CONFIANT

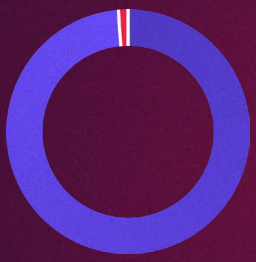
Malvertising and Ad Quality Index

The Foremost Benchmark Report on Digital Ad Quality, Security, and Privacy.

2024

January 1st - December 31st

CONTENTS

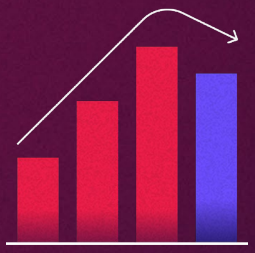


1 in 90

1 in every 90 ad impressions in 2024 was dangerous or highly disruptive to users.

0.21%

Progress: Industry-wide security violation rate dropped to 0.21%, ending a 3-year rising trend.



4x

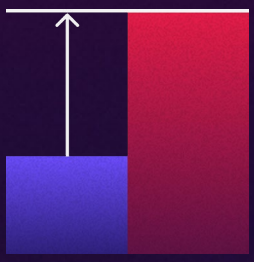
Browser wars: Firefox users were 4x more likely to experience security threats than Chrome or Safari users.

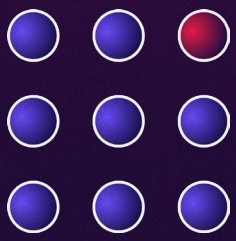
From 0.08% to 0.005%

The best security performance improvements: From 0.08% violation rates to an industry-leading 0.005%.

2.5x

Quality control: Ad quality violations surged, rising more than 2.5x from 0.63% in H2 2023 to 1.57% in 2024, driven by Heavy Ads.

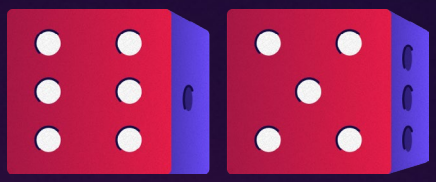




1 in 9

Record Breaking (not the good kind): One SSP recorded the highest daily security risk ever: 1 in 9 impressions were threats on May 14, 2024.

Google is moving in the right direction:
Its violation rates dropped from 0.93% to 0.88%.



Categories: Gambling was the most blocked, followed by Beauty Products, a category that skyrocketed out of Other in 2023

Rising Threat Actors in 2024

DCCBoost: Targeting desktop users with fake McAfee scareware pop-ups.

FizzCore: Specialized in cloaked investment scams using fake celebrity endorsements.

ScamClub: Expanded into video ads, injecting malicious JavaScript into VPAID content.

QuizTSS: 20% of all malicious impressions came from this top tech support scam network.

Top Threats

Forced Redirects

Fake Software Updates

INTRODUCTION

Welcome to Confiant's **Malvertising and Ad Quality (MAQ) Index**, the industry's first and leading benchmarking report on the security and quality issues affecting the digital advertising industry.

Our work with publishers, SSPs and DSPs gives us an unparalleled view into the entire digital ad ecosystem. Using a sample of hundreds of billions of impressions monitored in real time, this report answers fundamental questions about the state of the industry.

In 2018, Confiant released the industry's first benchmark report. This report, the 21st in the series, covers the entirety of 2024.

METHODOLOGY

To compile the research contained in this report, Confiant analyzed a normalized sample of more than **1 trillion advertising impressions** monitored from January 1 to December 31st, 2024, across tens of thousands of premium websites and apps from top publishers.

The data was captured by Confiant's **real-time creative verification solution**, which allows us to **measure ad security and quality on live impressions** (not sandbox scans) across devices and channels.

The violation rate is calculated by dividing the number of impressions exhibiting a particular issue by the total number of impressions monitored by Confiant.

Please note that in Q3 2020, we shifted from using U.S. to global data, necessitating a restatement of our results to allow quarter-to-quarter comparison. In H1 2022, we refactored our Quality score to remove an issue that was largely outside of the SSP's control. As a result, some historical metrics in this report may not match those in prior reports.

DEFINITIONS

Security Violations

Attempts to **compromise the user** through the use of malicious code, trickery, and other techniques.

Top issues include:

- **Forced Redirects**
- **Criminal Scams**
- **Fake Ad Servers**
- **Fake Software Updates**
- **High-Risk Ad Platforms (HRAPs)**[1]

Quality Violations

Non-security issues related to **ad behavior, technical characteristics,** or **content**.

Top issues include:

- **Heavy Ads**
  (including Chrome Heavy Ad Intervention)
- **Misleading Claims**
- **Video Arbitrage**
  (formerly In-Banner Video)
- **Undesired Audio**
- **Undesired Video**
- **Undesired Expansion**

[1] Ad platforms that consistently serve abnormal levels of malicious ads and are the preferred vector for malicious actors.

EXECUTIVE SUMMARY

For Confiant, securing the ad based internet means ensuring a better internet experience for users while maintaining a profitable business venture for advertisers, platforms, and publishers. This honest look at the state of ad quality and security across the ecosystem is meant to help push the industry in a positive direction and give AdTech professionals the knowledge they need to advocate for better ad quality and security practices.

The Good

Security and quality rates improved. In 2024, one in every 90 impressions was dangerous or highly disruptive to the end user. (in 2023, it was 1 in 79).

The industry-wide security violation rate broke its 3-year rising streak, lowering to a 0.21% average for 2024. Each quarter in 2024 was lower than the overall average in 2023.

The Bad

After falling from a high of 1.57% in Q4 2023, **the industry-wide quality rate rose again, reaching 0.93% in the second half of 2024**. The Quality rate is still very elevated compared to previous years, driven mostly by Heavy Ads.

Cloaking attacks, which surged at the end of 2023, have waned slightly—but they remain one of the year's top attacks.

Firefox remains the most vulnerable browser, with users more than 4x more likely to experience an issue than Chrome or Safari users.

The Ugly

Threat actors gravitated toward **scams featuring celebrities**, with FizzCore, eGobbler, and ScandalNewsNetwork launching fresh attacks featuring digitally altered images of injured stars.

Fake Updates/Downloads were the most consistent threat in 2024.

New threat actor DroidDrama put a sci-fi spin on the cloaked investment scam, targeting European users with robot ads and landing pages that impersonated reputable publisher sites.

CONFIANT

The State of the Industry

2024

In 2024, one in every 90 impressions was dangerous or highly disruptive to the end user.

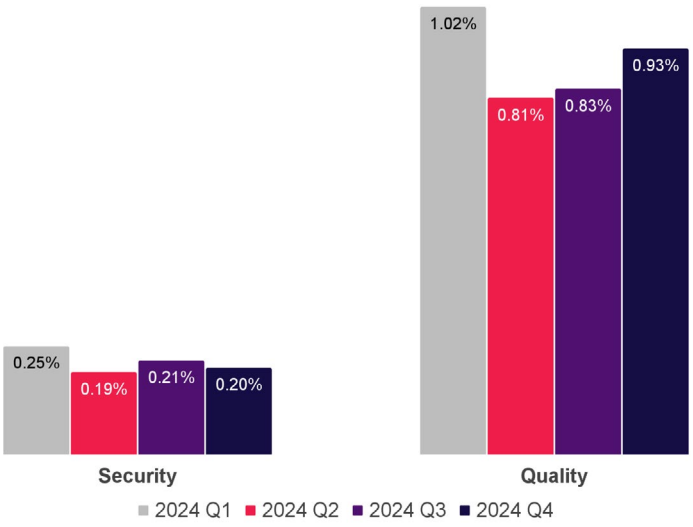
2024

AT A GLANCE

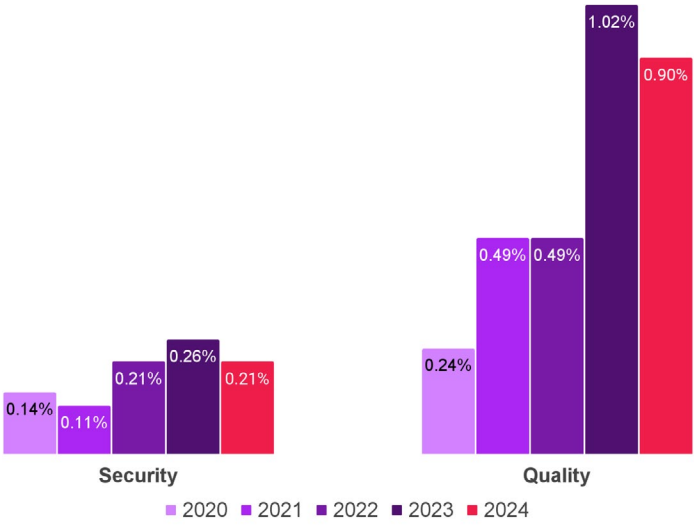
- **One in every 90 impressions revealed significant security or quality issues**.
- The **worst day** for security threats for each major SSP occurred in H1 2024.
- **SSP-H** is the first major SSP **to have underperformed in both security and quality since 2021**.
- **SSP-F claimed the top spot for both security and quality**.
- **Safari and Chrome users were over four times safer than Firefox users**, while Edge users were more than half as safe.
- Political Advertising has not appeared as a top blocked advertising category, even during the 2024 US Presidential Election, but the general News category has.
- On average, **one in every 476 impressions delivered in 2024 was a security risk to the user**.

How did the industry fare in 2024?

Quarterly view



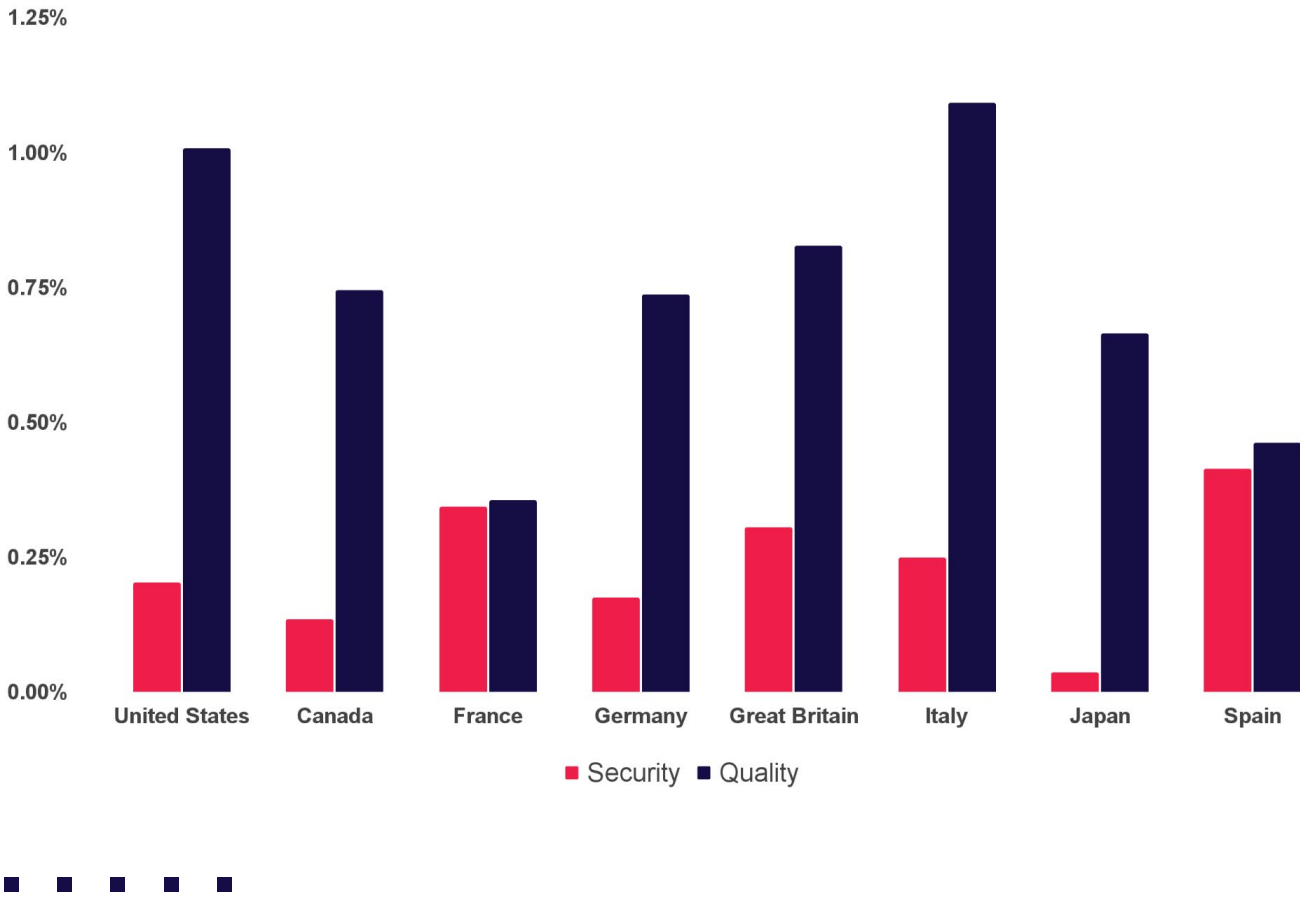
Annual view



The industry-wide security violation rate broke its 3-year rising streak, lowering to a 0.21% average for 2024. Each quarter in 2024 was lower than the overall average in 2023.

After falling from a high of 1.57% in Q4 2023, **the industry-wide quality rate started rising again, reaching 0.93% in the second half of 2024**. The Quality rate still very elevated compared to 2022 and previous years, driven by Heavy Ads.

Violation Rates by Country



Since 2023, every country experienced a shift, up or down.

