



# Malvertising and Ad Quality Index

---

Confiant's Malvertising and Ad Quality (MAQ) Index is a view into creative quality and security in digital advertising. Using a sample of hundreds of billions of impressions monitored in real time, Confiant is able to answer fundamental questions about the state of creative quality.

**2023 Report**  
Based on 2022 Data



# INTRODUCTION

Confiant’s Malvertising and Ad Quality (MAQ) Index is a view into creative quality and security in digital advertising. Using a sample of hundreds of billions of impressions monitored in real time, Confiant is able to answer fundamental questions about the state of creative quality.

Digital advertising delivers significant value to publishers but also introduces myriad risks related to security, privacy, and user experience. Malicious, disruptive, and annoying ads degrade user experience and drive adoption of ad blockers. Apart from the MAQ, there are few — if any — systematic studies on the frequency and severity of ad quality issues as experienced by the real victims: end users.

Part of this is due to data issues: it had historically been challenging to estimate impact without client-side instrumentation in place on a large and diverse set of publishers. The advent of Confiant’s real-time creative-verification solution in 2017 created a new way to examine the problem, revealing the underlying causes for the first time. 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.

In 2018, Confiant released the industry’s first benchmark report. This report, the 17th in the series, covers all of 2022.



# METHODOLOGY

To compile the research contained in this report, Confiant analyzed a normalized sample of more than 850 billion advertising impressions monitored from January 1 to December 31, 2022, across tens of thousands of premium websites and apps from top publishers like Paramount, Gannett, Nexstar, and CafeMedia.

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 metrics in this report may not match those in prior reports.



# WHAT'S NEW

## Different in 2022

- We added two new SSPs — SSP-O and SSP-P — bringing our total to 14. The SSP Rankings now include Google, Magnite, OpenX, Xandr, Yahoo, Index Exchange, Pubmatic, GumGum, Sonobi, TripleLift, Sharethrough, Media.net, 33Across, and Sovrn.
- We refactored our quality score to remove an issue that was largely outside of the SSP's control. We've restated quality numbers for 2021 to provide an apples-to-apples comparison.
- We broadened the set of publishers from which we pull our data.
- For the full year report, we added Amazon TAM to the bidding framework report.



## 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)<sup>1</sup>

## Quality Violations

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

Top issues include:

- Heavy Ads
- Misleading Claims
- Video Arbitrage (formerly In-Banner Video)
- Undesired Audio
- Undesired Video
- Undesired Expansion

---

<sup>1</sup> Ad platforms that consistently serve abnormal levels of malicious ads and are the preferred vector for malicious actors.



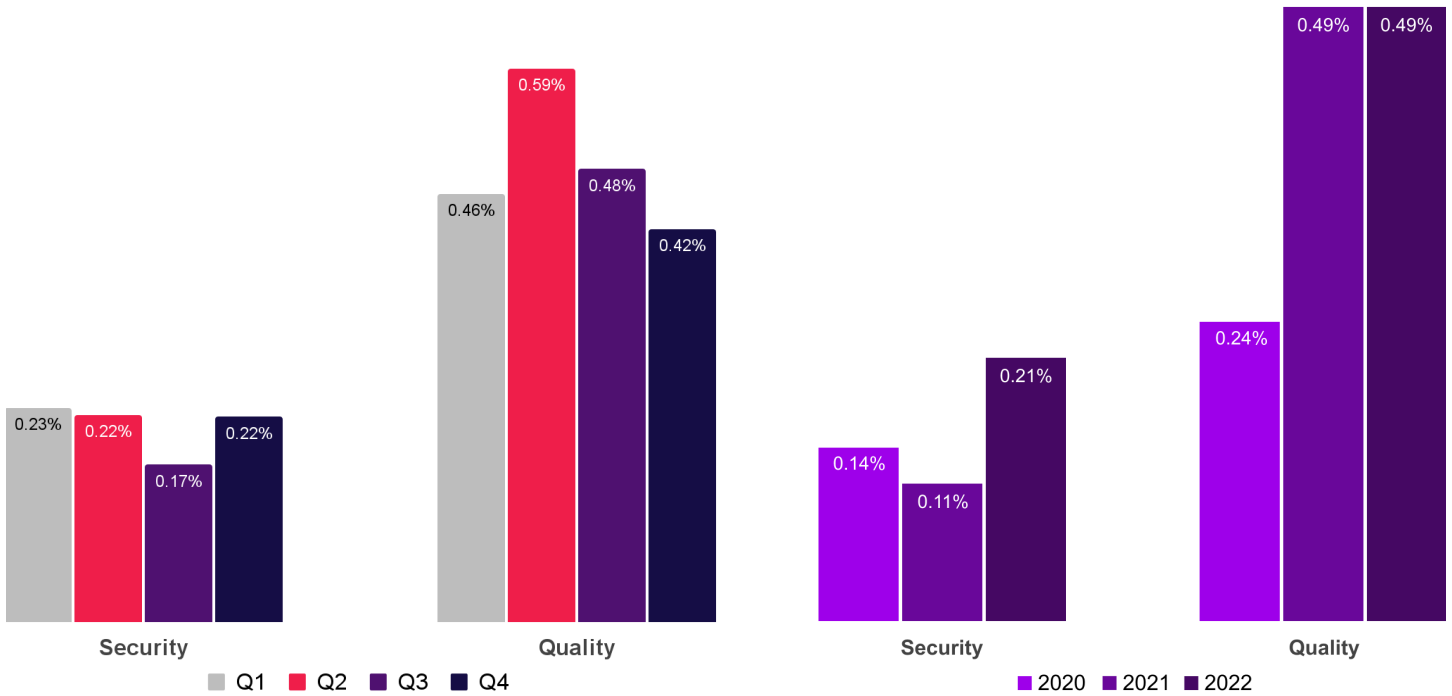
# Industry View

2022



## Quarterly View: 2022

## Annual View



### How did the industry fare?



The industry-wide **security violation rate** nearly doubled in 2022, reaching its highest level since 2019.

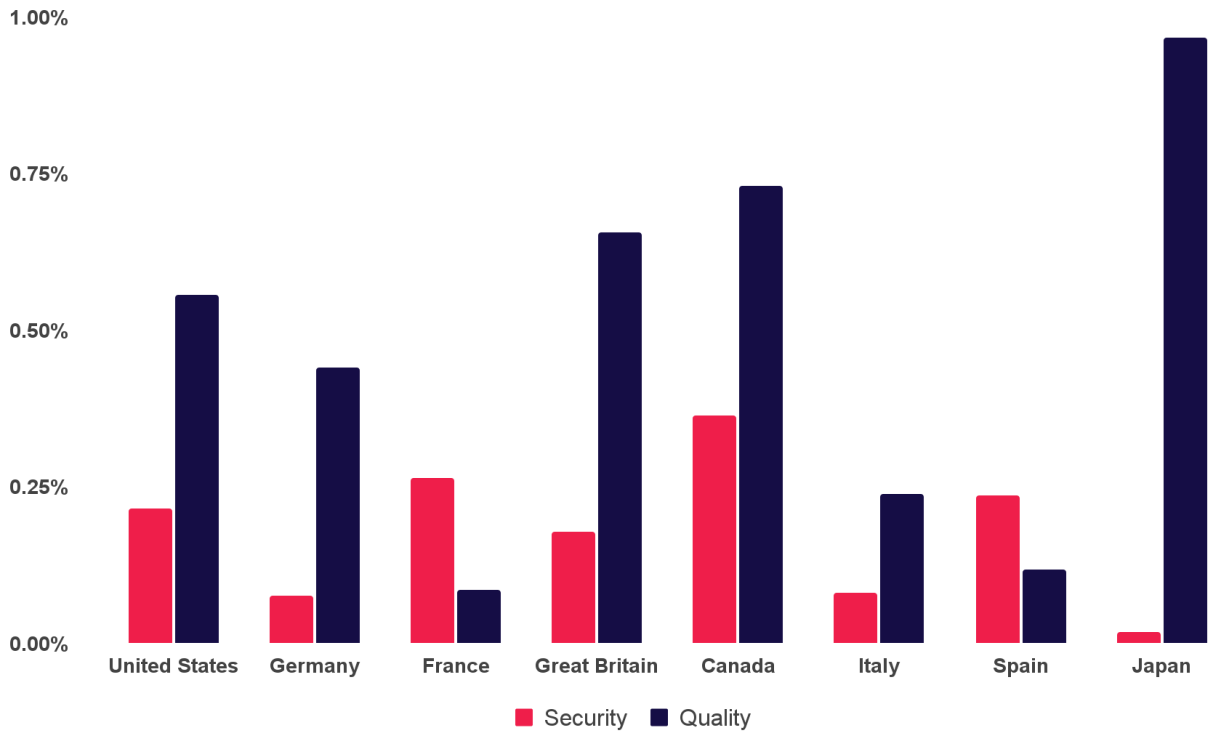
The **quality violation rate** held steady at 0.49%, but has increased 104% since 2020. The rate has been on a downward trend since peaking in Q2.



