CONFIANT

Malvertising and Ad Quality Index

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

H1 2024

January 1st - June 30th

CONTENTS

H1 2024 First Impressions

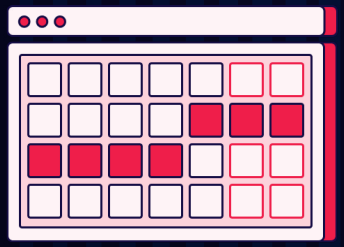
HEAVY ADS

Top Quality Issue

FAKE SOFTWARE UPDATES MALICIOUS DOWNLOADS

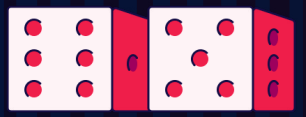
Top Security Issue

7 DAYS



Fastest Average Response Time

GAMBLING

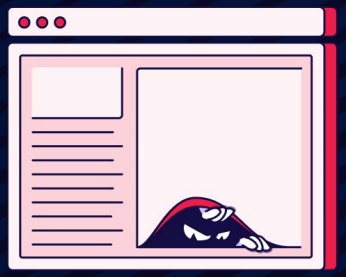


Most Blocked Category

1 IN 88

Dangerous and Disruptive

1 IN 454



User Security Risk

INTRODUCTION

Confiant's **Malvertising and Ad Quality (MAQ) Index** is the oldest and most comprehensive analysis of creative quality and security in the digital advertising industry.

Issued twice a year, the report draws on Confiant's proprietary sample of hundreds of billions of impressions monitored in real time.

The MAQ tracks the frequency and severity of ad quality issues as experienced by the real victims of malicious, disruptive and annoying ads: end users.

The MAQ Index, which leverages Confiant's position as the vendor of choice for ad security, quality, and privacy monitoring, aims to provide a comprehensive view into the creative issues facing the industry.

For decades, this kind of analysis was impossible because the industry lacked widespread client-side instrumentation across publishers.

That all changed in 2017, with the launch of Confiant's real-time creative-verification solution, which allowed us to reveal the underlying causes of creative quality and security issues for the first time.

In 2018, Confiant released the industry's first benchmark report. This report, the 20th in the series, covers the first half of 2024.

METHODOLOGY

To compile the research contained in this report, Confiant analyzed a normalized sample of almost **500 billion advertising impressions** monitored from January 1st to June 30th, 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 **measures 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.

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.

CONFIANT

The State of the Industry

H1 2024

In H1 2024,
one in every 88
impressions was
dangerous or
highly disruptive
to the end user.

H1 2024

AT A GLANCE

- **One in every 454 impressions** was a user **security risk**.
- **One in every 88 impressions** had significant **security or quality issues**.
- The **industry-wide quality violation rate halved** from Q4 2023.
- **Firefox's security violation rate has consistently increased** since 2022.
- **Google** maintains a **security violation rate of almost 1%**.
- **SSP-S** holds onto the worst quality block rate, almost double that of the second worst SSP.
- **SSP-H** underperformed in both security and quality violation rates, the first time since 2021.
- **Sharethrough and OpenX** both surpassed the previous security frontrunner: **SSP-E**. Top performer **SSP-G** and **SSP-F** also performed very well this period.
- The SSPs with the **most security incidents** continue to have the fastest response times.

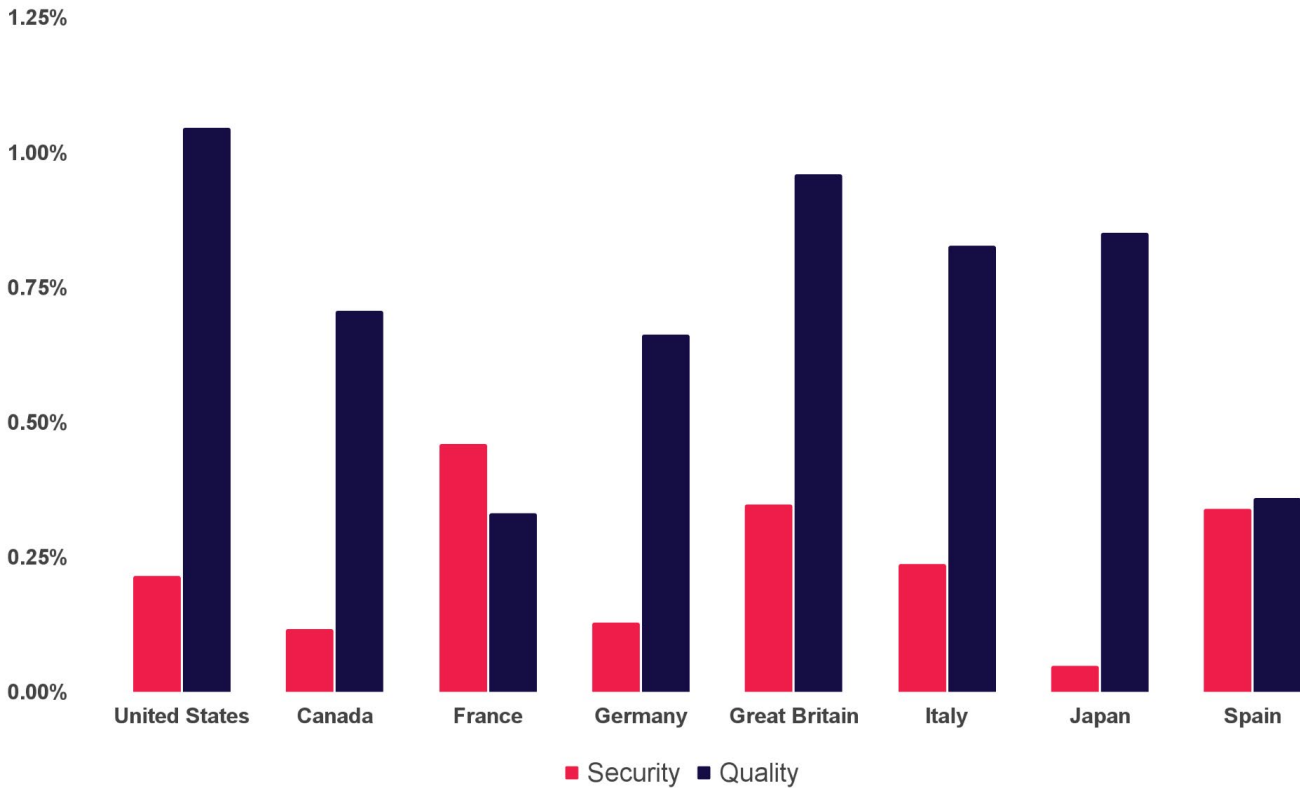
Violations down, but still above 22-23 averages

The industry-wide security violation rate steadied, averaging 0.22% for H1 2024. While this is a welcome fall and lower than the rate seen in any half of 2023, it is still slightly above 2022's yearly average of 0.21%.

In only half a year, the industry-wide ad quality violation rate almost halved from 1.57% to 0.81%. However, this is still noticeably higher than H1 2023, which averaged 0.67%.

While the quality violation rate in Q2 2024 was cut in half to 0.81%, it is still almost double the 2021 average.

Violation Rates by Country



In France, Italy, and Spain, security issue rates doubled from 2023 averages.

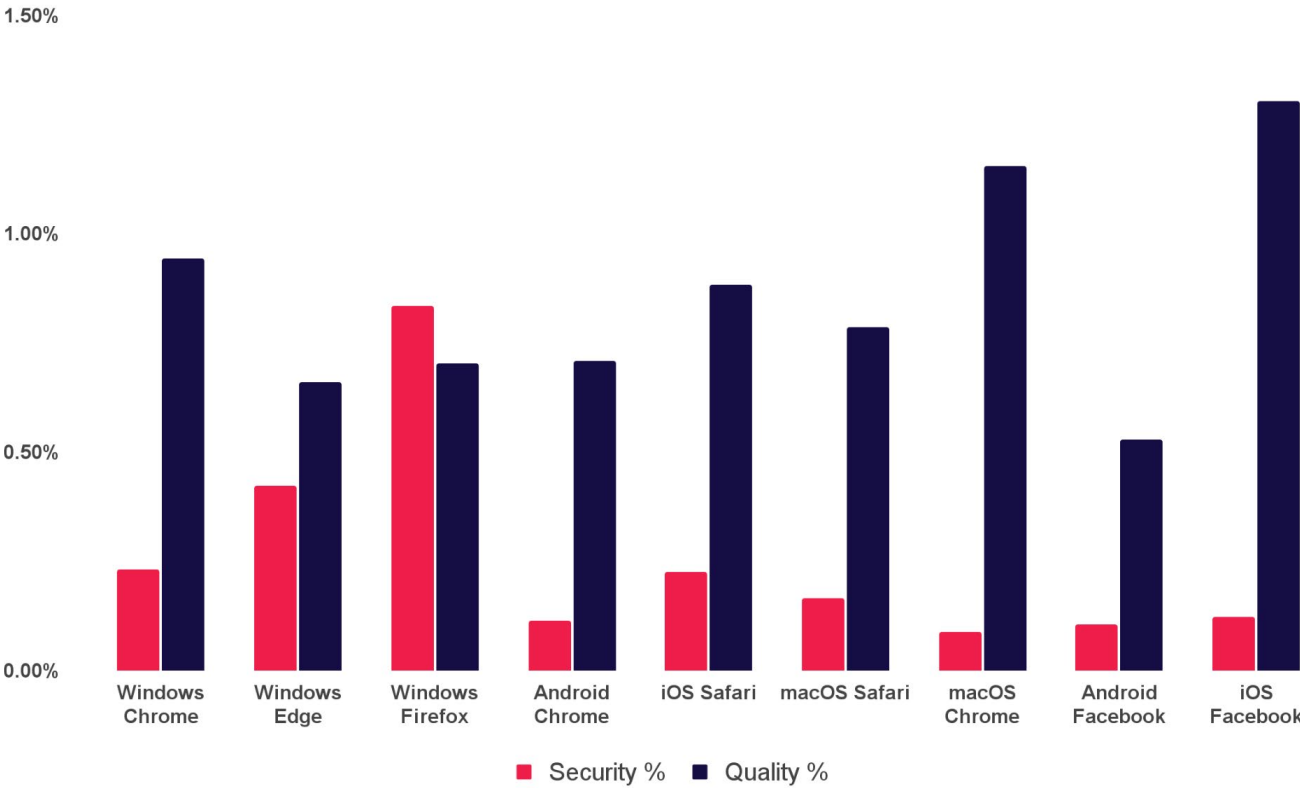
While the USA and Canada saw improvements in Security and Quality issues, the **USA still retained the highest rate of quality issues** of any country surveyed.

