising, and conducting regular trainings to ensure that employees understand the negative impact of malvertising and how to fight it effectively.

Develop a "zero tolerance" policy for ads infected with malware. Communicate it clearly throughout your organization and to all of your partners.

Earn the TAG Certified Against Malware Seal to ensure that your brand is ready to partner effectively with your chosen media agencies and anti-malware vendors.



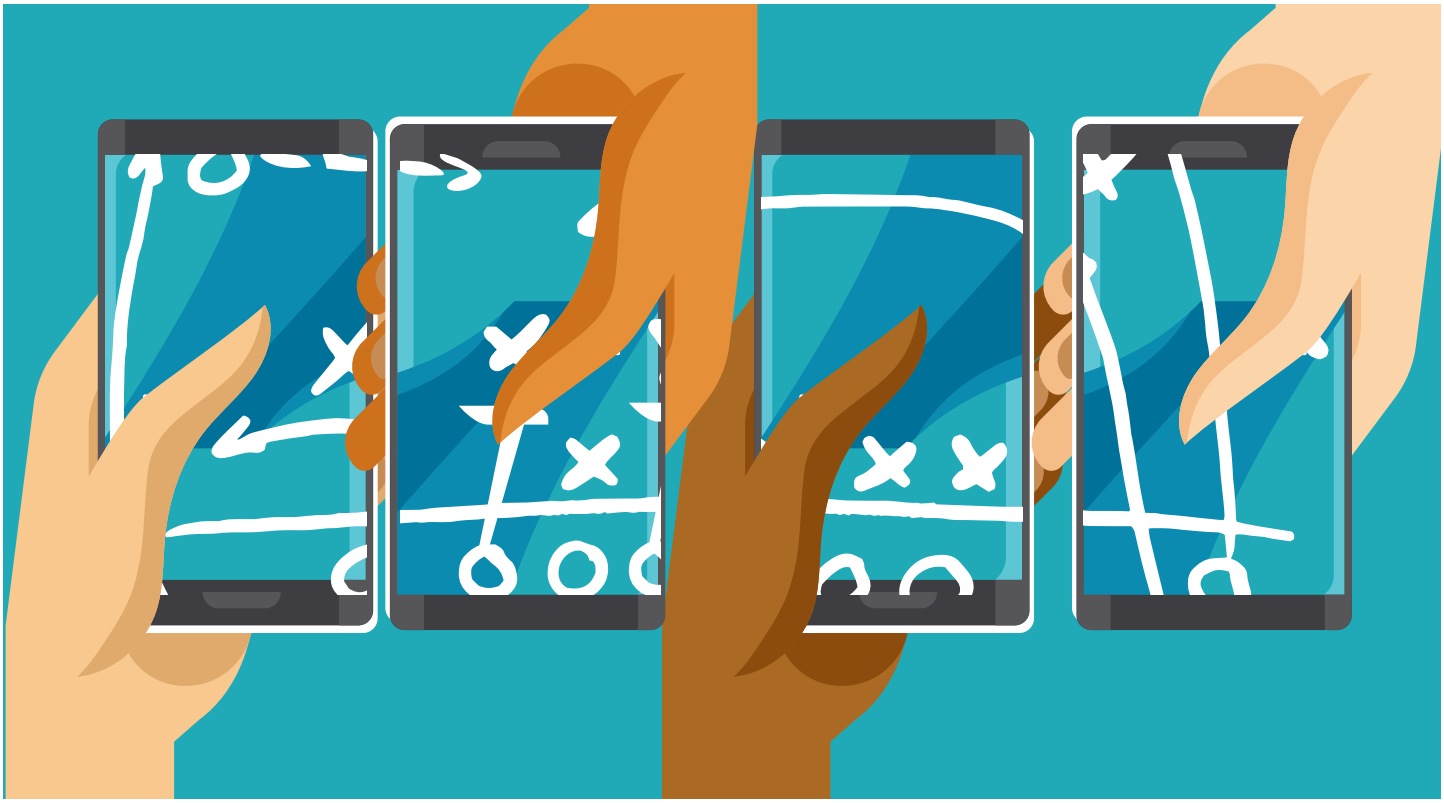
Partnership
Choose the Right Partners

Marketers that are serious about brand safety should work with trusted partners, including those who are Certified Against Malware.

Know your risk tolerance and choose partners that share and can accommodate those values. For example, a site that allows user-generated content might seem high-risk because users may upload copyrighted material, but strong policies against IP and copyright infringement, technology solutions like fingerprinting, clear user policies, and a strong arsenal of takedown tools can ultimately make it a much lower-risk placement for advertisers.

