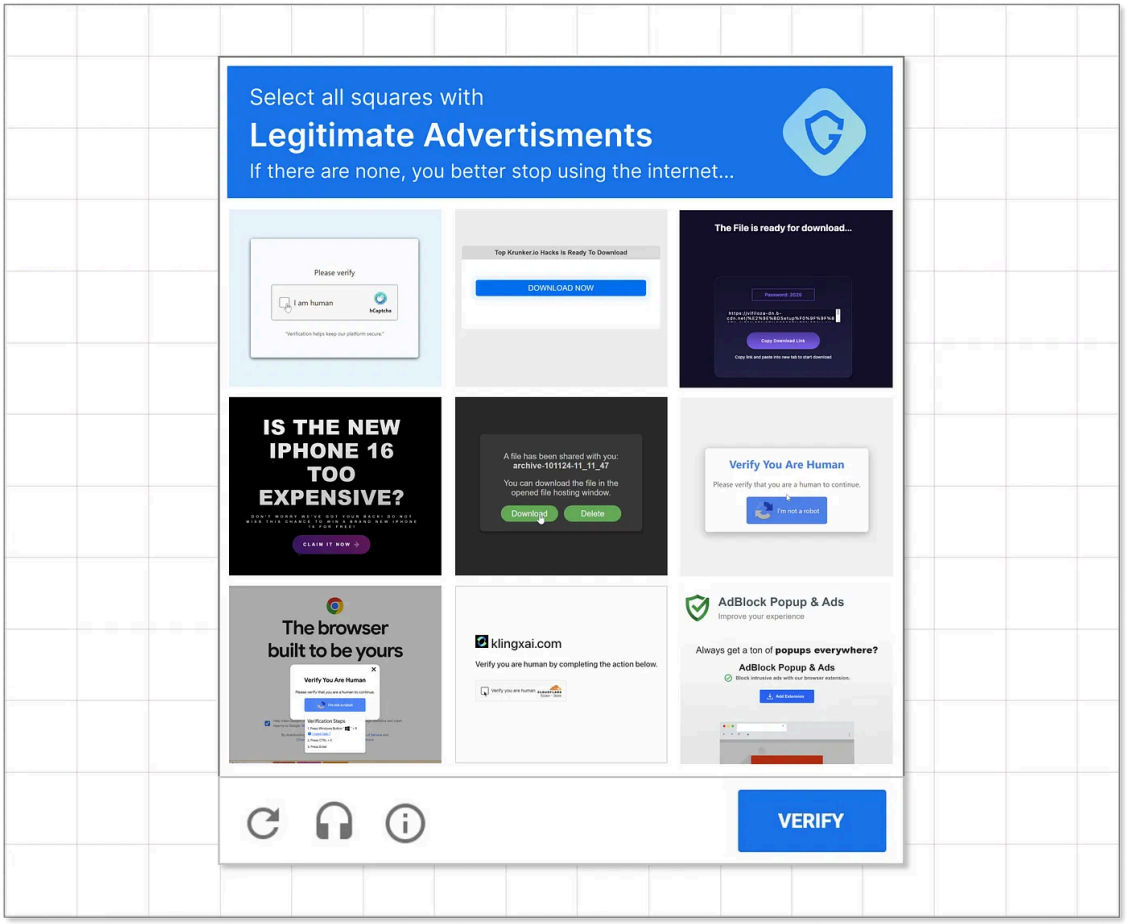
“DeceptionAds” — Fake Captcha Driving Infostealer Infections and a Glimpse to the Dark Side of Internet Advertising

By Nati TalDecember 16, 2024•17min read

Published: 2024-12-16 · Archived: 2026-04-10 03:03:42 UTC

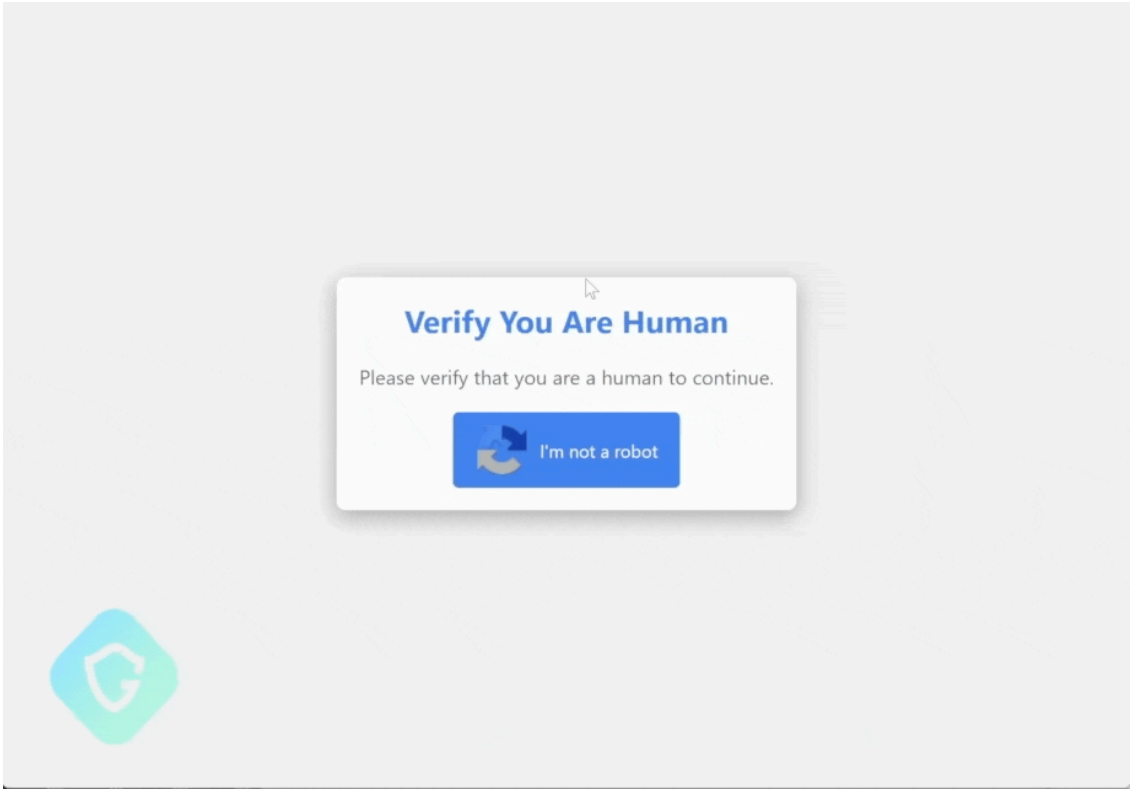


The Fake-Captcha Lumma Stealer Campaign

For several weeks, a large-scale deceptive campaign has leveraged a cunning technique: tricking users into installing dangerous stealer malware via a captcha verification page. This seemingly legitimate captcha page appears unexpectedly as you browse a content site, perfectly mimicking a real verification process. It asks you to confirm you’re human through a series of keyboard clicks, which ultimately trigger the Run dialog on your Windows system. Unknowingly, you paste and execute a cleverly crafted PowerShell command, instantly installing stealer malware that targets your social accounts, banking credentials, passwords, and personal files. Vicious, effective, and dangerously evasive!

Despite recent news coverage, the question remains: How does a fake captcha suddenly appear, tricking unsuspecting users into executing a malicious PowerShell command under the guise of verifying their human

identity? What keeps this campaign not only active but thriving?



The fake captcha flow — forcing site visitors to unknowingly execute a PowerShell command

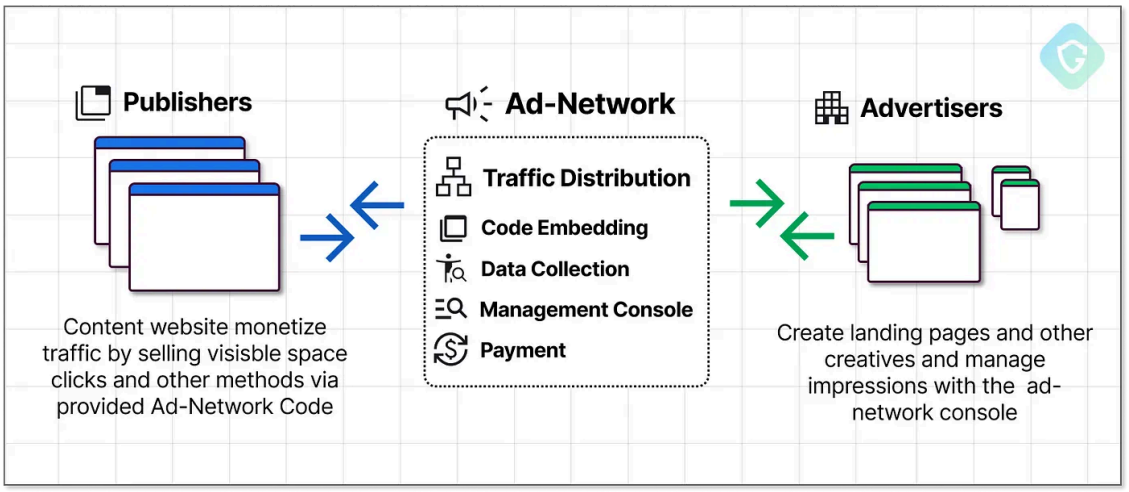
What are we overlooking? It's not solely the clever disguise of captcha imitation that marks the success of this campaign. The real concern lies in how this perilous page makes its way onto our screens. The answer is **malvertising — malvertising on steroids**. This initial deceit is just the surface; the ad network underlying mechanics reveal a darker, more complex web of digital threats.

Ad-Networks As Enablers

Since the early days of the internet, advertising has been a cornerstone, growing increasingly vital over the years. For instance, in 2023, almost 70% of Google's revenue stems from advertisements, highlighting the lucrative nature of this industry.

However, the ad tech industry has also taken a darker turn, becoming a prominent channel for malicious activities. Examples abound, from fake e-commerce sites advertised on Facebook to deceptive "Download" buttons that deliver unexpected software and even rogue sponsored results in Google.

The responsibility often falls on **Ad Networks**. These services form the link between advertisers seeking to sell products or services and website publishers looking to monetize available space. Ad networks handle the coding, analytics, and management necessary for both parties.



