Hacker's Mindset

Vidio: Deliver uninterrupted streaming across any device

Vidio is one of Indonesia's largest video streaming platforms, with more than 60 million monthly active users.

The platform has seen more than 150% growth, and the Vidio app has been downloaded more than 5 million times.

During the Tokyo Olympics, the app reached the number one spot on Apple's App Store in Indonesia across all categories.

When Indonesia reached the finals of the Southeast Asian Football Federation (AFF) Suzuki Cup championship, demand at the height of the tournament topped 3.5 terabytes of data per second, with a peak of 1.77 million fans tuning in.

Vidio stays ahead of the online over-the-top streaming competition in Indonesia by delivering high-quality, uninterrupted programming to millions of viewers all over the country, including a fast-growing audience of sports fans, especially football fans.

To deliver a smooth, sharp picture – even during periods of high demand – Vidio uses Akamai's content delivery network (CDN) to store online video and deliver it to multiple devices and formats, from smartphones to smart TVs.

> *Smooth playback is everything, whether you're sitting in front of an ultra-high-definition smart TV or holding a smartphone*
>
> *– Tommy Sullivan, CTO, Vidio*

Akamai's CDN presence in Indonesia also means that the majority of Vidio programming is streamed within the country. Not relying on external networks (which bounce content around an international network before returning to Indonesian viewers) reduces exposure to software and infrastructure issues, such as damage to cables, and helps ensure a better experience for viewers.

"Fans are not shy about sharing a bad experience on social media, which could seriously damage our reputation. That's why Akamai is central to the quality of our video streams, which in turn helps us to stand out from the competition," says Tommy Sullivan, CTO at Vidio.

Deliver consistent, high-quality online video securely at a massive scale:

Adaptive Media Delivery

click to read

Learn how Vidio grew viewership by more than 150% with high-definition viewing powered by Akamai:

Uninterrupted: A Perfect Streaming Service for Sports Fans

click to read

Has piracy turned the corner in ASEAN?

As the broadcast/OTT industries transform into increasingly digital-first organizations, piracy has become a significant information security concern. Every year, cybercriminals cost the media and entertainment industry billions in lost revenue due to piracy.

Piracy is a complex topic to cover, because there are so many elements involved. Considerations include economic factors (both from the criminal's viewpoint and the legitimate business world), technological factors, and the scale of piracy itself.

Dealing with piracy is a security concern – one that business leaders are taking very seriously within their organizations. On the flip side, piracy is a moneymaker for criminals who pirate live events, streaming media, software, publications, and other digital services.

On a base level, the impact is both reputational and financial.

Reputations are affected as the pirated streams can suffer performance issues, which anger paying customers. The financial impact is straightforward, as those pirating live events typically don't pay the producer or event organizers for their access.

Piracy techniques and processes

Pirates will leverage a number of attacks and techniques. Here are just some of the more common ones:

Link sharing and token harvesting

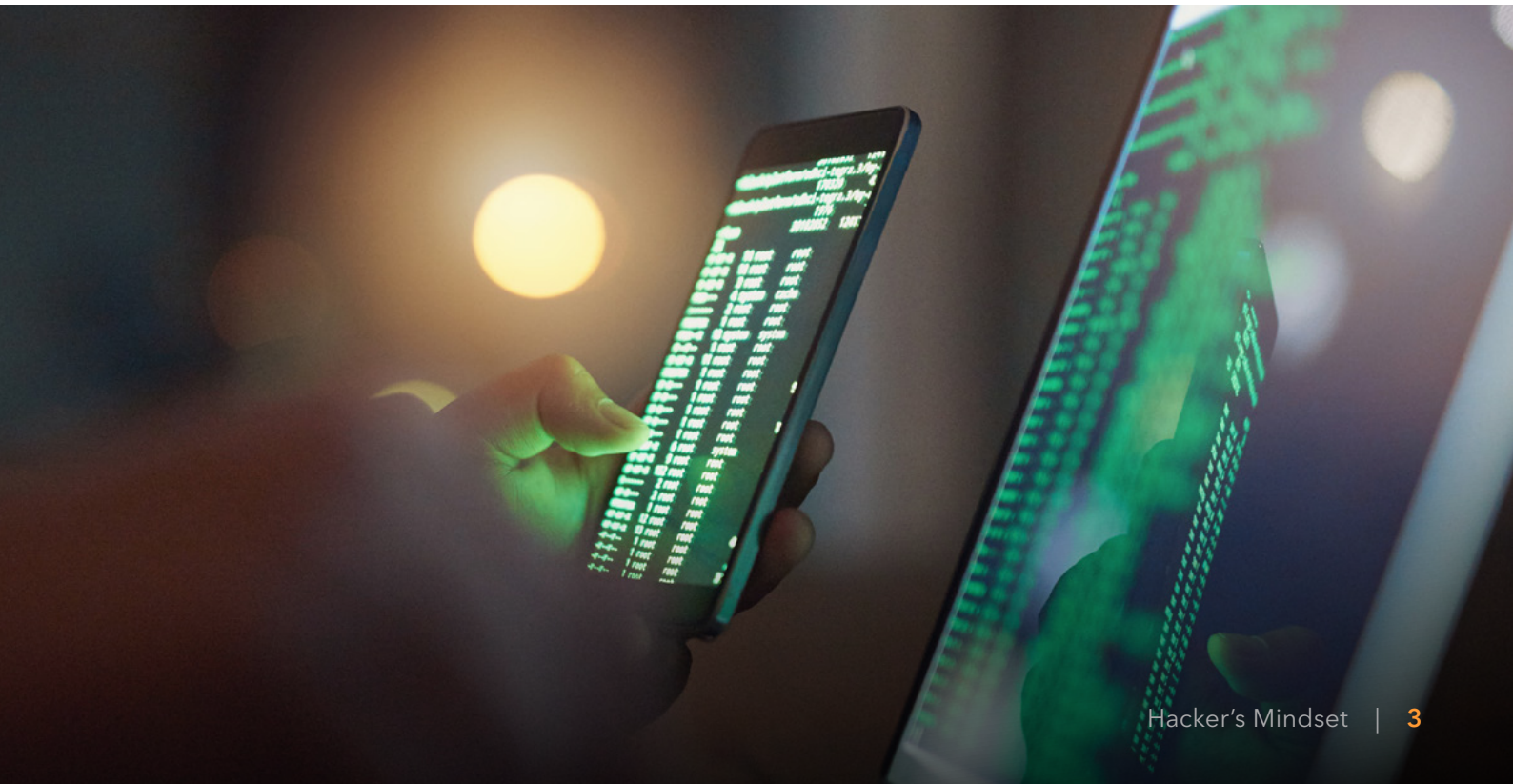
Mobile and desktop applications will monetize pirated events with their own ads, and access them via compromised or recycled access tokens.

Stream ripping and re-streaming

Pirates will stream events via public social channels such as Twitch, YouTube, and Facebook.

VPN/proxy

Pirates and users will bypass geo-restrictions to access content.



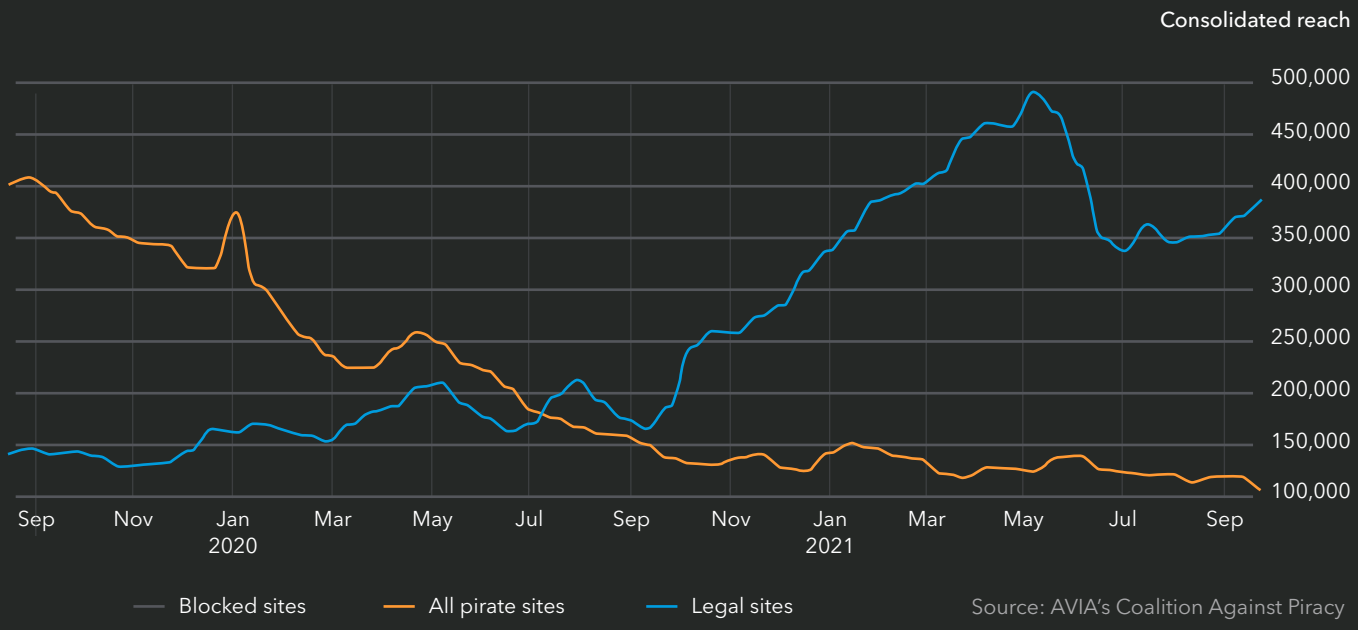
The knock-on effect of piracy impacts the lives of those who work in the background, who are often forgotten by pirates who focus their ire on athletes, actors, and musicians as a justification for their actions.

