AdSecure's Violations Report 2020

2020 will always be known as the COVID year, and even a pandemic doesn't stop cyber criminals using digital advertising as a form of exploitation. In our easy to digest bite sized Threat Intelligence Report for 2020 we look back at the ad security trends of last year.

1. Violations detected increased by 56.98% compared to 2019

Number of violations every 10,000 scans

1,542 more violations

Violations detected: AdWare, Malware, Scareware, Phishing, Auto Downloads, Auto Redirects, Unsafe Content, Malicious URL & Threat Intelligence

2. This is why you need a solution that can detect several threats in one digital ad flow

Cyber criminals can place threats inside the ad format creative and in the landing page the ad redirects to, then the bad actor also locks the user on the landing page whilst malware automatically downloads to the victim's device.

As you can see in the chart below 4.21% of scans detected at least 3 violations.

of analyses contained at least 1 violation
Down 3.06% on 2019

of analyses contained at least 2 violations
Up 4.76% on 2019

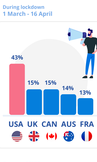
of analyses contained at least 3 violations
Up 3.1% on 2019

3. Covid Update

Malicious attacks grew exponentially alongside first lockdown and hit a peak of +116.14% on 28 March

We observed an increase in threats worldwide, particularly in the digital advertising ecosystems of prized "Tier 1" GEOs, with a huge spike during the week 22-29 March, with cyber criminals launching more attacks, before subsiding slightly early April 2020.

Malvertisers exploited well known logos



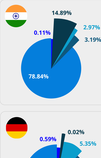
During first lockdown the terms "Coronavirus", "COVID-19", and WHO (Word Health Organisation) were constantly in the news. We discovered a mobile banner ad running in Italy, one of the countries worst hit by the pandemic. The ad delivers Malware via an auto-download, using the logo of the World Health Organisation (WHO) & GooglePlay logo to imply legitimacy.

We also discovered phishing attacks leveraging fake Walmart offers in the US, Intermarché in France, and Amazon in multiple countries.

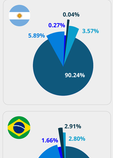
Read our COVID lockdown report

Top 5 GEOs targeted with violations

During lockdown
1 March - 16 April

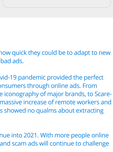


Post lockdown
17 April - 30 June



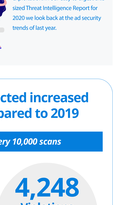
Summer COVID
1 July - 31 Aug

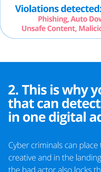
Autumn/Winter COVID
1 Sept - 31 Dec

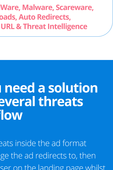


4. Malvertisers weapons of choice targeting the top 5 GEOs with the most violations in 2020:

Scareware	48.84%
Browser locker	43.63%
Phishing URL	4.1%
Malware	3.26%
Adware	0.53%







Conclusion:

Throughout 2020, malvertisers showed how quick they could be to adapt to new situations in order to extract profit from bad ads.

There is opportunity in crisis, and the Covid-19 pandemic provided the perfect cover with which to manipulate digital consumers through online ads. From social engineering scams that play off the iconography of major brands, to Scareware attacks that took advantage of the massive increase of remote workers and the very fear of the virus itself, bad actors showed no qualms about extracting profit from misery.

These types of behaviour will likely continue into 2021. With more people online than ever before, malicious, misleading, and scam ads will continue to challenge the digital advertising industry.

In order to stop these ads from harming end users, dissolving consumer trust, and weakening the overall ecosystem, digital platforms and publishers need the resolve to tackle the problem head on, and the right tools to eliminate them.

Protect your business from threats: contact@adsecure.com