CONFIANT

Demand Quality Report

Q3 2020

Introduction

Confiant's **Demand Quality Report** is a quarterly look into the quality of demand in digital advertising. Using a sample of over 135 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 tenth in the series, covers Q3 2020.

Methodology

To compile the research contained in this report, Confiant analyzed a normalized sample of **more than 135 billion advertising impressions** from July 1 to September 30, 2020 from **40,000 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 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, we shifted from using U.S. to **global data**, necessitating a restatement of our Q2 results to allow quarter-to-quarter comparison (see slide 6).

Definitions

Security violations

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

- **Mobile redirects**
- **Criminal scams**
- **Fake ad servers**
- **Fake software updates**
- **High-Risk Ad Platforms (HRAPs)**[1]

Quality violations

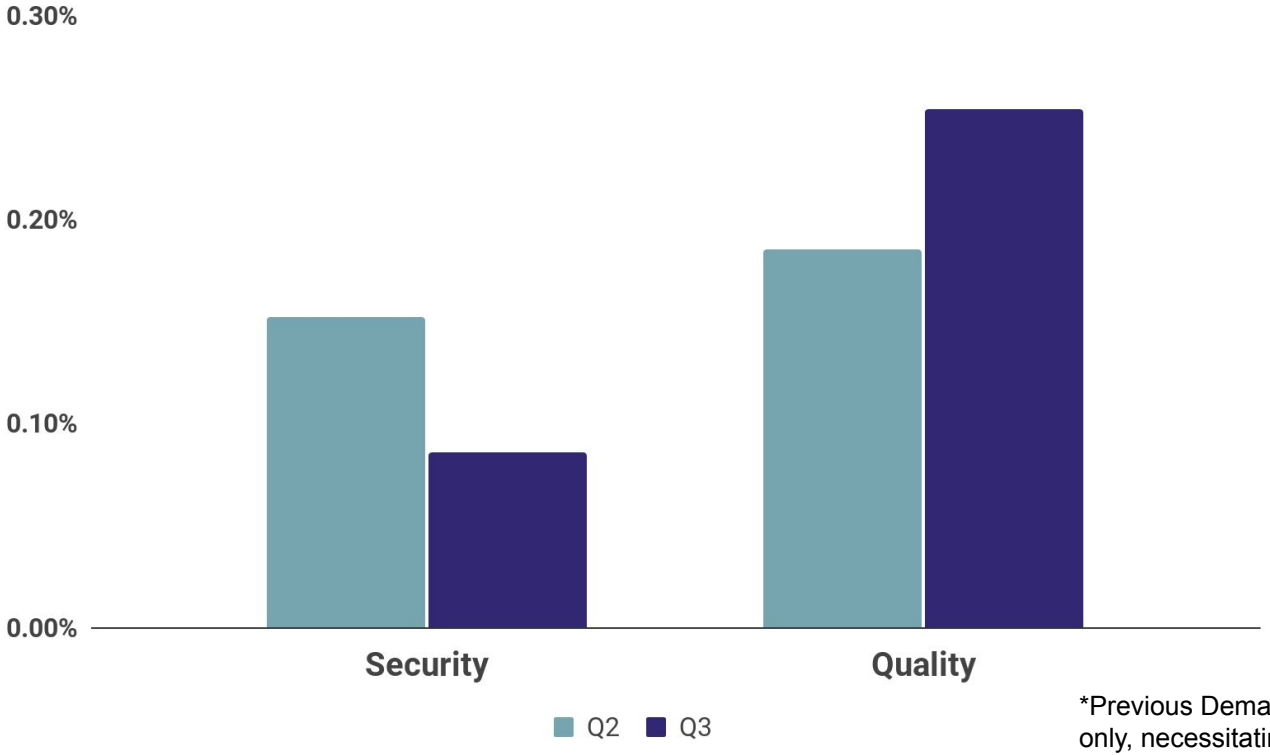
Non-security issues related to **ad behavior**, **technical characteristics**, or **content**. Top issues include:

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

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

Industry View

How did the industry fare in Q3 2020?

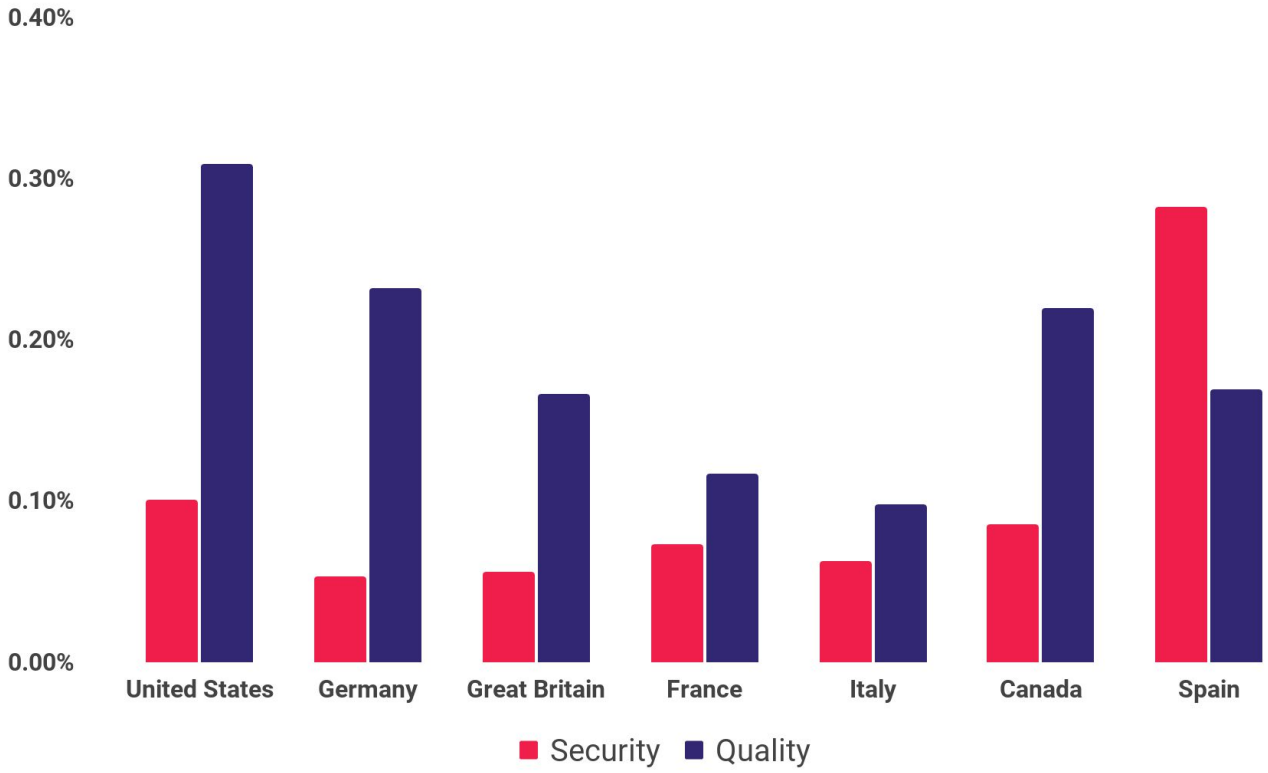


The global* **Security violation rate** declined significantly from Q2 to Q3, driven by continued improvements at a number of large SSPs.

