CONFIANT

Demand Quality Report

Q1 2020

Introduction

Confiant's **Demand Quality Report** is a quarterly look into the quality of demand in digital advertising. Using a sample of over 200 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**, **In-Banner Video**, and **Low Quality ads** diminish the value of demand and drive user 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 October 2018, Confiant released the industry's first benchmark report. This report, the eight in the series, covers Q1 2020.

Methodology

To compile the research contained in this report, Confiant analyzed a normalized sample of **more than 200 billion programmatic advertising impressions** from January 1 to March 31, 2020 from **over 30,000 sites 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.

With the exception of the Q1 Rates by Country slide, all data and charts are based on traffic generated in the United States.

Definitions

Malicious ad A creative that includes (usually obfuscated) Javascript that spawns a forced redirect or loads a secondary, or tertiary, payload for similar malicious purposes. Most malicious creatives exist for the purpose of forcing users to interact with phishing scams, but some perform cryptojacking or infect the user's device to propagate botnets and other nefarious activities.

In-Banner Video (IBV) ad The practice of serving video ads in banner placements without the publisher's consent, and often without the advertiser's consent either. In these cases, a video ad unit is loaded within a banner placement as a display unit, instead of playing within a media player.

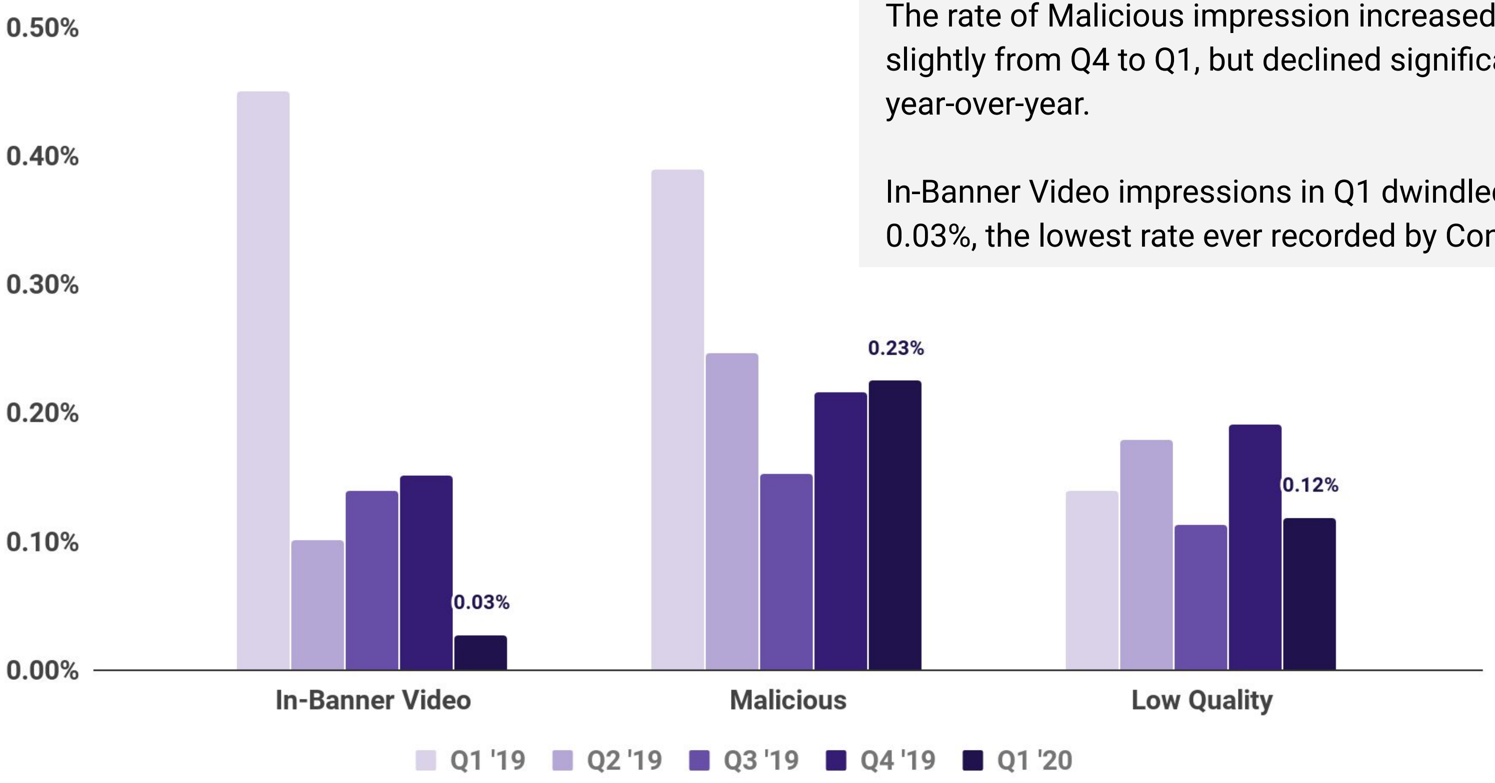
Low Quality ad Creative violations across a range of different quality specifications selected by the publisher. The dimensions include audio/video related violations, creatives probing for user's geolocation, the network load of the ad, and much more.

High-Risk Ad Platforms (HRAPs) Ad platforms are ad platforms that consistently serve as major vectors for malicious actors. For a platform to receive this designation from Confiant, we have to have observed malicious campaigns persist on an ongoing basis to a point that it is unclear if the platform is negligent, complicit, or just overwhelmed.

Security The aggregation of all sources of elevated security risk, including Malicious ads and those from High-Risk Ad Platforms.

Industry View

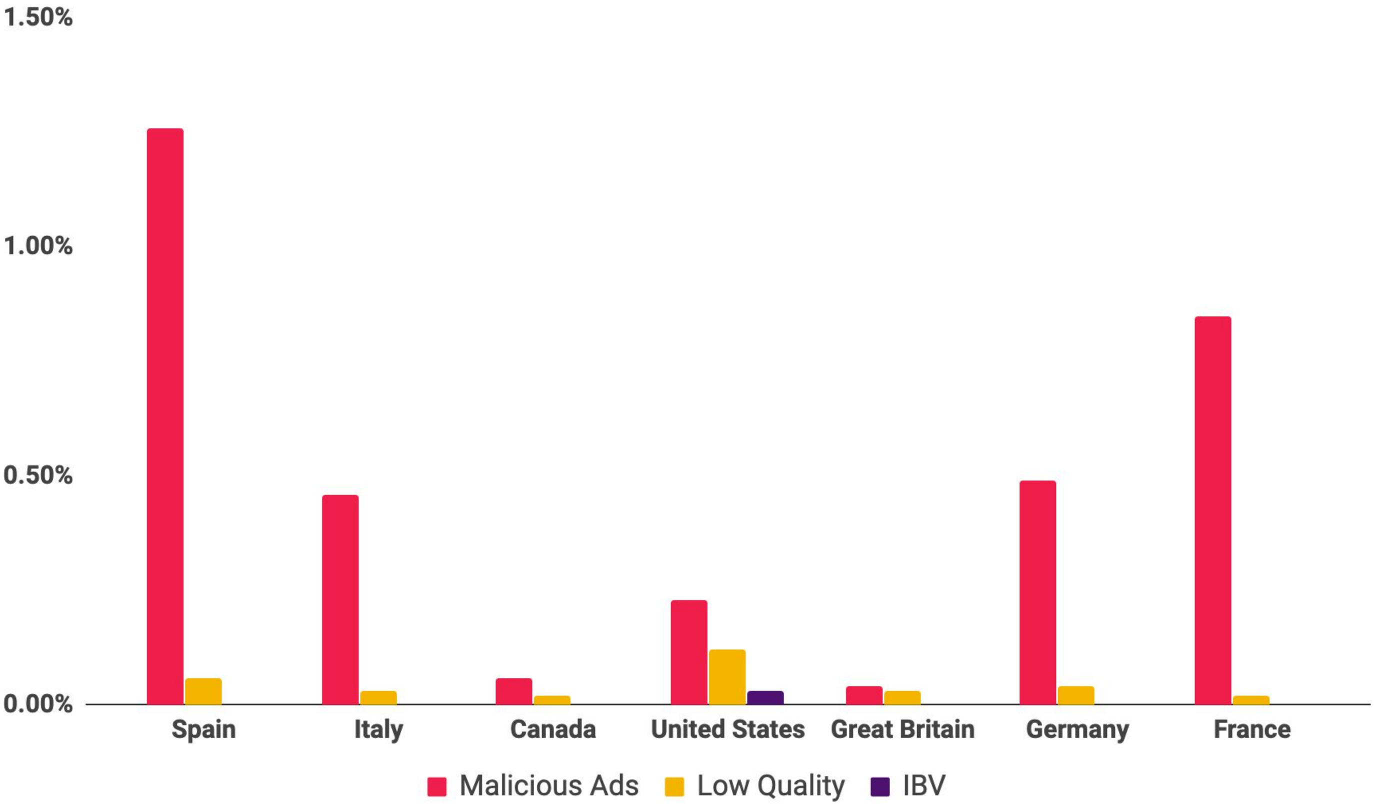
How did the industry fare in Q1 2020?



