DCA CONSUMER ALERT

OFFSIDES

How Criminals are Exploiting the COPA do Brasil to Spread Malware Via Piracy Sites

digitalcitizens alliance

whitebullet

UNIT 221B
GUIDED BY INTEGRITY | DISCREET BY DESIGN

October 2024

Table of Contents

Executive Summary

In early November, tens of millions of futebol fans in Brazil and around the world will tune in to watch the Copa do Brasil finals. But what many of these fans may not realize is that criminals are counting on them to watch these matches via unauthorized piracy devices – so they can infect their computers.

A joint investigation found that piracy operators and other criminals are targeting events such as the Copa do Brasil as a devious way to prey on unwitting Internet users enticed by the lure of "free" access to major events available on piracy sites. Once they start watching the event, viewers are bombarded with ads, many of which are specifically designed to spread malware.

Fans who watch the Copa do Brasil on their mobile devices using a piracy site or app are especially vulnerable, according to the findings of the investigation, which was conducted by the Digital Citizens Alliance, White Bullet, and Unit 221B. The investigation found that bad actors in Brazil are increasingly targeting mobile devices as a means of spreading malware.

The investigation reviewed advertising on over 500 piracy platforms focused on the Brazilian market. It found dozens of instances of malware-ridden ads on these sites, ranging from mildly to highly malicious – including a virus laden KMSpico file that enables criminals to spy on its victims, steal data, and even open a device to be used for crypto-mining without the knowledge of the user.

In early October, investigators also specifically tested whether viewers who watched the Copa do Brasil semi-finals on piracy platforms would be subjected to misleading ads that are typically used to trick users into downloading malware. To conduct this test, Unit 221B investigators visited multiple sites offering pirated streams for the Copa do Brasil games occurring on October 2. While on these pirate sites, Unit 221B was subjected to deceptive ads such as those claiming the user's device was already infected or ones that displayed a false video player, followed up by the claim that a user needed to sign up for an advertised VPN or utility to continue playing the video.

Below are examples of deceptive ads that appeared while investigators watched a Copa do Brasil semi-final match. The first attempts to trick the user into believing their device is infected with viruses. The second tries to trick the user into clicking on a video. These are the tell-tale signs of how bad actors trick users – either through scare tactics or the lure of something - to make the fateful click that infects their device.