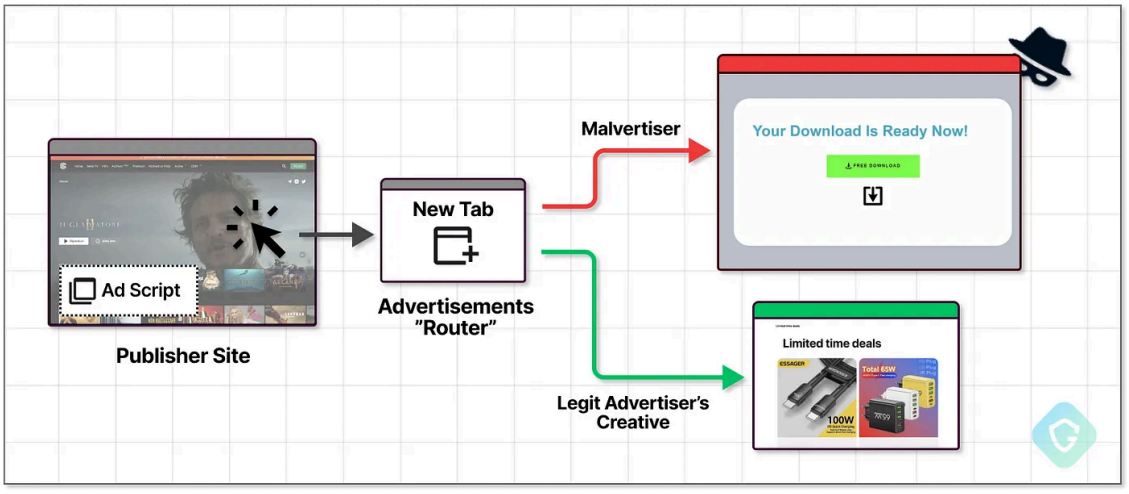
The Ad-Network ecosystem — Publishers monetizing on ad zones and Advertisers seeking impressions

The process is straightforward: website owners register with an ad network, receive code snippets to integrate into their sites, creating “Advertisement Zones.” These zones, when activated, direct traffic to the network’s Traffic Distribution System (TDS), which houses numerous domains and redirectors. The system then selects the most optimized advertisement to display based on visitor analysis, campaign budgets, and settings — all in milliseconds. The advertisers focus on optimizing landing pages for conversion, while website owners collect their earnings.

Evolving From Advertising to Malvertising Captchas

Ad networks have proven exceptionally successful; they are fine-tuned machines built from the ground up to distribute traffic on a massive scale, from advertisers to internet users across a vast ecosystem of websites. But what happens when advertisers are replaced with threat actors? Yea, you’re right—we get **Malvertising**.

Many active ad networks are raising alarms with the content they distribute today. Although they don’t have sole control or responsibility for this content, the overtly malicious intent and scale of the activities exploiting their networks are too significant to ignore or absolve them of all responsibility.



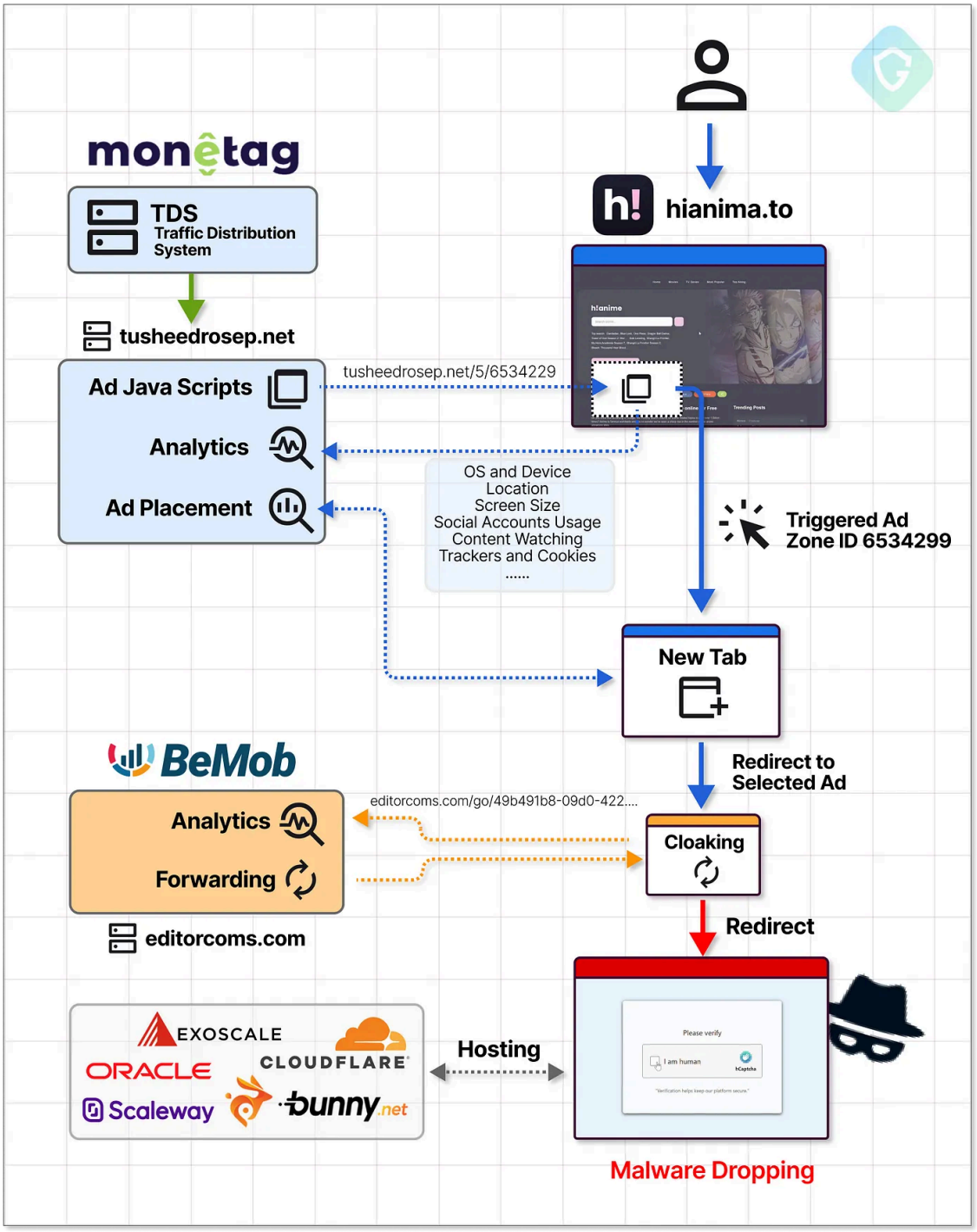
A visitor activating an ad-placement process and the ad network selecting the target creative (good or bad)

The scenario above is a real-life example of how just three simple clicks on an ostensibly benign website can lead you down an unexpected path—perhaps when you only want to watch a movie. But will you actually get to see that movie? Unfortunately, that's far from guaranteed…

Fake-Captcha's Malvertising: End-2-End Analysis

This Fake Captcha campaign might be the holy grail study case of how ad networks fuel the mass distribution of today's malicious activity. Analysis shows that all the traffic directed to fake captcha pages came from ad clicks—thus, **this entire campaign is based on malvertising**! But who is behind this ad network abuse?

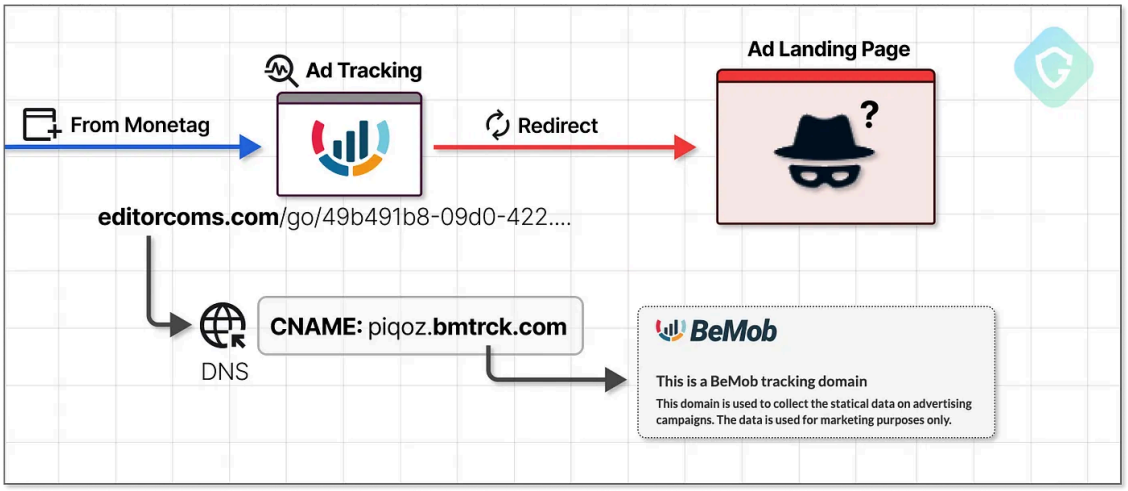
Upon examining the ad-related scripts embedded on these sites, it became clear that they originate from **a single ad network service**. These scripts lead to thousands of domains with odd names but share common parameters. Through a detailed examination of DNS fingerprints, server IPs, and locations, we linked these domains to "Omnatuor/Vane Viper" — a threat actor previously discovered and since tracked by our friends at Infoblox. Notably, this isn't the first instance of this ad network being associated with the distribution of malicious content. Surprised?



Example of a full fake captcha malvertising attack flow including all services in use

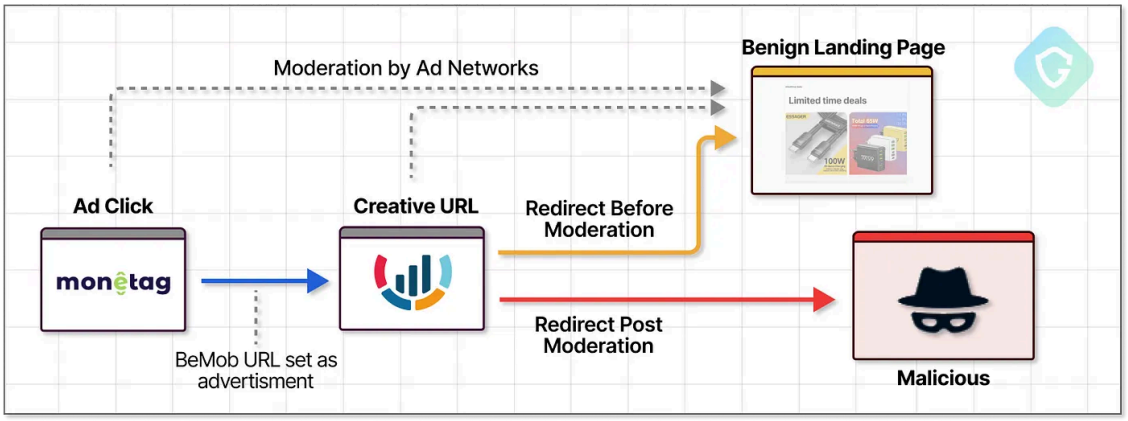
In collaboration with Infoblox and through meticulous deobfuscation of JavaScript snippets responsible for triggering ad events, we identified the ad network service responsible—**Monetag**. Monetag is a subsidiary of PropellerAds, a large ad network company based in Cyprus. As with Infoblox's analysis, PropellerAds activity had already come up on the radar of the cyber security community in the past.

