Uncovering 2017’s Largest Malvertising Operation

blog.confiant.com/uncovering-2017s-largest-malvertising-operation-b84cd38d6b85

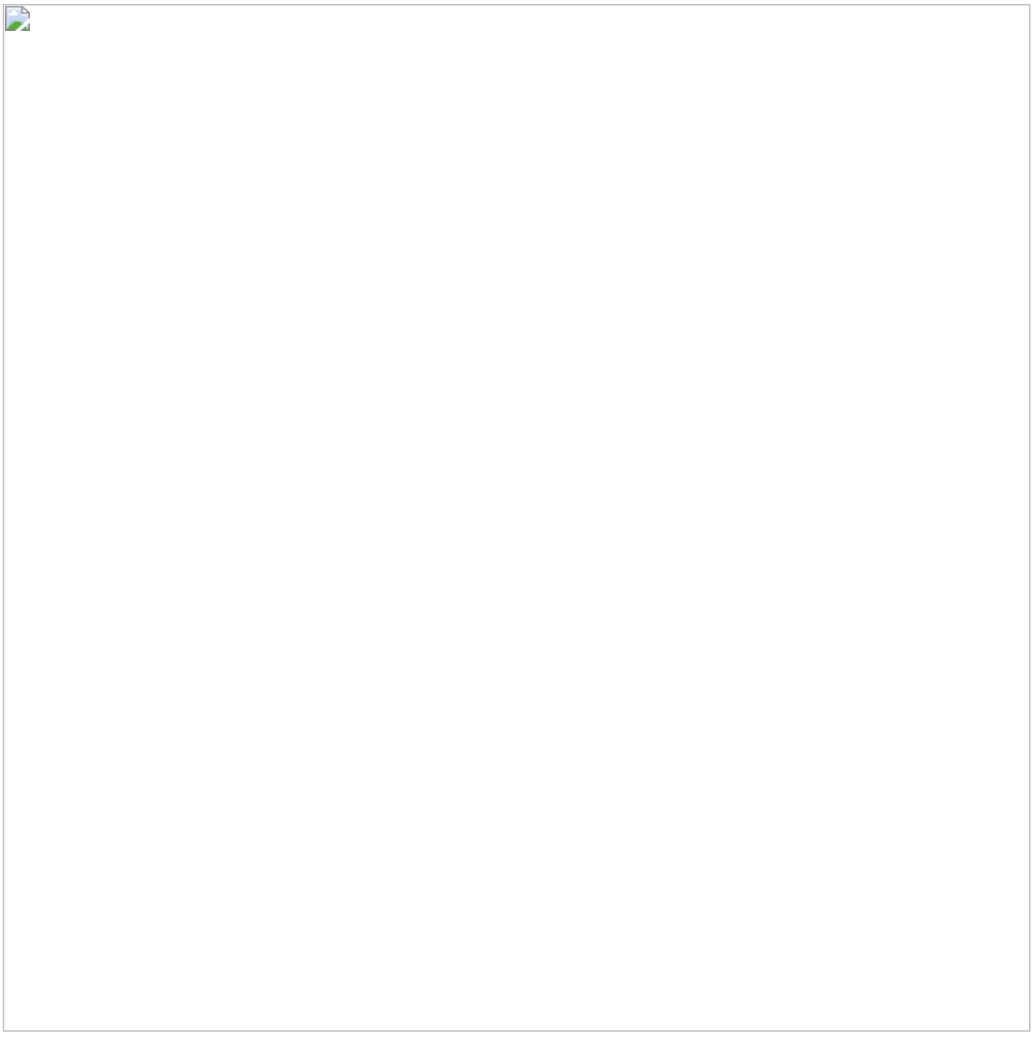
Jerome Dangu January 25, 2018

Jerome Dangu
Follow
Jan 23, 2018

.

10 min read

The Zirconium group successfully created and operated 28 fake ad agencies to distribute malvertising campaigns through 2017, buying an estimate of 1 billion ad views throughout the year, and reaching 62% of ad-monetized websites on a weekly basis.



Forced redirects

Through 2016 and 2017, the prevalence of exploit kits in online advertising has decreased, as browsers became more secure. A few drivers explain this evolution:

- The standardization of browser sandboxes (not only Chrome/Safari but now Firefox and Edge)

- The decline of Adobe Flash as a vector for exploit kits, accelerated by the ban of Flash ads in Google Chrome from September 2015
- The high profile demise of Angler Exploit Kit in June 2016
- The rise of exploit detection and sophisticated telemetry that uncovers attacks in spite of evasion

As a consequence, many malvertising campaigns moved to “forced redirects” as the second best attack vector. A forced redirect is when a person is surfing the web on a computer or mobile device and through no action of their own gets redirected to a different website. Usually the website they are redirected to is a vehicle for some form of affiliate fraud or malware.

Although forced redirects require social engineering (tricking users into falling for a scam or infecting their computer), they can durably stay under the radar by avoiding to trigger in situations that may correspond to security investigations.

Execution and chain of redirection

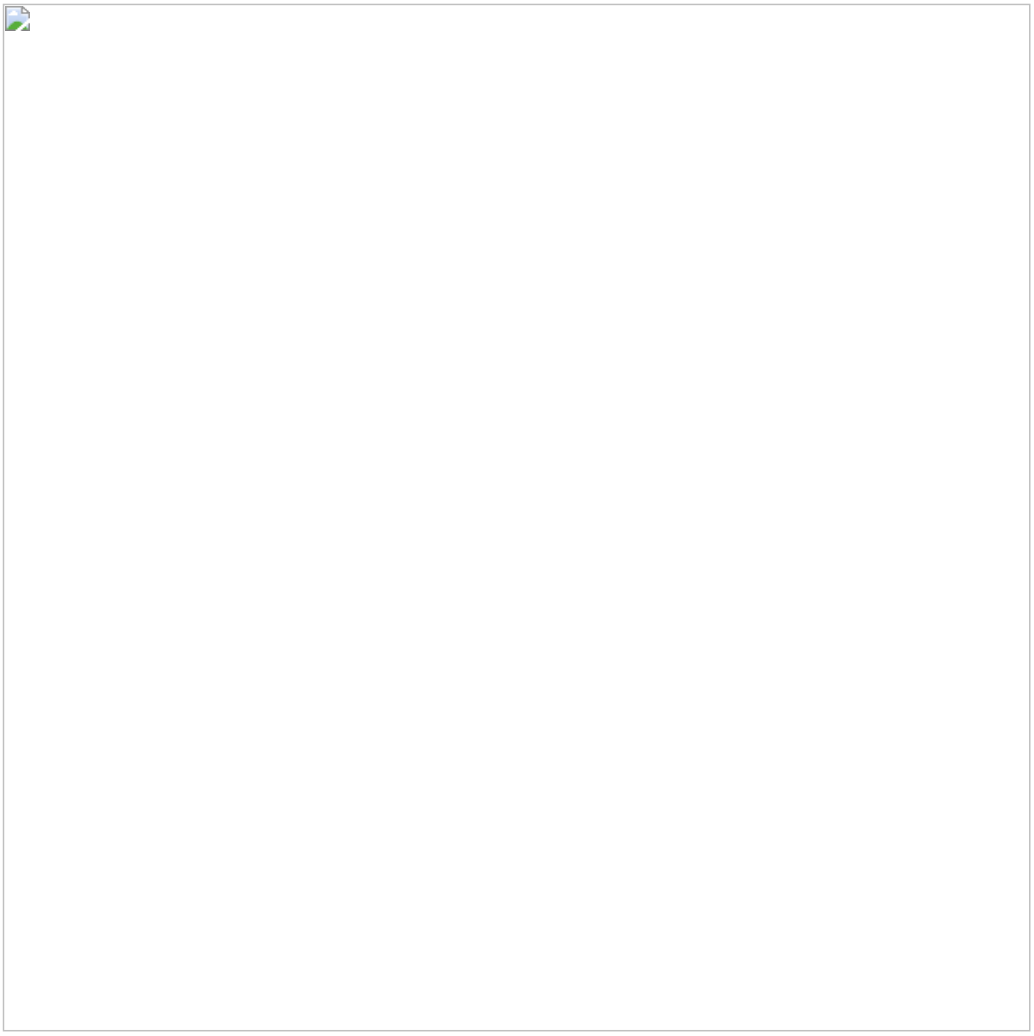


Fig. 1: Redirection flow

Beginads was only briefly used to establish relationships with ad platforms as a fake ad agency. Confiant observed it as a stand-alone ad server in March 2017, but it later became the domain that acts as the TDS (Traffic Direction System) on behalf of all the campaigns running on all the fake agencies’ ad servers.

Zirconium established a well thought-out organization to maximize both Supply (user traffic) and Demand (landing pages).

Supply is brought in by the fake agencies, establishing relationships with legitimate ad platforms, and buying traffic. Having multiple relationships makes the operation more robust (in case an agency gets caught) and stealthier — as each agency poses as a long-tail small business agency and buys small amounts at a time.