Ask the right questions during your RFP process. For example, review whether potential partners use malware scanning and real-time detection techniques that ensure proactive avoidance of malware infections are in place for all campaigns.

Look for the TAG Certified Against Malware Seal. Ensure that your media agencies and their anti-malware partners are TAG Certified Against Malware. Consider whether such TAG Certified partners have also achieved the TAG Certified Against Fraud and Certified Against Piracy Seals. Malware, piracy and fraud often go hand in hand, so having a partner with expertise in all of these areas can deepen your protection.



Strategy
Work Closely with Partners to Develop and Execute Your Strategy

Designate a trained Brand Safety Officer to work with partners in protecting your ad creative from carrying malicious payloads and infecting potential customers.

Document appropriate points of contact at partner companies. Identifying key contacts at partner companies allows rapid and precise escalation and notification when malvertising attacks occur.

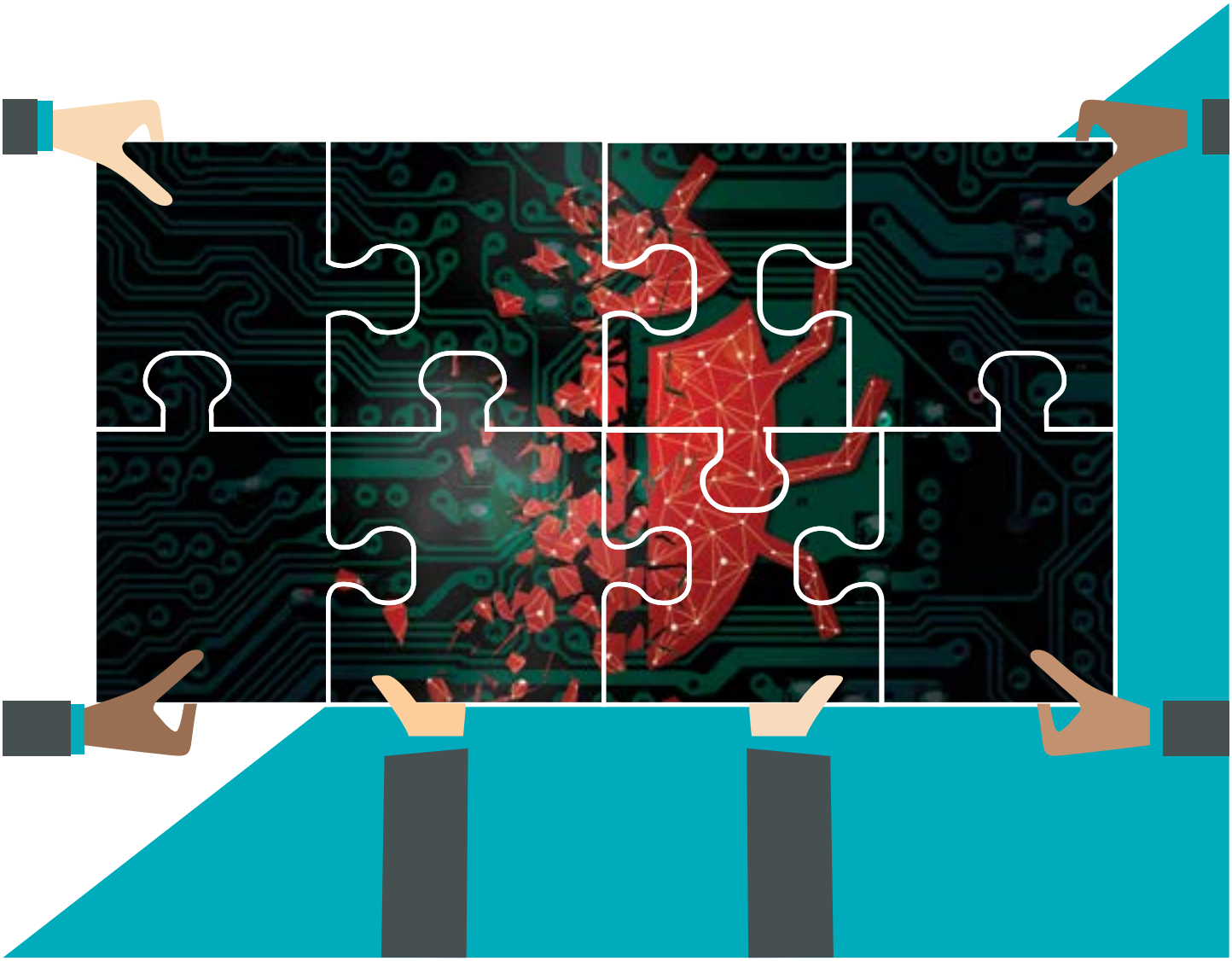
Clearly communicate a plan to protect your assets before a campaign launches. Require partners to employ technical and business process measures to prevent malware. These measures will differ depending a partner's position and role in the digital ad supply chain, but any malware prevention responsibilities should be documented in legal agreements. TAG's Certified Against Malware Guidelines speak to such requirements in greater detail.

