Q2 2020

SMART

[Summary of Malicious And Reputational Threats]

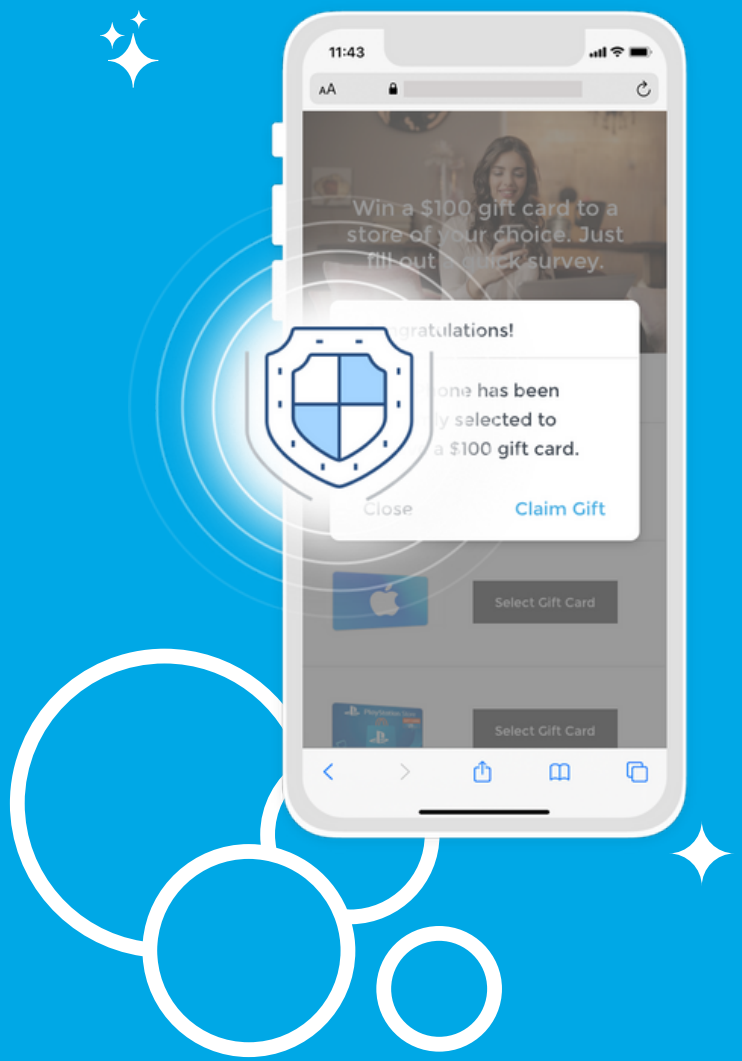
Report

clean.io

Every Ad, Every Threat

TABLE OF CONTENTS

KEY MALVERTISING DATA TAKEAWAYS



ABOUT THIS REPORT

This report is built using threat and attack data gathered from sites across the entire clean.io network.

The data included in this report is collected through behavioral analysis of tens of billions of impressions each month in real time on over 7 million websites and apps.

Q2 2020 SMART REPORT

Q2 2020 KEY TRENDS

COVID EFFECTS

HOW HAS COVID AFFECTED THE MALVERTISING LANDSCAPE?

Major changes in the way we work and consume content, shifts in the behavior of brand advertisers, as well as spikes in the virus itself have all contributed to trends observed in Q2.

