CONFIANT

Demand Quality Report

Q2 2020

Introduction

Confiant's **Demand Quality Report** is a quarterly look into the quality of demand in digital advertising. Using a sample of over 170 billion impressions monitored in real time, Confiant is able to answer fundamental questions about the state of ad quality in the industry at large.

Digital advertising delivers significant value to publishers but introduces myriad risks related to security 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 has historically been challenging to estimate impact without client-side instrumentation in place on a large and diverse set of publishers. The Demand Quality Report, which leverages Confiant's position as the vendor of choice for real-time creative verification, aims to change that.

In September 2018, Confiant released the industry's first benchmark report. This report, the ninth in the series, covers Q2 2020.

Methodology

To compile the research contained in this report, Confiant analyzed a normalized sample of **more than 170 billion programmatic advertising impressions** from April 1 to June 30, 2020 from **over 30,000 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 real impressions for real users 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.

With the exception of the Q2 Rates by Country slide, all data and charts are based on traffic generated in the United States.

Definitions

Security violations

Attempts to **compromise the user** through the use of malicious ads, trickery, and other techniques. In this report, we break out:

Malicious ads

A creative that includes (often obfuscated) JavaScript that spawns a forced redirect or loads a secondary payload for malicious purposes. Most malicious ads exist for the purpose of forcing users to interact with phishing scams, but some infect the user's device to propagate botnets and other nefarious activities.

High-Risk Ad Platforms (HRAPs)

Ad platforms that consistently serve as major attack vectors for malicious actors. For a platform to receive this designation, we have to consistently observe malicious campaigns on an ongoing basis so that it becomes unclear whether the platform is negligent, complicit, or just overwhelmed.

Quality violations

Non-security issues related to the ad behavior, file weight, or content. In this report, we break out:

In-Banner Video (IBV) ads

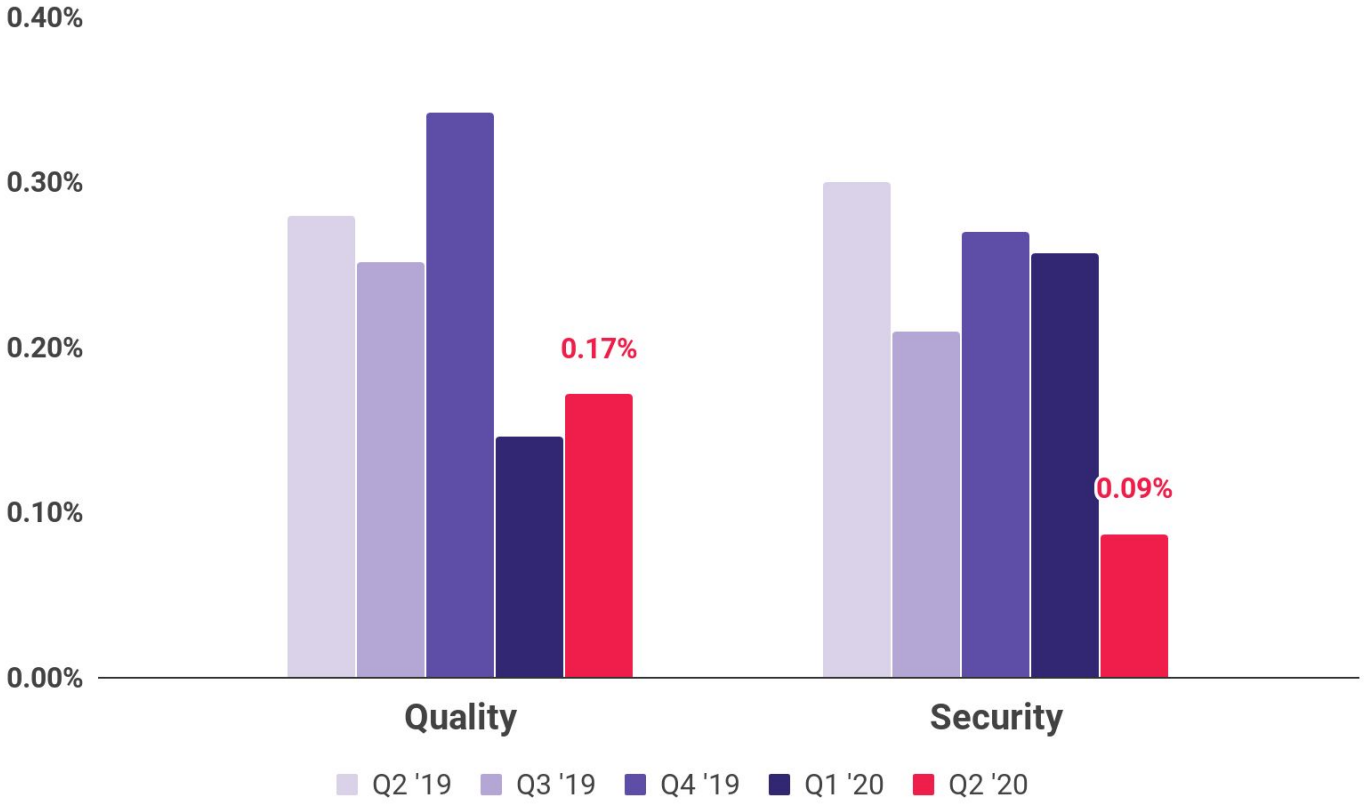
The practice of serving video ads in banner placements without the publisher's consent, and often without the advertiser's consent, either. Exploiting an arbitrage opportunity between Display and Video marketplaces, a video ad unit is loaded within a banner placement instead of playing within a media player.

Other Quality issues

Creative violations across a wide range of different quality specifications selected by the publisher. The dimensions include audio/video related violations, creatives probing for user's geolocation, the network load of the ad, and much more.

Industry View

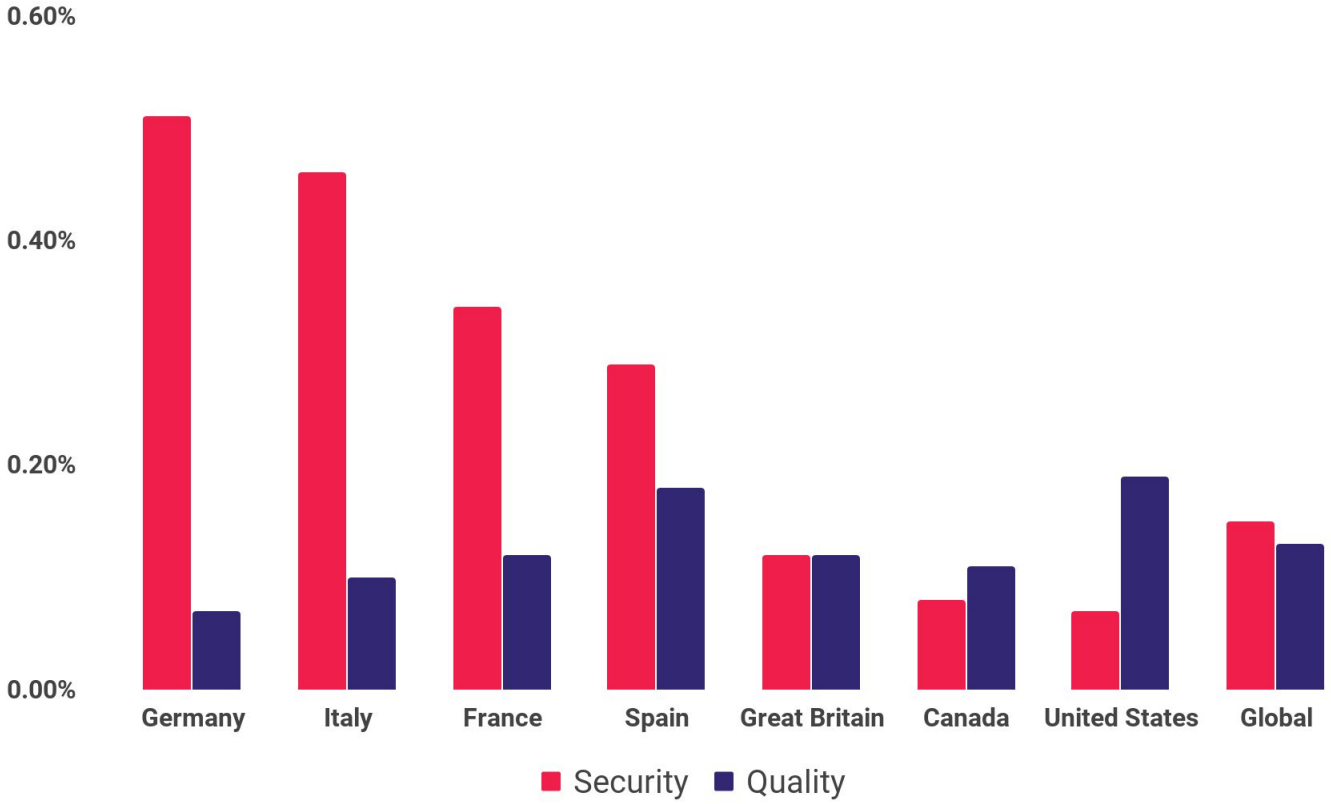
How did the industry fare in Q2 2020?