Aggregating Demand is the other key component to Zirconium’s business model. Confiant established that Zirconium does not operate these landing pages on their own. Instead, they resell the traffic to affiliate marketing platforms.

Maintaining those relationships at the agency level would have been cumbersome and inefficient. Beginads.com became the central gateway to manage the demand. Just like a legitimate advertising operation, this requires constant optimization and testing to yield the most revenue. Beginads.com became the centralized place were Zirconium could rationalize its revenue.

MyAdsBro, the not-fake ad network by Zirconium

Confiant found yet another level of redirection between Beginads / Horizon-media and the affiliate networks, going by the name “MyAdsBro” and operated by Zirconium.

Essentially, Zirconium’s own campaigns run via MyAdsBro but anyone can also push traffic to it and leave a revenue commission to them. MyAdsBro claims to pay out in crypto-currencies.

Going as far as to build a black-hat affiliate network shows the level of sophistication that they reached in their operations.

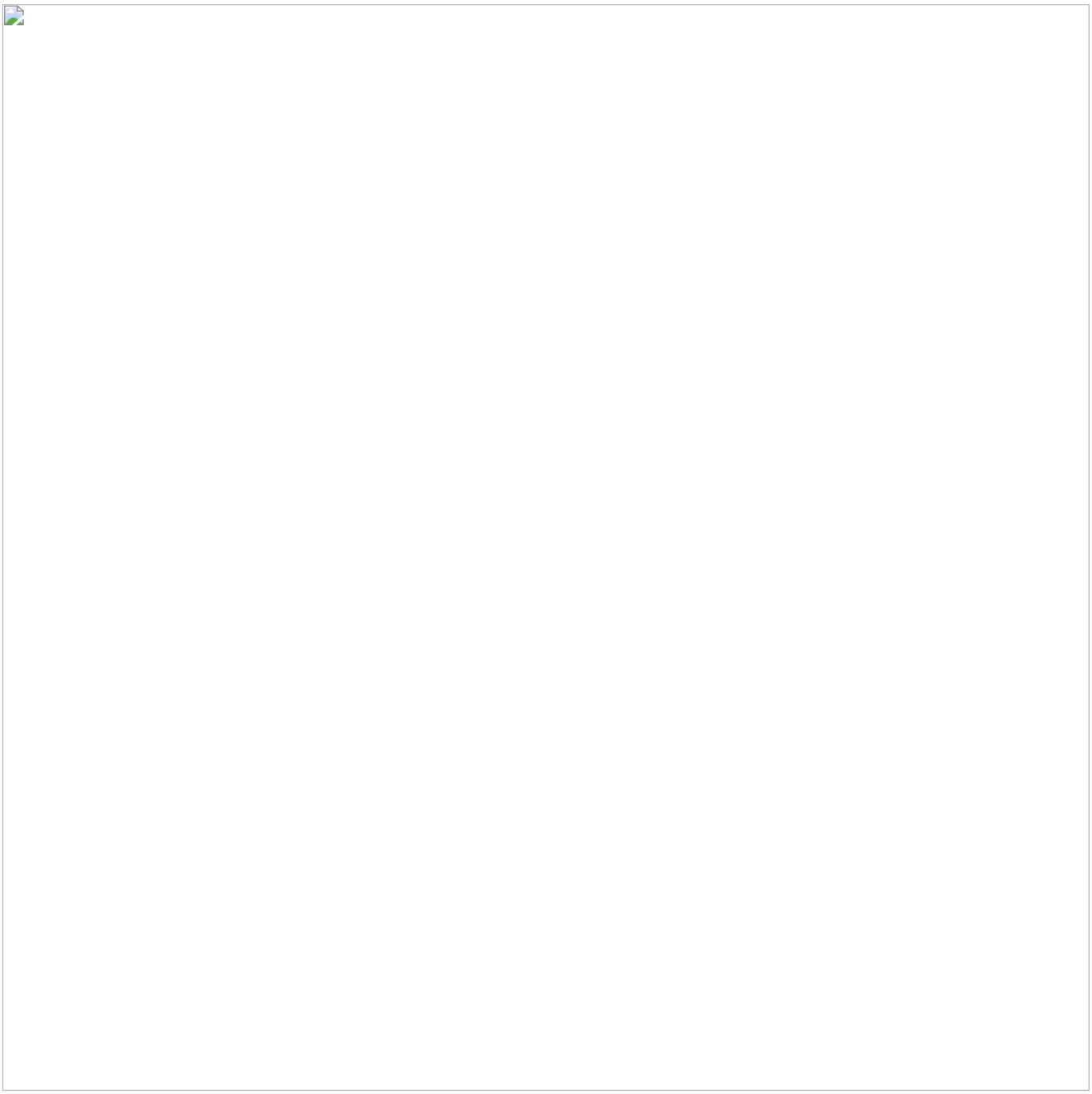


Fig. 1: MyAdsBro home page (left) and customer web panel (right)

Payloads

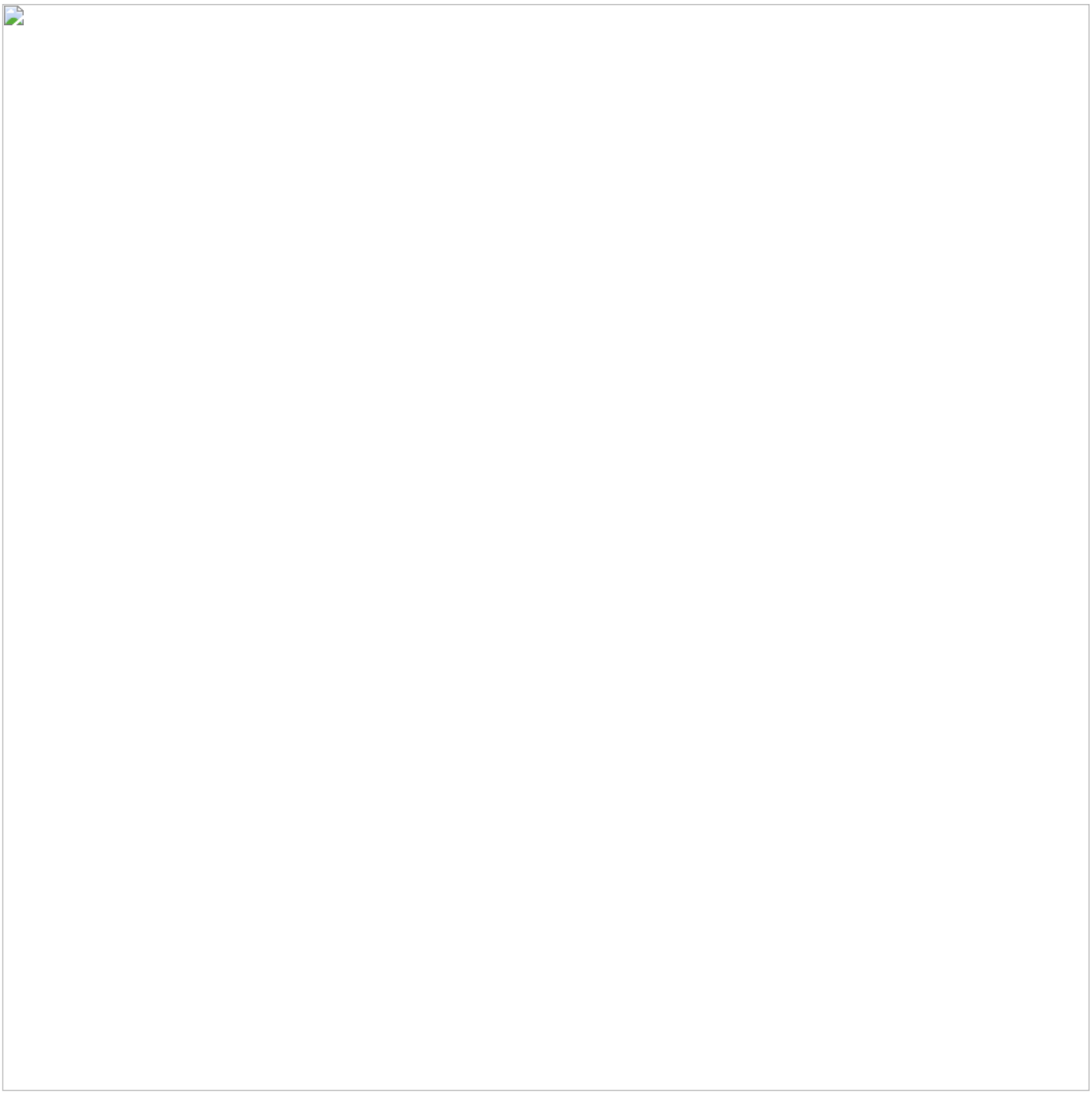
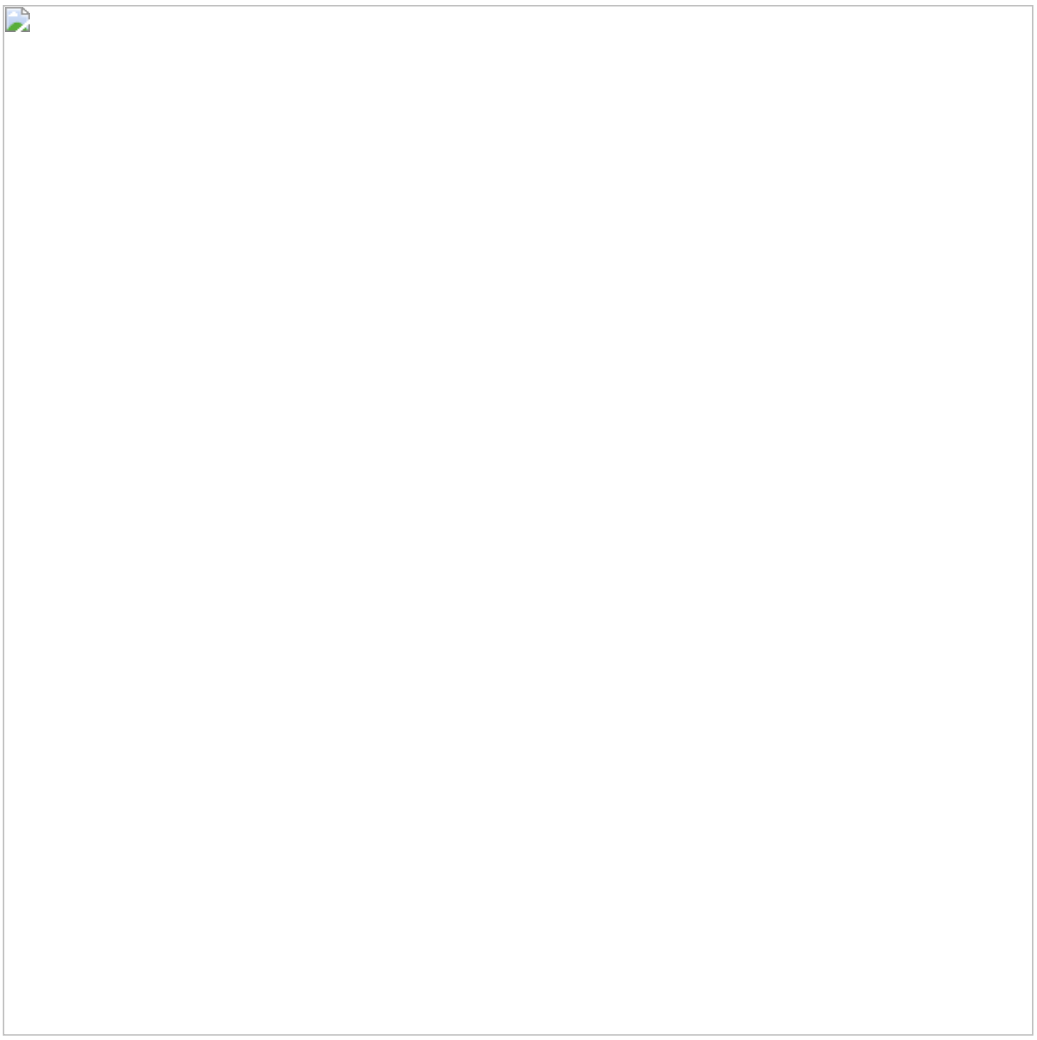