Another crucial clue further in the flow is a redirect chain from a Monetag TDS domain to another unique URL pattern. This is yet another TDS from a specific service called **BeMob,** an advertisment tracking service, as we realized quite quickly from the DNS's A-Records pattern (`xxxx.bmtrck.com`) that is shared to all those domains:



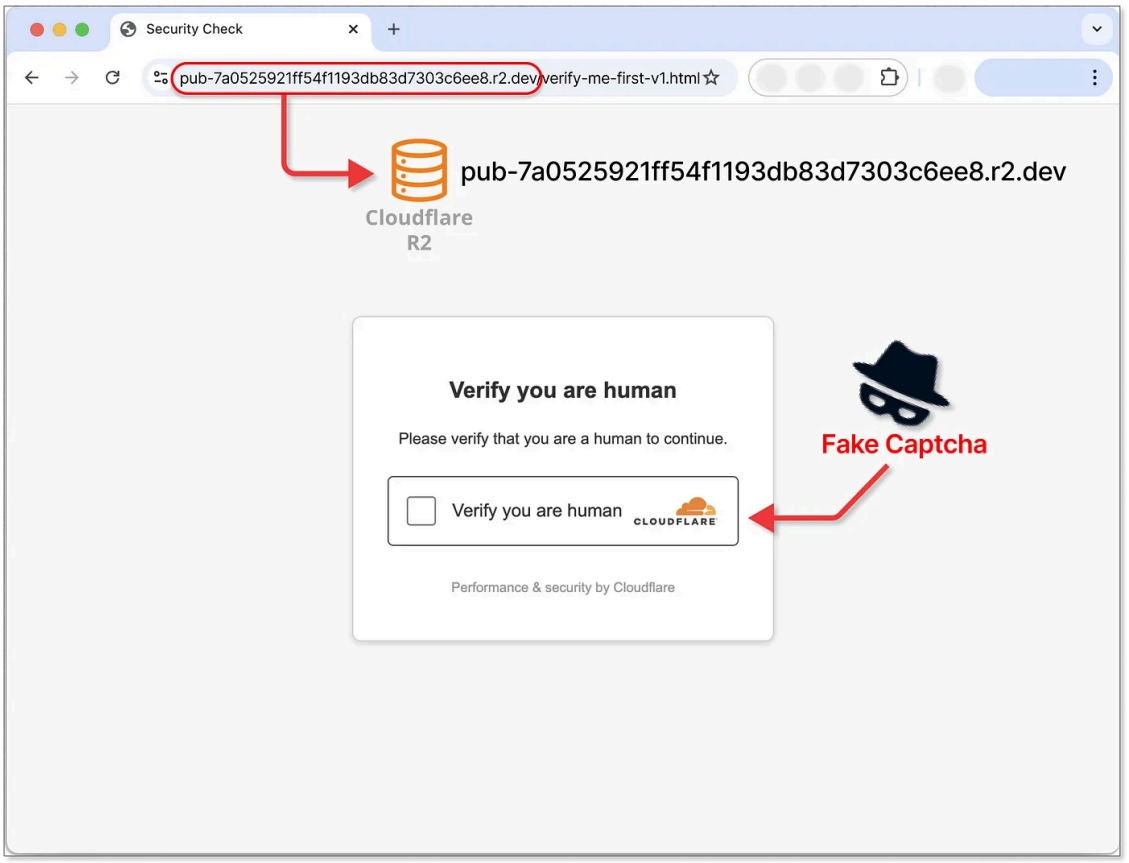
Revealing the TDS behind the fake captcha cloaking mechanism via DNS records

Ad tracking, like BeMob provides, is quite a common service for ad campaigns. Although we can think the threat actor would like to track and optimize their “advertisement” campaign via a service like this — this is not the case here. It is used solely for **cloaking**. By supplying a benign BeMob URL to Monetag’s ad management system instead of the direct fake captcha page, the attackers leveraged BeMob’s reputation, complicating Monetag's content moderation efforts. We’ve seen this practice many times in the past and in various variants, just like MasquerAd-ing on Google.



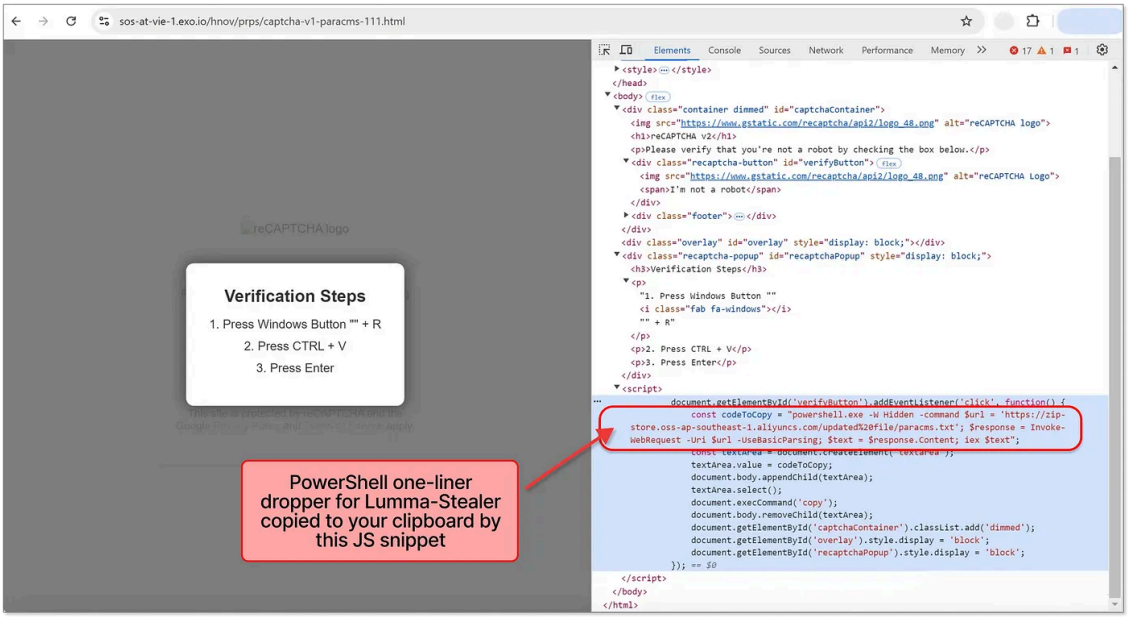
Cloaking in action — Moderator sees a benign creative seemingly changed to malicious upon activation

This BeMob TDS finally redirects to the malicious captcha page, hosted on services like Oracle Cloud, Scaleway, Bunny CDN, EXOScale, and even Cloudflare’s R2 itself! What would Alanis Morissette say about that?!

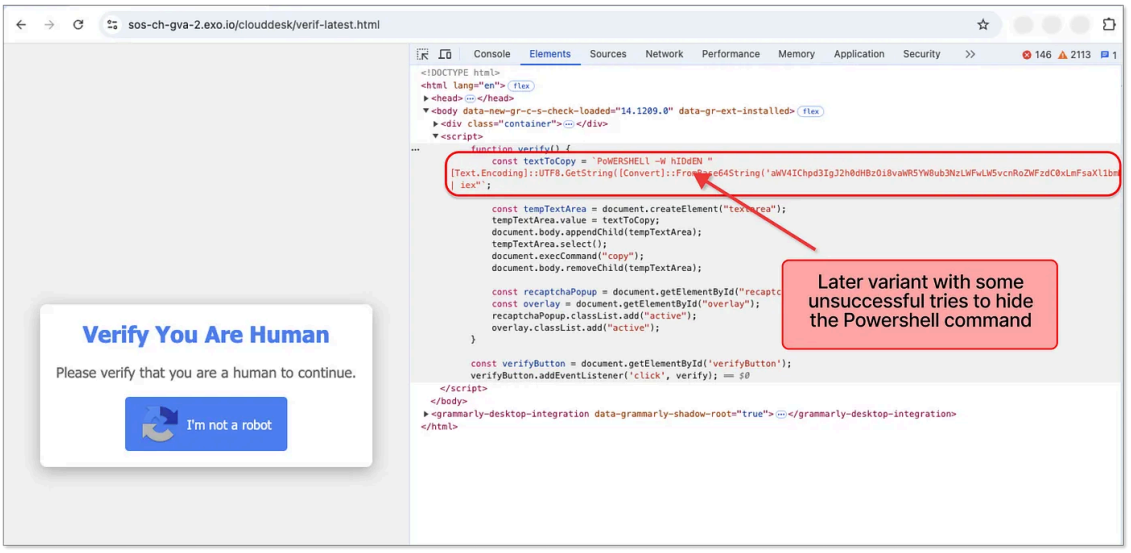


A Cloudflare-themed fake captcha page hosted on… Cloudflare R2 storage!

The ability to propagate in scale using an ad network and cloaking their intent using yet another ad service allows this campaign to gain traction and keep on going. Moreover, the malicious pages are frequently updated with new variants to evade detection. Those use different PowerShell one-liners, different script obfuscation to copy the PowerShell script to the clipboard, as well as changes in visual design:



The JS snippet on fake captcha page copying the malicious PowerShell one-liner to clipboard



Another JS snippet variant introduced later on, trying (unsuccessfully) to hide its real intent

The numbers are quite astonishing. Over just the past ten days, our analysis estimated up to **1M** "ad impressions" per day, arriving from around **3000+**publisher sites. Some use the popup script that creates new tabs on any click, and some are designed from the ground up to redirect users to "direct links" — a special URL provided by Monetag to trigger an ad event.