France overtook Great Britain as the country with the highest rate of security issues.

While **Japan was the safest market for security issues, its rate of quality issues doubled** from its 2023 average.

Canada and Germany were the second and third safest markets, with Germany's violations rate staying steady since 2023.

Violation Rates by Browser



In H1 2024, **users of Firefox for Windows experienced the highest rate of security issues**, with their Security issue rate rising from an average of 0.63% in 2023 to 0.83%. That's 1 in every 120 advertisements.

Conversely, **Chrome marginally improved its Security rates across all platforms**, but remained the worst in terms of Quality issues.

The Facebook browser on iOS saw a dramatic doubling in Quality issues, from a 2023 average of 0.62% to 1.30%

Security Violation Rates by Browser Family

...Firefox users were the most impacted by security issues...

In H1 2024, Firefox users were the most impacted by security issues, experiencing double the encounters compared to Edge users. Chrome and Safari users were less than a quarter as likely to experience ads with security issues.

Firefox's H1 2024 security violation average is 0.83%, an increase of over 30% from its 2023 average. Firefox in 2023 already saw a 50% increase in its Security rate in 2022.

Chrome and Safari both saw a 0.01% reduction in their Security rate compared to 2023, but Edge saw a healthy improvement, dropping from 0.54% to 0.42%.

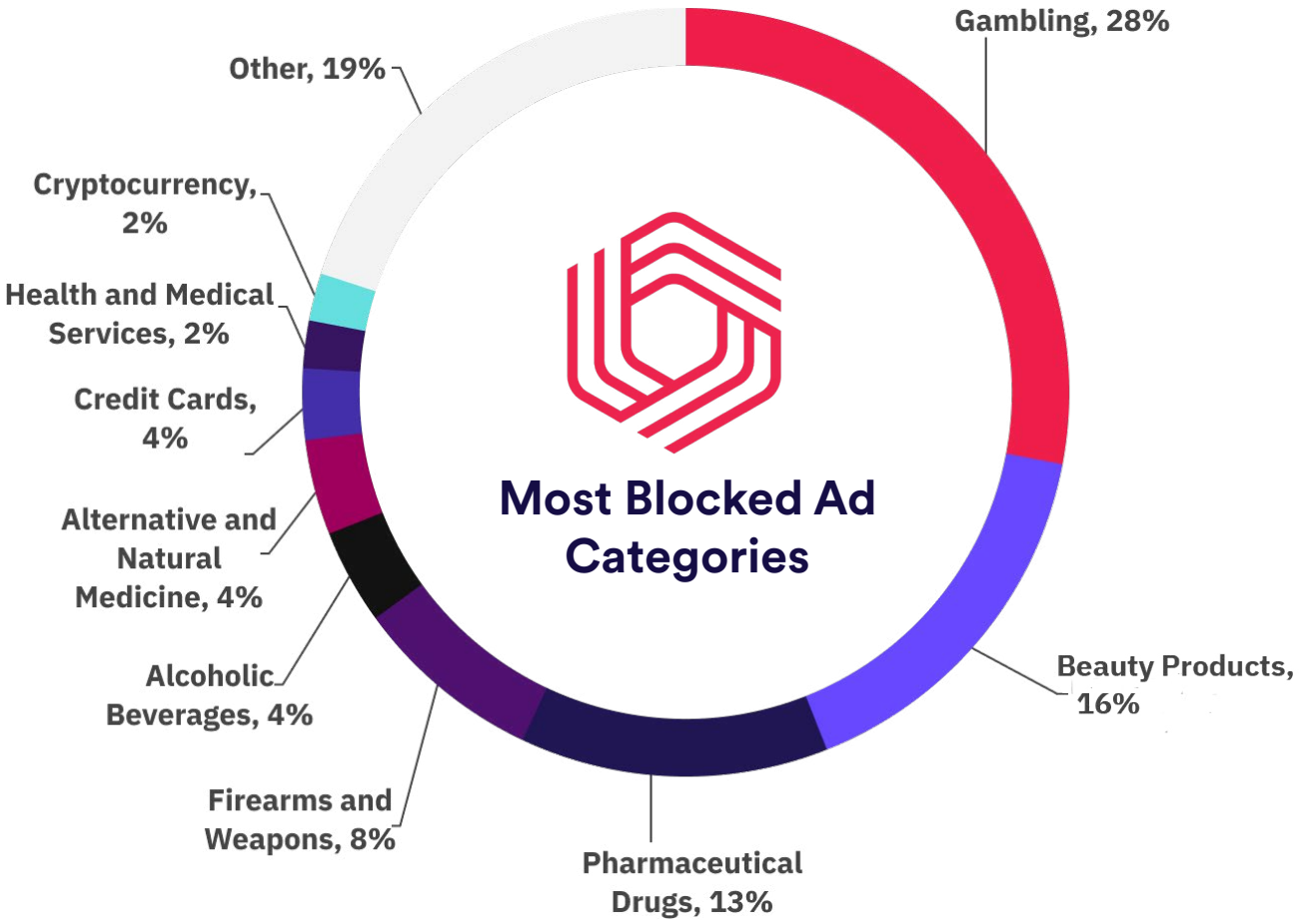
Violation Rates by Bidding Framework

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.

In H1 2024, Google and Amazon TAM performed relatively equally, outclassing Prebid.

Amazon's Quality issue rate dropped from 1.81% in 2023 to 0.79% in H1 2024, while Prebid's increased from 0.99% to 1.16%.

Google performed the same as in 2023.



"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 H1 2024, Gambling remains the most blocked category, followed by Beauty Products. Pharmaceutical Drugs holds onto its respectable 3rd position. **The newest category to surge out of Other is Firearms and Weapons, taking 4th place**. These four categories make up 66% of all blocked categories.

Alcohol continues its fall from being the 2nd most blocked category in H1 2023 to 5th place, and Cryptocurrency reemerged, but only represented 2% of blockings.

Even with many European elections, Political Advertising has not made an appearance since 2022. This is expected to change in H2 2024 in timing with the USA Presidential Election.

CONFIANT

SSP Rankings

H1 2024

SSP Rankings

In H1 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 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.

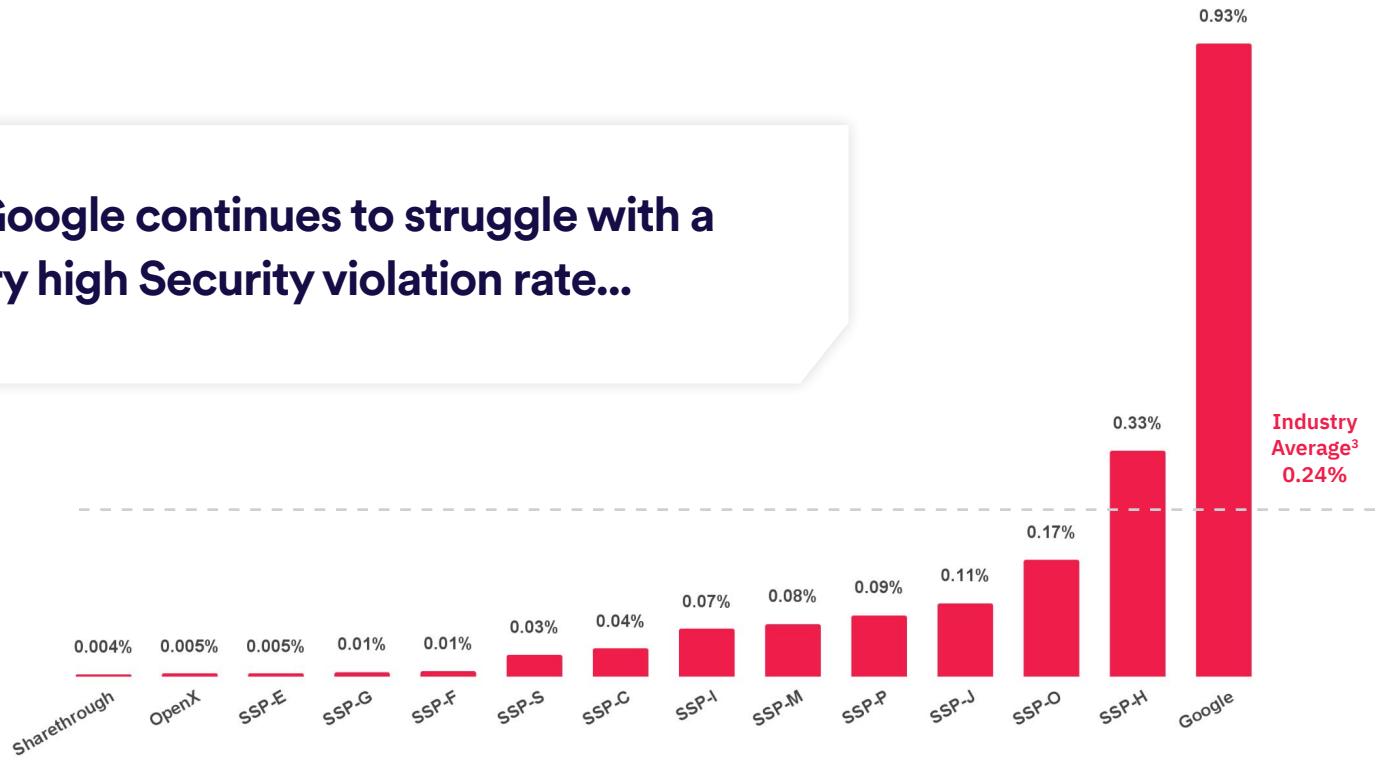
To qualify for inclusion, a provider had to have been a consistent source of **at least one billion Confiant-monitored impressions per quarter** across a cross-section of publishers in our global sample.