**The security violation rate in 2022 hit its highest level in three years.**





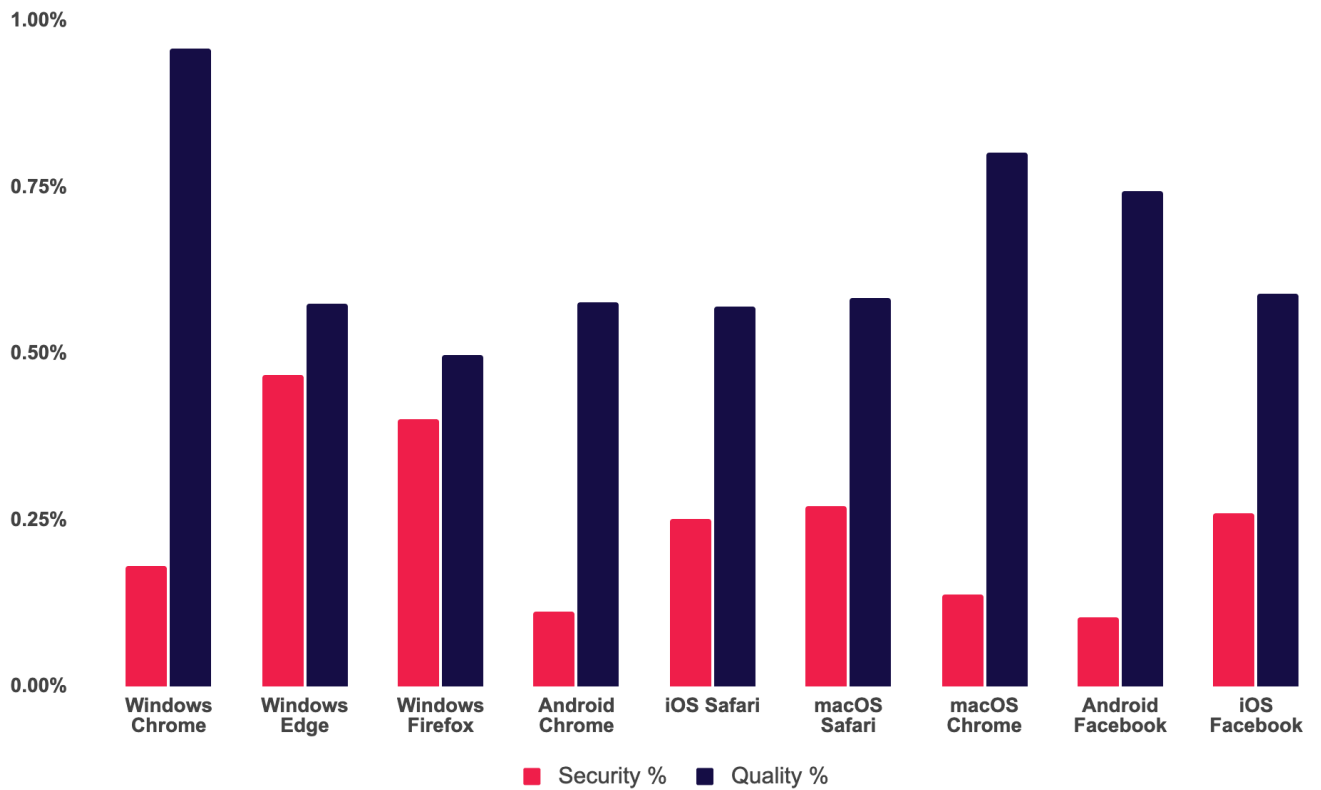


## 2022 Violation Rates by Country



For the year, **Canada had the highest rate of security issues**, 27.8% higher than the next highest, France. Security rates moderated in most of the European market, with **Germany and Italy being the safest markets**.

**The quality violation rate was highest in Japan, Canada, and Great Britain**, driven by Heavy Ads and Misleading Claims.



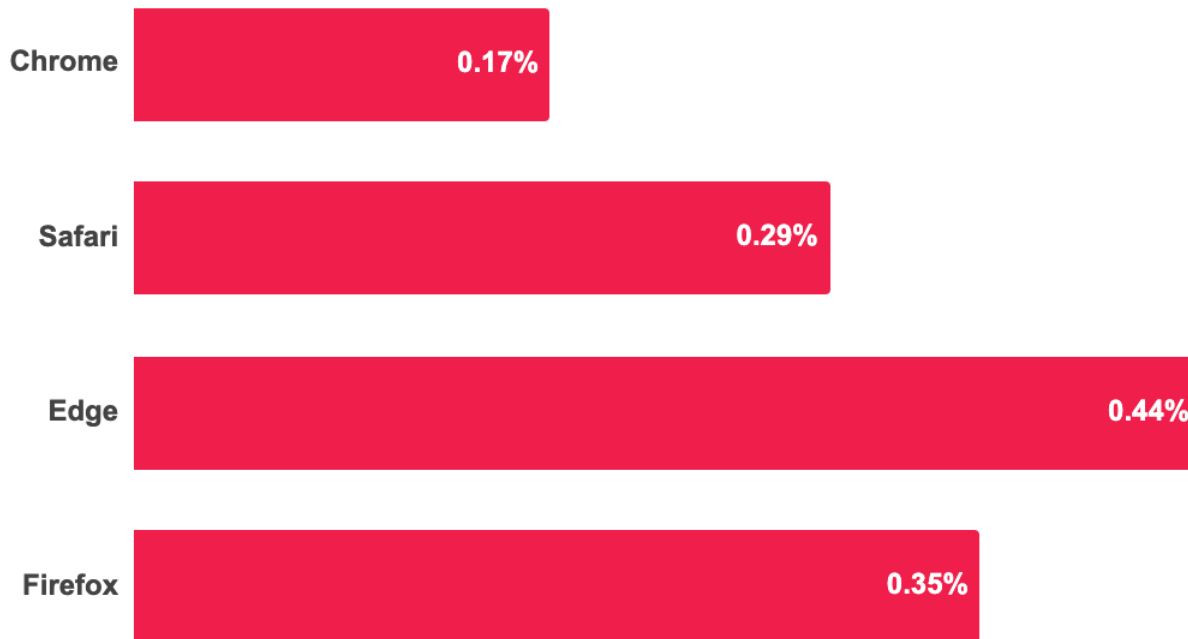
## 2022 Violation Rates by Browser



For the year, **users of Edge for Windows experienced the highest rate of ad security issues, barely edging out Firefox users.**

Conversely, browsers that performed well for security such as Chrome for Windows and macOS tended to be relative laggards when it came to quality.

Of course, it's difficult to disentangle whether these rates are influenced more by differing user bases or actions taken by the browsers, but given how widespread Chrome is, superior defenses are a strong possibility.



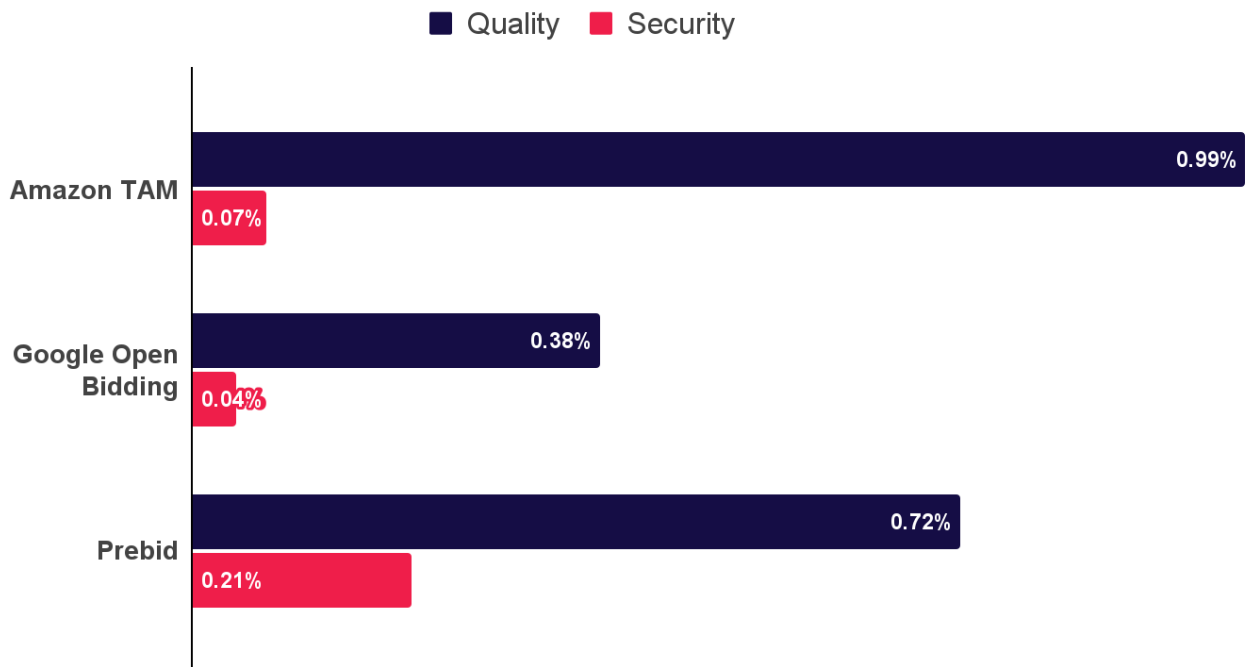
## 2022 Security Violation Rates by Browser Family



Most browsers are available for multiple operating systems and devices. When browsers are grouped as a family, interesting patterns emerge.

