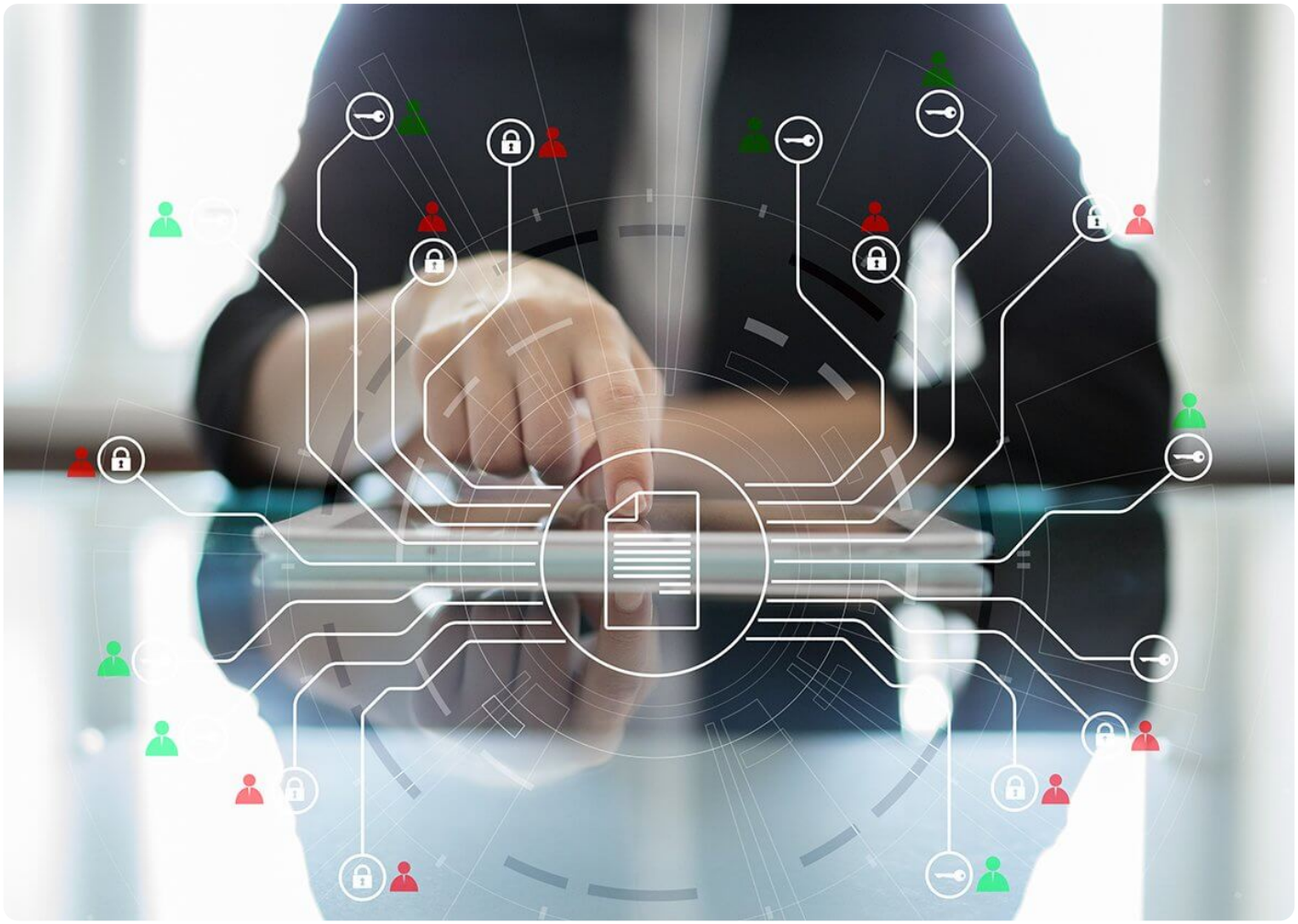
Using Website Contacts and Categorization Tools for More Effective Digital Rights Management

Posted on November 5, 2019



Digital rights management (DRM) is a systematic approach to copyright protection for all kinds of digital media. It prevents unauthorized redistribution of digital media and stops consumers from copying the content they purchase.

DRM products were developed in response to a rapid rise in online piracy of commercially marketed materials aided by the widespread use of peer-to-peer (P2P) file exchange applications, more widely known as torrent clients.