Major Themes

4

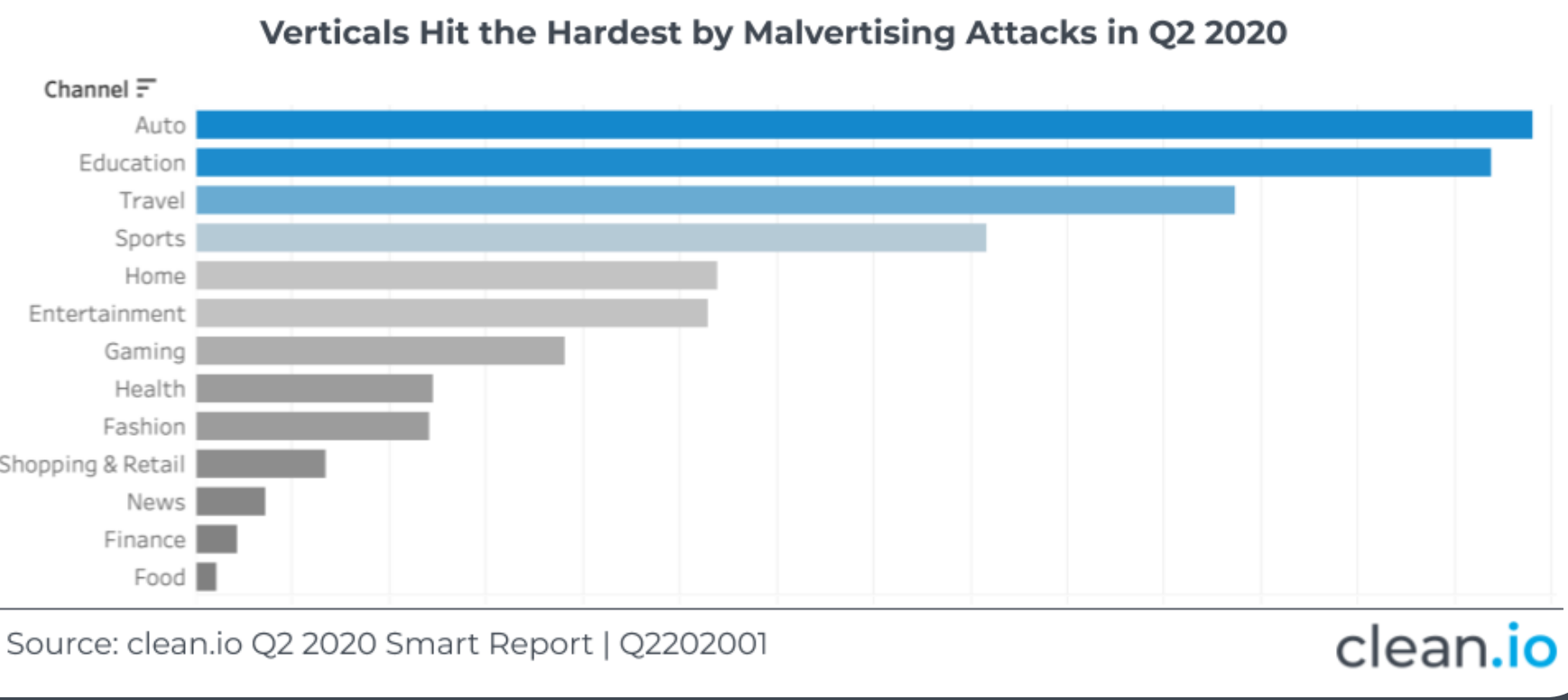
Key Content Verticals Impacted

Threat Level

follows

Demand

KEY IMPACTED VERTICALS



CLICK TO TWEET

But, what does it all mean?

COVID LIFESTYLE CHANGES

We observed increased threat levels in verticals that saw increased traffic from “Work From Home” lifestyle adjustments (Education, Home).

DEMAND DRIVES THREAT

Verticals that likely saw a drop in advertising spend level from brand advertisers (Travel, Sports, Auto), and thus driving lower CPMs, maintained higher threat levels.

SAVED BY PRICE FLOORS

News Sites, which often have increased price floors and stricter category blocks, were 20x less likely to see Malvertising than Auto and Education Sites.

“COVID has changed the way the world, and malvertisers themselves, operate.

Matt Gillis,
CEO

COVID-19 has changed the way the world operates. In the last few months many jobs have shifted to work-from-home, education has moved online, global sports and entertainment have paused, and travel has massively decelerated.

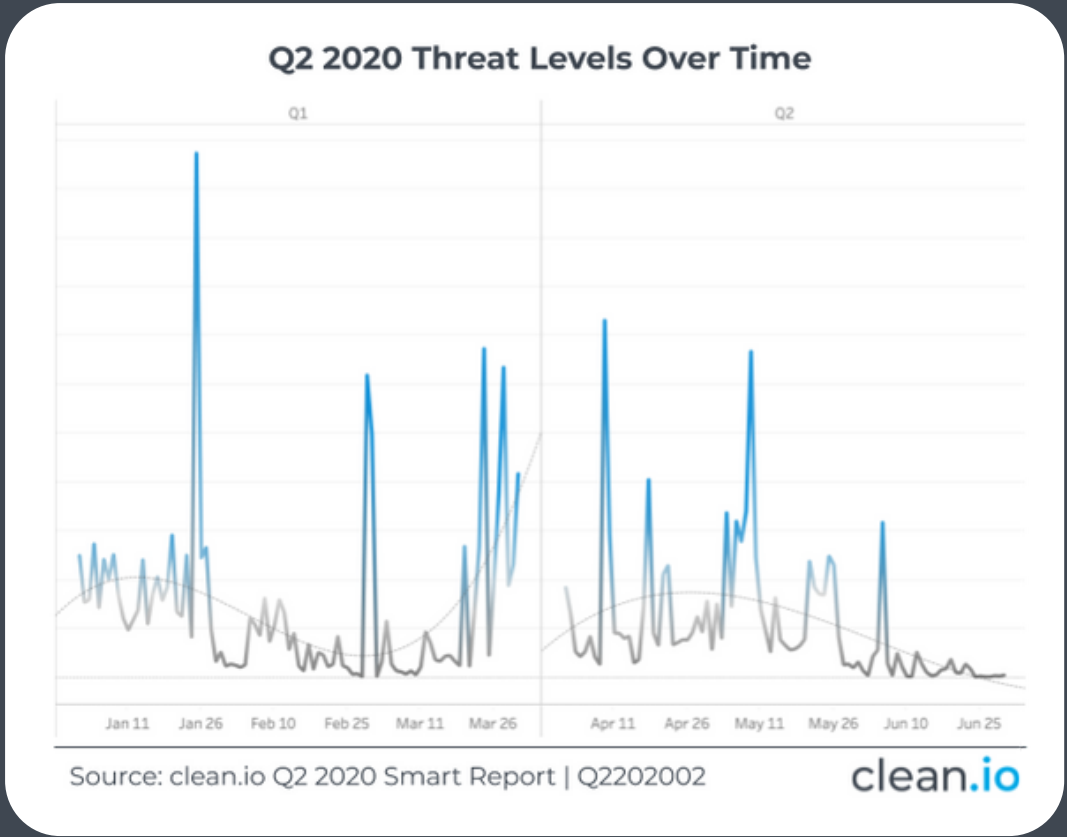
This activity is reflected in malvertising as well; Automotive, Travel, Education, and Sports were the most commonly attacked site verticals in Q2.