The **U.S. Security violation rate** declined significantly from Q1 to Q2, driven by massive improvements at one of the largest SSPs as well as a **general shift in threat activity toward Europe**.

Conversely, we saw a modest increase in the rate of **Quality** violations.

Q2 Violation Rates by Country

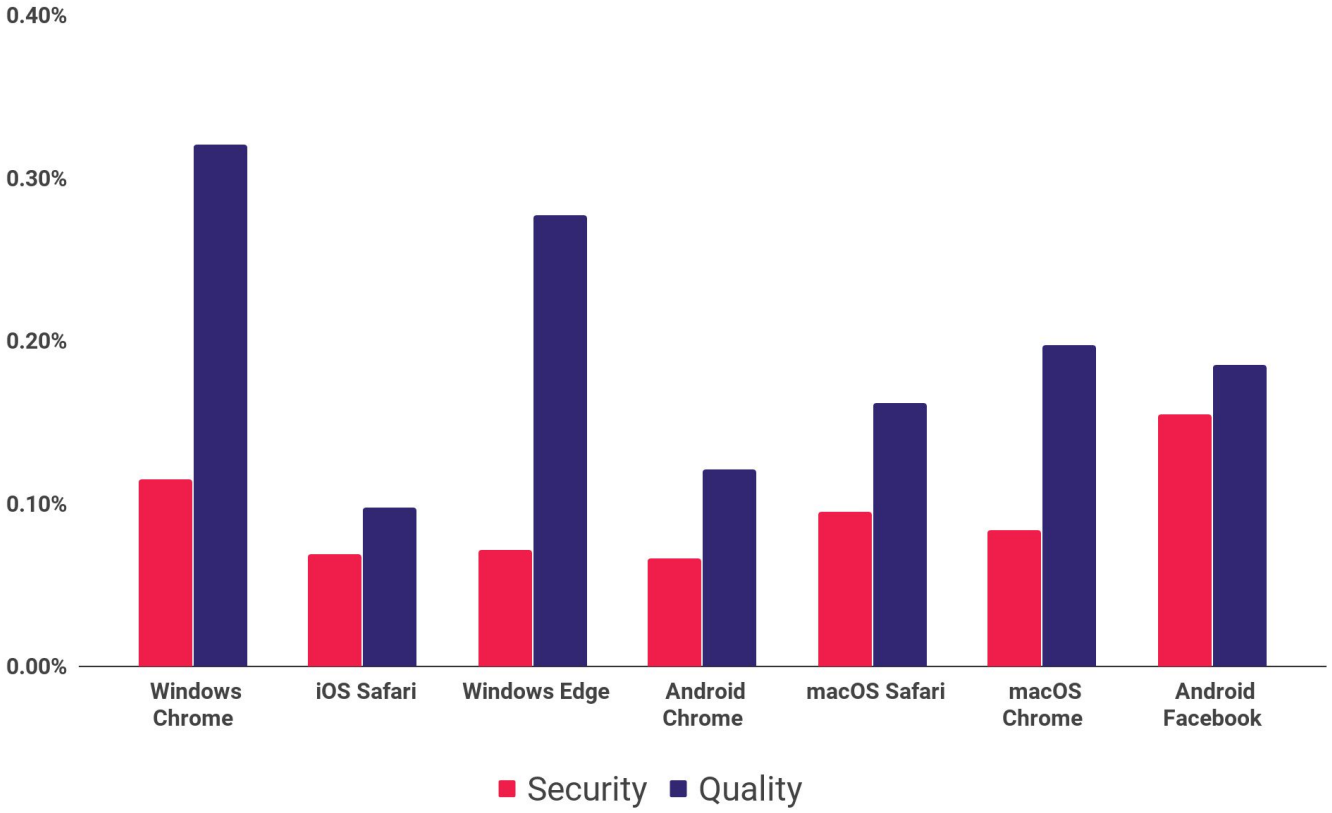


European markets—Germany and Italy in particular—saw far higher rates of Security issues than the U.S.

In fact, some of the most serious threats we see, such as Fizzcore, were largely confined to Europe.

Quality issues tended to be slightly more prevalent in the U.S. than elsewhere.