Spain had the highest rate of Security issues for 2024, coming in at 0.41%. Canada and Japan were the safest markets.

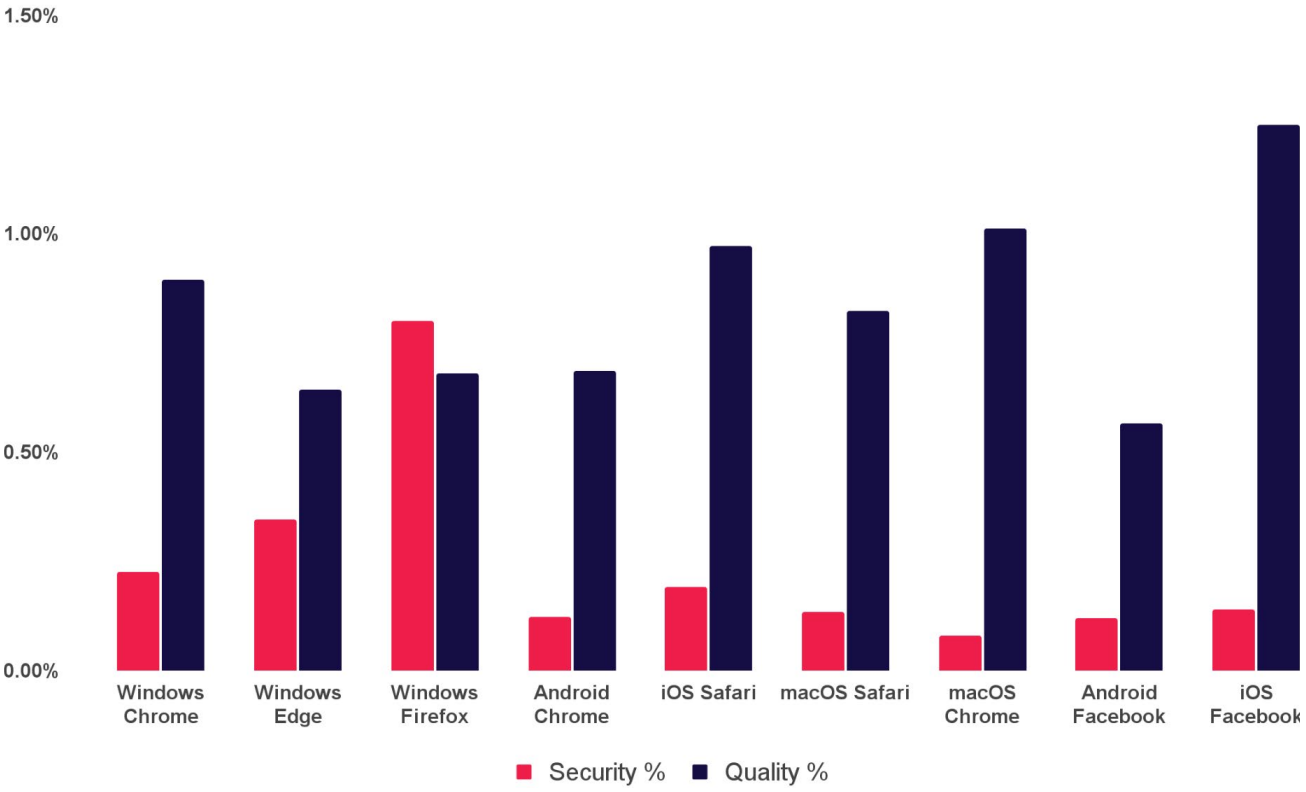
The Quality violation rate was highest in the USA, Great Britain, and Italy. Great Britain had both the highest Security and Quality violation rates in H1 2023, but improved in 2024.

While both are still below average for both rates, the USA and Great Britain have seen the relatively best improvement since 2023. Great Britain in particular saw their security rate halve and their quality rate drop by 30%. The USA is no longer worst in quality, nor 2nd worst in security.

Italy and Spain saw the worst shifts since 2023. Both of their security rates doubled, while their quality rates almost doubled as well.

Firefox users were more than four times more likely than Chrome and Safari users to experience a security issue in 2024.

Violation Rates by Browser

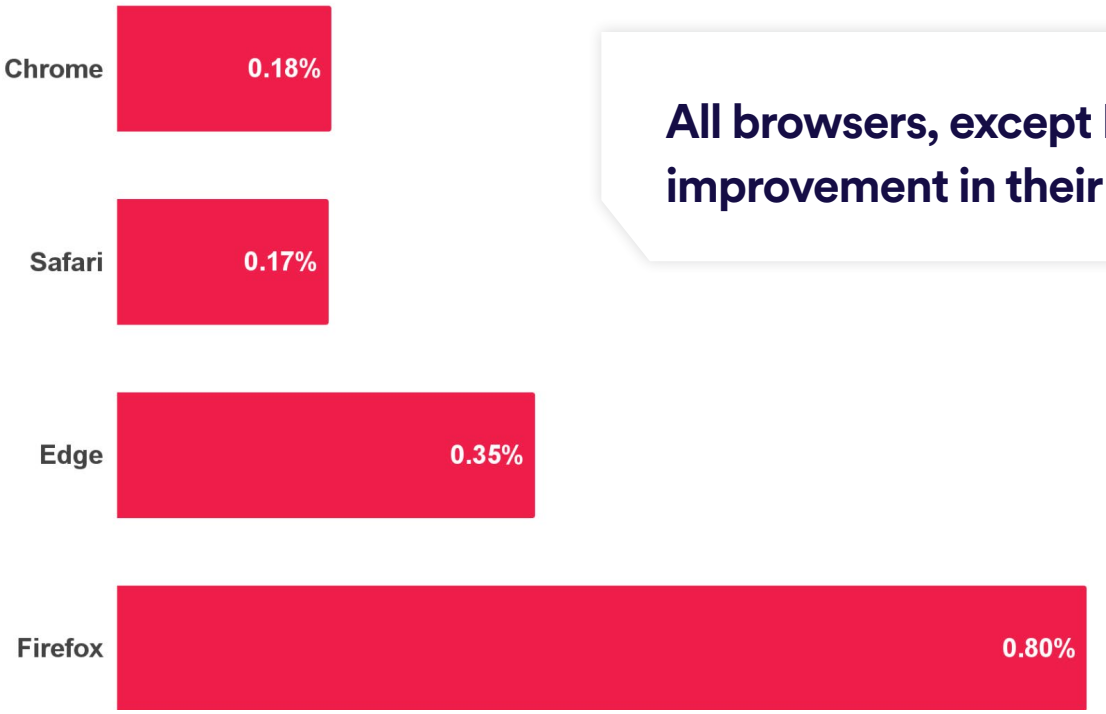


Users of Firefox for Windows experienced the highest rate of security issues. However, Firefox for Windows improved in the later half of 2024 while Windows Edge worsened, almost taking the top spot.

Conversely, **Chrome performed well for security issues across all platforms,** but not as well for quality.

Remarkably, the rates for all browsers stayed very consistent throughout the year.

Security Violation Rates by Browser Family



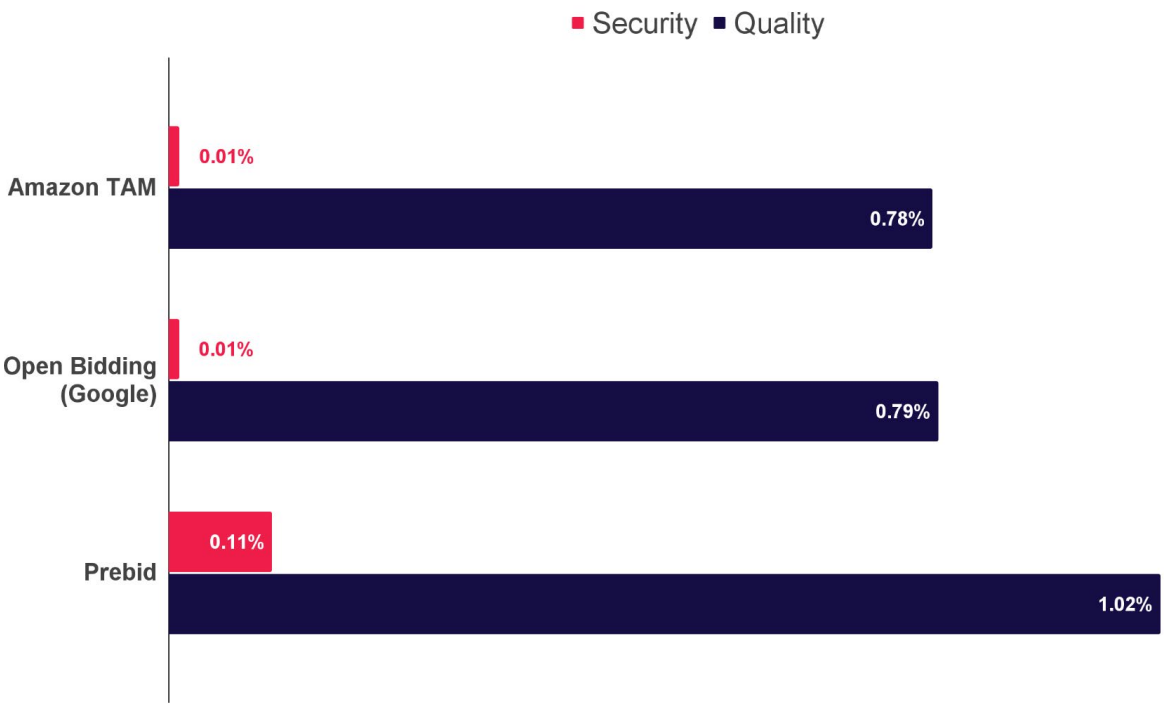
All browsers, except Firefox, saw an improvement in their security rates...

When browsers were grouped as a family across all operating systems and devices, interesting patterns emerged.

All browsers, except Firefox, saw an improvement in their security rates compared to 2023.

In 2024, Firefox users were the most impacted by security issues, continuing the trend it took over from Edge in H1 2023. **Safari and Chrome users were over four times safer, while Edge users were more than half as safe. Firefox's 2024 security violation average is 0.80%, an increase of just over 25% from its 2023 average, which already saw a dramatic 50% increase from 2022.**

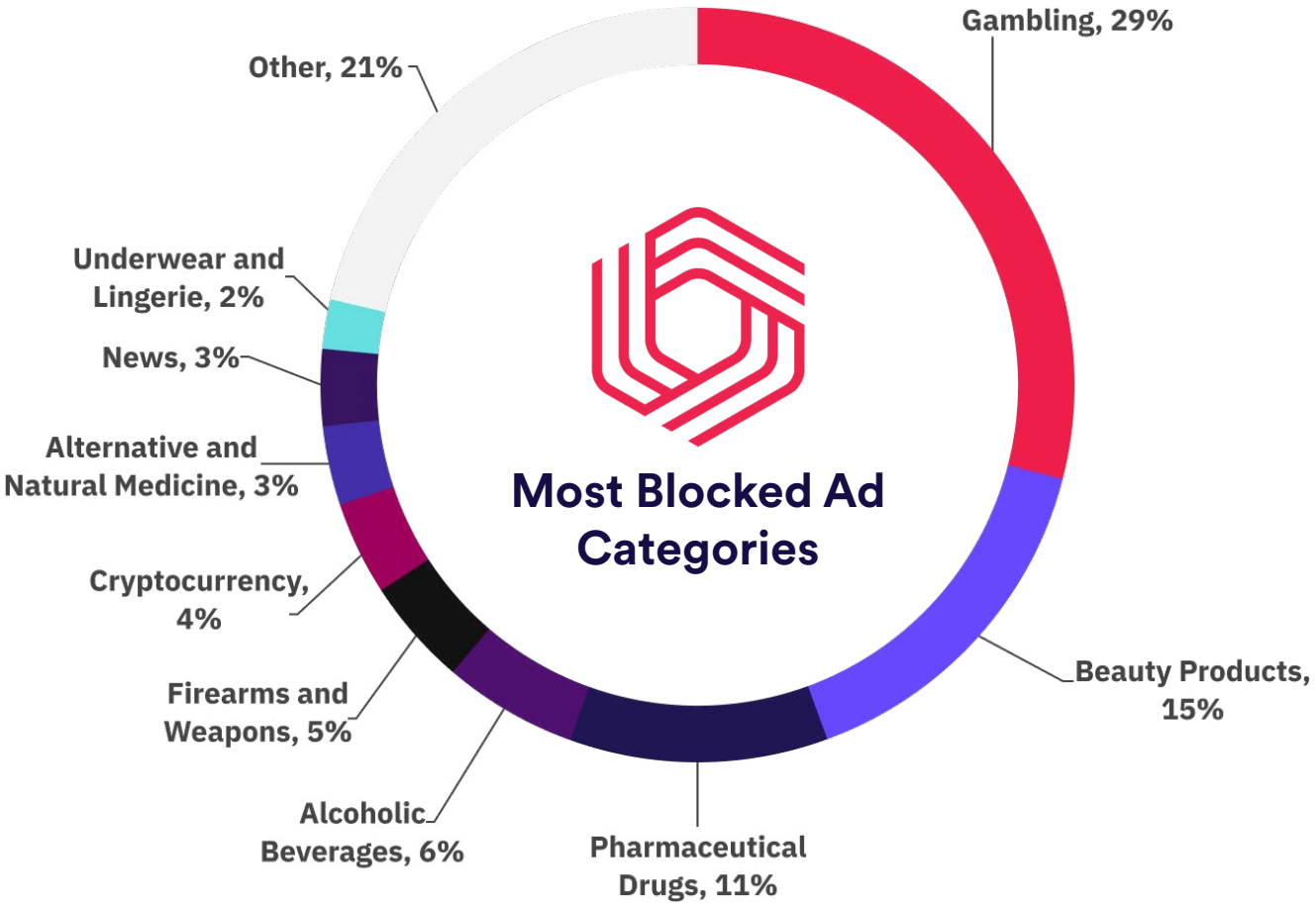
Violation Rates by Bidding Framework



Publishers use frameworks like **Prebid** and **Open Bidding** to manage bidding from multiple SSPs. In both cases, demand from a diverse set of SSPs flows through the framework, exposing publishers to security and quality issues.