As the world continues to adjust to life in a pandemic (the return of sports, a new school year in the upcoming quarter) we expect to see elevated threat levels in the most impacted industries.

Q2 ATTACK TRENDS

ATTACK TRENDS MIRRORED COVID-RELATED DEMAND SHIFTS.

Threat level increased as demand levels reduced, and threats reduced as demand recovered with COVID-19 and quarantine shifts.



CLICK TO TWEET

The only thing that is predictable about the behavior of bad actors is that they are unpredictable.

Kathy Knott,
VP Client Success

While malvertising attacks are predictable around certain holidays, threat levels are otherwise erratic. Add a pandemic to the mix, and the volatility in attacks has been even more severe. Staying vigilant and protected is more important now than ever before.

Q2 began in the midst of a growing pandemic which created a vacuum of brand demand and allowed bad actors to infiltrate the ecosystem. Acclimation to life in a pandemic, alongside natural growth in demand towards the end of the quarter, yielded declines in threat level.

Q2 THREATS BY GEOGRAPHY

TOP COUNTRIES BY THREAT LEVEL CLOSELY MATCHED THE MOST HEAVILY AFFECTED COUNTRIES BY THE PANDEMIC.

CLICK TO TWEET

Malvertisers will take advantage of any and all environmental changes that present an opportunity.

Geoffrey Stupay,
Co-Founder

The Americas and Europe are the top two regions impacted by COVID-19 thus far; conversely it follows that they are the two regions most impacted by malvertising in Q2. The US, Canada, and 8 European nations make up the Top 10 countries by threats in Q2.

Just as the pandemic has inflicted pain on specific countries at different times and with different volumes of cases, malicious code exhibited the same pattern.

Within our Top 10 countries for Q2, we saw Peak Threat Levels occur at different times and at varying maxima.

KEY TAKEAWAYS

Shifts in demand are key.

What is happening in the world has significant effects on supply prices, thus creating an opportunity for bad actors to access more inventory, more cost effectively, thus driving threat levels up.

Attacks are well coordinated.

Bad actors very quickly shift approaches and conduct attacks that are well coordinated by date and location to make their attacks easier to execute and more effective.

SSP & DSP ATTACK TRENDS

HOW ARE ATTACKERS USING PLATFORMS TO ORCHESTRATE THEIR ATTACKS?

Q2 data shows how bad actors take full advantage of the way the programmatic advertising ecosystem is built and how ad creative flows through that system.

clean.io

DATA FROM Q2 SHOWS THAT

90% OF TOTAL THREATS

ORIGINATED FROM

9 SSPs

clean.io

CLICK TO TWEET

FLOW OF THREATS

DSP

Attacker submits ad creative to a DSP.

A single DSP allows access to many SSPs.

SSP

SSP enables bids from countless DSPs on ads across their entire network of sites.

A single SSP allows access to many sites.

Ad Views

Ad impressions are seen by users.

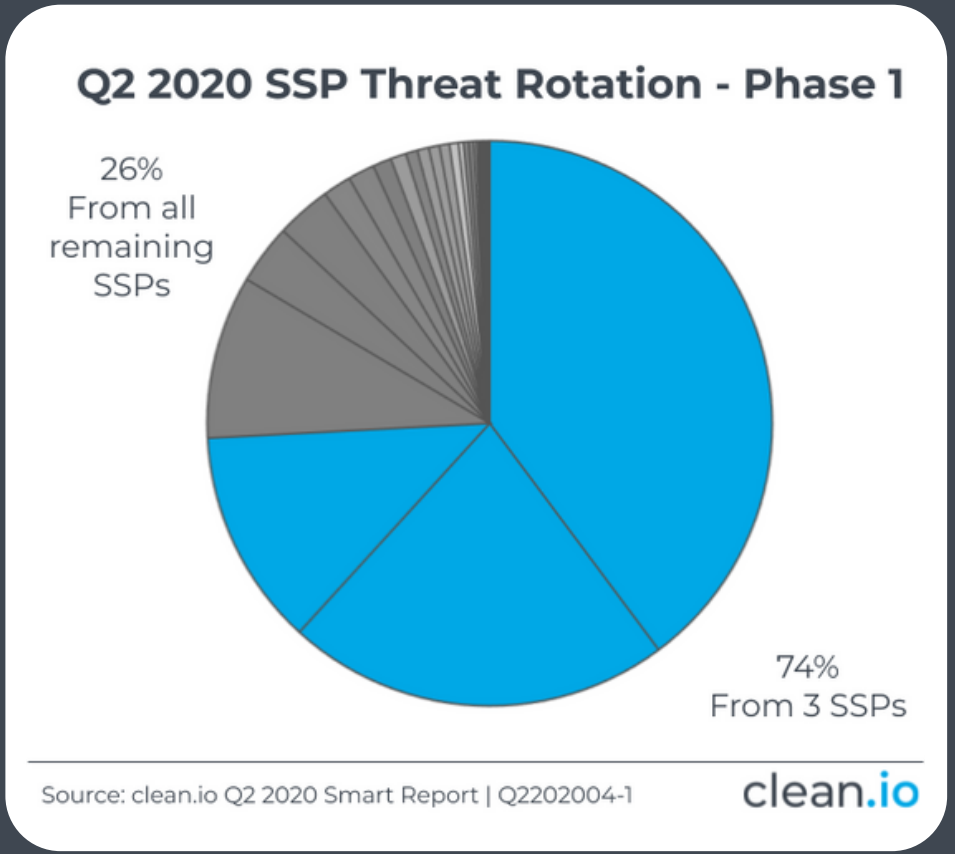
Through a single DSP, attackers can create a massive impact.