Q2 Violation Rates by user agent

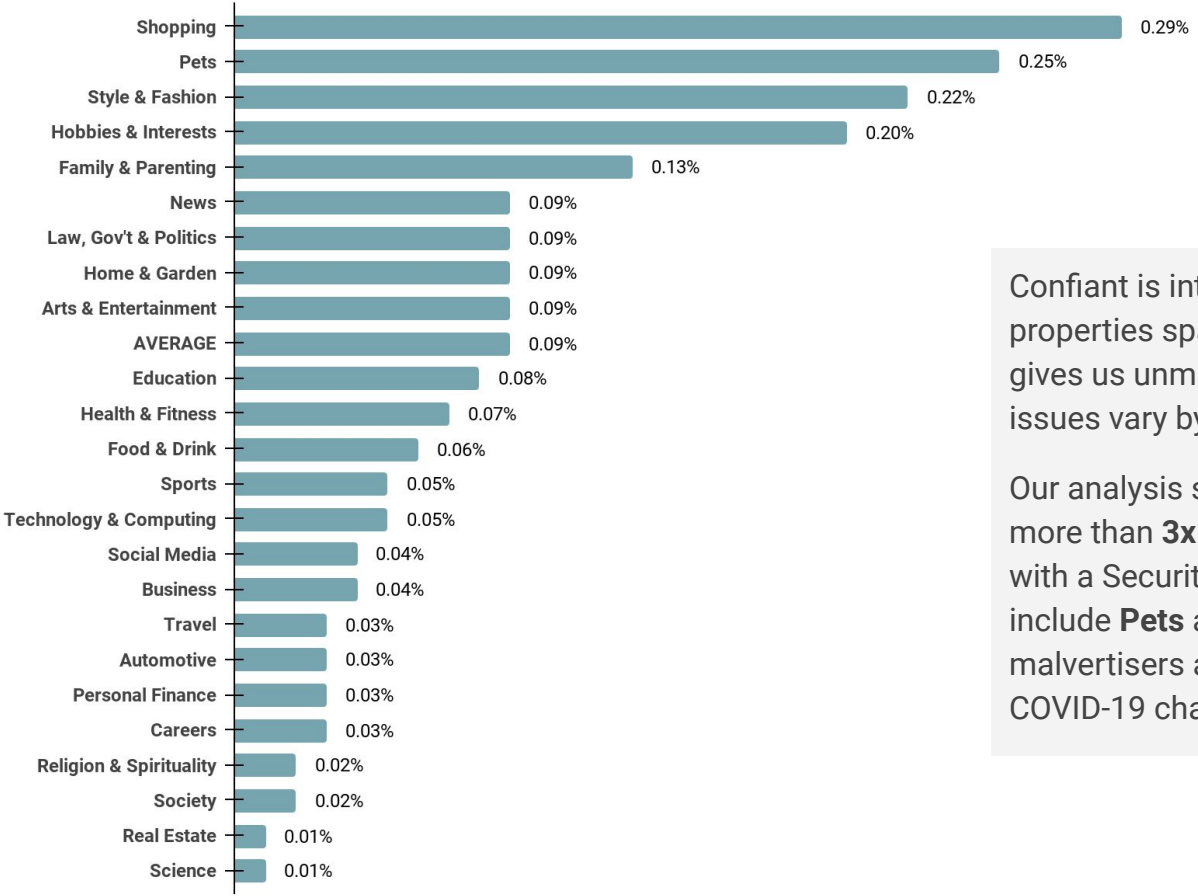


In past reports, violation rates have varied significantly by browser and operating system.

However, in Q2, **Security violation rates were remarkably uniform across the major browsers**. Quality violations varied more, with Chrome for Windows and Edge showing the highest rate of issues.

iOS Safari has shown the most improvement over the past 3 quarters, moving from the top source of Security issues in Q4 2019 to one of the least in Q2 2020.

Security Violation Rates by Site Category



Confiant is integrated into over 30,000 publisher properties spanning all major categories. This gives us unmatched insight into how Security issues vary by category.

Our analysis showed that **Shopping** sites were more than **3x as likely** as the average site to be hit with a Security issue. Other impacted categories include **Pets** and **Hobbies & Interest**, a sign that malvertisers are following the audience as COVID-19 changes browsing patterns.

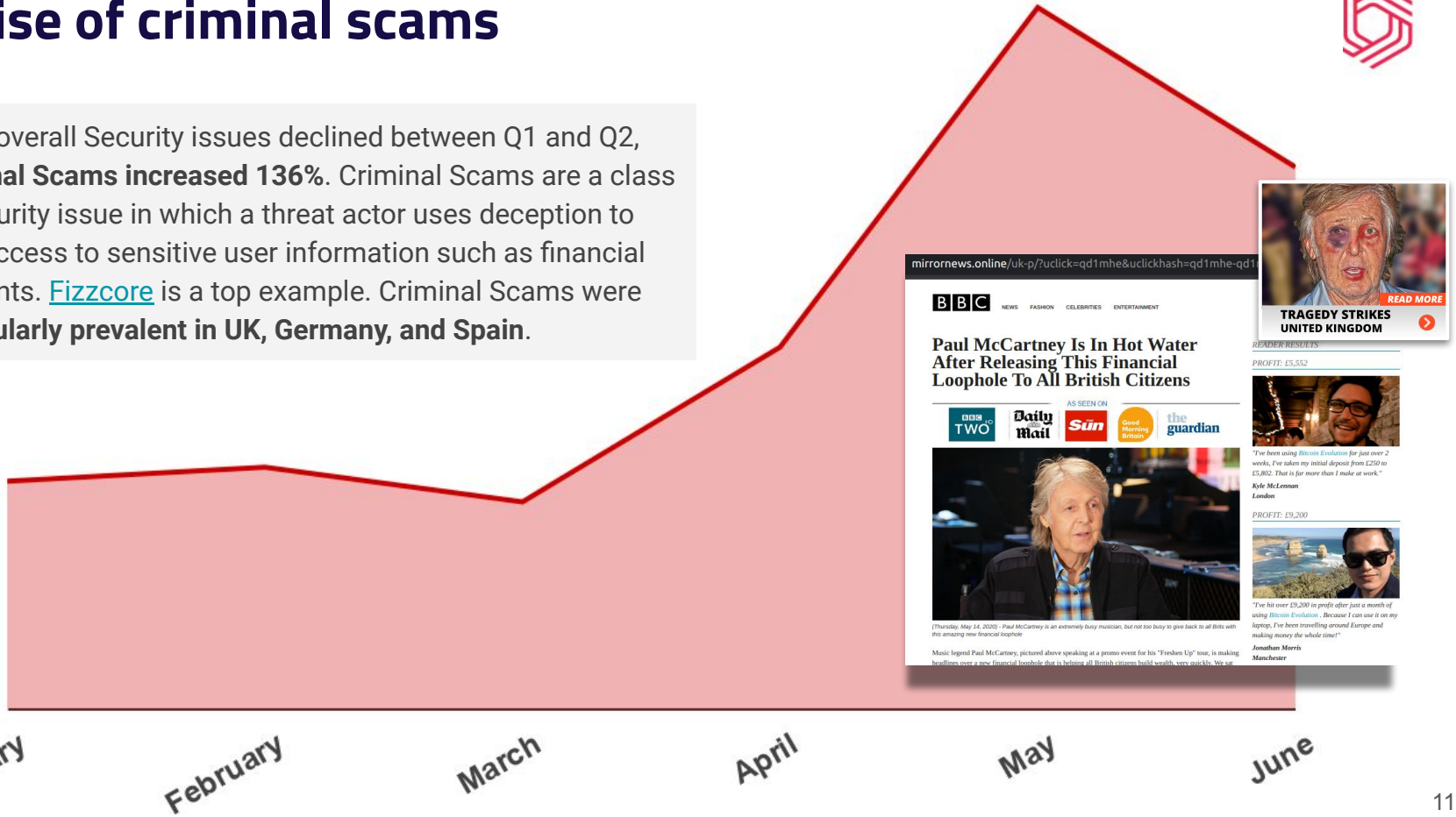
Violation Rates by Header Bidding Framework

Publishers increasingly use frameworks like **Prebid** to manage bidding from multiple SSPs. Google offers a similar feature within Ad Manager called **Open Bidding.** In both cases, demand from a diverse set of SSPs flows through the framework, putting the publisher at risk of Security and Quality issues.

We found that demand flowing through **Open Bidding was significantly cleaner than Prebid**, perhaps a result of the stringent standards Google imposes on SSPs participating in the program.

The rise of criminal scams

While overall Security issues declined between Q1 and Q2, **Criminal Scams increased 136%**. Criminal Scams are a class of security issue in which a threat actor uses deception to gain access to sensitive user information such as financial accounts. Fizzcore is a top example. Criminal Scams were **particularly prevalent in UK, Germany, and Spain**.



SSP Rankings

Q2 2020 US SSP Rankings

In Q2, Confiant tracked impressions from over **100 SSPs**. However, **nearly 80% of impressions originated from just 12 providers**[1] commonly used by publishers. These 12 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.