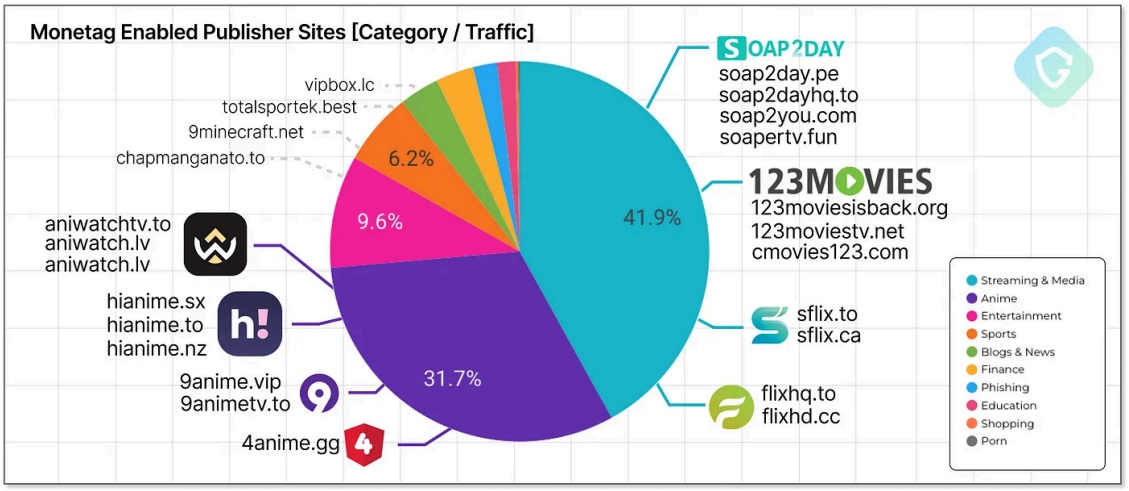
> As we delve deeper into the distribution method known as malvertising, it becomes clear how intricate and complicated the fake captcha campaign truly is. Yet, the core operations heavily rely on the ad network — essentially, their standard business practice is transformed for malicious use.

This investigation sets the stage for a deeper exploration of the ad network's ecosystem. How have they cultivated such a robust, active network of publishers in the first place? Let's start with analyzing what stands behind the scenes of this distribution ecosystem…

The Publishers: Pirated Content and Click-Baits

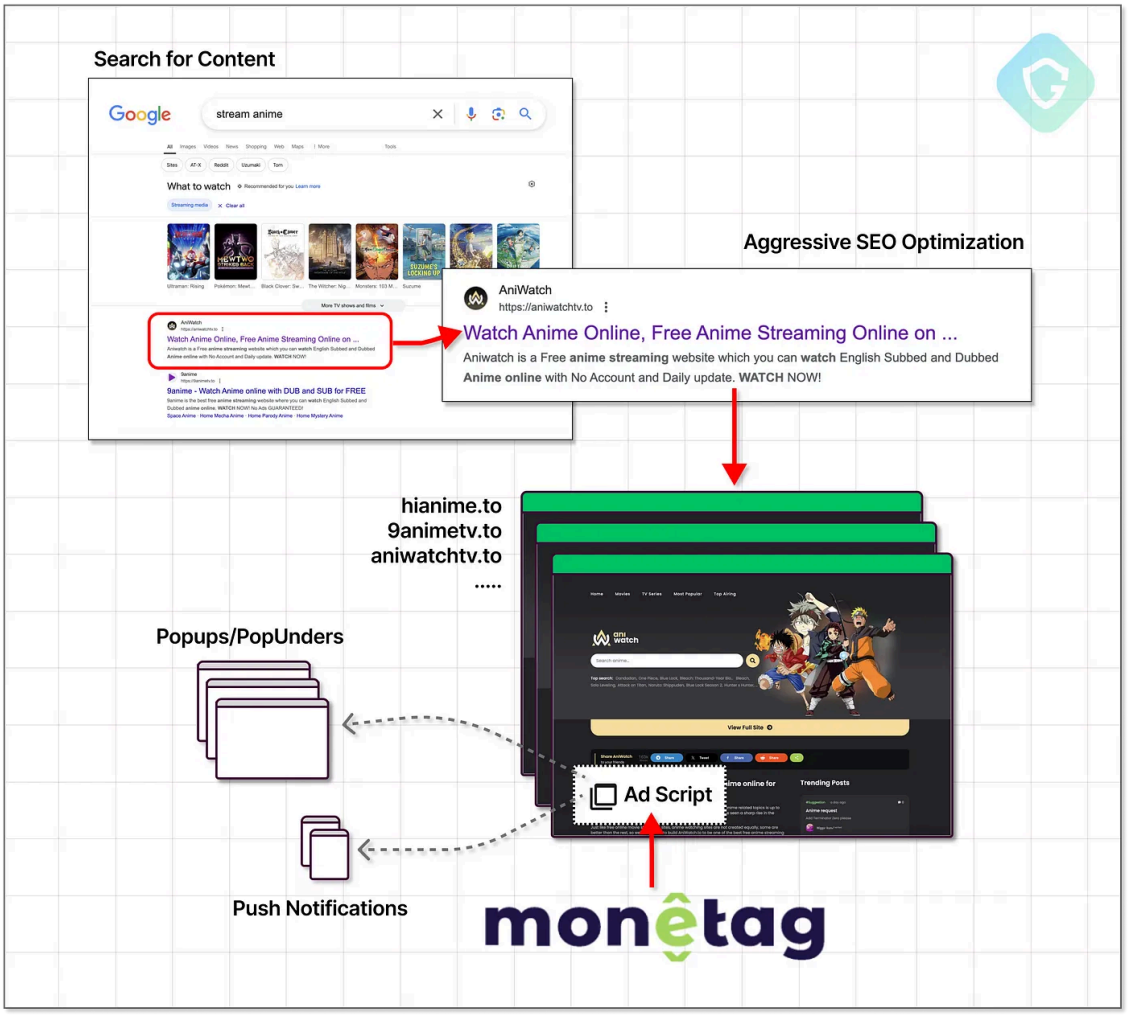
An ad network is only as effective as its funnel of users. With Monetag's vast catalog of publishers, the "infection chain" begins with a plethora of websites. Yet, most of them share some characteristics that raise questions about their nature and origin.

In our analysis, we identified approximately 3,000 publisher sites actively using Monetag ad-zone scripts in the last ten days. These scripts track visitors and trigger intrusive actions such as push notifications and new tab pop-ups. For instance, the anime site "**hianime[.]to**" alone garnered over 100k+ unique visits last month. Looking at the overall list shows interesting classifications that can teach us a lot about this activity:



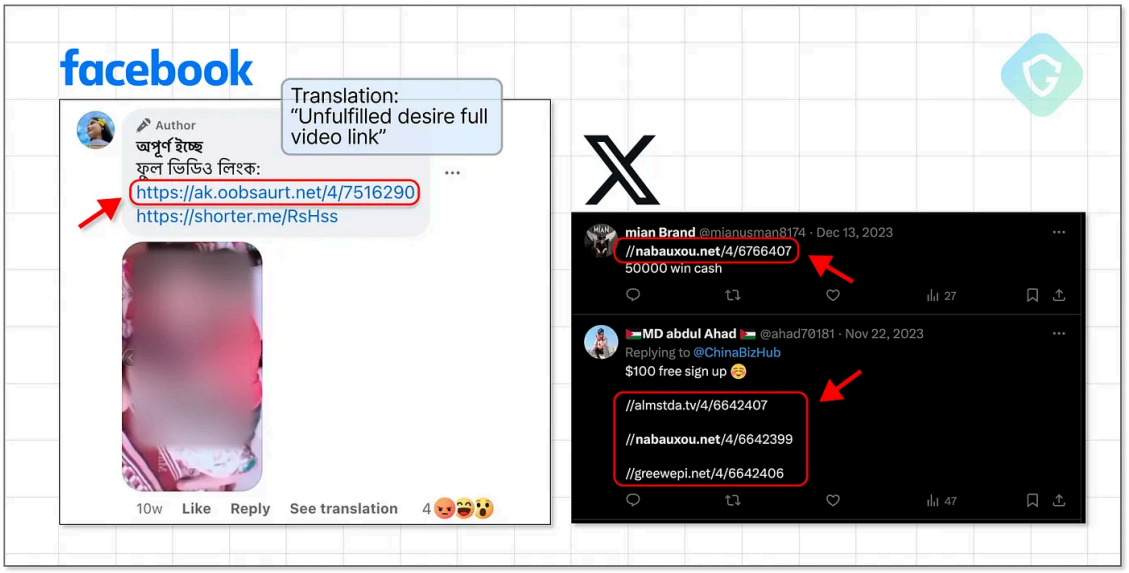
Monetag's Publisher sites in the past 10 days by categories perc. of total combined traffic

Visitors seeking anything from streaming videos to downloading academic documents inadvertently land on these sites. A simple search like " `stream anime` " can lead directly to these cloned sites, prominently positioned in Google search results due to aggressive SEO (Search Engine Optimization):

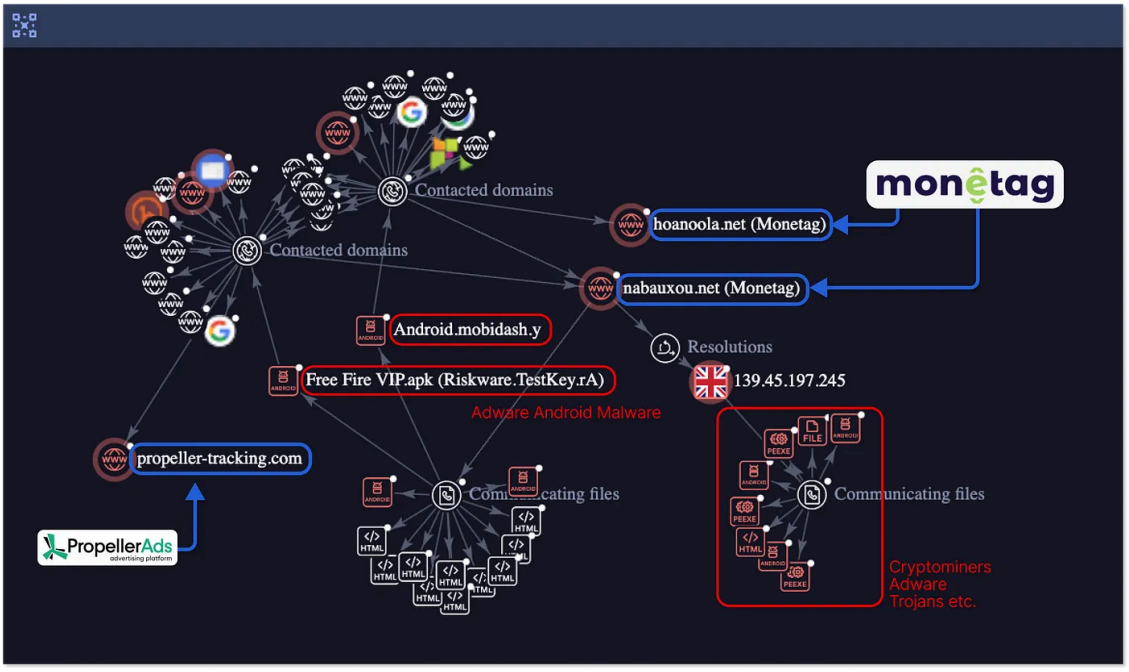


A real example of powerful SEO - First Google Search results pointing to a Monetag-enabled site

But the machinations don't stop there. Monetag also promotes the use of direct links, which circumvent the need for a website entirely. Imagine the myriad ways to deploy these links: social media posts, instant messages, deceptive website buttons, or even ad-ware attacks that forcibly open browser windows on your system without your acceptance.