The rate of Malicious impression increased slightly from Q4 to Q1, but declined significantly year-over-year.

In-Banner Video impressions in Q1 dwindled to 0.03%, the lowest rate ever recorded by Confiant.

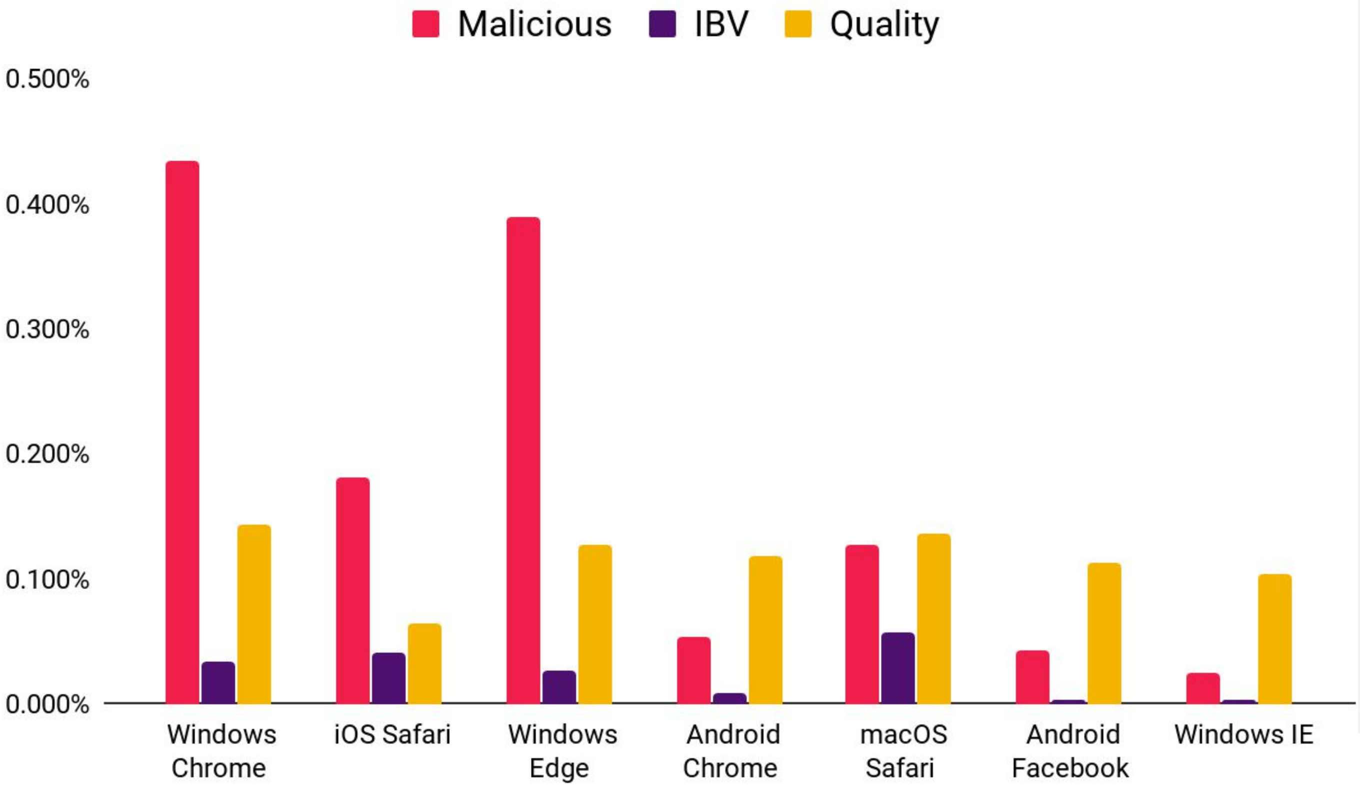
Q1 Rates by Country



As in past quarters, **European markets saw far higher rates of Malicious ads than the U.S.**, but generally a lower rate on other issues.

The variety of rates by country exemplifies how malvertisers continually shift their campaigns and targets to remain under the radar.

Q1 Rates by user agent

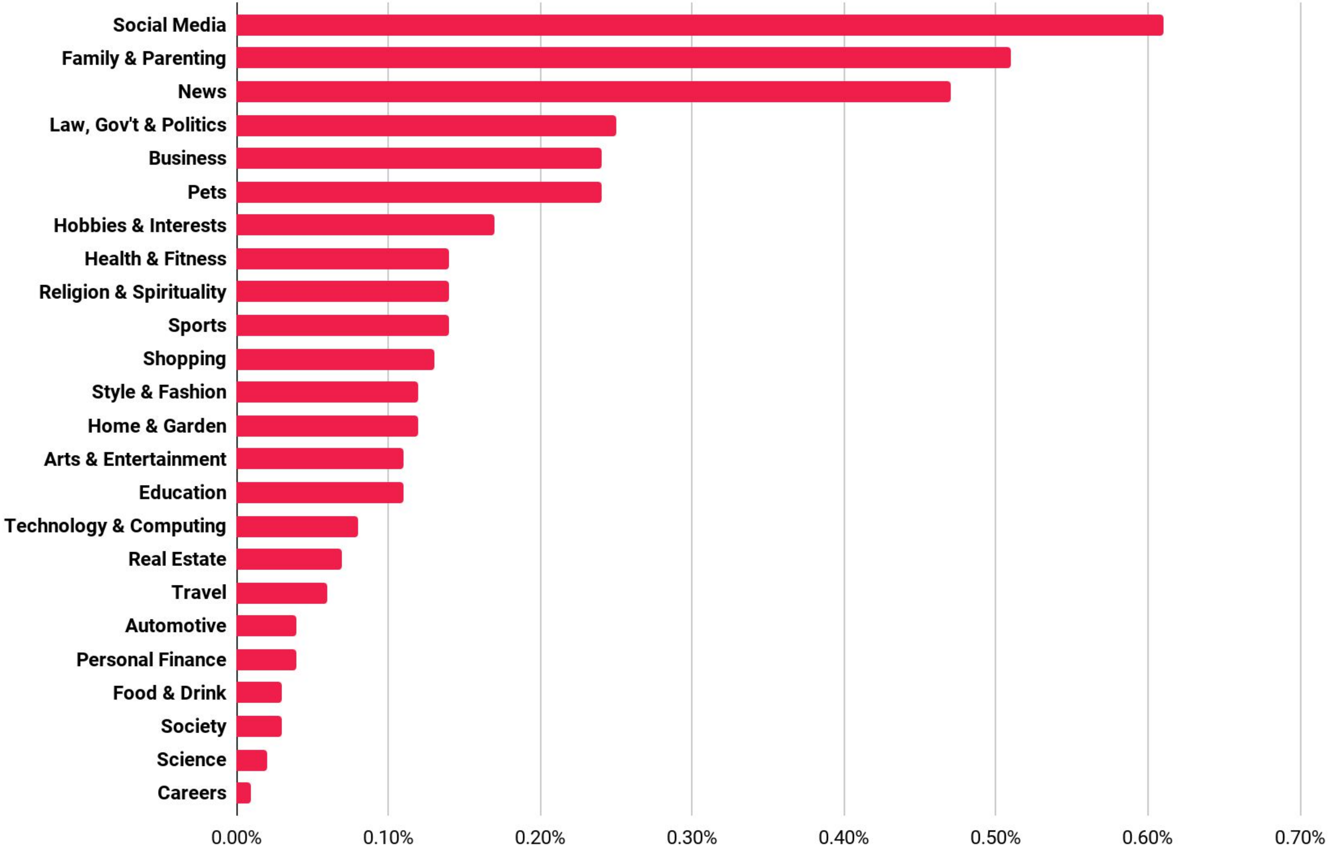


The frequency of issues varies considerably by browser and operating system.

