Volume 8, Issue 1
[State of the Internet]

# Pirates in the Outfield

# Table of Contents



# TL;DR

During an 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 live event received 5.5 billion hits that triggered DDoS protection and 38 million requests that triggered application-layer protections, which were 100% blocked.

During an event in July 2021, the top 10 shared tokens (which enable some pirates to re-stream or access events) were used more than 65,000 times. The number one shared token was seen more than 19,000 times alone.

In addition to our own visibility and data, we partnered with MUSO for this report. According to MUSO, between January and September 2021, the global piracy demand reached 3.7 billion. Based on the data, we can see that an overwhelming majority of consumers (61.5%) are directly accessing pirated materials, while 28.6% of them are searching for it. At just over 67 billion total visits, television is the top pirated industry among MUSO's data. This is followed by the publishing and film industries.

# Introduction

Welcome to the eighth volume of the State of the Internet / Security report, lovingly called the SOTI by those of us who work on it. In this first report of the year, we are going to focus on the media industry. However, unlike our other media-centric reports, this edition will focus on a topic we've only briefly covered in the past: 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.

Over the years, Akamai has studied piracy from a number of viewpoints, and assisted our customers in tackling this issue. Along the way, we've learned a few key lessons. The largest lesson? Piracy is no longer *just* a cost of doing business. It's a massive and growing business issue.

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

Akamai has a great deal of visibility into the piracy landscape. This is critical to our media partners, so we worked with them to develop something to help tackle that problem. This is where our Managed Content Protection (MCP) tools come from.

Everything related to MCP originated from a customer request. Years ago, a customer reached out after a rights owner for a sporting event told them they were failing to protect the streaming content. The customer asked Akamai for assistance, and thus the toolset we now know as MCP was born. There's more to that story, of course, but that is essentially where things started.

When it comes to content protection, Akamai's work in this space has revealed that many motivated threat actors leverage the illicit lure of pirated content — be that of a movie, game, book, or sporting event — as a passive delivery vehicle for a number of targeted attacks. Some of these attacks can include credential and information phishing, malware, and botnet aggregation. Moreover, some threat actors simply leverage piracy as a revenue stream, charging outsiders for access to digital content.

> ***"It quickly became evident that Akamai was uniquely positioned to provide a previously unattained capability to our media and broadcasting customers. We were able to give them proactive protection, detection, and mitigation of piracy in mere seconds, not days or weeks."***
>
> ***— Eric Elbaz, Lead Strategic Engagement Manager, Broadcast Media***

In addition to our own visibility and data, we partnered with MUSO for this report. MUSO, to put it succinctly, helps media and entertainment companies make better decisions. They give them better visibility, and the information needed to protect and increase the value of their digital content. Their data covers streaming piracy and download piracy across a number of industries, and overlaps nicely with Akamai's insights — as such, we felt it would be a highly useful addition to this report.

Throughout this report, we're going to examine the piracy landscape through two different lenses: our own by analyzing piracy in the sporting world, and MUSO's — a company that tracks television, movies, software, and publications.

# The piracy landscape

Video streaming, in particular, has been a boon to the entertainment industry. During the COVID-19 lockdowns in 2020, all of the major studios turned to streaming platforms to keep the industry moving. In the sports world, especially live sports, streaming makes it possible for fans to follow their favorite teams from the safety of their own homes. "Cutting the cord" and turning to one of the many streaming platforms has been a go-to option for millions of people. But as these services expand, the line between piracy and consumption is blurred. Perhaps it's closer to a complete perception shift.

For some people, since the content isn't physical, downloading a copy or re-streaming an event isn't perceived as theft. The original remains — or the broadcast still took place. Therefore, such actions harm no one, right? People with this mindset forget that events, or content, can take millions of dollars to produce, and the livelihoods of hundreds of people (who often earn median wages) are directly impacted by piracy.

In 2019, the U.S. Chamber of Commerce's Global Innovation Policy Center estimated that the rapid expansion of creative and technology industries led to the employment of up to 2.6 million workers in the United States alone, and provided $229 billion in economic benefits. However, piracy is responsible for at least $29 billion in lost revenue each year.

If production studios don't see the return on investment, they're less likely to work on developing new properties or projects. It isn't always about A-list actors — producers, athletes, and other people are impacted by piracy as well. In the end, those who work behind the scenes and the fans themselves ultimately suffer if new content isn't developed.