**In 2022, Edge browser users were the most impacted by security issues**, followed closely by Firefox (the previous year's worst performer). Safari and especially Chrome were far less likely to experience ads with security issues.

**...Edge browser users were the most impacted by security issues...**

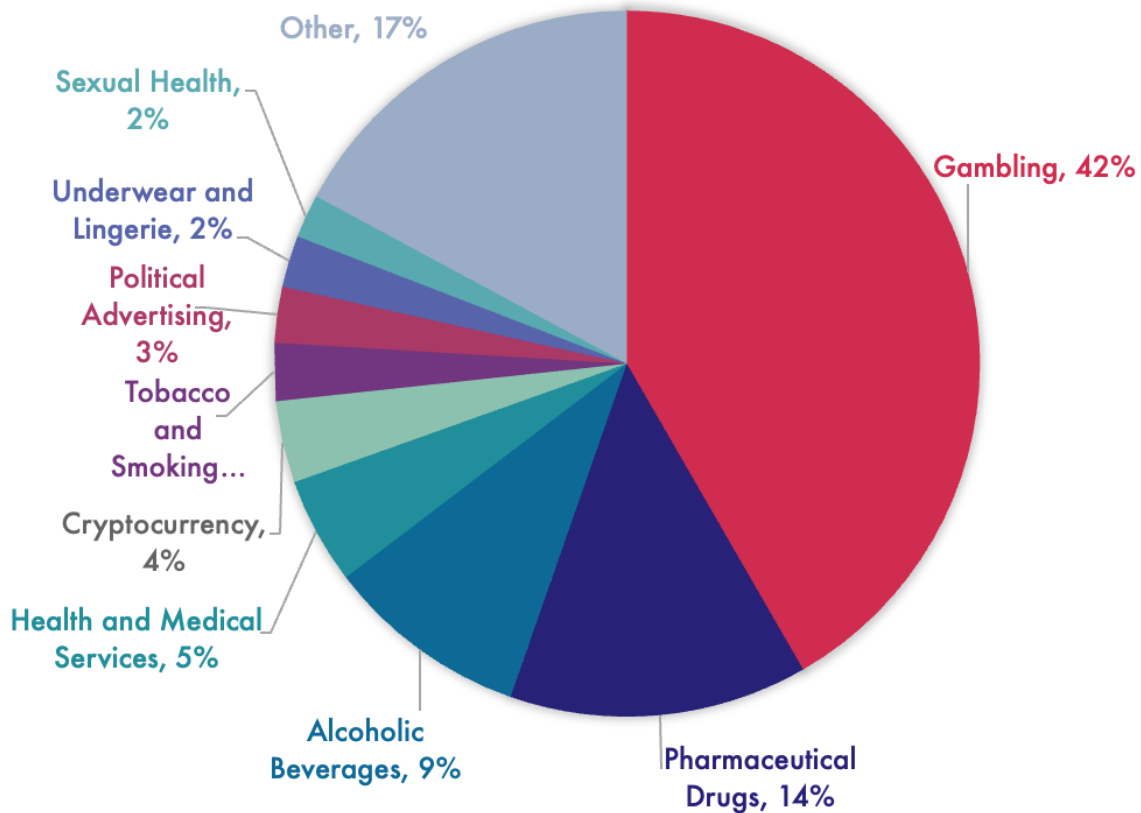


## 2022 Violation Rates by Bidding Framework



Publishers use frameworks like **Prebid** and **Amazon TAM** to manage bidding from multiple SSPs. Google offers a similar feature called **Open Bidding**. In each of these cases, demand from a diverse set of SSPs flows through the framework, exposing publishers to security and quality issues.

In 2022, **Google Open Bidding outperformed Prebid and Amazon TAM on both security and quality issues.**



"Other" includes over 100 other categories

## Most Blocked Ad Categories



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

**Gambling and Pharmaceutical Drugs remained the most blocked ad categories** by publishers in both H1 and H2. These two ad categories alone represent over 50% of all blocks. Blocks for Alcoholic Beverages, Health and Medical Services, and Cryptocurrency rounded out the top five blocked categories of the year.

**Blocks for Cryptocurrency ads declined precipitously in the second half**, no doubt driven by the implosion in that sector.



# SSP Rankings

2022



## 2022 SSP Rankings

In 2022, Confiant tracked impressions from over **100 SSPs and demand sources**. However, the majority of **global impressions originated from 14 providers**<sup>2</sup> 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.

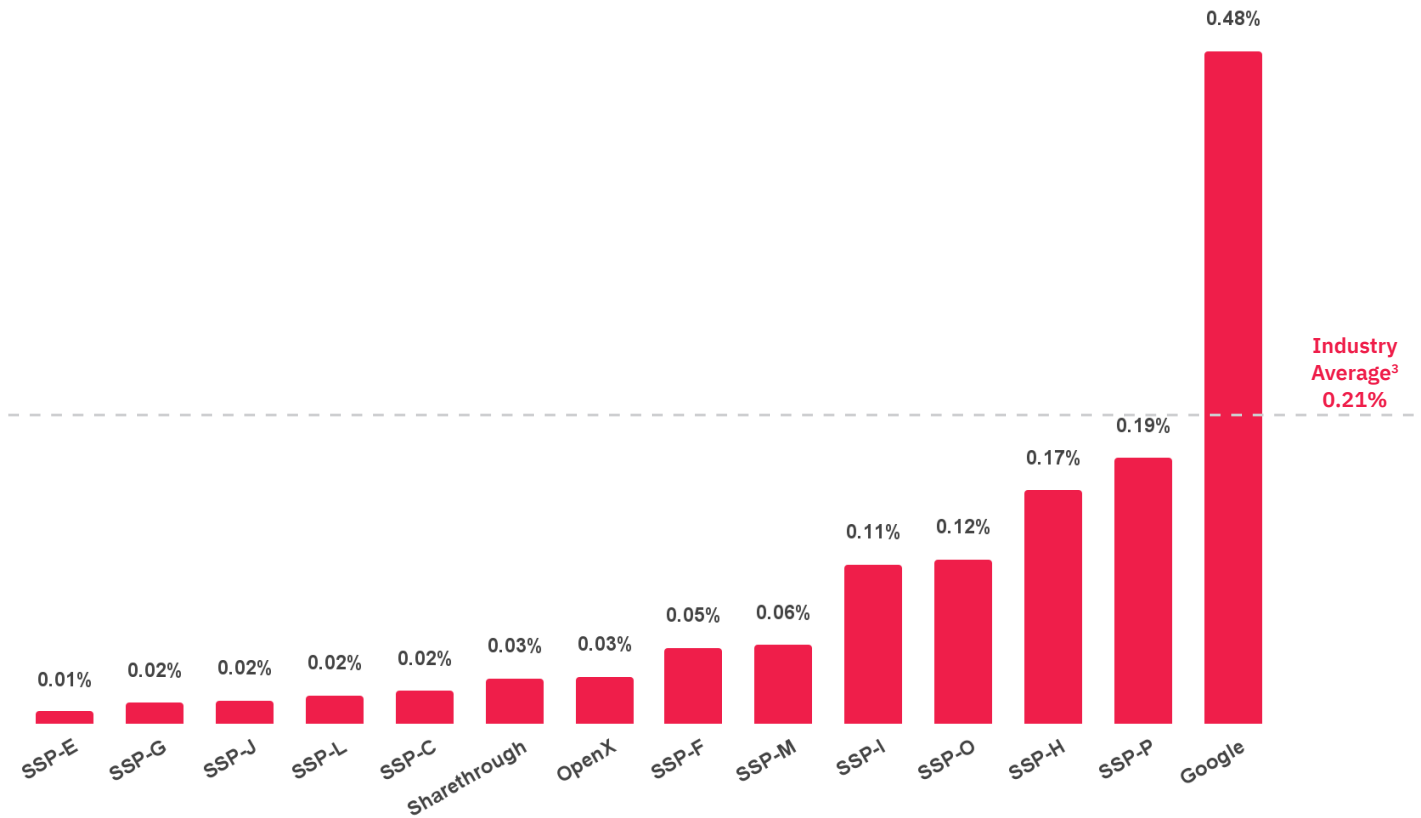
To qualify for inclusion, a provider had to have been a consistent source of **at least one billion Confiant-monitored impressions** per quarter across a cross-section of publishers in our global sample.