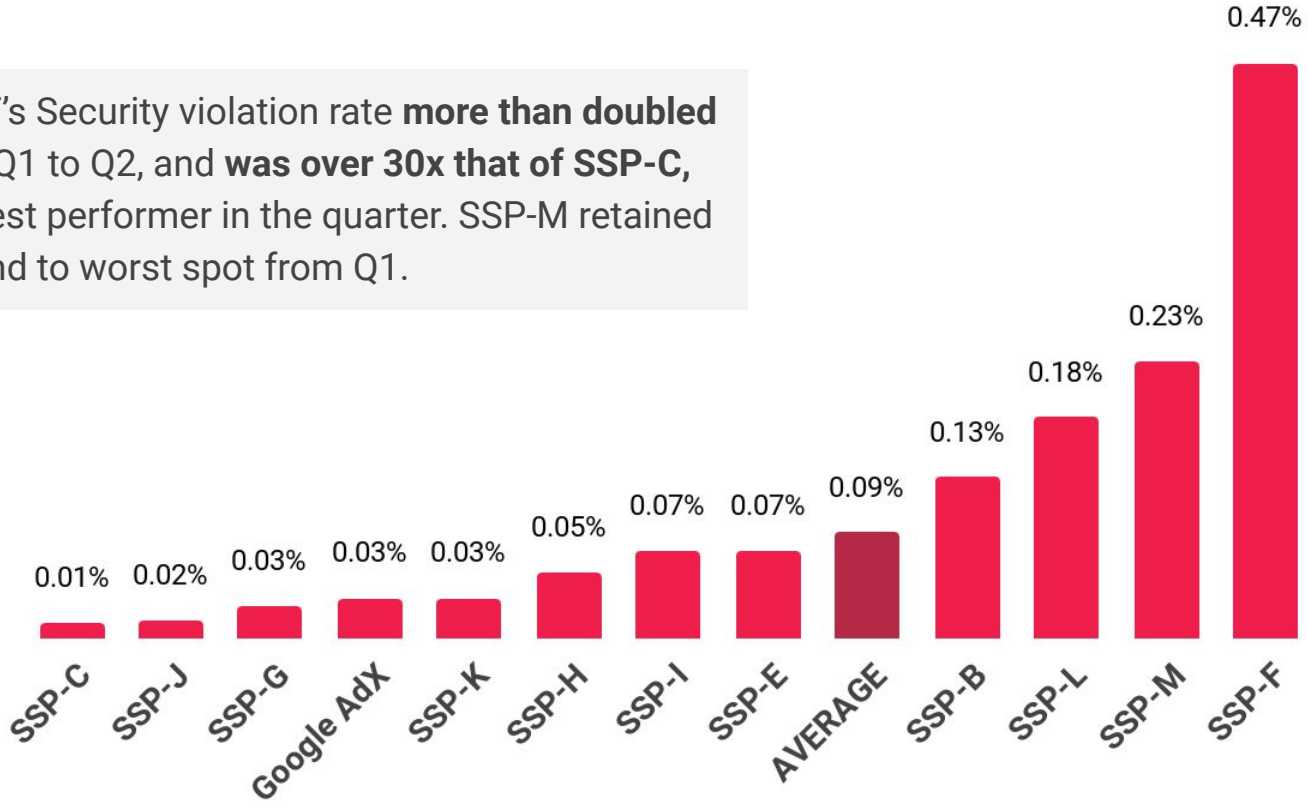
To qualify for inclusion, a provider had to have been a consistent source of **at least 1 billion impressions** in each of the last few quarters.

We identify Google Ad Exchange within these rankings. As the operator of the largest exchange, Google has access to data and resources beyond what's available to other exchanges, which one could reasonably expect to translate into higher efficacy when it comes to catching issues. Our data confirms this assumption, with Google Ad Exchange consistently placing among the top performers.

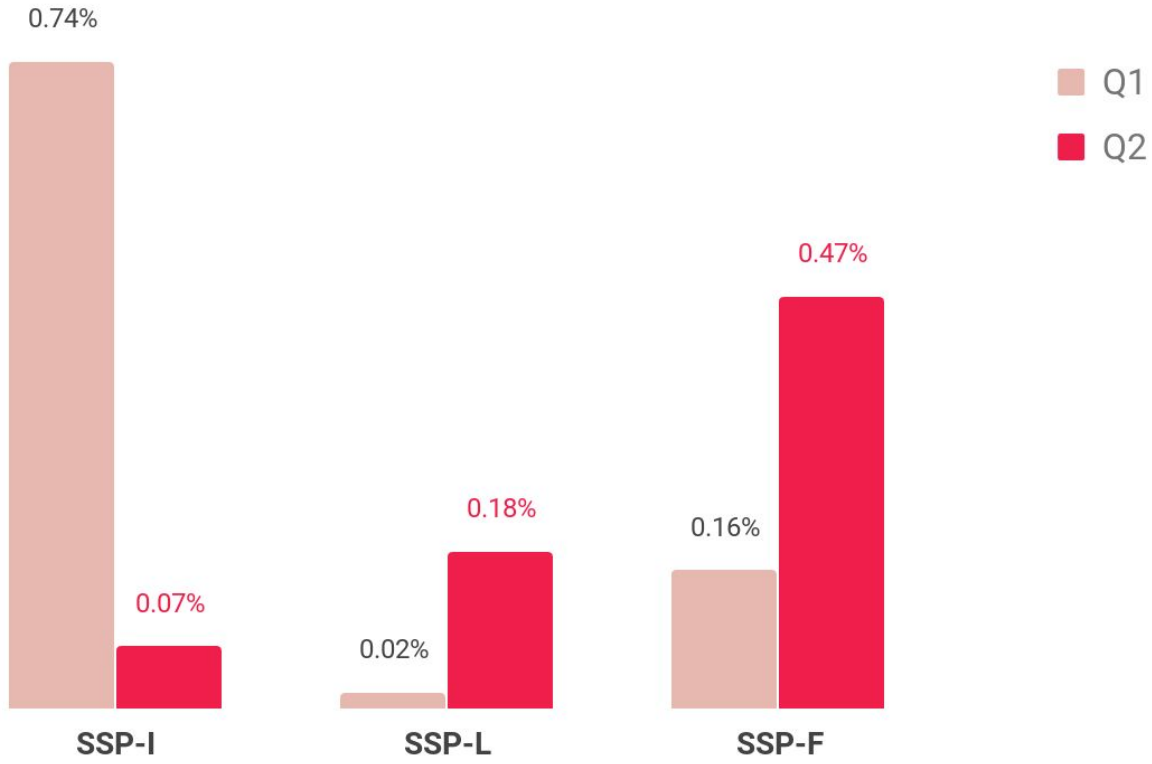
[1] Google AdX, Rubicon Project, OpenX, Xandr, Verizon Media, Index Exchange, Pubmatic, Sonobi, TripleLift, District M, 33Across, and Sovrn

Security Violation Rate by SSP

SSP-F's Security violation rate **more than doubled** from Q1 to Q2, and **was over 30x that of SSP-C,** the best performer in the quarter. SSP-M retained the 2nd to worst spot from Q1.