Q2 SSP THREAT ROTATION

BAD ACTORS ROTATED THROUGH 3 MAJOR CYCLES OF SSP ATTACKS IN Q2.

PHASE 1

The first 6 weeks showed attacks were primarily focused on just 3 SSPs, accounting for 74% of attacks in phase 1.

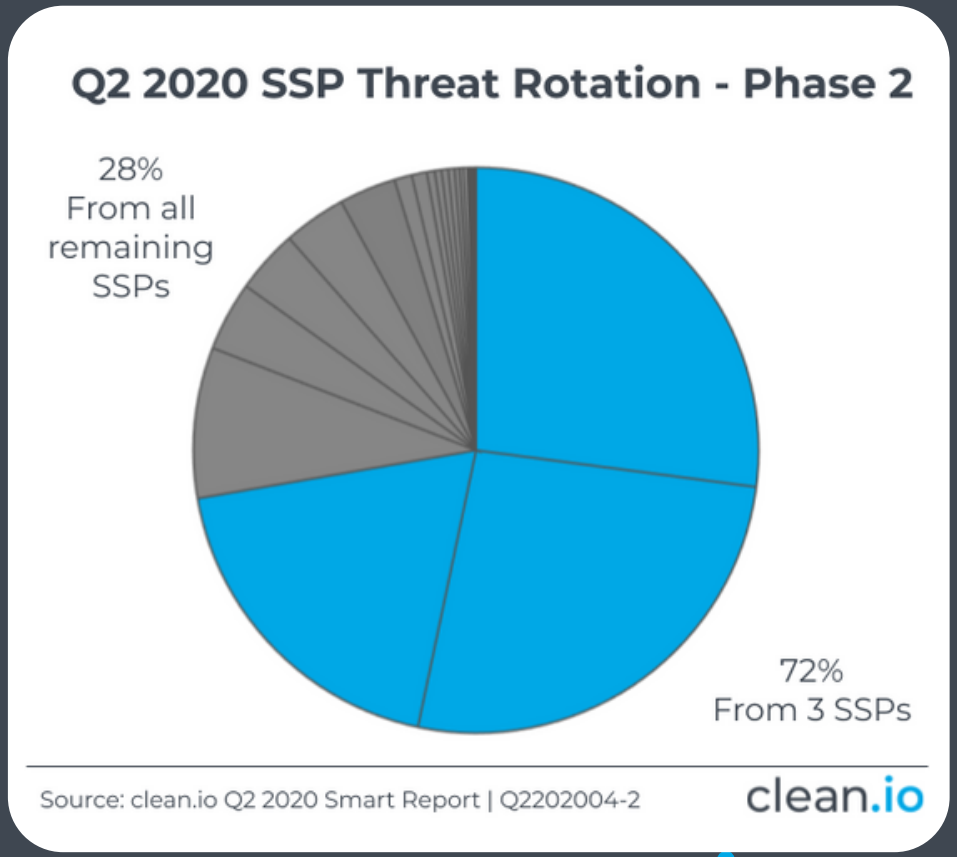


clean.io

CLICK TO TWEET

Q2 SSP THREAT ROTATION

BAD ACTORS ROTATED THROUGH 3 MAJOR CYCLES OF SSP ATTACKS IN Q2.



PHASE 2

The following four weeks showed a rotation of attacks on 3 new SSPs, accounting for 72% of attacks in phase 2.