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 continues to struggle with a very high Security violation rate...



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

In H1 2024, **Google continues to struggle with a very high Security violation rate**, which dramatically increased from an average of 0.48% in 2022, to 0.90% in 2023, and now is maintaining at 0.93%.

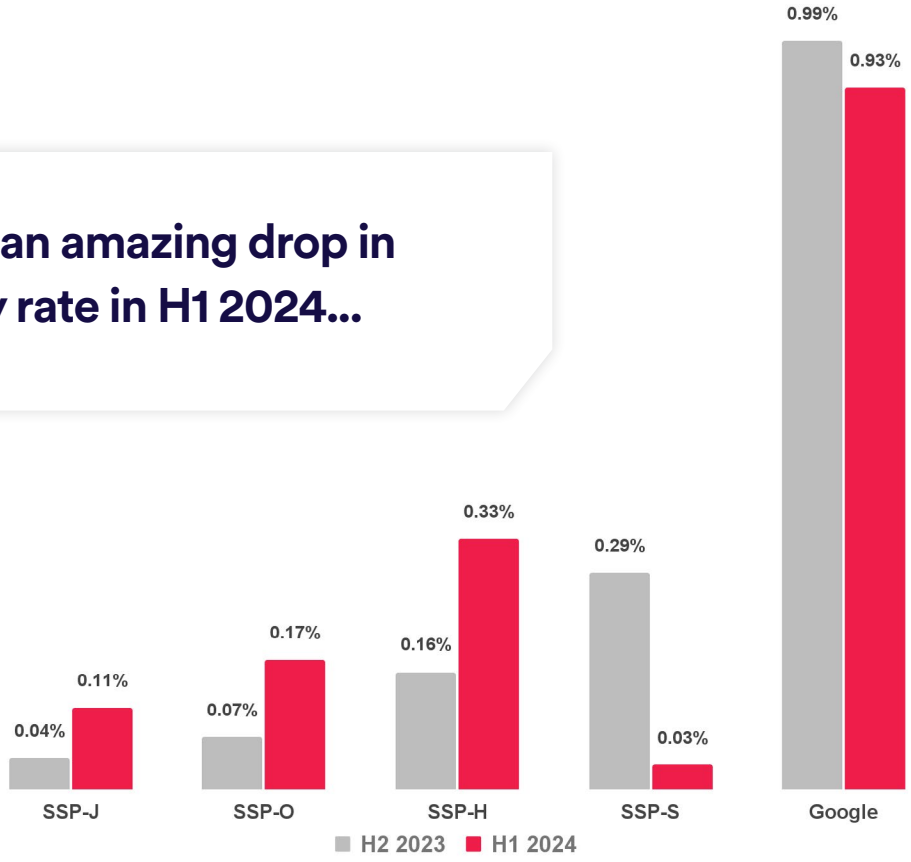
SSP-S, newly added last year, **saw an incredible drop 0.23% in 2023 to 0.03%**.

SSP-H saw the opposite happen, **increasing from 0.12% to 0.33%**.

The SSPs with the lowest rate of security violations for the period were **Sharethrough, OpenX, and SSP-E**, each achieving a rate of less than 0.01%, with **Sharethrough taking the frontrunner position** from SSP-E, who held the title since H2 2022. The Top 5 positions continue to be highly competitive.

Security Violation Rate: H2 2023 vs. H1 2024

...SSP-S saw an amazing drop in their security rate in H1 2024...



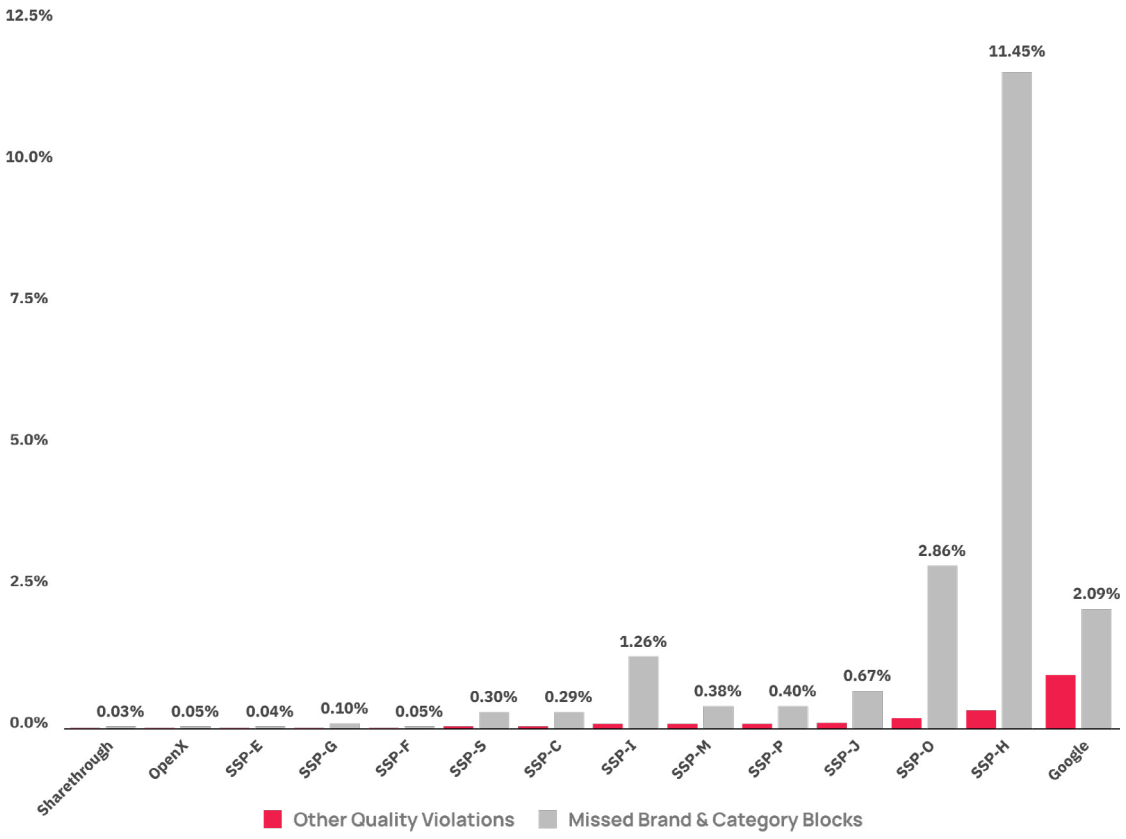
Google's security violation rate dipped from 1% in H2 2023 to 0.93% in H1 2024, maintaining its incredible rate. This is largely driven by Fake Software Updates and malicious downloads. These malicious campaigns optimize to stay within Ad Platform policies, and as a consequence are very prevalent, especially in Google Ads.

SSP-S saw an amazing drop in their security rate in H1 2024.

SSP-H, SSP-J, and SSP-O saw significant increases to their security rates in H1 2024.