Throughout 2024, Google and Amazon TAM were in a dead-heat for the best security and quality rates. Amazon TAM in particular saw a massive improvement in its quality rate since 2023, dropping from 1.81% to just 0.78%

All frameworks saw improvements in both their security and quality rates compared to 2023, except Prebid's quality rate, which ticked up a few points.



"Other" includes over 100 other categories

Confiant allows publishers to block creatives across 100+ different ad categories, including common verticals like Automotive and sensitive topics like Alcoholic Beverages.

In 2024, Gambling was the most blocked category, followed by Beauty Products. Alcohol and Pharmaceutical Drugs still remain top categories that are blocked. These four categories represent 61% of all blocks in 2024. **Gambling is still down from its all-time high 42% in 2022**.

Political Advertising has not appeared since 2022, despite an expected appearance for the 2024 US Presidential Election. Instead, the general category, News, has made its debut in the second half of 2024 with a respectable 3%.

CONFIANT

SSP Rankings

2024

SSP Rankings

In 2024, Confiant tracked impressions from over **100 SSPs and demand sources**. However, the majority of **global impressions originated from only 14 providers**[1] that are commonly used by publishers. These 14 providers[1] are noted in the charts that follow using a coding system that carries over from one quarter to the next to allow comparisons over time.

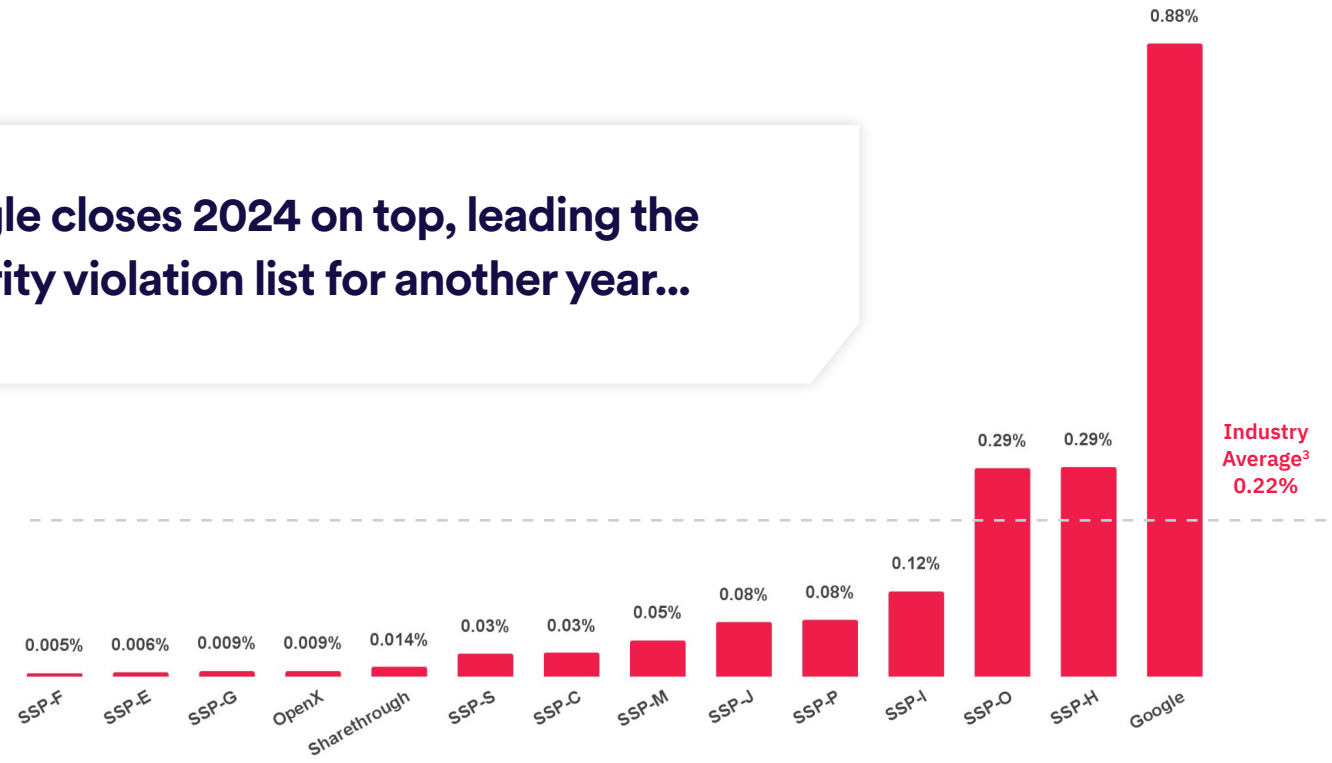
To qualify for inclusion, a provider had to have been a consistent source of **at least one billion Confiant-monitored impressions per quarter** across a cross-section of publishers in our global sample.

We identify three SSPs in these rankings: **Google, OpenX**, and **Sharethrough**. As the operator of the largest exchange, Google has access to data and resources beyond what's available to other exchanges. **OpenX** and **Sharethrough** have consented to have their names and their data included in our reports without obfuscation, which is an option we offer to any SSP upon request.

[1] Google, Magnite, TripleLift, OpenX, Xandr, Index Exchange, Pubmatic, Sharethrough, Sovrn, Yahoo, GumGum, Sonobi, Media.net, and YieldMo

Security Violation Rate by SSP

Google closes 2024 on top, leading the security violation list for another year...



[3] The weighted average across all SSPs based on impression volume.

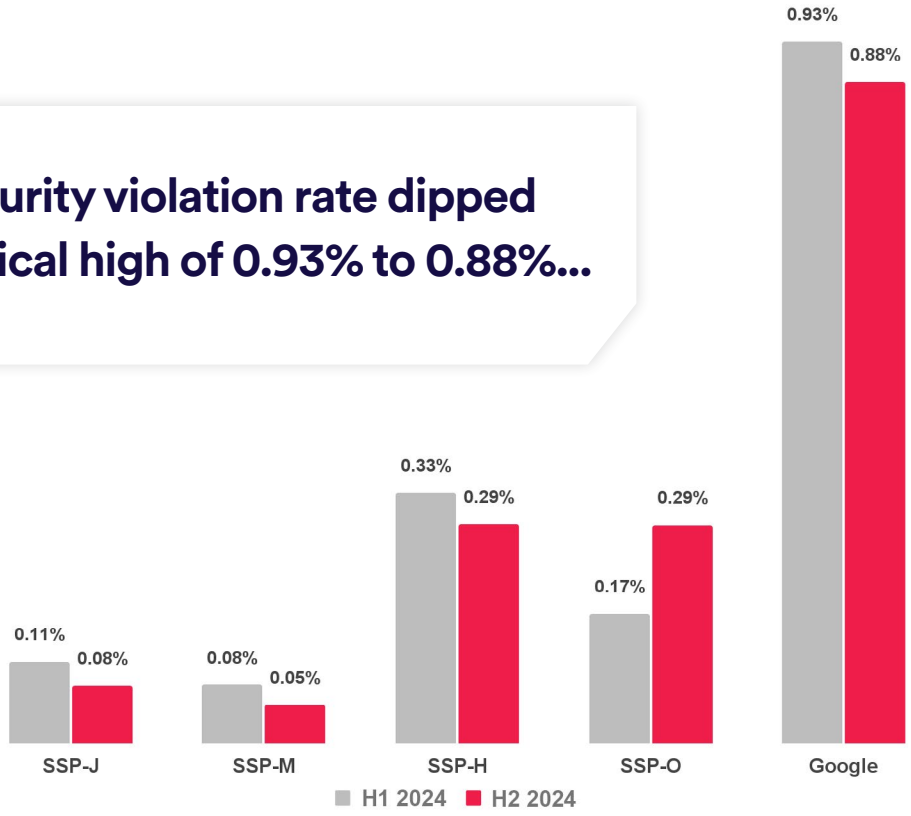
Google is down from its high in H1 2024, but it continues to struggle with high security violation rates.

SSP-O and **SSP-H** have seen a drop off since 2023, quickly rising from an honest 0.09% and 0.12% respectively to end the year in tie at 0.29%.

The SSPs with the lowest rate of security violations for the period were **SSP-F, SSP-E, SSP-G, and OpenX**, each achieving a rate of less than 0.01%, with **SSP-F taking the frontrunner position**. **SSP-F** had an incredible performance this year, shooting from the middle of the pack in 2023 with 0.08% to an astounding 0.005%.

Security Violation Rate: H1 2024 vs. H2 2024

Google's security violation rate dipped from a historical high of 0.93% to 0.88%...



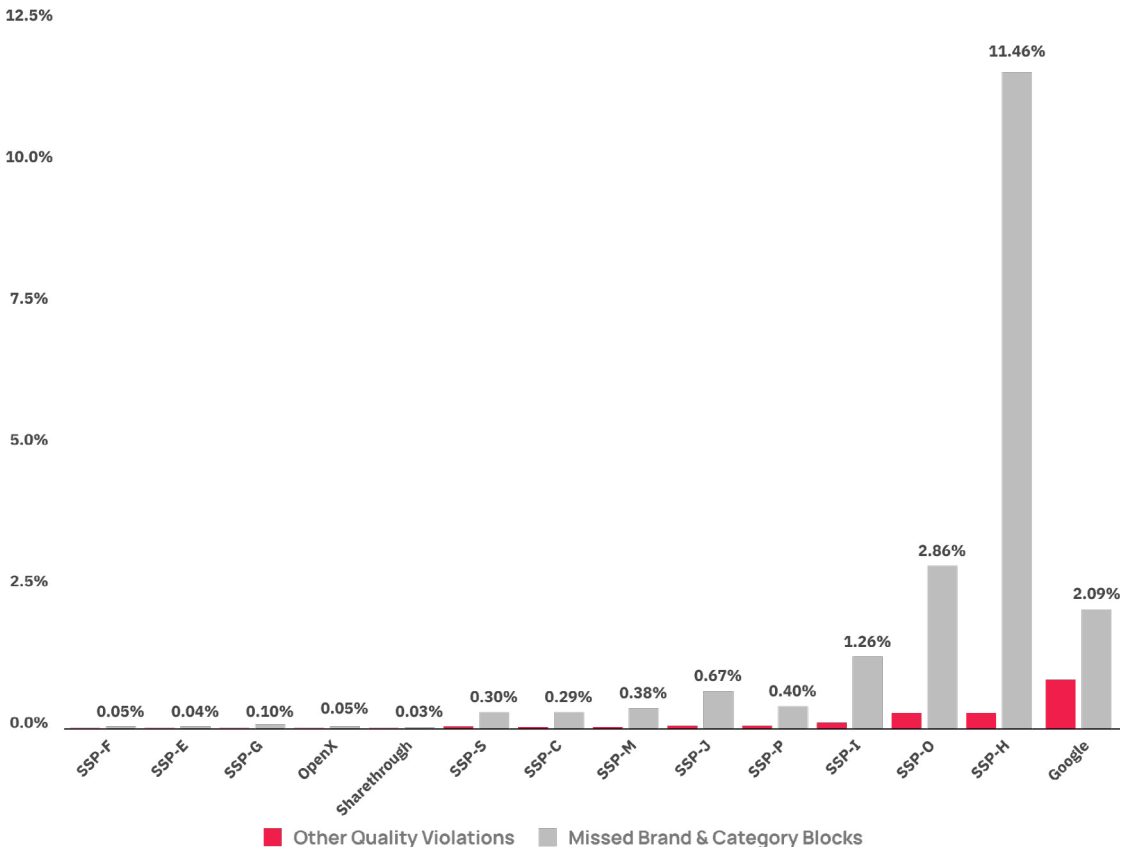
Google's security violation rate lowered from its historical high of 1% in H2 2023 to 0.88%. This heightened level is largely driven by Fake Software Updates and malicious downloads. These malicious campaigns optimize to stay within Ad Platform policies, and as a consequence are very prevalent, especially in Google Ads.

While **SSP-O and SSP-H** tied in the end, SSP-H had the tougher year.

Outside of the top performers, the only other two SSPs with noticeable improvements were **SSP-J and SSP-M**, dropping their security rates by a few points.