In Q1, we observed **high malicious ad rates for Windows OS**, with Chrome and Edge on that platform exhibiting similar numbers. This differs markedly from 2019, where iOS Safari had the highest rate of malicious ads by a significant margin.

Notably, non-security issues were about equally represented across the various browsers.

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 malicious ads affect sites in different categories.

Our analysis showed that **Social Media** sites were more than **twice as likely** as the average site to be hit with a security issue (a malicious or HRAP ad). **News** and **Family & Parenting** also were standouts when it came to malware risk.

SSP Rankings

Q1 2020 US SSP Rankings

In Q1, Confiant tracked impressions from over 75 SSPs. However, **over 75% of impressions originated from just 13 providers**[1] commonly used by publishers. These providers are noted in the charts that follow using a coding system that carries over from one quarter to the next.

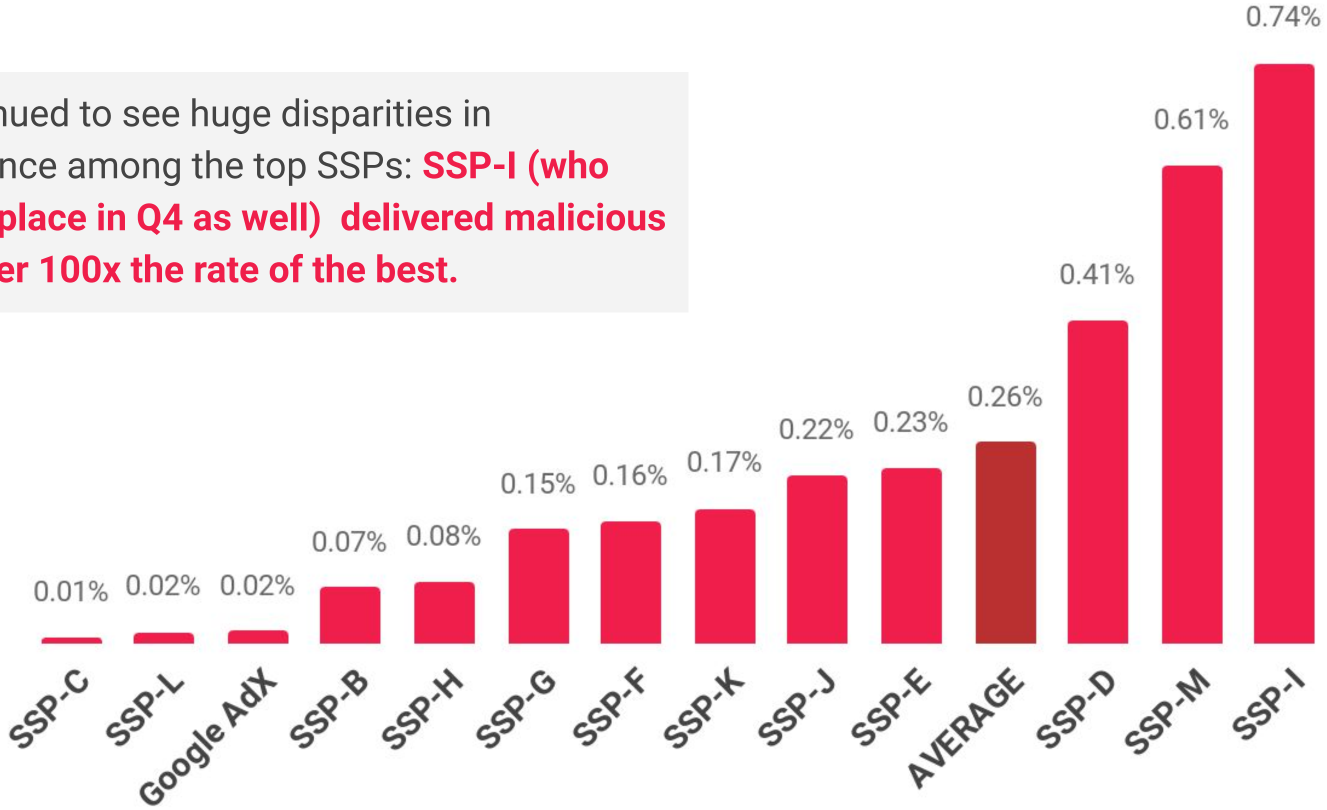
To qualify for inclusion, a provider had to have been a consistent source of **at least 1 billion impressions** in each of the last few quarters.

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.

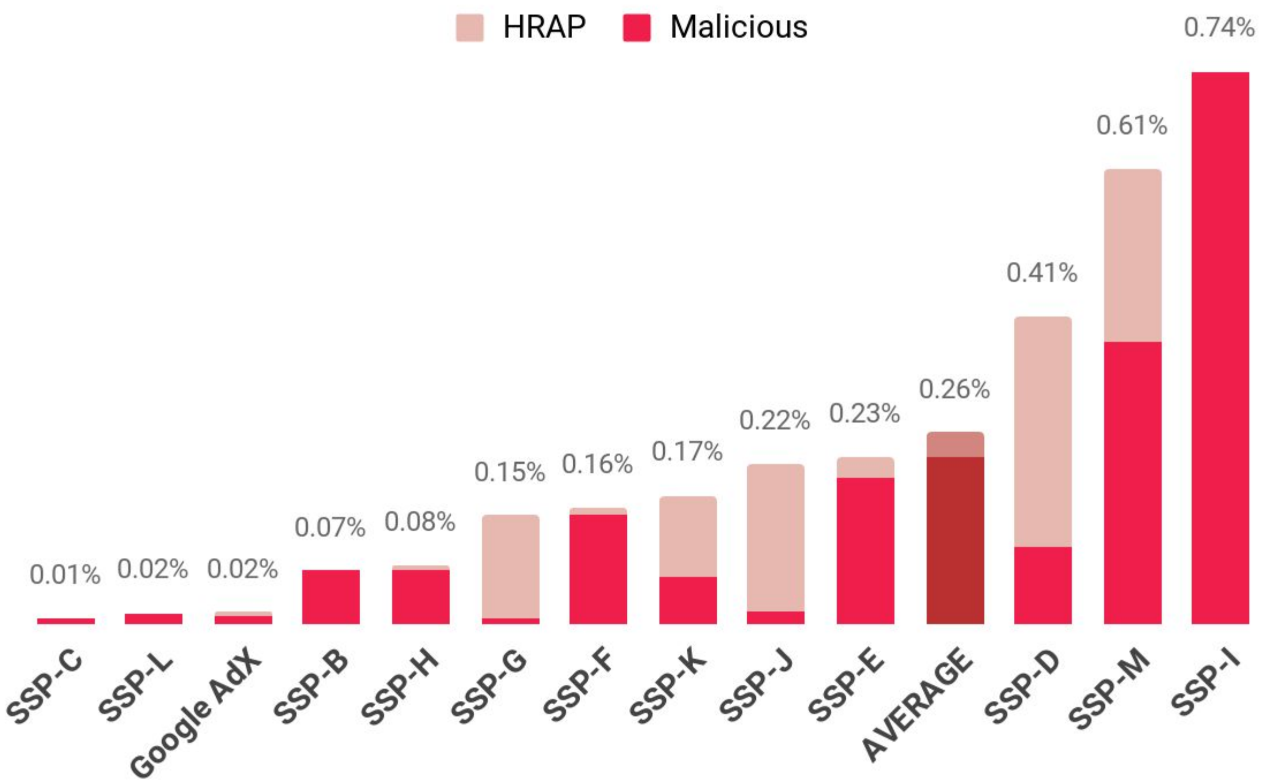
[1] Google AdX, Rubicon Project, OpenX, Xandr, Verizon Media, Index Exchange, Pubmatic, EMX, Sonobi, TripleLift, District M, 33Across, and Sovrn

Security Violation Rate by SSP

We continued to see huge disparities in performance among the top SSPs: **SSP-I (who held last place in Q4 as well) delivered malicious ads at over 100x the rate of the best.**