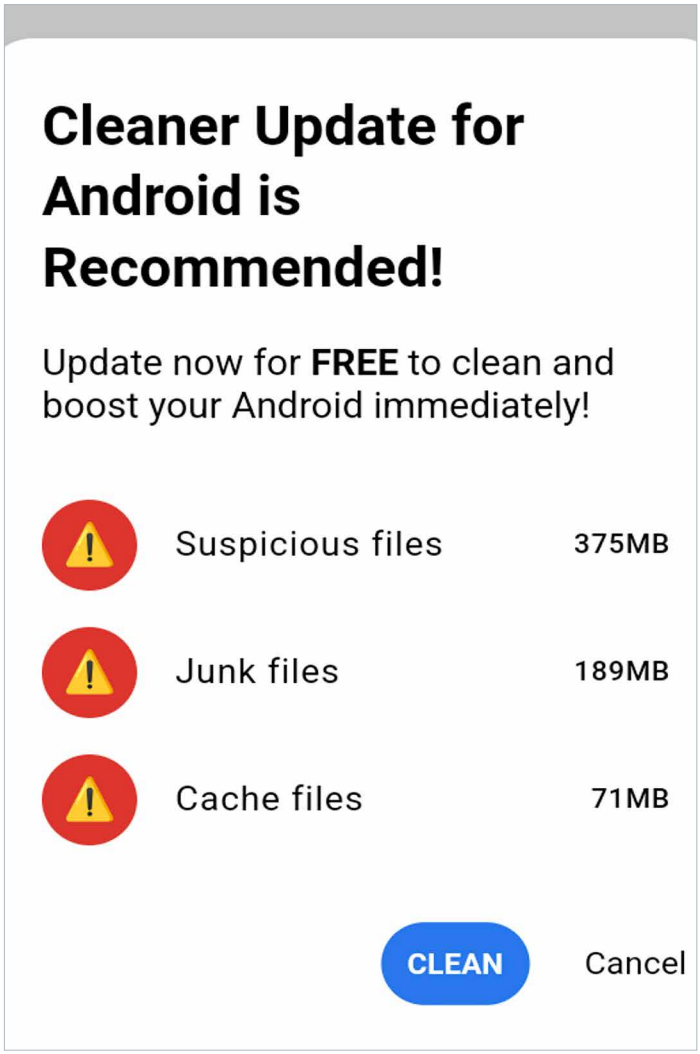

IMAGE 1

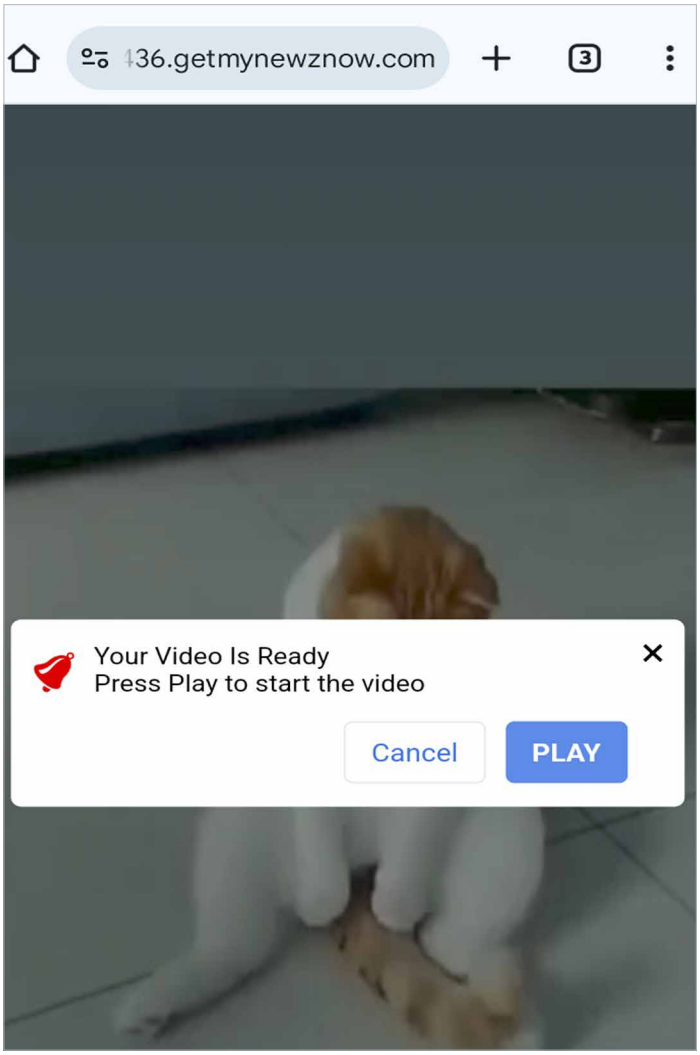

IMAGE 2

What these bad actors know is that Copa do Brasil presents a target-rich opportunity for piracy operators and the criminals they do business with to target viewers. Here's why:

- Seventy-eight percent of Brazilians say they intend to watch the upcoming Copa do Brasil finals, according to a recent research survey. Thirty-four percent of them say they'll rely on their mobile device to watch the finals.

- Like many of their counterparts in other countries, Brazilians are drawn to the lure of access to live events, movies, and TV shows. Sixty-one percent of Brazilians said they have visited piracy sites, according to the research, which surveyed over 1,000 Brazilians in September.

- As mobile devices become an increasingly popular way to watch live events, bad actors are focusing their efforts on spreading dangerous malware on those devices. The investigation of how malware is spread on piracy platforms in Brazil found that ads on mobile devices are four times more likely to be malware-ridden than on laptop or desktop computers.

- Brazilians who use piracy sites to watch live sporting events or movies and TV shows are likely unaware of the risks. But the risks are real. Brazilians who reported visiting piracy sites on at least a monthly basis are:

    - Three times more likely to report having an issue with malware or other type of virus than those who say they don't visit piracy sites. And while less common, Brazilians who visit piracy sites are four times more likely to have endured a ransomware attack (when a user's data is locked by criminals to extort a ransom financial fee).

    - Twice as likely to have reported credit card theft than those who don't visit piracy sites. Investigations have found that users who sign up for piracy subscription services are much more prone to report credit card abuse.

    - Four times as likely to have reported theft of financial information than those who don't visit piracy sites. Those who regularly visit those sites are also two times as likely to report ID theft.

Perhaps most telling is the disparity of reported breaches. Fifty-two percent of Brazilians who report they don't visit piracy sites said they haven't had an issue with their digital security in the last year. But only 11 percent of those who said they regularly visit piracy sites could say the same.