Conversely, the **Quality** violation rate increased by more than a third.

*Previous Demand Quality Reports included U.S. data only, necessitating restatement of the Q2 values.

Q3 Violation Rates by Country

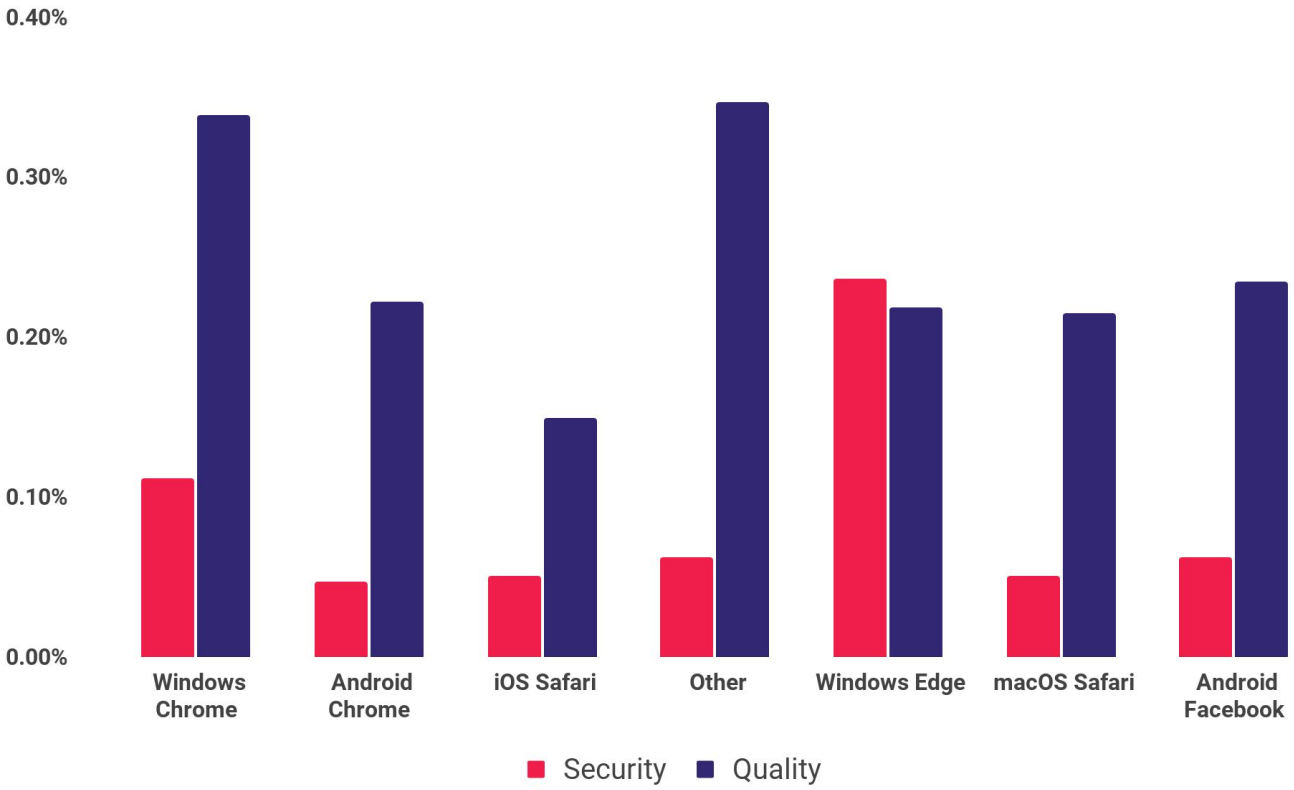


Differing from past quarters, the **rate of Security issues in the U.S. exceeded that of all European countries except Spain**.

This is despite the fact that many serious threats like Fizzcore are largely confined to Europe.

Quality issues also tended to be more prevalent in the U.S. than elsewhere, again a departure from past reports.

Q3 Violation Rates by user agent

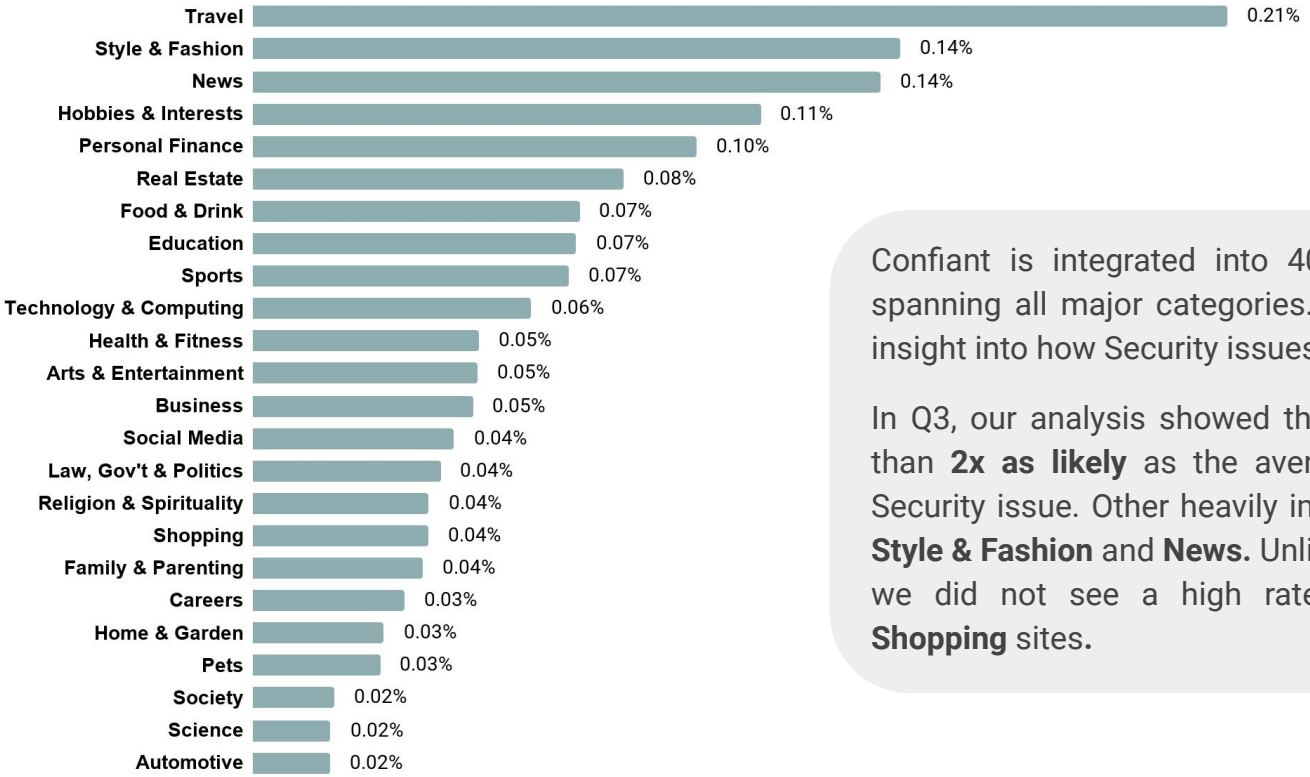


In Q3, all browsers except Windows Edge fell into a fairly narrow band for Security. **Edge was the outlier, with more than twice the rate of Security issues as the next highest browser.**

For Quality issues, we saw more pronounced variance between the major browsers. Windows Chrome came in significantly worse than average, while iOS Safari was significantly better than average.