clean.io

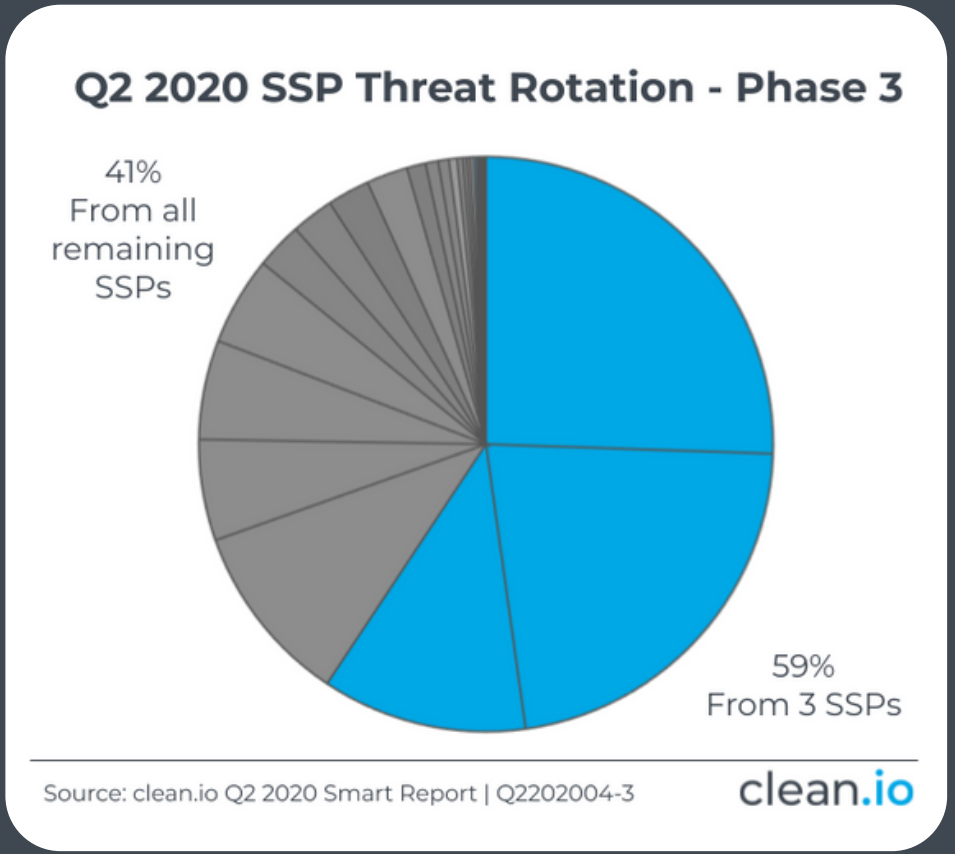
CLICK TO TWEET

Q2 SSP THREAT ROTATION

BAD ACTORS ROTATED THROUGH 3 MAJOR CYCLES OF SSP ATTACKS IN Q2.

PHASE 3

Finally, the last 3 weeks rotated further to attacks primarily focused on 3 new SSPs, accounting for 59% of attacks in phase 3.



CLICK TO TWEET

Malvertisers constantly run novel small probing campaigns prior to widespread attacks.

Jason Dobrzykowski,
Director, Platform &
Channel Partnerships

Bad actors are using multiple SSPs as entry points to launch their infectious code onto devices.

The clean.io Network sees attacks focus on a small number of SSPs at once, first through small probing campaigns before scaling to widespread attacks.

This cycles through several groups of SSPs throughout the quarter, and the landscape is always shifting. In general, malvertisers are going full throttle on a few SSPs while already testing on their next batch of platforms to constantly evade being caught.

KEY TAKEAWAYS

Attack rotations.

Bad actors systematically rotate attacks across multiple SSPs and DSPs to find vulnerabilities that will drive them the greatest gain.

Exponential impact.

While we saw 90% of the threats coming from 9 SSPs in Q2, we also prevented threats coming from over 63 unique SSPs total, indicating that there is a long tail of SSP probing that occurs.

BROWSER & DEVICE TRENDS

HOW ARE BAD ACTORS SELECTIVELY ATTACKING SPECIFIC TECH?

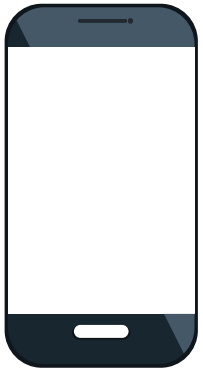
Always on the lookout for vulnerabilities, Q2 data shows how attackers rotate their attack attempts across different browsers, devices and operating systems.

