Profiling hackers using the Malvertising Attack Matrix by Confiant

blog.confiant.com/profiling-hackers-using-the-malvertising-attack-matrix-by-confiant-9341838887b7

taha aka lordx64 October 18, 2021

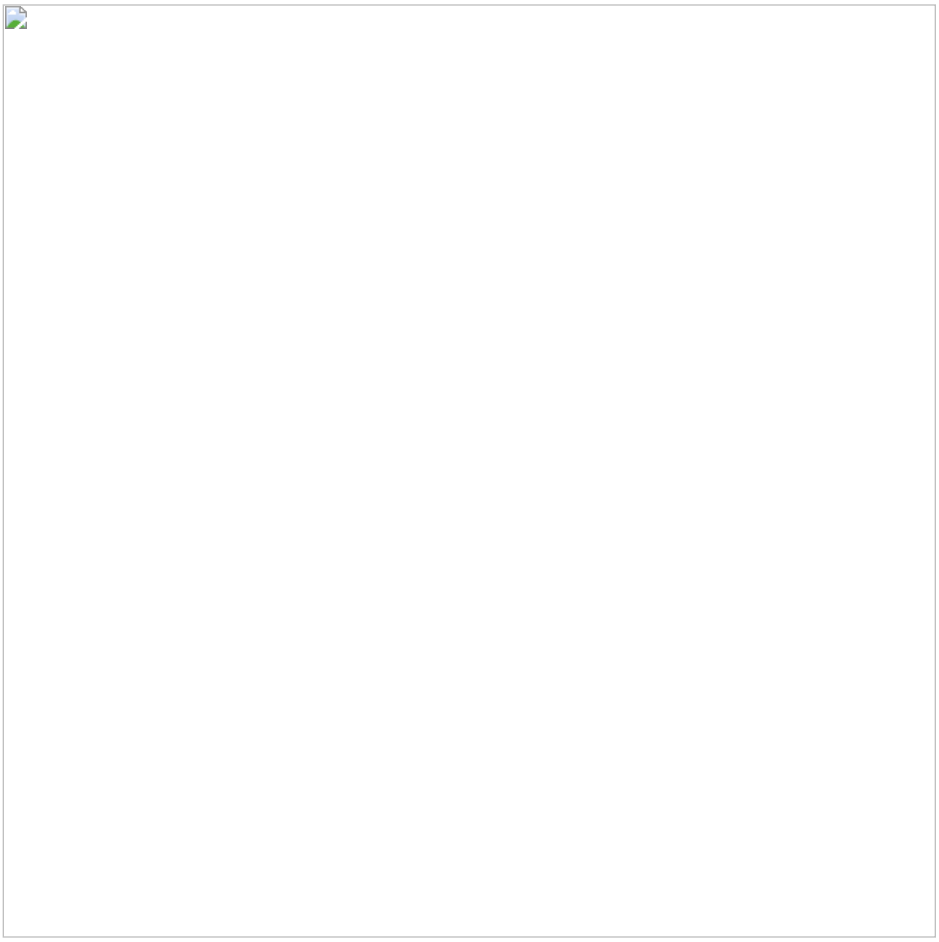


Photo by on

What is Malvertising?

A relatively new threat vector, Malvertising is a cyber-attack relying on ad networks and digital ads exposing virtually any internet user surfing the web to the risk of infection.

From my experience, if I have to compare with what we know from the cyber security world, I would define Malvertising as the following: Malvertising is a mixture of watering holes, exploit kits, web attacks and drive-by downloads all combined and run by now identifiable threat groups called Malvertisers.

Malvertisers rely heavily on the advertising ecosystem and its complexity to funnel their persistent and complex to detect cyber attacks.