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.

---

<sup>2</sup> Google, Magnite, OpenX, Xandr, Yahoo, Index Exchange, PubMatic, GumGum, Sonobi, TripleLift, Sharethrough, Media.net, 33Across, and Sovrn





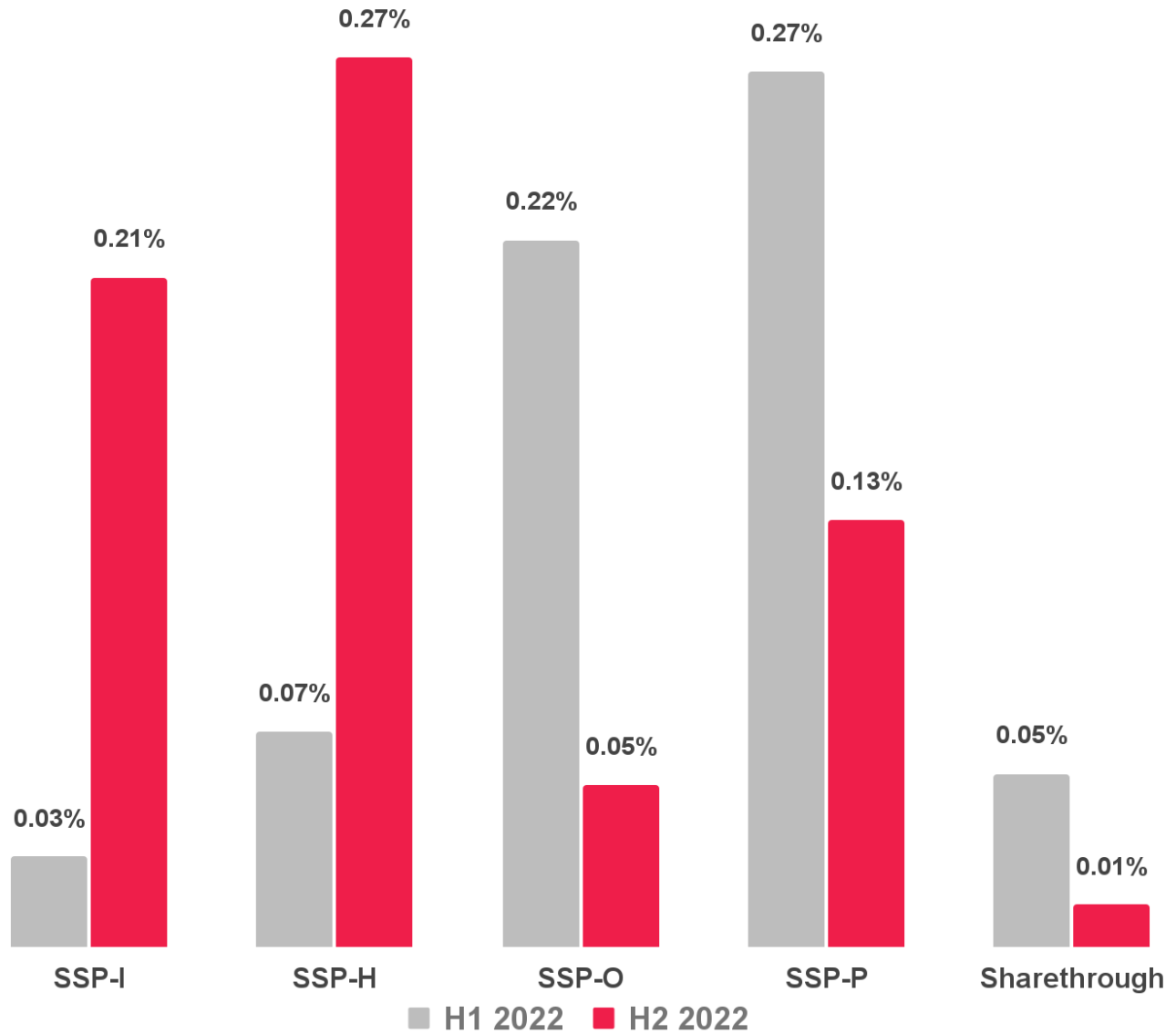
<sup>3</sup> The weighted average across all SSPs based on impression volume.

### Security Violation Rate by SSP



In 2022, SSPs H, P, and Google struggled with high security violations rates.

The top performers for the year for security were SSP-E, SSP-G, and SSP-J, with SSP-E beating 2021's winner SSP-G by a hair.



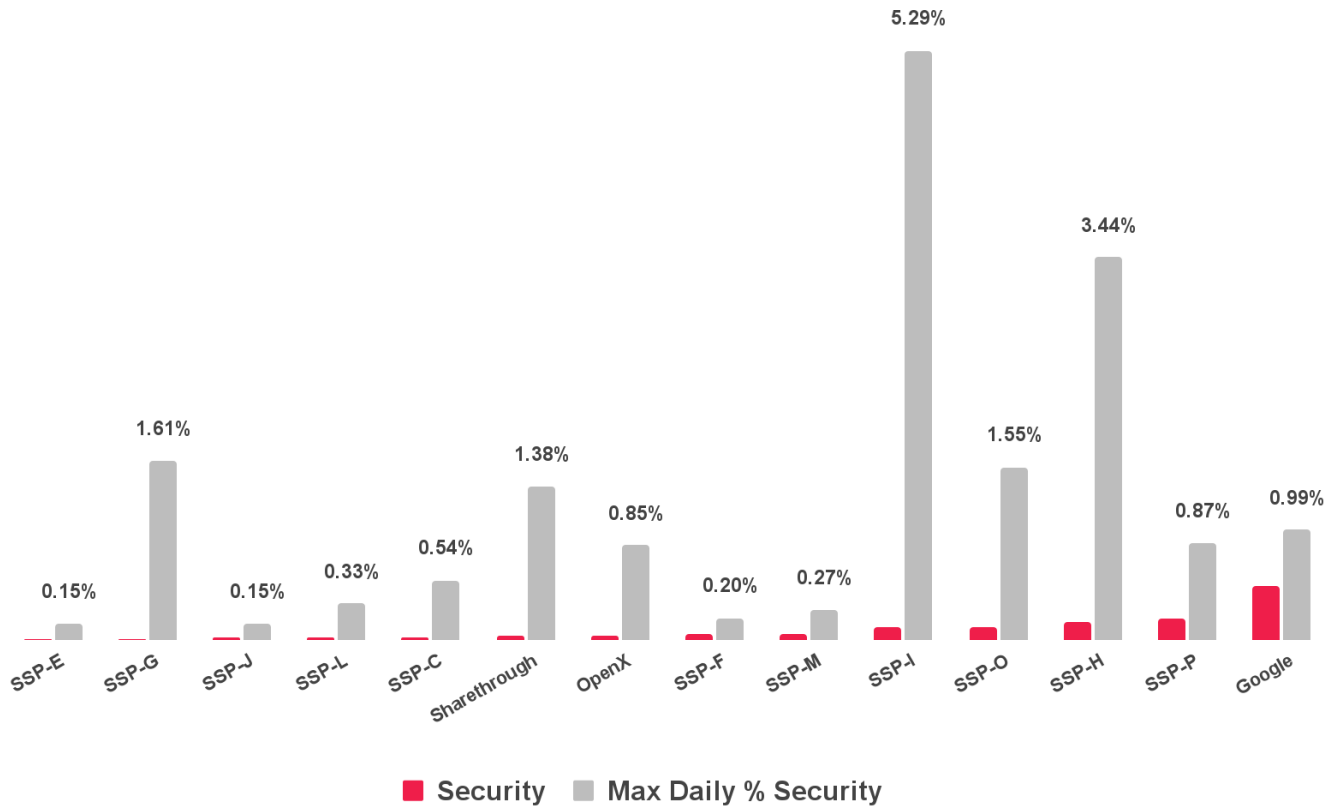
### Security Violation Rate: H1 VS. H2



When comparing H1 and H2 in 2022, security violations decreased dramatically at **Sharethrough**, **SSP-O**, and **SSP-P**.

While Google's violation rate got better in H2 compared to H1, its violation rate was still highest of all included SSPs in both periods. **SSP-H** had a bad second half, marring a reasonably good performance in the first half.

