tag

THREAT
INTELLIGENCE

EXPLOITING TRUST:

Social Engineering Tactics On The Rise In Malvertising

July 2023

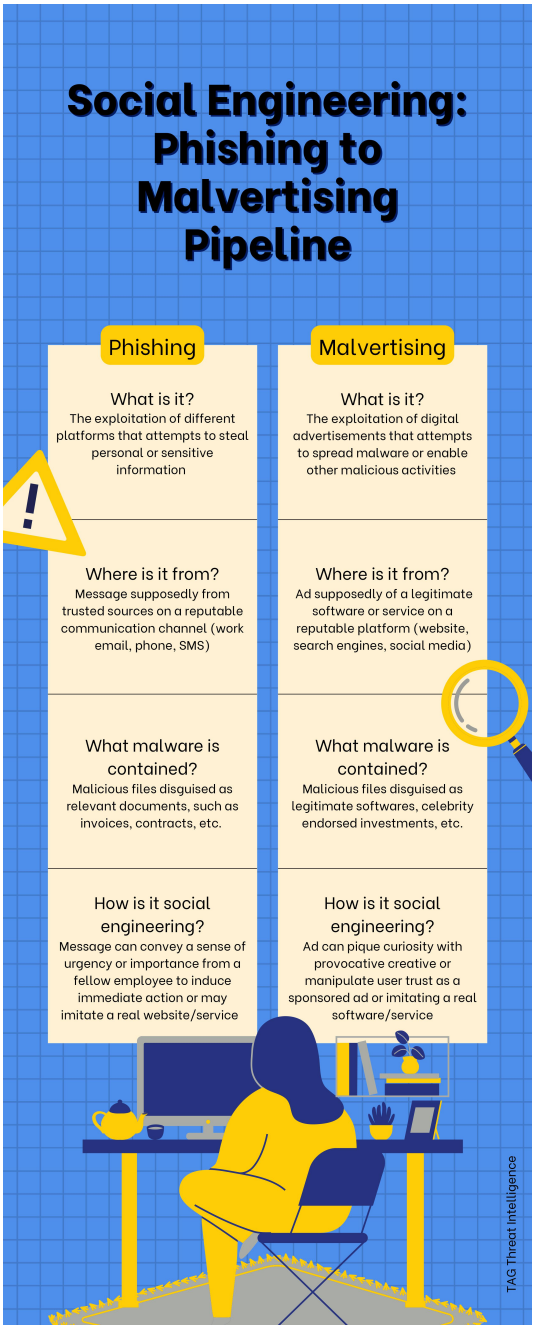
Internet users remain largely unaware of the threat of malicious and low-quality advertisements on popular and trusted websites, social media platforms, and within search engine results because traditional cybersecurity training programs focus almost exclusively on the dangers of social engineering attacks via email and text messages - a gap that cybercriminals are increasingly using to their advantage.

Executive Summary

TAG Threat Intelligence assesses cybercriminals are all but certain to expand their use of digital advertising-enabled social engineering attacks over the next year. We are observing criminals rapidly adapt the core social engineering principles that make email phishing campaigns successful to online ads, a threat that is far less known to potential victims. The slowing rate of market expansion as well as other economic uncertainties also make advertising inventory more readily available to less reputable advertisers, enabling bad actors to display malicious or low-quality ads. We have high confidence in our assessment, which is based on reliable open sources and verified threat intelligence shared within the TAG Malvertising Threat Exchange (MTX) corroborated by highly reliable, third-party technical data and qualified subject matter experts.

Malvertising Overview

The TAG Malvertising Taxonomy defines malvertising as the malicious use of digital advertisements to spread malware and compromise systems to harm end users, publishers, and platforms. Threat actors take advantage of the vulnerable areas within the advertising supply and demand chain by exploiting the various elements of digital ad designs, such as pixels, code, landing pages, or other elements, to deploy malicious payloads while also circumventing current security countermeasures in place. As malvertisers are constantly evolving their tactics and techniques, TAG continues to update the Malvertising Taxonomy and inform the digital advertising industry of the most relevant and current malvertising-focused threat intelligence.[i]



Digital Ads a Perfect Match for Social Engineering

Social engineering is not a new concept; for decades, threat actors successfully exploited users' trust by running email phishing campaigns. More recently, cybercriminals are increasingly using multichannel phishing to evade email security and instead exploit less protected SMS, voicemail, and chat-based collaboration tools. Malvertising campaigns cataloged in the MTX increasingly utilize the same core social engineering principles behind other phishing campaigns, but instead leverage scam ads on trusted websites and within search engine results.