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



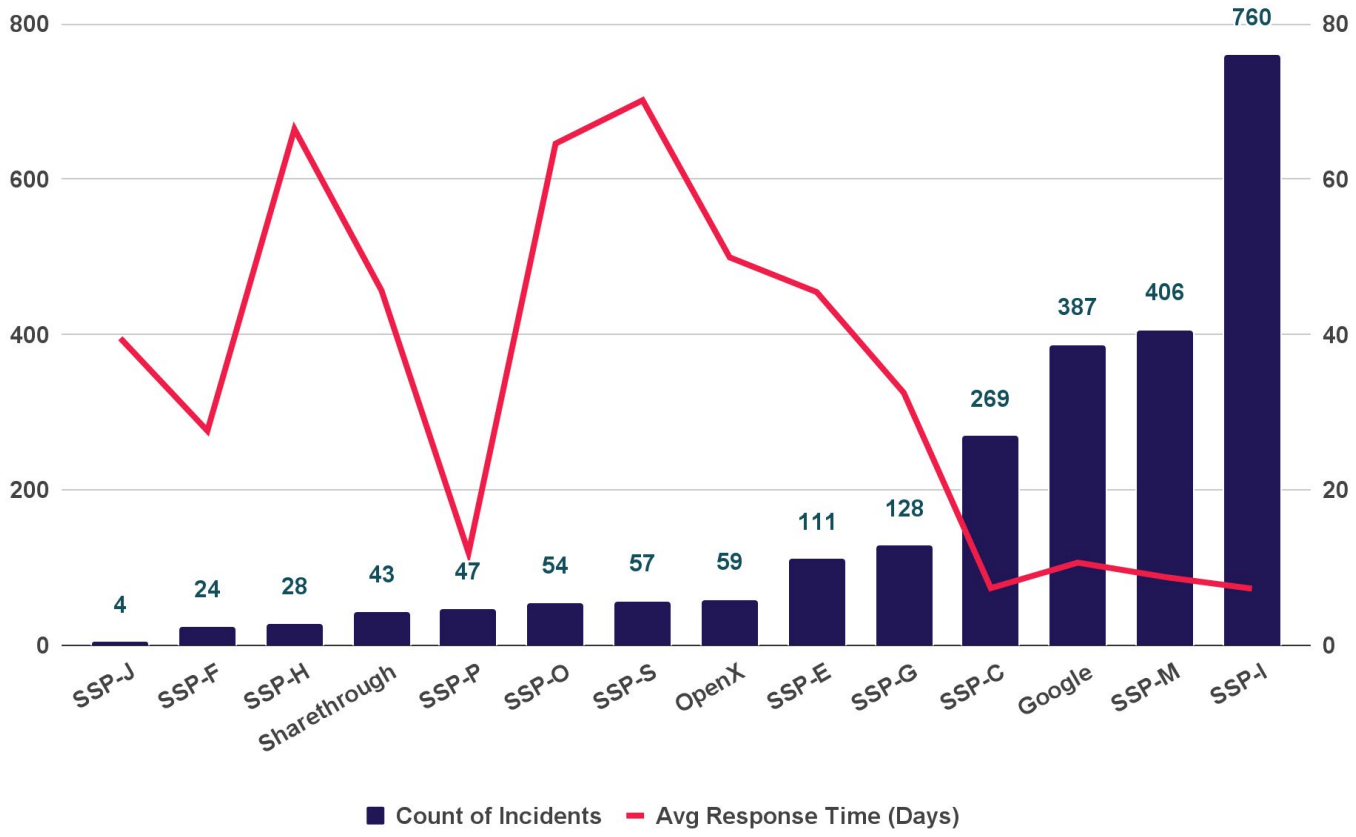
Averages can mask significant variation in day-to-day performance, so it's important to note the **upper bound of the security violation rate** for each SSP to get a sense of overall risk.

In H1 2024, **SSP-H, SSP-O, SSP-I, and Google recorded the highest daily security rates for the period by far**.

SSP-H set a staggering record at 11.45%, beating the record held by SSP-I in 2022 at 5.3%. This means that on **May 14th 2024, more than 1 in 9 impressions from SSP-H had security issues**.

Sharethrough had both the lowest average security rate and the lowest daily security rate in H1 2024.

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.

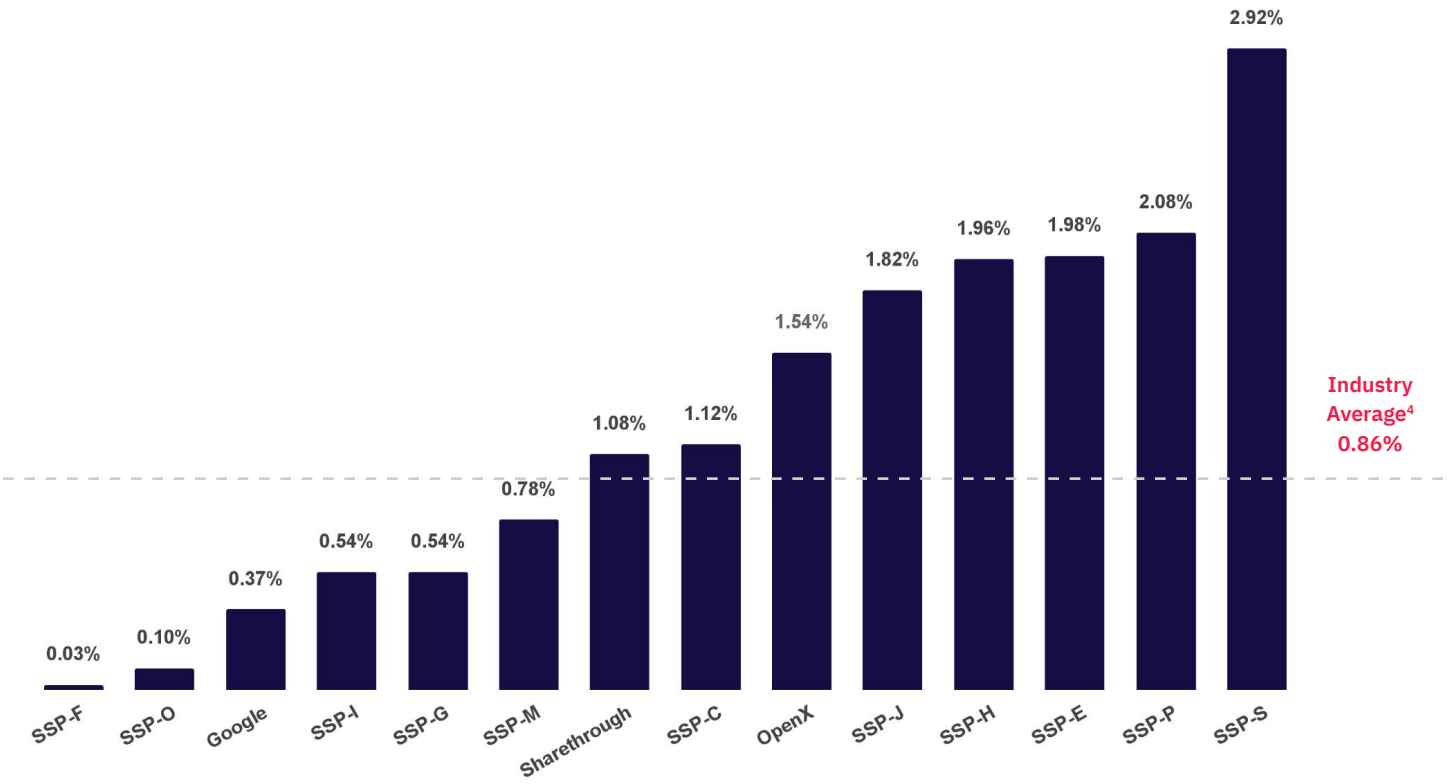
While the Security rate decreased from H2 2023 to H1 2024, the number of incidents dramatically increased. In H2 2023, SSP-I and SSP-M had the highest number of incidents at 167 and 72 respectively. In H1 2024, they have recorded numbers several times worse, with Google and SSP-C also seeing enormous increases.

Interestingly, **all four of those SSPs had the best response times**, with Google at 11 days, SSP-M at 9 days, and SSP-I and SSP-C tied at being the fastest at 7 days.

Sharethrough, while boasting the best security rate in H1 2024, performed in the middle of the pack in terms of response time.

The SSPs with the fewest incidents usually had the fastest response times, but the last time this was true was in H1 2023.

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.

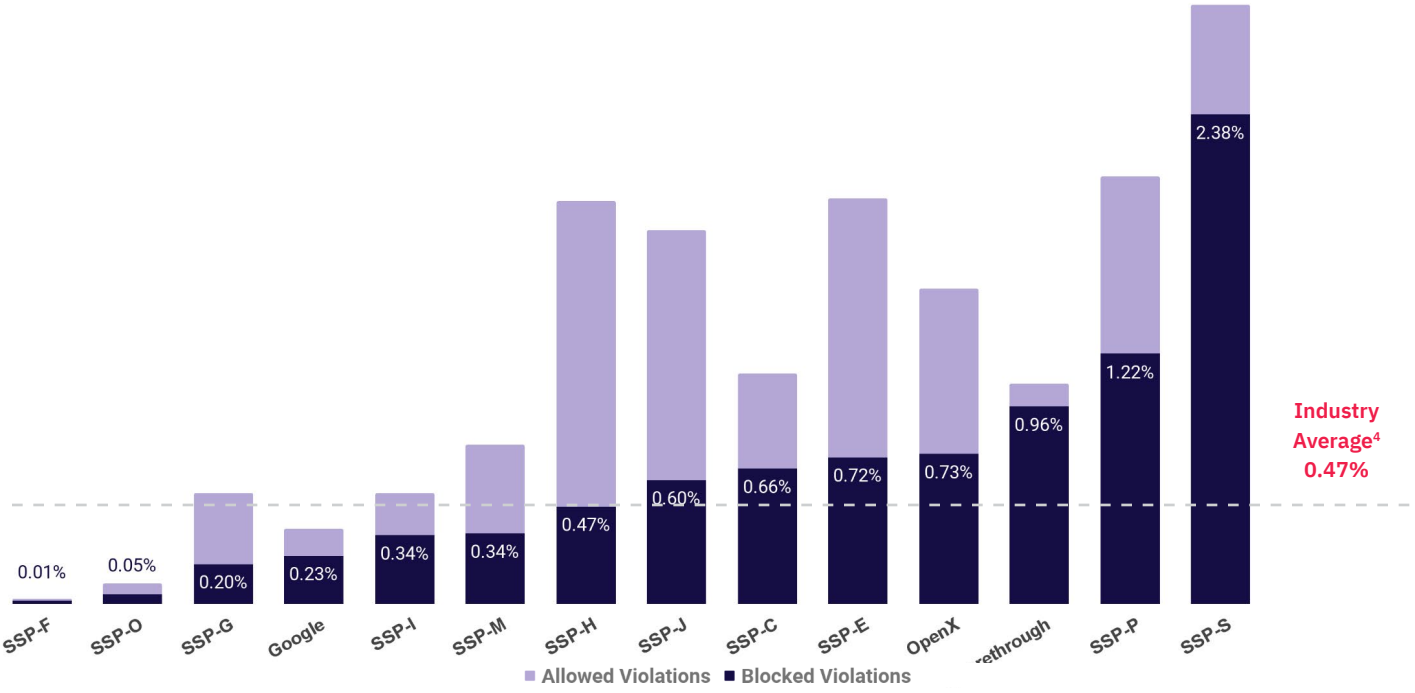
Google, while having the worst Security rate, has a very good Quality rate of 0.37%.