Security Violation Rate Breakdown



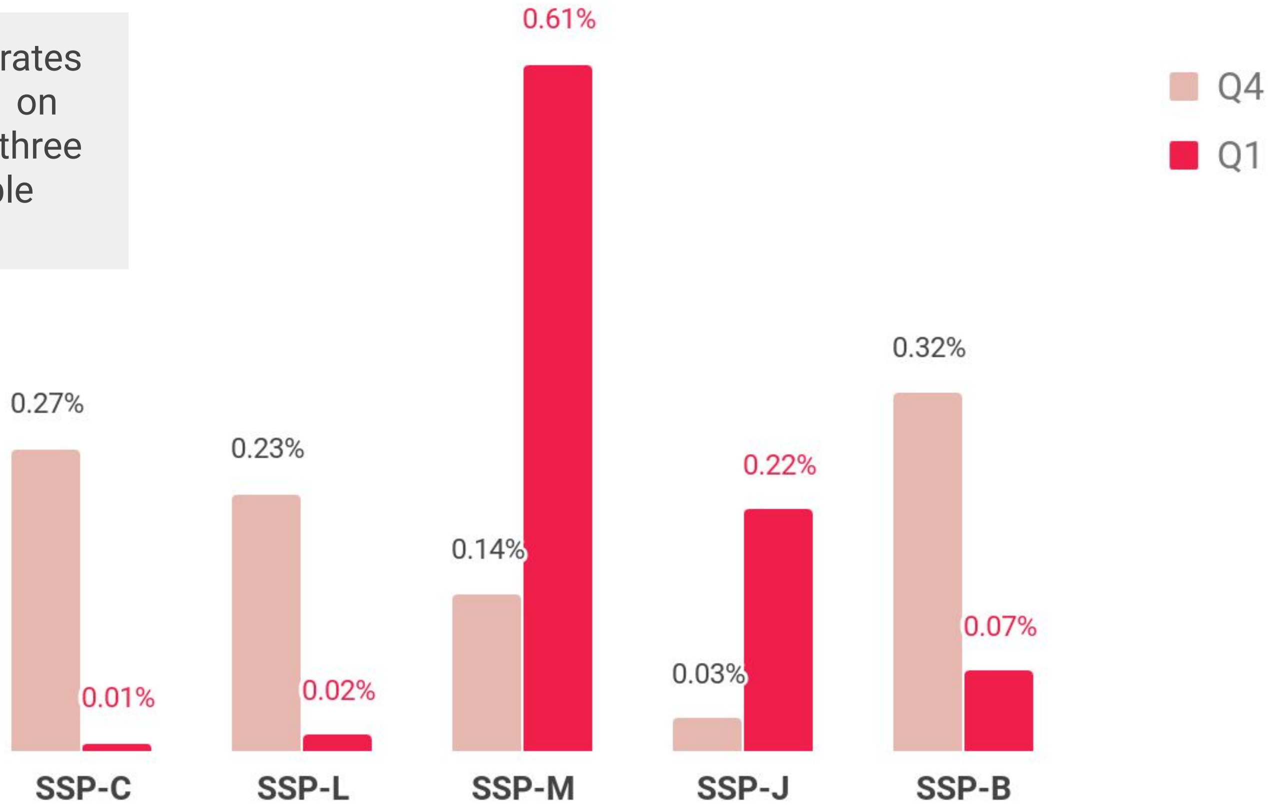
High Risk Ad Platforms (HRAPs) are ad platforms that consistently serve as major vectors for malicious actors.

For a platform to receive this designation from Confiant, we have to have observed malicious campaigns persist on an ongoing basis to a point that it is unclear if the platform is negligent, complicit, or just overwhelmed.

This chart shows how the inclusion of impressions from HRAPs **increases the risk profiles of SSPs G, J, and D.**

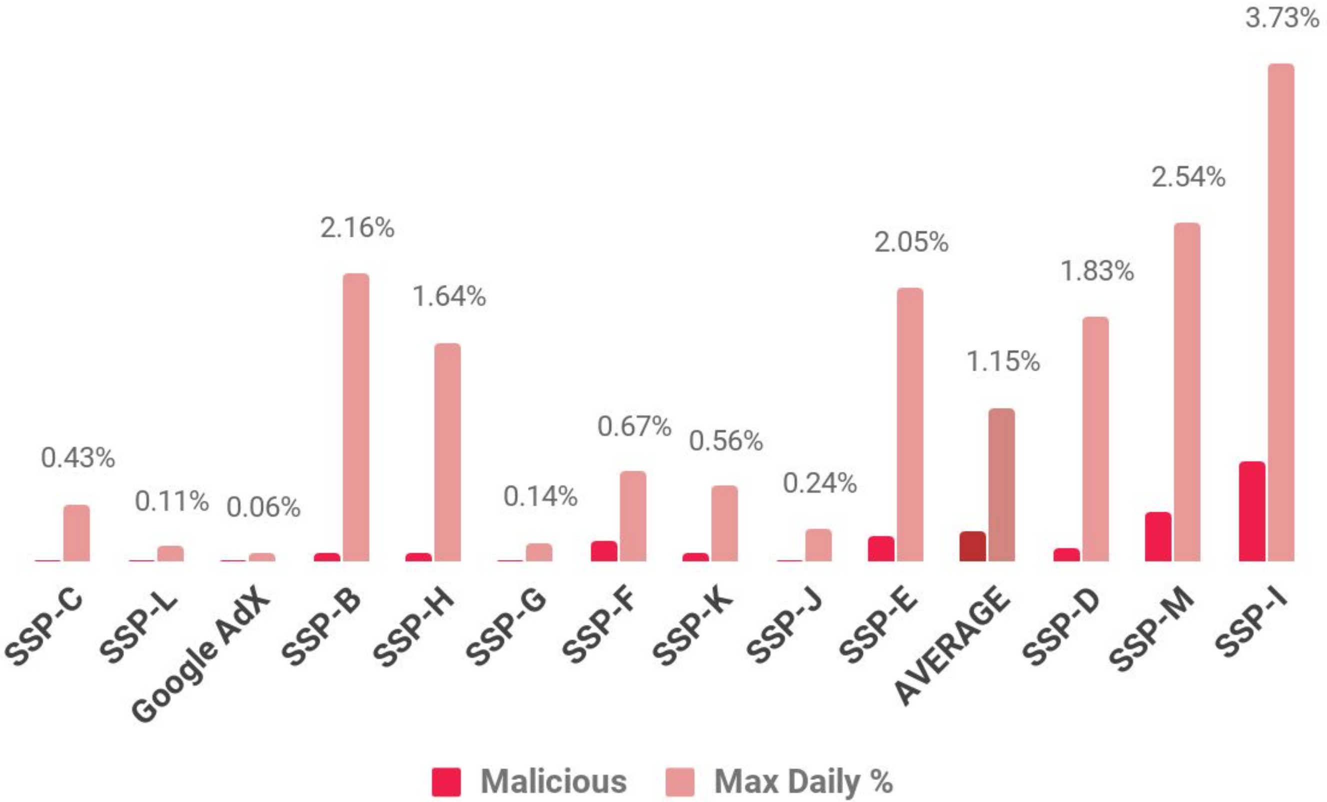
Security Violation Rate: Q4 '19 vs. Q1 '20

Security violation ad rates spiked from Q4 to Q1 on SSPs M and J, while three others showed notable improvement.