DRM is typically implemented by embedding code in materials to prevent users from copying them. At times, it limits the amount of time when content can be accessed or the number of devices the media can be consumed on. Despite its widespread use, however, online piracy still runs rampant.

So, what can digital media producers do to protect their intellectual property from online pirates? Would limiting access to their distribution platforms help? How do they make sure that they're not keeping legitimate consumers out along with the digital pirates? These are just some of the questions that this post answers.

Table of Contents

The Case: The Kickass Torrents Story

Kickass Torrents, also known as “KAT,” was a website that provided users with a directory for torrent files and magnet links to facilitate P2P file sharing via the BitTorrent protocol. It was founded in 2008 and by November 2014 became the most visited BitTorrent directory in the world, knocking down The Pirate Bay from the number 1 spot.

Over time, KAT consistently received complaints from content owners for infringement. And though it claimed to comply with the igital Millennium Copyright Act (DMCA) by removing reported torrents, it kept changing domains — a tactic to avoid takedown. The following list shows the various domain changes KAT went through over the years:

- 2008: kickasstorrents.com
- 21 April 2011: kat.ph (probably in response to the seizure of the Demonoid, Torrentz, and other similar domains in the U.S.)
- 2011–2013: ka.tt (part of the seizure-evasion tactic employed by KAT every six months or so)
- 14 June 2013: kickass.to (a likely response to the U.K. move to block access to KAT and other torrent sites countrywide)
- December 2104: kickass.so (a response to being delisted by Google and after other countries, including Belgium, Ireland, and Malaysia, followed the U.S. and the U.K.’s move to block access to it)
- 9 February 2015: kickass.to (a move made after kickass.so was banned on the WHOIS database)
- 23 April 2015: kickasstorrents.im (a response to blocking on Steam)

- 24 April 2015: kat.cr (a move made after the Isle of Man domain was blocked)
- June 2016: .onion address (a response to the removal from Google search results, further blocking in Portugal and on Google Chrome and Mozilla Firefox browsers
- December 2016: katcr.co

KAT went offline on 20 July 2016 when the U.S. government seized its domains. Its proxy servers were shut down by its staff at the same time. Its alleged owner, Artem Vaulin, a 30-year-old Ukrainian man, was arrested in Poland. Going by the nickname “tirm,” Vaulin was charged with four counts of criminal indictment. Soon after the domain’s takedown, multiple unofficial mirrors were also rendered offline despite having no official connections to the case as an additional measure against copyright infringers.

The Victims: The Media Producers Who Suffer from Online Piracy

Watching your favorite shows and movies, using the best software, reading books and other published works, and listening to your favorite music artists for free is the primary reason why torrent and other P2P sharing sites abound. What consumers may not know or care about, however, if they do is that they’re ultimately hurting the content creators by violating their intellectual property rights.

It takes many resources to produce a film, and most independent filmmakers struggle to pitch their work for financing and global distribution all the time. So, when online pirates steal and illegally distribute their work to the public, the studios don’t earn enough to at times even pay for production costs. The result? The studio folds, its staff members lose their jobs, your favorite actors don’t get paid, and the world no longer gets to enjoy quality movies.

The same thing happens in the publishing, music, and other media industries. Authors, singers, musicians, directors, and other creative artists, not to mention the people behind the scenes

(camera operators, editors, etc.) lose not just their livelihood means but also their pensions due to online piracy.

Things get even worse when work leaks out before its official launch. That was the case with "Expendables 3." By the time it was shown, an estimated 70 million viewers could have already watched it. How could the filmmakers earn if the pirates even beat them to the punch? Is DRM the answer?

A Potential Solution: How Website Contacts and Categorization Tools Can Enhance DRM Solutions

DRM may well be an excellent means to combat online piracy but let's face it, gauging by how fast and easy digital pirates can move their infrastructure from one location to another (as KAT's domain changes showed), it's not a foolproof solution.

DRM allows media owners to:

- Restrict or prevent users from editing, saving, forwarding, and printing content;
- Only allow content viewing, printing, or copying up to a limited number of times;
- Disallow users from creating screenshots or screengrabs of content;
- Set an expiration date on content after which users will no longer be able to access it; this is possible to do by limiting the number of uses a consumer has;
- Lock access only to specific IP addresses, locations, or devices;
- Watermark content to establish ownership and identity.

While those steps are effective, limiting access to content can still be improved. First, media owners need to realize that online pirates are mostly content consumers too. A KAT staff member

can, for instance, subscribe to a streaming service, thus legally consuming content. He would only differ from a regular user in that he somehow manages to copy the said content and distribute it to others.