Daily Maximum Security Rate by SSP

Peak Date	
Sharethrough	2/24
OpenX	2/24
SSP-E	1/2
SSP-G	5/19
SSP-F	4/8
SSP-S	2/16
SSP-C	2/1
SSP-I	6/11
SSP-M	3/21
SSP-P	3/3
SSP-J	4/12
SSP-O	5/17
SSP-H	5/14
Google	1/5



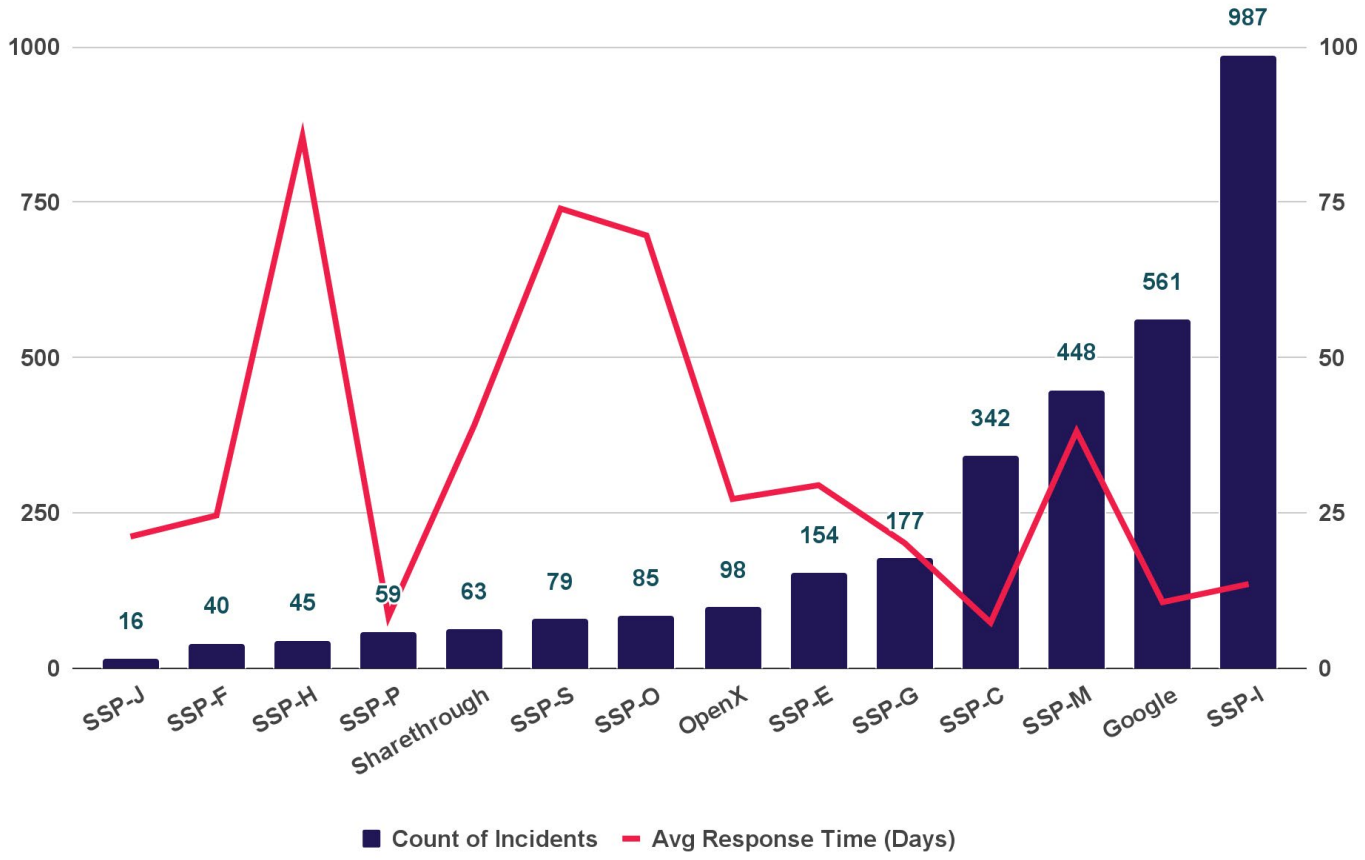
Averages can mask significant variation in day-to-day performance, so it's important to note the **upper bound of the security violation rate** for each SSP to get a sense of overall risk.

In 2024, **SSP-H, SSP-O, SSP-I, Google and SSP-O recorded the highest daily security rates by far**.

SSP-H set a staggering record at 11.45%, beating the full-year record held by SSP-O in 2023 of 3.11%. This means that **on May 14th 2024, more than 1 in 9 impressions from SSP-H had security issues**.

Remarkably, the first half of 2024 was so much worse for security issues, that the Peak Date for each SSP is unchanged from our H1 2024 Report!

Incidents and Average Response Time



SSPs differ in their ability to respond to attacks once they are underway. We measure how long it takes from when a threat first appears on an SSP to when it's last seen. On this measure, we see huge differences among the major SSPs.

With the security rate in 2024 generally improving from 2023, some SSPs recorded a lower yearly total of incidents, with cuts of up to 50% being common, but **SSP-J** saw a decrease of 80%!

SSP-F, boasting the best security performance in 2024, also performed very well in terms of incidents and response time.

However, the other side of the story was even more dramatic.

Google saw a 480% yearly increase from 116 to 561 incidents.

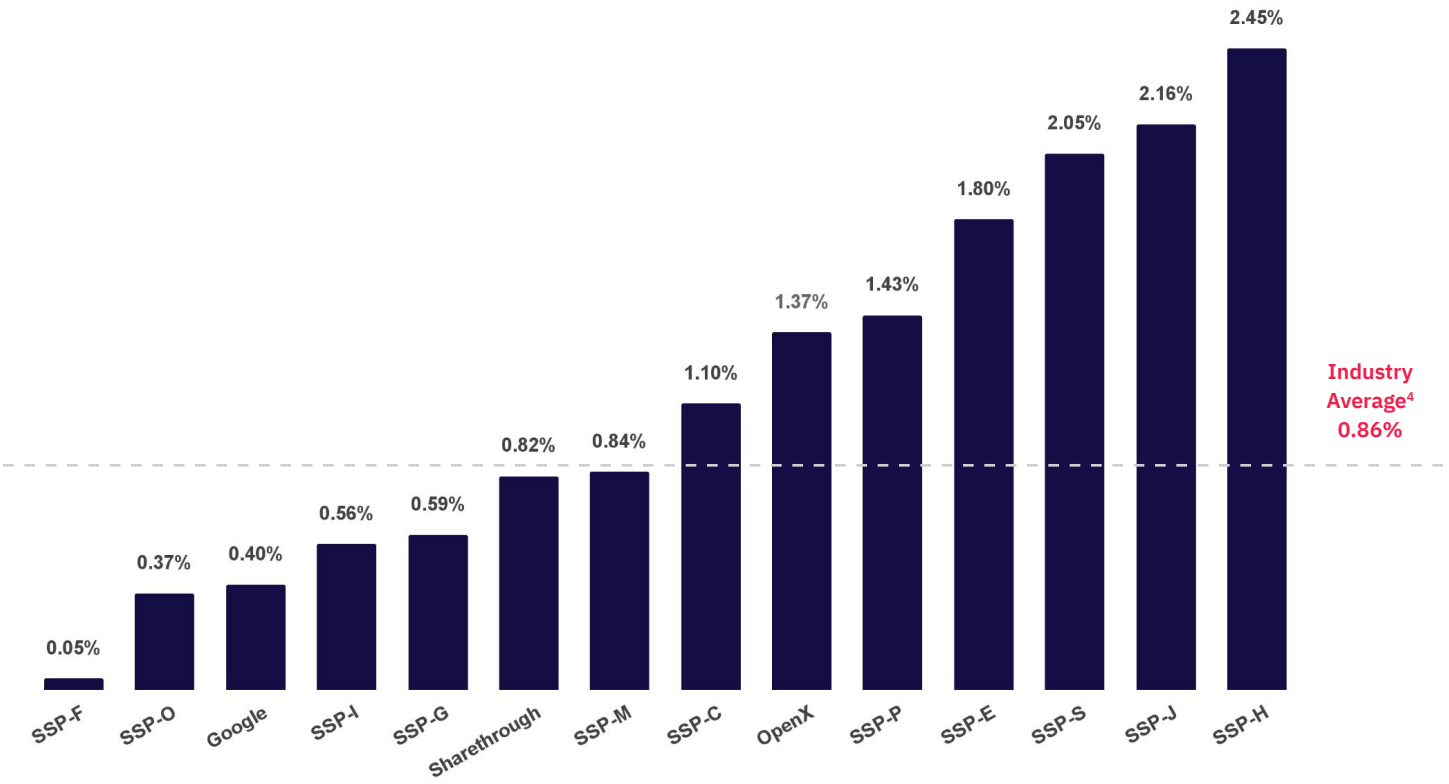
SSP-I saw a 350% increase from 291 to 987 incidents.

SSP-C and **SSP-M** saw increases between 250% and 300%.

Average response times generally worsened for SSPs with low incident counts, but the biggest winner in this category is **SSP-P**, dropping their response time from one month in 2023 to one week in 2024.

At first, the number of incidents and average response times usually had matching trends, but for multiple reports in a row, this has not held true.

Quality Violation Rate by SSP



[4] The weighted average across all SSPs based on impression volume.

Quality violations cover a diverse array of non-security issues that publishers can monitor on the Confiant platform. Examples include **Auto Video, Heavy Ads**, and **Misleading Claims**. These controls correspond to ad behaviors that disrupt or impair the user experience.

SSP-O, the previous year's best at 0.10%, still maintains second place at 0.37%.

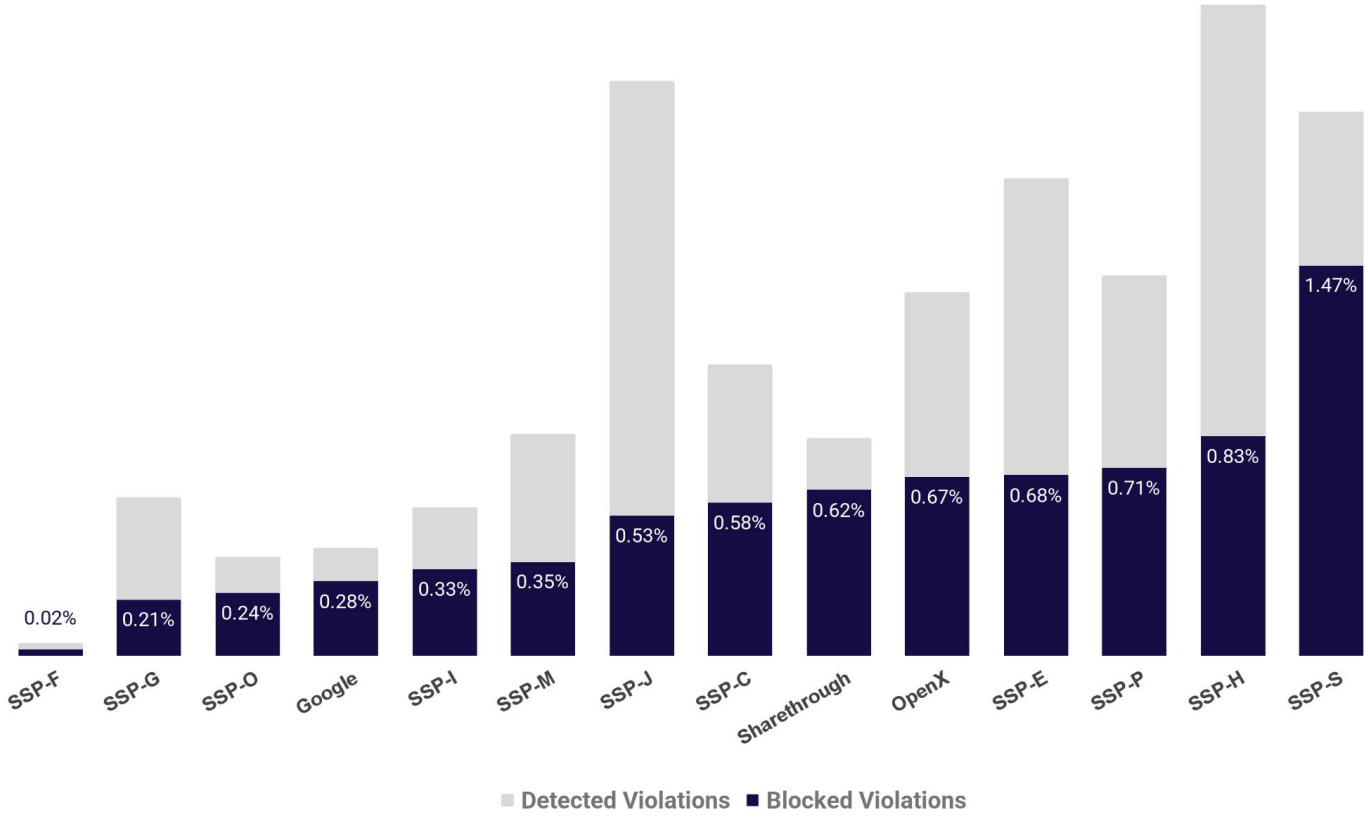
SSP-F claims a second crown, achieving an amazing quality rate of 0.05%. They impressively lowered their rate down from 1.47% in 2023.

SSP-C, while in the middle of the pack, is a big winner this year, cutting their quality rate by almost half of what it was in 2023. On the other hand, **SSP-S** saw their rate almost double.

Google has always performed strongly in quality, consistently keeping their rates below 0.50%

During 2024, 1 in 41 ads from SSP-H had quality violations.

Quality Blocks vs Detections by SSP



[4] The weighted average across all SSPs based on impression volume.

However, it's not entirely fair to rank the SSPs on quality without greater context. Since quality is subjective from Publisher to Publisher, Confiant grants its clients comprehensive customization to activate monitoring for quality issues in accordance with their business needs and expectations with their audience.