Security Violation Rate: Q2 vs. Q1

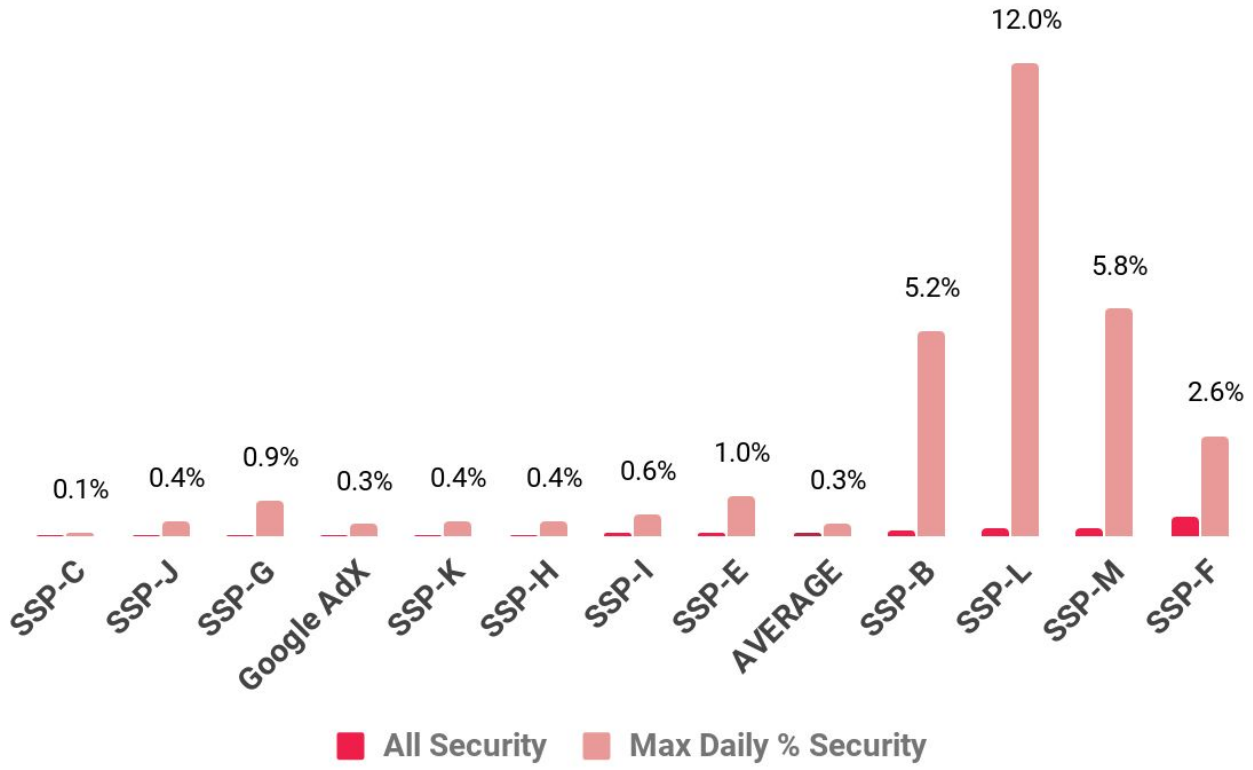


SSP-I and SSP-F had a reversal of fortune between Q1 and Q2.

A perennial poor performer, **SSP-I went from the largest source of Security violations in Q1 to a better-than-average** performer in Q2.

Meanwhile, **SSP-F fell to the bottom spot** after several quarters of good performance.

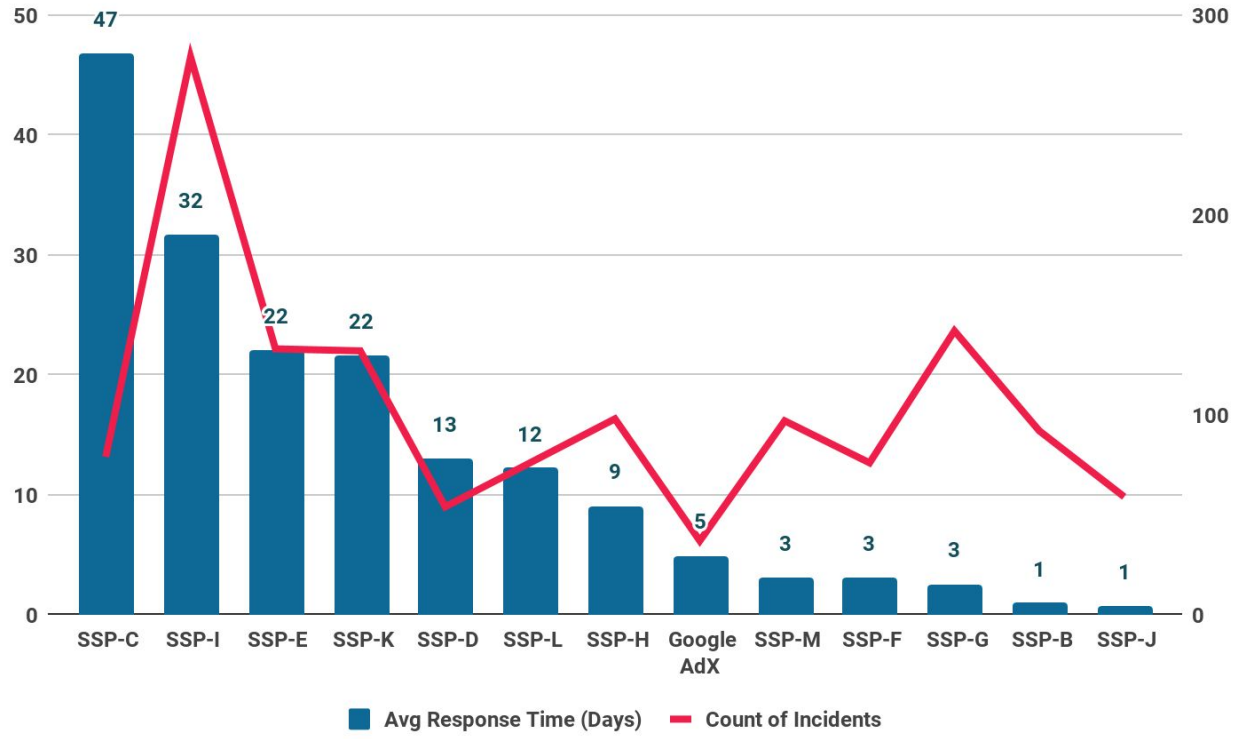
Daily Maximum Malicious Rate by SSP



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 risk.

When under sustained attack, **SSPs had days where over 1 in 10 impressions was a Security risk,** putting publishers and users at considerable risk.