Fig. 2: Typical Fake flash update, as pushed by Zirconium on Mac (left) and Windows (right).



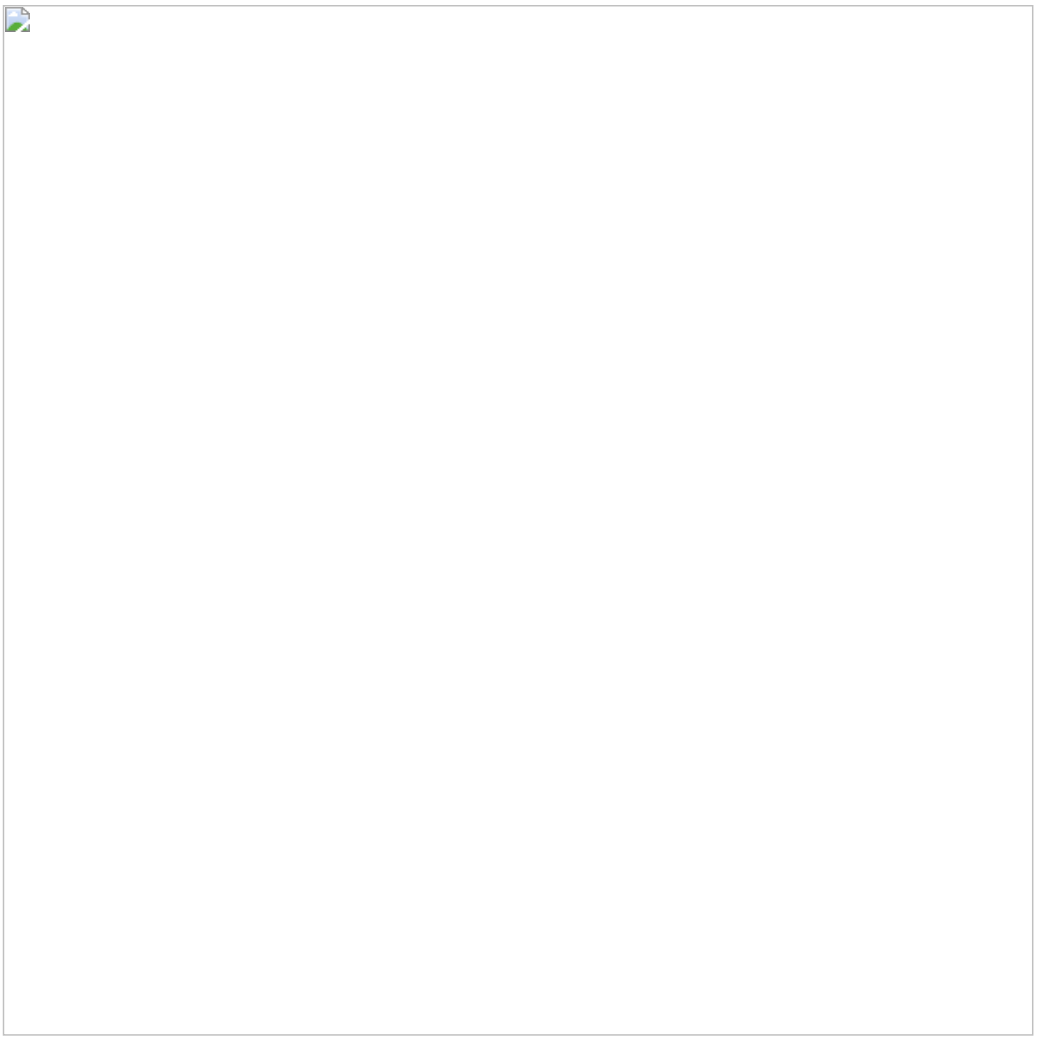


Fig. 3: Fake Antivirus on Mac

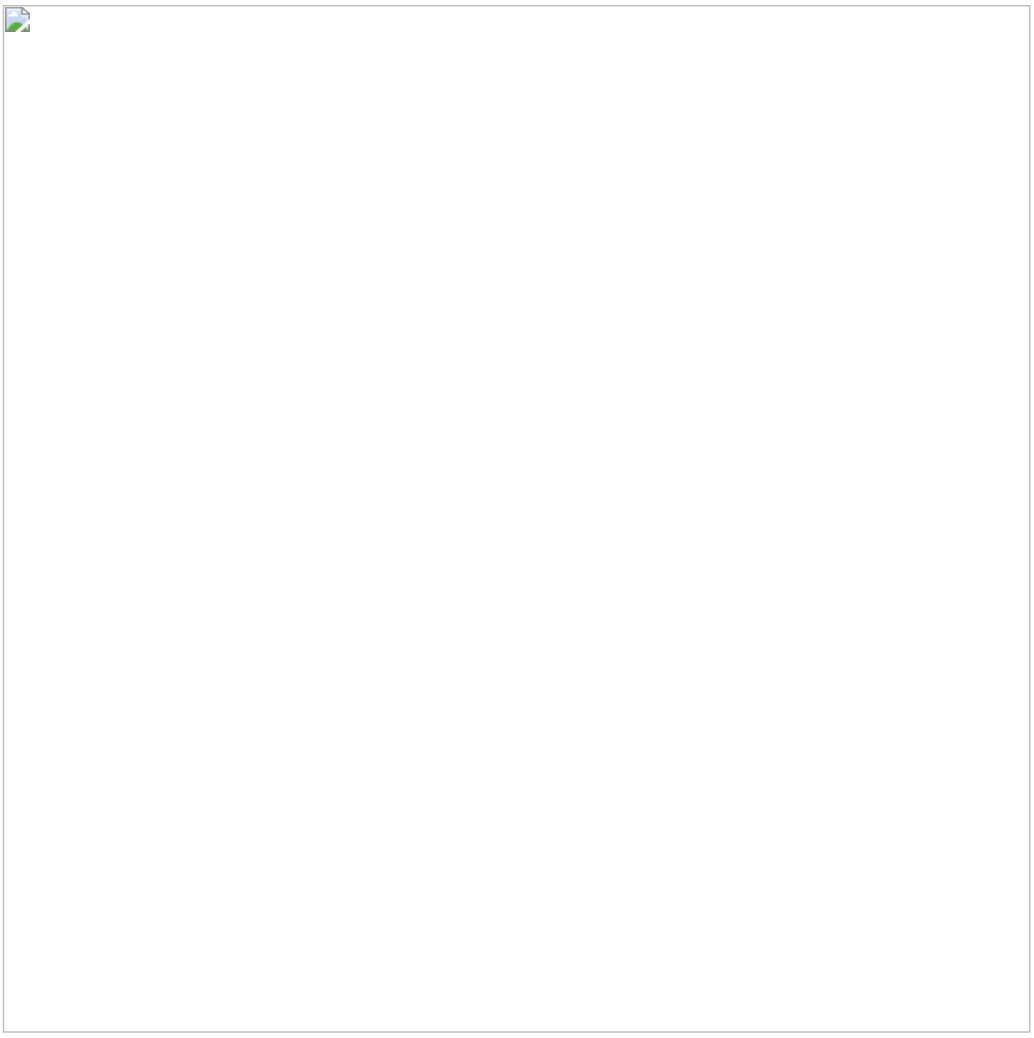


Fig.4: Tech support scam, as pushed by Zirconium. Note the now-classic .

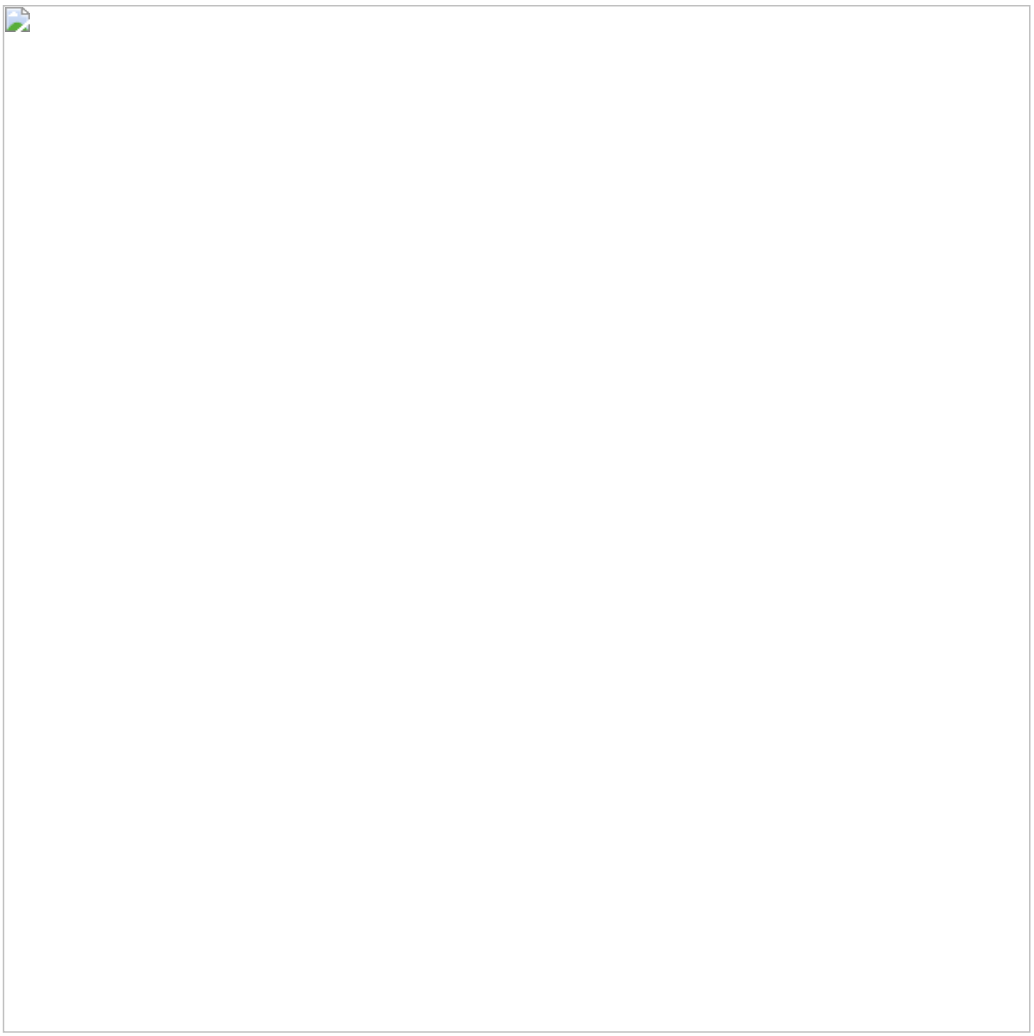


Fig. 5: Another scareware tech support scam via Zirconium's "beginads" TDS

Previous research by @ExecuteMalware identified Zirconium's *PlaiMedia* serving landing pages operated by the Kovter Group. Another large malvertising operation, Kovter has embraced social engineering schemes in recent years. [Edit Jan 24] After review and feedback from Kaffeine at ProofPoint, there is no evidence that ties Zirconium to Kovter.

ROI and Evasion

Just like any other business, malvertising is driven by return on investment. But crucially, it needs to operate behind sophisticated evasion techniques. This means that only a small portion of the acquired traffic actually delivers a payload. Using Confiant's telemetry, we estimate the group served in the order of 1 billion ad impressions through 2017.

Starting in October, the group became more aggressive at optimizing for ROI, at the risk of more overtly showing suspicious activity, by using "fingerprinting". Fingerprinting is the process of gathering data on the browser/device to target a subset of the audience. The goal is to evade detection, and this is typically done from within the browser in JavaScript. Attackers decrease their chances of delivering their payload to security scanners, which means they can trigger their payload more often and increase their ROI. This is a risky endeavor because this javascript is visible to anyone paying attention.

Fingerprinting

Fingerprinting is a client-side mechanism (javascript) used by attackers to forge a signature of the browser / device, focusing on minute differences between a realistic user environment and a researcher / scanner / bot environment.

Alternatively, server-side mechanisms are more evasive because they cannot be inspected by a security researcher, unless they actually trigger. Such mechanisms include detecting the type of connectivity used by the user, by looking up the "ASN" from the browser client's IP. Datacenter IPs are commonly used in ad scanners and attackers will ensure that absolutely no payload triggers under a datacenter IP.

Server-side is more wasteful than client-side, it involves serving large volumes of ads that do not trigger their payload.

Client-side brings more data to assess the user so allows for more aggressive payload triggers, but the mere fact of collecting this data exposes the attacker and so is more risky.

Confiant observed Zirconium switching to more javascript fingerprinting roughly from October. We believe this trend was accompanied by an increase in traffic.