Sharethrough, while having the best Security rate this period, doubled its Quality rate from 0.46% in 2023 to 1.08% in H1 2024.

SSP-F had an incredible improvement from an average of 1.47% in 2023 to 0.03% in H1 2024.

During H1 2024, 1 in 35 ads from SSP-S had quality violations.

Blocked Quality Violation Rate by SSP



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

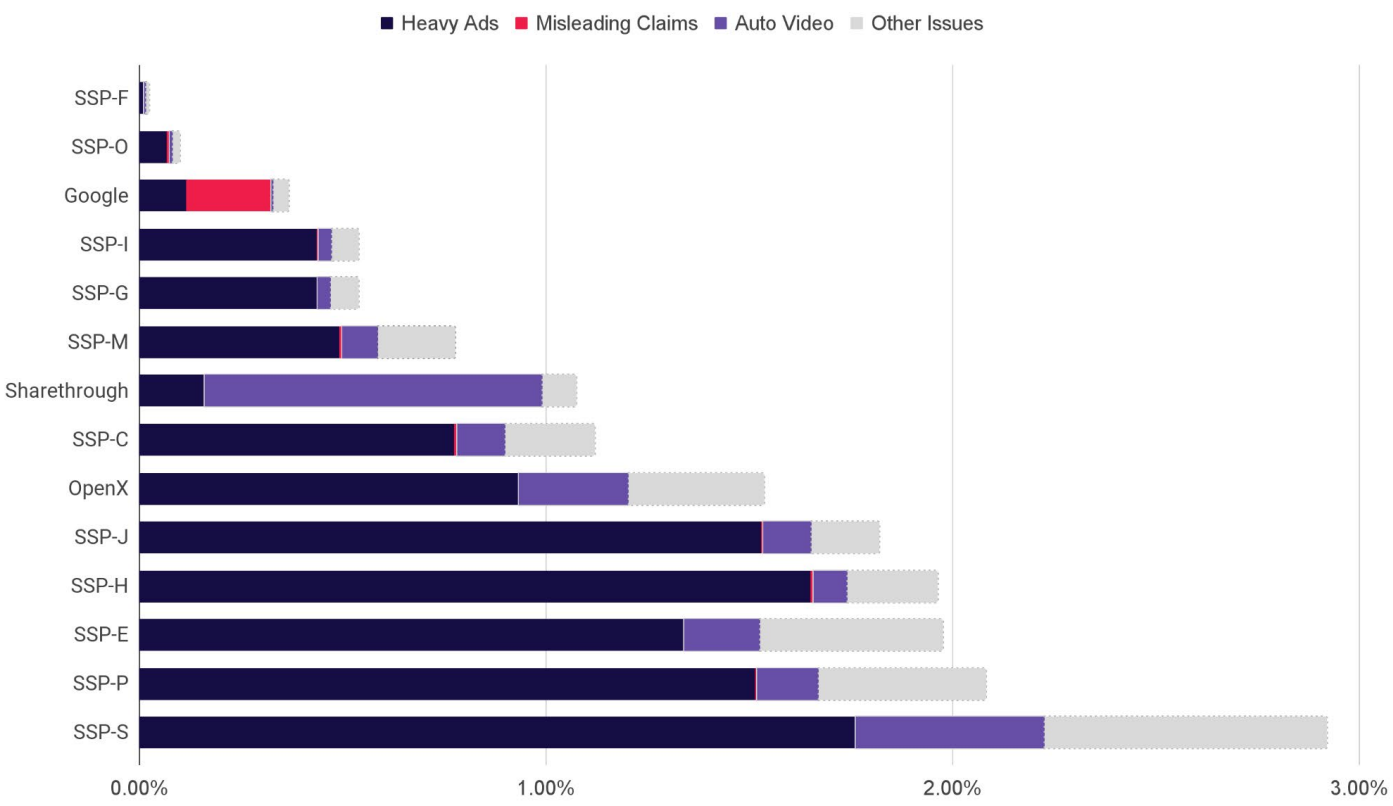
Just because a Quality violation is detected, does not mean it is blocked. That ultimate authority is reserved for Confiant's Publisher clients, who can turn on or off the blocking of different Quality specifications. Measuring the difference between allowed and blocked quality violations leads to interesting results in the SSP Quality ranking.

There is a shakeup in SSP ranking and performance due to half of the quality violations of many SSPs not being blocked. This is largely due to, on average, half of all Heaviness violations being allowed across all major SSPs, although the range is between 10% and 75% depending on the SSP. Most of the remaining allowed violations are derived from how each SSP personally handles auto-video, video-on-click, and video-on-hover violations.

SSP-S remains in last place, with a Block Rate of almost double of the second worst performer.

Sharethrough is the SSP with the lowest Allowed-to-Blocked ratio, moving them further back in the ranking.

Quality Violation Detail

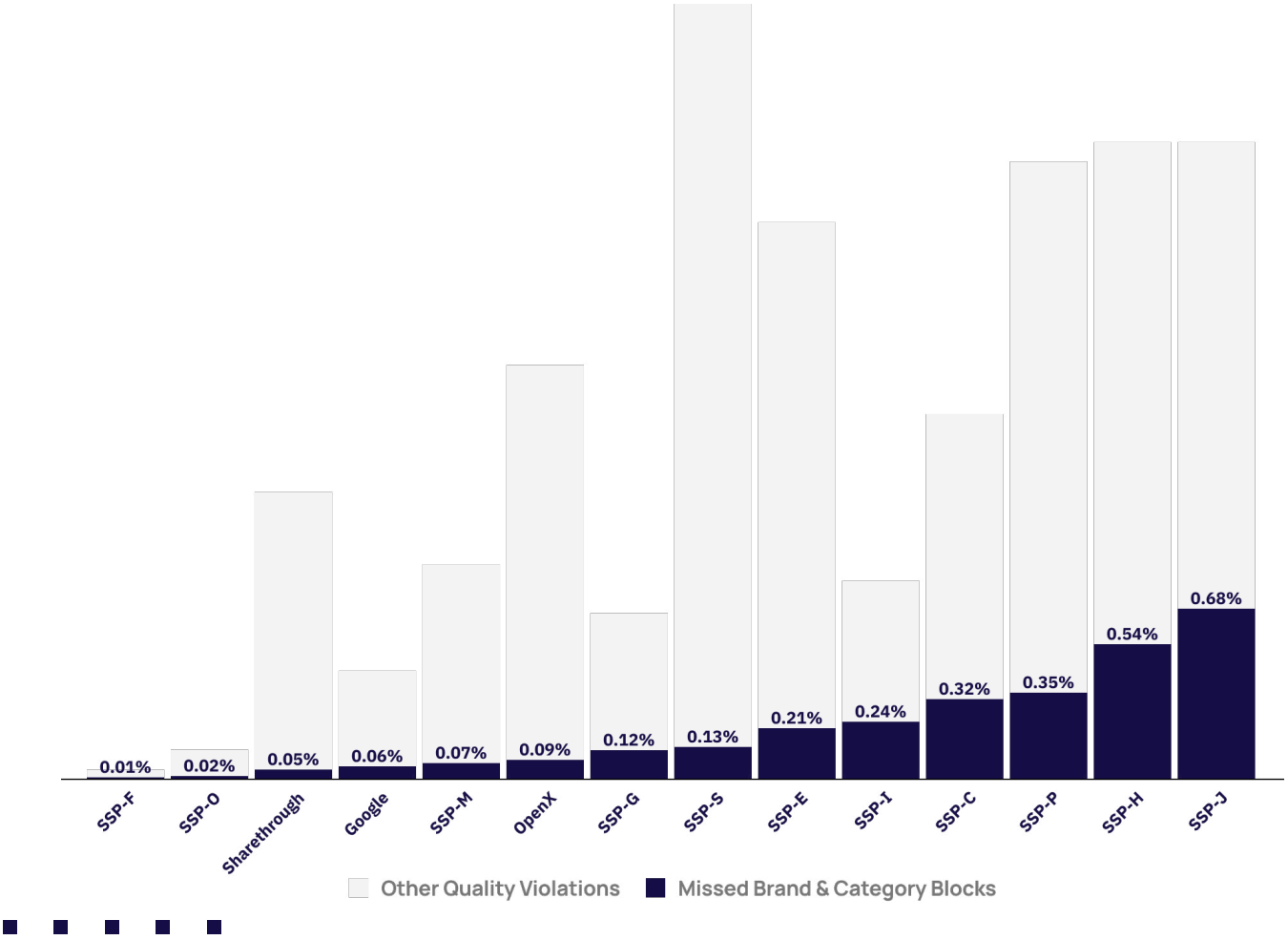


For nearly all SSPs, **Heavy Ads** — ads with characteristics like high network load, large number of unique hosts, or Chrome Heavy Ad Intervention — were consistently the most common quality issue. Display ads that **auto-play video** without any user interaction were also quite common.