Brazilian futebol fans are among the most passionate in the world. And the Copa do Brasil is a premiere event – which is why it offers an ideal opportunity for criminals and other bad actors to target fans for harm.

Given these revelations, Digital Citizens urges Brazilian authorities and consumer safety organizations to warn citizens about the serious cyber security risks of relying upon digital piracy sites to watch the Copa do Brasil finals.

When it Comes to Piracy, Users are the "Big Game"

Piracy and malware now go hand in hand. And it makes sense. Piracy is a $2.3 billion global industry operated by savvy criminal organizations. These bad actors entice tens of millions of viewers with the lure of "free" access to movies, TV shows, and events. And Brazilians are among the most rabid users of piracy sites, behind only the United States, Russia, India, and China.

Piracy operators are engaged in an illegal activity, so perhaps it's no surprise that they are willing to harm their users if the price is right. That is where so-called malvertisers come into play. They pay the piracy platforms to run their malicious ads as a mechanism to spread malware. The ads are designed to trick users into clicking on them. The fateful click then activates hidden malware that infects the user's device. In the end, the users of piracy sites get more than they bargained for: infected devices, stolen credit card information, and even ransomware.

And it's big business for global piracy operators: they are paid over $120 million a year to help malvertisers infect the devices of the users of their piracy services.

The investigation of 500-plus piracy sites that target Brazilians was rife with malicious ads. In one month, Brazilian visitors to these piracy sites were bombarded with an estimated 5.7 million ads designed to spread malware or defraud. Ultimately, it's a game of "Piracy Roulette" - during the investigation, 1 in 7 visits from Brazil to piracy sites encountered malicious ads. When Brazilians use a mobile device, the risk of a malicious ad is 1 in 4 visits.

The source of these malicious ads that target Brazilian users of piracy sites were 141 businesses that deal in malicious advertising, according to White Bullet, a global firm that specializes in piracy detection and mitigation. Of these businesses, five accounted for 65 percent of all malicious ads found on these sites. They are not household names, and often come and go only to resurface as a new entity. In fact, the top purveyor of malicious advertising, a company called iosvpncontrol.com which accounted for 25 percent of all malicious ads, disappeared after the completion of the preliminary stage of the investigation in May.

Piracy Operators & Malvertisers Win, Users Lose

The malvertising these companies spread via piracy sites can be devastating. The KMSpico file threat found on dozens of piracy platforms most popular in Brazil is a good example. The journey towards an infected device starts with the lure: KMSpico is offered as a means to illicitly use Microsoft Windows and Office. However, it is often loaded with a virus that poses multiple threats.

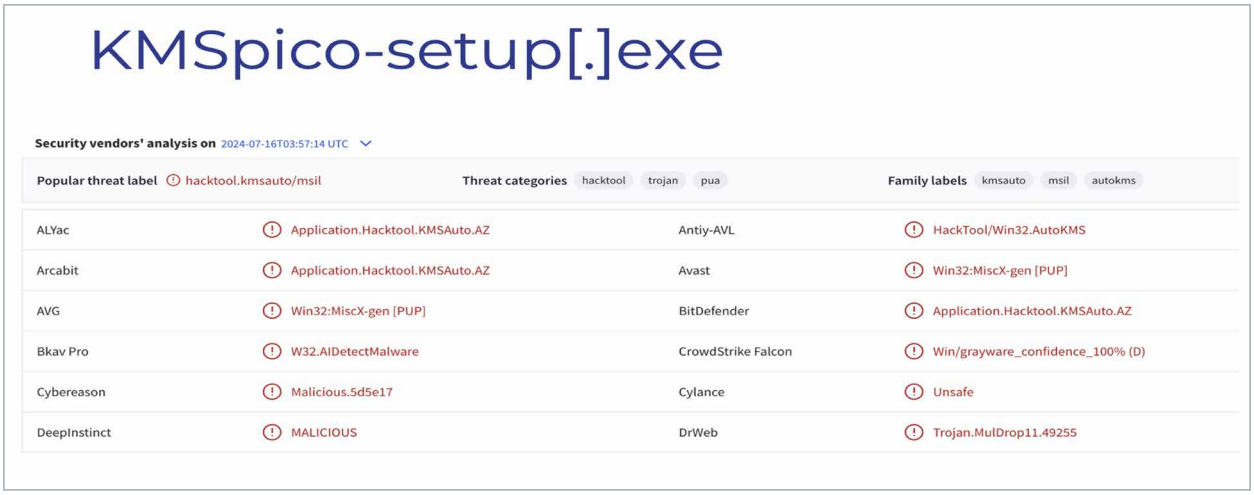

IMAGE 3

According to Sensor Tech Forum, once installed KMSpico can wreak havoc:

- **Trojan Clients** — The made infections will create a persistent and secure connection to a hacker-controlled server which allows the hackers to take over control of the infected machines, steal their files and deploy other malware.
- **Data Theft** — The KMSpico malware may include an information harvesting ability which is capable of acquiring data that can directly expose the identity of the victim users.