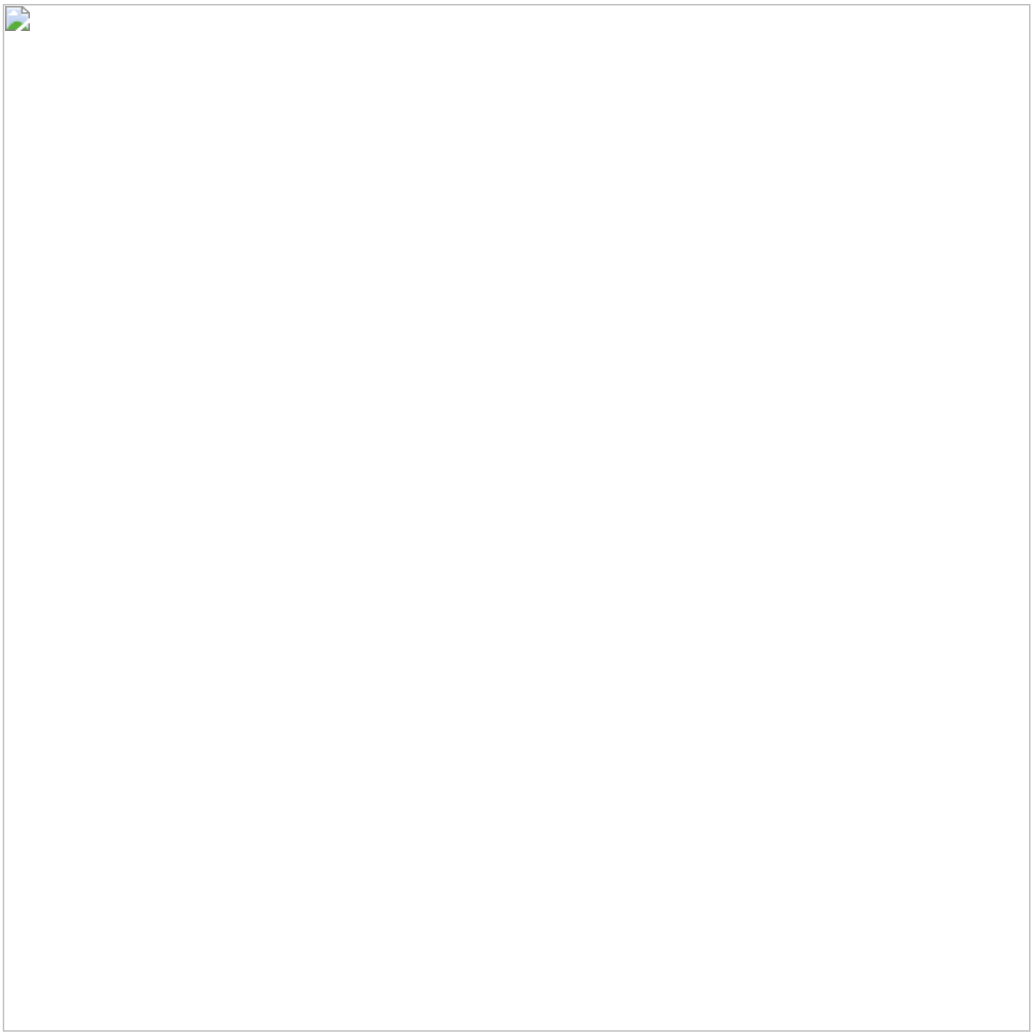


Fig. 6: Javascript fingerprinting used in Zirconium's AdTekMedia malvertising campaign

This code snippet was found in one of the ads served by the "adtekmedia" agency. Note the odd "RegExp" override for matching the user agent to expected browsers. Zirconium campaigns have been observed to exclusively target desktop browsers, excluding mobile — not only targeting Windows, but also Mac, ChromeOS and even Linux.

Aside from very basic data points like the user agent, they also check:

- Hardware concurrency: How many cores in the CPU?
- Availability of webGL APIs
- Availability of Chrome-specific objects in JavaScript

Virtual machines typically don't expose the full set of CPU cores available at the hardware level. This is true both in cloud computing (where scanners run) and on researchers virtual environments.

WebGL is only available in "real" full-featured modern browser. Most importantly, WebGL leaks the GPU chipset powering the device's graphics rendering. Cloud machines typically lack a GPU.

Identifying Chrome-specific javascript objects allows the attacker to identify potential user agent spoofing. When a Chrome browser declares itself as an IE browser for example, the attacker can pick up that inconsistency.

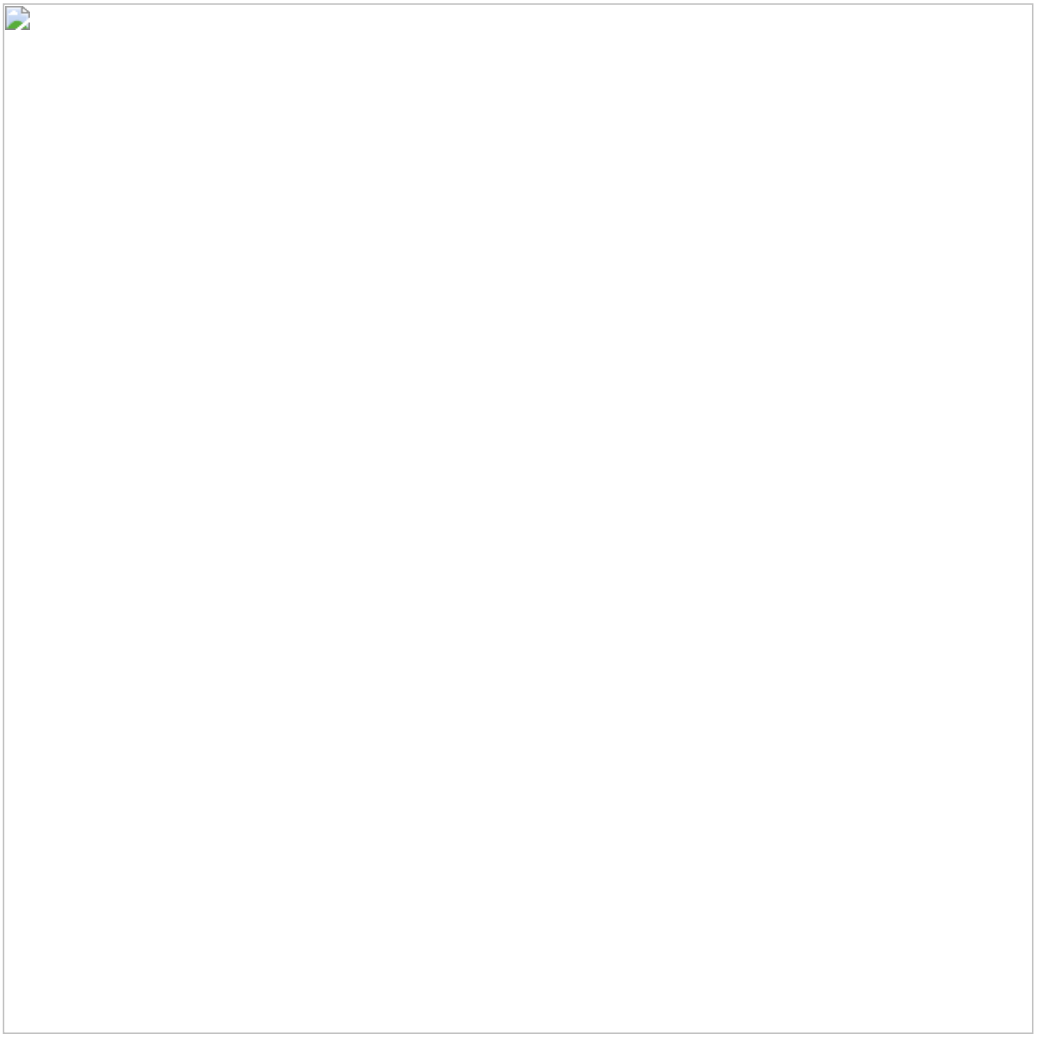
By checking these elements, the attackers can weed out the traffic that corresponds more to patterns found in researchers rather than victims.

Beyond evasion, malvertising actors want to keep fake traffic away from their campaigns, to maximize conversion rates. Similar fingerprinting / anti-bot technique was very recently documented in the RIG Exploit Kit.

Clumsy beginnings

On March 15, 2017 IndiaOnClick made its entrance in online advertising exchanges.

The website was a poorly executed copy-cat of a large ad exchange.