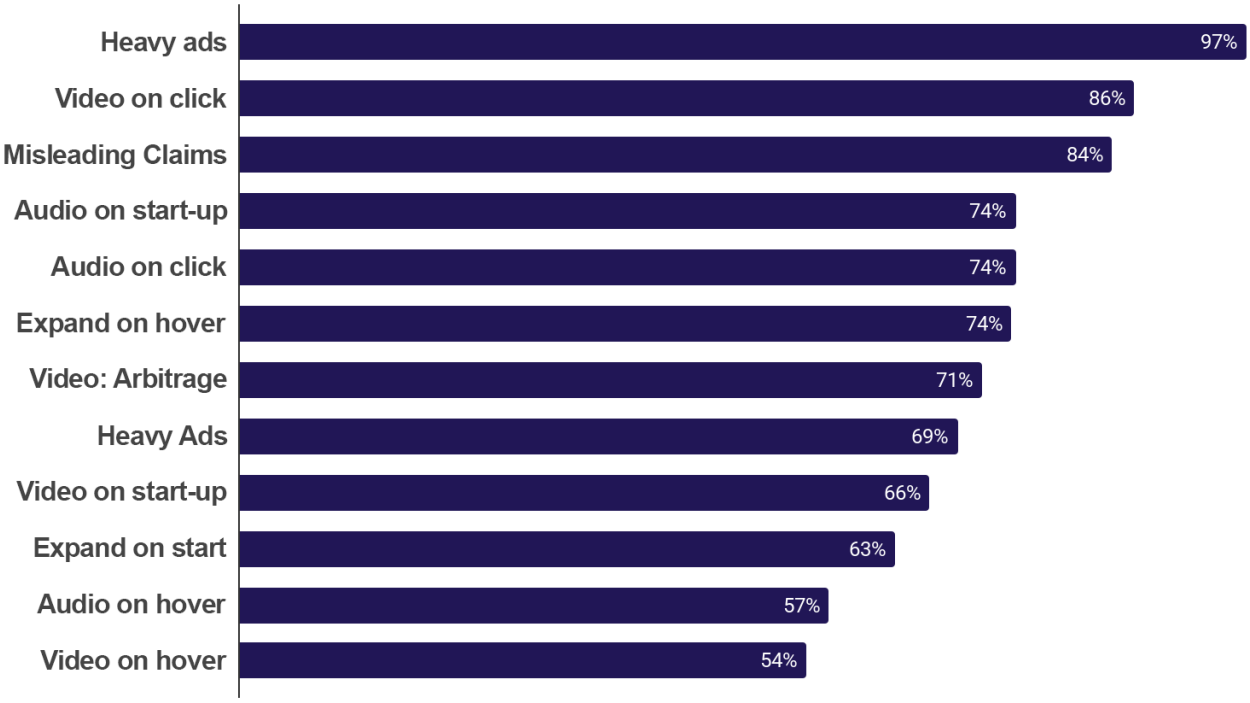
By categorizing quality violations between those that were blocked versus those that weren't, we can order SSPs once again by blocked impressions. By doing so, there are notable shifts in the ranking when ordering SSPs.

SSP-J enters the top half of performers, while **SSP-S** claims the last spot by a wide margin.

While the top SSPs remain largely unchanged, **SSP-G** sneaks into second place from fifth.

The best insight by this new categorization is the fact that only about half of quality violations are actually blocked. The rest of the impressions, while still violating a quality specification, were decided to not be blocked by the Publisher.

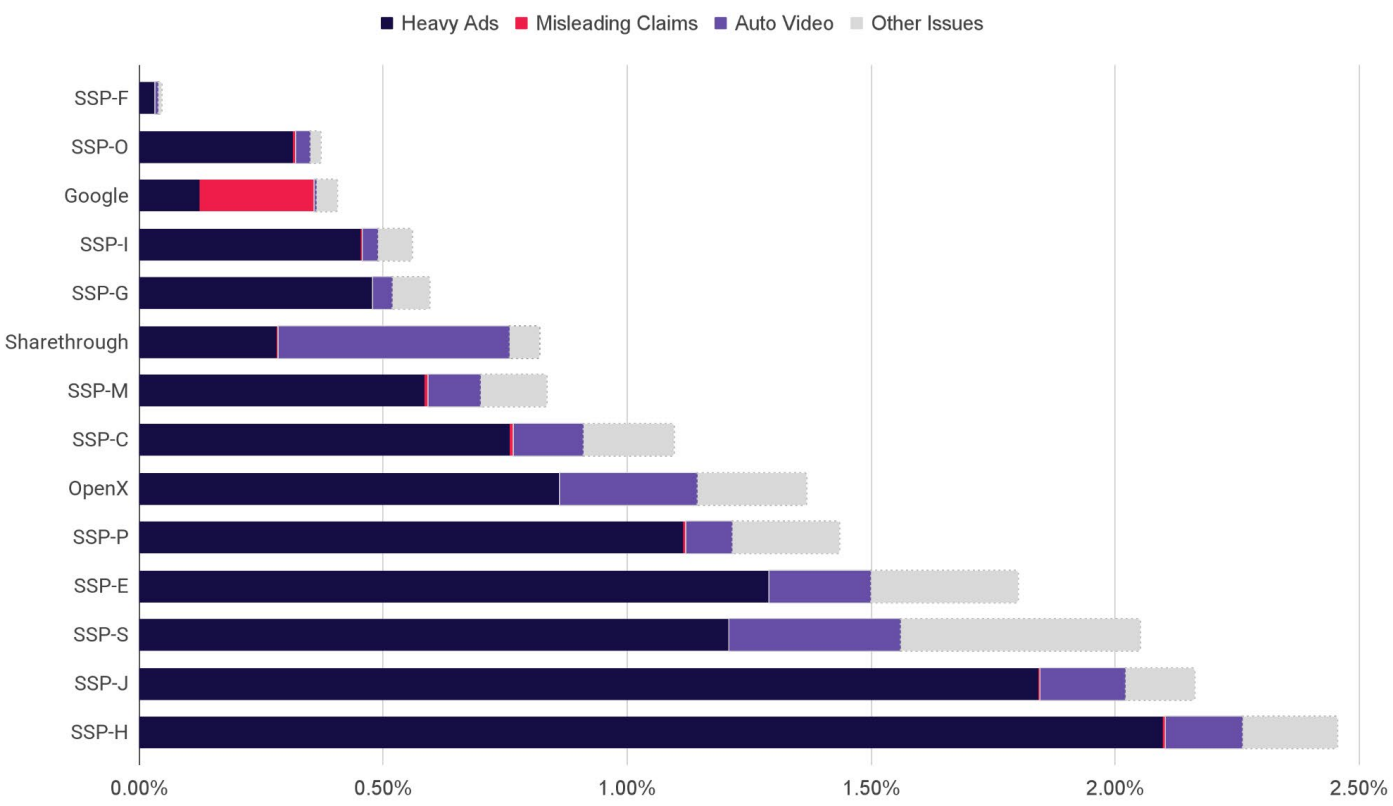
Quality Issue Activation Rates



This chart summarizes the rate at which various rules were activated by our Publishers for blocking across all impressions monitored by Confiant in 2024. It is a highlight list, not an exhaustive list, of Confiant's vast array of quality rules.

Unsurprisingly, **blocking activation rates tend to be higher for automatic creative behaviors** (e.g. Audio on start-up) than those requiring user action (e.g. Audio on click).

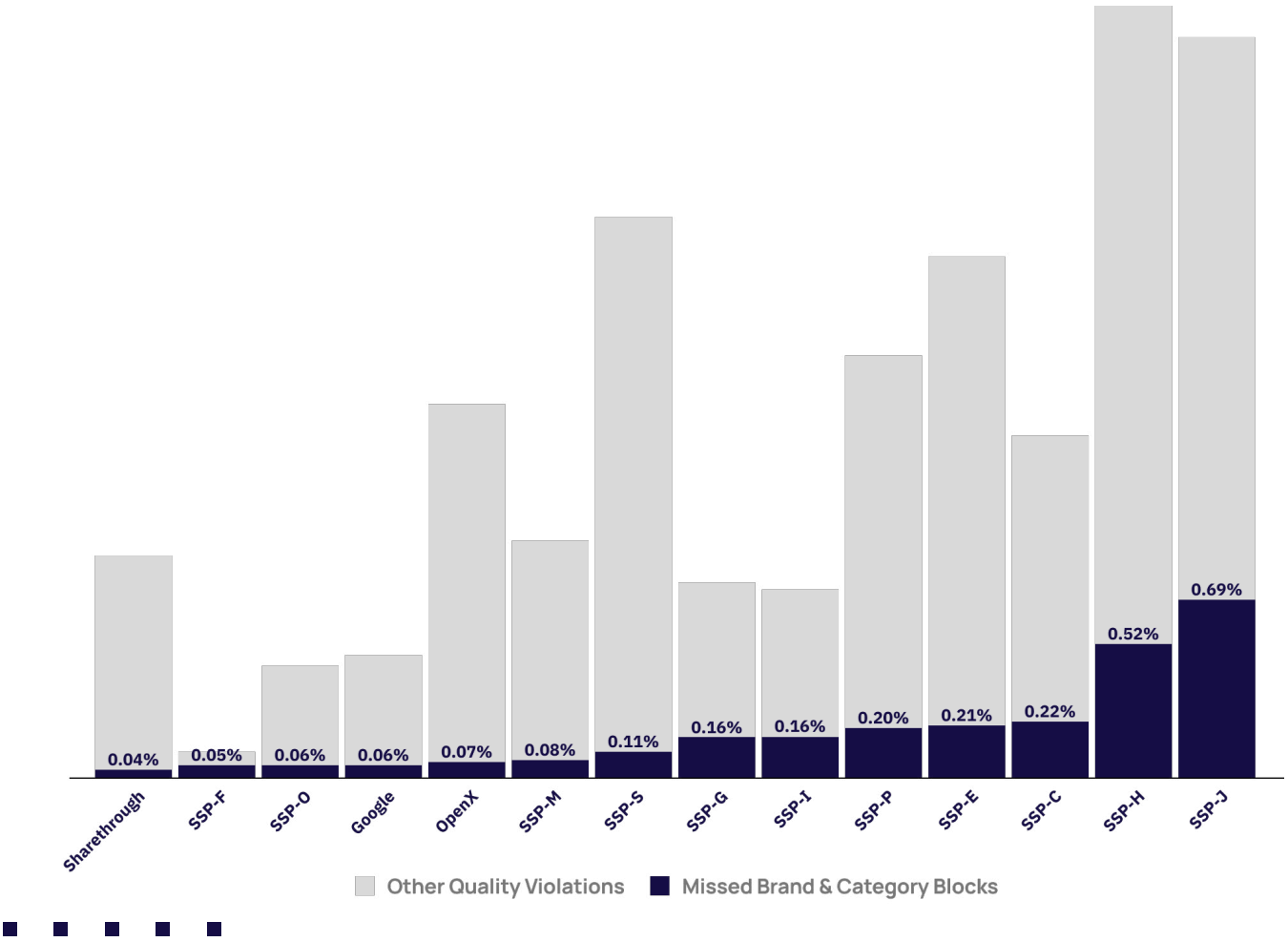
Quality Violation Detail



For nearly all SSPs, **Heavy Ads** — ads with characteristics like high network load, large number of unique hosts, or Chrome Heavy Ad Intervention — were consistently the most common quality issue. Display ads that **auto-play video** without any user interaction were also quite common.

Misleading Claims — ads that use misleading language or imagery to garner clicks or sell products and services of dubious quality — was still the largest issue for Google, maintaining a rate over 50%.

Missed Brand/Category Blocks



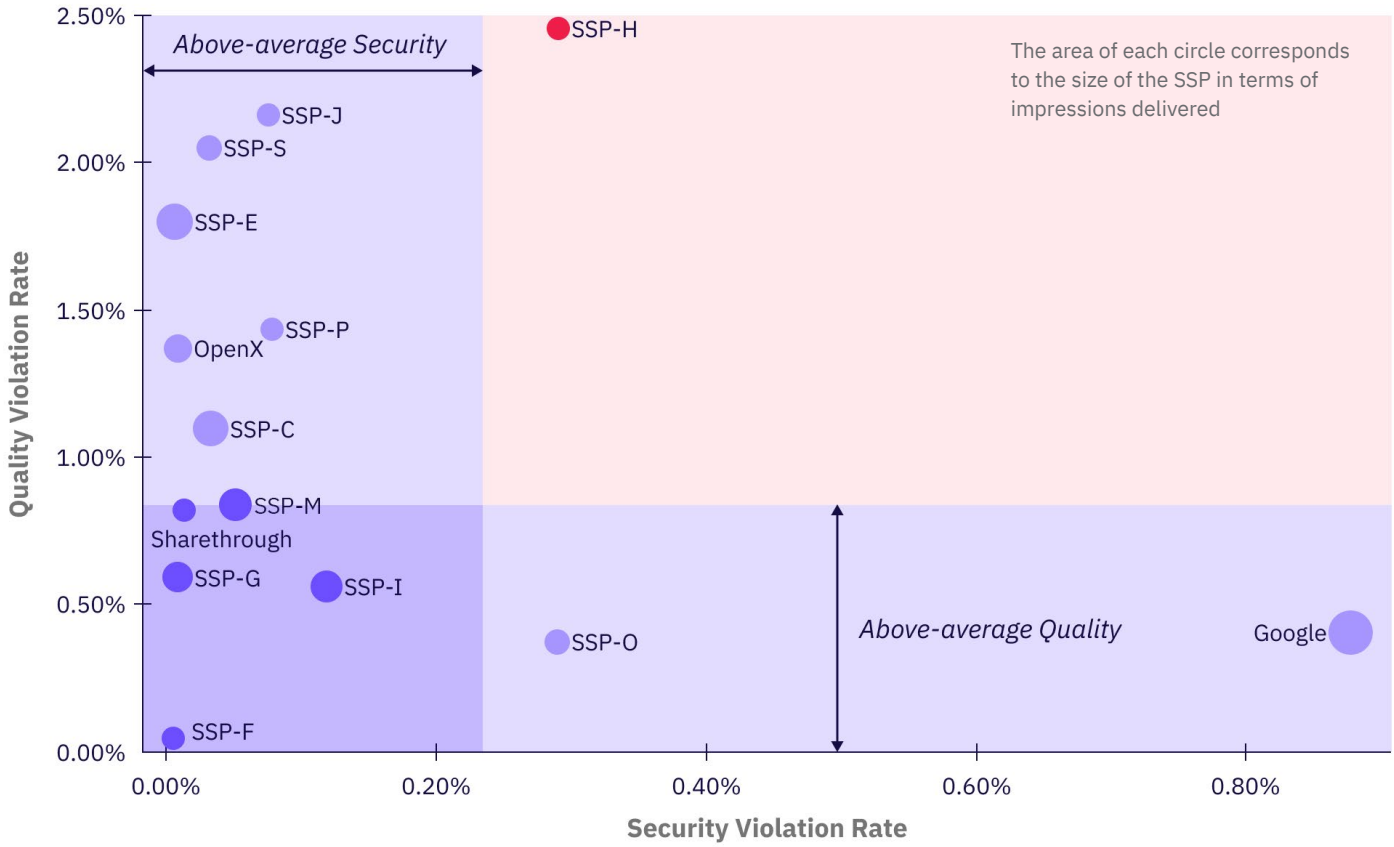
Publishers rely on SSPs as their first line of defense against ads associated with **unsuitable brands and categories**. However, these controls are not always effective.