- According to multiple cybersecurity researchers, multichannel phishing is on the rise, with

cybercriminals leveraging social engineering tactics in highly tailored and targeted attacks across email, SMS, and chat-based platforms. The current success of these attacks stems from having a wider attack surface, and their effectiveness will only rise with the help of generative AI.[ii]

- Most recently, malvertisers utilized a hybrid of search engine optimization (SEO) poisoning and social engineering tactics to exploit sponsored ads disguised as legitimate software download pages on popular search engines and social media platforms. The success of these attacks hinge on users having an implicit trust in well-known platforms and the ads they display.[iii],[iv],[v],[vi]
- In an ongoing malvertising campaign dubbed FizzCore, malvertisers use provocative ad creatives featuring celebrities to entice users to click, which leads to a landing page promoting a cryptocurrency investment scam. The use of ad creatives to pique users' curiosity garnered much success, with the cybercriminals behind FizzCore earning up to $1M in a single day.[vii] FizzCore's success has not gone unnoticed by other cybercriminals, with copycat tactics accounting for a plurality of threat intelligence shared by MTX members in 2023.[viii]

Cybersecurity Training Shortfall

Traditional cybersecurity training programs caution internet users against threat actors that may attempt to infiltrate a company through trusted means within a workplace, such as through their email application. However, these programs fail to teach best practices for maintaining online security outside of an organization's perimeter, where users are likely to encounter malvertising.

- Internet users usually receive cybersecurity training through their school or workplace, which generally focuses on securing their own information systems. However, cybercriminals leverage a broader array of threat vectors, including malvertising, that leverages social engineering principles. This aspect of the threat is not taught in most, if any, traditional cybersecurity programs.[ix]
- The U.S. National Institute of Standards and Technology (NIST) publication titled NIST SP 800-50 serves as a framework and guide for organizations to create their own cybersecurity training programs; however, NIST does not include malvertising or any subject related to digital advertising among the 27 recommended training topics, though the standard is updated periodically.[x]
- In 2013, the MITRE Corporation released the MITRE ATT&CK Framework, a benchmark for a curated knowledge base documenting known tactics and techniques of threat actors. However, it was not until April of this year that MITRE added malvertising to the list of attack methods.[xi]

Market Conditions Increase Opportunities for Bad Ads

The ad tech industry is seeing a slowing growth rate in global ad spending due to economic uncertainties, which may give cybercriminals more opportunities to enter the ad ecosystem and take advantage of the current market conditions.

- Global advertising spend is forecast to only grow around 3.3% in 2023, a change from the 3.5% projection just a few months ago in December 2022. Overall digital advertising spending will also experience its third slowest rate of expansion in the past two decades, leading to further budget cuts and ad tech layoffs.[xii],[xiii],[xiv]
- The recent stagnant growth of overall ad spending has led some digital platforms to lower their ad pricing, creating opportunities for lower-quality advertisers.[xv]
- Cybercriminals have a history of exploiting economic or social disruptions, some of which include the recession in 2008 and the COVID-19 crisis in 2020. With the current economic downturn, the ad tech industry can expect to see an increase in criminal activity, particularly malvertising, in their ecosystem.[xvi]

Outlook

While we have not seen advertising exploited as part of a multichannel phishing attack, it is plausible this scenario emerges in the coming year. TAG lacks the corroborated evidence to confidently estimate the probability of this event; however, a logical next step for cybercriminals would be to leverage micro- and geo-targeted ads in multichannel phishing attacks on the employees of, for example, a specific corporate campus or critical infrastructure location. Cybercriminals recently demonstrated this kind of creativity in their ability to rabidly adapt social engineering principles to new attacks in the development, and subsequent rapid proliferation, of SEO poisoning and FizzCore-like scam ads.