In H1, Sharethrough had the lowest violation rate apart from SSP-E. Conversely, the **violation rate at SSP-I and SSP-H spiked**, pushing them out of the top performers.

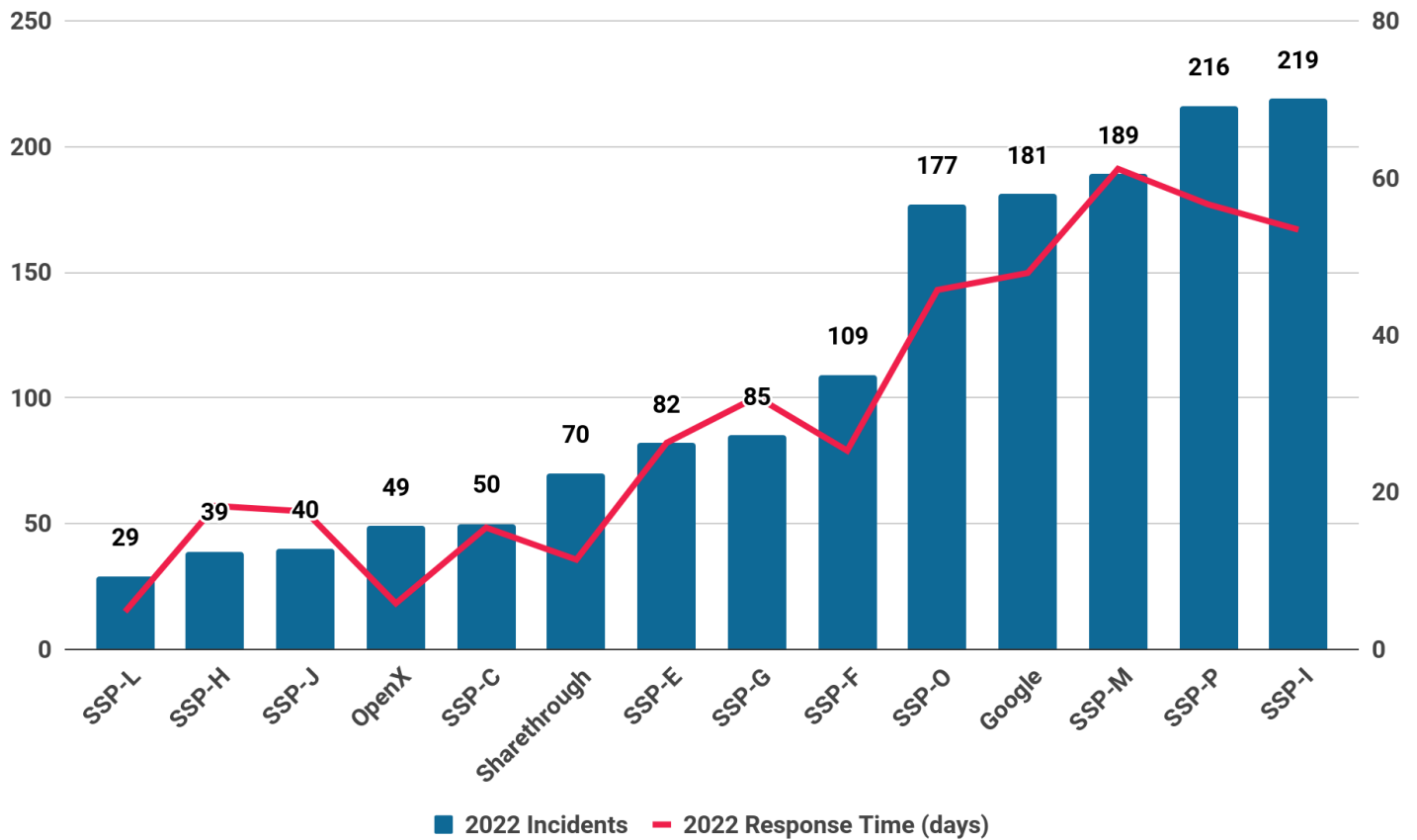


## Daily Maximum Security Rate by SSP



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 2022, **SSP-I recorded the highest daily security rate for the quarter**, at 5.29%, meaning that for a particular day, more than one in 20 impressions from SSP-I had security issues. Other outliers included SSP-H, at 3.44%, and SSP-G at 1.61%.

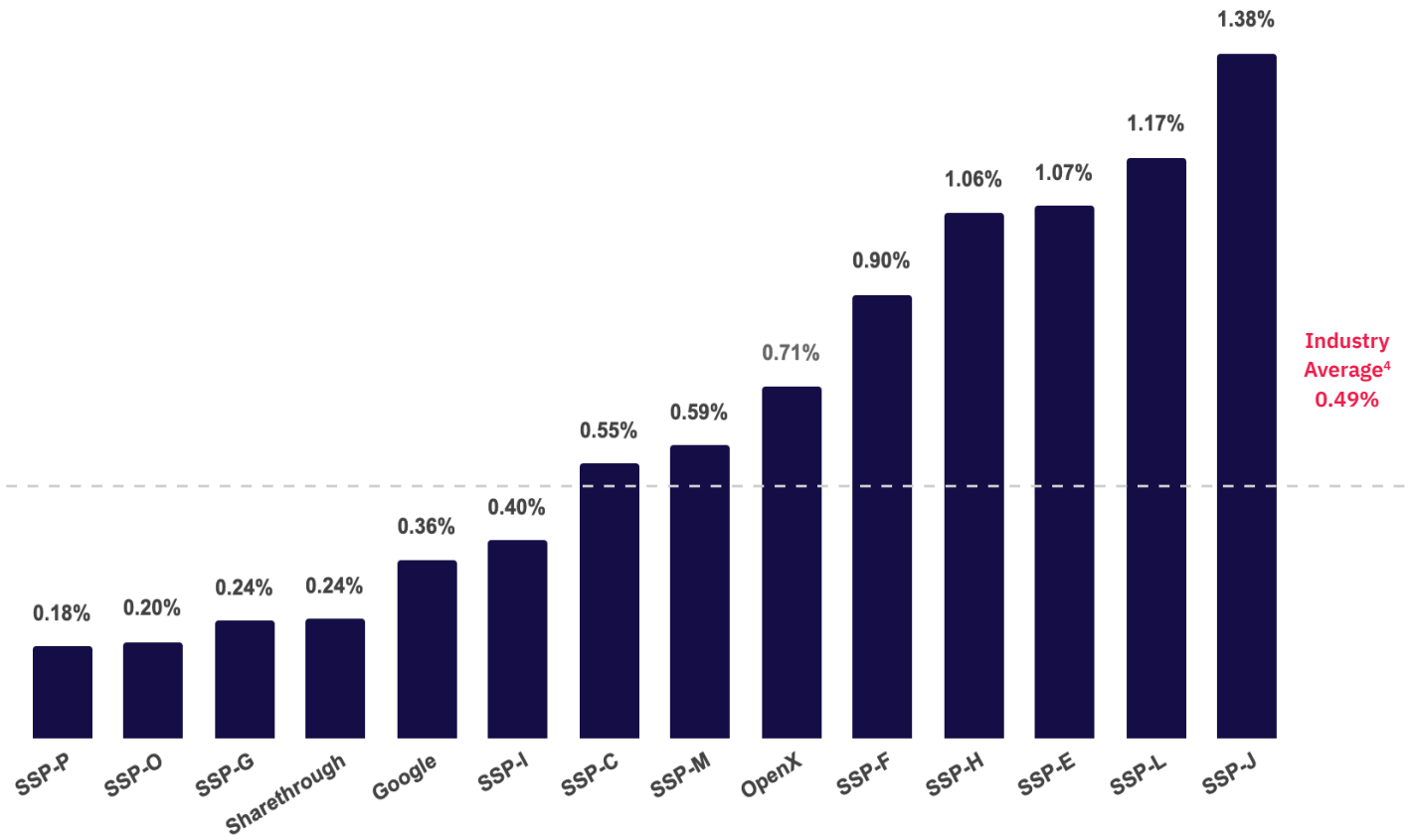


## Incidents and Average Response Time



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.

In 2022, **SSP-L and OpenX had the fastest response time**, while **SSPs L and H experienced the fewest incidents**. SSPs P and I performed poorly on both measures.