Sharethrough saw a unique increase in auto-playing video ads, this issue alone contributing to its increase in its Quality rate this period.

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.

Missed Brand/Category Blocks



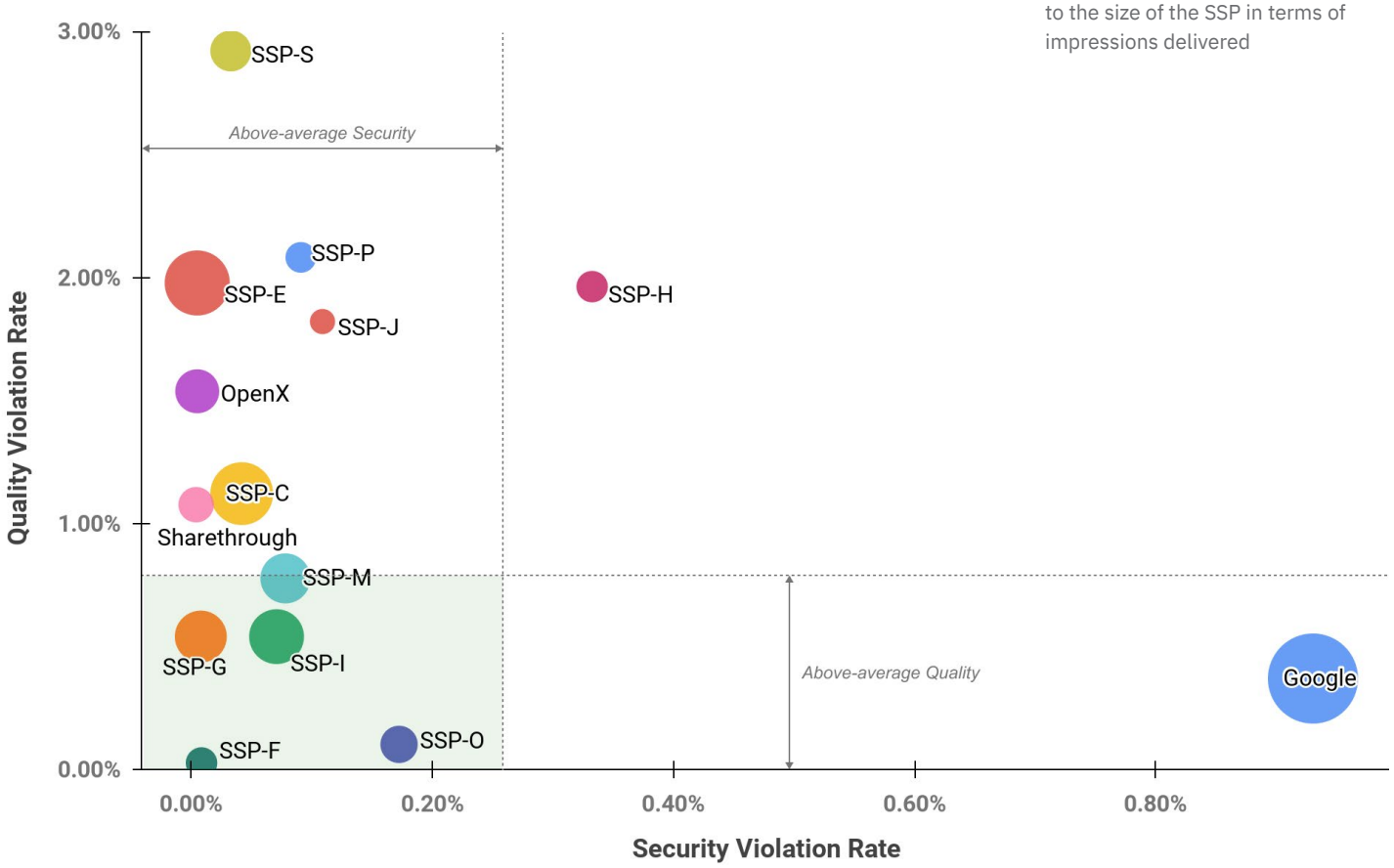
Publishers rely on SSPs as their first line of defense against ads associated with **unsuitable brands and categories**. However, these controls are not always effective.

Every SSP saw a major improvement in this topic compared to 2023.

...Every SSP saw a major improvement in this topic compared to 2023...

Violation Rates by SSP

The area of each circle corresponds to the size of the SSP in terms of impressions delivered



Five SSPs had better-than-average performance for both security and quality: Sharethrough, SSP-F, SSP-G, SSP-I, SSP-M, and SSP-O. SSP-F is new to this group, with Sharethrough and SSP-P leaving the club after being a members since H1 2022 and H2 2022 respectively.

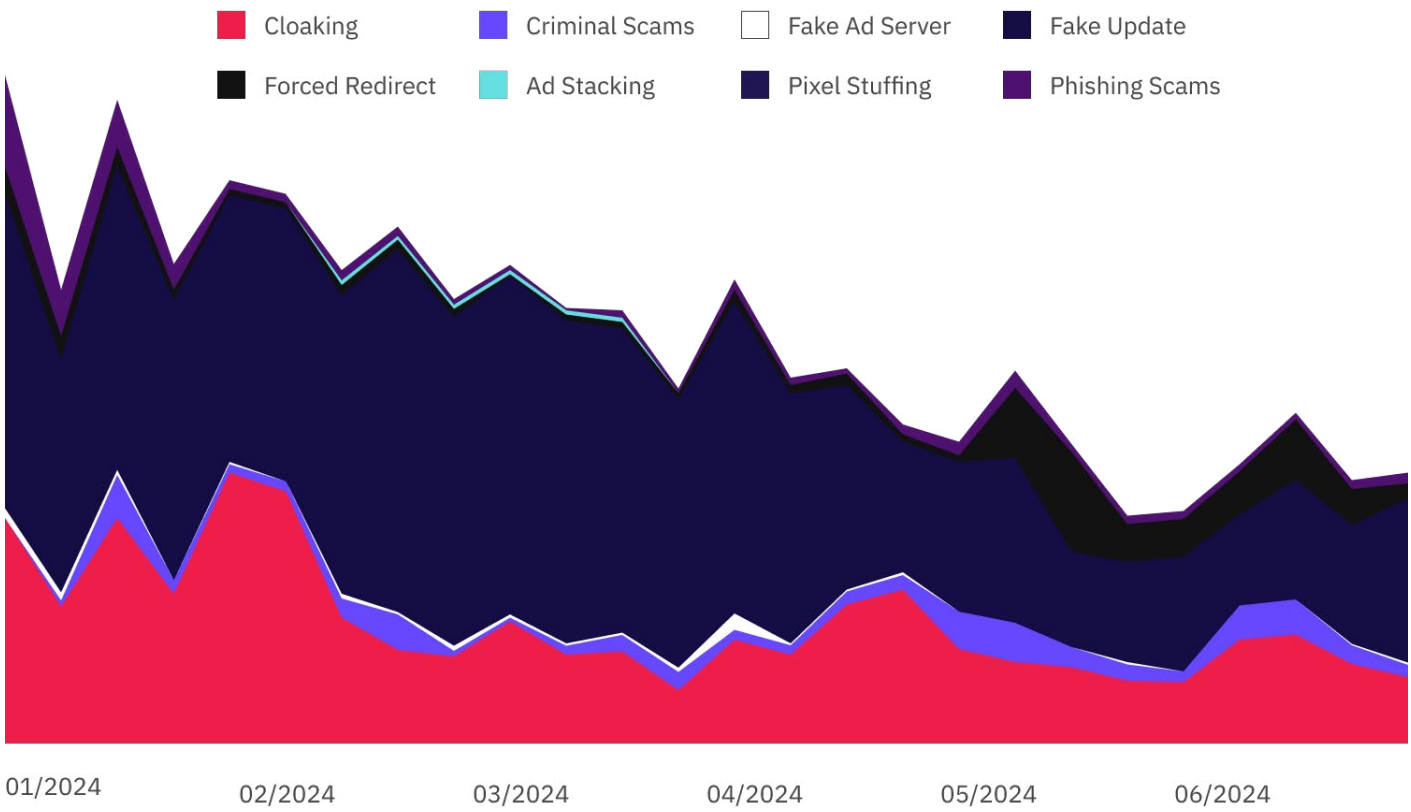
All other SSPs performed well on one measure but not the other. **Except for SSP-H**, being the only major SSP to have underperformed in both categories simultaneously since 2021.