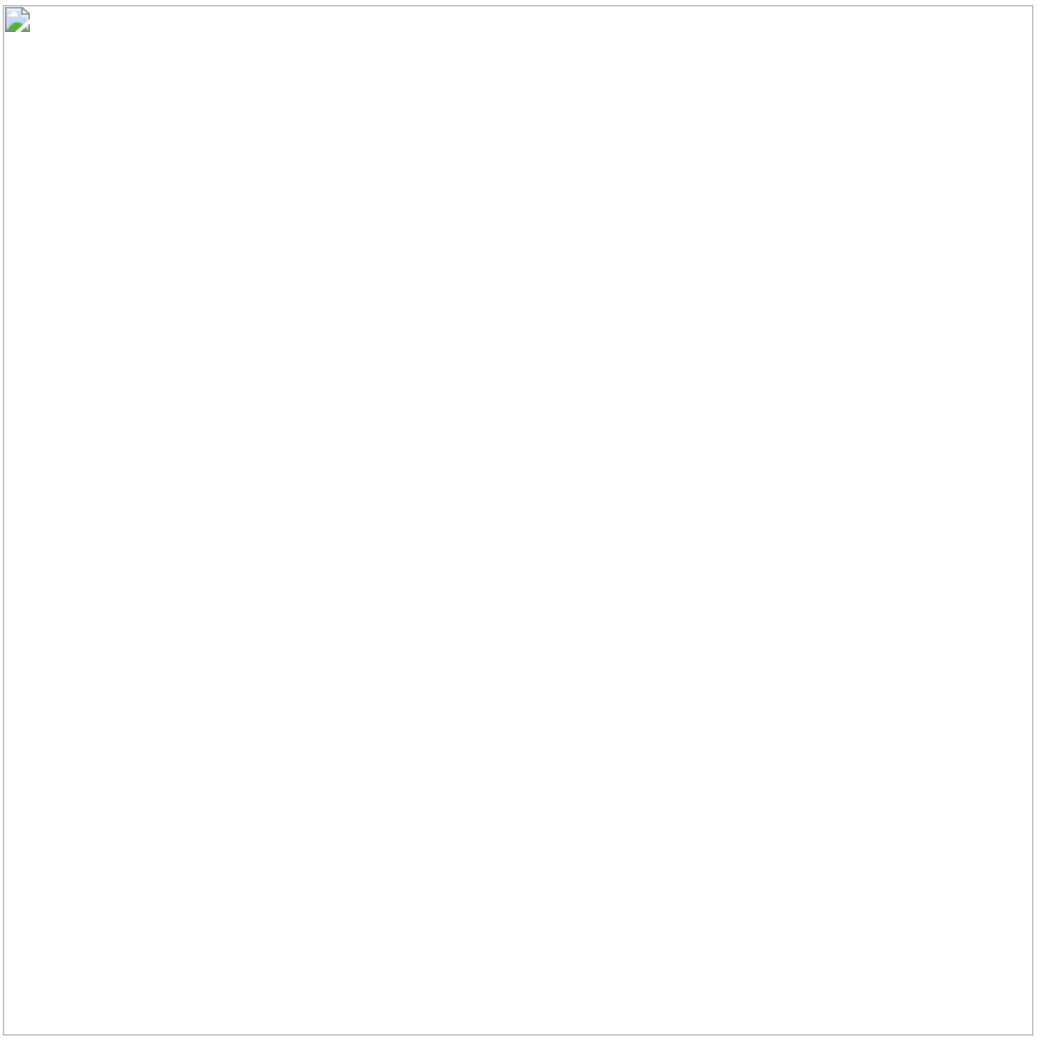


Fig. 7: On the left, IndiaOnClick fake ad agency; on the right, legitimate ad exchange

IndiaOnClick was later revamped, with an original design and original content — just like the other 27 ad agencies that Zirconium operated.

Reaching a massive scale

Everything is the same but everything is different: Each of the companies has been staged with a deliberate effort to

Fake CEO personas with LinkedIn presence like Ferdinand Konrad (98 connections), and countless others.

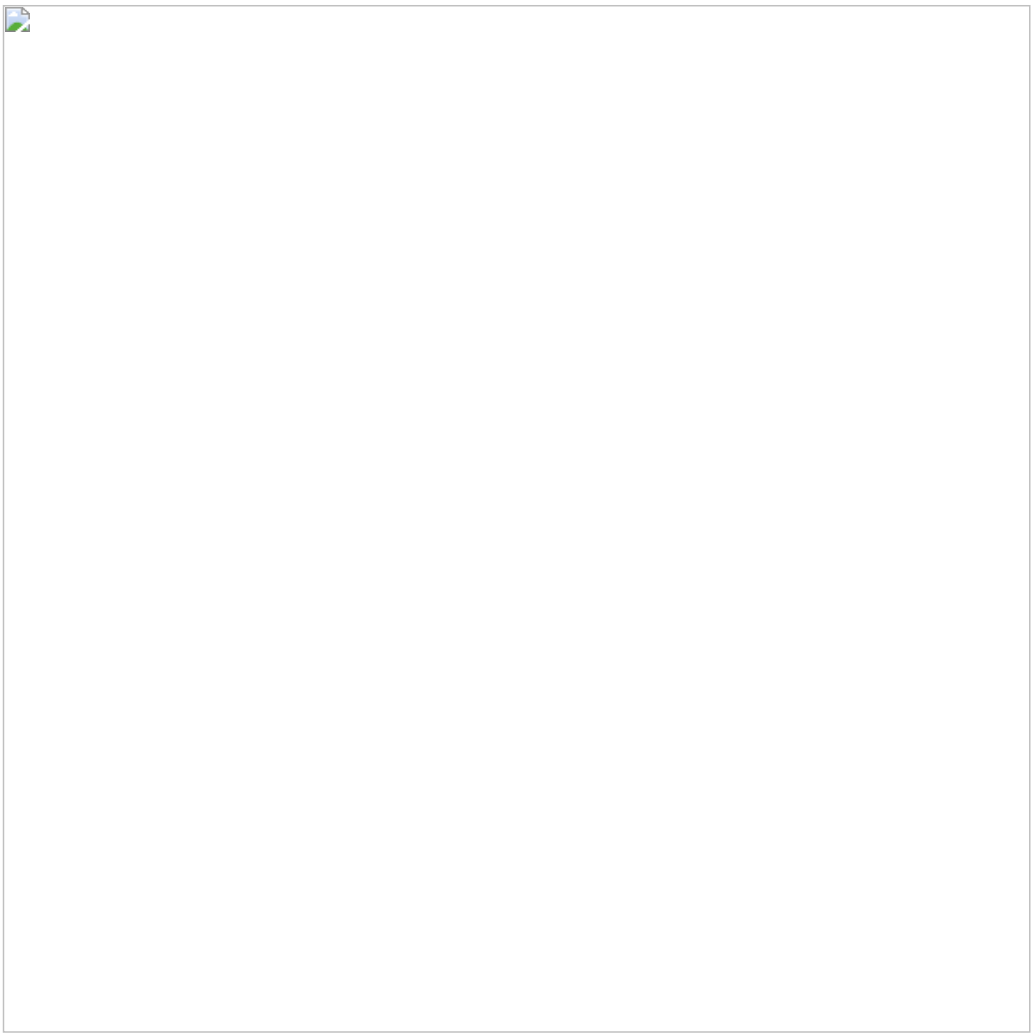


Fig. 8: Ferdinand Konrad's LinkedIn profile, the founder and CEO at Grandonmedia, based in Stuttgart, Germany

- Stock business photos (laptop and a coffee, suits in a meeting room, …)
- Regular social media posts with seemingly machine-generated content.
- Efforts to generate unique content, especially branded photos with marketing messages.

From a technical perspective, each fake company is operated by a completely independent infrastructure, from hosting to SSL servers to domain registration. Ad serving code is unique to each fake company.

Social Media content generation

Zirconium leverages a mysterious "marketing-o-tron" to generate automated content on social media via bots.

As of this writing, the bots are still active. Here's a sample of deep marketing mantras for January 10, 2018, as found on Twitter:

> *“There can’t be any peak prices for your online campaigns”*
> - ElixMedia
>
> *“You must choose a valuable approach to all online campaigns”*
> - DeshMedia
>
> *“The best way to solve online ad problems is to use quality packs from k5market“*- K5Market
>
> *“There must be an array of options to provide quality online services”*
> - HoffmanBroker
>
> *“Without a doubt, it is very important to have a chance to take a credit at the beginning of the advertising”*- Face2Trade
>
> *“This company doesn’t make naked promises about the quality of provided services”*- MediaParade
>
> *“We always allow our clients to use our online services for free”*
> - GrandonMedia

Zirconium’s concept is to build independant marketing brands from scratch, en-masse. The vast majority went live in March/April 2017 according to Twitter account creation dates. At the date of this writing, 8 remain unused, ready to be leveraged when the ones currently exploited dry out.

In each case, Confiant found that the attacker was acquiring/building a large amount of media at once to support their malvertising campaigns, which then trickled down over months.

Long tail ad agencies are numerous and widely embraced by the ad industry. Zirconium was extremely successful at replicating the “small business” ad agency style. The attackers successfully built direct business relationships with as many as 16 ad platforms.

Leveraging a swarm of fake ad agencies gives a strong justification for running custom ad servers, a critical part of the scheme because it allows for javascript execution on websites running ads.

Dormant ad agencies

Out of the 28 fake ad agencies, only 20 ever had any activity in advertising markets. We believe Zirconium was progressively rolling out their agencies to overcome occasional bans, as they progressively got caught. We observed a pace of 1 to 3 releases per month. Since the majority of agencies were created around February 2017, the dormant ones progressively built precious reputation (mostly history, and social media following) to pose as established companies and maximize their potential of striking deals with more ad platforms.

The group had also recently started to come up with new agencies, like Big Shark Media (November 2017).