- **Machine Identification** — Many similar threats are programmed to extract the list of installed hardware components, specific operating system environment values and user settngs which are then processed by a special algorithm that will ouput an unique infection ID that is to be assigned to each different computer.
- **Windows Registry Changes** — The KMSpico malware can create entries for itself in the Windows Registry which can make its removal more difficult. If it edits existing values then serious performance issues can arise. Data loss and errors are a common side effect of this operation.
- **Boot Menu Options Modification** — Some KMSpico malware versions can modify the boot options in order to automatically start themselves when the computer is powered on. By disabling access to these options manual user removal guides can become worthless.
- **Data Removal** — The engine can be configured to locate and delete files such as system backups, restore files and shadow volume copies. This makes recovery much more difficult and in this case the use of a data recovery solution needs to be used.

On Reddit, one user recounted a story of what happened after downloading KMSpico: "There so many kmspico site that honestly look legit but it is not. Long story short, My ID has been compromised, they created another bank account under my social and transfer all my money to that bank."

The lure of installing KMSpico to get access to Microsoft tools has also been used by criminals to infect devices to steal financial information as well as sensitive information users may store on Google Chrome or Mozilla Firefox browsers.

Brazilian visitors to piracy sites were also targeted for the Setup.msi virus. The malvertisers that seek to spread this virus disguise it as a legitimate setup file for another application. But once it's installed it steals sensitive information and opens so-called backdoors on a device to enable criminals to get additional access.

KMSpico-setup[.]exe

Security vendors' analysis on 2024-07-16T03:57:14 UTC

Popular threat label	hacktool.kmsauto/msil	**Threat categories**	hacktool, trojan, pua
Family labels	kmsauto, msil, autokms		

ALYac	Application.Hacktool.KMSAuto.AZ	Antiy-AVL	HackTool/Win32.AutoKMS
Arcabit	Application.Hacktool.KMSAuto.AZ	Avast	Win32:MiscX-gen [PUP]
AVG	Win32:MiscX-gen [PUP]	BitDefender	Application.Hacktool.KMSAuto.AZ
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/grayware_confidence_100% (D)
Cybereason	Malicious.5d5e17	Cylance	Unsafe
DeepInstinct	MALICIOUS	DrWeb	Trojan.MulDrop11.49255

IMAGE 4

Previous investigations have also shown that piracy and malware can lead to the equivalent of the "digital death penalty": ransomware that, once installed, locks a user's data unless the criminals are paid. The image below is of a ransomware attack that occurred while Unit 221B was investigating malware on piracy sites.