Looking at format, desktop web shows a higher rate of issues than mobile web or app.

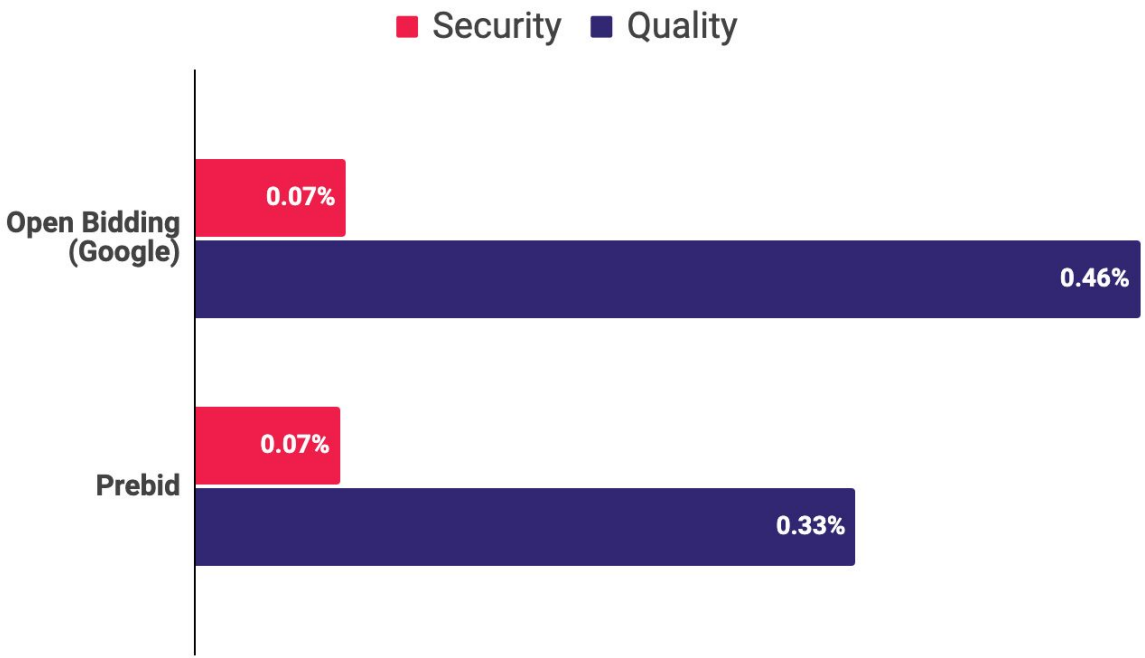
Security Violation Rates by Site Category



Confiant is integrated into 40,000 publisher properties spanning all major categories. This gives us unmatched insight into how Security issues vary by category.

In Q3, our analysis showed that **Travel** sites were more than **2x as likely** as the average site to be hit with a Security issue. Other heavily impacted categories include **Style & Fashion** and **News.** Unlike some previous quarters, we did not see a high rates of Security issues on **Shopping** sites.

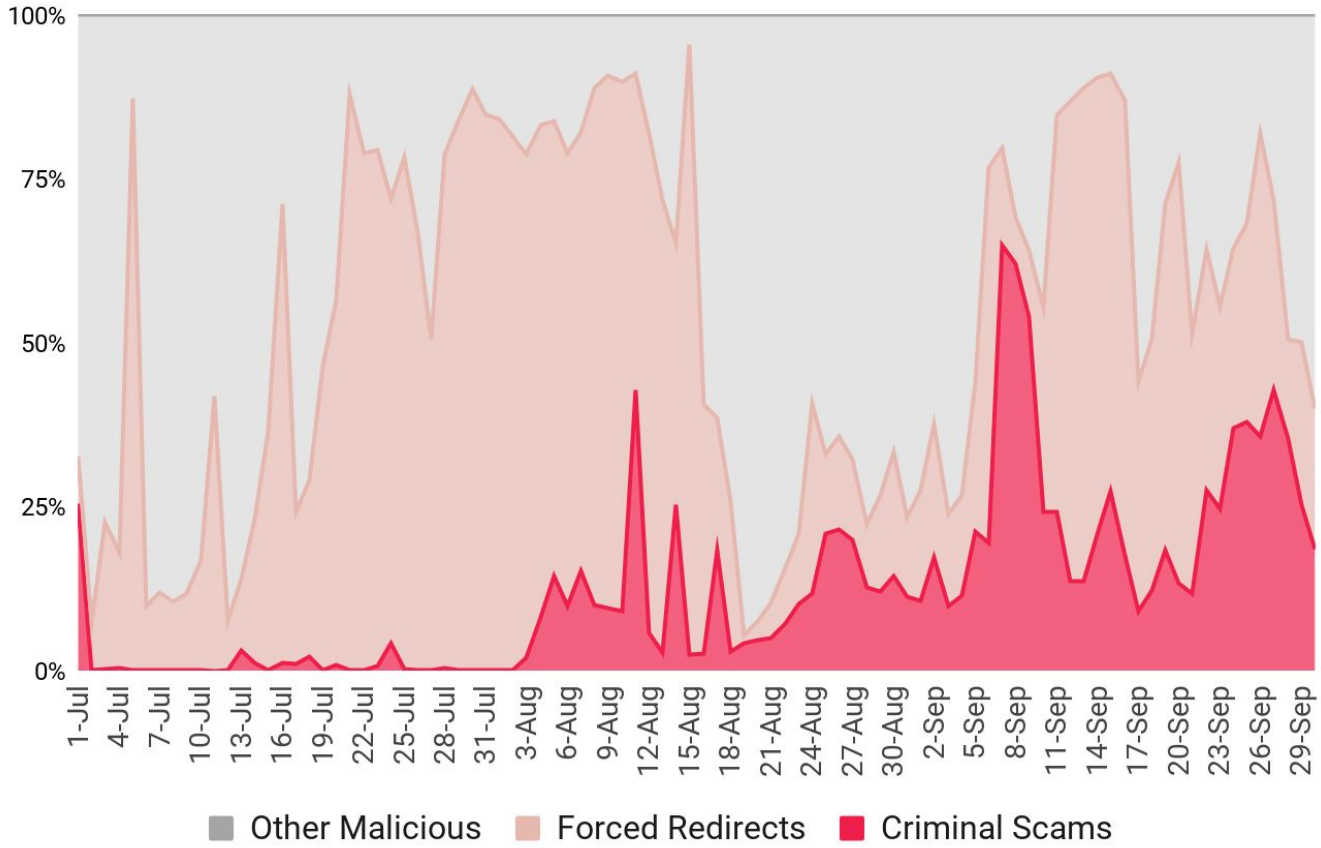
Violation Rates by Header Bidding Framework



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.