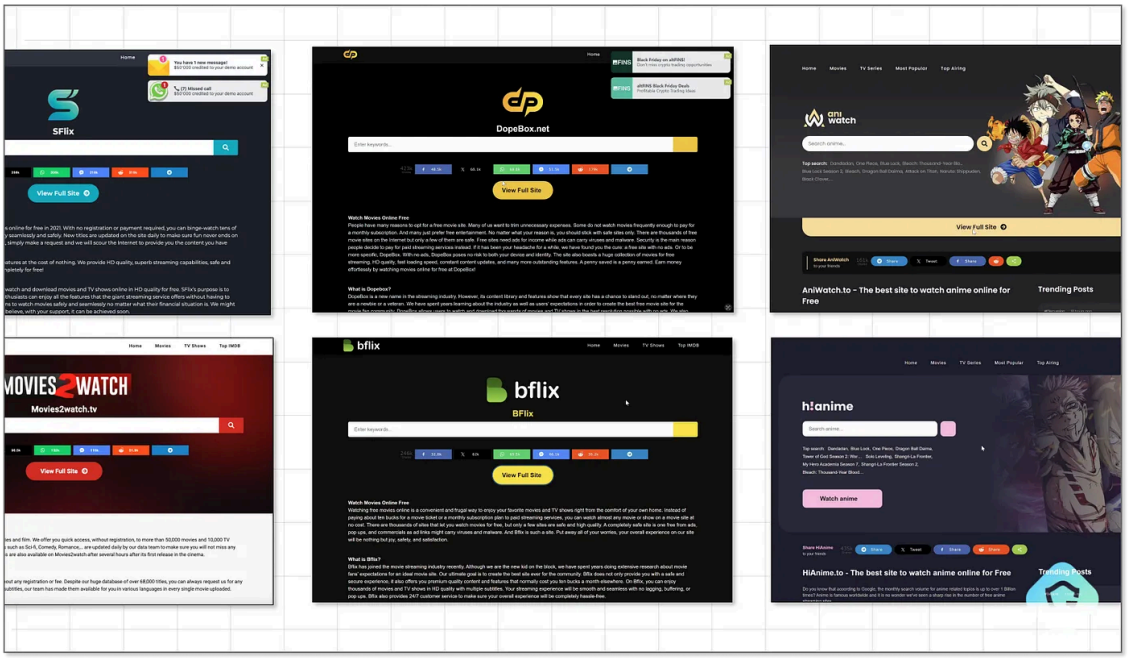


Social click-baits on Facebook and X pointing to Monetag's direct links



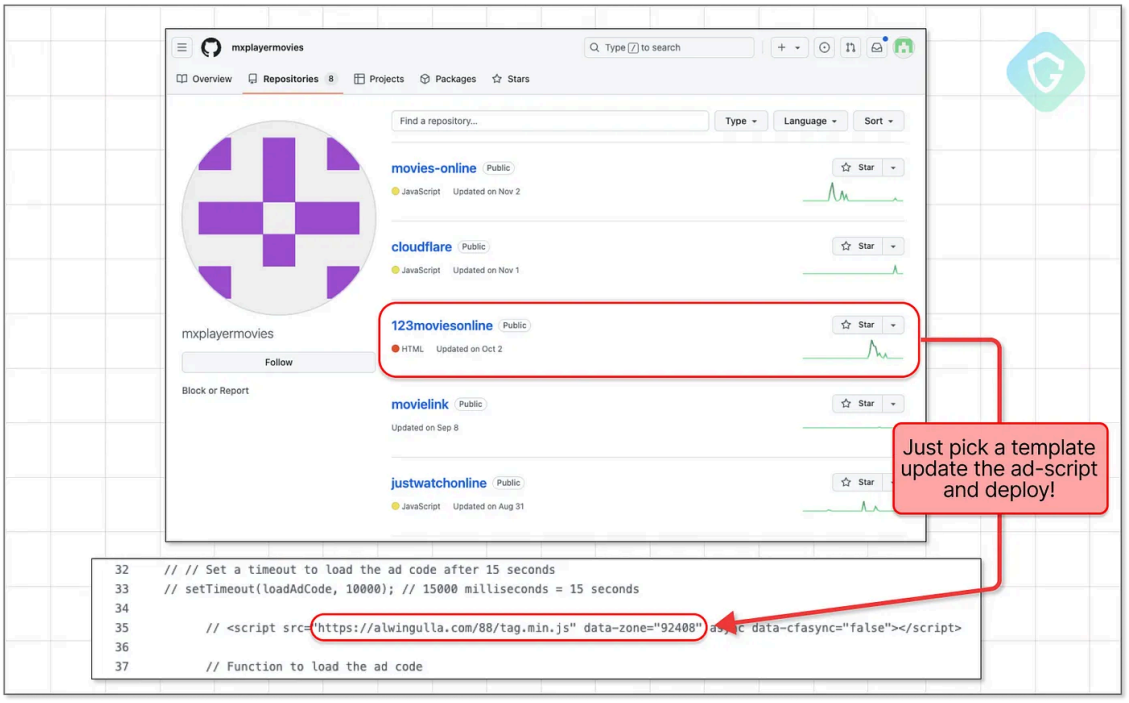
VirusTotal: Monetag's TDS domains direct link to Android/Desktop adware as well as Propeller-Ads infra

So, who operates these sites? Are they legitimate businesses or mere facades for illicit earnings? While no definitive evidence proves the latter, the uniformity across many sites suggests a coordinated effort. Many websites, appearing unique at first glance, share identical content and layouts, either translated or slightly tweaked:



Copy-Paste Content Site Kits for Streaming

Public repositories on GitHub even offer ready-to-deploy website templates that require only the insertion of ad script codes:



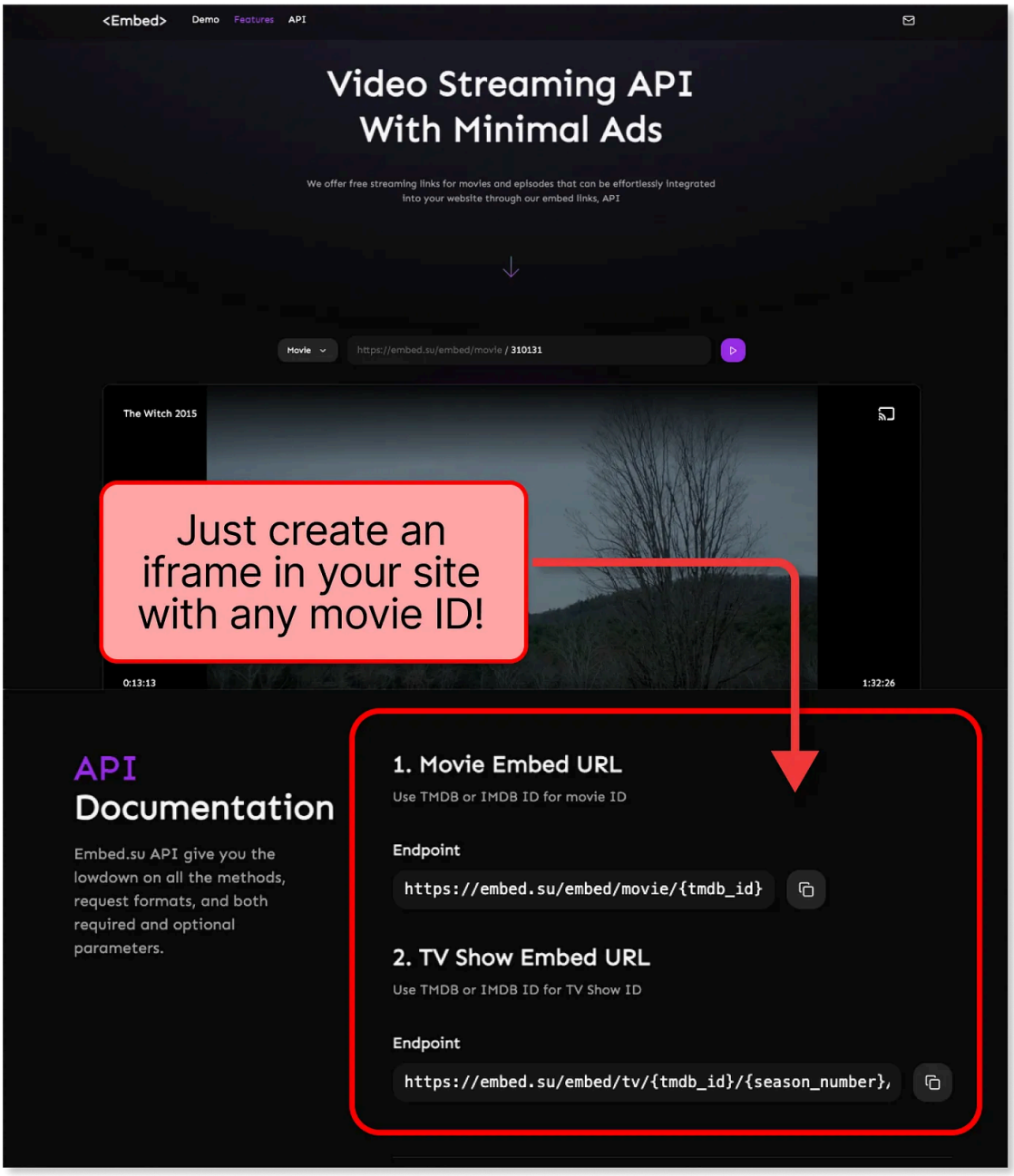
Example of a repo providing several streaming site kits with ready-to-go Monetag integrations

There are so many streaming websites offering the latest movies — some of which have not even been released yet! And all this clickbaity content is offered to you **free of charge**.