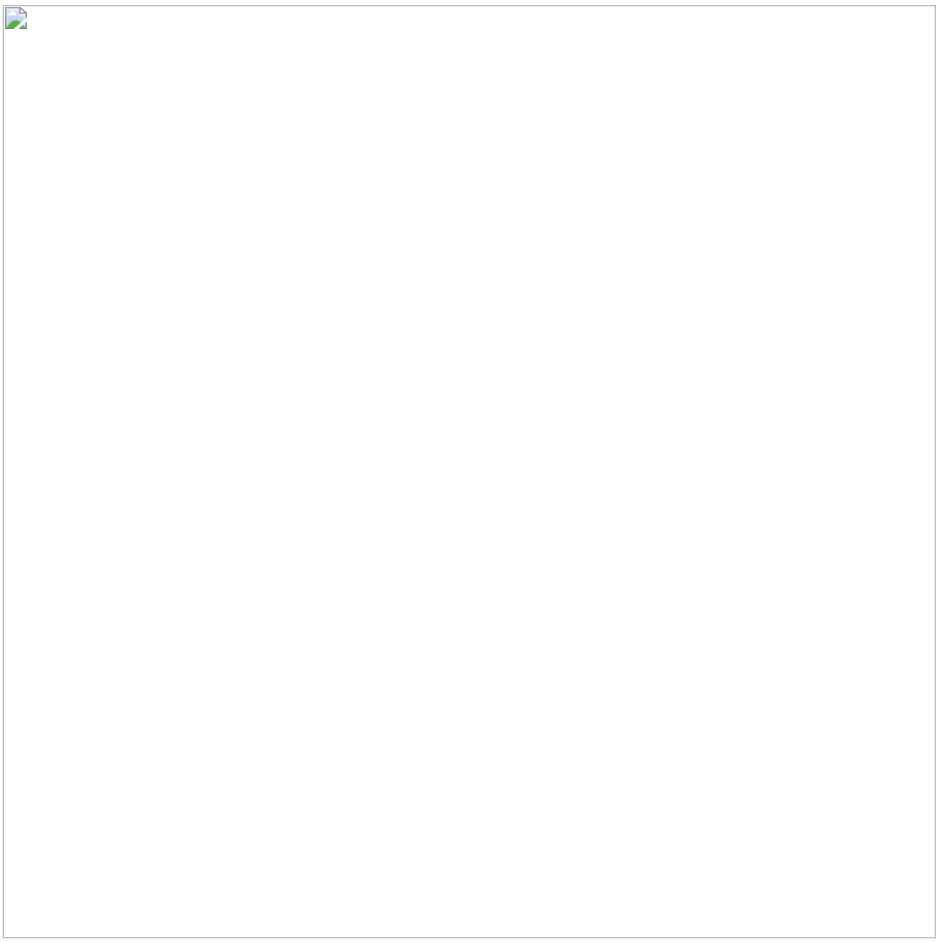
The Modus Operandi (MO) and Tactics, Techniques & Procedures (TTPs) that we tracked so far on different malicious actors within ad networks helped shape a new kill chain.

Malvertising Kill Chain:

Understanding the AD tech ecosystem:

Due to the nature of this new kill-chain and the complexity of the ad tech stack, it is essential to understand how ads are displayed on a web page.

Let's quickly explain one crucial piece from the ad tech world, called **real-time bidding** or RTB (or what is the process an ad go through before it is displayed)



Courtesy of Circus Street, taken from this video

> Note: The video link above is one of the best quick explanations I found so far, and if you are new to ad tech, I highly recommend you checking it out, or continue reading below.

Before an ad is displayed on the web page, it has to go first through a complex ad stack involving DSPs, ad exchanges, and SSPs define below:

- DSP: or demand-side platforms are used by the buyers, media agencies, or advertisers who have a demand for ad inventory. DSP holds information from the buy-side about criteria they need: targeted audience, maximum bid price, location, etc.
- SSP: or Supply-Side Platforms are used by the sellers, media owners who are supplying ad inventory. They hold a record of the inventory a media owner wants to sell: the different audience segments that visit the media owner site, the minimum price the media owner wants to sell for, etc.
- Ad Exchange: is the piece of technology that auctions off the ad inventory made available by the SSPs.

The whole process is buyers will be entered in if the inventory available matches the criteria in their DSP. The one with the maximum bid price will win the auction. The auction process starts when a user opens a web page with an ad unit on it, and the ad that wins the auction appears at the same time that the rest of the page loads.