SSP-J and **SSP-H, both in last for the quality rates, also had the highest rate of blocks for brands and categories requested by Confiant publishers**.

Sharethrough leads the pack, having the lowest rate of blocks for brands and categories.

Sharethrough leads the pack, having the lowest rate of blocks for brands and categories...

Violation Rates by SSP



Five SSPs had better-than-average performance for both security and quality: Sharethrough, SSP-G, SSP-M, SSP-F, and SSP-I, the first three maintaining their positions since 2022.

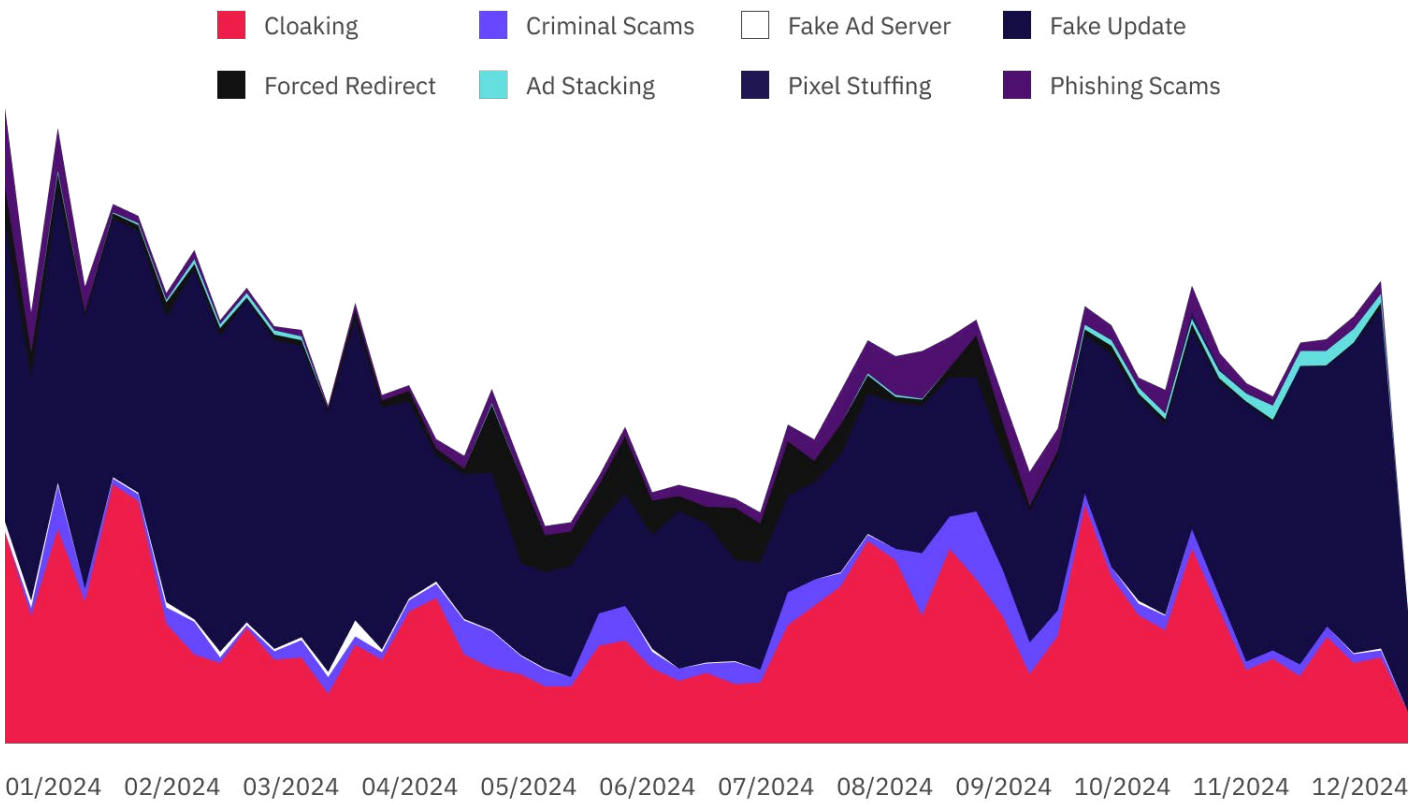
All other SSPs performed well on one measure but not the other, except for **SSP-H**, the first major SSP to have underperformed in both categories simultaneously since 2021.

CONFIANT

Major Threat Activity

2024

Threat Detail



The nature of security threats shift constantly as attack techniques fall in and out of favor.

While **Fake Updates** and **Cloaked Ads** swapped the top spot several times, there was a surge of **Forced Redirect** activity in late Spring and **Ad Stacking** in Q4.

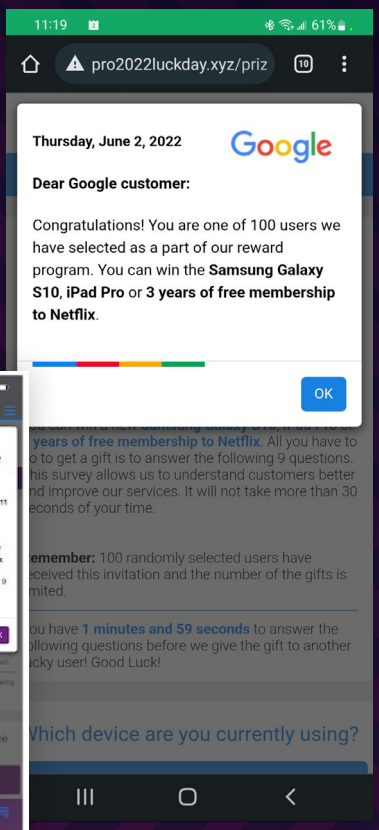
Fake Updates/Downloads was the most consistent threat in 2024.

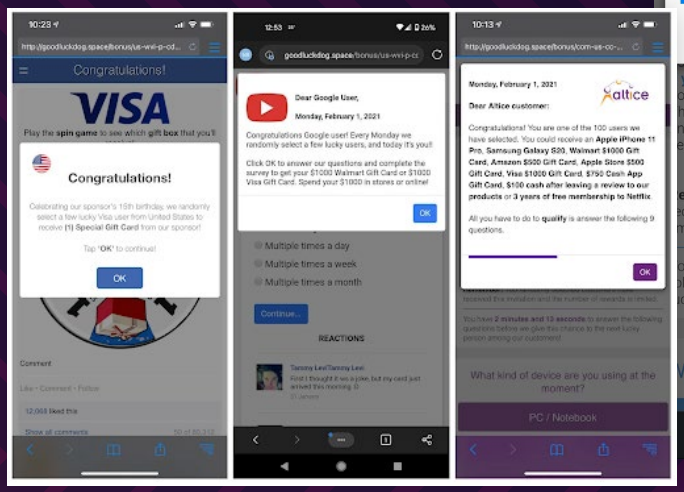
There was a surge of **Forced Redirect** attacks from late August to the end of September.

SCAMCLUB

ScamClub uses forceful redirects to silently lead users to harmful websites....

Take-Down Target





Category:

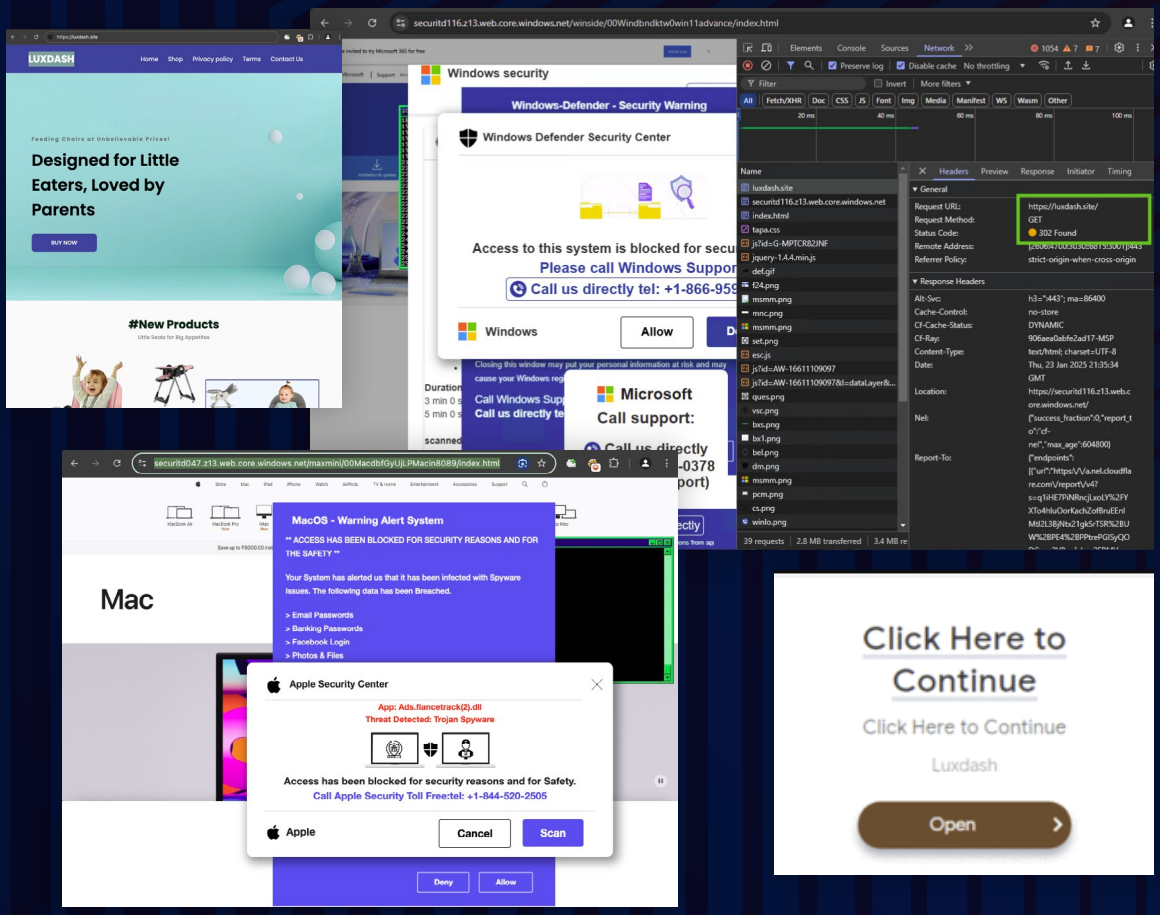
- **Cloaking**
- **Criminal Scams**
- **Fake Ad Servers**
- **Forced Redirects**
- **Phishing Scams**

Highlights: ScamClub uses forceful redirects to silently lead users to harmful websites, often featuring scams like Scareware and fake giveaways.

TA Description: ScamClub primarily uses forceful redirects to subtly lead users to harmful websites, often involving Scareware, fraudulent gift card schemes, carrier-branded scams, and giveaway scams. They expertly infiltrate established advertising networks, bypassing standard security measures to reach a wider audience. Recently, ScamClub has advanced its strategy by incorporating video ads, signaling a shift toward increasing their revenue streams. By embedding malicious JavaScript into conventional VPAID (Video Player-Ad Interface Definition) ads, they manipulate video content for malicious purposes in a simple yet effective way. In September 2023, Confiant published a threat intelligence and takedown report on ScamClub, enabling coordinated actions to dismantle its supply chain. ScamClub had been exploiting browser vulnerabilities, including CVE-2021-1801, CVE-2021-23957, and CVE-2021-5840, all of which were identified and reported by Confiant.

QUIZTSS

Big Button ads that send victims to fake infection pages with tech support scams....