Stay involved once campaigns are launched. Work with partners to ensure that ads are monitored for malicious payloads and confirm that the proper mitigation strategies are in place to stop malvertising attacks at any point in a campaign – from preflight to conclusion.

Seeing the Bigger Picture

Provide partners with information about incidents of malware-infected creative so that they can be on the lookout for recurrences of those issues throughout your campaigns.

Support industry-wide threat sharing to strengthen your own defenses. Proactive information sharing helps build industry resilience against evolving threats. Get involved in programs like the TAG Threat Exchange to share information about threats you see, and stay abreast of new and emerging threats that could affect your campaigns. Encourage your partners to do the same so that they can better protect your assets all across the digital advertising supply chain.



Staying Ahead of the Curve

While the digital advertising industry has had some huge collective successes combatting malvertising in recent years, criminals continue to look for new ways to subvert the digital advertising supply chain and infect ad creative and malicious payloads that endanger consumers. Awareness of the evolving nature of malvertising is key to staying ahead of emerging threats – and achieving greater success in preventing and remediating malvertising attacks.

Emerging Threats

Malvertising in a Quarantined World

While most of the world is lamenting the COVID-19 pandemic and resulting quarantine, malvertisers have been taking full advantage of the situation to launch new attacks with malicious ads focused on COVID-19, and taking advantage of security issues arising as companies around the globe shift their workforces to work from home. According to recent research, daily malware threats to the digital ad supply chain have increased an average of 18% as news of COVID-19 drove increased web traffic.[14]

As a result, there have been increased threat levels in verticals like Education and Home, which saw increased traffic due to quarantine lifestyle adjustments.[15] At the same time, verticals including Travel, Sports and Auto – which saw drops in ad spend as a result of quarantine – continued to see high threat levels because lower CPMs attracted malvertisers looking to make a profit.[16]

With unemployment skyrocketing, malvertisers whose criminal pursuits might have previously been a hobby have ramped up activity in an effort make the launch of malware attacks a full-time job. For example, incidents of the well-known ICEPick-3PC or eGobbler attacks increased by 300% or more beginning in March 2020, just as COVID-19 quarantine began in many parts of the world, with a single one of those incidents potentially impacting hundreds of thousands of web or mobile app users.[17] Many of those attacks come on weekends, when consumers are most likely to be online and adtech staff are least likely to be working and able to react quickly.

[14] "Enterprises on the Alert for New Malware and Breach Sources," The Media Trust, April 2020.
[15] "Q2 2020 Smart Report," clean.io, July 2020
[16] Ibid.
[17] "Enterprises on the Alert for New Malware and Breach Sources," The Media Trust, April 2020

Enticing Ad Environments

The higher the traffic, the more enticing an advertising environment is for malvertisers. Recent research showed that social media sites were more than twice as likely as the average site to fall victim to malvertising, with family and parenting sites and news sites also at high risk of being targeted by malvertisers.[18]

Mobile web and in-app environments continue to be the most attacked ad environments in the digital ad ecosystem, with many malvertising attacks focusing specifically on mobile devices.[19] Embedded mobile browsers are a particularly fraught threat vector.[20] All of this makes the protection of user experience on mobile devices a greater challenge.

Same Attacks, New Techniques

Criminals don't give up – they just try new techniques. Bad actors are constantly launching new malvertising attacks that leverage unique and creative ways to target users – and to disguise their activities from those in the digital advertising ecosystem working to guard against malware. New techniques that result in successful attacks spread rapidly among criminal communities, leading to fast-paced adoption of tried and true methods within the digital supply chain.