The Asia Video Industry Association (AVIA) has been an active industry coalition to combat piracy by introducing site blocking protocols. According to AVIA, its Coalition Against Piracy (CAP) has been able to block more than 60 sites every two weeks in Indonesia.

When sites are blocked, there is increased friction to accessing pirated content. The good news is that making it difficult for consumers to access pirated content has led to a shift toward consuming legitimate content, based on a separate survey by YouGov.

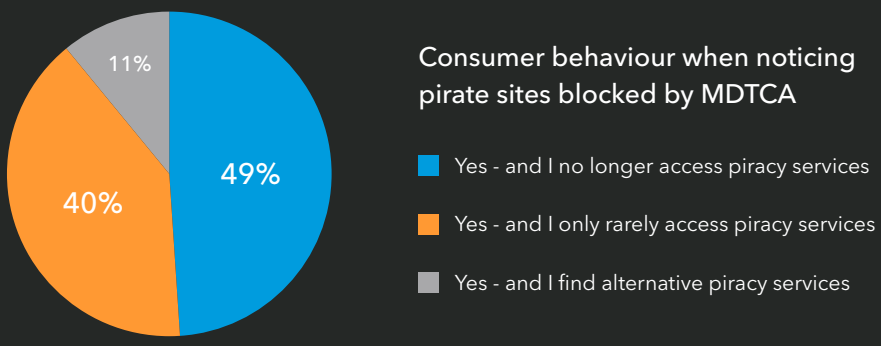
During a live event in 2020, Akamai was able to lower piracy levels for one partner from 40% at the start to 15% by the end of the event. The pirates reacted badly to their efforts being blocked. The event received 5.5 billion hits that triggered DDoS protections and 38 million requests that triggered application-layer protections, which were 100% blocked.