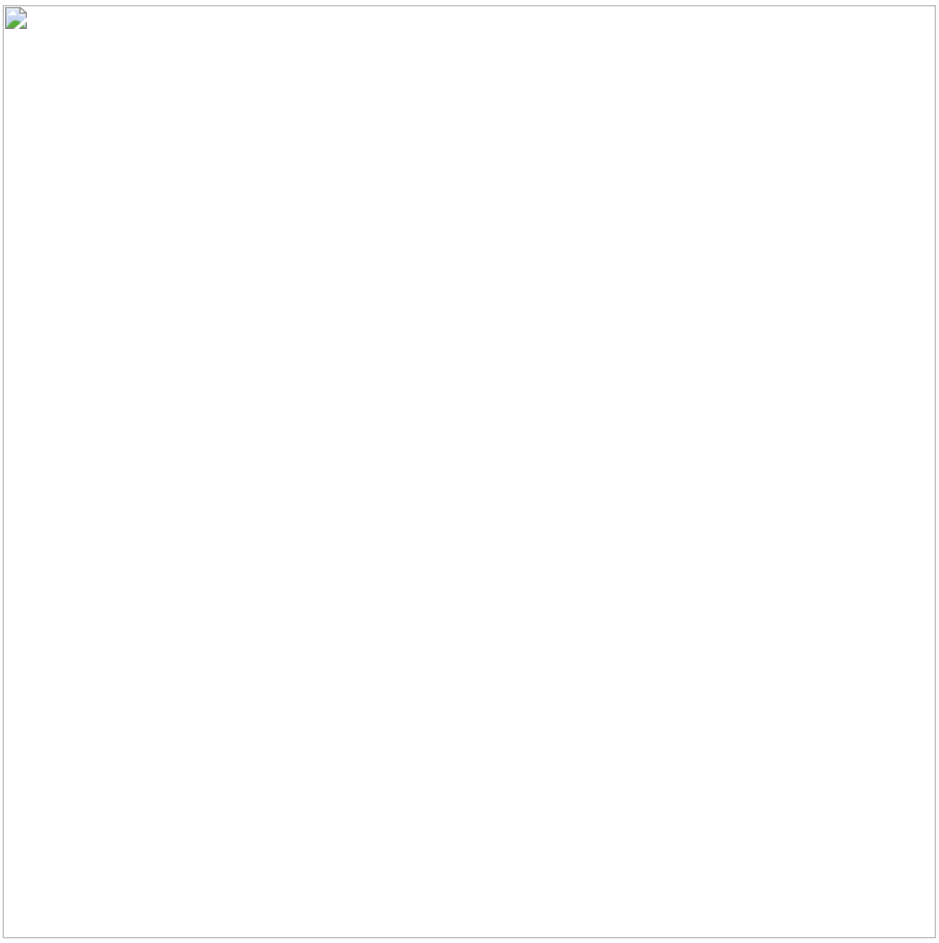
This whole process is what we call RTB, and all this complex process takes a **fraction of a second to execute.**

Advertisers and Publishers are using the technologies above to transact billions of impressions daily.

Like any ecosystem that generates billions of impressions, it will be subject to hacking and cyber-attacks. Threat actors infiltrated this ad ecosystem and turned it to their advantage.

As we will see in the Kill Chain below, threat actors could be present at different steps of this RTB process.

Malvertising Kill Chain:



Malvertising Kill Chain

A typical Malvertising Kill Chain is a sequence of the following phases:

- Initial Access is the first step where the Malvertisers enters the Advertising ecosystem. Usually Malvertisers access the ad ecosystem by creating fake agencies for the purpose of establishing relationships with ad buying platforms (DSPs) or by creating fake ad creatives.
- A tactic used by Malvertisers to execute malicious code typically via forceful redirects.
- : the step where Malvertisers persist within the ad ecosystem, ensuring their campaigns can last the longest time possible while evading detection mechanisms.
- : A tactic where Malvertisers implement specific fingerprints and techniques that helps them define whether or not to cloak a landing page, which is the rendering/reveal of the final landing page
- : After several redirect chains, visitors end up on a final page, the landing page. Typically a landing page is the Malvertisers final “payload” and comes in different forms and purposes ranging from Drive-by downloads, Exploit kits, or investment scams, etc.