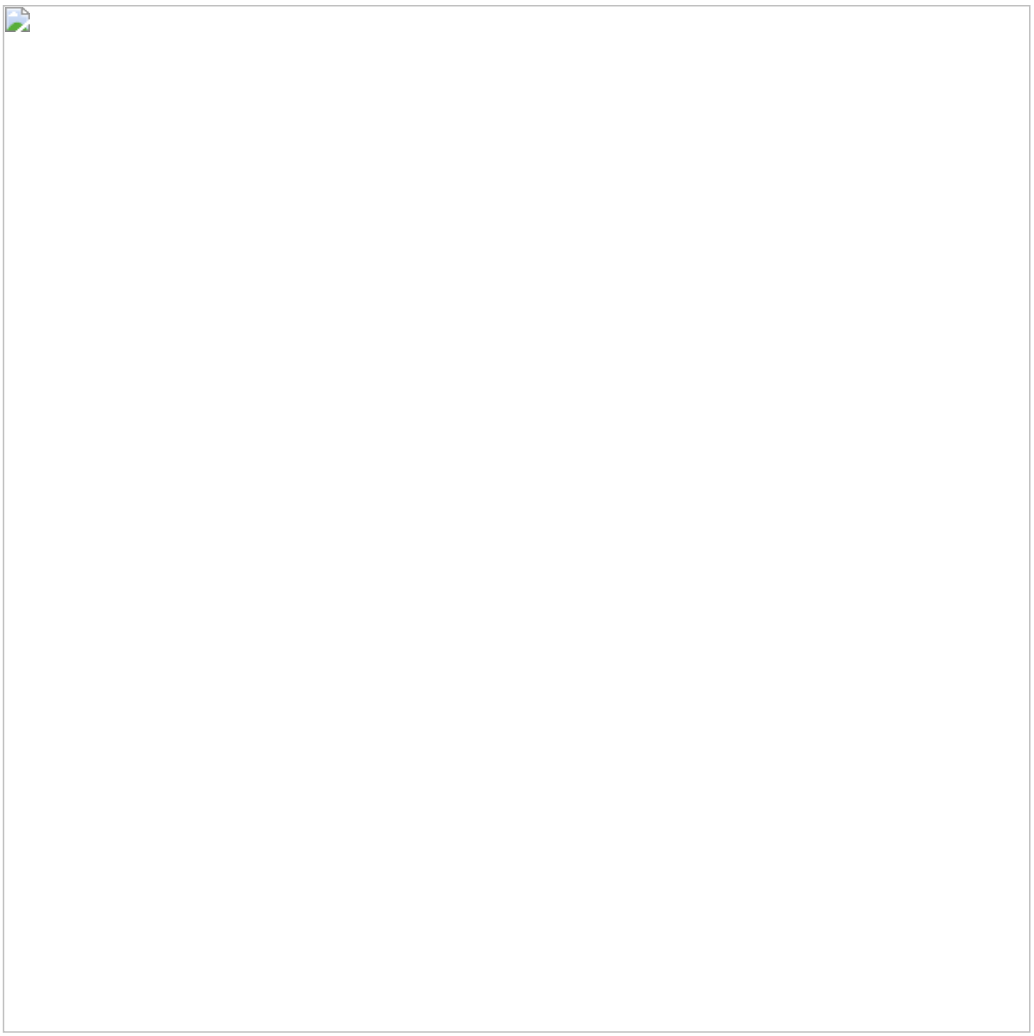


Fig. 9, Twitter, @BigsharkMedia, a dormant fake ad agency: “We’ll give you full advertising support in all your campaigns”

A classic business model

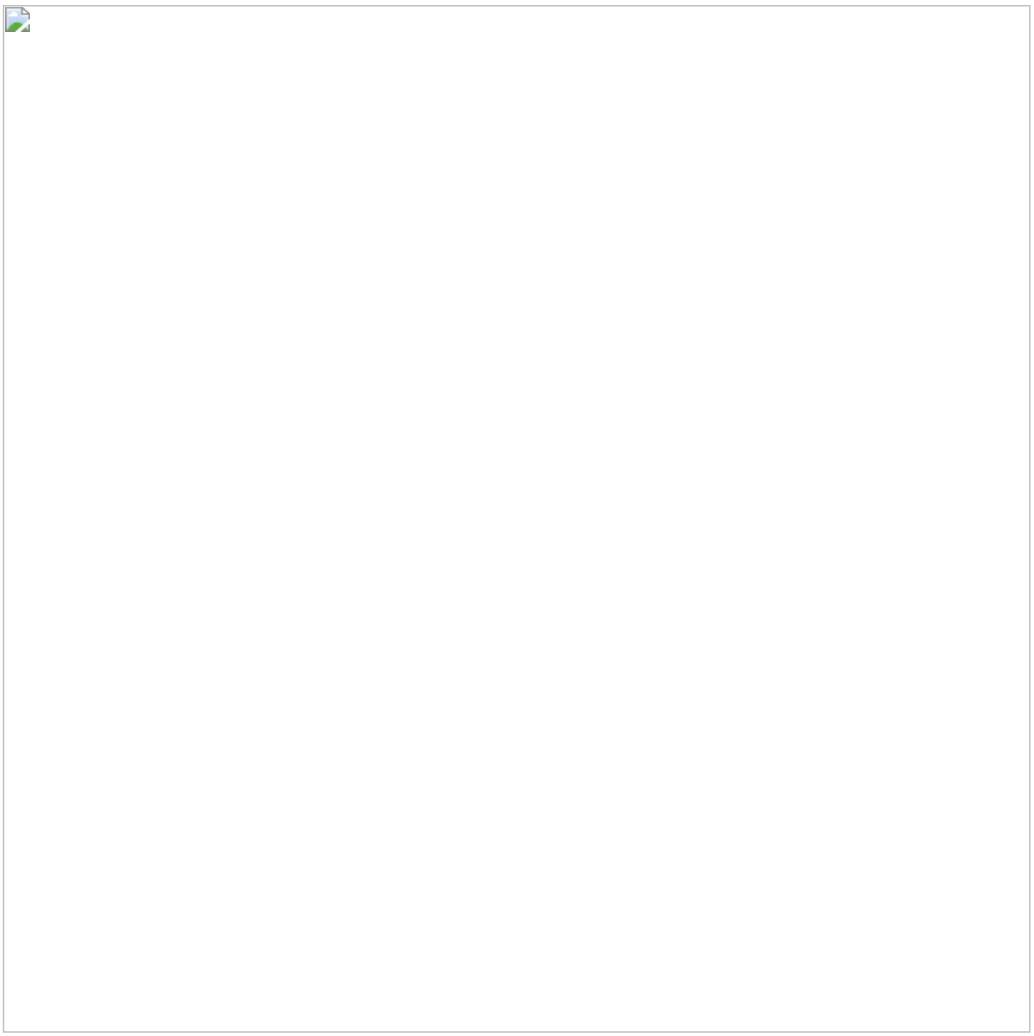


Fig. 10: Zirconium business model

A sophisticated legal structure

Thanks to cooperation with partners in the ad industry, Confiant identified the legal entity fronting the Zirconium activity as Cape Diamond LP, a shell company incorporated in Scotland with partners in the Seychelles — Damitra Group LTD and Lamen Business LTD.

The Zirconium business model is capital intensive and it makes sense that they would need to shield themselves behind an opaque offshore corporate structure.

Through 2017, both offshore companies have been extensively involved in online fraud activities, some of which crypto-currency related, most notably btc-e.com — a crypto exchange shut down by the US authorities in June 2017.