Category:

Cloaking

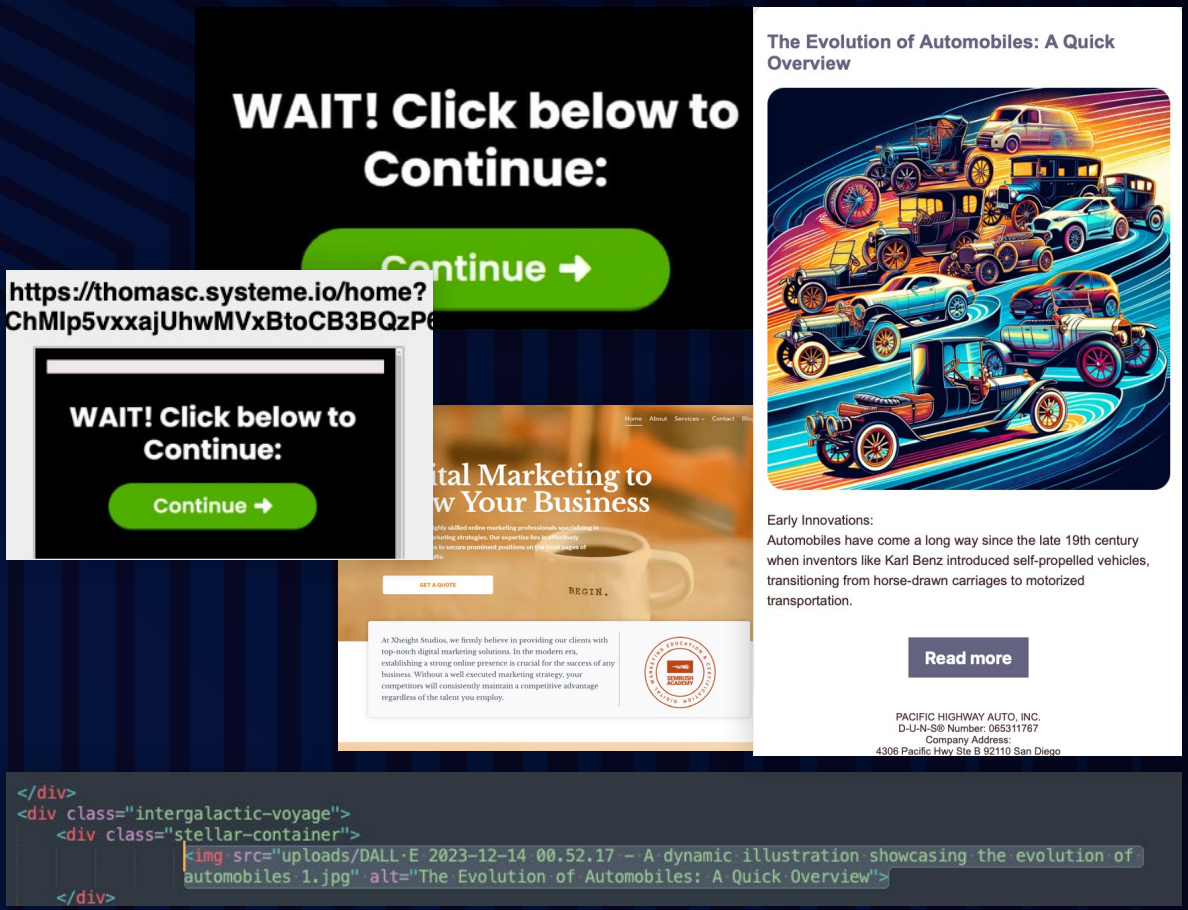
Criminal Scams

Highlights: Extremely adaptive. QuizTSS's large impression volume creates a need for constant adjustment of its ads, cloaked pages, and its TSS to break through ad security mechanisms. We see development and new clusters pertaining to QuizTSS activity regularly.

TA Description: Big Button ads which sends victims to a fake infection pages with leads tech support scams.

QUIZTSS

Generative AI based content strategy resulting in cohesive messaging on cloaked landing pages....




```
</div>
<div class="intergalactic-voyage">
    <div class="stellar-container">
                <img src="uploads/DALL·E 2023-12-14 00.52.17 – A dynamic illustration showcasing the evolution of automobiles 1.jpg" alt="The Evolution of Automobiles: A Quick Overview">
    </div>
```

Category:

Cloaking

Criminal Scams

QuizTSS 2024 Common Tactics:

- Generative AI based content strategy resulting in cohesive messaging on cloaked landing pages

- Borrowed assets from digital marketing and SEO websites to establish a unique cluster of cloaked websites.

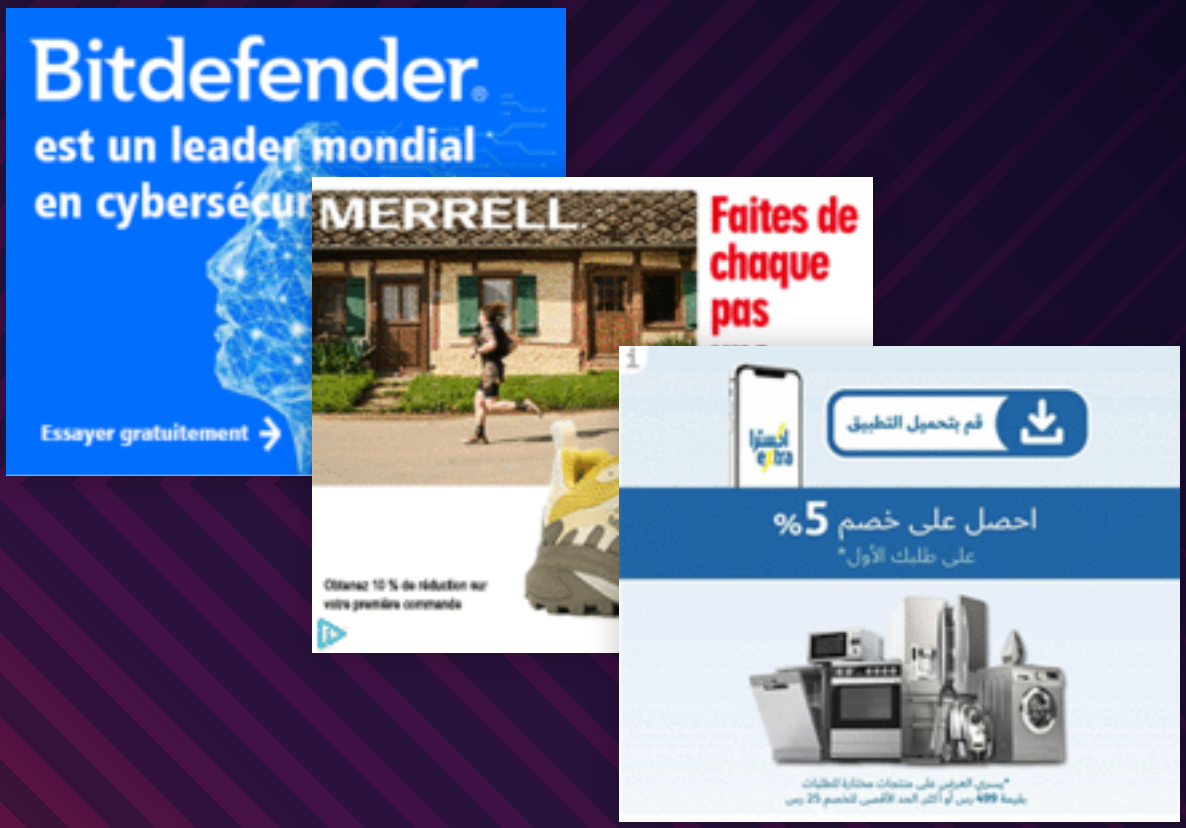
- Individual ad campaigns targeting landing pages with siloed infrastructure leveraging hosted web site builders.

- Iterative ad copy that circumvents previously blocked content targeting this specific threat.

- Stolen content from Shopify web stores that are used for cloaked pages.

MUTANTBEDROG

MutantBedrog uses client-side fingerprinting and forced redirects to lead users to scams...



Category:

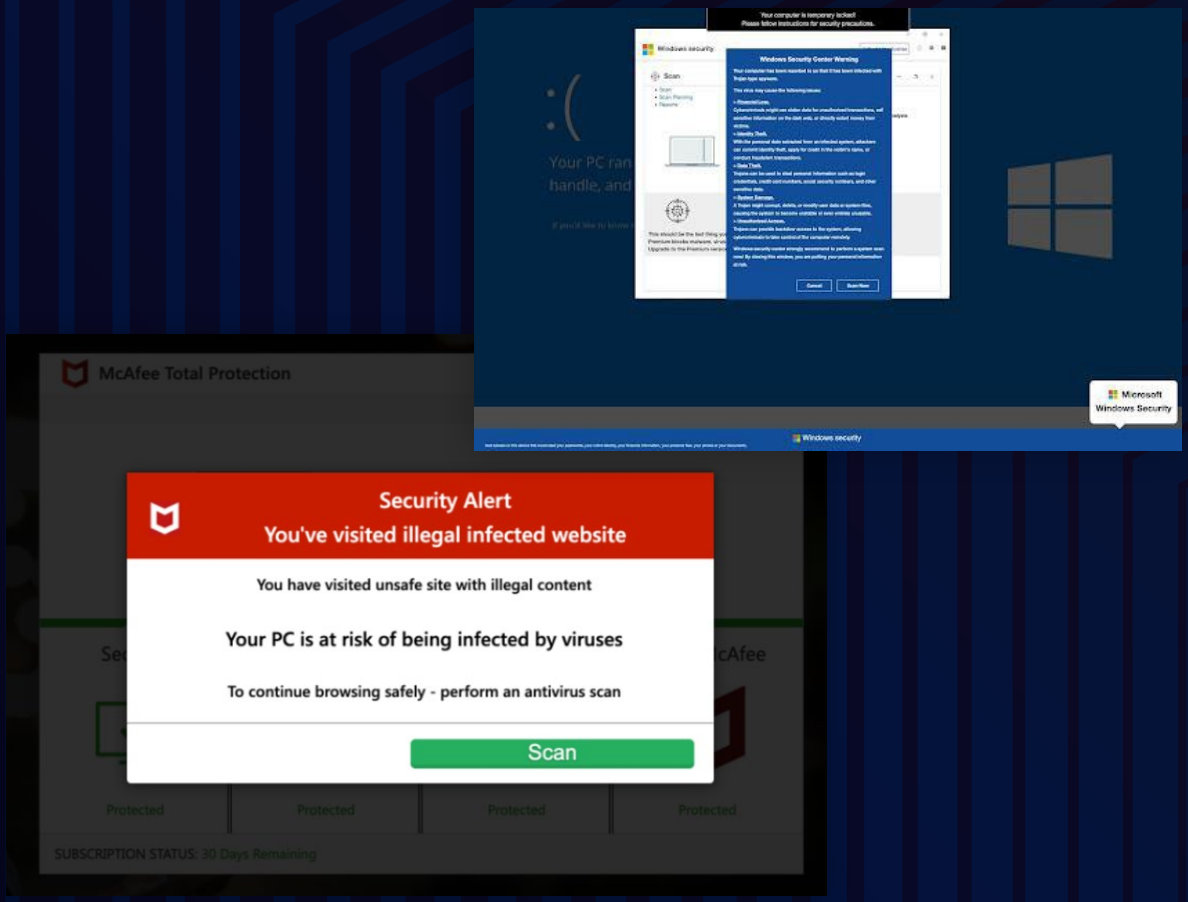
Cloaking
Criminal Scams
Fake Ad Server
Forced Redirect

Highlights: MutantBedrog uses client-side fingerprinting and forced redirects to lead users to scams. MutantBedrog is highly adaptive, changing and adding new techniques rapidly.

TA Description: MutantBedrog uses forced redirects to lead users to giveaway scams. Well-known brands are abused in the creatives and loads malicious, heavily-obfuscated Javascript that does client-side fingerprinting of the user's browser. It checks for things like language, if the device is a mobile device and is NOT plugged in, and in one of its iterations even uses steganography to hide its malicious code. MutantBedrog used several different versions of its malicious script over a short period of time. In the case that the user does not satisfy the conditions of a potential victim, the user will be sent to the page of the brand being abused. Victims are led to an iPhone giveaway scam. In addition to the tricks mentioned above, MutantBedrog uses a creative method to bypass CSP on Chrome-based browsers.

DCCBOOST

DCCBoost is continuously executing a sophisticated scareware campaign, orchestrating multiple forceful redirects...



Category:

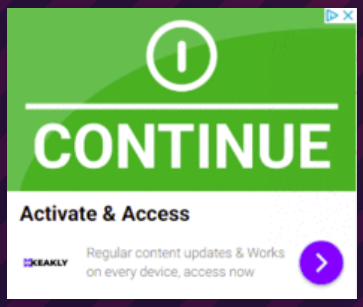
Criminal Scams
Fake Ad Server
Forced Redirect

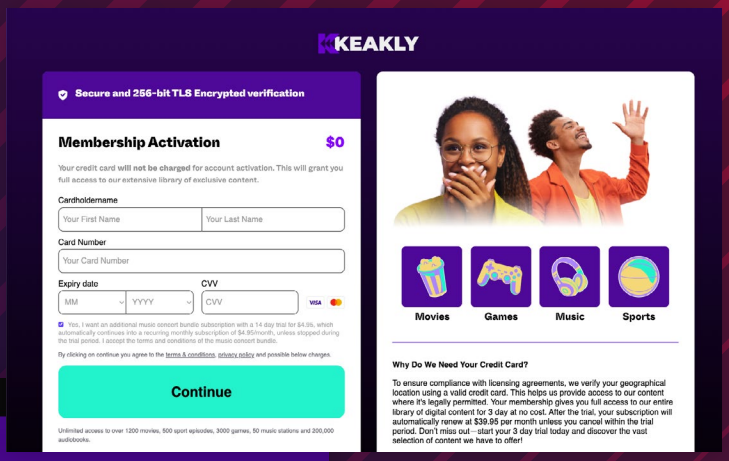
DCCBoost is continuously executing a sophisticated scareware campaign, orchestrating multiple forceful redirects predominantly impacting desktop users in the United States, the United Kingdom, and Canada. Known for deploying counterfeit McAfee scareware attacks since late 2021, DCCBoost has now shifted focus from mobile devices, redirecting users to scareware imitating McAfee and tech support scams mimicking a fake Windows screen, leading to significant financial losses for victims.