There are those who don't care about the people behind the scenes, and choose to focus on their own pockets. These are the pirates who are not content consumers, but opportunists who charge for their services and access. They re-stream live events and charge for access, or on-demand replays; or they maintain websites that mirror legitimate streaming services, charging their own fees for books, comics, music, television, and film. If there is no fee involved, then the content is typically provided in exchange for either a page full of advertisements, or registration, from which the visitor's information can later be sold.

# Live streams and sports

There's a question that customers ask Akamai when discussing live events and streaming content: "What percentage of our traffic is piracy?" Often, this question is followed by another: "What's the impact?" It's a tough set of questions to answer, because the answers change with each event.

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. 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.

## MCP production case study (2020 event):

When it comes to live event piracy, malicious actors leverage multiple attack surfaces. Understanding how live events are pirated is a key element in defending them. Many of the protections deployed by MCP only exist due to extensive research into the attack surfaces targeted by content pirates.

Interest in streaming events grew to record highs in 2020. Many concerts and sporting events were either closed to the public completely, or only allowed spectators in limited capacity. The answer for content owners and distributors was to stream these events to the internet, and either bundle access with existing services, or charge a moderate fee for access.

In 2020, during a sporting event in southern Asia, Akamai observed a wide variety of tools and techniques being used by malicious actors attempting to pirate the live stream.

## 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.

One of the first techniques observed was user-agent spoofing against API endpoints. This is where pirates attempt to mimic devices, or operating systems, that might have delegated access. If the workflows for these devices (e.g., Apple TV, WebOS, Fire TV, etc.) are different, then the pirates will look to exploit them.

Rebroadcasting was another issue during this event. This is when pirates share access to the live stream across a number of known social platforms, including Twitch, YouTube, and Facebook. These platforms quickly terminate pirated streams when they're reported, but the pirates themselves just keep streaming from new accounts and/or locations.

There were also instances of HTTP replay against API endpoints. This is when pirated apps leverage a single user's credentials in order to get multiple playback tokens. This leads to token exploitation, where if the assigned tokens have a Time to Live (TTL) longer than the event, the pirates will attack during non-event times. Since the tokens are not bound to IPs, this leads to token sharing.

One of the biggest challenges came from modified Android Package (APK) instances. These modified APK files are found on third-party app stores, and are repackaged versions of the original application. However, the protections and obfuscations used to protect access are bypassed via a number of techniques.

During this live event, with MCP, combined with other Akamai services that the customer uses, we were able to detect direct piracy attempts and active attacks. Akamai brought down piracy levels from 40% at the start to 15% by the end of the event. For obvious reasons, we're not going to release the methodologies or techniques used to detect or block these attacks.

The level of piracy could have been dropped even lower — possibly even to single digits — but the need to balance access for legitimate customers versus combating piracy is a business decision that has to be evaluated constantly during every event.

Sometimes it is better to err on the side of caution and be alert to a possible problem, rather than to assume something is bad and block it entirely. This trade-off is always going to exist when it comes to content piracy, and content producers and distributors will need to determine their own tolerance levels.

This production use of MCP wasn't cut-and-dry. While the tool proved it could cut piracy off at the source, the pirates themselves were not willing to give up so easily. During the event, they resorted to DDoS attacks to trigger failover events that would have converted their temporary tokens to full access tokens, thus enabling them to continue to pirate the stream.

The live event received 5.5 billion hits that triggered DDoS protection, of which 2.07 billion were mitigated. 3.4 billion of those hits triggered rules that were created for visibility and were logged in alert mode. In addition, there were 38 million requests that triggered application-layer protections, which were 100% blocked.

During this event, it was clear that the pirates understood the event's workflow, which led the customer and Akamai's teams to take the approach of Zero Trust — acting on the presumption that all clients are compromised, and only validated clients should be allowed to play the stream.

## MCP production case study (2021 event):

Fast-forward to July 2021 during a single-day sporting event in the United States. MCP was once again used for a live broadcast, which pirates were targeting. Unlike the event from 2020, which lasted several weeks, this one lasted just over three hours.