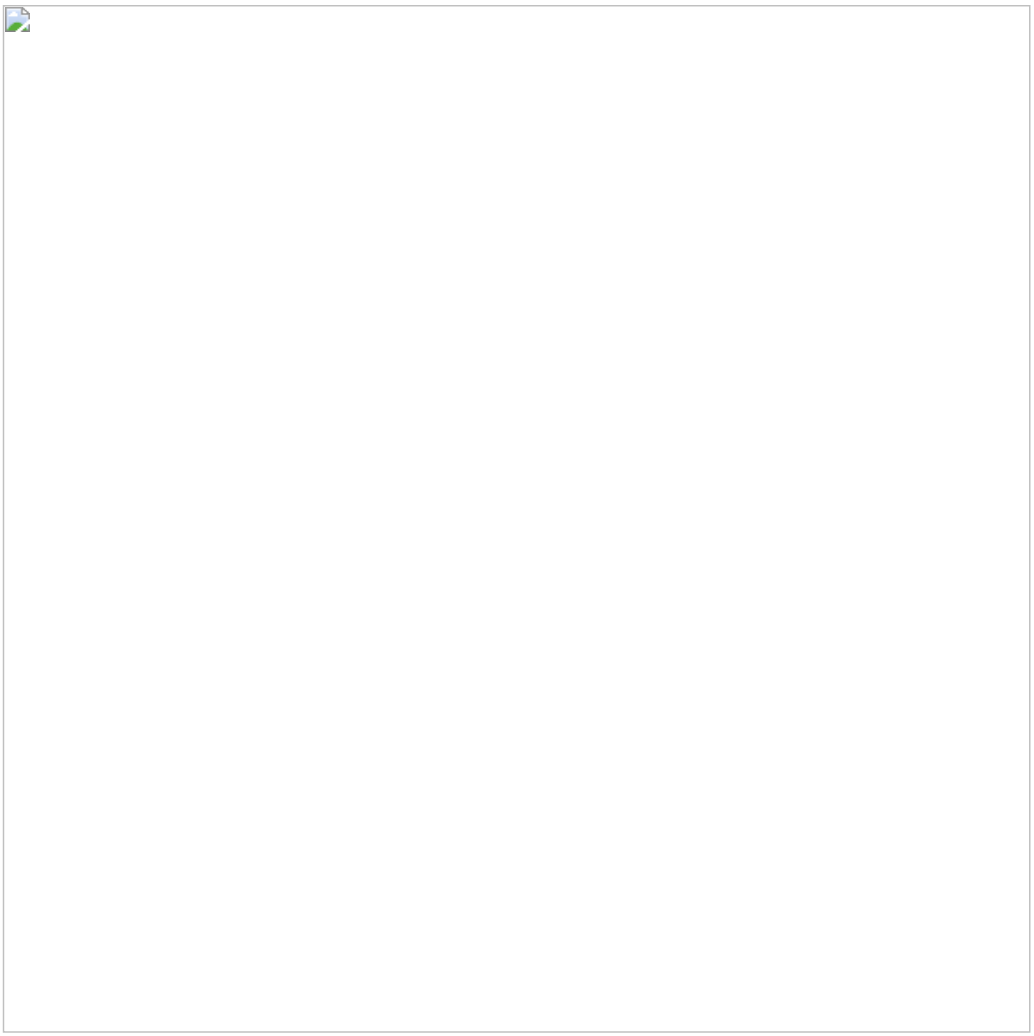


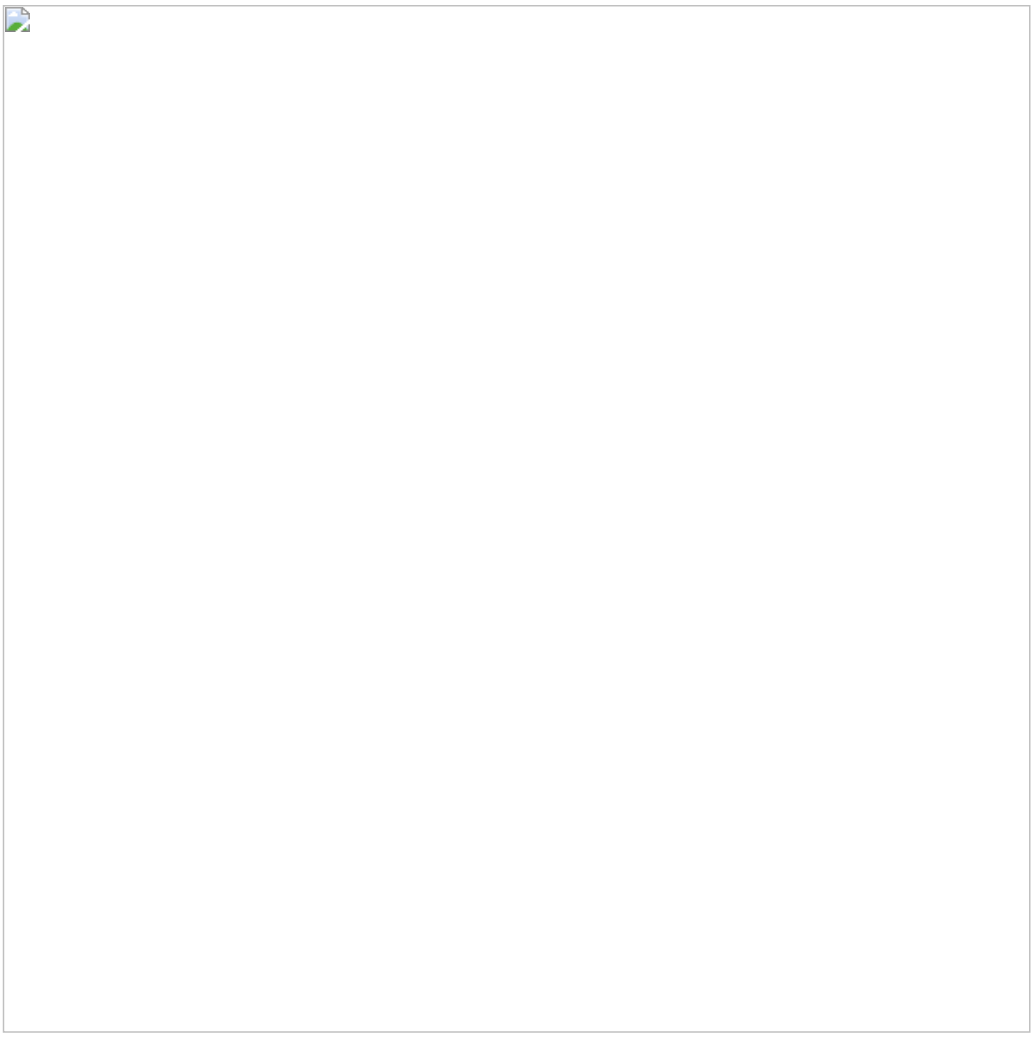
Fig. 11: Legal entities directed by Cape Diamond's offshore partners. source:

Conclusion

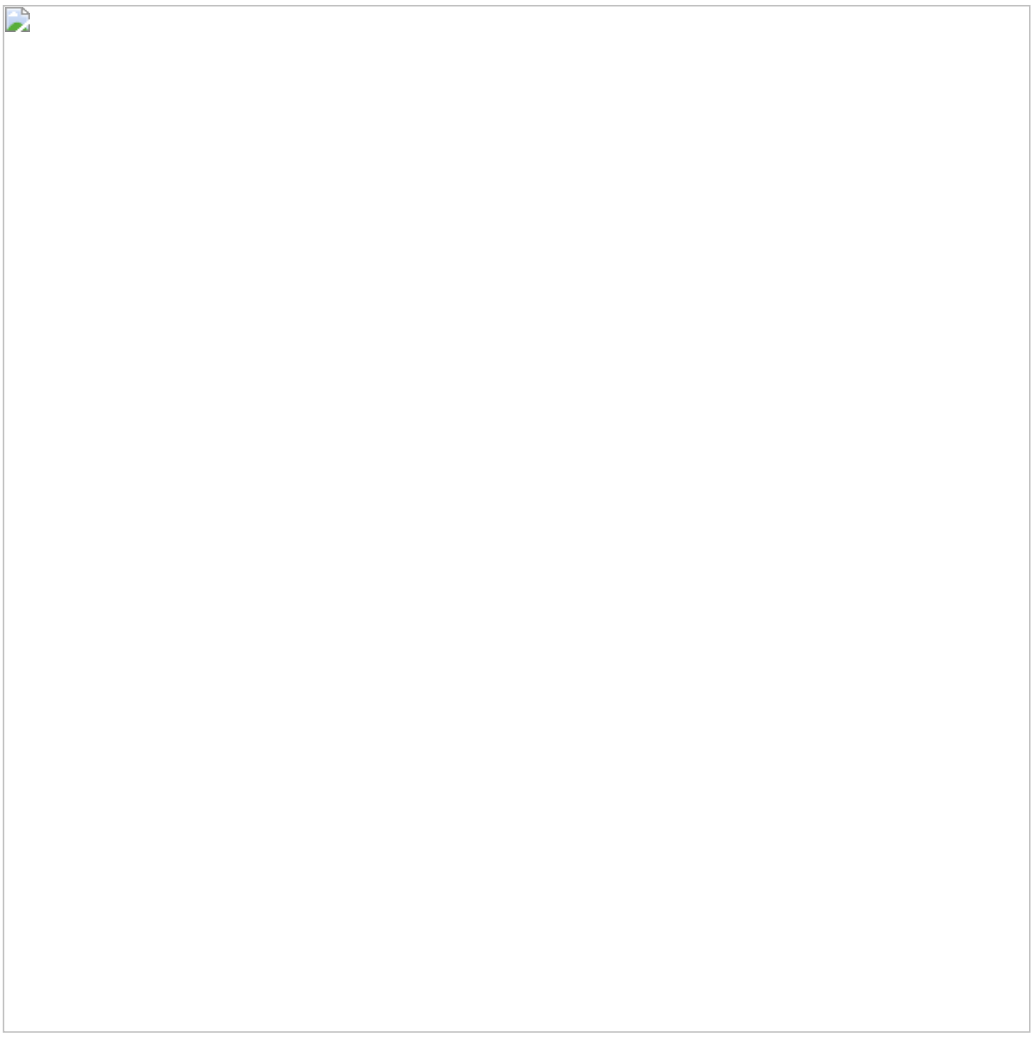
The Chrome team announced that forced redirects will be blocked in Chrome 64 scheduled for release on January 23. Google is fixing the hole that largely allows for this illegal business to thrive. They've already proven their adaptability and this will shift their efforts to some new threat vectors. Confiant will be here to greet them!

Appendix

Zirconium by the numbers



List of fake ad agencies



Dates and lifespans are based on actual activity in online advertising exchanges, last seen date populated as of Dec 21

About Confiant

Confiant is a cyber security company that came out of a recognition that the world's most sophisticated advertisers aren't Verizon or P&G, but criminals using the industry for their own, selfish ends. These criminals are hijacking programmatic advertising and giving publishers a bad name.

Confiant protects publishers' and platforms' reputations, revenue, and resources with always-on anti-malware software that provides protection for desktop, mobile, and video ads. Our sole focus is on helping advertising platforms and publishers rid the world of malware. This focus enables us to evolve quickly and meet our clients' needs for defeating the bad actors trying to undermine the industry.

We are the first to come to market with a technology that does not just detect the malicious activity, but actively blocks it. We believe in the intelligent application of this new technology to fight back and make media safe for everyone.