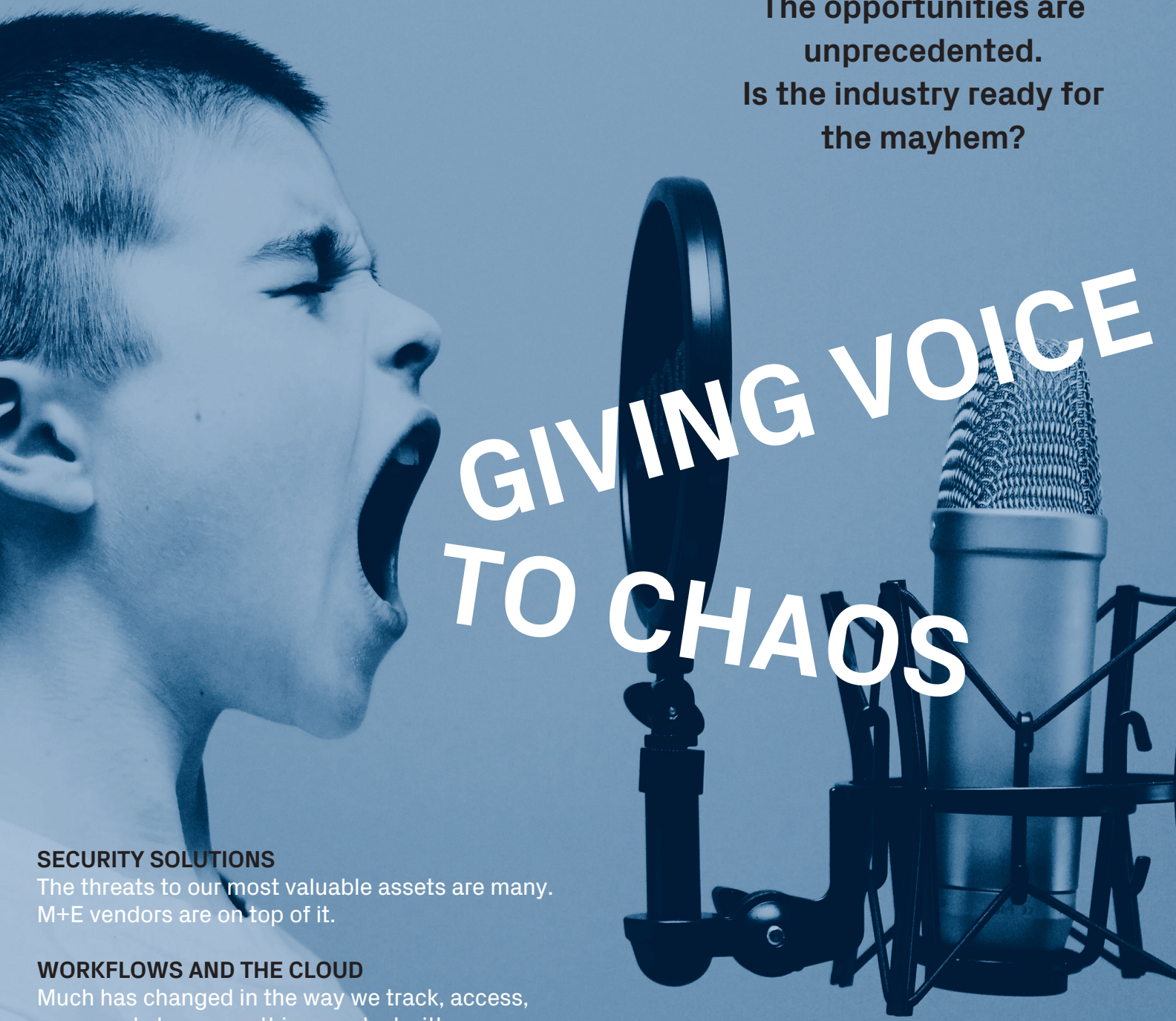
M+E JOURNAL

Today's localization challenges are enormous. The opportunities are unprecedented. Is the industry ready for the mayhem?