Glossary

Malvertising – 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.

Social engineering – the use of psychological manipulation to deceive a victim into revealing personal identifiable information (PII) or allowing access to a computer system.

Phishing – a form of social engineering in which cybercriminals attempt to steal sensitive information or gain access to computer systems using fraudulent emails or other communication platforms by disguising as legitimate and trusted sources.

Multichannel phishing – the expansion of phishing to reach several channels of communication beyond email, SMS, and phone.

Search engine optimization (SEO) poisoning – a technique used by cybercriminals to boost the overall ranking of their malicious website to appear higher on search result pages, leading unsuspecting users to click on the site and potentially download malware or other malicious content.

Authored By TAG Threat Intelligence

Contact TAG/TI at info@tagtoday.net.

TAG is the Information Sharing and Analysis Organization (ISAO) for the digital advertising industry, a U.S. Department of Homeland Security designation making TAG the primary forum for sharing cyber threat intelligence in our industry.

The TAG Malvertising Threat Exchange (MTX) enables the TAG Community to share real-time intelligence about threats they see, stay abreast of new and emerging threats that could affect their operations, and protect the digital advertising supply chain as a whole.

The MTX enables companies to:

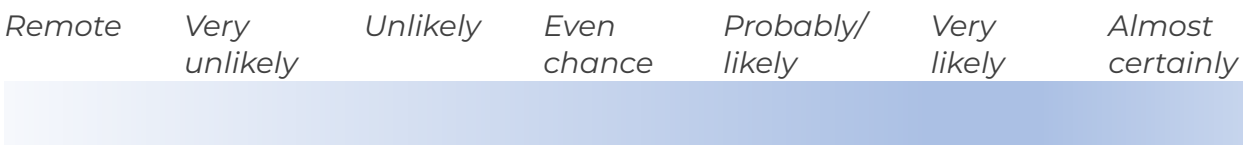
- Leverage a centralized intelligence platform to collaborate within your company, with other companies working to combat the same threat, or with the TAG Community as a whole;
- Share and receive timely, actionable and highly relevant threat intelligence between trusted parties in the TAG Community;
- Enrich, enhance, and shorten your own investigations with high-fidelity intel.

What We Mean When We Say: An Explanation of TAG's Estimative Language

We use phrases such as we judge, we assess, and we estimate—and probabilistic terms such as probably and likely—to convey analytical assessments and judgments. Such statements are not facts, proof, or knowledge. These assessments and judgments generally are based on collected information, which often is incomplete or fragmentary. Some assessments are built on previous judgments. In all cases, assessments and judgments are not intended to imply that we have "proof" that shows something to be a fact or that definitively links two items or issues.

In addition to conveying judgments rather than certainty, our estimative language also often conveys 1) our assessed likelihood or probability of an event; and 2) the level of confidence we ascribe to the judgment.

Estimates of Likelihood. Because analytical judgments are not certain, we use probabilistic language to reflect the Community's estimates of the likelihood of developments or events. Terms such as probably, likely, very likely, or almost certainly indicate a greater than even chance. The terms unlikely and remote indicate a less than even chance that an event will occur; they do not imply that an event will not occur. Terms such as might or may reflect situations in which we are unable to assess the likelihood, generally because relevant information is unavailable, sketchy, or fragmented. Terms such as we cannot dismiss, we cannot rule out, or we cannot discount reflect an unlikely, improbable, or remote event whose consequences are such that it warrants mentioning. The chart provides a rough idea of the relationship of some of these terms to each other.



Confidence in Assessments. Our assessments and estimates are supported by information that varies in scope, quality, and sourcing. Consequently, we ascribe high, moderate, or low levels of confidence to our assessments, as follows:
High confidence generally means good quality of information, evidence from multiple collection capabilities, and possible to make a clear judgment. A "high confidence" judgment is not a fact or a certainty, however, and such judgments still carry a risk of being wrong.

Moderate confidence generally means evidence is open to several interpretations or is credible and plausible but lacks correlation.
Low confidence generally means the assessment is based on fragmentary information, or from collection capabilities of dubious reliability.