One way of preventing copyright infringement is by screening content consumers for malicious intent. While this could be a tedious process and riddled with guesswork, it should afford better security. It's hard to confirm a consumer's motives, but intelligent assumptions can still be handy. For instance, a regular content consumer would most likely work for a living (he can't just sit all day, say, watching movies). If that's the case, he'd need to rest and do other things (run errands, interact with others, etc.) to survive. So, a regular content consumer is likely to have a maximum of eight hours (providing he or she has no social life and doesn't travel long distances to get to work and back home) for leisure time. If (s)he's an avid movie fan, (s)he can only watch 4–6 movies back-to-back in a day. That said, a streaming service provider can automatically flag a user who consumes more than that as a potential online pirate.

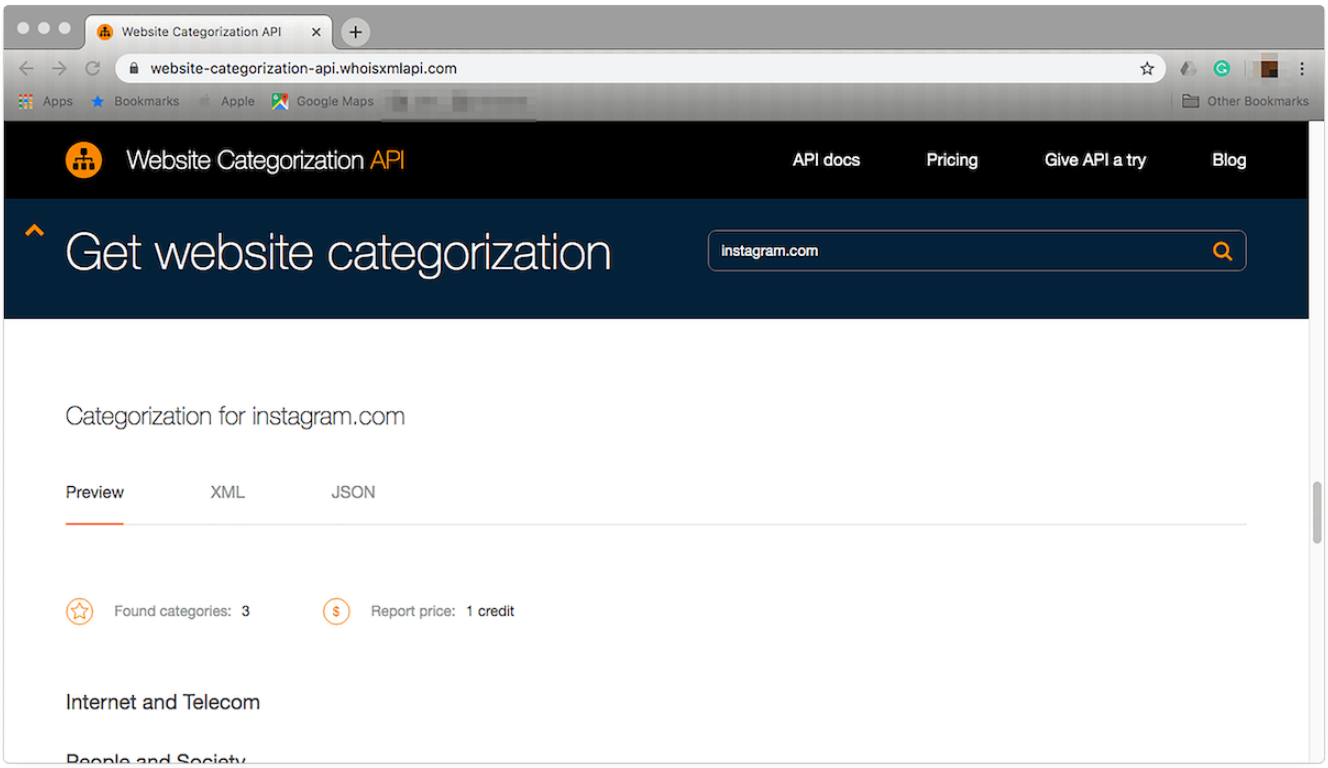
The next step would be confirming one's suspicions. This process is where a website categorization tool may come in handy. A website contacts and categorization database, for instance, can provide a media owner with a site owner's personal information and more. A website categorization API, meanwhile, instantly tells users if a particular site is malicious. Both tools can help media owners block access from unwanted domains (tied to suspected pirates' names, email addresses, etc.) to their portals, thus preventing online pirates from preying on their content.