The July event generated more than 18 million records to be analyzed, with 4 million of them being flagged as suspect. In fact, there were 39 suspect referral links, nearly 7,000 VPN addresses, and 34,120 shared tokens identified among the suspect group.

Credential sharing is done at various levels in the piracy world. The goal is to get a legitimate access token, and use that in an app or as part of a re-streaming service. As we work with customers to protect their broadcasts, we look at token reuse — and the count of both the short and long tokens — to understand the exposure to credential sharing as a piracy vector.

For this particular event, the top 10 shared tokens combined were used more than 65,000 times. The number one shared token was seen more than 19,000 times alone. Clearly, pirates had taken a serious interest. Digging deeper, we observed 292,000 unique user-agents. Tracking user-agents can sometimes help identify the source, or cause, of the attempted piracy.

A few of the top video players identified for the July event are well known to home viewers, such as Kodi, Lavf, VLC, and others. Kodi was observed more than 275,000 times during the event, followed by Lavf, and IPTV. To be fair, the software packages' open-source tools themselves are not malicious. However, these products are used by pirates, often because they are easily enhanced by additional development, or easily deployed and widely available.

Another way to track piracy, and take action against it, is to track referral links. As mentioned, during the July event there were 39 suspect referral domains connecting to the broadcast event. Combined, these referrers represented more than 65% of the suspect traffic, and were easily identified by their domain name.

## MCP observations

While only two examples were selected for this report, the SOTI team examined dozens of logs and after-action reports as part of our research. As we worked, several common themes started to emerge.

The first is that credential reuse and credential compromise play a big role in broadcast piracy. After that, it's clear that broadcasters need to address API-based issues, including access controls and workflows. Finally, broadcasters can't just focus on a single method of piracy, as criminals will layer their attacks across several surfaces (often at the same time) in order to confuse defenders and bypass restrictions.

# Global piracy demand

One of the interesting things within the MUSO dataset is "piracy by title." Here the data is examining piracy on an attribution level, so the traffic is tied to a particular movie or television show.

For this report, Akamai looked at the global piracy by title data, which includes all genres, all titles, all production companies, television, and film, as well as streaming and torrent data. According to MUSO, between January and September 2021, the global piracy demand reached 3.7 billion. This figure is a measurement of a demand for pirated content, counted by visits to websites offering access to movies or television shows, either directly through a browser or mobile application, as well as torrent downloads. Essentially, this metric covers unlicensed streams and downloads.

### Top 10 most pirated films
(January–September 2021)

1. **"Godzilla vs. Kong"**
2. **"Zack Snyder's Justice League"**
3. **"Black Widow"**
4. **"F9"**
5. **"Mortal Kombat" (2021)**
6. **"The Suicide Squad" (2021)**
7. **"Cruella"**
8. **"Wonder Woman 1984"**
9. **"Raya and the Last Dragon"**
10. **"Jungle Cruise"**

### Top 10 most pirated television shows
(January–September 2021)

1. **"Loki," Season 1**
2. **"WandaVision," Season 1**
3. **"Rick and Morty," Season 5**
4. **"The Falcon and the Winter Soldier," Season 1**
5. **"The Walking Dead," Season 10**
6. **"Game of Thrones," Season 8**
7. **"The Flash," Season 7**
8. **"Vikings," Season 6**
9. **"True Beauty," Season 1**
10. **"Superman & Lois," Season 1**

# Piracy by industry

MUSO's piracy by industry data is complex and rich in information. In this subset of data, there isn't a direct attribution to a given content title, but a measurement of consumption. Within this dataset, how consumers are accessing their pirated content is a key metric to follow.