GIVING VOICE TO CHAOS

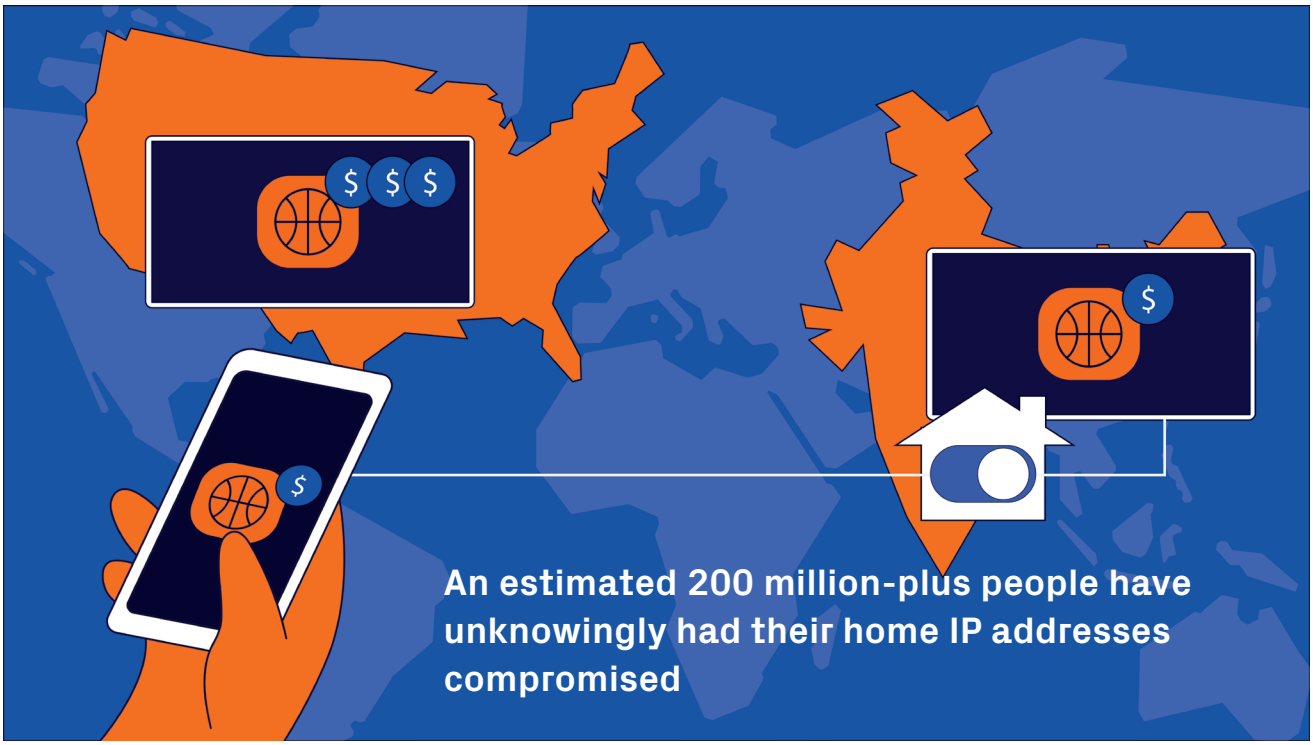
SECURITY SOLUTIONS
The threats to our most valuable assets are many. M+E vendors are on top of it.

WORKFLOWS AND THE CLOUD
Much has changed in the way we track, access, move and store everything we deal with.

SMART CONTENT
The many ways the industry adopts new technologies to make content smarter.

22.02

HIJACKED RESIDENTIAL IP ADDRESSES: A RISING THREAT TO CONTENT EXCLUSIVITY



ABSTRACT: Pirate viewers use virtual private networks (VPNs) and proxies to access territorially restricted content. However, VPN providers keep unearthing sophisticated geo-piracy methods, such as selling hijacked residential IP addresses to rogue users. The technology required to pinpoint genuine subscribers helps streaming providers uphold territorial licensing and protect revenue.

By James Clark, General Manager, Media, Entertainment, GeoComply

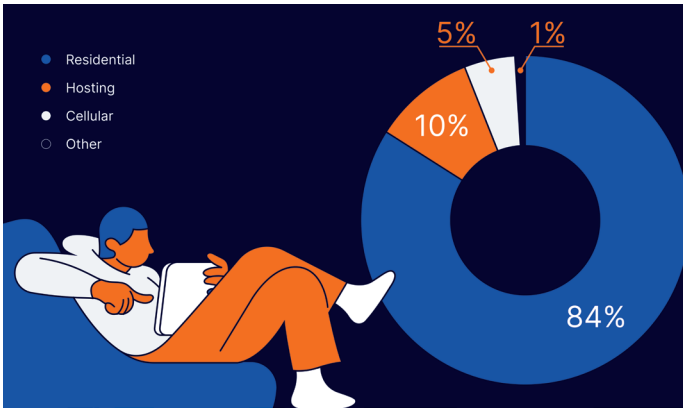
Today's viewers have an endless array of content at their fingertips. Unfortunately, many users circumvent VPN blocking controls to access territorially restricted content for free or at a lower price. For example, people in the U.S. who want to subscribe to the NBA's League Pass pay $199.99 each year, while in India it costs 1,500 rupees, or a mere $19.

In their quest for free or cheaper content, pirate viewers are getting more sophisticated. Their latest trick? Hijacked residential IP addresses.