In Q1, **75%** of impressions with **security issues** came from just **2 SSPs**

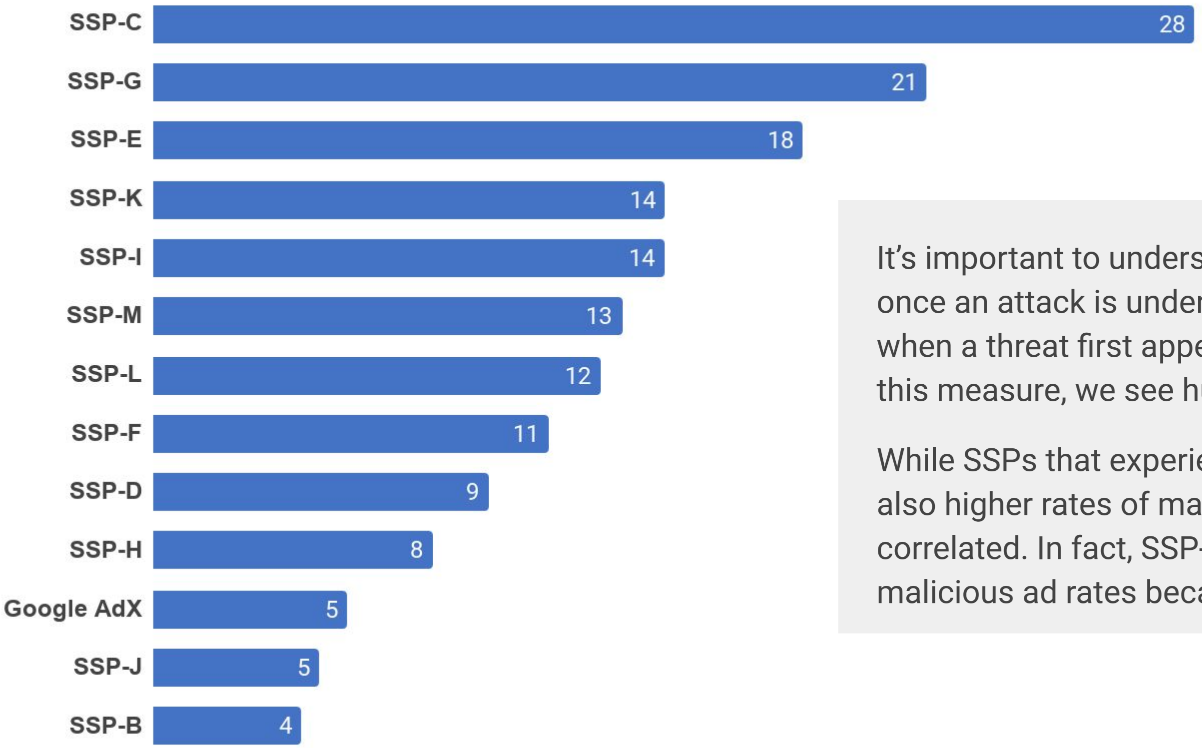
Daily Maximum Malicious Rate by SSP



Quarterly averages can mask significant variation in day-to-day performance, so it’s important to measure the **upper bound of the Malicious ad rate** for each SSP to get a sense of risk (excluding HRAP ads).

When under sustained attack, **SSPs had days when 2 of every 100 impressions were malicious**, putting publisher relationships at considerable risk.

Avg Duration of Attack by SSP (in days)



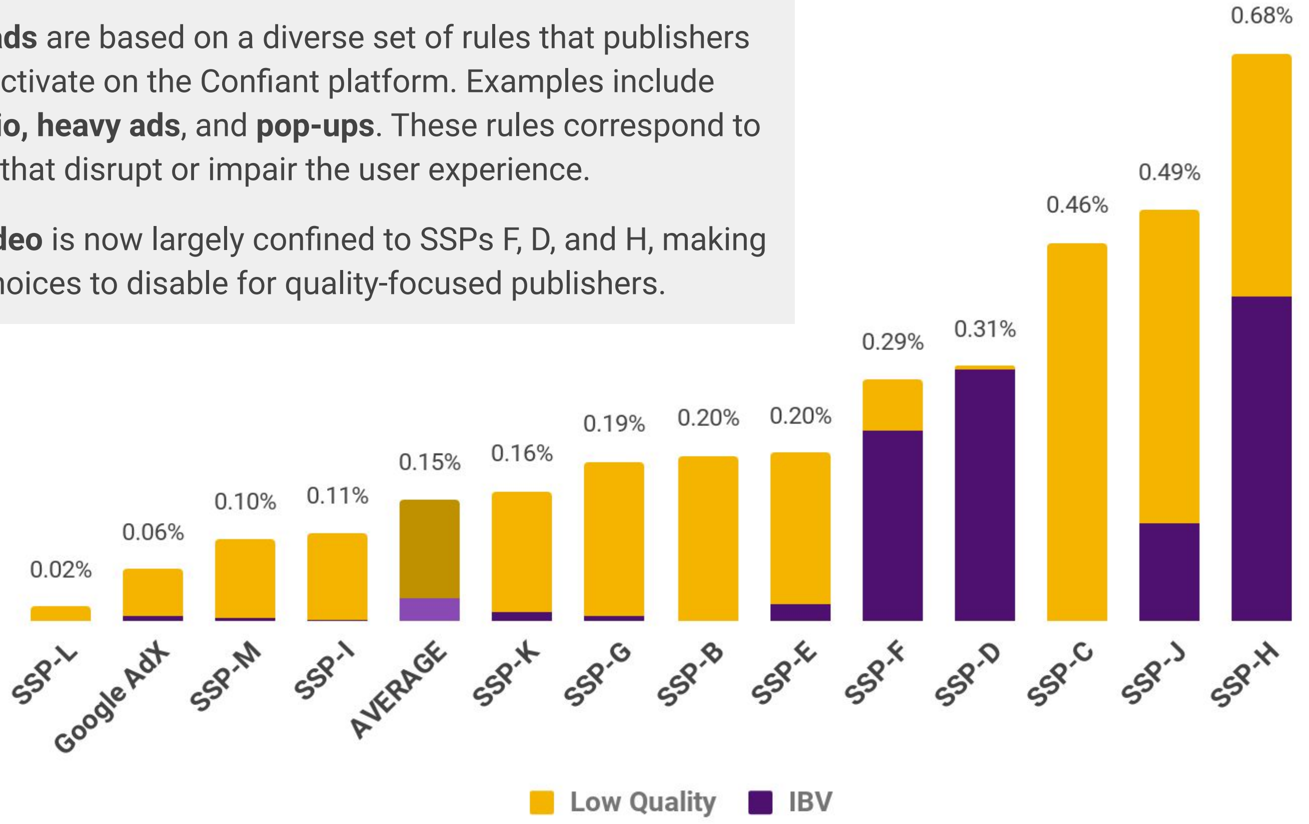
It’s important to understand **how long threats persist on an SSP** once an attack is underway. We measure how long it takes from when a threat first appears on an SSP to when it’s last seen. On this measure, we see huge differences among the major SSPs.

While SSPs that experience long-duration attacks also tend to also higher rates of malicious ads, the two aren’t perfectly correlated. In fact, SSP-C had a high average duration but a low malicious ad rates because the number of incidents was low.

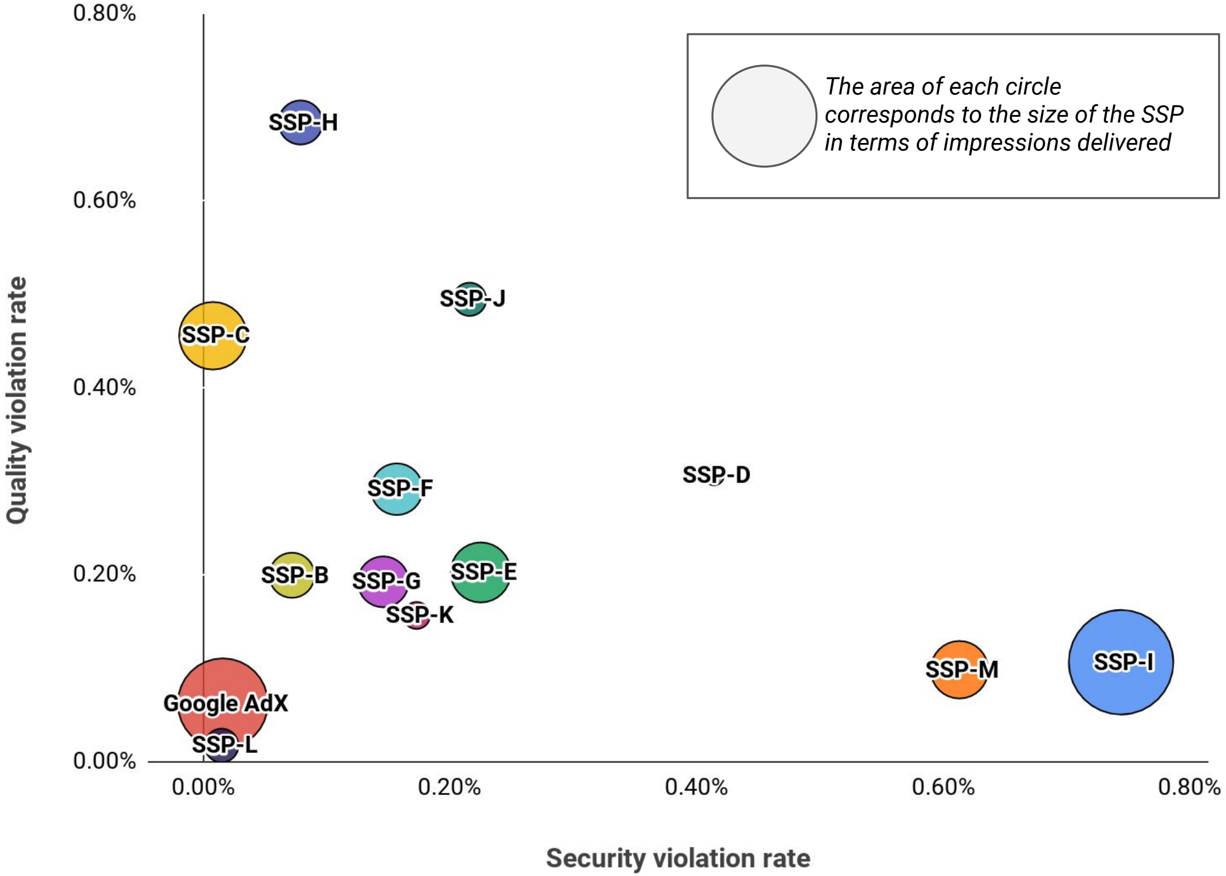
Quality Violation Rate by SSP

Low Quality ads are based on a diverse set of rules that publishers can elect to activate on the Confiant platform. Examples include **autoplay audio, 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, D, and H, making them good choices to disable for quality-focused publishers.