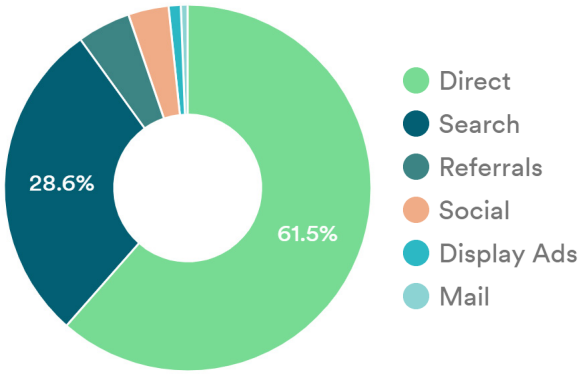


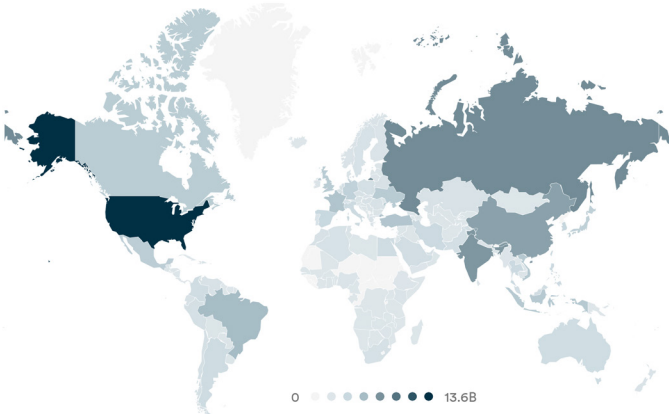

*Fig. 1: As shown by MUSO's data, a majority of consumers directly access pirated materials*

Based on the data, we can see that an overwhelming majority of consumers accessing the pirated materials are doing so directly (61.5%), while 28.6% of them are searching for it. The remainder are accessing content via referrals from other websites, social media, display ads, or email ads.

Considering the television and film industries alone — including both public and private torrent files, as well as web downloads, stream ripping, and direct streaming — there were 82 billion visits to piracy websites between January and September 2021. If you add in music, software, and publishing to these figures, the total jumps to over 132 billion.

Globally, during the nine-month reporting window, the United States (13.5 billion), Russia (7.2 billion), India (6.5 billion), China (5.9 billion), and Brazil (4.5 billion) were the top five locations for piracy website visits.

Clearly, piracy has the numbers to mark it as a critical issue. If these counts were related to malware infections, or a single data breach, it would be classified as one of the worst incidents on record.




| Rank | Country | Visits |
|---|---|---|
| 1. | United States of America | 13,558,211,764 |
| 2. | Russian Federation | 7,201,499,453 |
| 3. | India | 6,503,638,719 |
| 4. | China | 5,913,142,174 |
| 5. | Brazil | 4,533,436,207 |
| 6. | France | 3,889,291,887 |
| 7. | Turkey | 3,758,288,952 |
| 8. | Viet Nam | 3,561,238,902 |
| 9. | Indonesia | 3,494,551,117 |
| 10. | Ukraine | 3,342,906,062 |
| 11. | United Kingdom | 3,331,110,669 |
| 12. | Canada | 3,267,146,365 |
| 13. | Mexico | 3,126,434,106 |
| 14. | Japan | 2,926,208,373 |
| 15. | Germany | 2,808,971,369 |

*Fig. 2: The United States was the number one location for piracy website visits, followed by Russia and India. Combined, there were more than 27 billion piracy website visits between the three.*

But what about the individual industries? Here is a breakdown of how they looked between January and September 2021.

## Television:

At just over 67 billion total visits, television is the top pirated industry among MUSO's data. The average visits per internet user reached 20.01 across the nine-month reporting window, with the United States, followed by Russia, and China ranking as the leading three sources of visitor traffic.

In a way, these numbers can be explained by basic demand, as many of the titles being pirated are not generally available in the areas where the visitors are coming from. Looking at the top piracy websites, the traffic leaders are anime and general television streaming services. The top domain generated over 940 million visits from January through September 2021.

## Publishing:

With over 30 billion total visits, publishing is the second-largest pirated industry in MUSO's data. The average visits per internet user reached 9.03 during the reporting window, with the United States, Japan, and Russia ranking as the top three sources of visitor traffic. The top piracy websites focus heavily on manga and other book-based content, with the top website clocking more than 955 million visits during the reporting period.

## Film:

As the third-largest pirated industry in MUSO's dataset, the film industry is still the one most people think of when discussing piracy online. During the nine-month reporting period, the film industry accounted for 14.5 billion website visits, with an average visits of 4.31 per internet user. The top domain in this dataset generated 17% of the traffic delivered to the top 100, with 726 million visits. India was the top source of traffic in the film dataset, followed by Turkey, the United States, China, and Brazil.