Let's take a closer look at how Website Categorization API works.

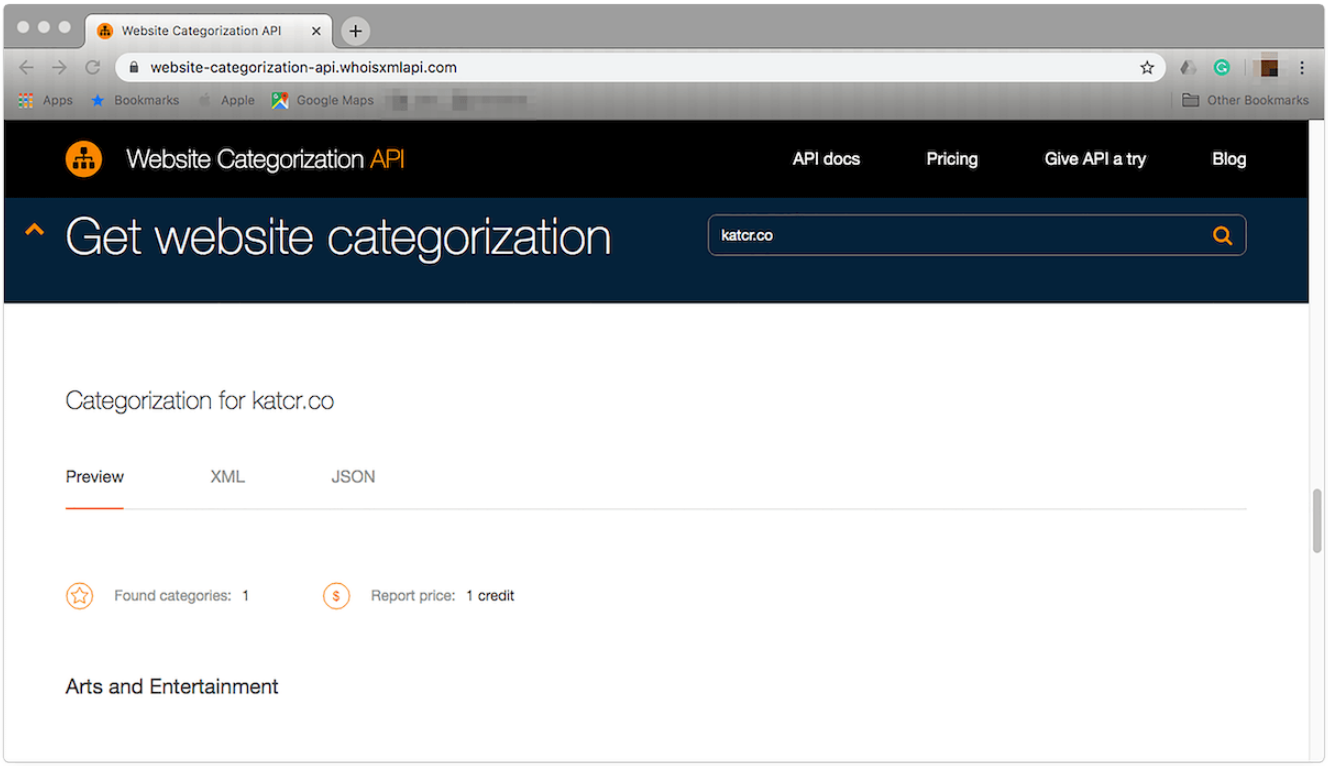
1. Access the tool by logging in to https://website-categorization-api.whoisxmlapi.com

2. Let's say that you discovered that one of your streaming service customers is a KAT employee. For all intents and purposes, you weren't entirely sure that KAT is a torrent provider and so you launch an investigation on the site. For this demonstration, let's use KAT's latest domain, katcr.co.