Violation Rates by SSP Size



Interestingly, **we did not observe a correlation between SSP size** (as measured by the number of impressions an SSP delivered to publishers) **and violation rates**.

The best overall performer, SSP-L, was one of the smallest among the top 13 SSPs we tracked, while the worst performer, SSP-I, was one of the largest SSPs in the sample.

Major Threat Groups Active in Q1

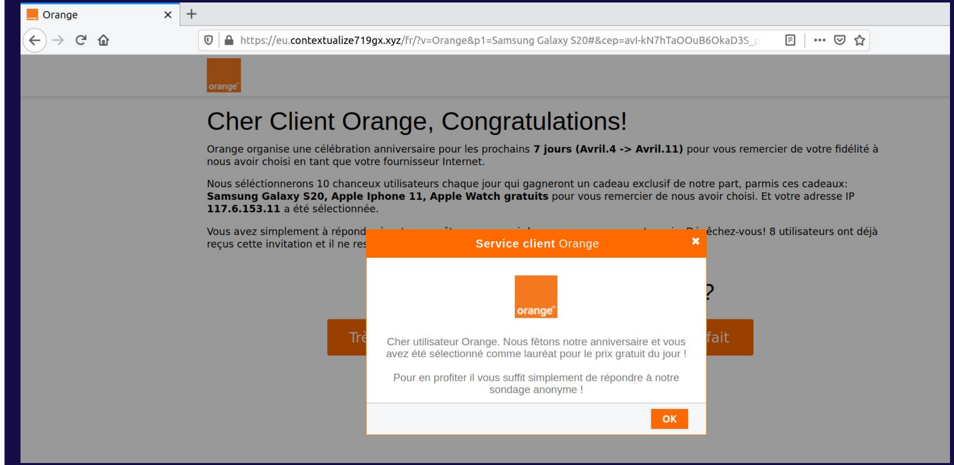
Nephos7

Peak activity: Mid to late February

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

The primary mode of operation for Nephos7 is to churn and burn dozens of CDN domains, 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.


Orange
https://eu.contextualize719gx.xyz/fr/?v=Orange&p1=Samsung Galaxy S20#&cep=avl-kN7hTaOOuB6OkaD3S_
orange
Trè
?
fait
orange
OK

Cher Client Orange, Congratulations!

Orange organise une célébration anniversaire pour les prochains **7 jours (Avril.4 -> Avril.11)** pour vous remercier de votre fidélité à nous avoir choisi en tant que votre fournisseur Internet.

Nous séléctionnerons 10 chanceux utilisateurs chaque jour qui gagneront un cadeau exclusif de notre part, parmis ces cadeaux: **Samsung Galaxy S20, Apple Iphone 11, Apple Watch gratuits** pour vous remercier de nous avoir choisi. Et votre adresse IP **117.6.153.11** a été sélectionnée.

Vous avez simplement à répond échez-vous! 8 utilisateurs ont déjà reçus cette invitation et il ne res

Service client Orange

Cher utilisateur Orange. Nous fêtons notre anniversaire et vous avez été sélectionné comme lauréat pour le prix gratuit du jour !

Pour en profiter il vous suffit simplement de répondre à notre sondage anonyme !

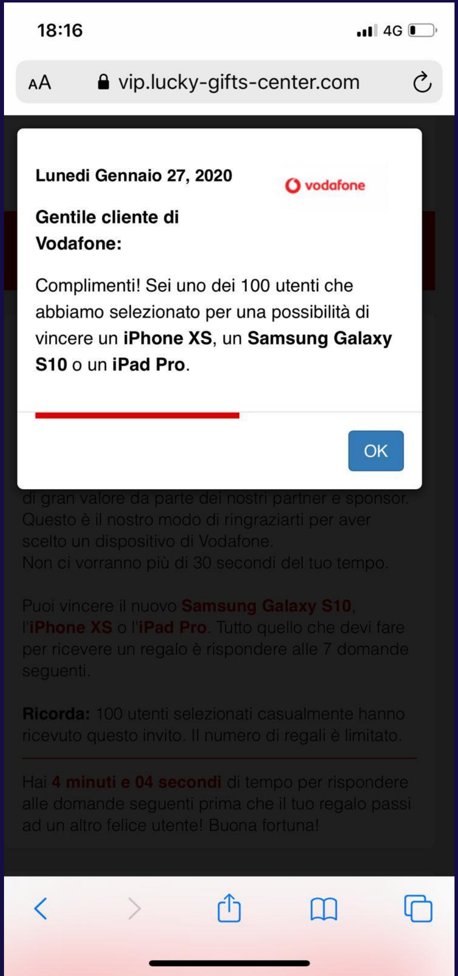
DCCBoost

Peak activity: mid-February

Notable characteristics: DCCBoost campaigns have shown 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.



Lunedi Gennaio 27, 2020

Gentile cliente di Vodafone:

Complimenti! Sei uno dei 100 utenti che abbiamo selezionato per una possibilità di vincere un **iPhone XS**, un **Samsung Galaxy S10** o un **iPad Pro**.

di gran valore da parte dei nostri partner e sponsor. Questo è il nostro modo di ringraziarti per aver scelto un dispositivo di Vodafone.
Non ci vorranno più di 30 secondi del tuo tempo.

Puoi vincere il nuovo **Samsung Galaxy S10**, l'**iPhone XS** o l'**iPad Pro**. Tutto quello che devi fare per ricevere un regalo è rispondere alle 7 domande seguenti.

Ricorda: 100 utenti selezionati casualmente hanno ricevuto questo invito. Il numero di regali è limitato.

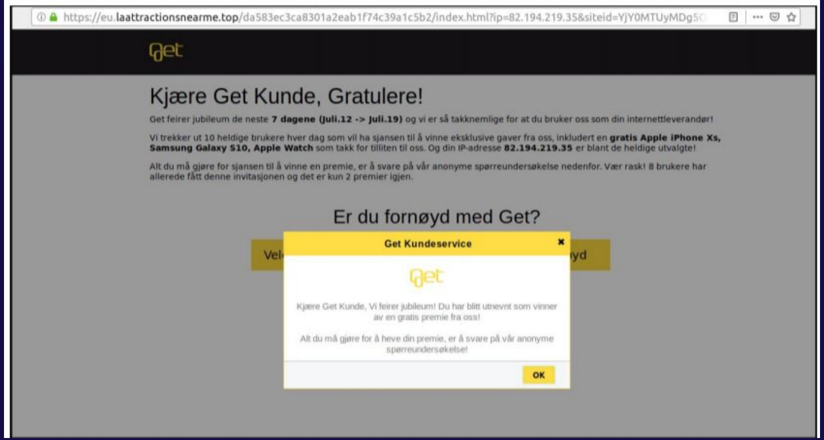
Hai **4 minuti e 04 secondi** di tempo per rispondere alle domande seguenti prima che il tuo regalo passi ad un altro felice utente! Buona fortuna!

eGobbler

Peak activity: mid-February

Notable characteristics: This Asia-based attack group has a history of exploiting obscure browser bugs to bypass built-in browser protections against pop-ups and forced redirects.

After Confiant discovered a previous vulnerability in early 2019 and worked with the Chrome team to shut it down, eGobbler introduced a Webkit exploit.



https://eu.laattractionsnearme.top/da583ec3ca8301a2eab1f74c39a1c5b2/index.html?ip=82.194.219.35&siteid=YjY0MTUyMDg5

Kjære Get Kunde, Gratulere!

Get feirer jubileum de neste **7 dagene (Juli.12 -> Juli.19)** og vi er så takknemlige for at du bruker oss som din internettleverandør!

Vi trekker ut 10 heldige brukere hver dag som vil ha sjansen til å vinne eksklusive gaver fra oss, inkludert en **gratis Apple iPhone Xs, Samsung Galaxy S10, Apple Watch** som takk for tilliten til oss. Og din IP-adresse **82.194.219.35** er blant de heldige utvalgte!