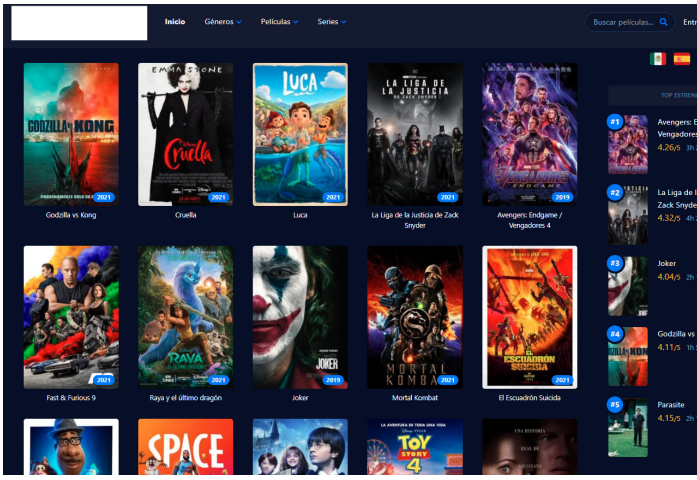



*Fig. 3: A website offering pirated newly released movies for streaming. Often the movies are streamed on pages filled with invasive advertising, and some websites are malicious.*

## Music:

At 10.8 billion, with an average 3.21 visits per internet user, music is the fourth-largest pirated industry in MUSO's data. However, piracy in the music industry has led to a number of content protection technology advancements. Moreover, when discussing piracy, music is usually the second item considered after film, due to the long history of music piracy being in the public eye.

While the days of Napster and LimeWire are long gone, music piracy services are still thriving online. The top domains associated with piracy visits are those that deal with downloading or converting other types of streaming media, most notably YouTube videos. Many of the domains listed in the dataset for the nine-month recording period have since closed down, but their successors are still operational, offering direct downloads of albums or singles.

The top traffic sources include India, followed by Iran and the United States.

## Software:

Software piracy is another type of piracy that has existed online for almost as long as the internet has. It's a broad category that includes video games as well as modern PC software. With 9 billion total visits, an average of 2.68 per internet user, a fifth-place showing is still a rather large problem. Combined, the top three piracy websites accounted for more than 16% of the overall visitations in the top 100, with more than 722 million visits during the nine-month recording period. The top traffic sources were China, followed by Russia, and the United States.


*Fig. 4: A piracy website offering software and games. Websites like these are frequently used to spread malware, or serve up malicious ads.*

> *"MCP delivered by Akamai's BOCC brings together advanced toolsets, intelligent capabilities, and broadcast experts to create a managed service that helps detect and mitigate broadcast-layer piracy."*
>
> *— Harish Menon, Senior Director, Broadcast Operations and Events*

# Conclusion

The global piracy demand in the first three quarters of 2021 exceeded 3 billion. Each day, hundreds of millions of connections to piracy websites are recorded, proving that the public's appetite for streaming content is only growing, and their choice of access is fluid.

In fact, it shouldn't surprise anyone to learn that those who pirate content are not dedicated to piracy. Instead, many of the conversations that Akamai researchers observed online related to piracy show that while a given show or movie is being pirated, those looking for this content pay to access other streaming services. The reason — outside of criminal enterprise — that many are pirating the content that they do is lack of access and availability. 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.

As mentioned, 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 a hold of the situation.

See you at the movies!

# Credits

## Editorial Staff

Martin McKeay
Editorial Director

Steve Ragan
Senior Technical Writer, Editor

Amanda Goedde
Senior Technical Writer, Managing Editor

Chelsea Tuttle
Senior Data Scientist

## Broadcast Operations Staff

Eric Elbaz
Lead Strategic Engagement Manager, Broadcast Media

Harish Menon
Senior Director, Broadcast Operations and Events

Vito Politano
Senior Manager, Technical Support

## MUSO

James Mason
CTO

Edmund Hall
Lead Data Analyst

## Marketing Staff

Georgina Morales Hampe
Project Management, Creative

Shivangi Sahu
Program Management, Marketing

## More State of the Internet / Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet / Security reports. akamai.com/soti

## More Akamai Threat Research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. akamai.com/our-thinking/threat-research

## Access Data from This Report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided Akamai is duly credited as a source and the Akamai logo is retained. akamai.com/sotidata