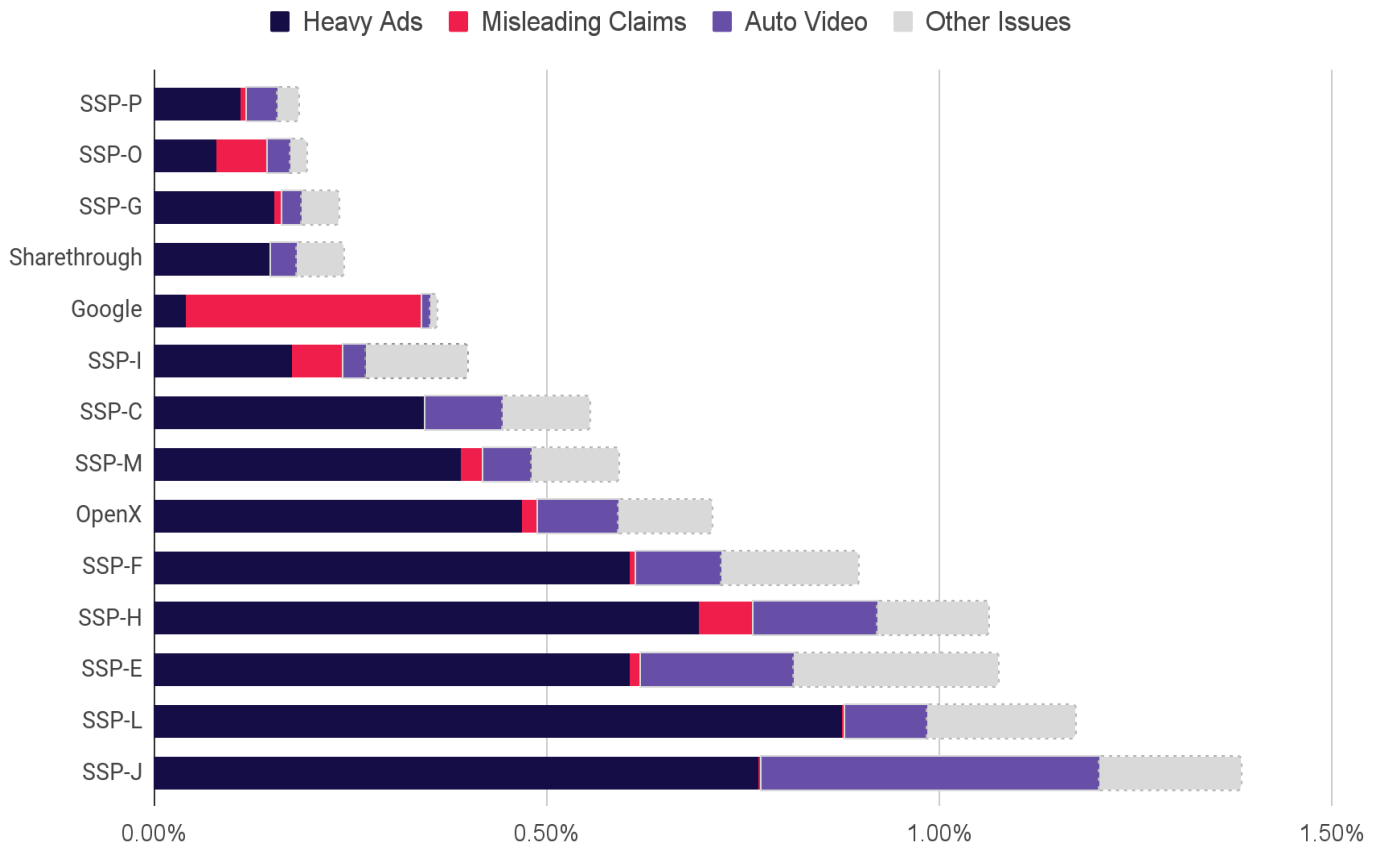
<sup>4</sup>The weighted average across all SSPs based on impression volume.

## Quality Violation Rate by SSP



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

**SSP-J** continued to trail all other major SSPs, as they did in 2021, while newcomers **SSP-O** and **SSP-P** lead the pack.



## 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 — are a growing issue with Google, SSP-O, SSP-I, and SSP-H. For the worst-performer of the group, one in every 330 impressions was a misleading claim, which was far more than the others.



## VIOLATION RATES BY SSP



A record five SSPs had better-than-average performance for both security and quality (as indicated by the shaded square): **Sharethrough, SSP-G, SSP-O, SSP-I, and SSP-P**. All other SSPs tended to perform well on one measure but not the other.