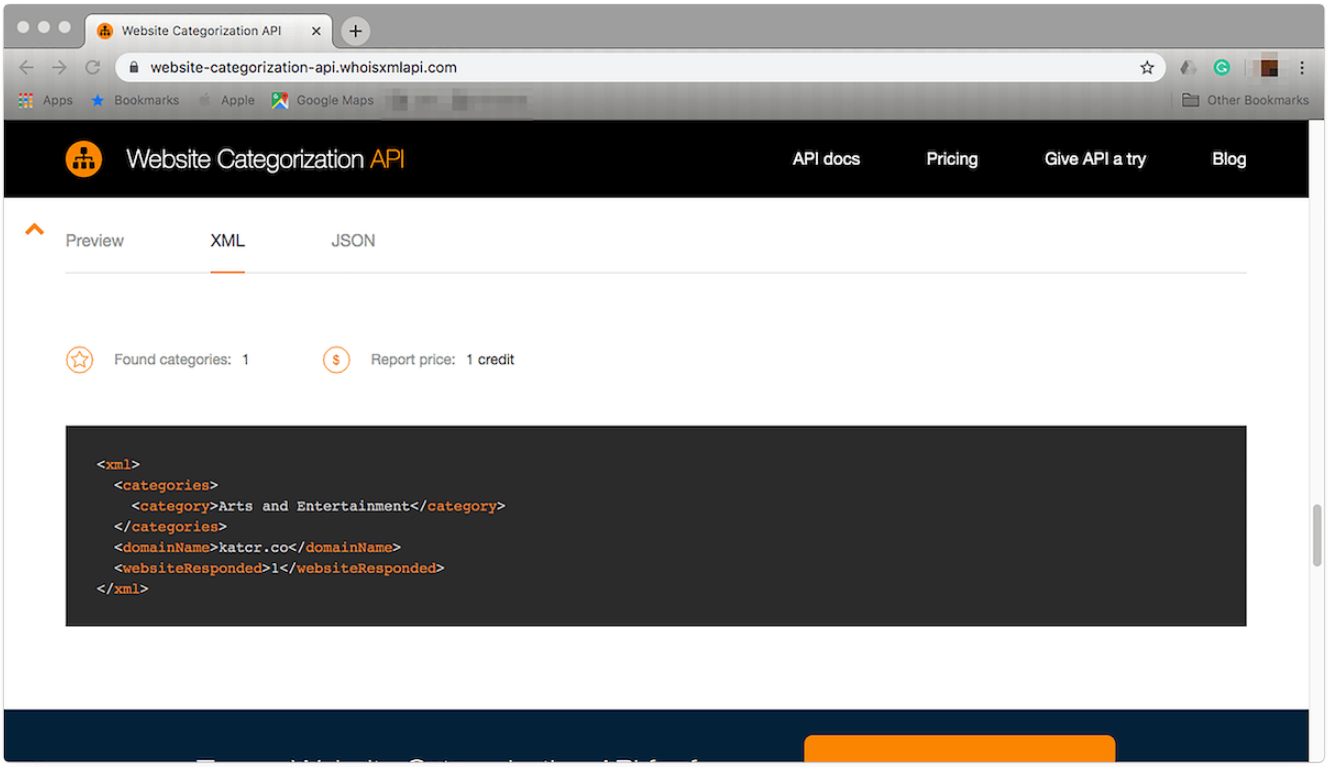
3. After you've successfully logged in to the tool, click Give the API a try. You should see the bottom of the page where you can start using the product.