If you want to get even more conspiratorial, you can argue that this entire ecosystem of publisher sites is fueled by the ad network itself, providing site templates, SEO optimizations, and maybe even the content itself, like pirated

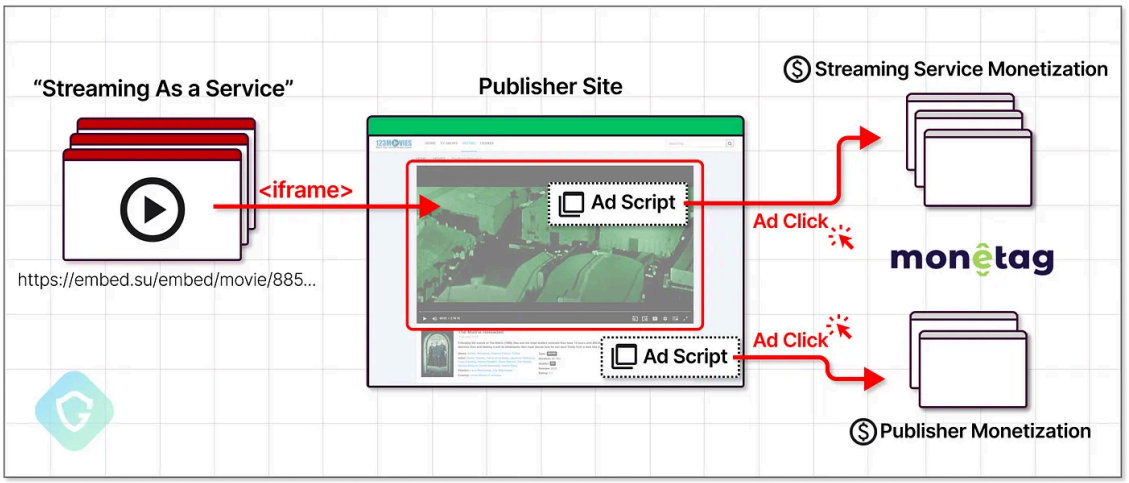
movies and live sports game streams. **We are not saying this is the case,** but one should judge for themselves:

Look at this “service” offering a ready-to-use video player loaded with unlimited movies that integrate seamlessly into any site. Under the hood, this video player iframe uses Monetag ad scripts to monetize this traffic directly from the ad network:



Online service providing unlimited video libraries in an iframe —with integral Monetag monetization

This service’s ubiquity across multiple web pages (and site templates ready to deploy as mentioned above) suggests a systematic strategy to amplify traffic and, consequently, ad revenue.



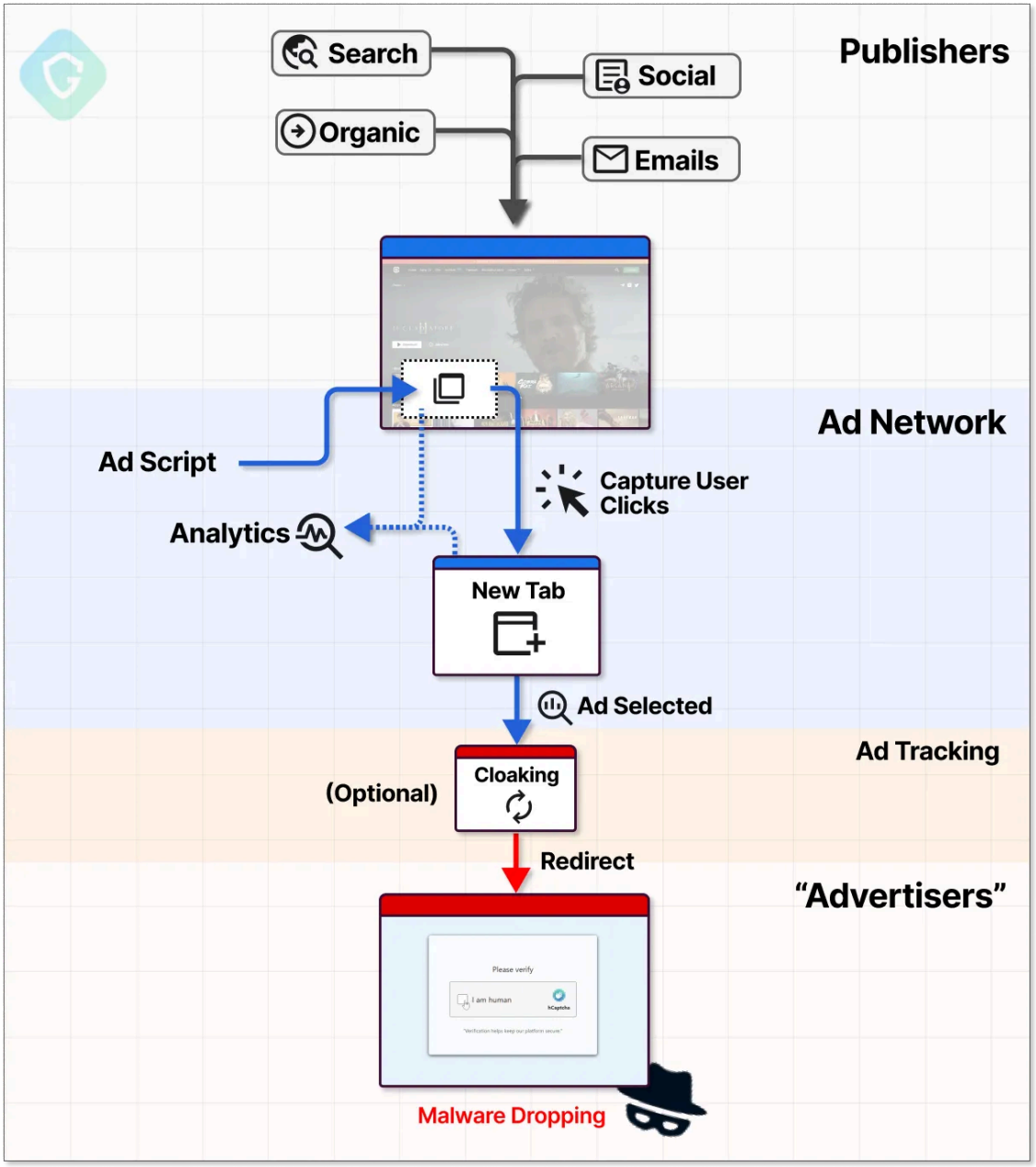
Double the fun — both video service as well as the content site monetize on Monetag

Ha, and what about sites that never intended to monetize their content, not to say, to infect their visitors with stealers? A branch of the publishers' ecosystem is just compromising WordPress sites (and others, of course) to inject their Monetag scripts directly in there. Talking about passing the buck….

Reflecting on the broader scope, the scale of potential manipulation and malvertising becomes even more daunting if we consider all other active ad networks combined. The statistics are so against us — if you look for content, you will probably land on a shady ad network-enabled website quite instantly…

A Mind Game of Plausible Deniability

In such campaigns, responsibility is fragmented among numerous parties — each playing a role yet avoiding full accountability. From the threat actor (the ad network customer) to everyday internet users (the victims), a single ad click sets off a chain reaction involving multiple service providers, domains, servers, and stakeholders — all within milliseconds:



The chain of responsibility — how a malvertising campaign abuses the entire ads eco-system

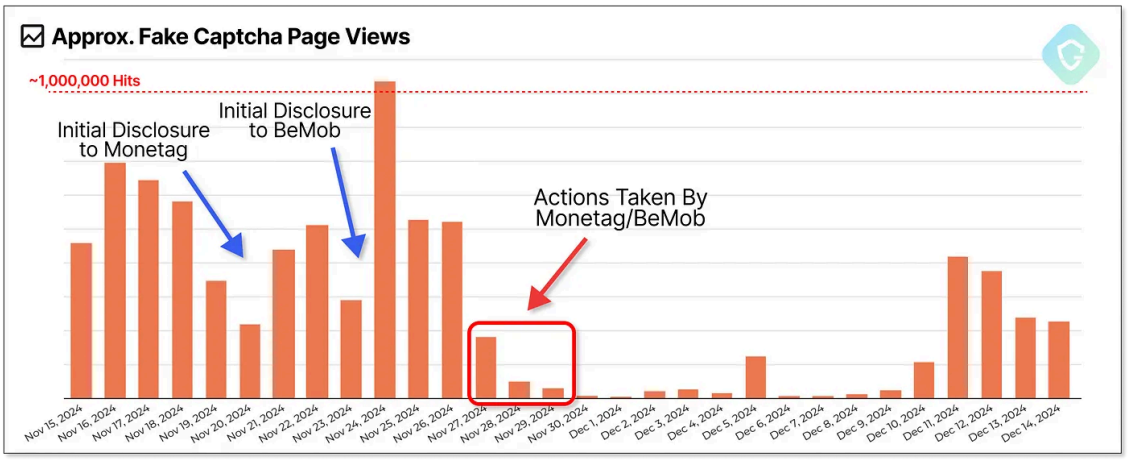
So, who is to blame? Who is turning a blind eye, acting irresponsibly, or perhaps even complicit? The reality is that responsibility is widely shared, but each player in this ecosystem has a convenient excuse:

- **The Ad Network** claims it cannot moderate the creative content because it's cloaked behind an ad statistics service. Yet, moderation post-approval, not just during initial configuration, is entirely possible.
- **The Ad Tracking Service** argues it's merely an analytics tool, leaving the advertiser and ad network responsible for the creative. With cloaking techniques, the advertiser can swap the creative after approval, avoiding detection.
- **The Publishers** insist they're simply monetizing their websites via third-party services like ad networks, distancing themselves from the malicious creatives delivered to their visitors.
- **The Hosting Services** that provide the infrastructure for these malicious pages largely claim ignorance. But are they also part of the willful negligence that perpetuates this ecosystem?

> This fragmented chain of ownership creates a perfect storm of plausible deniability, making it exceptionally difficult to pinpoint and enforce accountability. It's a system designed to shift blame while allowing malicious campaigns to thrive.

Responsible Disclosure

We reached out to Monetag and BeMob, disclosing all IOCs associated with their TDSs, and both acted to stop the campaign's propagation. Monetag, the primary propagation channel abused for this campaign, responded on November 28th, 2024, removing over 200 accounts linked to the threat actor. While this action effectively halted the campaign on their platform, it took eight days from our initial disclosure to implementation. Similarly, BeMob responded within four days, removing accounts used for cloaking. These swift actions highlight how quickly a major malvertising campaign can be dismantled when taken seriously.