As companies get smarter about their malvertising defenses, criminals continue to look at new ways to hide their attacks. One recent malicious campaign affecting iPhone users of over 100 publisher websites was notable for its use of a unique method to deliver its malware payload through a multi-stage redirect mechanism, making it harder to identify, and using two methods to evade conventional scanning and blocking tools.[21]

Another popular type of obfuscation seen in recent malvertising attacks is the abuse of WebRTC protocols, the open framework that provides browsers and apps with Real-Time Communications (RTC).[22] Taking advantage of peer-to-peer protocols like WebRTC makes blocking these malvertising attacks more difficult, since there is not a domain or server that can be blocked. In the last year, 87% of WebRTC attacks appeared in header bidding, with 84% of the attacks occurring on mobile devices and 16% on tablet.[23]

Other malvertisers are eschewing the work necessary to hide behind carefully crafted fingerprinting and targeting in favor of bombardment tactics. For example, one recent attack operates by generating anywhere from dozens to hundreds of ad creatives each day – each with subtle variations – with the intent of overwhelming platforms and security vendors with a flood of demand that will slip through their defenses.[24]

Newer attacks are also further blurring the lines between malvertising and other brand safety issues. One attack identified early this year falls into the categories of both malvertising and deceptive advertising as it exploits users interested in cryptocurrency investment. It is notable for having perfected the art of avoiding ad quality reviews using evasion techniques such as cloaking (display of fake ad creatives and landing pages to ad quality scanners).[25] Another recent attack used trusted brand names to mask their deception, exploiting users' IP addresses to serve deceptive messages from their Internet Service Providers offering a gift lottery in return for completing a malicious service survey.[26]

Malvertisers stay ahead of marketers by shifting the means by which already well-known attacks take advantage of the supply chain as well. For example, the well-known eGobbler/ICEPick-3PC attack previously operated by exploiting obscure browser bugs to bypass built-in browser protections, allowing it to create pop-ups and forced re-directs. After a previous vulnerability

[19] "Confiant Data Quality Report Q1 2020," Confiant, January 2020.
[22] "Q2 2020 Smart Report," clean.io, July 2020.
[20] Ibid.
[21] "Krampus-3PC: Persistent Malware Using Multiple Techniques Hits Online Readers in Time for the Holidays," The Media Trust, December 2019.
[22] "WebRTC Malvertising: Fighting a New Form of Obfuscated Attacks," GeoEdge, March 2019.
[23] "WebRTC Is the Newest, Trickiest Front in the Fight Against Redirects", GeoEdge, March 2019
[24] "Confiant Data Quality Report Q1 2020," Confiant, January 2020.
[25] "Confiant Data Quality Report Q1 2020," Confiant, January 2020.
[26] "Global Malvertising Attack Morphixx Exploits Users IP Address," GeoEdge, July 2020

was shut down in early 2019, eGobbler instead began using a Webkit exploit, taking advantage of the open source web browser rendering engine created by Apple.[27] This is a powerful shift, given that a single vulnerability in WebKit may impact all WebKit-based Apps. Similarly, just two years ago, the malvertisers behind Zirconium were focused on creating large numbers of fake agencies to win seats on buying platforms. They have since shifted their approach, and Zirconium is now a very sophisticated attack notable for leveraging unique fingerprinting techniques that are carried out in multiple stages.

As malvertisers continue to look for new ways to subvert detection and security technologies, they are also increasingly taking advantage of the adtech backbone of the digital ad industry in order to launch malvertising attacks. For example, a new type of redirect attack seen this year has cast doubt on a security approach known as the Sandboxing Doctrine by launching attacks through legitimate ad servers, enabling malvertisers to breach browser security mechanisms and bypass security companies that rely on Sandboxing.[28]

Evolving Techniques to Keep Ads Clean

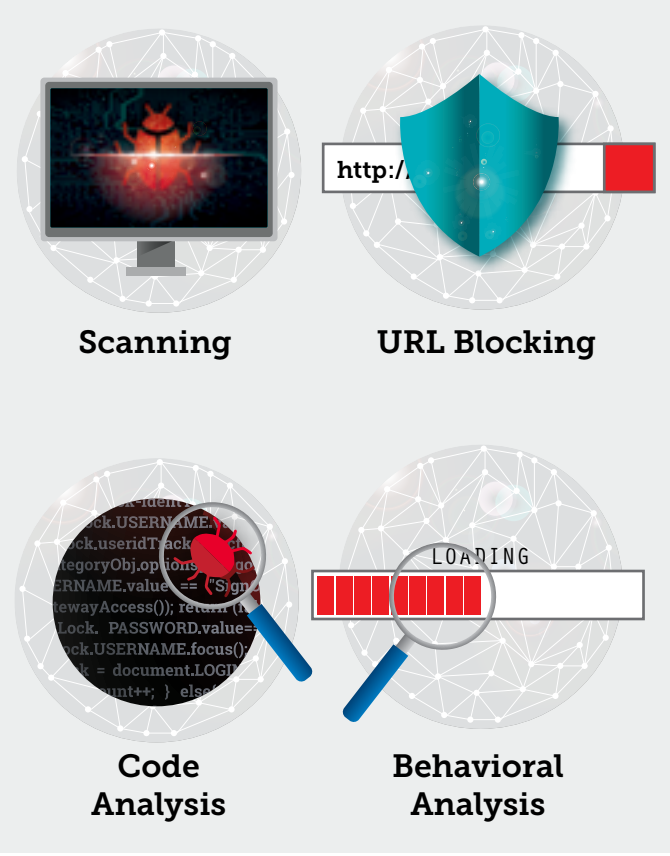
As criminals constantly work to evade defenses, it is vital that players across the digital ad ecosystem do the same if publishers and their end users are to remain safe from malicious payloads. Since an ad can become infected at any point as it traverses the digital ad supply chain, everyone from the brand to the publisher has a role to play in fighting malvertising.