Sources

[i] Information Sharing and Analysis Organization (ISAO); Trustworthy Accountability Group; retrieved 2 June 2023, https://www.tagtoday.net/threat-sharing#malvertisingtaxonomy (source reliability – N/A)

[ii] Cybersecurity vendor; Splunk; Phishing Scams & Attacks: What To Expect in 2023; retrieved 31 May 2023; https://www.splunk.com/en_us/blog/learn/phishing-scams-attacks.html; (source reliability – medium)

[iii] U.S. government; Federal Bureau of Investigation; Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users; retrieved 30 May 2023; https://www.ic3.gov/Media/Y2022/PSA221221 (source reliability – high)

[iv] Subject matter expert; Jérôme Segura, Sr. Director of Threat Intelligence at Malwarebytes; LinkedIn post: Some of the same threat actors buying ads on Google are also active on Bing [screen capture of search results]; retrieved 31 May 2023, https://www.linkedin.com/posts/jeromesegura_malvertising-searchengines-download-activity-7067988072218439680-3F_e?utm_source=share&utm_medium=member_desktop (source reliability – high)

[v] Technology-focused news and opinion; Tech Monitor; Malvertising On Google Ads is A Growing Problem That isn't Going Away; retrieved 40 May 2023; https://techmonitor.ai/technology/cybersecurity/malvertising-google-ads-malware (source reliability – medium)

[vi] Cybersecurity-focused news and opinion; GBHackers on Security; Malicious ChatGPT Chrome Extension Steal Facebook Accounts; retrieved 30 May 2023; https://gbhackers.com/malicious-chatgpt-chrome-extension/ (source reliability – medium)

[vii] Cybersecurity vendor; Confiant; FizzCore: A Growing Threat to Publishers' Revenue and Audiences; retrieved 30 May 2023; https://www.confiant.com/news/fizzcore-threat-actors (source reliability – medium)

[viii] Information Sharing and Analysis Organization (ISAO); Trustworthy Accountability Group (TAG) Malvertising Threat Exchange (MTX) proprietary data from 1 January 2022 – 26 May 2023; retrieved 29 May 2023 (source reliability – high)

[ix] Academic research; Department of Political Science, University of Michigan; Communicating Cybersecurity: Citizen Risk Perception of Cyber Threats; retrieved 30 May 2023; http://www-personal.umich.edu/~nadiya/communicatingcybersecurity.pdf (source reliability – high)

[x] U.S. government; National Institute of Standards and Technology (NIST); SP 800-50 Building an Information Technology Security Awareness and Training Program; retrieved 30 May 2023; https://csrc.nist.gov/publications/detail/sp/800-50/final (source reliability – N/A)

[xi] U.S. Federally funded research and development centers; MITRE; MITRE ATT&CK framework v13; retrieved 30 May 2023; https://attack.mitre.org/techniques/T1583/008/ (source reliability – N/A)

[xii] Market analysis vendor; Insider Intelligence; Worldwide Ad Spending Update 2023; retrieved 5 June 2023; https://www.insiderintelligence.com/content/worldwide-ad-spending-update-2023 (source reliability – medium)

[xiii] Intergovernmental organization; Organisation for Economic Co-operation and Development (OECD); Competition in digital advertising markets; retrieved 31 May 2023; http://www.oecd.org/daf/competition/competition-in-digital-advertising-markets-2020.pdf (source reliability – high)

[xiv] Advertising Agency; Dentsu; Global Ad Spend Forecasts May 2023; retrieved 6 June 2023; https://insight.dentsu.com/ad-spend-may-2023/#block-6a5fa256-de43-4b20-ab74-816c798efb48 (source reliability – medium)

[xv] General news; New York Times; Why Are You Seeing So Many Bad Digital Ads Now?; retrieved 30 May 2023 https://www.nytimes.com/2023/02/11/technology/bad-digital-ads.html#commentsContainer (source reliability – medium)

[xvi] U.S. government; Cybersecurity & Infrastructure Security Agency (CISA); COVID-19 Exploited by Malicious Cyber Actors; retrieved 30 May 2023; https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-099a (source reliability – high)

tagtoday.net