tag

JUL 2025

THREAT INTEL

DEMYSTIFYING THREAT INTELLIGENCE

IN DIGITAL ADVERTISING

INTRODUCTION

Digital advertising is a cornerstone of the global economy, driving substantial ad revenue across many industries e.g. telecommunications, retail, etc. In 2024, US ad revenue climbed to $259 billion and global ad revenue topped $1 trillion for the first time.

Digital advertising plays a critical role in supporting the growth of businesses around the globe. However, as the value of digital advertising continue to rise, the industry becomes a bigger target for criminal elements. Malicious actors are increasingly targeting companies across the digital advertising ecosystem – employing a variety of sophisticated tactics to exploit vulnerabilities to harm end users and steal valuable advertising revenue.

Since 2017, the TAG AdSec Threat Exchange has addressed this evolving threat landscape by:

- facilitating the strategic use of threat intelligence to safeguard the integrity of digital advertising, and
- collectively combating criminal threats to our global industry.

To effectively combat these risks, it is essential to understand the principles of threat intelligence, and how it can be applied specifically within the context of digital advertising.

WHAT IS THREAT INTELLIGENCE?

Threat intelligence is knowledge gained through the collection and analysis of data related to potential or active threats. At its core, threat intelligence provides actionable insights into the threat landscape, helping organizations understand the risks they face and take proactive steps to defend against them.

Threat intelligence can generally be described as falling into one of three categories[1], each offering different insights and value to organizations:

Tactical Intelligence
Tactical intelligence is the most immediate and actionable form of threat intelligence. It includes specific details related to current or emerging threats, such as malicious IP addresses, URLs, file hashes, or malware samples. By identifying these “Indicators of Compromise” (IOCs), organizations can quickly block or mitigate threats in real-time.

Operational Intelligence
Operational intelligence provides a more detailed understanding of threat campaigns and attack methodologies. It includes information about how cybercriminals execute their attacks, the tools and infrastructure they use, and their targeting behaviors.

Strategic Intelligence
Strategic intelligence is higher-level information on threat trends and motivations. This type of intelligence allows decision-makers to make strategic security investments.

Organizations typically benefit from all three types of intelligence, which together describe and enable both short-term and long-term. This intelligence is obtained and processed through the cyclical threat intelligence lifecycle.

[1] https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence

Through the intelligence lifecycle, threat intelligence requirements determine what is collected, processed, and turned into actionable intelligence to be disseminated. Critically, there is a feedback loop from internal and external (e.g. service providers or law enforcement) intelligence requirements. This lifecycle helps ensure stakeholders adapt to evolving threats.

WHAT'S THE ROLE OF TAG'S ADSEC THREAT EXCHANGE

The digital advertising ecosystem is made up of several key players that work together to deliver online ads to consumers. At a basic level, brands and their advertising agencies create advertisements and pay to have them shown to users. Advertising technology companies connect advertisers with publishers seeking to increase revenue by displaying ads on their websites or apps. Each of these types of companies work together to deliver relevant ads to users online and each may be targeted by criminal elements looking to steal advertising revenue or harm users.

Since 2017, TAG has held the US Department of Homeland Security (DHS) designation as the Information Sharing and Analysis Organization (ISAO) for the digital advertising industry, making TAG the primary body facilitating the industry's threat-sharing operations.

TAG's AdSec Threat Exchange brings together leading digital advertising companies and security vendors to share intelligence regarding criminal threats to the digital advertising industry in three categories:

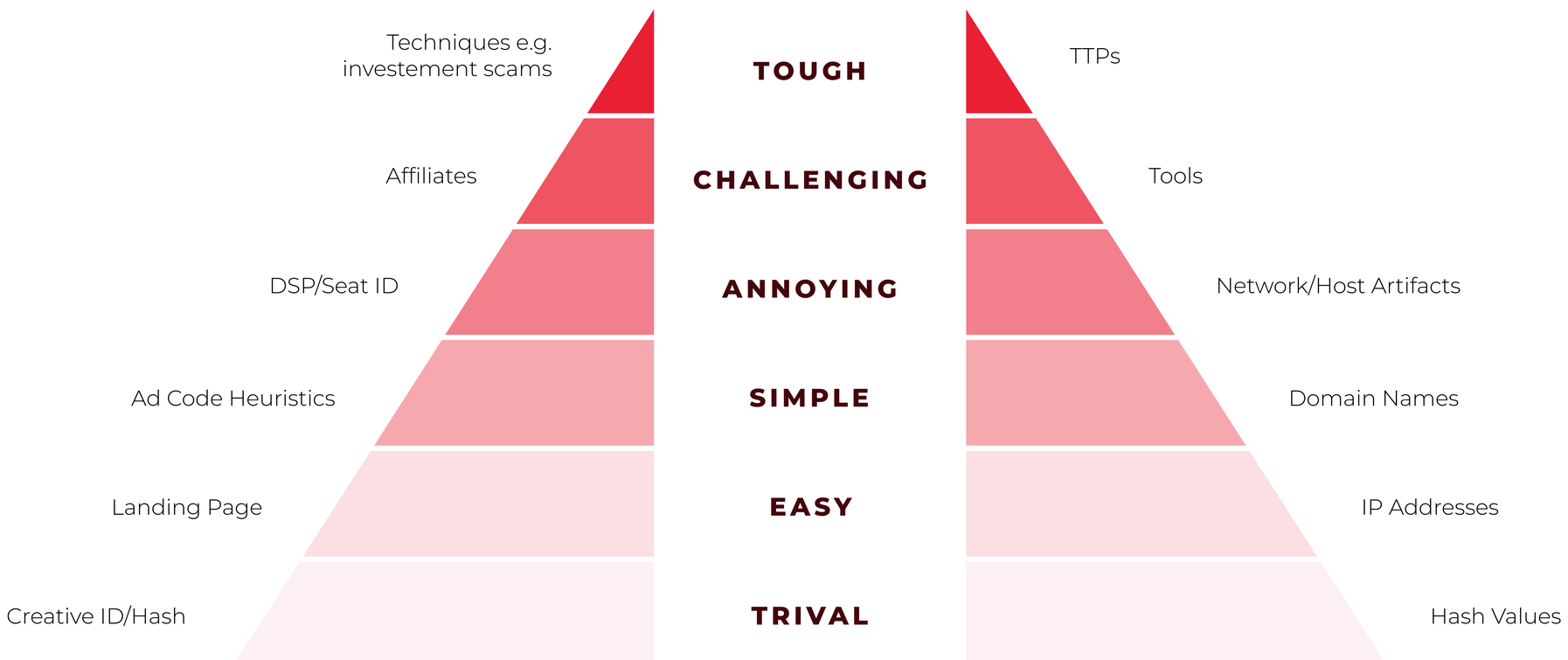
- Malicious advertising,
- Ad-funded piracy,
- Cybersecurity.

In this instance, we'll focus on operations aimed at combating malicious advertising, which take place within the AdSec Threat Exchange's "Malvertising Threat Exchange" (MTX).

WHAT IS MALVERTISING THREAT INTELLIGENCE?

Malicious advertising, or malvertising, is the exploitation of digital advertising campaigns, where bad actors misuse the digital advertising supply chain in ways that harm both businesses and consumers. TAG's MTX focuses on combating this type of threat through the real-time sharing of threat intelligence and coordinated take-down of malvertising threats. In 2024, the MTX grew to include practitioners from 11 countries spanning 7 time zones and providing 21.5 hours of human coverage in a typical day.

Pyramid of Pain



To understand how threat intelligence can be applied to malvertising, it's useful to use the "Pyramid of Pain" concept from traditional cybersecurity threat intelligence[2]. The pyramid separates intelligence into layers that are increasingly hard to gather as you go up the pyramid. However, the effort to gather the harder intelligence remains worthwhile as there is greater impact on an adversary, if you deny those things to them.