Avg Duration of Attack by SSP



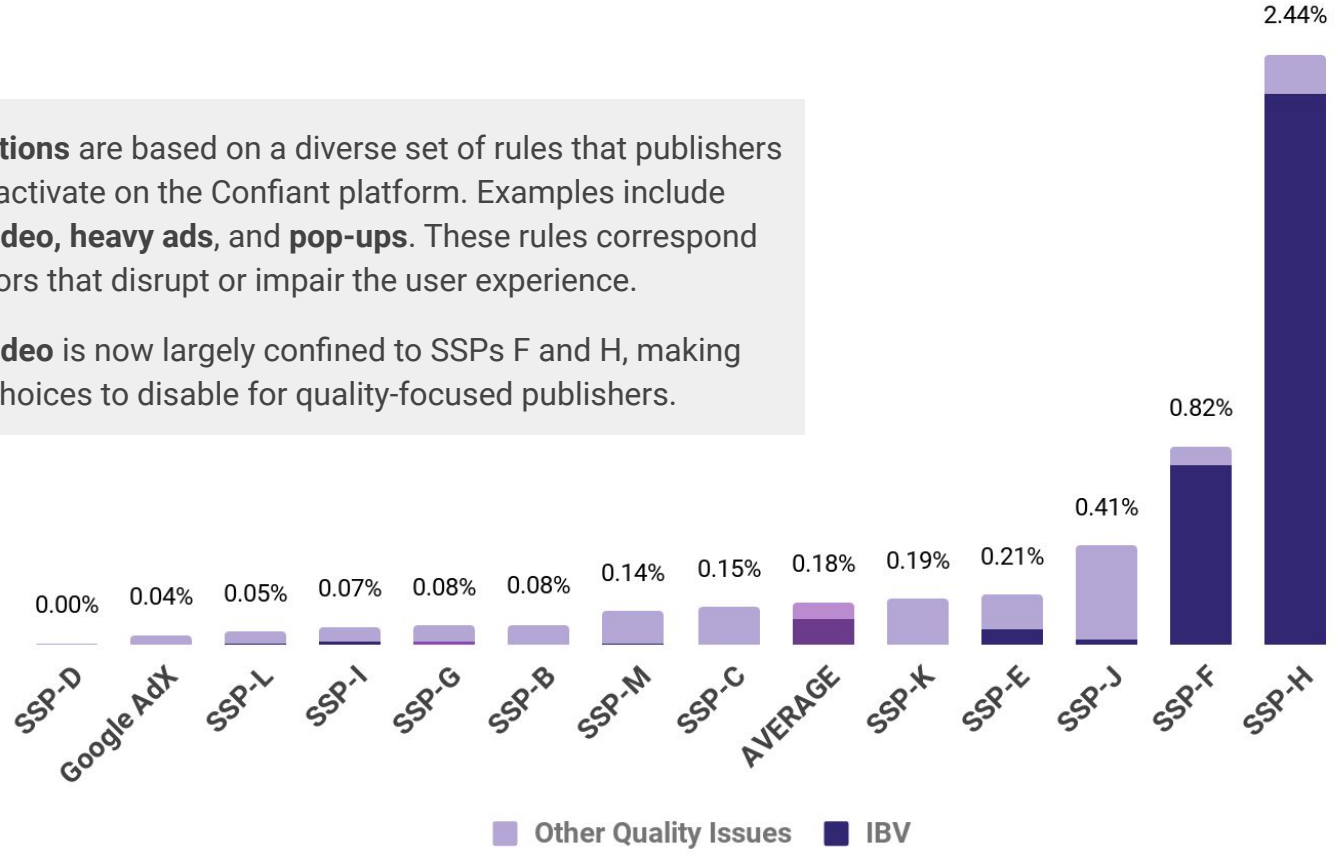
It's important to understand **how long threats persist on an SSP** once an attack is underway. We measure how long it takes from when a threat first appears on an SSP to when it's last seen. On this measure, we see huge differences among the major SSPs.

While SSPs that experience long-duration attacks also tend to have higher rates of Security violations, the two aren't perfectly correlated. In fact, SSP-C had a high average duration but a low Security violation rate because the number of incidents was relatively low.

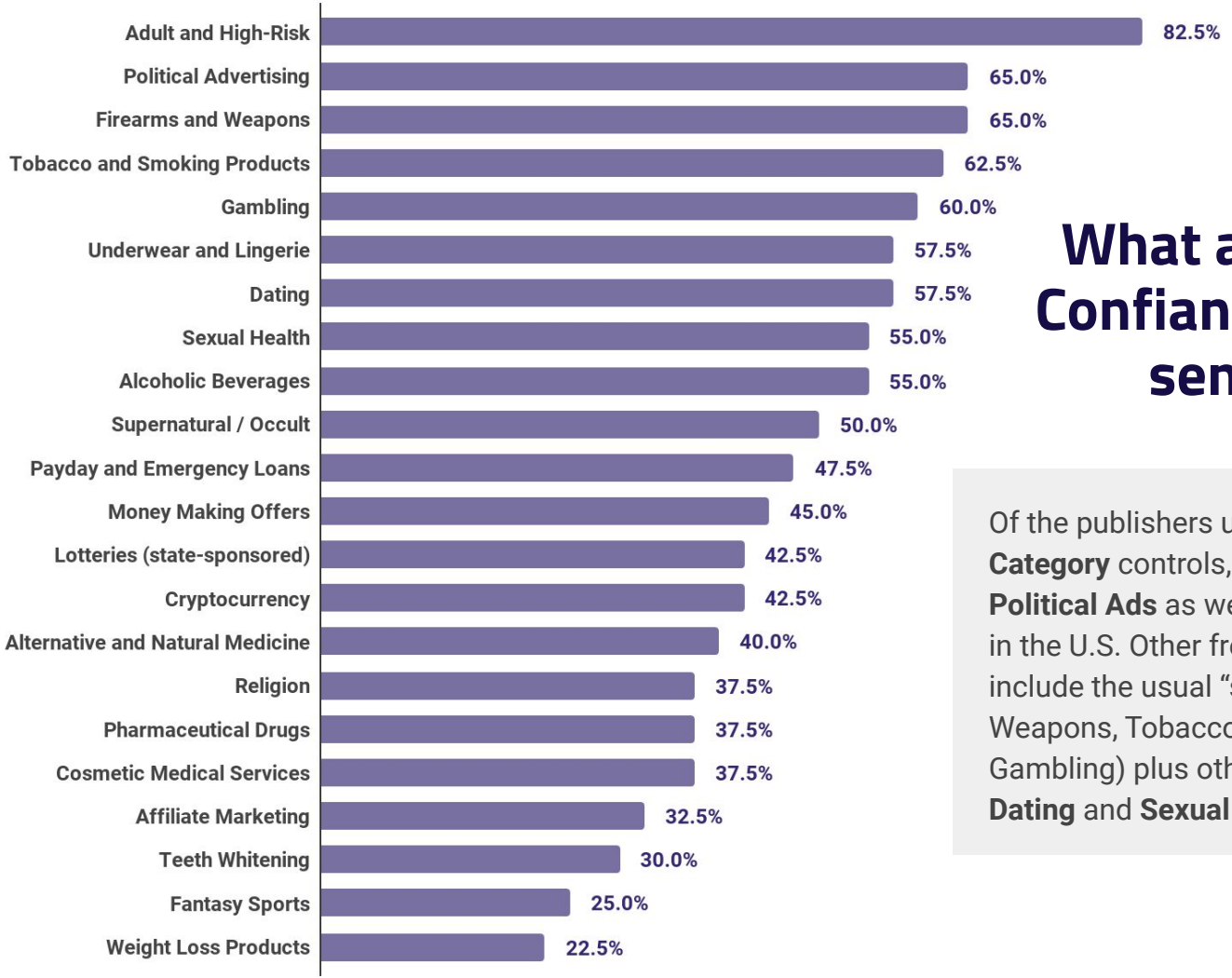
Quality Violation Rate by SSP

Quality violations are based on a diverse set of rules that publishers can elect to activate on the Confiant platform. Examples include **In-Banner Video, heavy ads**, and **pop-ups**. These rules correspond to ad behaviors that disrupt or impair the user experience.

In-Banner Video is now largely confined to SSPs F and H, making them good choices to disable for quality-focused publishers.