Due to the sophistication of Malvertising cyber attacks and their deceptive nature, we have seen attackers using more tactics, not in a specific order, at different phases of this Kill Chain multiple times:

- , and can be used before and/or after the orthe phase.
- Attackers can have multiple with some/all of them using the tactic.

Theis another tactic that we added to help Enterprise assess the risks of such attacks and understand whether they are of a destructive nature, causing a denial of service, hijacking resources, or causing a financial loss.

Therefore, we extended this model from five sequential phases to nine tactics to represent it within a matrix.

Malvertising Attack Matrix

The Malvertising Attack Matrix is derived from the MITRE ATT&CK Framework representation. Multiple techniques can be employed to accomplish the same tactic, depending on the attacker’s main objective. however, not all nine tactics need to be employed.

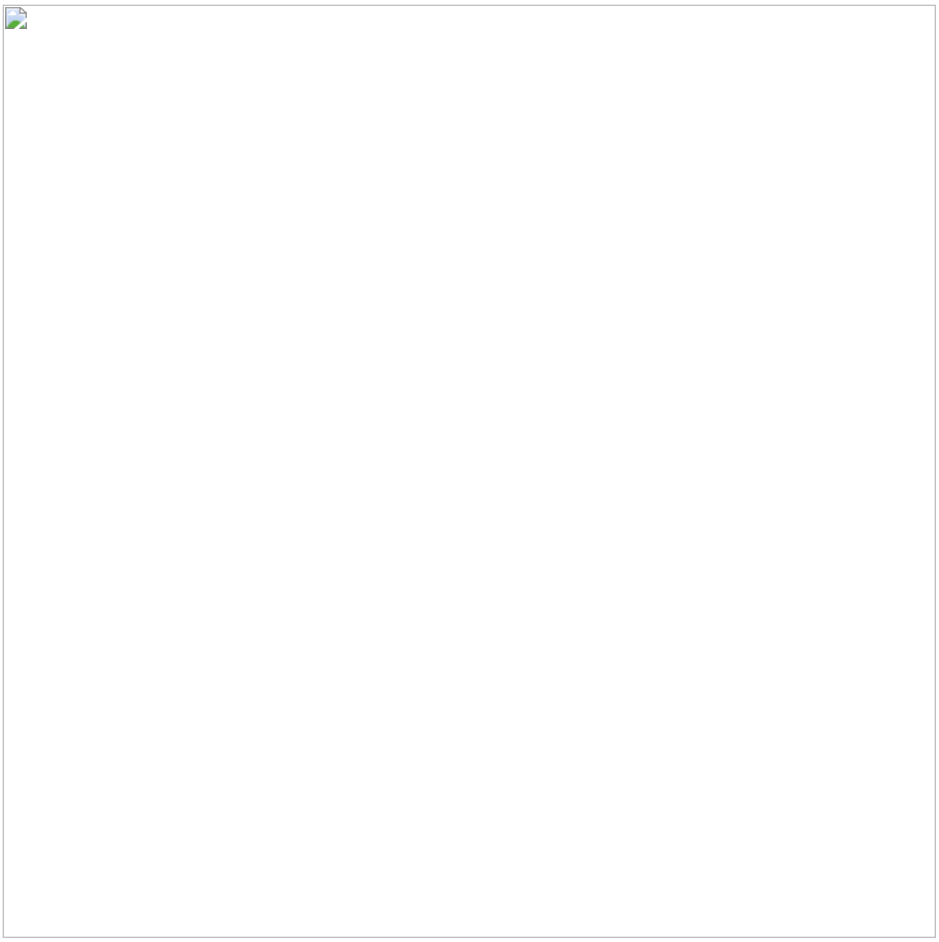
This representation has the advantage of aggregating the techniques used in previous attacks by documenting techniques, tactics and tools used. This aggregation is known as behavior profile.