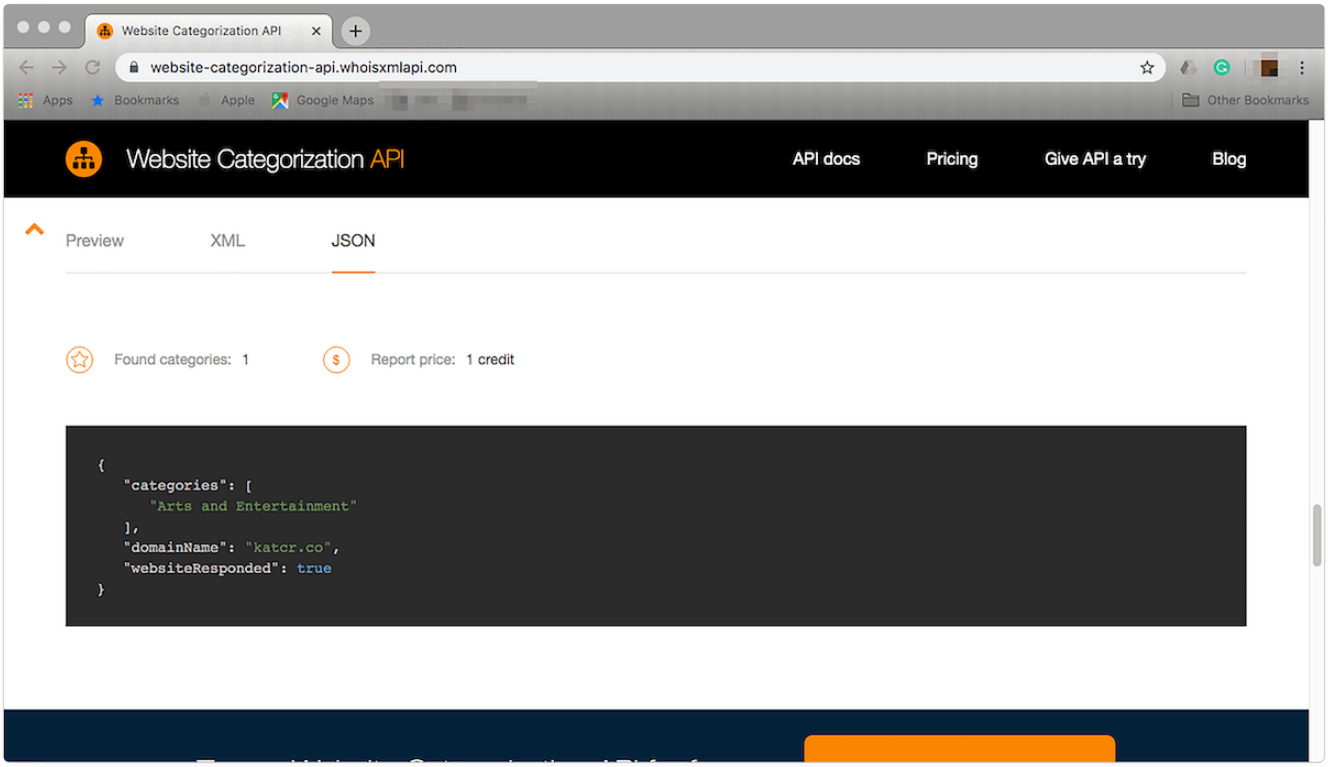
4. Type the domain in the Search field then hit the Enter key. You should see at least one category that the domain falls under. In this case, that is Arts and Entertainment.



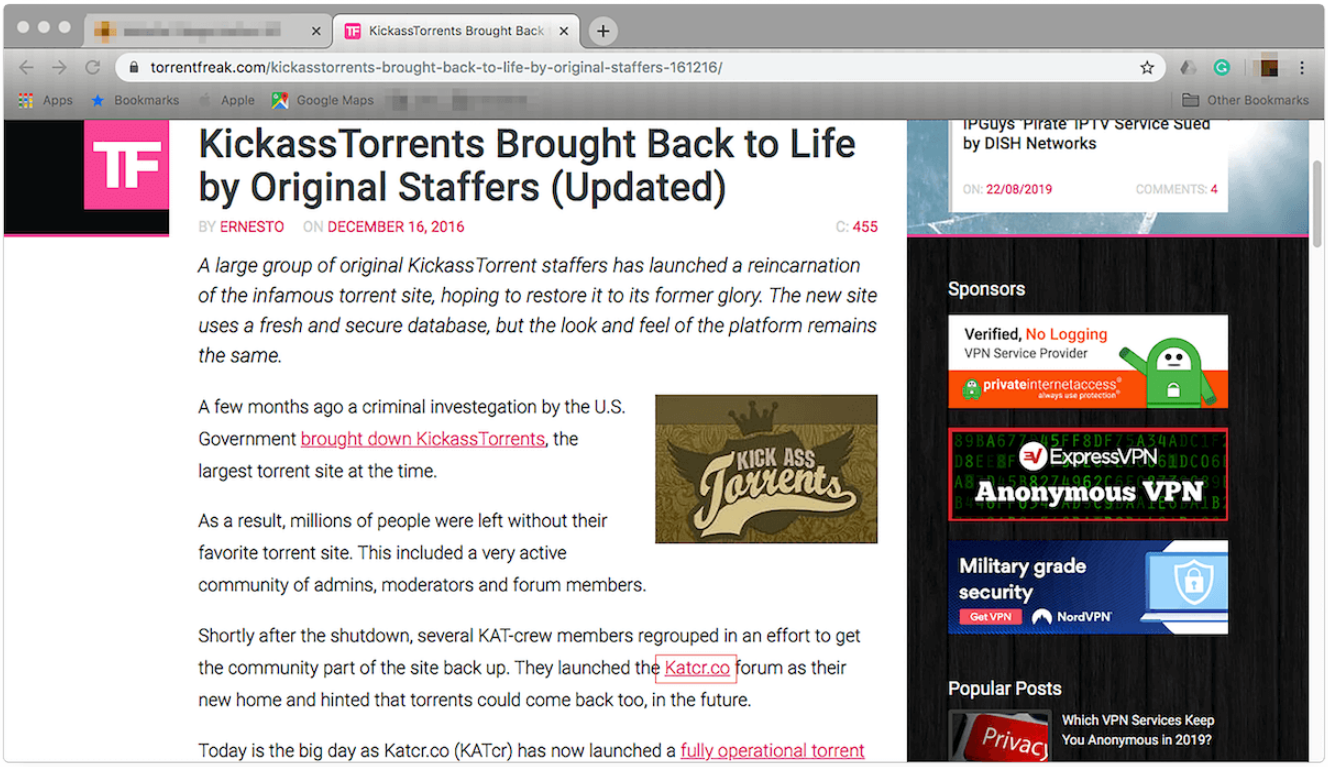
If you're comfortable viewing API results in code or would like to integrate these into your existing DRM solution, you can do so by clicking XML or JSON. The result in the XML format looks like this:



If you're more comfortable with the JSON format, you can opt for this instead:



5. It seems pretty harmless, right? Let's say you're not convinced. You did flag the domain for a reason. So, you do a Web search for the domain to corroborate your findings with news reports. You may end up finding this:



6. Your suspicion is then confirmed. You may be under attack by an online pirate. Now, you can safely blacklist any customer with ties to the site from accessing your network.

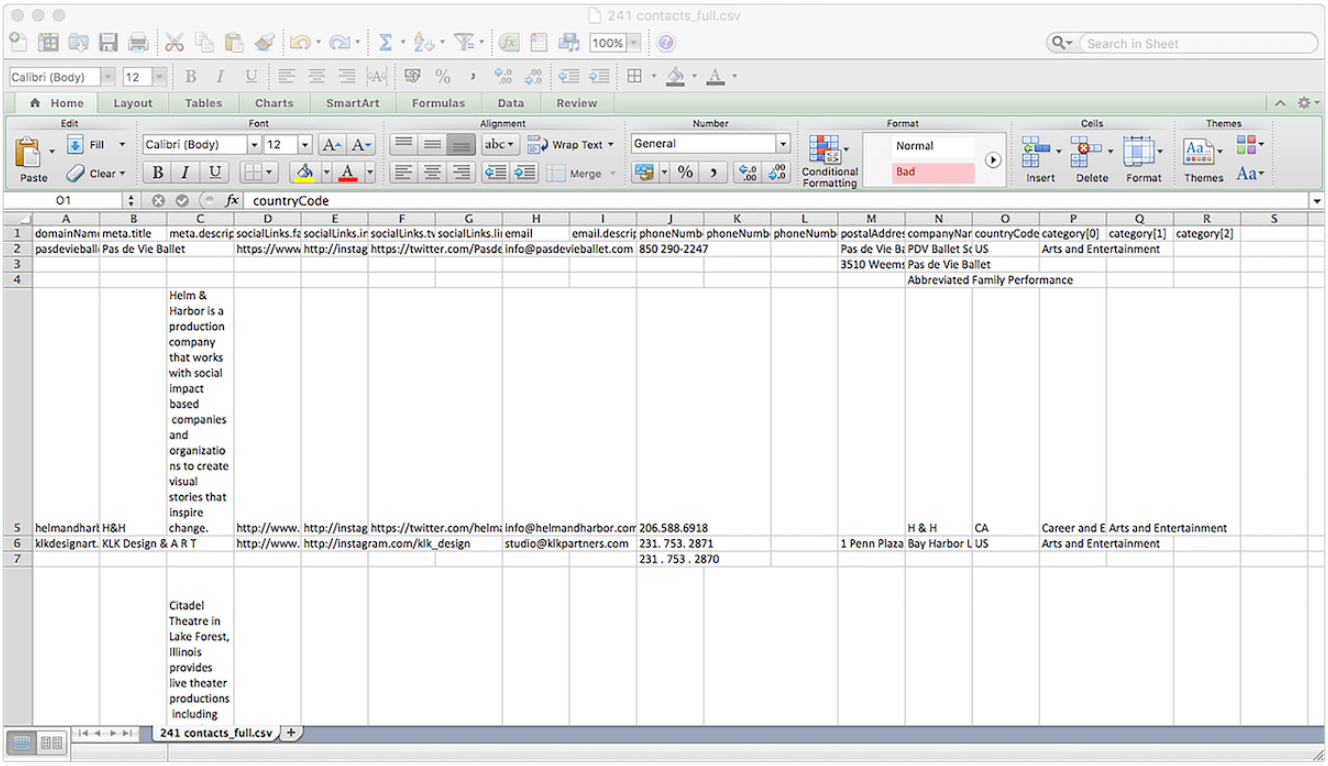
7. Follow the same steps with every suspicious user to rid your network of online pirates.