There are several different techniques used across the digital ad supply chain to keep ads clean of malware. Among the most long-standing techniques is the periodic scanning of campaign assets including ad creative, tags and corresponding landing page URLs. This is done both preflight and throughout the lifecycle of a campaign, and generally involves scanning from a variety of profiles covering diverse geography, device, browser/OS and behavioral combinations.

Other malvertising detection techniques take a different approach to keeping ads clean – monitoring ads and preventing malvertising "in real time," based on blocklists or code analysis. In the case of blocklists, publishers and platforms weed out known bad ads at the time of attempted purchase by the bad actor by comparing the URL to a list of known malicious URLs. If the URL is deemed to be malicious, the auction will not complete and the bad actor will be blocked from buying the impression they were seeking to purchase. In prevention through code analysis, the platform looks at the ad code itself for characteristics and markers that correlate with malvertising, such as code that is overly obfuscated, and will block the ad before it has a chance to serve.

Another real-time approach is known as run-time behavioral analysis. With this technique, JavaScript code on a site or within an ad server executes in the user's browser when the user loads a page. As the ads load, the code monitors for specific behaviors deemed nefarious and blocks only the malicious JavaScript, while allowing the original ad purchased from the bad actor to render. While the bad actor's ad is allowed to render, it is not able to achieve any ROI or engagement, as the end user is not redirected to the malicious landing pages.

There are strengths and weaknesses to each of these techniques, but each prioritizes both consumer and brand safety by creating a more secure digital ad ecosystem.



[27] "Confiant Data Quality Report Q1 2020," Confiant, January 2020.
[28] "Why Sandboxing Won't Cut It When It Comes to Malvertising," GeoEdge, February 2020.

Conclusion

When a malvertiser fails to make money targeting one site with malicious ads because the publisher and its supply chain partners have implemented the strongest possible defenses, that bad actor is less likely to target the same site again. The site's visitors are safer from malware infections, and the brands advertising there are safer from financial and reputational risk.

Unfortunately, in the current environment that simply means the bad actor looks to target another player in the digital advertising ecosystem, continuing to take money out of the pockets of legitimate companies and harm consumers. Criminals will continue to target the digital advertising supply chain until it is easier to target something else.

By instituting best practices, tightening our collective defenses against malware threats and building a threat-sharing culture throughout digital advertising, the digital advertising ecosystem can change the criminal equation and put an end to the malvertising attacks plaguing our industry today.

Appendix: TAG Certified Against Malware Companies

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. The companies listed have been awarded the TAG Certified Against Malware Seal in one or more covered party category. Learn more about the Certified Against Malware Program at https://www.tagtoday.net/malware/.

Ad Lightning
Certified as a Malware Detection Vendor

Adform
Certified as an Intermediary

eBay
Certified as a Buyer & Seller

Google
Certified as Buyer, Intermediary & Direct Seller

Index Exchange
Certified as an Intermediary

Media Math
Certified as a Buyer & Intermediary

OpenX
Certified as an Intermediary

Publicis Media
Certified as a Buyer

RhythmOne
Certified as an Intermediary & Direct Seller

RiskIQ
Certified as Malware Detection Vendor

Roku DSP
Certified as an Intermediary

Sovrn
Certified as an Intermediary

SparkLit
Certified as an Intermediary

SpotX
Certified as an Intermediary

OpenX
Certified as an Intermediary

Publicis Media
Certified as a Direct Buyer

Publishers Clearing House
Certified as a Direct Seller

RhythmOne
Certified as an Intermediary and Direct Seller

RiskIQ
Certified as a Malware Detection Vendor

Sizmek
Certified as an Intermediary

Sovrn
Certified as an Intermediary

SpotX
Certified as an Intermediary

The Media Trust
Certified as a Malware Detection Vendor

Uproxx
Certified as a Direct Seller

Verizon Media
Certified as an Intermediary

Walmart.com
Certified as a Direct Seller

Xandr
Certified as a Direct Seller