In Q3, we found that demand flowing through Open Bidding performed similarly to Prebid and other sources for Security, with greater variance seen in Quality.

Criminal scams are becoming more prevalent



While Criminal Scams remain less common than Forced Redirects, they are growing steadily in frequency and important. **Criminal Scams represented about 16% of total Security issues** in Q3, but saw **peak levels as high as 65%**.

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.

SSP Rankings

Q3 2020 US SSP Rankings

In Q3, Confiant tracked impressions from over **100 SSPs**. However, **75% of global 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.

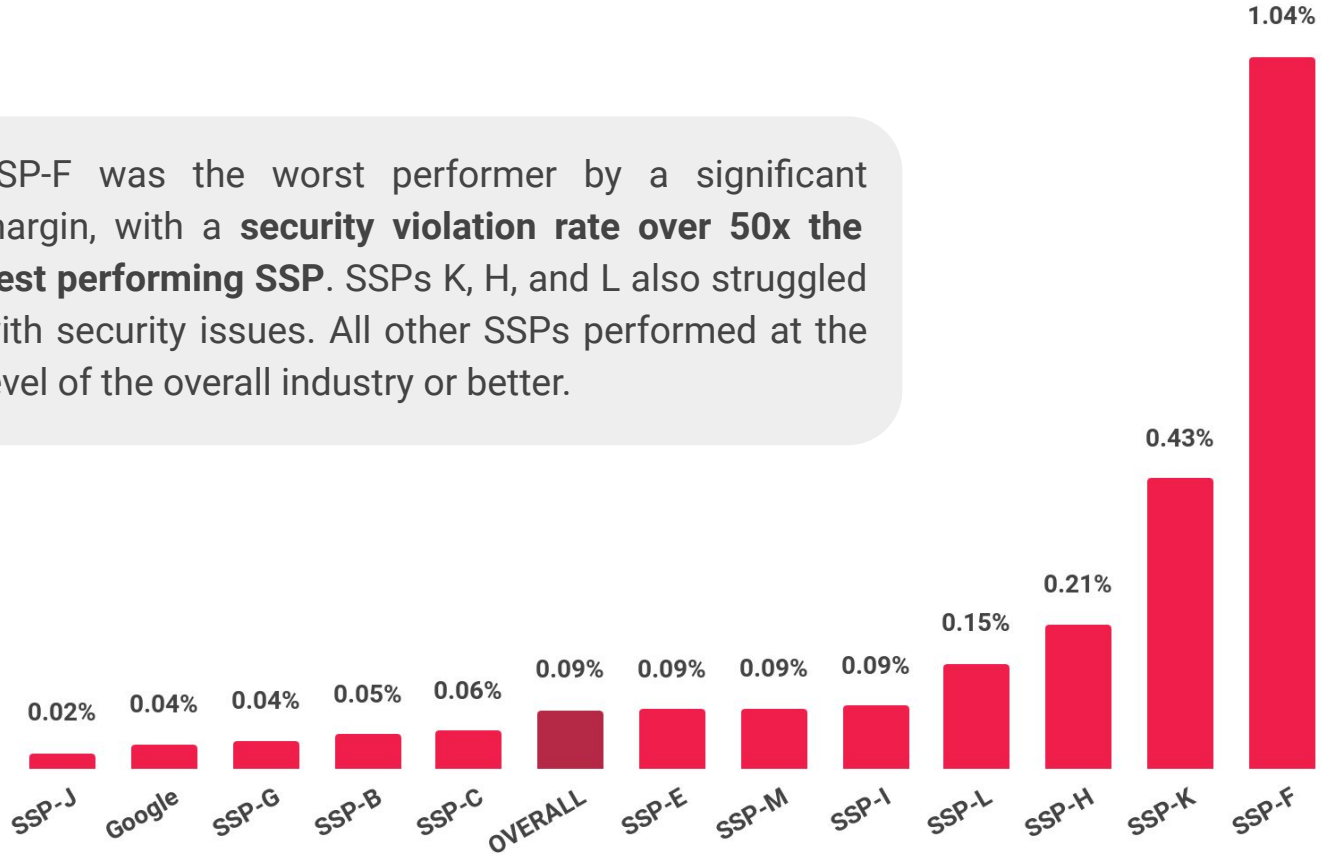
To qualify for inclusion, a provider had to have been a consistent source of **at least 1 billion impressions** a quarter.

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.

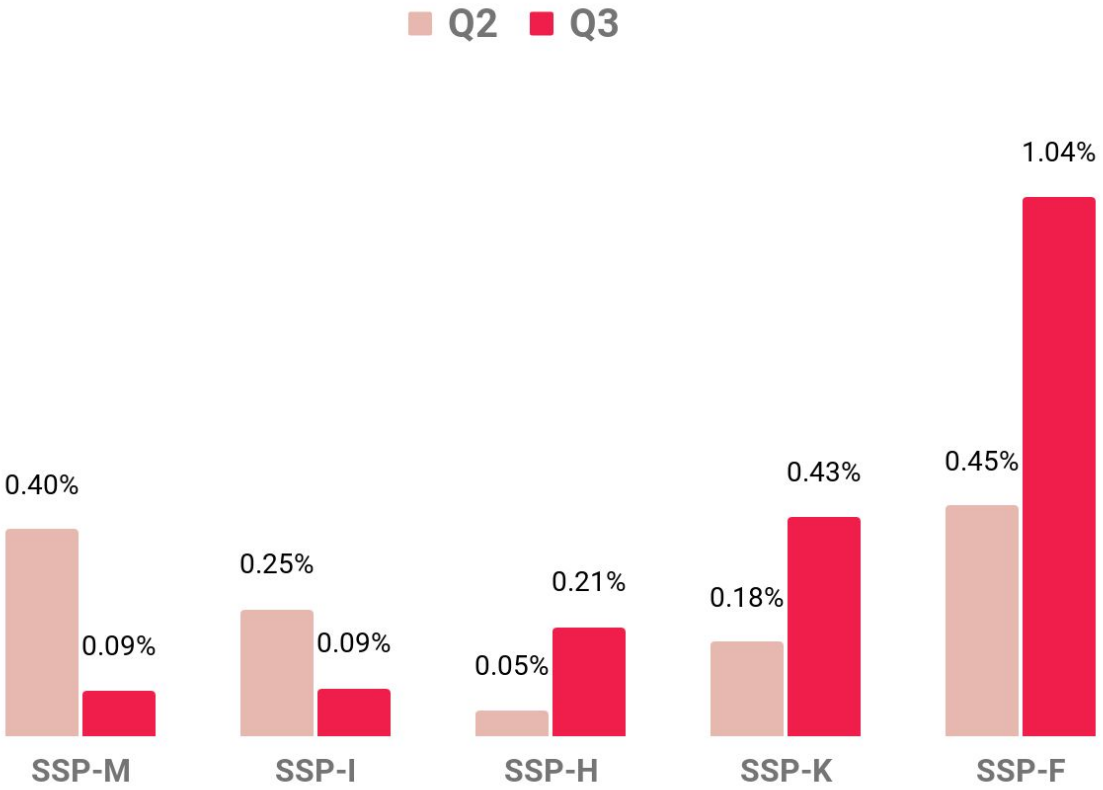
[1] Google AdX, Magnite, OpenX, Xandr, Verizon Media, Index Exchange, Pubmatic, Sonobi, TripleLift, District M, 33Across, and Sovrn

Security Violation Rate by SSP

SSP-F was the worst performer by a significant margin, with a **security violation rate over 50x the best performing SSP**. SSPs K, H, and L also struggled with security issues. All other SSPs performed at the level of the overall industry or better.