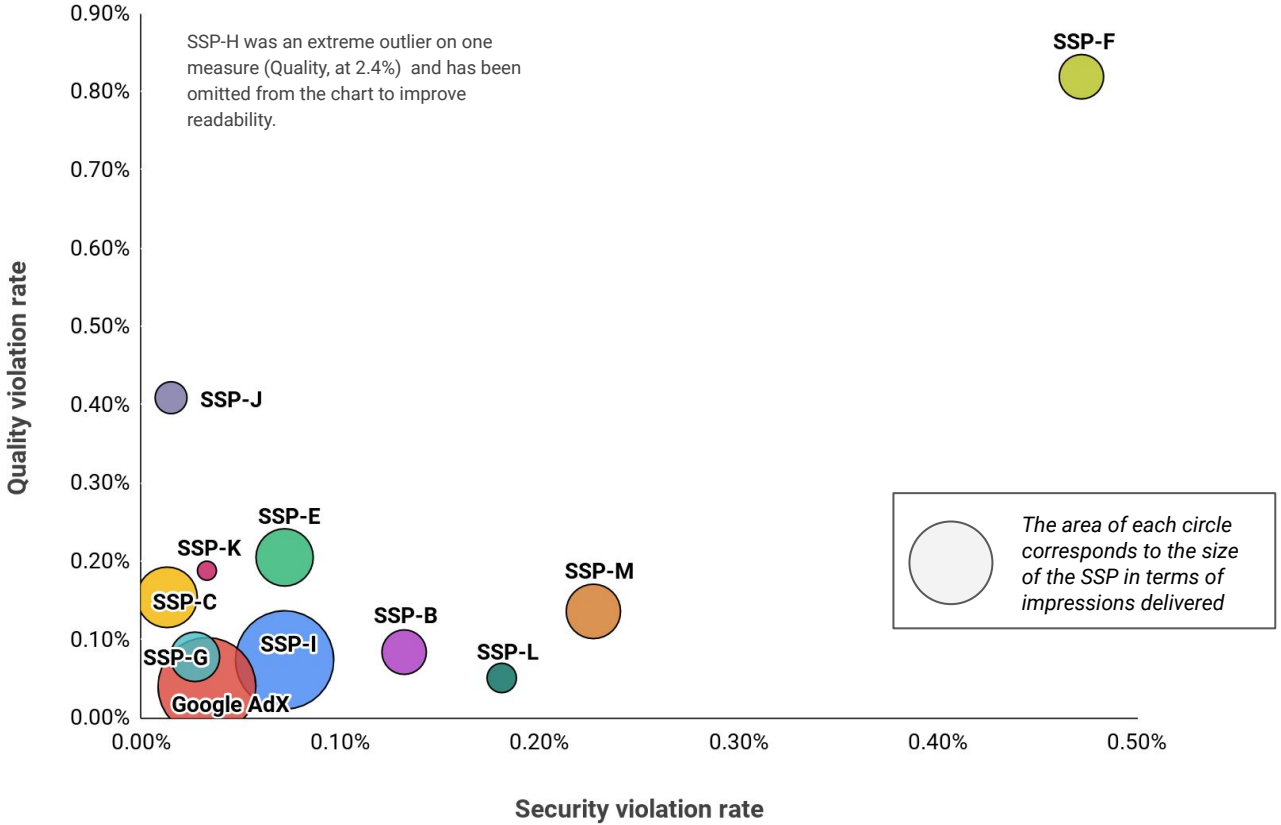
In Q2, **80%** of **unwanted In-Banner Video** impressions came from just **2 SSPs**



What ad categories are Confiant publishers most sensitive about?

Of the publishers using **Confiant's Brand and Category** controls, **65% have set up alerts for Political Ads** as we head into the Fall election season in the U.S. Other frequently flagged categories include the usual "sin" categories (Adult, Firearms & Weapons, Tobacco and Smoking Products, and Gambling) plus other risky topics for publishers like **Dating** and **Sexual Health**.

Violation Rates by SSP Size



Departing from previous quarters, the two largest SSPs (as measured by the number of impressions delivered to publishers) are now both among the best performers when it comes to blocking Security and Quality issues. But SSP-G performs similarly well despite being half the size.

SSP-F stands alone as the only major SSP with **both severe Security and Quality issues** in Q2.

Major Threat Groups Active in Q2

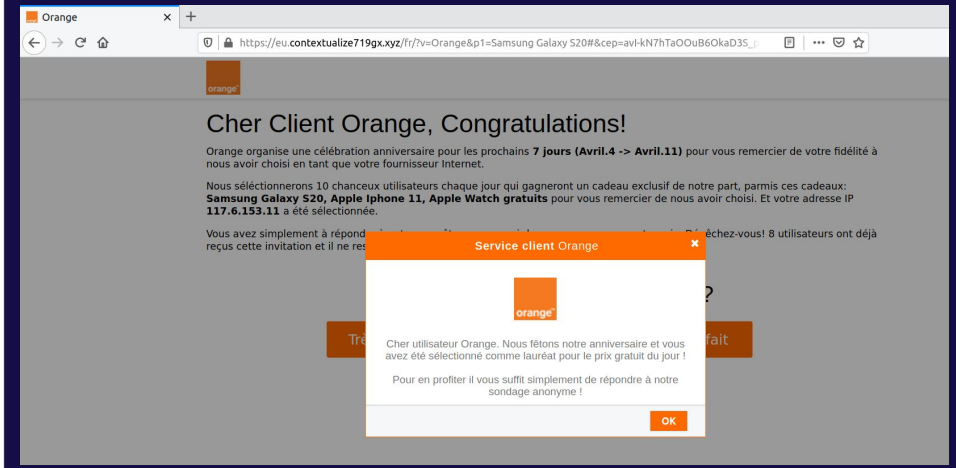
Nephos7

Peak activity: weekends

Notable characteristics: This relatively new attacker has been buying large volumes of traffic since Q4 2019 to execute forced redirects to carrier-branded scams.

The primary mode of operation for Nephos7 is to churn and burn dozens of CDN subdomains, sometimes for a single push. They leverage well-known CDN providers in order to avoid registering multiple domains.

This is a common tactic used by malvertisers who try to fly under the radar, but Nephos7 relies on it quite heavily.

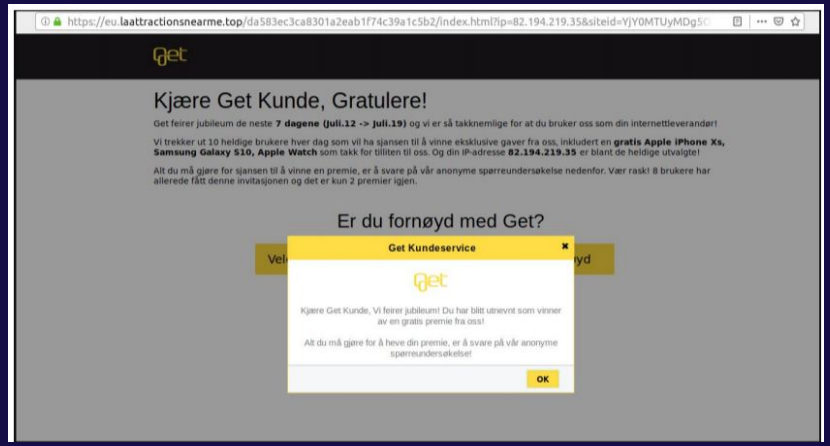


eGobbler

`Peak activity: weekends`

Notable characteristics: eGobbler runs their campaigns in big waves that usually gravitate around the weekends. Lately, the majority of their activity has been centered around European countries, where they deliver disruptive, highly targeted carrier-branded scams.

This is a sophisticated attacker that has been observed to exploit sandbox bypasses in both Chrome and Webkit in order to maximize the impact of their campaigns.