Major Themes

Browsers

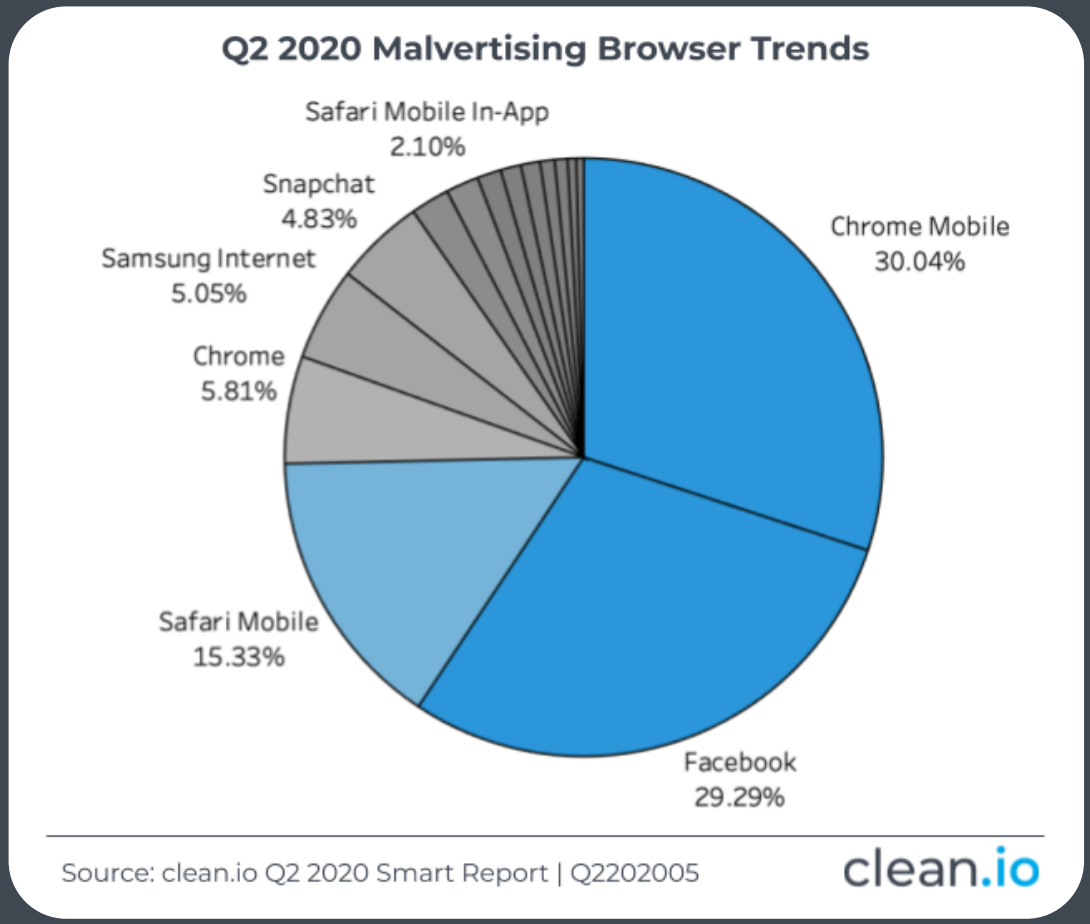
Facebook and Chrome Mobile lead the way as the most impacted browsers.

Devices



Mobile continues to be the most attacked in the ecosystem.

Q2 BROWSER TRENDS



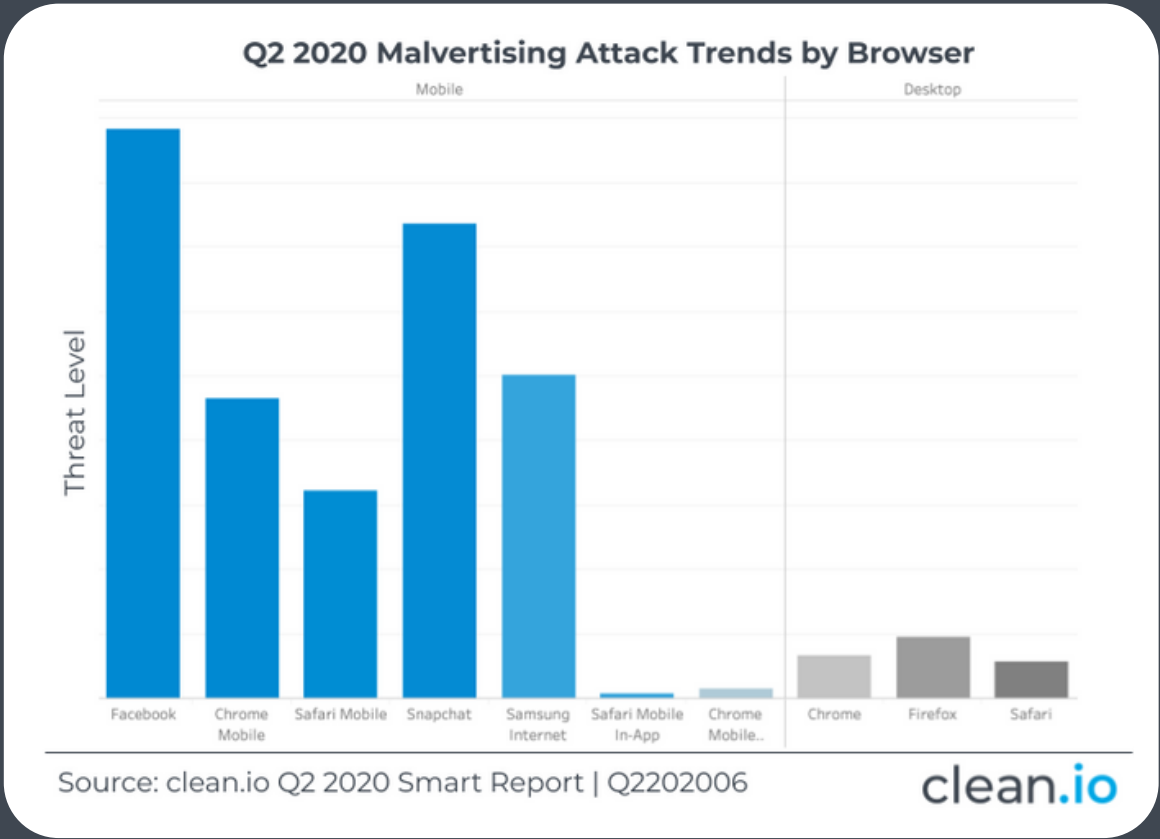
Facebook's embedded browser and Chrome Mobile continue to be the most attacked in the ecosystem.