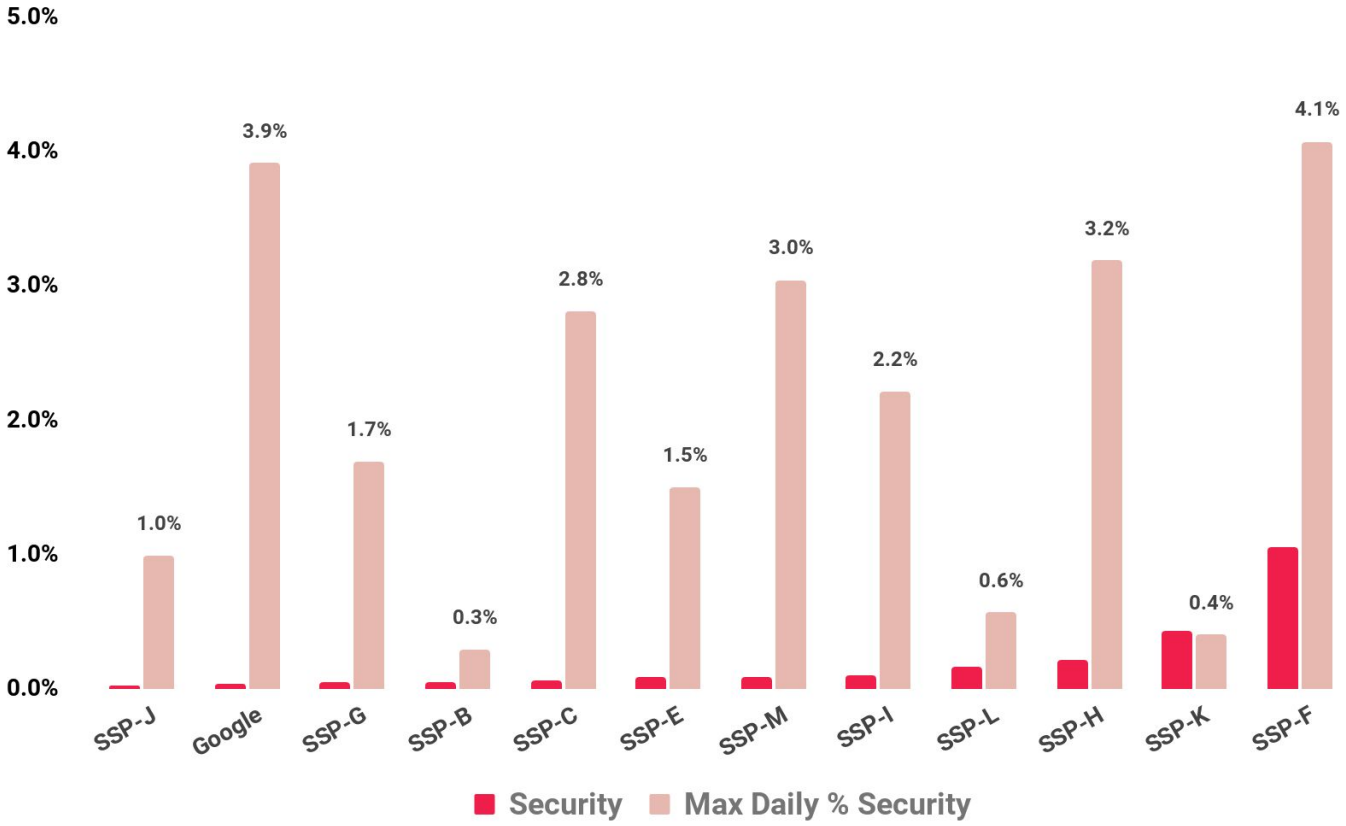
Security Violation Rate: Q2 vs. Q3



SSP-I, one of the largest SSPs in the industry, continued to show strong performance, **reducing their security violation rate by over 50%**.

Meanwhile, **SSP-F** remained mired in the the bottom spot, with its **violation rate having more than doubled for the second quarter in a row.**

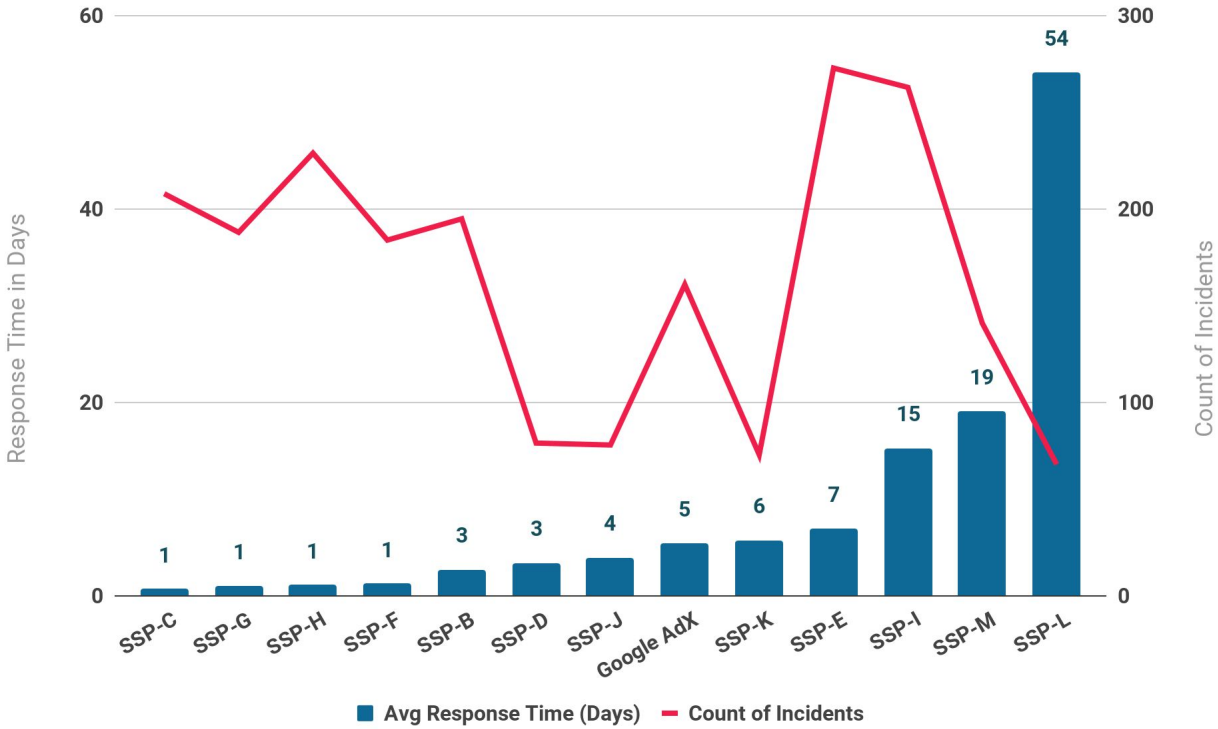
Daily Maximum Malicious Rate by SSP



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, even the best-performing **SSPs had days where 1 in 25 impressions was a Security violation,** putting publishers and users at considerable risk.