As an example, at the base of the pyramid is intelligence that is relatively easy for attackers to change if blocked by defenders, such as anti-virus software blocking the hash (i.e. fingerprint) of malware. At the top are the tactics, techniques, and procedures (TTPs) used in attacks and campaigns, which if mitigated by defenders, will force an adversary to come up with new tradecraft at great expense.

At the base level in the context of malvertising, unique advertisement identifiers – Creative IDs – may be shared quickly within the TAG Community to block malicious activity. However, these can be changed relatively quickly by an adversary. Intelligence on how adversaries operate, such as how they obtain advertising accounts and subsequently deliver malvertising, sits atop the Pyramid of Pain. This is because denying adversaries' methods has a much greater impact on their ability to conduct malicious activity.

Thus, the digital ad supply chain cooperates in the collection and sharing of threat intelligence, the ability to detect and respond to these threats improves significantly, ultimately helping to reduce the overall impact of malicious activity across the global advertising ecosystem.

[2] https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

CASE STUDY

METHBOT: THREAT INTEL IN ACTION

Case studies can provide a valuable insight to better understand the real-world application of threat intelligence in combating cyber threats in digital advertising. One such example is Methbot[3], one of the largest and most sophisticated ad fraud operations ever uncovered and brought to justice. The Methbot scheme was independently discovered in 2016 by multiple members of the TAG Community, who then worked with one another to develop a comprehensive picture of the threat at hand. Methbot targeted digital advertising networks and bypassed traditional fraud detection mechanisms to generate millions of dollars in fraudulent ad revenue.

Methbot was an advanced botnet operation that utilized fake traffic to simulate real user interactions with digital ads. The perpetrators behind Methbot set up a network of more than 250,000 bots running across a vast network of fake IP addresses that mimicked legitimate users on top-tier websites. These bots visited popular websites, watched video ads, and clicked on display ads, all while masking their real identities. As a result, the fraudsters earned fraudulent revenue by exploiting the systems of ad networks and publishers.

Some of the key pieces of intelligence that helped identify Methbot were anomalous traffic patterns and unusual IP address behavior. By analyzing the traffic patterns generated by the bots, security experts were able to fingerprint the fraudulent activity back to the botnet, despite its efforts to hide behind fake identities and other obfuscation tactics.

The scale and sophistication of Methbot made it a particularly challenging threat for digital advertisers and ad networks to detect. While multiple members of the TAG Community had independently conducted extensive analysis on Methbot, there was no industry-wide coordination in the investigative phase. Working together with what was then White Ops (now HUMAN), TAG organized an emergency briefing on the fraud operation, attended by more than 170 anti-fraud executives from leading companies across the industry. This enabled companies to understand, evaluate, and respond to this threat in near real time. Additionally, TAG expedited their review of the IP addresses found to be associated with Methbot and provided that comprehensive list to the TAG Community, and included those IP addresses in TAG's own Data Center IP List tool.

By leveraging threat intelligence tools and threat-sharing platforms, stakeholders were able to significantly reduce the financial damage caused by Methbot.

[3] https://www.justice.gov/usao-edny/pr/russian-cybercriminal-sentenced-10-years-prison-digital-advertising-fraud-scheme

CLOSING THOUGHTS

The Methbot case is a prime example of how effective the sharing of intelligence can be in identifying, analyzing, and responding to large-scale malvertising and ad fraud operations.

It is important the digital advertising industry comes together to share threat intelligence – their unique piece of the puzzle – in what can be a complex supply chain. This enables the industry to block threats in real-time and understand our adversaries better, allowing us to work with partners to make a meaningful impact such as: reducing user harm; significantly increasing the cost for adversaries to operate; or law enforcement action.

TAG is committed to be at the forefront of this fight against crime.

tagtoday.net