Alt du må gjøre for sjansen til å vinne en premie, er å svare på vår anonyme spørreundersøkelse nedenfor. Vær rask! 8 brukere har allerede fått denne invitasjonen og det er kun 2 premier igjen.

Er du fornøyd med Get?

Get Kundeservice ×

Kjære Get Kunde, Vi feirer jubileum! Du har blitt utnevnt som vinner av en gratis premie fra oss!

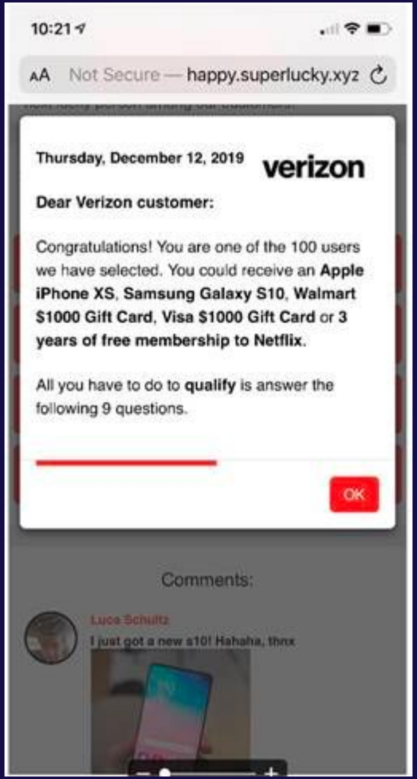
Alt du må gjøre for å heve din premie, er å svare på vår anonyme spørreundersøkelse!

Scamclub

Peak activity: late February

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.



Thursday, December 12, 2019

verizon

Dear Verizon customer:

Congratulations! You are one of the 100 users we have selected. You could receive an **Apple iPhone XS**, **Samsung Galaxy S10**, **Walmart $1000 Gift Card**, **Visa $1000 Gift Card** or **3 years of free membership to Netflix**.

All you have to do to **qualify** is answer the following 9 questions.

Comments:

Luca Schultz

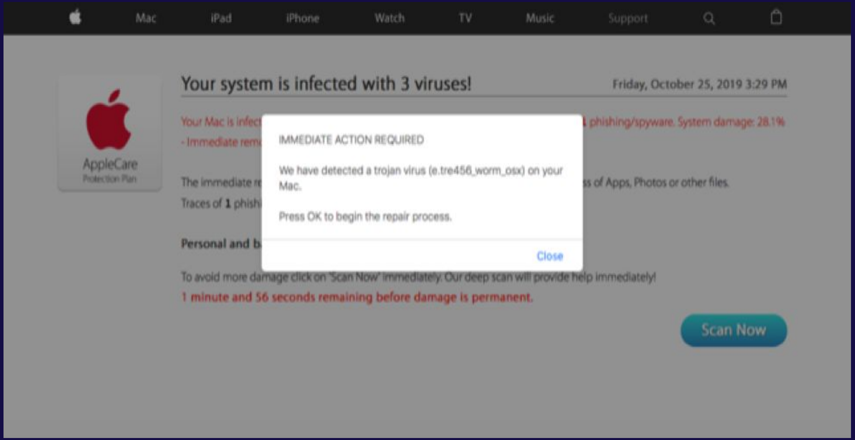
I just got a new s10! Hahaha, thnx

Yosec

Peak activity: late Feb.- early March

Notable characteristics: One of the new kids on the malvertising block, Yosec had close to 100 unique malicious creatives active as of 10/31, predominantly via AdForm.

Named after their CTA messaging along the lines of “Your Mac Security”, this attacker based in Eastern Europe has been consistently serving up redirects to threatening malware pages.



Your system is infected with 3 viruses!

Friday, October 25, 2019 3:29 PM

Your Mac is infect … 1 phishing/spyware. System damage: 28.1%

- Immediate rem…

The immediate r… …s of Apps, Photos or other files.

Traces of **1** phish…

Personal and b…

To avoid more damage click on 'Scan Now' immediately. Our deep scan will provide help immediately!

1 minute and 56 seconds remaining before damage is permanent.

IMMEDIATE ACTION REQUIRED

We have detected a trojan virus (e.tre456_worm_osx) on your Mac.

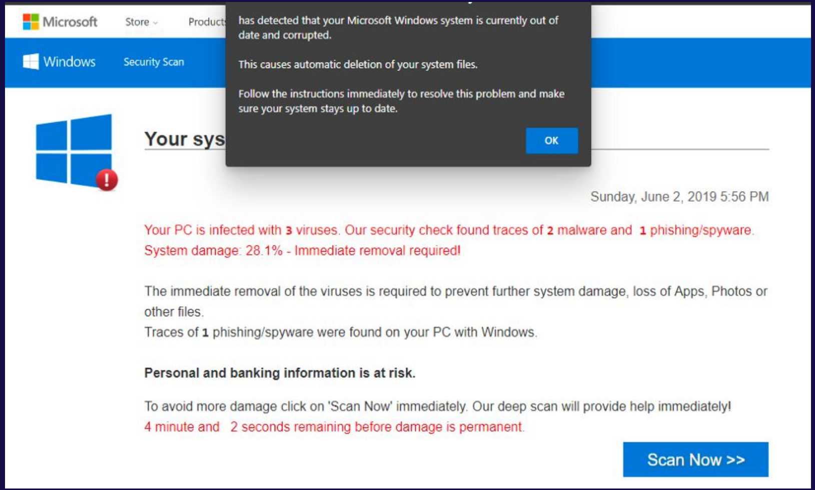
Press OK to begin the repair process.

SelfRef10

Peak activity: mid-February

Notable characteristics: We first called the industry's attention to this malvertising middleman about 6 months ago in our blog post here.

SelfRef10 specializes in forming bi-directional ad tech relationships that empower them both to buy and to sell so that they can play both sides of the coin. They've shown no signs of slowdown in the last half year and continue to run desktop redirect campaigns, often choosing vague domains as delivery vehicles. They've been active through November via Index Exchange on MediaSmart DSP as "ClickFollow Ltd".



has detected that your Microsoft Windows system is currently out of date and corrupted.

This causes automatic deletion of your system files.

Follow the instructions immediately to resolve this problem and make sure your system stays up to date.

Your sys

Sunday, June 2, 2019 5:56 PM

Your PC is infected with 3 viruses. Our security check found traces of 2 malware and 1 phishing/spyware.
System damage: 28.1% - Immediate removal required!

The immediate removal of the viruses is required to prevent further system damage, loss of Apps, Photos or other files.
Traces of 1 phishing/spyware were found on your PC with Windows.

Personal and banking information is at risk.

To avoid more damage click on 'Scan Now' immediately. Our deep scan will provide help immediately!
4 minute and 2 seconds remaining before damage is permanent.

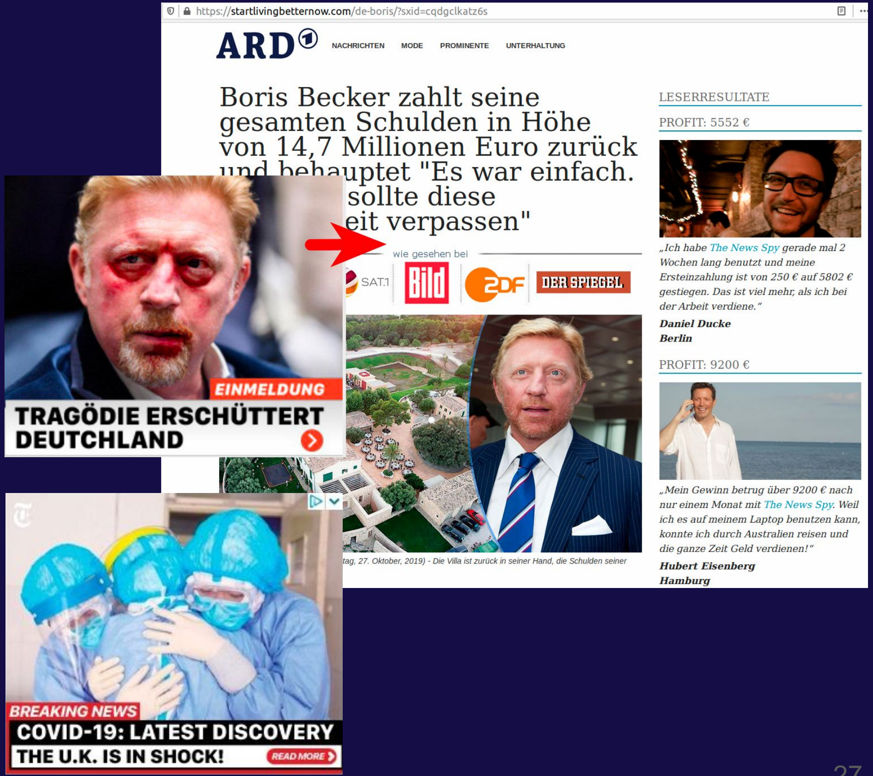
FizzCore

Peak activity:throughout 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 implements techniques to evade 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.