Approx. Fake Captcha page views in the past 2 weeks: Disclosure Milestones

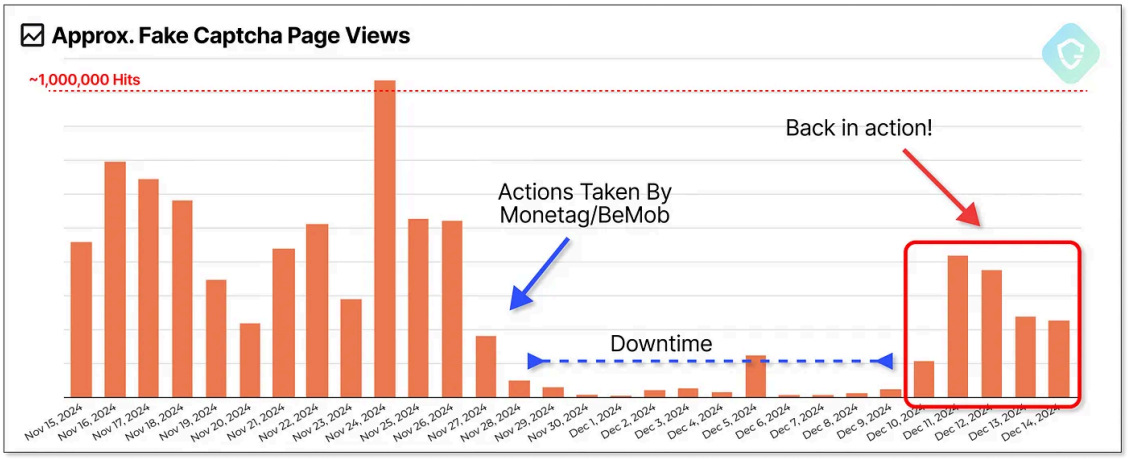
We appreciate Monetag and BeMob's prompt responses and willingness to act decisively. However, this campaign underscores the need for stronger proactive measures. Ad networks must prioritize ongoing content moderation, robust account validation to prevent fake registrations, and more accessible reporting mechanisms for the cybersecurity community. Waiting for external reports to address such abuses is not enough. These systems require continuous oversight to protect not just their clients but all internet users.

Monetag shared valuable insights about the threat actor's abuse of their network, including the use of falsified documents and hundreds of fraudulent accounts. Their official response is included below:

> "At Monetag, we take the security of our network, publishers, and users extremely seriously. Upon identifying malicious activities, we acted swiftly to ban over 200 accounts linked to the abuse. We remain committed to strengthening our defenses, working collaboratively with researchers like Guardio, and refining our processes to minimize abuse on our platform. The safety and integrity of our ecosystem are paramount, and we will continue investing in measures to mitigate threats effectively." **(Monetag)**

Lastly, if you noticed something curious in the activity graph above - you're not mistaken. The campaign may have paused for a few days, but its value to the threat actors proved too enticing to abandon. They're back — this

time leveraging both Monetag once again as well as other ad networks. Rest assured, we'll continue monitoring and addressing this evolving threat:



Approx. Fake Captcha page views in the past 2 weeks: downtime and resurrection

Final Thoughts

From deceptive publisher sites offering pirated or clickbait content to complex redirect chains and cloaking techniques, this campaign underscores how ad networks, designed for legitimate purposes, can be weaponized for malicious activities. The result is a fragmented chain of responsibilities, with ad networks, publishers, ad statistics services, and hosting providers each playing a role yet often **avoiding accountability**.

This fake captcha campaign is just one example that exposes the darker side of the internet's advertising ecosystem. While advertising is a cornerstone of the modern internet, the same ecosystem now faces a significant conflict of interest — **creating a security gap that leaves users vulnerable**.

At Guardio, we continuously reveal, track, and analyze attack vectors exploiting foundational internet traffic systems, with ad networks being a prominent example. The takeaway is simple: be cautious of websites offering ***FREE*** content you would otherwise pay for. As we always say — **there's no such thing as a free gift on the internet.**

IOCs

Fake Captcha Pages:

```
 ajmaboxanherulv1.b-cdn[.]net/JSKADull.html
ajmaboxanherulv2.b-cdn[.]net/JSKADull.html
anti-automation-v2.b-cdn[.]net/verf-v2.html
anti-automation-v3.b-cdn[.]net/verf-v3.html
anti-automation-v4.b-cdn[.]net/verf-v3.html
anti-automation-v5.b-cdn[.]net/verf-v5.html
anti-automation-v6.b-cdn[.]net/Recap-v6.html
arcivevaxue34.b-cdn[.]net
bmy7etxgksxo.objectstorage.ca-toronto-1.oci.customer-oci[.]com/n/bmy7etxgksxo/b/...
```

```
bmy7etxgksxo.objectstorage.sa-santiago-1.oci.customer-oci[.]com/n/bmy7etxgksxo/b/
bot-check-v1.b-cdn[.]net
bot-check-v2.b-cdn[.]net
bot-systemexplorer.b-cdn[.]net/recaptcha-v4-protocol-nov23.html
botcheck-encrypted-system.b-cdn[.]net/recaptcha-verification.html
check-cf-ver1.b-cdn[.]net/version3/cf-check.html
check-in-cf.b-cdn[.]net/verify/cf-check.html
dedicloadpgeing.b-cdn[.]net/dedicated-captcha-page.html
dedicloadpgeingv10.b-cdn[.]net/dedicated-captcha-page.html
dedicloadpgeingv11.b-cdn[.]net/dedicated-captcha-page.html
dedicloadpgeingv12.b-cdn[.]net/final-step-to-continue.html
dedicloadpgeingv2.b-cdn[.]net/dedicated-captcha-page.html
dedicloadpgeingv4.b-cdn[.]net/dedicated-captcha-page.html
dedicloadpgeingv5.b-cdn[.]net/dedicated-captcha-page.html
dedicloadpgeingv6.b-cdn[.]net/dedicated-captcha-page.html
dedicloadpgeingv7.b-cdn[.]net/dedicated-captcha-page.html
dedicloadpgeingv8.b-cdn[.]net/dedicated-captcha-page.html
dedicloadpgeingv9.b-cdn[.]net/dedicated-captcha-page.html
encryption-code-verification.b-cdn[.]net/recaptcha-verification.html
encryption-code-verification.b-cdn[.]net/verify-human-recaptcha.html
encryption-module-botverify.b-cdn[.]net/recaptcha-verification.html
file-typ-botcheck-v1.b-cdn[.]net/prove-human-recaptcha.html
file-typ-botcheck.b-cdn[.]net/prove-human-recaptcha.html
full-fast-movie-downloader.b-cdn[.]net/KH6kjsdNVk4sUIEW4klsw43ep8piJHOl.html
itechtics[.]com/hide-show-taskbar
izmncdnboxuse01.b-cdn[.]net/final-step-to-continue.html
izmncdnboxuse02.b-cdn[.]net/final-step-to-continue.html
izmncdnboxuse03.b-cdn[.]net/final-step-to-continue.html
izmncdnboxuse04.b-cdn[.]net/final-step-to-continue.html
izmncdnboxuse05.b-cdn[.]net/final-step-to-continue.html
izmncdnboxuse06.b-cdn[.]net/final-step-to-continue.html
izmncdnboxuse07.b-cdn[.]net/final-step-to-continue.html
newverifyyourself-system.b-cdn[.]net/recaptcha_verification-v1.html
newverifyyourself-system1.b-cdn[.]net/recaptcha_verification-new.html
nikutjyjgchr.b-cdn[.]net/RYFTGJcaptchv1.html
nikutjyjgchr.b-cdn[.]net/SYNCfuzzv2.html
nikutjyjgchrv21.b-cdn[.]net/SYNCfuzzv2.html
nikutjyjgchrv22.b-cdn[.]net/SYNCfuzzv2.html
nikutjyjgchrv23.b-cdn[.]net/SYNCfuzzv2.html
nikutjyjgchrv24.b-cdn[.]net/SYNCfuzzv2.html
nikutjyjgchrv25.b-cdn[.]net/SYNCfuzzv2.html
objectstorage.ap-mumbai-1.oraclecloud[.]com/n/bmy7etxgksxo/b/bucket-aws-vip/o/
objectstorage.ap-mumbai-1.oraclecloud[.]com/n/bmy7etxgksxo/b/buket-aws/o/
objectstorage.ap-mumbai-1.oraclecloud[.]com/n/bmy7etxgksxo/b/fetchbucket/o/
objectstorage.ap-mumbai-1.oraclecloud[.]com/n/bmy7etxgksxo/b/lusbucket/o/
objectstorage.sa-santiago-1.oraclecloud[.]com/n/bmy7etxgksxo/b/to-continue/o/
precious-valkyrie-cea580[.]netlify.app/recaptcha-sep-v2-1-baba.html
```

```
pub-7a0525921ff54f1193db83d7303c6ee8.r2[.]dev/verify-me-first-v1.html
sos-at-vie-1.exo[.]io/bucketrack/dir62/final/
sos-at-vie-1.exo[.]io/cloudcask/
sos-at-vie-2.exo[.]io/sanbuck/
sos-bg-sof-1.exo[.]io/amdbuck/
sos-bg-sof-1.exo[.]io/asgbuck/verify/hcaptcha-human-check.html
sos-ch-dk-2.exo[.]io/ataniya/bigot/
sos-ch-dk-2.exo[.]io/bucketofbits/modi-cloudflare-update-new.html
sos-ch-dk-2.exo[.]io/filebyte/
sos-ch-gva-2.exo[.]io/bytebin/
sos-ch-gva-2.exo[.]io/clouddesk/
sos-ch-gva-2.sos-cdn[.]net/bytebin/
sos-de-fra-1.exo[.]io/sandisk/step/
sys-update-botcheck.b-cdn[.]net/get-this-puzzle-solved.html
system-update-botcheck.b-cdn[.]net/security-challenge-captcha.html
upgraded-botcheck-encryption.b-cdn[.]net/verify-human-recaptcha.html
verification-module-v2.b-cdn[.]net/recaptcha_verification_updated.html
verification-module-v3.b-cdn[.]net/recaptcha_verification_updated.html
verification-module-v4.b-cdn[.]net/recaptcha_verification_updated.html
verification-module-v5.b-cdn[.]net/recaptcha_verification_updated.html
verification-module-v6.b-cdn[.]net/recaptcha_verification_updated.html
verification-module-v7.b-cdn[.]net/recaptcha_verification_updated.html
verification-module-v8.b-cdn[.]net/recaptcha_verification_updated.html
verification-module-v9.b-cdn[.]net/recaptcha_verification_updated.html
verifyyourself-newsystem.b-cdn[.]net/recaptcha_verification.html
verifyyourself-system.b-cdn[.]net/recaptcha_verification-new.html
weoidnet01.b-cdn[.]net/IQWJDolx.html
weoidnet010.b-cdn[.]net/IQWJDolx.html
weoidnet011.b-cdn[.]net/IQWJDolx.html
weoidnet012.b-cdn[.]net/IQWJDolx.html
weoidnet013.b-cdn[.]net/IQWJDolx.html
weoidnet015.b-cdn[.]net/IQWJDolx.html
weoidnet02.b-cdn[.]net/IQWJDolx.html
weoidnet03.b-cdn[.]net/IQWJDolx.html
weoidnet04.b-cdn[.]net/IQWJDolx.html
weoidnet05.b-cdn[.]net/IQWJDolx.html
weoidnet06.b-cdn[.]net/IQWJDolx.html
weoidnet07.b-cdn[.]net/IQWJDolx.html
weoidnet08.b-cdn[.]net/IQWJDolx.html
weoidnet09.b-cdn[.]net/IQWJDolx.html
ytgvjh65archi.b-cdn[.]net/
cloud-checked[.]com/cf/verify/{dddddd}/check
fiare-activity[.]com/cf/verify/{dddddd}/check
chromeupdates[.]com
marimarbahamas[.]me/downloads/index.html
cdn-downloads-now[.]xyz
fingerboarding[.]com/cha
```

```
restoindia[.]me/recaptcha/downloads
travelwithandrew[.]xyz/assets/index.html
foodrailway[.]cfd/tracker/index.php
```