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



# Major Threat Activity

2022



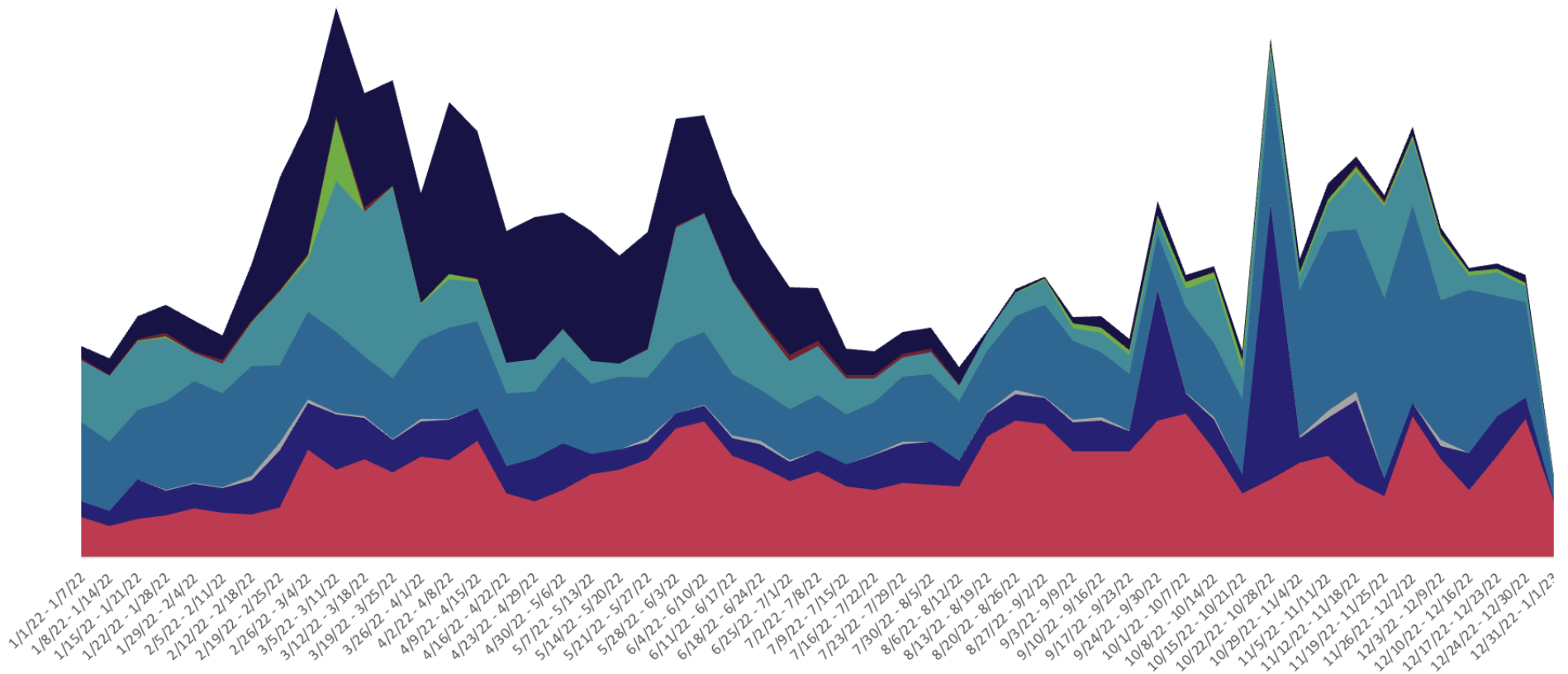


## Threat Detail



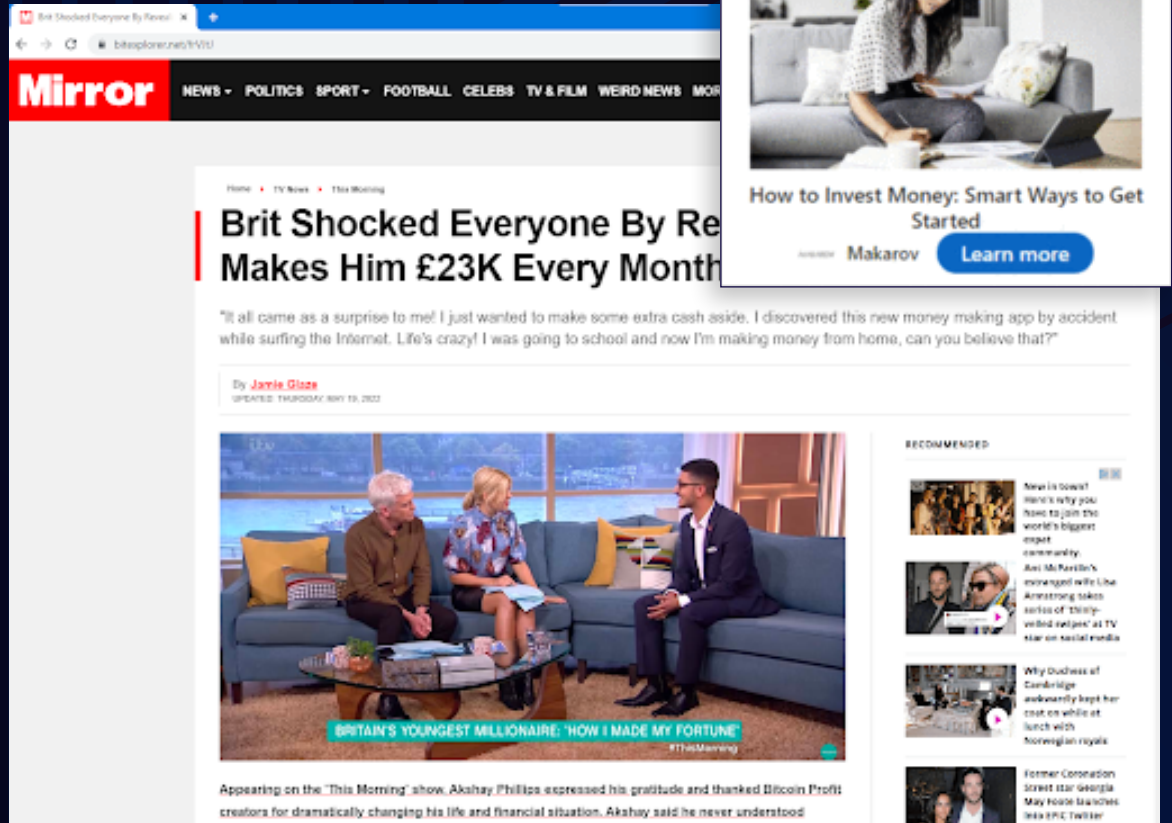
The nature of security threats shifts constantly as attack techniques fall in and out of favor. During Q1 and Q4, **Fake Update ads** predominated. In Q2, **Phishing Scams** came to the fore. **Forced Redirects** came in two large waves, first in March and again in late May to mid-June, but were quiet for much of the second half of the year.

- Cloaking
- Criminal Scams
- Fake Ad Server
- Fake Update
- Forced Redirect
- Ad Stacking
- Pixel Stuffing
- Phishing Scams
- Crypto-mining



# LOOSECNTACT

LooseContact is a new malicious actor focused exclusively on crypto-themed investment scams trafficked via LinkedIn...



Peak activity:  
Continuous

LooseContact is a fairly new malicious actor focused exclusively on crypto-themed investment scams trafficked via LinkedIn (including LinkedIn DSP).

LooseContact uses an innovative “cloaking sandwich” approach with multiple layers. The outer layer uses URL shortening services like Bitly to mask a malicious domain. In the inner layer, a malicious domain behaves like a regular click tracker, simply forwarding clicks to legitimate websites (like Nerdwallet).

This technique, combined with very innocuous looking ad creatives, makes it very challenging for ad tech providers to weed out this threat actor.



# CASHREWINDO

First seen in 2018, CashRewindo distributes attacks all around the globe, smuggling malicious code...



Peak activity:  
**June, Sep-Oct  
2022**

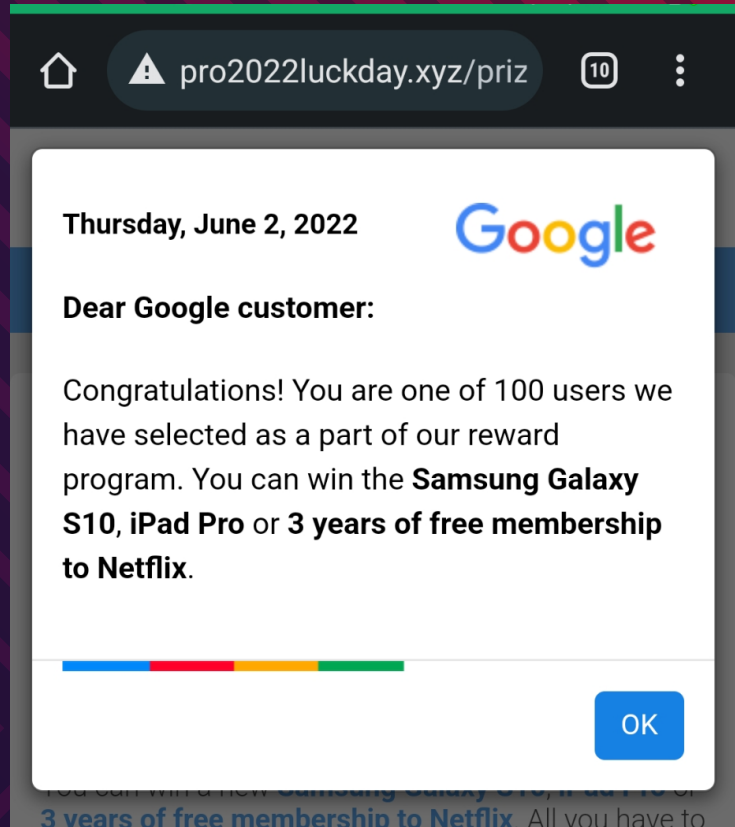
First seen in 2018, CashRewindo distributes attacks all around the globe, smuggling malicious code in common JavaScript libraries and aging domains like fine scotch.

CashRewindo's creative strategy consists of flipping between scam ads and innocuous wording. At the beginning of the campaign, they typically run placeholder ads that don't trigger language detection and only later switch to actual call-to-action ads.

CashRewindo has another trick up its sleeves: domain aging. Most of the IOCs we collected have domains that were registered two or three years ago, only to be activated just in time for a new campaign.

# SCAMCLUB

ScamClub malvertisements are defined mainly by Forced Redirects to fake gift or reward scams.



Peak activity:  
**Continuous**

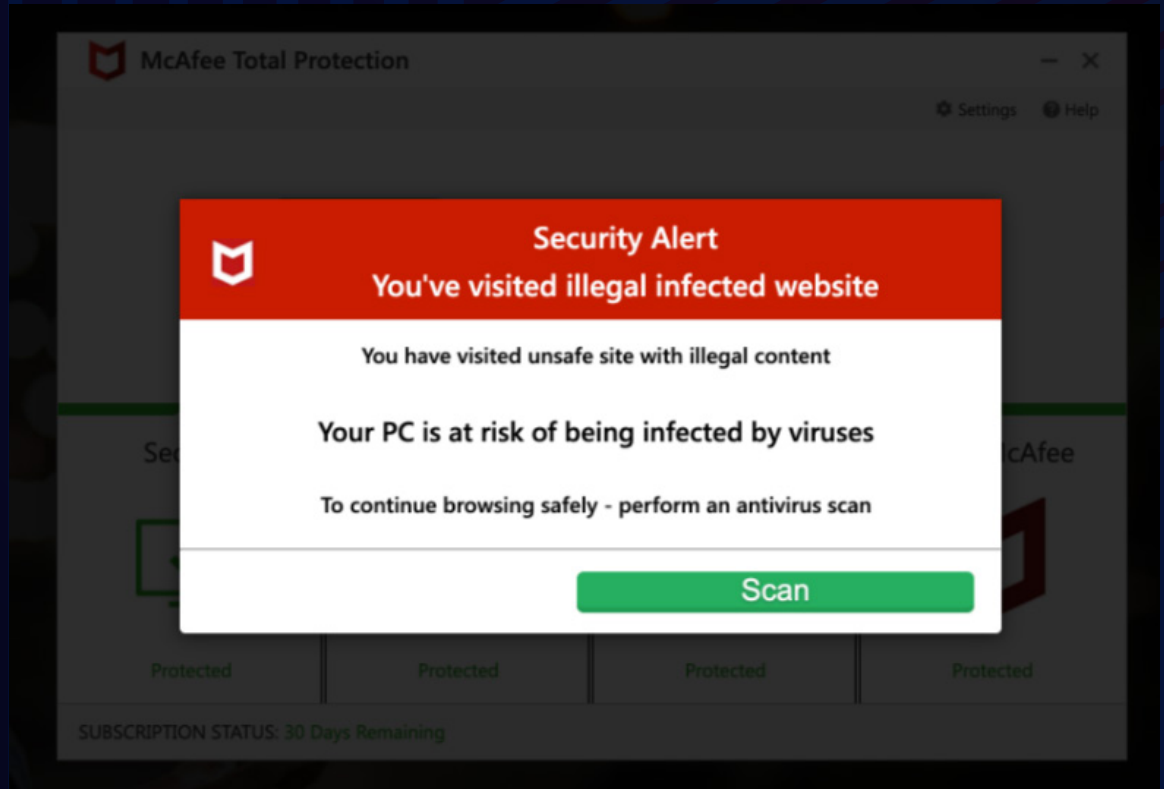
Active for many years now, ScamClub malvertisements are defined mainly by forced redirects to fake gift or reward scams.