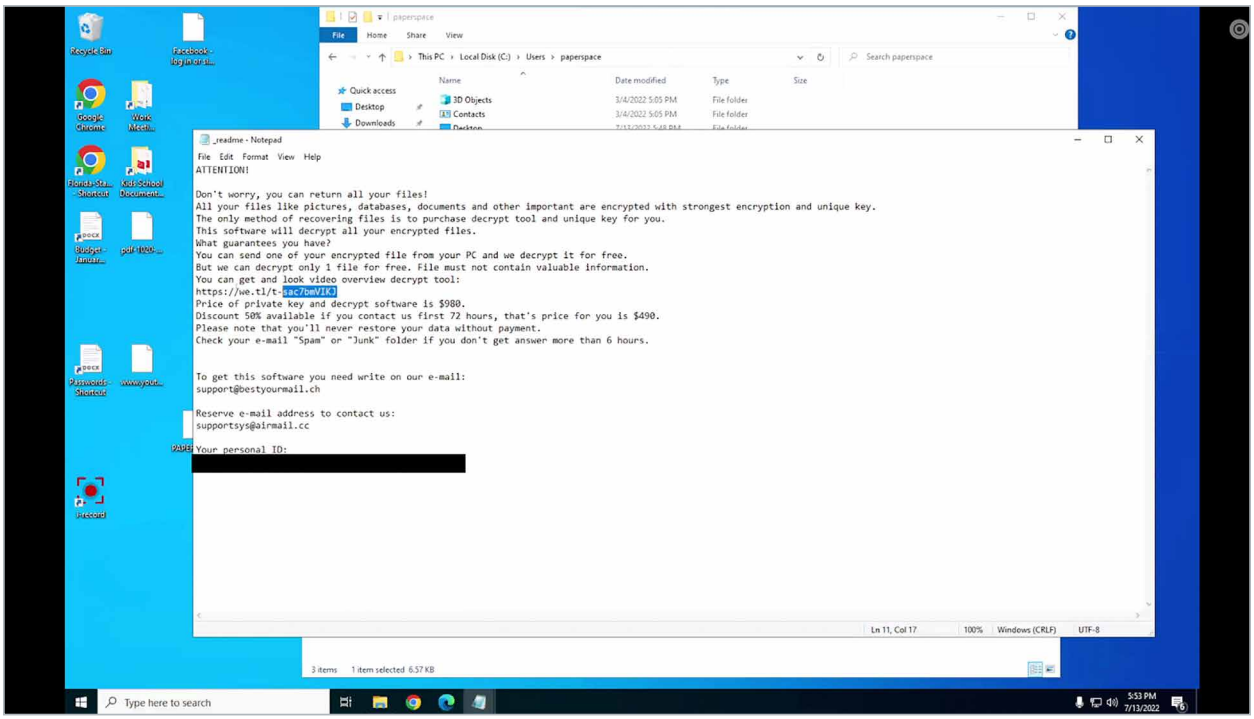

IMAGE 5

Copa do Brasil Viewers: Don't Be Bait

Over the last decade, piracy operators have diversified their businesses. They no longer solely rely upon exploiting the creative works of others (such as movies, TV shows, live events, music, and gaming) and now also exploit the visitors to their sites. Digital Citizens investigators have observed as piracy operators and malvertisers negotiate the prices to install malware on users' devices.

And events such as the Copa do Brasil that draw tens of millions of viewers are an ideal opportunity for piracy operators and malvertisers to exploit fans. Which makes it vital that fans of the Copa do Brasil, whether located in Brazil or around the world, understand the risks they face when lured into watching on illicit piracy platforms.

The scheme these bad actors employ demonstrates that access to free content is rarely consequence free. That is most visibly reflected in the fact that Brazilian visitors to piracy sites are nearly five times less likely to report having an issue with their digital security in the last year compared to those that avwhothese sites.

Piracy and malvertising are a toxic combination.

Consumers need a better understanding of how piracy is set up to bait them, how advertising on these sites often isn't what it appears to be, and the dangers that can come from just one catastrophic click. When it comes to the Copa do Brasil, piracy, and malware there is only one winner: Criminals.

Appendix

Research Survey Highlights

1,203 respondents surveyed from September 28-29, 2024

Q1. The Copa do Brasil 2024 semi-finals and finals will be held in October and early November. How likely are you to watch?

Very likely	56.86%
Somewhat likely	20.62%
Not sure	11.47%
Somewhat unlikely	5.32%
Very unlikely	5.74%

Q2. If you intend to watch, tell us the ways you are likely to do so? (Choose as many as apply)

On a mobile device	33.17%
On a laptop or desktop	30.92%
On a television	67.91%
On the radio	8.65%
Not sure	4.32%
Don't intend to watch	3.24%

Q3. Have you ever visited websites or apps that enable users to watch unauthorized content such as pirated movies, TV shows, and live sporting events?

Yes	61.01%
No	31.59%
Not sure	7.40%

Q4. Have you faced any of the following issues in the last year? (Choose as many as apply)

	Visit Piracy Sites at least once a month	Don't visit piracy sites
Malware	34%	12%
Credit Card Theft	33%	16%
Theft of Financial Info	19%	5%
ID Theft	8%	4%
No Issue with Digital Security	11%	51%