BeMob campaign URLs used for Cloaking:

```
 https://addonclicks[.]com/go/aa22d074-412b-41b9-ba13-7dcf967019d9
https://addonclicks[.]com/go/b37e8c6f-ddee-4501-8a45-c5a466afee72
https://adstrails[.]com/go/3a2f0420-aa82-403a-a04e-4df13708bc04
https://adstrails[.]com/go/708fba2f-fbc0-45d0-831f-4e92054b1b73
https://adstrails[.]com/go/ac3d7719-d344-478a-b3b6-06bf5461f189
https://boltsreach[.]com/go/83afb110-50f2-4b29-a93e-15e37801c7e2
https://camplytic[.]com/go/7110a328-a727-4c2c-9e88-3a71adf76cb1
https://clickzstreamer[.]com/go/7110a328-a727-4c2c-9e88-3a71adf76cb1
https://clickzstreamer[.]com/go/cdff9f96-8cbd-4c44-b679-2f612a64cd00
https://clovixo[.]com/go/35b66391-3541-4d40-a116-52515cc39b9e
https://editorcoms[.]com/go/49b491b8-09d0-422d-8735-275dc82a37ca
https://editorcoms[.]com/go/dd423e06-1ace-4a1f-80be-1790bdbbe75d
https://fineclouding[.]com/go/0160ee85-0b3d-45cf-adbd-4801966ce1dd
https://fineclouding[.]com/go/134f0807-4dc8-4a61-895c-acf5107b611a
https://fineclouding[.]com/go/7ffe1a51-dc79-4e3f-ac7e-ab76c4741738
https://fineclouding[.]com/go/83a7f27f-d3ae-4935-b854-fdf492984ed3
https://fineclouding[.]com/go/e331e010-c671-4ea5-83c7-7518b2f08b7b
https://freeofapps[.]com/go/9f900112-9d2f-41f7-a8db-cd21dd738750
https://gamebalri[.]com/go/6818d61d-1f2e-4bc0-a98b-c63669acc41f
https://gawanjaneto[.]com/go/180f58b8-38df-46cb-a0d2-d6f12d8aa8a8
https://gawanjaneto[.]com/go/7b4c672a-7787-45cc-913b-1f2f9108d002
https://getcodavbiz[.]com/go/ce1c3e68-e155-4e87-992c-b66f1485aef9
https://glidronix[.]com/go/8eb5d9be-98ca-42c4-8185-090a299eb3ef
https://godagichi[.]com/go/10a84a68-b524-4885-adb2-bfbda4c17778
https://helpmemoverand[.]com/go/26131470-304e-4f6c-b6dc-1ffd5c5a9930
https://helpmemoverand[.]com/go/a895c485-d572-4e80-bd52-9dd3540c81d9
https://helpmemoverand[.]com/go/dc3ae9c2-de16-4dc0-b614-b0b36b81f319
https://impressflow[.]com/go/f7d8c7fb-c416-4972-94cd-2f1ede1bac38
https://insigelo[.]com/go/0e94e3bf-65a0-476a-b00e-5ababc6ff856
https://insigelo[.]com/go/96f84023-dd9d-4331-9788-5705babb7f0c
https://insigelo[.]com/go/fecdc64b-280d-4ee1-9f28-96efb38acb15
https://latestgadet[.]com/go/837d85a4-fda0-4b10-89c8-c840455acb25
https://linkspans[.]com/go/7110a328-a727-4c2c-9e88-3a71adf76cb1
https://mediamanagerverif[.]com/go/2bf025b9-52c0-4587-bf7f-9a8cdd459851
https://mediamanagerverif[.]com/go/9626641b-871b-45e1-b360-84e2767326cc
https://mediamanagerverif[.]com/go/d3aa1081-e2fd-4bc5-b168-5502eae928f1
https://mytecbiz.org/go/a8b87aed-1575-4d89-b503-974f4e932152
https://nettrilo[.]com/go/4c5443a1-ba90-487a-839a-b67a2b0317a8
https://nettrilo[.]com/go/708fba2f-fbc0-45d0-831f-4e92054b1b73
https://nowuseemi[.]com/go/e594bfab-e401-456c-a4fc-63d70055ff5b
```

```
https://offerzforu[.]com/go/7a343cf8-3eb1-4b24-9534-948f237f0941
https://offerztodayforu[.]com/go/61eba7aa-81b9-4836-9636-76b263f6f8cd
https://privatemeld[.]com/go/014e411a-91a4-44b3-9da2-5954404438dc
https://privatox[.]com/go/a391ee5e-c1f4-4654-90a8-f545126dc3a7
https://provenhandshakecap[.]com/go/3442df81-6329-4d47-8594-73a9455c5363
https://provenhandshakecap[.]com/go/c33549db-0cfb-4805-a3f6-64213cd4c3a9
https://provenhandshakecap[.]com/go/d2ce67cc-16c8-4a3a-938e-c3389b412786
https://purnimaali[.]com/go/b36d4019-1072-445e-8719-8fae7640ed7f
https://reachorax[.]com/go/2f3b2ad6-8c07-4095-ad09-89abc67a495d
https://regsigara[.]com/go/a78798ba-50d8-4cef-9a64-1bd0e917da8e
https://satisfiedweb[.]com/go/3710d145-158f-4faa-942f-467142fd9201
https://scrutinycheck.cash/go/180f58b8-38df-46cb-a0d2-d6f12d8aa8a8
https://scrutinycheck.cash/go/f94e2fd6-3569-4d2d-b596-5e07f79a5818
https://searchmegood[.]com/go/49c2dac8-63b7-46d9-a9f6-6ebdaa1ce3ee
https://searchmegood[.]com/go/897a19a7-2e55-408c-94a6-d82617b5361f
https://secureporter[.]com/go/c788f30c-9d6f-4fdd-96bc-1767e250f9c5
https://servinglane[.]com/go/83864c8d-2168-4d4e-bf47-b67a99e6178a
https://sheenglathora[.]com/go/3442df81-6329-4d47-8594-73a9455c5363
https://smartlinkoffer[.]com/go/15ef9db0-585b-4c85-9ffc-a2b6e81c4bfa
https://smartlinkoffer[.]com/go/6754805d-41c5-46b7-929f-6655b02fce2c
https://smartlinkoffer[.]com/go/b11f973d-01d4-4a5b-8af3-139daaa5443f
https://spotconningo[.]com/go/3119e6d0-9df0-4116-816f-0ff62631557b
https://startingdestine[.]com/go/ad3b65a2-9255-4017-a1e1-087bcca4e2ef
https://stephighs[.]com/go/34073388-1d3a-4671-804e-036143ad82e5
https://stephighs[.]com/go/4be1a5d1-14ab-44ae-bea7-d55de09afac0
https://stephighs[.]com/go/a8e78df0-c0cb-4d55-b4e9-48ed33fd2a6e
https://stephighs[.]com/go/ce1c3e68-e155-4e87-992c-b66f1485aef9
https://streamingsplays[.]com/go/1c406539-b787-4493-a61b-f4ea31ffbd56
https://streamingsplays[.]com/go/6754805d-41c5-46b7-929f-6655b02fce2c
https://streamingsplays[.]com/go/b11f973d-01d4-4a5b-8af3-139daaa5443f
https://streamingszone[.]com/go/b3ddd860-89c0-448c-937d-acf02f7a766f
https://tagsflare[.]com/go/0c3c343a-abfa-4467-b52d-0c20711b2d7e
https://taketheright[.]com/go/ee8430f6-c0db-4d47-95db-3fdcf5941225
https://techstalone[.]com/go/2bf025b9-52c0-4587-bf7f-9a8cdd459851
https://techstalone[.]com/go/9626641b-871b-45e1-b360-84e2767326cc
https://techstalone[.]com/go/d3aa1081-e2fd-4bc5-b168-5502eae928f1
https://tracksvista[.]com/go/b67f38ca-952b-44e3-b463-126a325e85c6
https://trailsift[.]com/go/5c881316-6dd0-46cb-b9aa-2d72b614d026
https://tunneloid[.]com/go/520c3874-eeb8-4f5c-bc79-849759f17715
https://vanshitref[.]com/go/e594bfab-e401-456c-a4fc-63d70055ff5b
https://verticbuzz[.]com/go/ca526b93-0797-4fd6-b107-fdf823a5badb
https://westreamdaily[.]com/go/2912600c-ec64-47fd-93cd-d7172bc29206
https://yourtruelover[.]com/go/76c79b3b-c3bd-409a-9f9d-d25f984b6ac5
https://yourtruelover[.]com/go/d05741b5-5782-4882-b0d0-d5cbf5c14f58
```

50 Most Active Publisher Domains Monetizing via Monetag:

```
 hianime[.]to
9animetv[.]to
aniwatchtv[.]to
sflix[.]to
myflixerz[.]to
hdtodayz[.]to
9minecraft[.]net
chapmanganato[.]to
y2mate[.]com
steamrip[.]com
y2meta[.]tube
tubemp4[.]is
moviesjoy[.]is
gomovies[.]sx
asuracomic[.]net
freek[.]to
flixhq[.]to
mangakakalot[.]com
coinpriceline[.]com
hurawatch[.]cc
movies2watch[.]tv
theflixertv[.]to
mangafire[.]to
z-lib[.]io
hydrahd[.]cc
cinego[.]tv
ouo[.]io
filecrypt[.]co
vipbox[.]lc
totalsportek[.]best
dopebox[.]to
sportshub[.]stream
manhwaclan[.]com
streameast[.]best
mangareader[.]to
kaido[.]to
megadb[.]net
mangabuddy[.]com
kisskh[.]co
bato[.]to
mangaread[.]org
manhuaus[.]com
gostream[.]to
alphatron[.]tv
readcomiconline[.]li
dramacool[.]bg
```

```
mixdrop[.]ps
e123movieswatch[.]com
totalsportek[.]games
aniwatch[.]to
travelmiso[.]com
```

Source: https://labs.guard.io/deceptionads-fake-captcha-driving-infostealer-infections-and-a-glimpse-to-the-dark-side-of-0c516f4dc0b6