While the phenomenon of forced redirects has progressively receded, ScamClub continues to operate on ad platforms that struggle with ad security and/or don't vet their buyers adequately.

ScamClub was abusing a browser vulnerability that Confiant [reported](#) last year (CVE-2021-1801).

# DCCBOOST

DCCBoost was very active in the first quarter of 2022, but then significantly slowed down their activity.



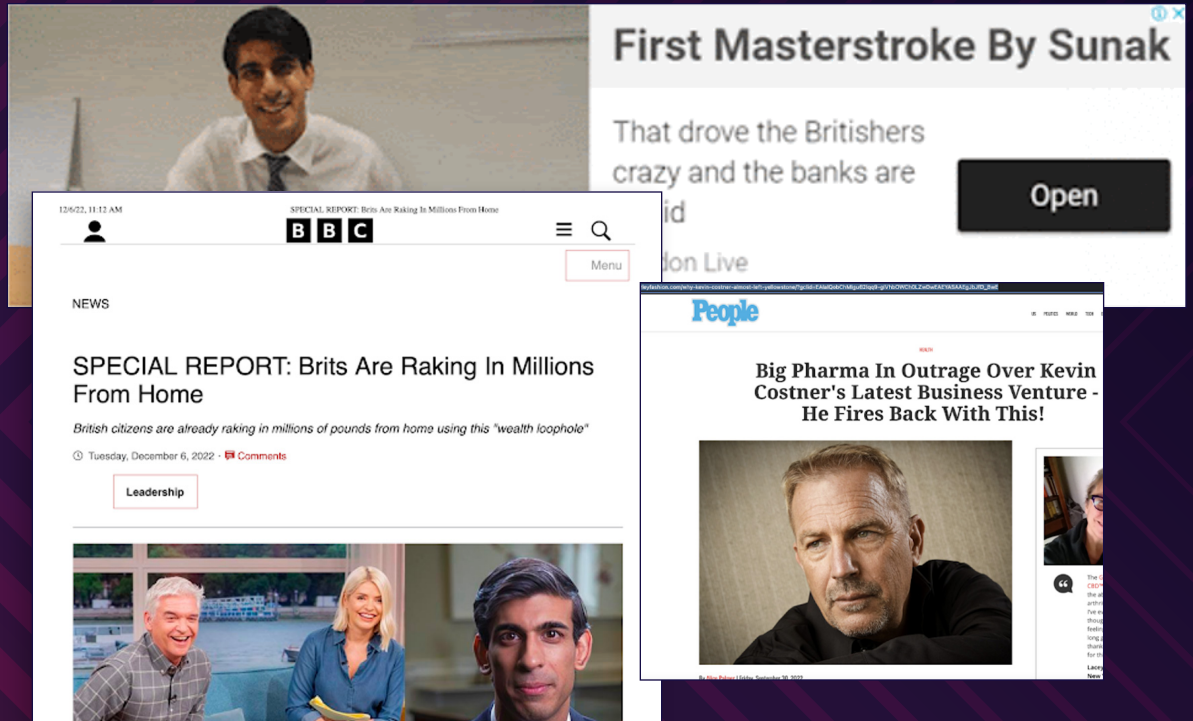
Peak activity:  
**Q1 and Q4 2022**

In Q4 2021, DCCBoost successfully transitioned to campaigns forcefully redirecting desktop users to a site that poses as McAfee and executes a fake antivirus scan. Previously, they had been targeting mobile devices for years.

DCCBoost was very active in the first quarter of 2022, but then significantly reduced their activity. They slowly and patiently ramped up again during the summer with multiple spikes in Q4.

UP225

Celebrities are big business. Especially when threat actors abuse their image to run criminal scams.



Peak activity:  
**October 2022**

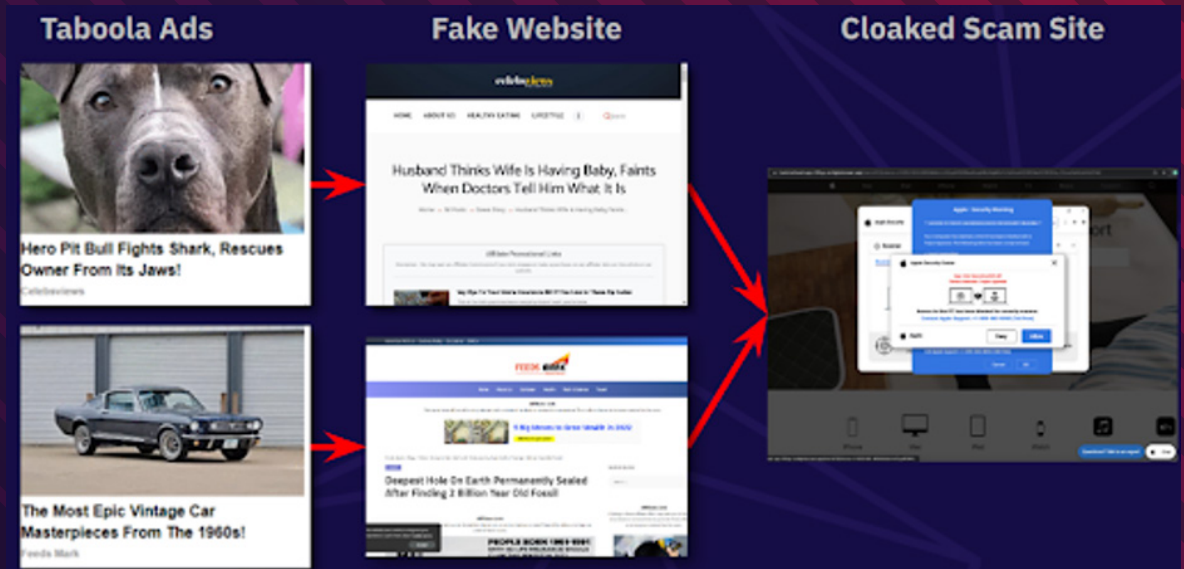
Celebrities are big business. Especially when threat actors abuse their image to run criminal scams. Malvertiser Up225 ran a malicious campaign focused on Rishi Sunak who became UK's prime minister in October. The attack posed as a BBC article to advertise for a supposed "wealth loophole".

In Australia, same scheme, different celebrity and news outlet: Threat actor Up225 posed as ABC News using Kevin Rudd, Australia's former prime minister.

In the US, Big Pharma is outraged. This time we have a health scam that leverages Kevin Costner and the People magazine brand.

# AALGMOR

First spotted in July of this year in Search ads (Bing), the actor quickly settled on Native ads primarily served through Taboola...



Peak activity:  
**August, October  
2022**








One of the leading purveyors of tech support scams was Aalgmor. First spotted in July of this year in Search ads (Bing), the actor quickly settled on Native ads primarily served through Taboola, with a large campaign in August.

Aalgmor was active every single day during the month of October with campaigns running on average for 13 days (up to 24 days). With 3 active campaigns going at once, they have mastered the art of persisting by reproducing the click-bait style of low quality native ads.

On peak days in October, Aalgmor's reach exceeded 0.4% of all Taboola ads, making it one of the largest sources of Tech Support Scams.



## CONCLUSION

-  **We detected serious security or quality issues in one of every 140 impressions**, a significant increase over both 2020 and 2021.
-  The **security violation rate** in 2022 hit its **highest level in three years**.
-  **Canada** had the **highest rate of security issues**, 27.8% higher than France. Security rates moderated in other European markets.
-  **Microsoft's Edge** browser users were the most impacted by security issues, **with a rate three times worse than Google Chrome users. Mozilla's Firefox users** followed closely behind Edge with the second highest security violation rate.
-  **Blocks for Cryptocurrency ads declined precipitously** in the second half, after ranking as the third most blocked category by publishers in the first half of the year.
-  We found high rates of ads with **Misleading Claims** across four of the top SSPs. For the worst-performer of the group, one in every 330 impressions was a misleading claim.
-  **Fake Update ads** predominated in Q1 and Q4, and were **the top security issue for the latter quarter**.



## 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 our 10th anniversary this year.

[LEARN MORE](#)



# Malvertising and Ad Quality Index

---

[confiant.com/maq-index](https://confiant.com/maq-index)

For more information on our entire suite of Security, Quality, and Privacy protection products please visit our website or email us at:

[marketing@confiant.com](mailto:marketing@confiant.com)

**2023 Report**  
Based on 2022 Data