CLICK TO TWEET

Q2 DEVICE TRENDS

7 OF THE TOP 10 ATTACKED BROWSERS ARE MOBILE

Mobile browsers overwhelmingly hold the lead in threat levels.

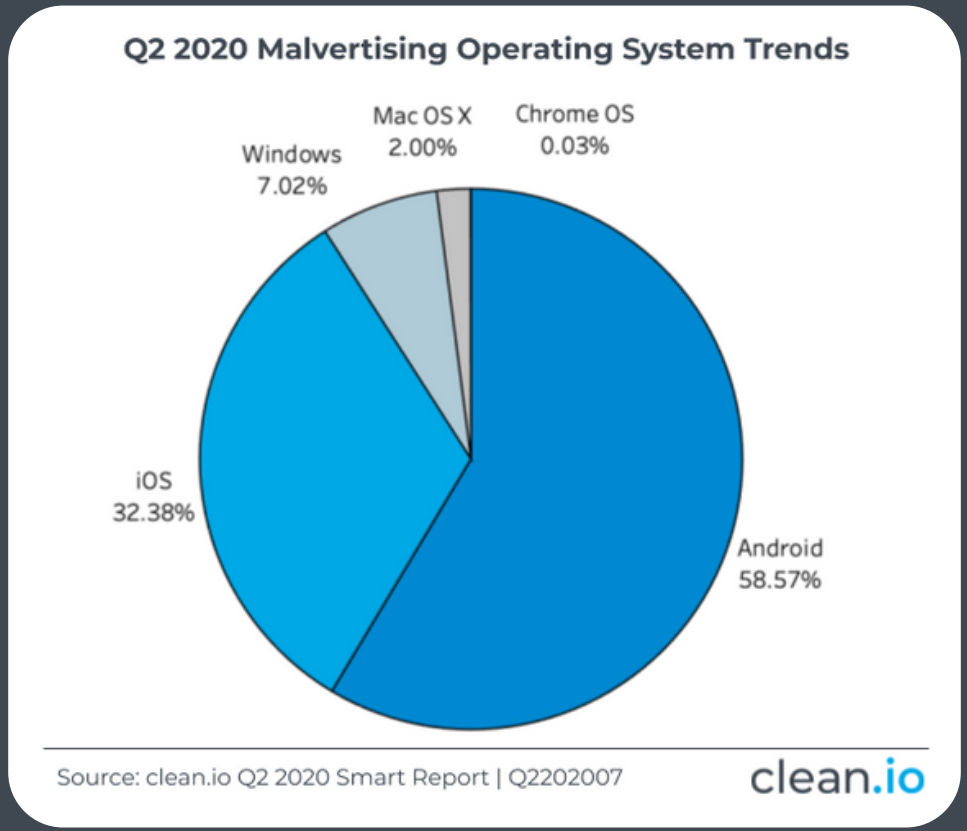


CLICK TO TWEET

Q2 OPERATING SYSTEM TRENDS

BAD ACTORS FOCUSED ON ANDROID DEVICES AS THEIR PRIMARY OS.

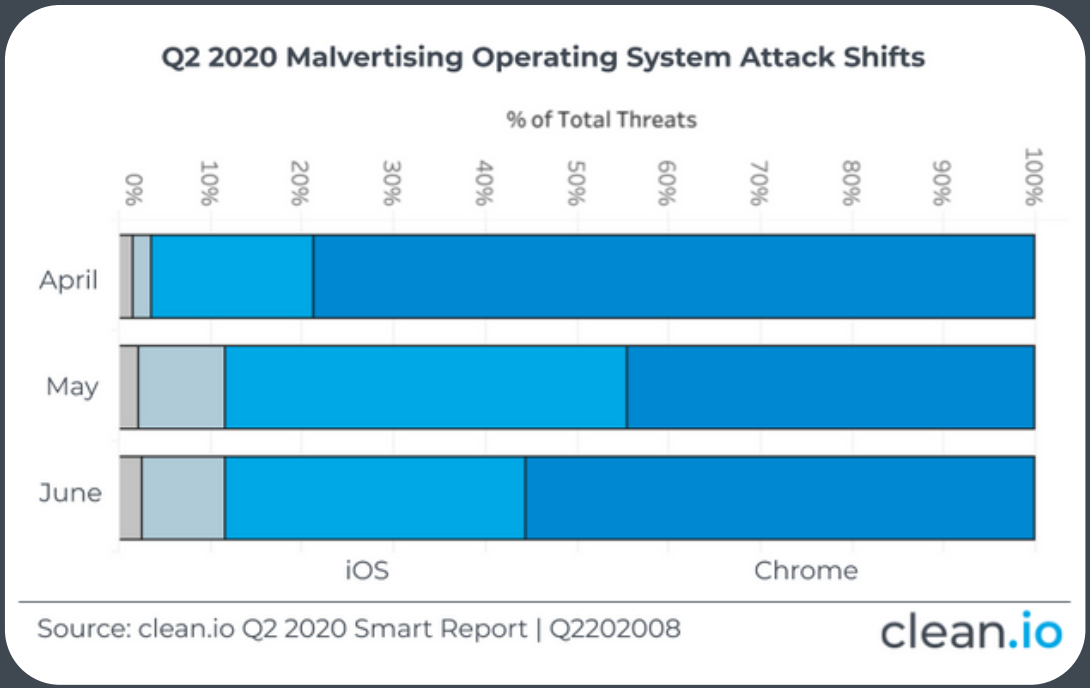
Android OS accounted for a total 58.57% of attacks across the quarter.