FizzCore

Peak activity: throughout the quarter

Notable characteristics: FizzCore is a significant newcomer. An attacker that sits at the increasingly blurred boundary between malvertising and deceptive ads, FizzCore has perfected the art of audit circumvention to exploit the gullibility of aspiring cryptocurrency investors.

Eschewing forced redirects, FizzCore uses evasion techniques to bypass ad quality reviews and drive users to cybersecurity scam sites.

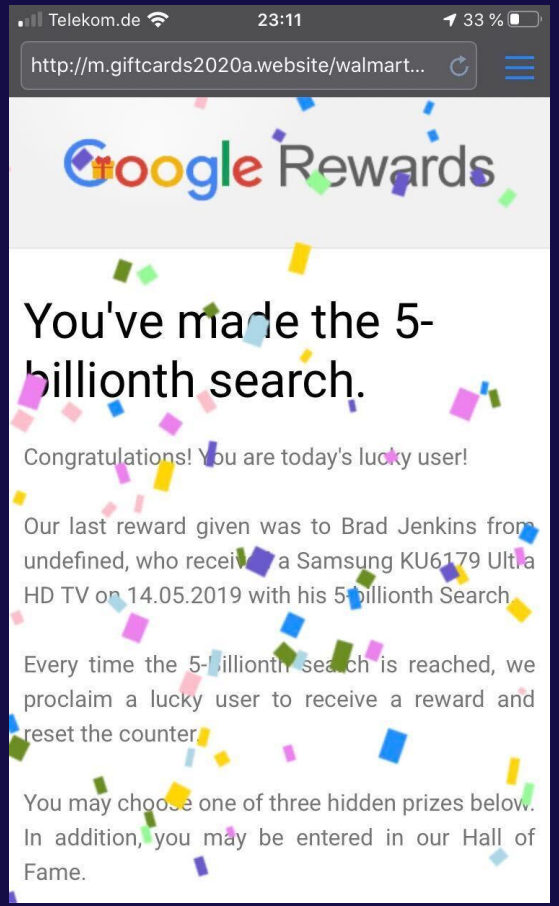
Evasion techniques include cloaking (display of fake ad creatives and landing pages to ad quality scanners), reputation and relationship building in the ad ecosystem, and carefully crafted localized campaigns using celebrity endorsement clickbait.

LP513

Peak activity: early May

Notable characteristics: As the malvertising world lately has seen a shift towards carrier-branded scams and tech support fraud, LP513 continues to serve up the familiar malicious gift card / reward / freebie landing pages that were so widespread when forced mobile redirects started to emerge a few years ago.

Evasion techniques by this attacker are not atypical, and neither are the payloads, but perhaps that's what makes them noteworthy — that the same old attacks are still prevalent.



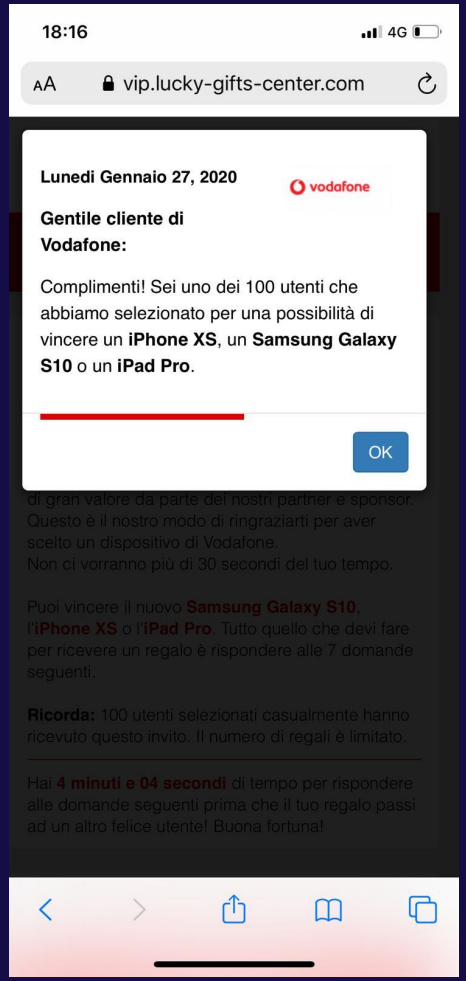
DCCBoost

`Peak activity: early May`

Notable characteristics: DCCBoost campaigns give us a glimpse into some of the more interesting innovations that have emerged in malvertising over the last year or so.

They use a combination of server-side targeting combined with a compartmentalized client-side payload in order to deliver the malicious ad in stages.

Often these “pieces” of the malicious ad will load from different resources and coordinate with each other using the postMessage API, providing a unique technique for misdirection.

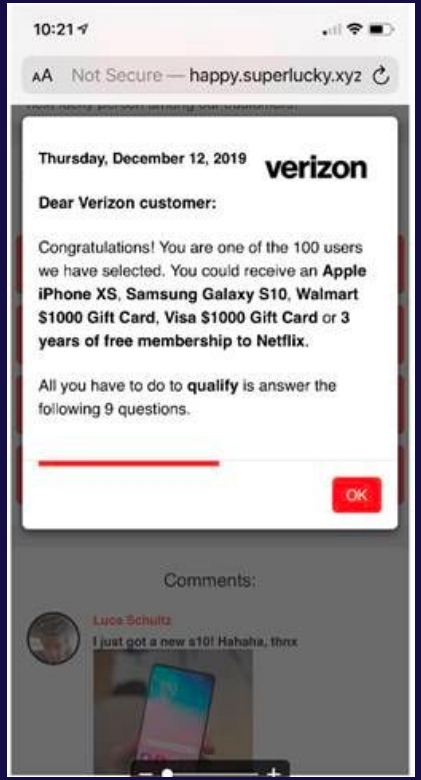


Scamclub

Peak activity: mid-June

Notable characteristics: Scamclub stands apart from their malvertising peers in their approach toward evasion. Whereas most high-profile malvertisers choose to hide behind carefully crafted fingerprinting and targeting, Scamclub relies on cranking out dozens (or hundreds) of creatives daily with subtle variations in very rudimentary obfuscation.

This bombardment tactic is designed to overwhelm platforms and security vendors by creating a flood of dangerous demand that they hope will spill beyond any anti-malvertising gatekeeping.



Conclusion

Q2

- ➔ Overall **Quality violations held steady** from Q1 to Q2, while **Security issues declined** in frequency in the U.S. market as threat activity shifted to Europe.
- ➔ Much of the improvement in Security violation rate was driven by a **marked improvement in performance from SSP-I**, one of the industry's largest sources of demand.
- ➔ Security violation rates in **top European markets** were **4 - 7x** the U.S. rate, a much larger delta than we've seen in past reports.
- ➔ **Criminal Scams**, a class of security issue in which a threat actor uses deception to gain access to sensitive user information such as financial accounts, **increased 136%** and were particularly prevalent in Europe.

About Confiant

We believe in making the digital world safe for everyone.

Confiant is a cybersecurity company that protects publishers and platforms from malicious actors and puts the control back in their hands to ensure that ads delivered to users are safe and secure. Our sole purpose is to rid the world of cybercriminals, bad actors, and malware.

Our founders, LD Mangin and Jerome Dangu, teamed up in September 2013 to reinvent how the industry tackled malvertising and low-quality ads. The then-current state of technology was at a data disadvantage against the bad actors that couldn't be surmounted without real innovation. That “never done before” innovation took a year to figure out, a year to build, and a year of beta to get right. In May 2017 Confiant launched the industry’s first real-time verification and blocking solution, giving publishers actual control of what ads are shown to their users.

Learn More