Based on the behaviors we identified, the Confiant security team has identified multiple threat actors like Zirconium, eGobbler, FizzCore, ScamClub, DCCBoost, Tag Barnakle, or YoSec along with multiple UNC groups with clusters of activity tied to Malvertising.

Malvertising threat actors' profiles can now be identified and tracked via the Malvertising Attack Matrix, see below.

How to

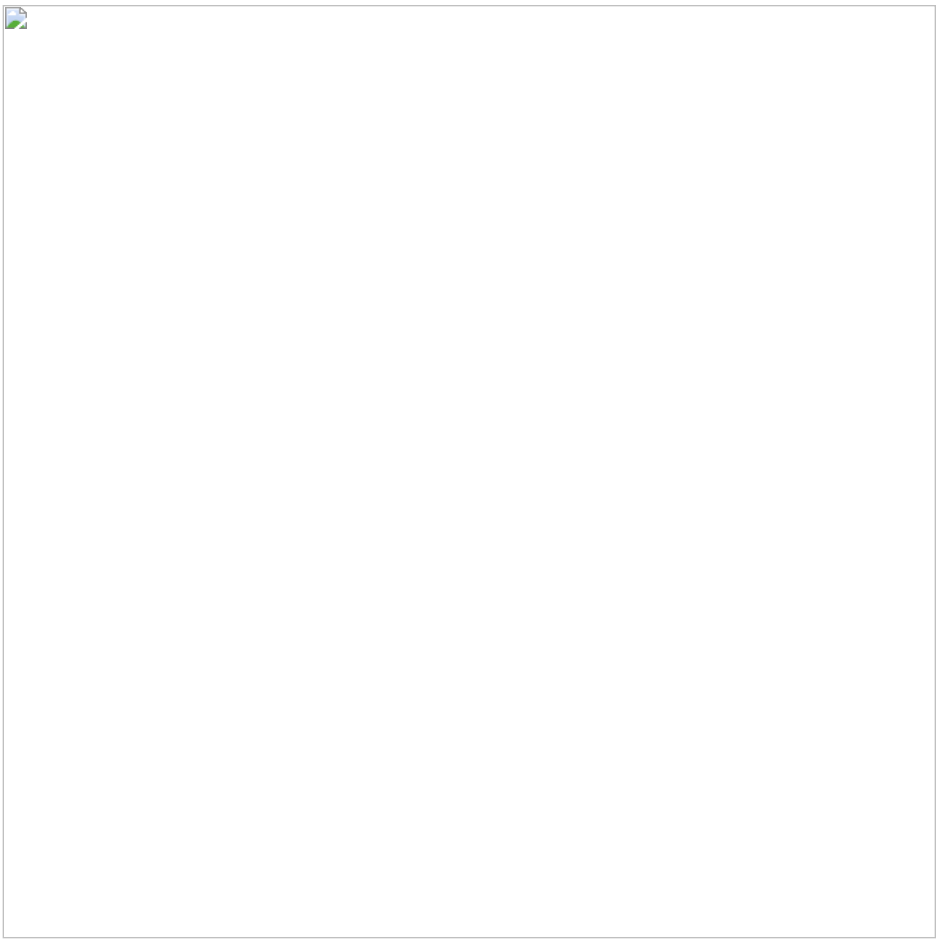
We built a website specifically for the Malvertising Attack Matrix that can be found at this URL: https://matrix.confiant.com



Malvertising Attack Matrix defined by Confiant

Along with the matrix, we have different behavior profiles aka Threat actors, that we identified and added their profiles to this Matrix. By selecting a threat actor profile, the matrix will show the associated Tactics and Techniques.