Avg Duration of Attack by SSP



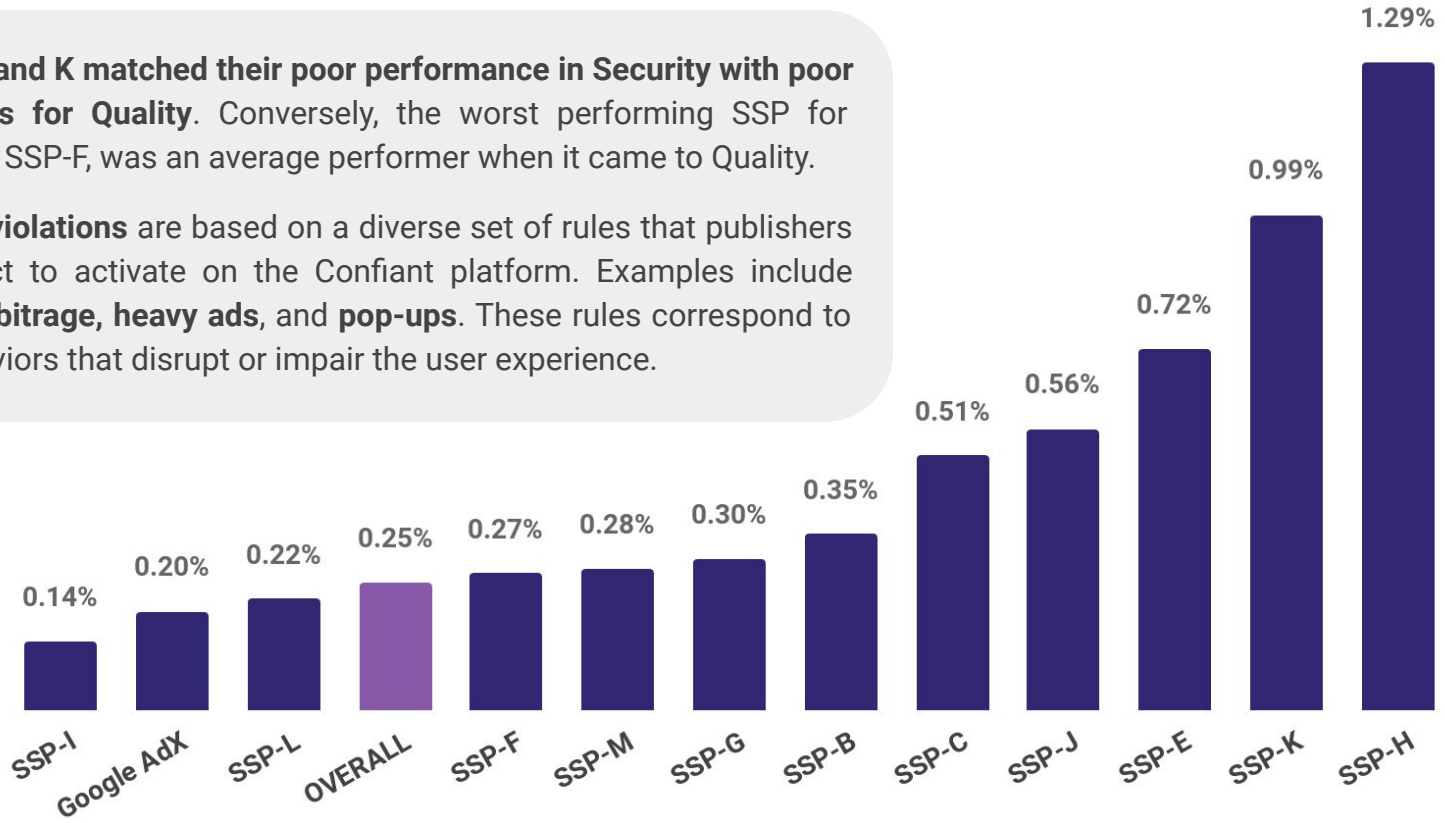
It's important to understand **how long threats persist on an SSP** once an attack is underway. We measure how long it takes from when a threat first appears on an SSP to when it's last seen. On this measure, we see huge differences among the major SSPs.

This quarter, **SSP-C leapt from a last-place showing in average response time in Q2 to first place** this quarter, despite an increase in the number of incidents. SSP-L, on the other hand, struggled with long response times despite relatively few incidents.