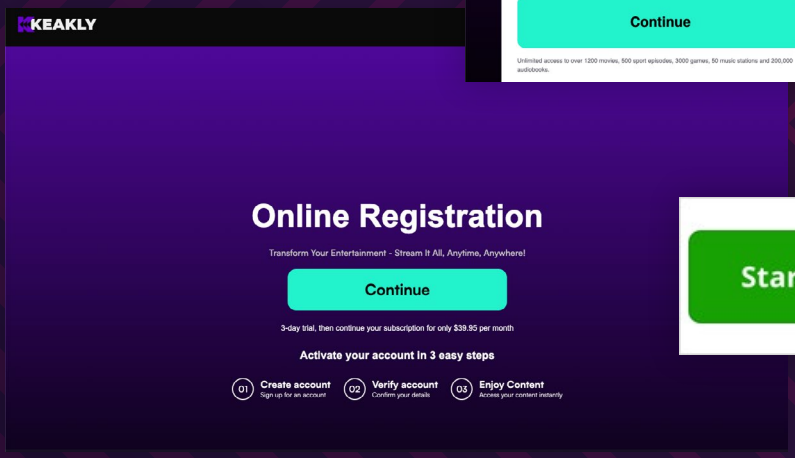
Utilizing multiple ad servers, enabling seamless switching in response to takedown efforts and deceptive ad creatives, DCCBoost redirects users via forceful redirects to the scam during real user sessions, employing various cloaking techniques to conceal the process.

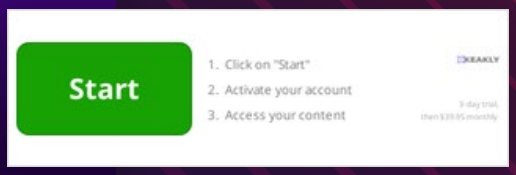
3EZSTEPS

Continue button landing page with “3 easy steps” modal that deceives the victim into providing credit card info...









Category:

Criminal Scams

Fake Ad Server

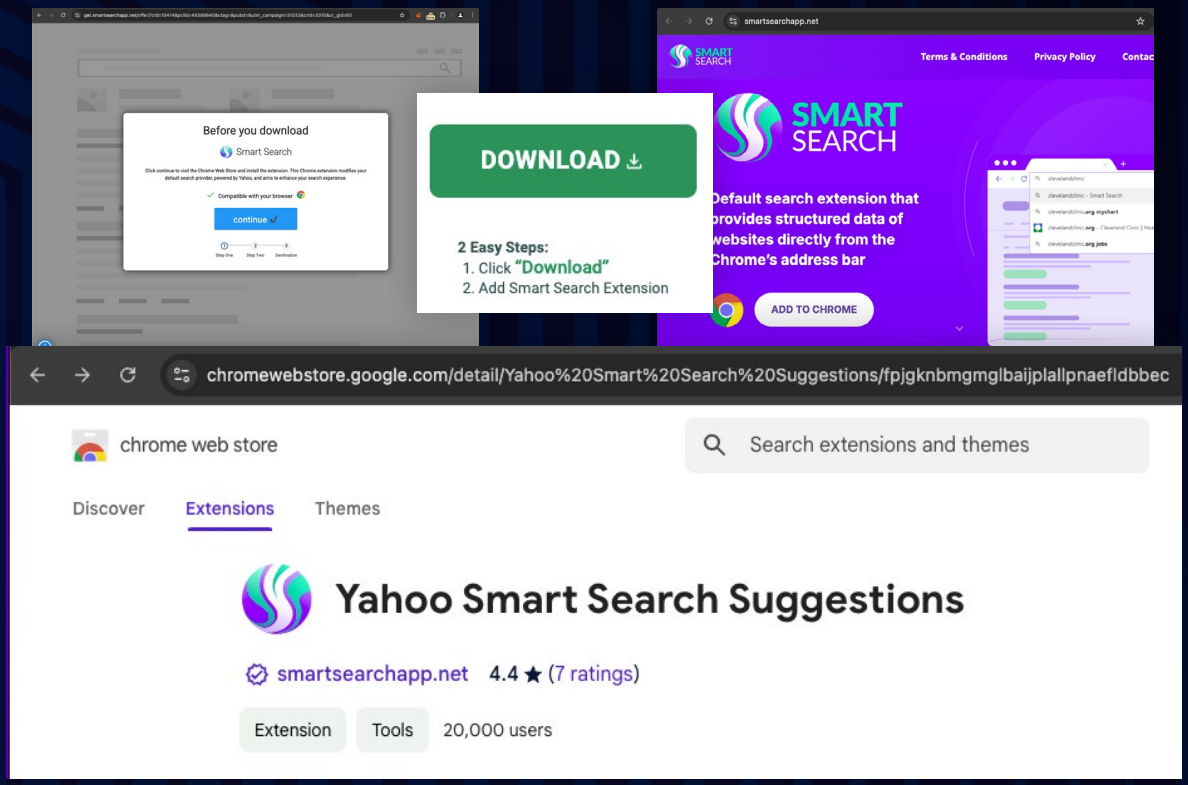
Forced Redirect

Highlights: Constant flow to its scams

TA Description: Continue button landing page with “3 easy steps” modal that deceives the victim into providing credit card info to verify an account for “free access” but subscribes them to an affiliate’s online service. After the victim enters an email and clicks continue, they are brought to a page asking for credit card details in order to proceed. It’s described that the credit card is only being used for verification. The products 3ezSteps offers to the victim is described broadly as access to content. Depending on the affiliate, it can serve offers with misrepresented payment responsibility for its product: mobile and desktop software including product keys, movie/audiobook/music streaming, video games, health and recipes, etc.

4PERCENT

Big button ads with “2 Easy Steps” in the ad text. Its landing page has victims install a web browser extension or download a file...



Category:

Fake Ad Server

Fake Update

Highlights: Shifted focus towards web browser extensions only.

TA Description: Big button ads with “2 Easy Steps” in the ad text. Its landing page has victims install a web browser extension or download a file. The ads are intended to steal the click of an action on the publisher’s page. Its landing page confuses the victim into believing that they must install the extension or file in order to do what they intended on the publisher’s page.

Screenshots: The example screenshots above show a malicious Ad Landing Page that is trying to convince the victim that they must download a web browser extension before they download what was intended to be the publisher’s actual webpage.

EGOBBLER

..launching malicious attacks targeting users across multiple European countries with investment scams...

May 5 2021	May 15 2024	September 2 2024	October 15 2024	November 26, 2024
				
				

Category:

Criminal Scams

Fake Ad Server

Highlights: After ~3 years dormancy, eGobbler has returned in 2024, launching malicious attacks targeting users across multiple European countries with investment scams. They are one of many threat actors currently using cloaking, sensationalist celebrity ad creatives, and fake versions of legitimate news sites to deliver Investment Scams.

TA Description: eGobbler was notorious for large-scale malvertising campaigns exploiting browser vulnerabilities, particularly in Chrome and Safari. They were highly targeted, frequently occuring during weekends and high-traffic periods when ad security staff might be off. They used highly sophisticated TTPs like Chrome & WebKit bugs, session hijacking, auto redirects, and highly targeted to deliver malicious content. The harm to users was typically **phishing attacks**. At their peak, they were persistent threat across multiple platforms. In 2021, eGobbler pivoted to **investment scams**, using fake endorsed clickbait imagery of celebrities to lure users into fraudulent investment schemes. Similar to FizzCore, they featured 'beaten up celebrity images' and were highly regionalized.

SCANDALNEWSNETWORK

...threat actor that leverages cloaking, sensationalist celebrity-themed ad creatives, and fake versions of legitimate news sites...

Highlights: Targeting multiple countries except the USA, this is another threat actor that leverages cloaking, sensationalist celebrity-themed ad creatives, and fake versions of legitimate news sites to deliver investment scams.

TA Description: This threat actor runs ads falsely claiming rumours and scandals about celebrities, often using photoshop to make them appear bruised or beaten up. They have refined the art of crafting fake landing pages which look like regular blog sites, with actual content about the same celebrity. When triggered, the scam pages are fake versions of established news websites, pushing victims to Investment Scams. The domains serve high volumes of impressions, with a few cases each week.

Category:
Cloaking
Criminal Scams

DROIDDRAMA

Predominantly targeted to European countries such as Czechia and Denmark, these are cloaked investment scams...

Category:

Cloaking

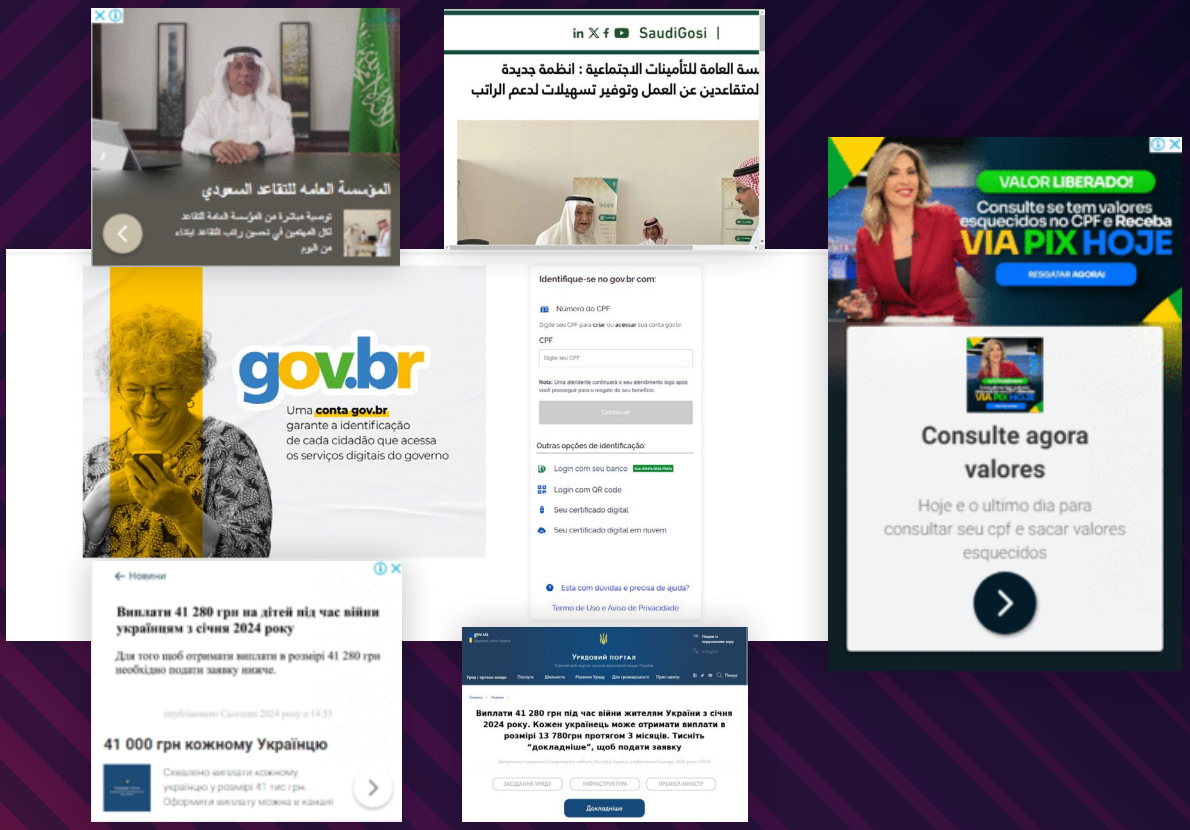
Criminal Scams

Highlights: Predominantly targeted to European countries such as Czechia and Denmark, these are cloaked investment scams depicting AI and futuristic robot/droid-themed content

TA Description: Tracked since July 2024, DroidDrama uses well-made, short-lived fake "white pages" that often promote ways to make money using AI. While the creatives themselves are not cloaked, the cloaked landing pages impersonate high-reputation publisher sites (e.g., Apple News) to give visitors a false sense of trustworthiness. The domains involved serve high volumes of impressions, with a few new cases emerging each week.

GOVERNMENT PHISHING

Phishing for personal information via Government Impersonation...



Highlights: Phishing for personal information via Government Impersonation

TA Description: We detected this type of government phishing targeting 3 countries:

- Saudi Arabia Government | Q2 2024 | GOSI: General Organization for Social Insurance
- Ukraine Government | Q2 2024 | Fraudulent war relief payments
- Brazil | Government | Q2 2024 | Phishing for CPF numbers (like the Social Security number)

Category:

Criminal Scams

Phishing Scams

About CONFIANT

Confiant is the cybersecurity leader in detecting and stopping Malvertising attacks. Having built hundreds of integrations directly into the web's ad tech infrastructure, Confiant has unparalleled visibility to the malware, scams and fraud serving through ads today. Leveraging our security expertise, we deliver complete control over ads to publishers and ad platforms, also remediating quality issues, privacy violations, and mis-categorized ads.

In publishing the industry's leading ad quality benchmark report and mapping the threat actors that use ads-as-an-attack-vector at matrix.confiant.com, Confiant is leading the charge in protecting users from criminals hijacking the ad tech supply chain. Trusted by customers like Microsoft, Paramount, and Magnite, we celebrate more than a decade supporting our ad tech partners.

LEARN MORE

CONFIANT

Malvertising and Ad Quality Index

Please visit our website at:

www.confiant.com

2024

January 1st - December 31st