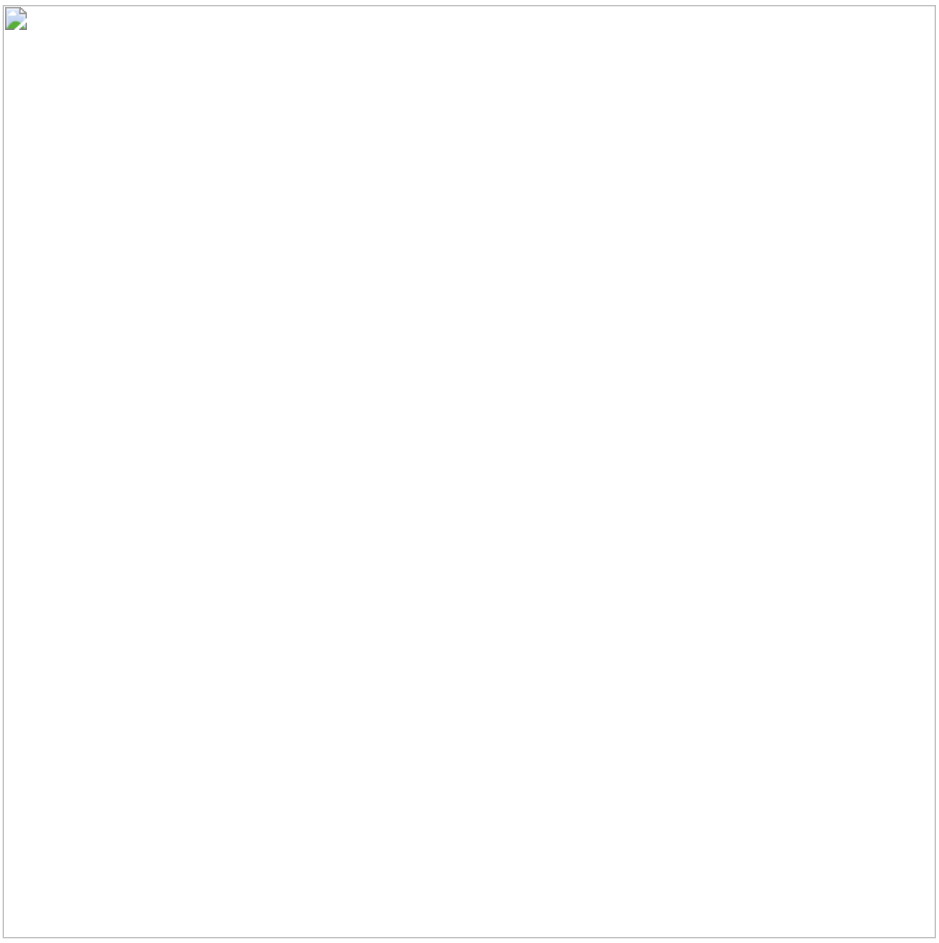
For example, this how the threat profile of Zirconium looks like:



Zirconium threat profile

Following the same standards as the MITRE ATT&CK framework, each of the 70+ techniques of the Malvertising Attack Matrix has a page that includes a brief summary of the adversarial technique, procedure examples, and references.

Example of **[C401]**Technique of the **[C400]** Tactic:



[C400] Browser Exploitation | [C401] By-pass Popup Blocker

Notations and Identifiers

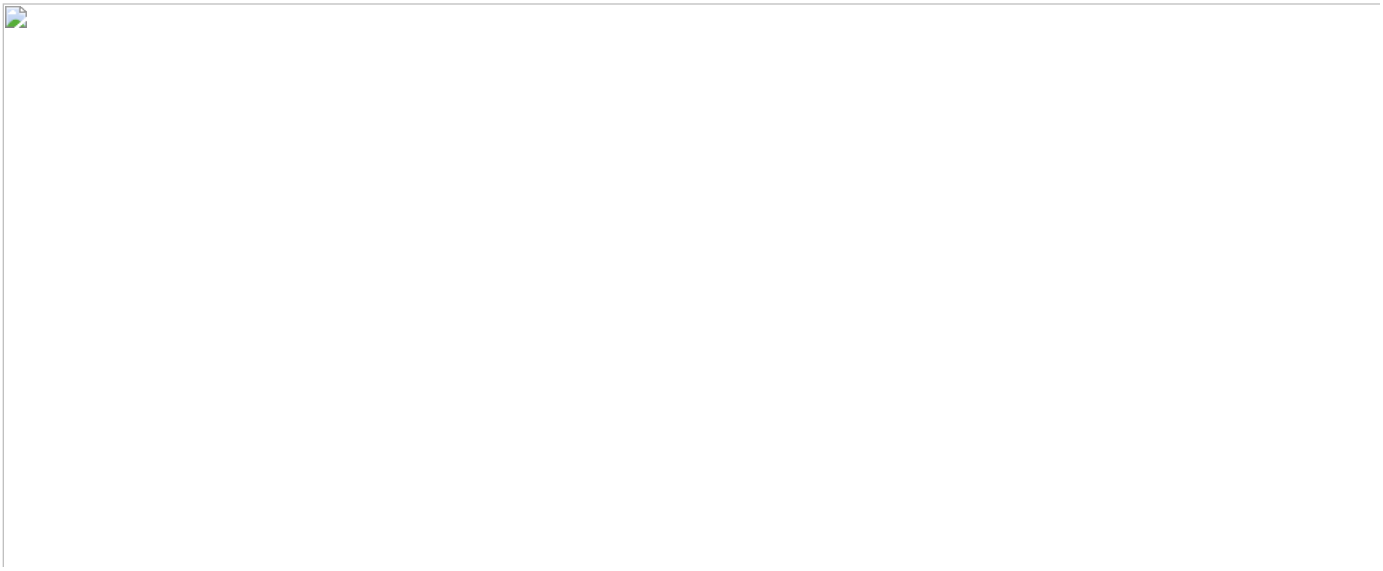
Each tactic and technique have an ID. This ID is used in the contextualized information present in our STIX v2.1 feeds at different places:

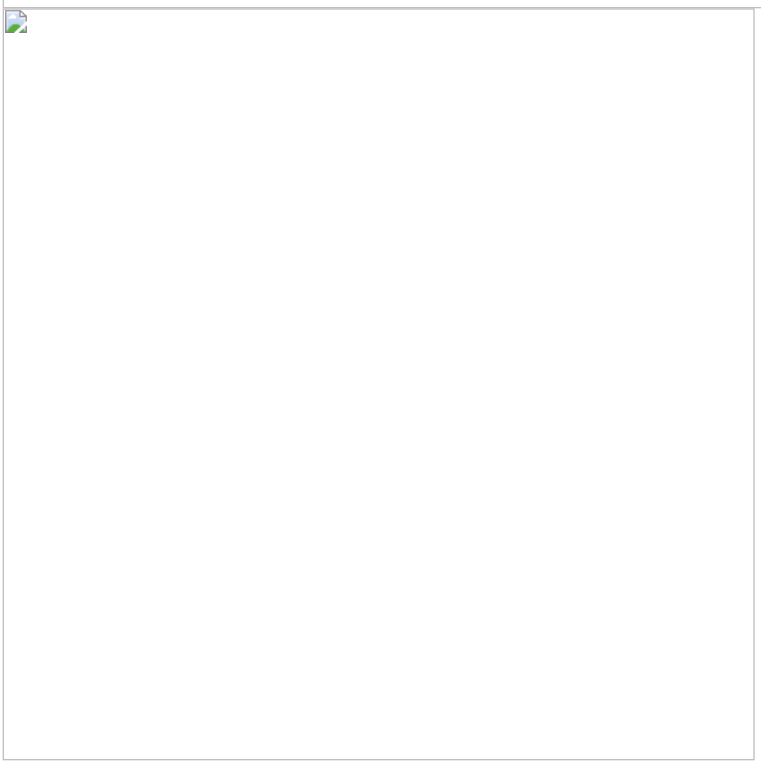
- We use this ID in the field of a STIX V2.1 as following:
- We use this ID to access the webpages referenced in the STIX V2.1 field of a STIX v2.1 , following this format:

Example

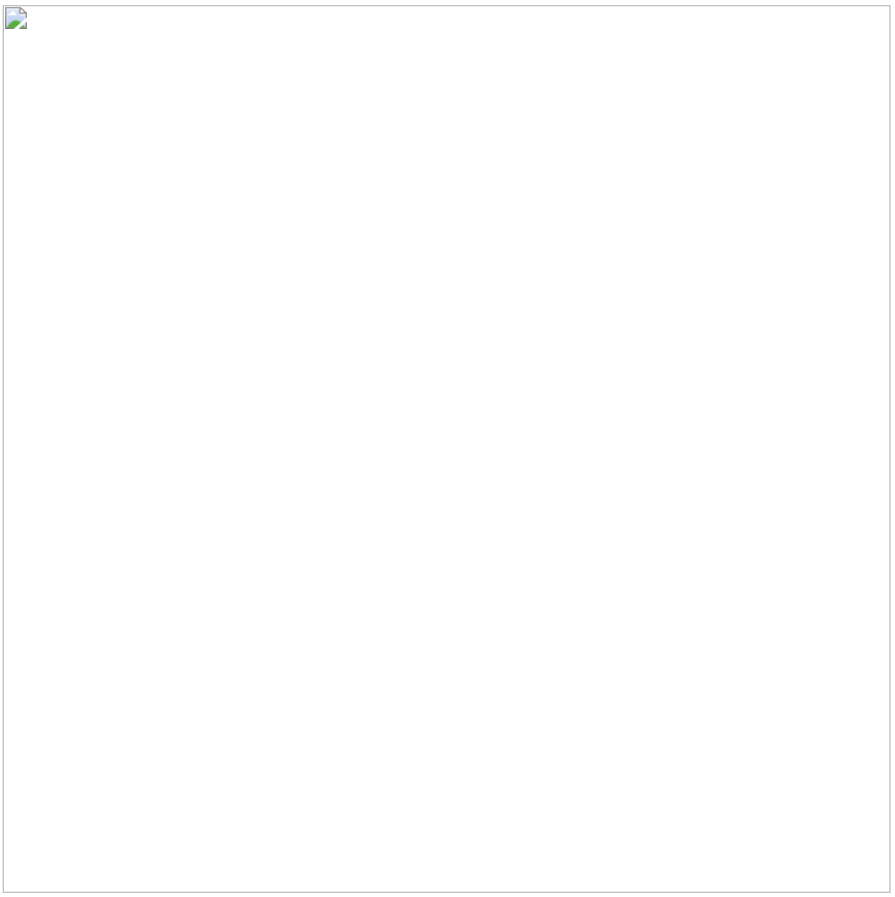
Below is our malvertising feed, representing a campaign (TI 950451017) we detected from a threat actor dubbed BRS.

We can see we have three Attack-patterns with references to the matrix for additional information, enabling threat intelligence to understand every attack and its full context:





STIXv2.1 Feed visualization of a BRS campaign TI 9504510174



Every Attack-Pattern STIX v2.1 object has an External Reference field, holding a link to its definition in the Malvertising Attack Matrix.

> Note: To receive these Threat intelligence feeds, our TAXII server is hosted at **taxii.confiant.com.**
>
> Please reach out to us to access to our malvertising feeds at the following email : **security@confiant.com**

Final Notes

Is Malvertising low risk?

Malvertising is interchangeably used with Adware. Many security companies historically have classified Adware as low priority, low risk.

This is mainly due to PUA/PUP software that caused little to no harm to infected computers in the past.

But the truth is things have changed now, and threat actors see Malvertising as a potential new attack vector and foothold into Enterprise networks, who do not really include Malvertising into their threat model.

Adware has evolved since, and it is now weaponized with backdoors, along with Malware, helping attackers establishing a foothold within Enterprise networks.

Our Objective

The objective of the Malvertising Attack Matrix isn't just profiling threat actors using different techniques and tactics.

It is also a tool helping Enterprise security teams taking into account Malvertising hopefully incorporate it into their threat model. This matrix will hopefully provide enough knowledge to understand Malvertising and the risks encountered by Enterprises when targeted.

Finally, this matrix is a way to communicate actionable threat intelligence to entities that are outside of the ad tech world and we will extensively use it going forward in our reporting.