Quality Violation Rate by SSP

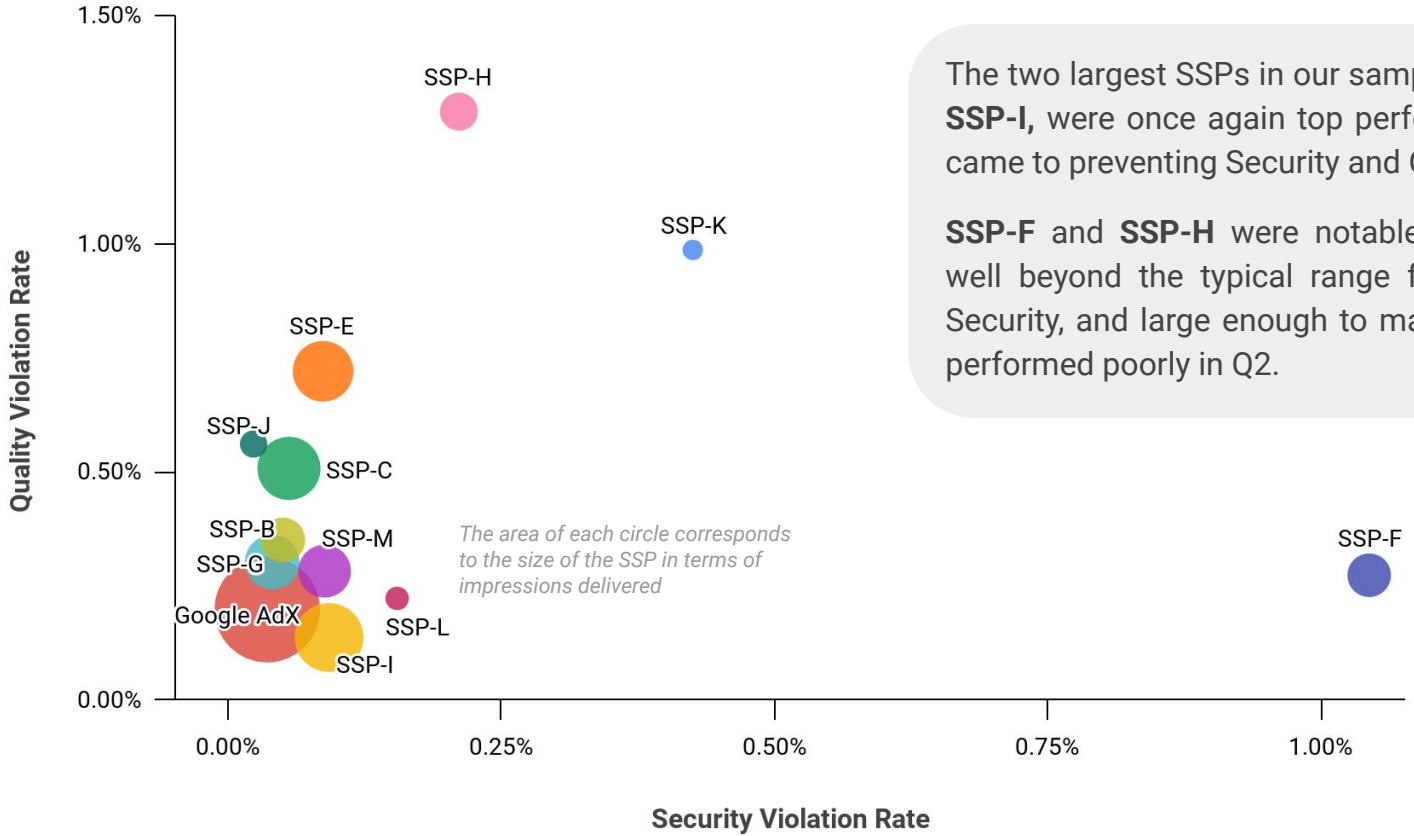
SSPs H and K matched their poor performance in Security with poor showings for Quality. Conversely, the worst performing SSP for Security, SSP-F, was an average performer when it came to Quality.

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



The worst performing SSP delivered security issues at **50x the rate** of the best

Violation Rates by SSP Size

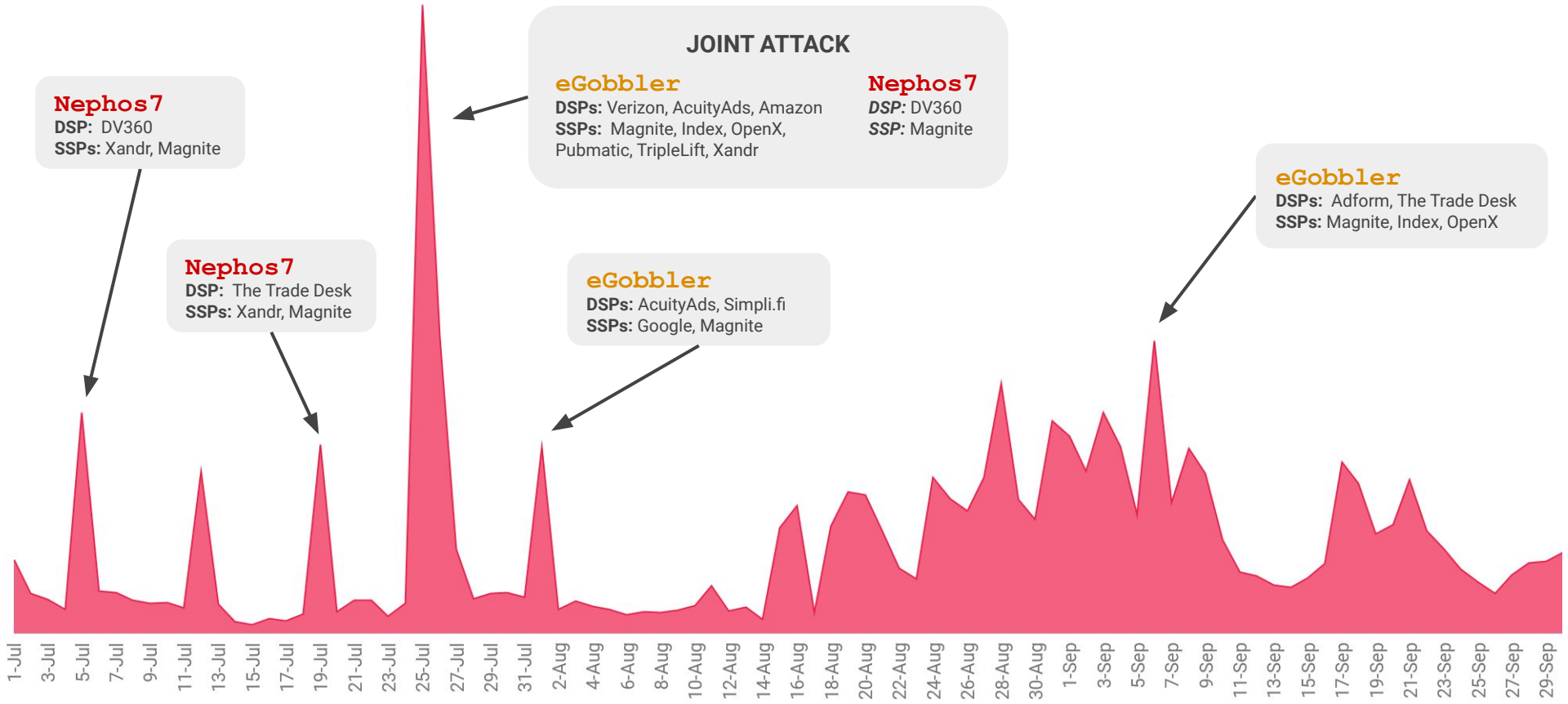


The two largest SSPs in our sample, **Google** and **SSP-I,** were once again top performers when it came to preventing Security and Quality issues.

SSP-F and **SSP-H** were notable outliers, both well beyond the typical range for Quality and Security, and large enough to matter. Both also performed poorly in Q2.

Major Threat Groups Active in Q3

Notable Threat Activity



Nephos7

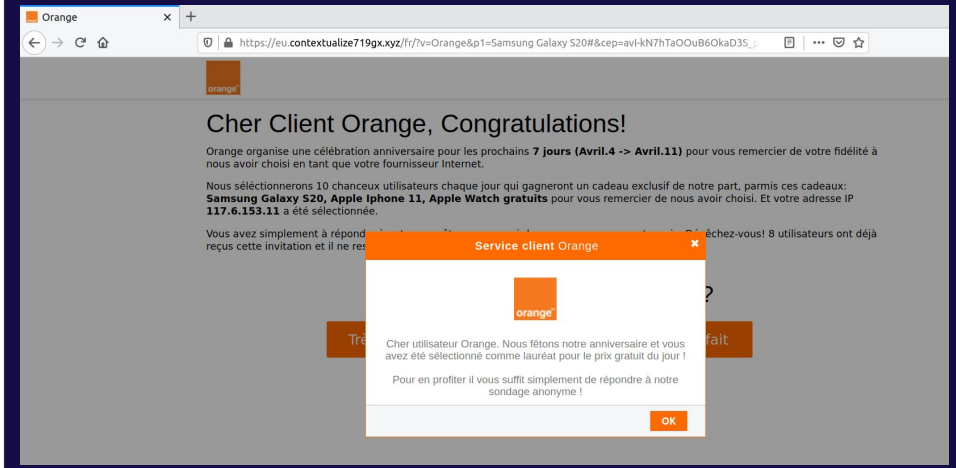
Peak activity: weekends in July

Notable characteristics: This 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.