Site popularity by type over time



Source: AVIA's Coalition Against Piracy

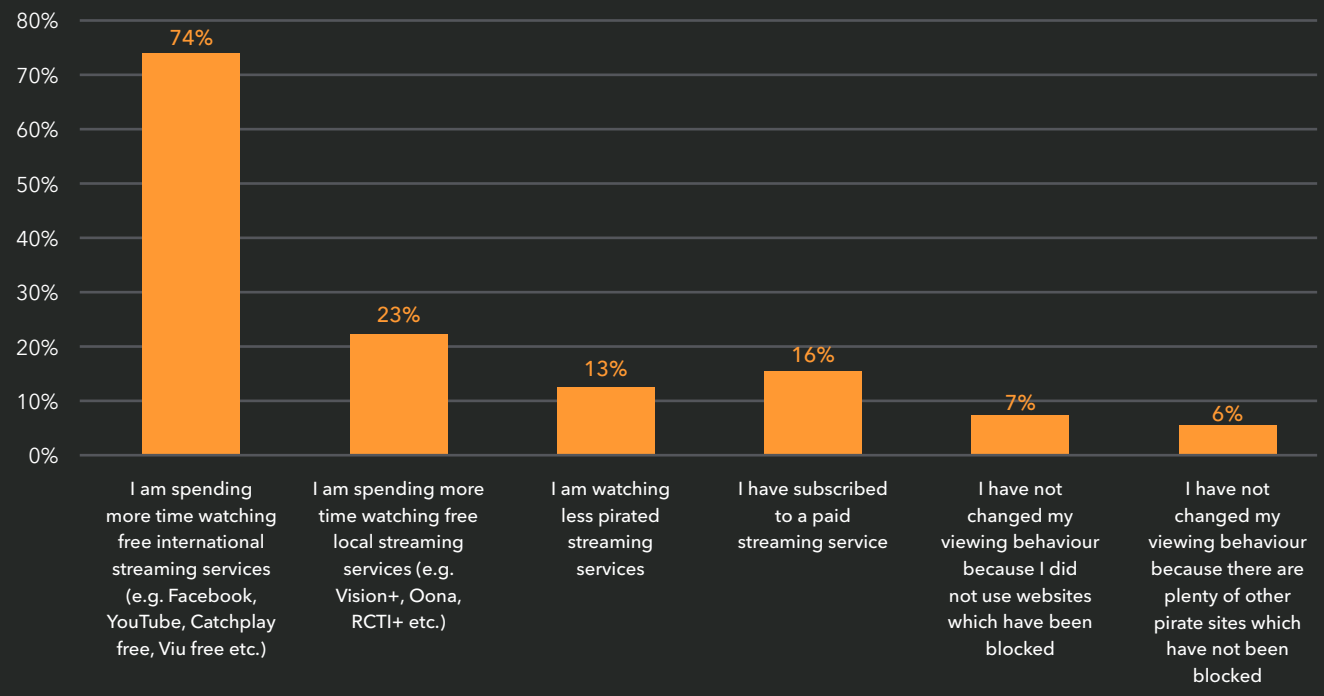
Malaysian viewers move away from piracy



Source: YouGov

Indonesian viewers are switching to legitimate streaming services

Because of piracy streaming services being blocked by the goverment, have you changed your viewing habits at all?



Source: YouGov

Piracy is a full-time job for those who organize and manage piracy services, and defending against it is also a full-time task.

Criminals will do whatever it takes to maintain their access to pirated content, because their customers demand it, and it generates a healthy income.

Defenders on the other hand are sometimes in the dark, as they lack visibility and context when it comes to their digital assets, as well as information about who or what is accessing them. This makes curbing piracy a difficult process, and it is why the topic is one of the biggest concerns among broadcasters and streaming services.

One of the things broadcasters and streaming services can do to defend themselves is address workflow issues and API-based problems, as criminals are constantly looking to exploit these areas. In addition, producers also need to remember that criminals won't just leverage a single method of piracy, and so defenses need to account for several attack types at once.

Piracy isn't a simple problem – it takes layers of protection to deal with, and with the right partner and the right visibility, an organization can put those defenses in place, and get ahold of the situation.

All DDoS mitigation is not created equal

The size of DDoS attacks has been doubling every two years, and the complexity – the number and combination of attack vectors – is unprecedented.

A DDoS attack in one game can not only affect other games, but they can also even disrupt entire platforms and ecosystems.

For example, when a DDoS attack is launched against a major multiplayer game and knocks it offline, players will keep trying to log in – overwhelming the authentication servers and causing an outage that shuts down all the servers on the platform.

While media and gaming organizations strive to maintain close to 100% application and network availability, hackers are incentivized to launch volumetric, protocol, and application-layer DDoS attacks to disrupt any potential point of failure – making internet-facing resources and assets unavailable to end users.

By conducting reconnaissance of victim environments, applications, and IP spaces, attackers can determine which DDoS vectors will inflict the most damage. There is no shortage of attack techniques and tools to help discover weaknesses or vulnerabilities in enterprise defenses.

The repercussions of a DDoS attack will only intensify as organizations continue to scale and protect remote access capabilities with a distributed workforce. According to Ponemon Institute, the average annual cost of a DDoS attack to an organization is $1.7 million, driven by increased technical support, consumption of incident response resources, internal escalations, legal costs, operational disruption, and loss of employee productivity.

As organizations decommission traditional data centers and move applications to cloud-hosted environments, security architectures become more complex.

Many organizations struggle with how to keep internet-facing assets protected with the same level of DDoS defenses as those located within the data center. Adding to the complexity, many cloud-hosted IPs fall outside of an enterprise's direct control, leaving them vulnerable to a successful DDoS attack if not properly protected.

Threat actors are aware of this accelerated migration to colocation facilities and the public cloud. They are eager to exploit weaknesses in an organization's security architecture and posture created by inconsistent security policies and requirements, as well as difficulties troubleshooting across disparate and fragmented cloud-hosted infrastructure.

One way to stay protected is best-in-class cloud security. Modern enterprises need adaptive defenses to keep a variety of web-facing assets and services protected, regardless of where they are located. And with more than 93% of enterprises (<1,000 employees) employing a multicloud strategy, the time to close defensive gaps driven by infrastructure complexity is now.

DDoS attackers will target any potential point of failure, such as:

- Websites
- Web applications and other enterprise services
- VPN concentrators for remote access to corporate resources
- SD-WAN controllers
- Application Programming Interfaces (API)
- Domain Name System (DNS) and origin servers
- Data center and network infrastructure

Akamai has the world's largest mature global DDoS mitigation clouds.

Whether you're protecting individual applications, entire data centers, or authoritative DNS, Akamai has architected DDoS mitigation with the highest capacity, utmost resiliency, and fastest mitigation in mind.

We have mitigated some of the largest DDoS attacks launched in the world:

DDoS Protection

click to read

If you would like to understand more about Akamai and the solutions we offer, please do

Contact Us