CONFIANT

Major Threat Activity

H1 2024

Threat Detail



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

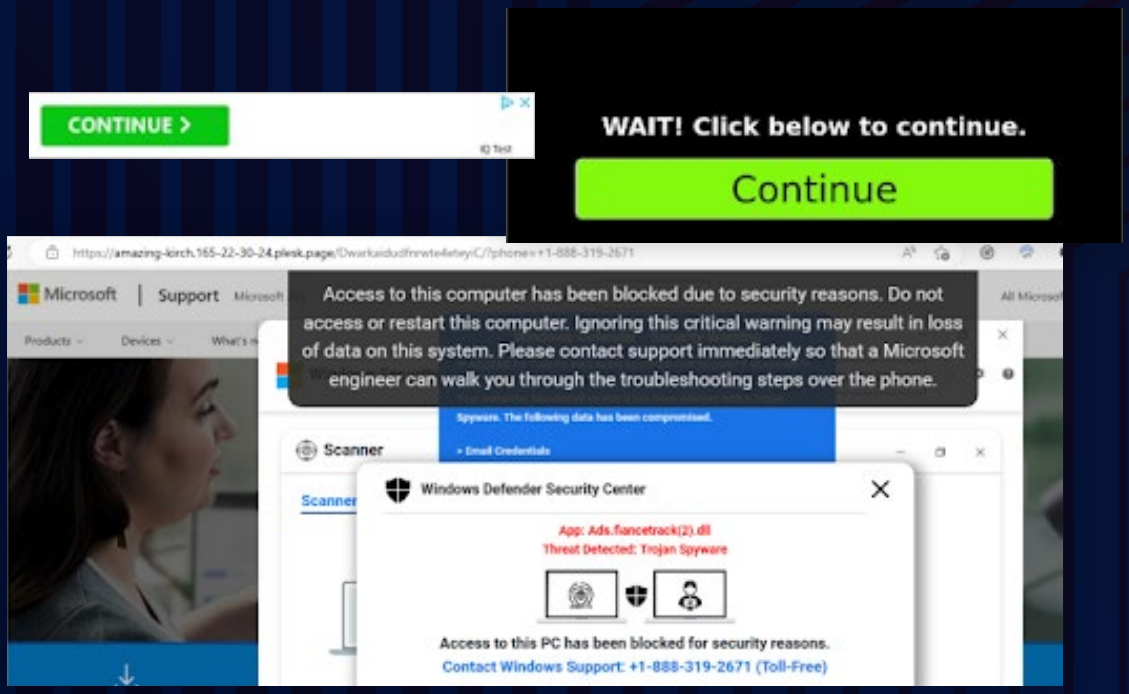
Throughout January 2024, **Cloaked Ads** accounted for half of the threats.

Fake Updates were the most consistent threat in H1 2024.

Forced Redirects saw a consistent increase in activity starting in May.

QUIZTSS

The top threat actor in 2023 was QuizTSS with total volumes that we estimate accounted for 20% of all malicious impressions...



Peak activity: **Continuous**

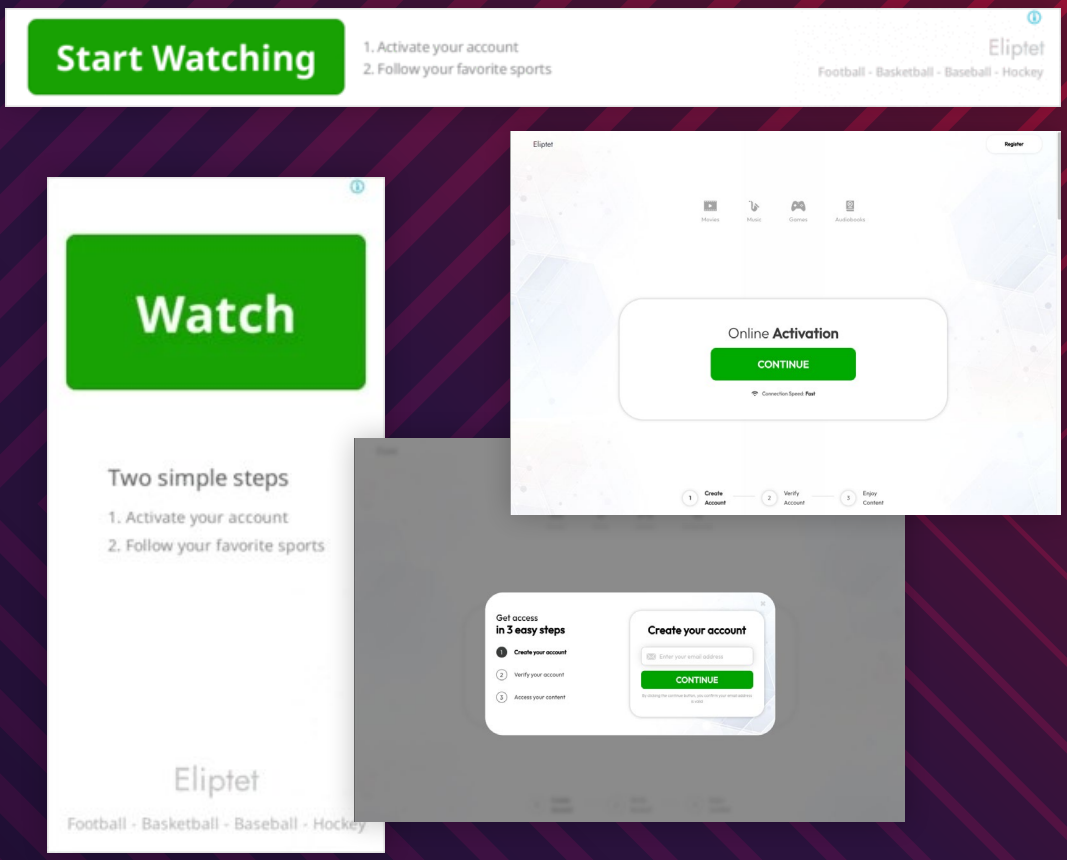
The Tech Support Scam (TSS) scene continues to evolve. The top threat actor in 2023 was QuizTSS with total volumes that we estimate at half a billion impressions.

QuizTSS uses seemingly innocuous “Start” and “Continue” buttons on cloaked AI generated or quiz landing pages as a conduit for malicious activities. These buttons, designed to blend seamlessly with legitimate quiz content, mislead users into clicking them under the guise of continuing their engagement.

However, instead of progressing through the quiz, users are redirected to fraudulent tech support websites. These sites often employ aggressive tactics, such as fake virus alerts or system warnings, to deceive users into believing their devices are compromised and coercing them into purchasing unnecessary technical support services.

3EZSTEPS

Big button ads leading to landing pages that always includes that phrase with another button which provokes an html modal for the victim to enter details...



Peak activity:
Continuous

Big button ads leading to landing pages that always includes that phrase with another button which provokes an html modal for the victim to enter details. After that the victim is delivered to checkout page for a subscription service where the terms of the service are tactfully unclear. They appear free or for a small cost but rise quickly in price.

Associated Risks of 3ezSteps ads:

- Experiencing ads which attempt to steal the click from legitimate actions on the publisher page.
- Unaware how they are being charged because the checkout pages can have conflicting statements and attempt to hide information.
- Having trouble canceling the subscriptions because the name that shows up in the merchant description on their credit card statement is unrelated to what they purchased.

8PROOF EXTENSION THREAT

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

Peak activity:
Continuous

Big button ads with “2 Easy Steps” in the ad image. 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.

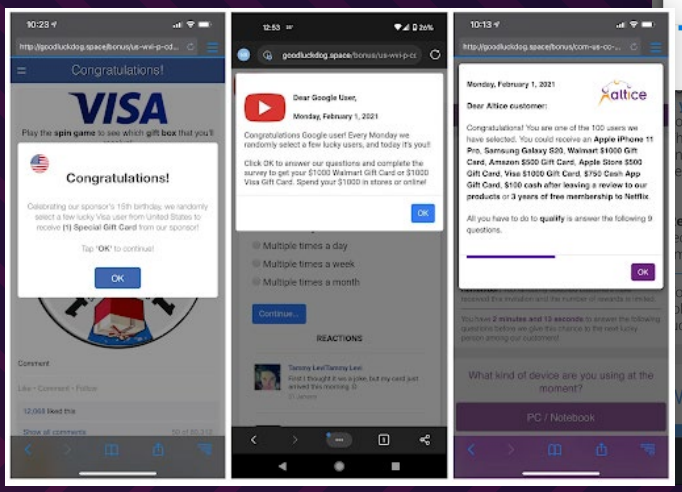
Associated Risks this threats ads:

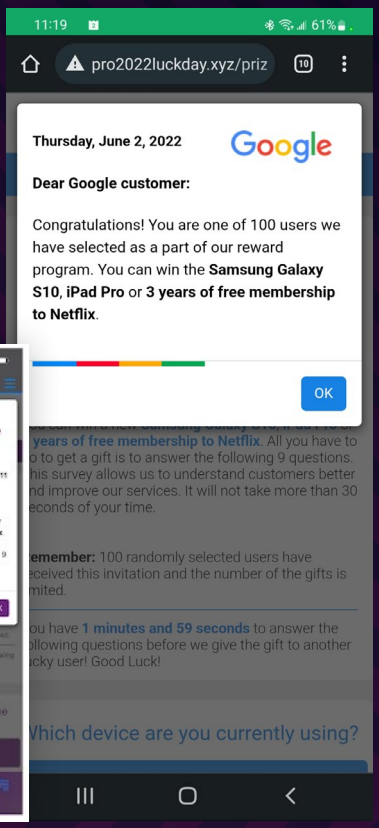
- Experiencing ads which attempt to steal the click from legitimate actions on the publisher page.
- Its ad landing pages entice the victim into installing a thier programs by leading them to believe they will be sent to where they intended to go on the publisher’s page.

SCAMCLUB

ScamClub's primary method involves using Forceful redirects, subtly guiding users to harmful websites...