https://startlivingbetternow.com/de-boris/?sxid=cqdgclkatz6s

ARD

NACHRICHTEN MODE PROMINENTE UNTERHALTUNG

Boris Becker zahlt seine gesamten Schulden in Höhe von 14,7 Millionen Euro zurück und behauptet "Es war einfach. sollte diese eit verpassen"

wie gesehen bei

tag, 27. Oktober, 2019) - Die Villa ist zurück in seiner Hand, die Schulden seiner

LESERRESULTATE

PROFIT: 5552 €

„Ich habe The News Spy gerade mal 2 Wochen lang benutzt und meine Ersteinzahlung ist von 250 € auf 5802 € gestiegen. Das ist viel mehr, als ich bei der Arbeit verdiene.“

Daniel Ducke
Berlin

PROFIT: 9200 €

„Mein Gewinn betrug über 9200 € nach nur einem Monat mit The News Spy. Weil ich es auf meinem Laptop benutzen kann, konnte ich durch Australien reisen und die ganze Zeit Geld verdienen!“

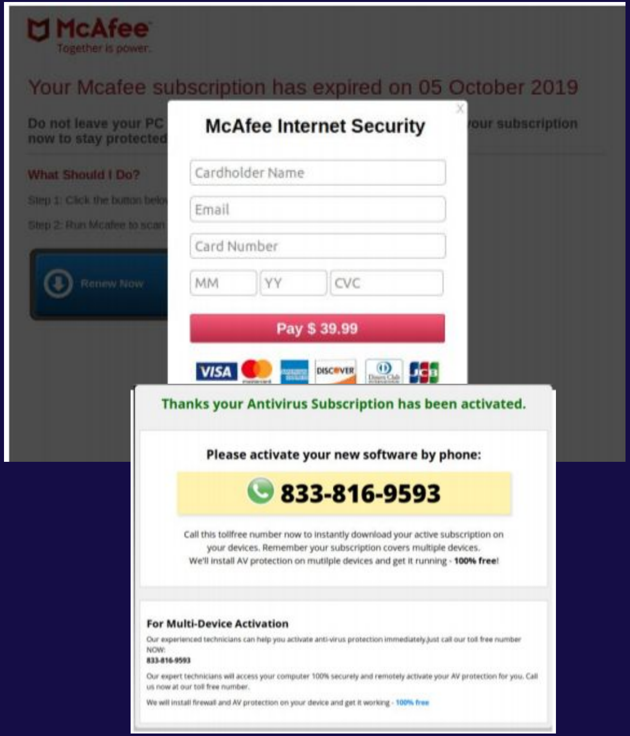
Hubert Eisenberg
Hamburg

Zirconium

Peak activity: January

Notable characteristics: Zirconium runs a very sophisticated malvertising operation that's notable for unique fingerprinting techniques that are carried out in multiple stages. This group, which just two years ago was focused on churning out fake agencies by the handful in order to win seats on buying platforms, has since shifted their approach, but are still running similar tech support focused malvertising campaigns.

The attacker stands out in their choice to target primarily desktop devices and their use of increasingly sophisticated Javascript obfuscation.



McAfee
Together is power.

Your Mcafee subscription has expired on 05 October 2019

Do not leave your PC ... your subscription now to stay protected

What Should I Do?

Step 1: Click the button belo...

Step 2: Run Mcafee to scan ...

Renew Now

McAfee Internet Security

Cardholder Name

Email

Card Number

MM YY CVC

Pay $ 39.99

Thanks your Antivirus Subscription has been activated.

Please activate your new software by phone:

☎ 833-816-9593

Call this tollfree number now to instantly download your active subscription on your devices. Remember your subscription covers multiple devices.
We'll install AV protection on mutilple devices and get it running - **100% free**!

For Multi-Device Activation

Our experienced technicians can help you activate anti-virus protection immediately.Just call our toll free number NOW:
833-816-9593

Our expert technicians will access your computer 100% securely and remotely activate your AV protection for you. Call us now at our toll free number.

We will install firewall and AV protection on your device and get it working - 100% free

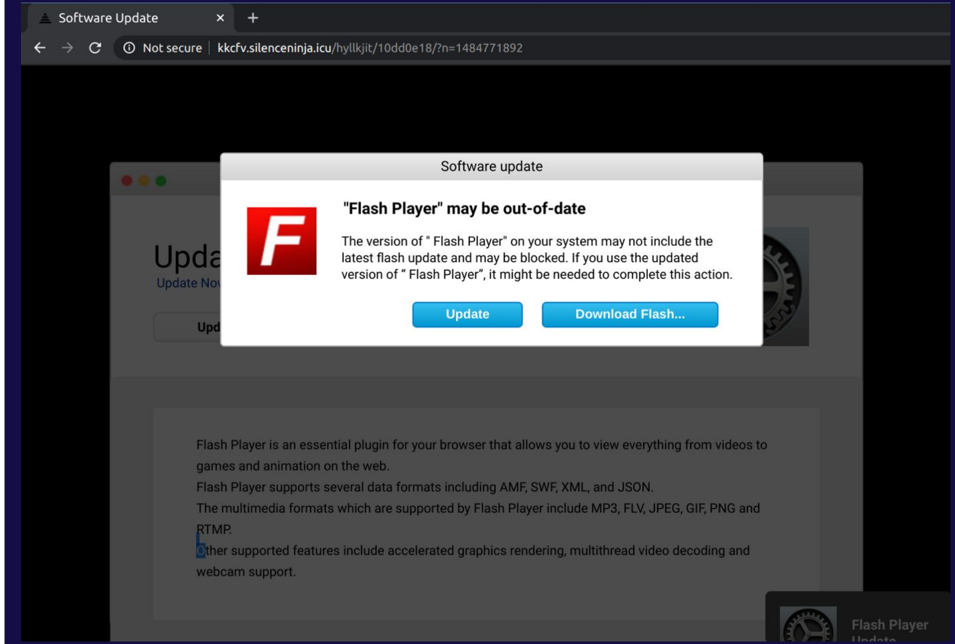
Tag Barnakle

Peak activity: Dec 2019 - Present

Notable characteristics: Ongoing malvertising campaign that is perpetrated by an attacker via mass compromise of Revive Ad Server instances.

Tag Barnakle will hack into publisher and advertiser ad serving infrastructure in order to append their malicious payload to existing ad slots, resulting in free access to publisher inventory.

Unlike most attackers, who must create fake agencies and run cloaked ad code in order to launch attacks, Tag Barnakle *doesn't have to spend a single cent on running ad campaigns*.



kkcfv.silenceninja.icu/hyllkjit/10dd0e18/?n=1484771892

Software update

"Flash Player" may be out-of-date

The version of " Flash Player" on your system may not include the latest flash update and may be blocked. If you use the updated version of " Flash Player", it might be needed to complete this action.

Update | Download Flash...

Flash Player is an essential plugin for your browser that allows you to view everything from videos to games and animation on the web.

Flash Player supports several data formats including AMF, SWF, XML, and JSON.

The multimedia formats which are supported by Flash Player include MP3, FLV, JPEG, GIF, PNG and RTMP.

Other supported features include accelerated graphics rendering, multithread video decoding and webcam support.

Conclusion

Q1

- ➔ **Malicious ads** increased modestly in Q1 compared to Q4, but the emergence of **new threat actors** like **Fizzcore** and their use of **advanced evasion tactics** and **COVID-19 imagery** suggest activity may be about to surge.
- ➔ The **size of an SSP** is **no guarantee of quality**. While we did not observe a correlation between SSP size and violation rate, one of the largest SSPs we tracked was the worst overall performer.
- ➔ Issues remained highly concentrated: **75% of security violations** came from just 2 SSPs.
- ➔ **In-Banner Video** activity was at the lowest level ever observed by Confiant.
- ➔ **Social Media sites** were **twice as likely** to be hit with **security issues.**

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, and 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