THE 200-MILLION-PERSON PROBLEM

We estimate that more than 200 million people have unknowingly had their home IP addresses compromised. A residential IP address is hijacked during a cyberattack or is harvested when users sign up for a free VPN or DNS proxy service without reading the terms and conditions.

This oversight allows the VPN provider to sublease and sell the IP address to an unknown person or entity. This stranger may use it for criminal purposes, like fraud, scams,



A Kingsmead Security study found that 84 percent of IP addresses aimed at two specific OTT vendors came from residential IP addresses.

or hacking – or for geo-piracy. By hiding behind a legitimate domestic IP address, viewers can bypass VPN restrictions because streaming providers can't take the risk of blocking genuine users.

Yet the failure to stop this form of geo-piracy puts streaming services at risk for non-compliance with rights holders' agreements for content exclusivity. It also erodes service revenue if the content is easily available from alternate countries with lower licensing costs.

A HIGH-TECH GAME OF HIDE-AND-SEEK

Pirate viewers who lurk behind residential IPs have a partner in mischief: the premium VPN vendors who provide those IPs. These vendors are just as eager to evade detection as the pirate viewers themselves and are constantly finding new ways to do so.

One way in which VPN vendors attempt to thwart detection is by targeting "high-value" OTT services with service-specific proxy servers. This means only the targeted OTT service can determine the IP address of the proxy server. All other OTT services — and VPN detection vendors — can only detect IP traffic from the VPN server.

Re-routing specific OTT services through proxy servers is a widespread practice. A simple web search for "best VPN for streaming" gives insight into which vendors might be targeting a specific service.

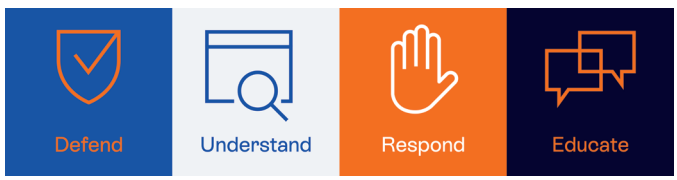
In a new white paper, "Residential IPs: A Rising Threat to Content Exclusivity,"

Content security consultancy Kingsmead Security analyzes these sophisticated techniques in-depth. The analysis found that 84 percent of the VPN IP addresses targeted at two OTT services were residential IPs.

Kingsmead notes its findings show that "leveraging residential homes is now widespread amongst VPN vendors, and hundreds of thousands of homes are now being actively used to route VPN traffic. This is an increasing threat to OTT services, who must be aware of the issue and take appropriate action."

FOUR WAYS TO COMBAT THE RESIDENTIAL IP THREAT

The use of residential IP addresses to bypass VPN detection may seem like a can't-win situation. Detecting their use is difficult since they may be indistinguishable from genuine user traffic. And any attempts to block residential IPs runs the risk of excluding legitimate users, who may not even realize they're hosting a proxy.



The strategies for tackling use of residential IP addresses to bypass VPN detection.

So, what can you do if you suspect residential IP addresses are being used to access your streaming service? The answer: quite a lot. No method of location masking — even hiding behind residential IP addresses — is 100 percent foolproof.

Defend. Make it difficult for a VPN vendor to target your streaming service with residential proxies. The Kingsmead paper describes several useful methods for doing so.

Understand. Gather information that is useful for

James Clark leads GeoComply's media and entertainment division, helping organizations use location to secure their services, reduce fraud, and protect their users. He has been involved with the ever-evolving challenge of secure media delivery throughout his career in the digital entertainment sector. James combines a technical understanding of security technologies with extensive experience working closely with businesses to fight piracy and fraud.
james@geocomply.com @GeoComply

detecting VPN activity, such as regularly reviewing the VPN market for vendors claiming to avoid detection by using your service. Internet searches for "Top VPNs for Streaming" or "Best VPN for Your Service" will give insight into those vendors targeting you.

Respond. By increasing the blocking rates on your service with a reputable VPN and proxy detection solution. If you do block a connection, provide the users with clear messaging and a way to report issues — mistakes do happen.

Educate. Teach consumers the risks associated with hijacked residential IPs. Most consumers will not even be aware of unwanted VPN or proxy traffic being routed through their home IP address.

We help rights owners around the world protect against VPN abuse. As part of this, we have investigated the digital risks of so-called "free" VPNs to consumers. The demand for these free services has been rising and therefore the pool of available residential IP addresses for sale will also grow.

We can — and should — apply the best technical strategies to thwarting geo-piracy threats. However, it's an obvious plus if we can get a customer to think about the personal privacy and security risks associated with using a free VPN. After all, one less customer who uses a "free" VPN is one less residential IP address for sale. And that's a big win for us all. ⊞