Take-Down Target





Peak activity: **Continuous**

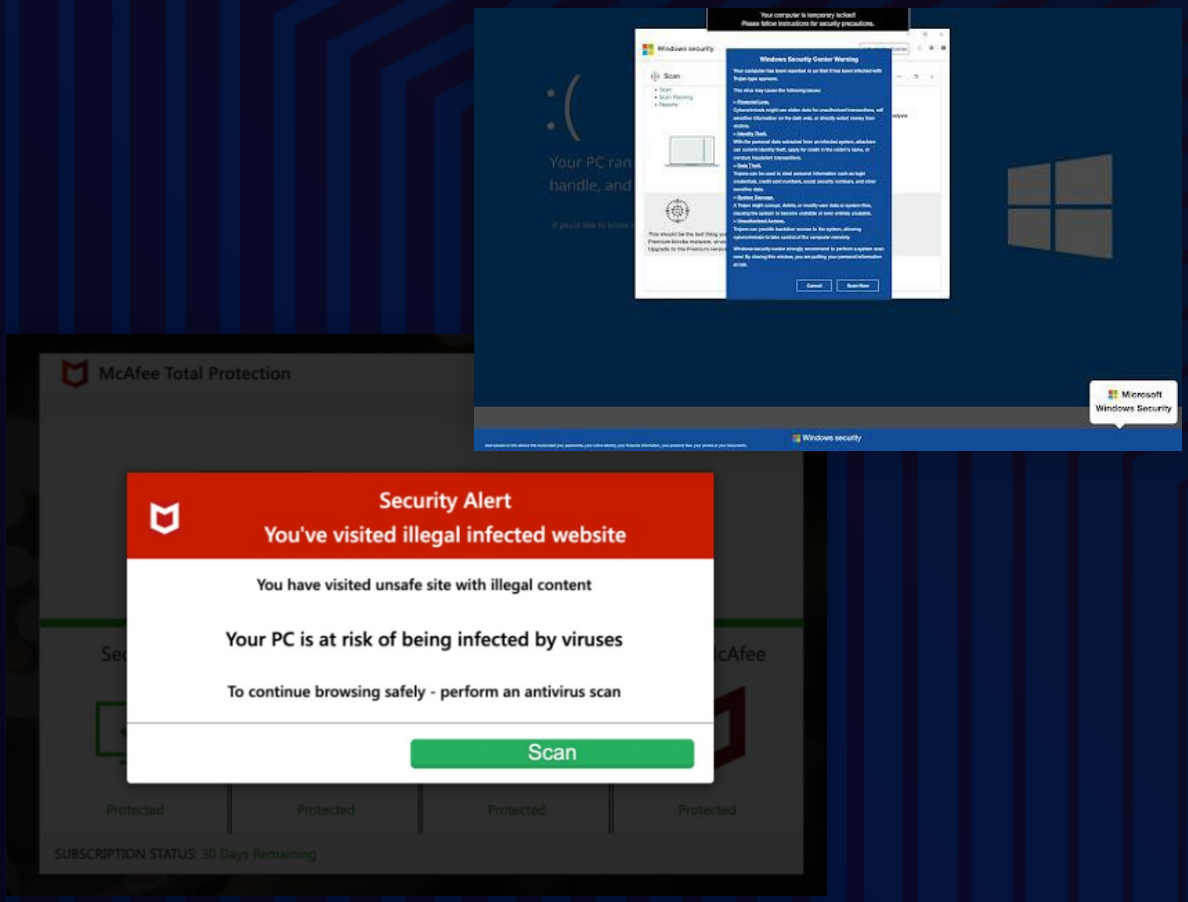
ScamClub's primary method involves using Forceful redirects, subtly guiding users to harmful websites, often hosting Scareware or fraudulent Gift-Card Scams, Carrier Branded Scams and Giveaway Scams. They skillfully penetrate established advertising networks, circumventing regular security measures to impact a broader audience.

ScamClub's recent integration into video ads marks an evolution in their strategy to ensnare more victims, and suggests a focus on amplifying their revenue streams. By injecting malicious JavaScript into conventional VPAID (Video Player-Ad Interface Definition), they employ a straightforward yet potent technique to manipulate video ad content for malicious purposes.

In September 2023 Confiant released a threat intelligence and takedown report on ScamClub enabling coordinated efforts to dismantle ScamClub's supply chain links. ScamClub had been exploiting browser vulnerabilities, including CVE-2021-1801 reported by Confiant, as well as integrating CVE-2021-23957 and CVE-2021-5840, also reported by Confiant.

DCCBOOST

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



Peak activity:
Continuous

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.

FIZZCORE

FizzCore, a malvertising threat actor primarily targeting Europe, has reemerged as a significant risk to online advertising...

Peak activity:
January, April, May, June, July

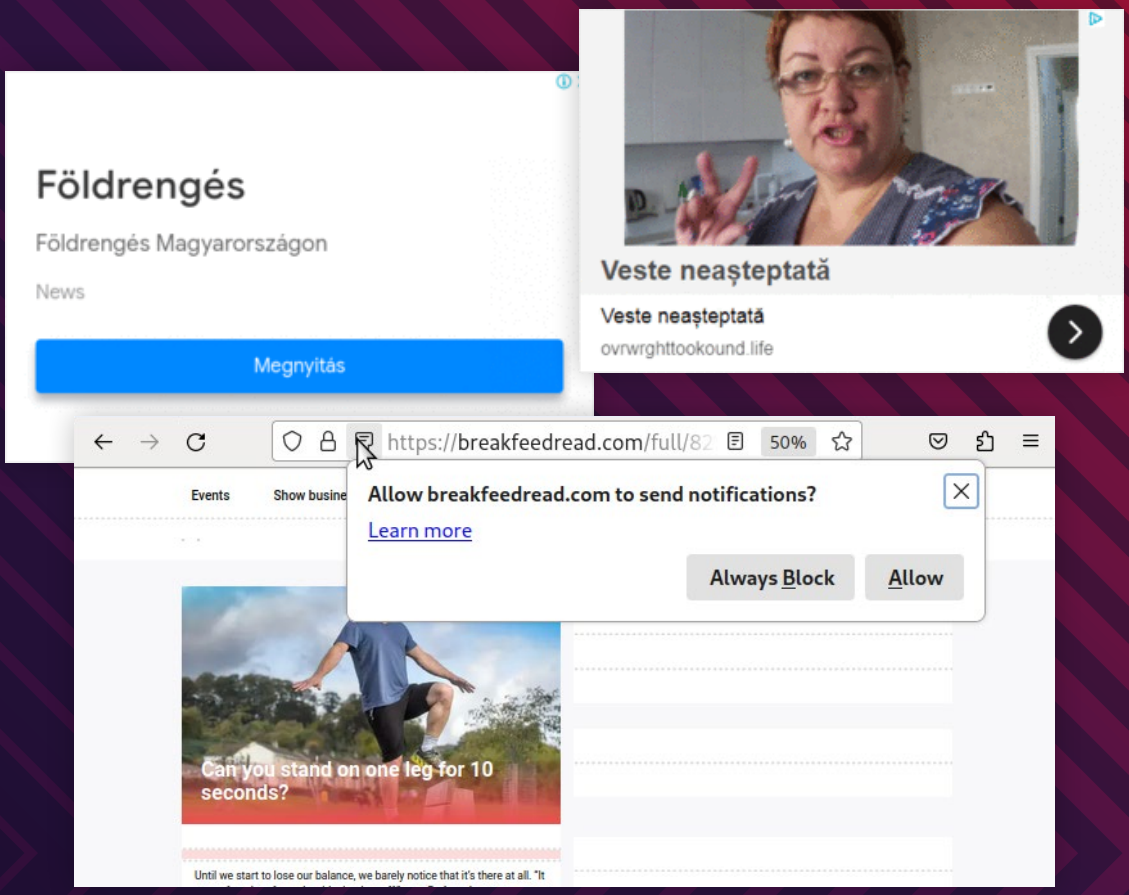
In the dynamic realm of digital threats, FizzCore, a malvertising threat actor primarily targeting Europe, has reemerged as a significant risk to online advertising and its audiences. Specializing in cryptocurrency scams, FizzCore employs a series of deceptive tactics: they start by publishing ads with shocking imagery, such as an injured celebrity, which leads to fake articles promoting Bitcoin investments, falsely appearing to be endorsed by celebrities. The misleading content often traps unsuspecting individuals, particularly retirees, into investing large sums, causing severe financial losses.

FizzCore's concern lies in its rapid and aggressive strategy of launching, leveraging the very high click-through-rate to send users to investment scams: They don't operate those investment scams, they are just a very successful affiliate.

Deeply embedded in Adtech: They are believed to have long Adtech experience. Through 2020 they touch virtually every tier1 DSP and then settled on Google DV360.

THENOVOSTI

TheNovosti is a sophisticated malvertising threat actor predominantly observed on Google Ads...



Peak activity: **Continuous**

TheNovosti is a sophisticated malvertising threat actor predominantly observed on Google Ads, with sporadic appearances on other advertising platforms such as Taboola and MGID.

TheNovosti is characterized by the employment of deceptive tactics to trick users into enabling malicious push notifications. Initially emerging in Eastern Europe, TheNovosti has shown signs of expansion but remains most active within its region of origin as of H1 2024. TheNovosti utilizes misleading page designs that appear partially loaded to coerce users into opting into push notifications, which then lead users through various malvertising chains. In some cases, the typical half-loaded page tactic is replaced by a barrage of aggressive native ads.

TheNovosti exhibits a rapid turnover of domain names, complicating tracking and mitigation efforts, with advertisement primarily featuring themes related to pensions and health, specifically targeting elderly demographics with clickbait content.

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

H1 2024

January 1st - June 30th