Now, that is a resource-intensive process, but there may be a faster way to eliminate unwanted access from your network. If you want to get a comprehensive list of similar domains, you can download a website contacts and categorization database.

Unlike the API that gives information piecemeal, Website Contacts & Categorization Database gives you all of the domains classified as Arts and Entertainment sites. It can help you filter the good from the bad (in this case, torrent sites). It also provides more information on a domainyou're digging deeper into, apart from the categories (top 3) it falls under, such as:

- Domain name
- Meta title and description
- Social media links (Facebook, Instagram, Twitter, and LinkedIn)
- Email address and description
- Phone numbers
- Postal address
- Company name
- Country

In the CSV format, the database looks like this:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	domainNam	meta.title	meta.descrip	socialLinks.fa	socialLinks.in	socialLinks.tv	socialLinks.li	email	email.descrip	phoneNumb	phoneNumb	phoneNumb	postalAddres	companyNar	countryCode	category[0]	category[1]	category[2]	
2	pasdevieball	Pas de Vie Ballet		https://www	http://instag	https://twitter.com/Pasde		info@pasdevieballet.com		850 290-2247			Pas de Vie Ba	PDV Ballet Sc	US	Arts and Entertainment			
3													3510 Weems	Pas de Vie Ballet					
4														Abbreviated	Family Performance				
5	helmandhart	H&H	Helm & Harbor is a production company that works with social impact based companies and organizations to create visual stories that inspire change.	http://www.	http://instag	https://twitter.com/helm		info@helmandharbor.com		206.588.6918				H & H	CA	Career and E	Arts and Entertainment		
6	klkdesignart.	KLK Design & A R T		http://www.	http://instagram.com/klk_design			studio@klkpartners.com		231. 753. 2871			1 Penn Plaza	Bay Harbor L	US	Arts and Entertainment			
7										231 . 753 . 2870									
			Citadel Theatre in Lake Forest, Illinois provides live theater productions including																

Using the database, an analyst can obtain more information on a domain of their interest. In this particular case, that is katcr.co. We already know it's a P2P sharing site, something that's illegal in many countries. So, if you are a media provider, it's a sure bet you don't want anyone from it accessing your content.

For less obvious potential threats, though, the Website Contacts & Categorization Database serves as a useful reference for determining your site visitors' motives. A legitimate business, for instance, would typically use social media to promote its products or services. That said, a domain that doesn't have social media ties could be hiding under the radar, and you should therefore deny access from thus identified sites to your network.

Filtering the contents of the database by company name, registrant, email address, or social media accounts also allows users to pinpoint relationships among online pirates. If one of a

registrant's domains proves malicious, for instance, blocking his other domains from accessing your network is a good idea. The database is an excellent means for users to spot visitors who may be using clever disguises to take advantage of your content.

The Verdict: Lessons Learned from the Kickass Torrents Case

Vaulin was caught when an IP address he used for an iTunes transaction was also used for logging in to KAT's Facebook page. FBI agents also posed as an advertiser to obtain information on bank accounts associated with the site. They also seized full copies of KAT's hard drives, including its email server.

Ties to social media and email accounts, as you know by now, can easily be determined with the Website Contacts & Categorization Database — something that proved critical to the investigation. Protecting against threat actors largely depends on determining where threats come from and what the perpetrators' motives are. Without good sources of threat intelligence, thwarting cybercrime and other cyber attacks won't be as effective.

We've seen this in KAT's case, for instance, as in December 2016, former staff members revived the community by creating a website with its predecessor's features and appearance. Putting its creator behind bars clearly isn't enough. Making sure your content databases remain unreachable to threat actors with DRM solutions and rich threat intelligence sources, however, is.