We believe there to be a close relationship between Nephos7 and eGobbler based on certain shared tactics, techniques, and timing.



eGobbler

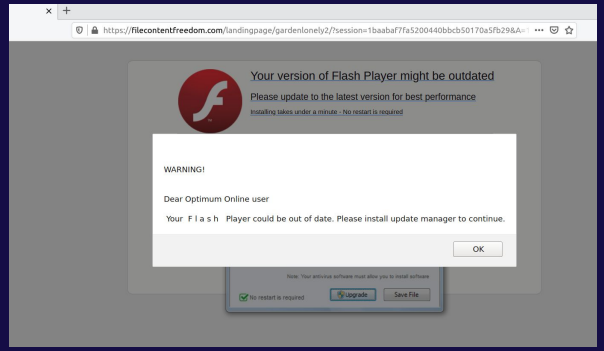
Peak activity: weekends

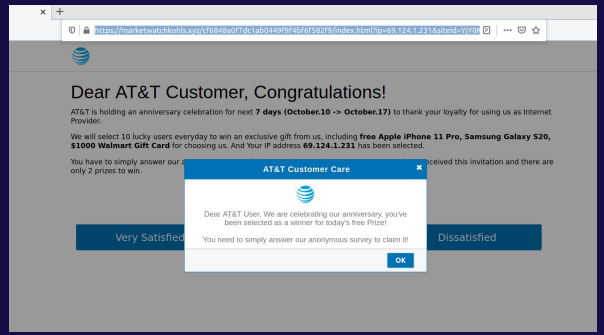
Notable characteristics: eGobbler runs their campaigns in big waves that usually gravitate around the weekends.

Lately, the majority of their activity has been centered around the United States, where they deliver disruptive, highly targeted drive-by downloads and carrier-branded scams.

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

We believe there to be a close relationship between Nephos7 and eGobbler based on certain shared tactics, techniques, and timing.





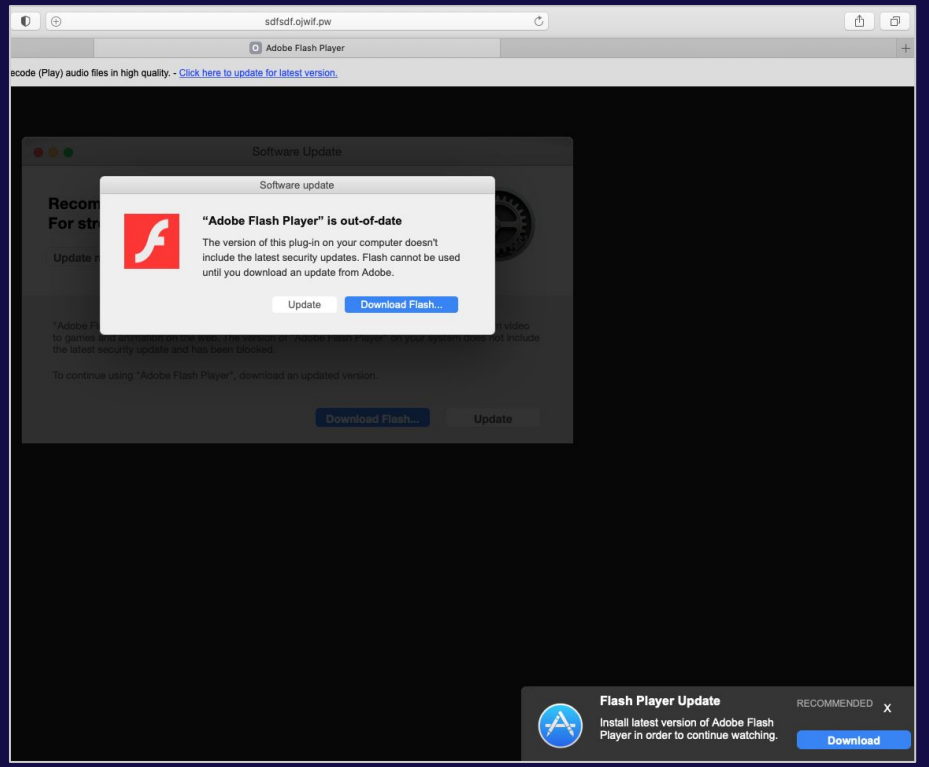
Yosec

Peak activity: throughout the quarter

Notable characteristics: Yosec is a threat actor that pushes fake Flash drive-by downloads and tech support scams via forced redirections.

The bulk of their activity targets Mac devices, particularly the Safari browser.

Yosec malvertising activities are categorized by short, targeted bursts, but at time we have observed up them to ramp up to large volumes over the course of several hours.



Spotlight part 1: FizzCore and Bitcoin Scams

[FizzCore] represents not a single threat actor, but rather a **group of attackers who employ similar techniques to perpetuate bitcoin scams**.

Notably, these threat actors make heavy use of fake celebrity endorsements and employ advanced evasion techniques to bypass ad quality reviews, engaging the industry in an unending game of cat-and-mouse.

Spotlight part 2 : FizzCore and Bitcoin Scams

IMAGE MANIPULATION

USE OF HOMOGLYPHS

Among the sophisticated tactics they use to evade detection are:

- **Cloaking:** Use of fake ad creatives and landing pages when rendering in ad quality scanners.
- **Campaign Flipping:** Running a realistic media buy for several days before switching to malicious messaging.
- **Domain Churning:** Automated algorithmic domain generation, registration, and deployment.
- **Image manipulation:** Highly manipulated images designed to defeat facial recognition.
- **Use of homoglyphs:** Substitution of characters of similar appearance to trip up OCR.

Over 2,800 algorithmically generated domains detected and blocked in the last 30 days.

Conclusion

Q3

- **Quality violations rose significantly from Q2 to Q3,** while **Security issues declined** for the second quarter in a row.
- Threat actors are **combining evasion tactics in ever more sophisticated ways**, with **cloaking**, **image manipulation**, and **use of homoglyphs** rising to the fore in Q3.
- SSP-I and SSP-F, two of the largest and best-known SSPs in the industry, continue their opposite trajectories, with **SSP-I becoming a top performer in Security** after years of struggling and **SSP-F's performance rapidly deteriorating**.
- Security violation rates in Q3 showed **less variance from country to country**, with the U.S. and most major European markets falling within a narrow band.

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