CLICK TO TWEET

Q2 OPERATING SYSTEM ATTACK SHIFTS

BAD ACTORS ROTATED EFFORTS BETWEEN CHROME AND IOS.



CLICK TO TWEET

Mobile allows access to ads at lower price points, making it easier for malvertisers to turn a profit.

Alexey Stoletny,
CTO

Mobile Browsers - specifically Chrome Mobile and Facebook embedded browser - are the most attacked Browsers in Q2.

While we see attacks across all devices, many attacks are consistently focused on mobile devices.

It follows that Android accounted for 58.57% of all threats in Q2; as it is generally less expensive than iOS inventory, and more popular globally, it allows bad actors access at lower price points to turn a profit at the expense of users.

KEY TAKEAWAYS

Protecting mobile is key.

Bad actors continue to focus more heavily on mobile in their attacks, so protecting user experience on mobile devices will be an important initiative.

Focus on embedded browsers.

Embedded browsers, particularly Facebook, continue to hold the highest threat vector. Finding ways to preserve user experience in embedded browsers is of utmost importance.

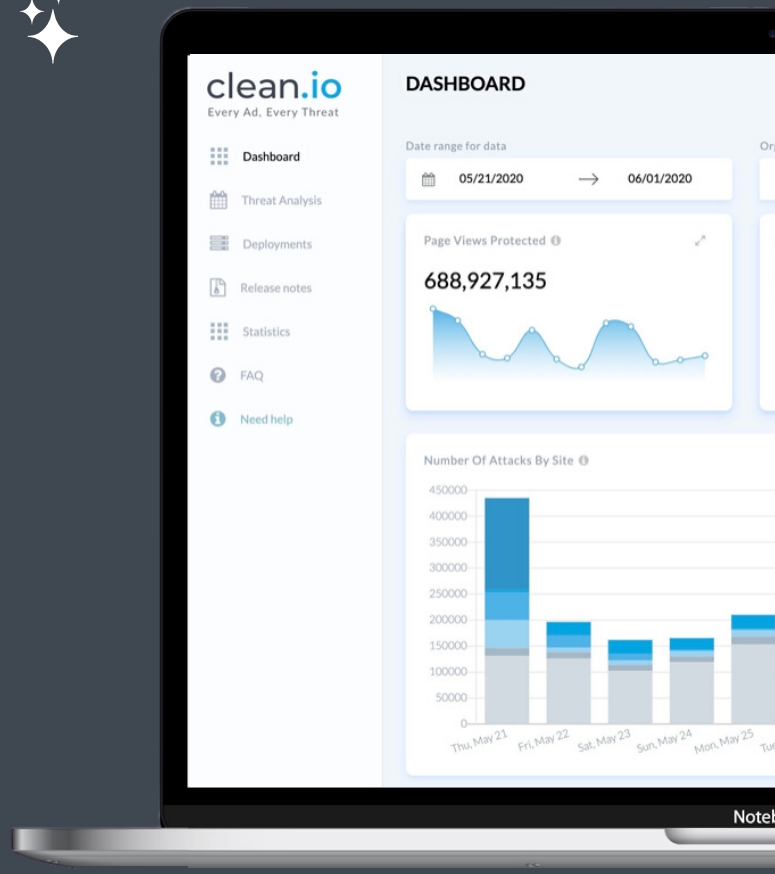
GET TO KNOW US

MORE ABOUT clean.io

ABOUT CLEAN.IO

clean.io is the most effective solution to prevent malvertising, as well as protect revenue and user experiences across all platforms.

EFFECTIVE ● SMART ● SIMPLE



CASE STUDY

LEARN HOW PUB+ ALLEVIATED MALICIOUS REDIRECTS THAT WERE CAUSING BUSINESS DISRUPTIONS AND EATING INTO REVENUE.

"The clean.io solution worked exactly as described. Simple, effective, and smart. Following implementation we saw all key financial KPIs improve... and our end users were no longer complaining about bad user experiences."

Omry Aviry,
Chief Product Officer
at PubPlus

clean.io

READ THE CASE STUDY

Choosing clean.io was one of the best investments we ever made for overall user experience.

Vince Banks,
SVP of Revenue Operations,
101 Network

Choosing clean.io was one of the best investments we ever made for overall user experience.

We were regularly dealing with unhappy readers who were frustrated with redirects, but all of that disappeared once we began using clean.io.

Getting up and running was quick and easy, and maintenance is almost non-existant.

What's more, clean.io gives us the confidence to test new demand quickly and more efficiently, since we know we are well protected now.