Piracy Sites Reviewed

037hdd.com	agit613.xyz	batmanstream.org
037hdmovie.com	agit614.xyz	bazenation.com
11mtv.com	agit616.xyz	bestlightnovel.com
123-hd.com	agit617.xyz	bgibola7.sbs
123-hd.me	akashinime.online	bolly4u.cash
123hd.tv	akashinime.site	bolly4u.day
123moviesfree.fan	allyoulike.org	bomoza.com
1337x.st	andaman888th.com	bontv29.com
24baze.com	androidfreeware.net	bontv31.com
300mbunited.me	anime-d.com	bontv32.com
33standard.com	animescx.com.br	bontv35.com
360media.com.ng	anime-subth.net	bontv42.com
447hd.com	animeworld.tv	booksfree.org
4download.net	anixverse.com	booktrk.com
4mirrorlink.com	anroll.net	bozatv41.com
7mscorethai.com	antenasport.ru	cakhia.de
7mscorethai.live	antupload.com	cakhia1.net
7mscorethai.net	aovivo.club	cakhia18.net
90phutc.tv	aovivo.gratis	cakhia19.net
90phuti.tv	aovivo.pro	cakhia21.net
90phutk.tv	apk.watch	cakhia247.tv
90phutv.tv	apkbe.com	cakhia3.vip
90phutx.tv	apkcap.com	cakhia33.live
90phutz.tv	apkfolder.net	cakhia365.tv
90p-tv.tv	apkrings.com	cakhia5.vip
91phut.net	arvenscans.com	cakhia68.tv
91phuttv.tv	asuralightnovel.com	cakhia7.vip
91phutz.net	audiotrimmer.com	cakhia8.vip
91phutz.tv	ball24hr.com	cakhiav.com
a2zapk.io	bamoza.com	cakhiav.live
agit611.xyz	baskadia.com	cakhiaztv.net
agit612.xyz	batman-stream.live	ceenaija.com

chachatv24.pro	doku.pub	filmestorrent.tv
chachatv27.pro	dontorrent.in	filmeviatorrents.org
chachatv28.pro	dontorrent.tv	findaudiobook.com
chachatv35.pro	dooballfree24hr.com	fitgirl-repack.com
chachatv36.pro	dood.pm	flexyokay.com
chainsaw-man.net	downloadcrew.com	flvto.biz
chainsaw-man-manga.online	downloadgameps3.com	flvto.com.mx
chapmanganato.com	downturk.net	freelistenonline.com
clickndownload.org	dramaclub.com.br	freepcgamesden.com
clicknupload.cc	dramacool.cy	fshare.vn
clicknupload.club	dramacool.pa	ftv.bg
clicknupload.co	dramafansubs.net	futbol-tv.com
clip.ninja	drop.download	futebolgratis.net
clipconverter.cc	dropapk.to	futemax.link
cmp3.eu	dunia21.net	game-2u.com
codelist.cc	dunia21.pw	gamedva.com
codexpcgames.com	dvdcover.com	gamulator.com
coffeemanga.io	elamigos-games.com	getfvid.com
comiko.net	elamigos-games.net	getmetal.club
consoleroms.com	eleceed.me	getyarn.io
coolrom.com	e-reading-lib.com	gnula.life
coolrom.com.au	ez4mods.com	gofile.io
coworkcayman.com	eztv.yt	gofilmes.me
cracked-games.org	fakaza2018.com	grantorrent.wtf
crotorrents.com	fanseriesthaisub.com	hackstore.ac
darkscans.com	fastpic.ru	hackstore.re
daveplay.com	fbox.to	hackstore.rs
dbree.org	fbstreams.pm	hajime-noippo.com
descargamix.net	filehippo.com	harimanga.com
desiupload.co	filmebrasil.com	hd24bit.com
dizicaps.net	filmeserialeonline.org	hdmovies23.ws
dizigom1.com	filmesonlinehdgratis.com.br	hdonline.cc
dlpsgame.org	filmesonlinemax.com	hhpanda.cc
doballzod.com	filmesonlinex.me	hifimov.co

hiperdex.com	kunmanga.com	mavanimes.co
hiperfilmes.org	legendei.top	maxseries.in
hugball.net	lightnovelworld.com	mdzsmutpcvykb.net
hulkshare.com	likemanga.io	mediafire.com
idope.se	listnovel.com	medicostimes.com
ifunny.co	livestream247.pw	megacanais.com
ilgeniodellostreaming.online	lk21.dad	megafilmes.club
i-moviehd.com	lk21.pictures	megafilmeshd50.org
iptvsmarters.com	lk21official.wiki	megatorrent4k.com
isohunt.ch	lmp3.org	megatorrent4k.site
isohunting.com	loveflix.black	metal-tracker.com
issuu.com	loveflix.com.br	mgeko.com
itdmusics.com	loveflix.tv	miobt.com
itunemachine.com	luotphim1.net	mitom.bio
jamznet.com.ng	m3uiptv.com	mi-tom.net
jokerstream.co	m4uhd.net	mitom10.tv
juraganfilm.ink	machinenano.com	mitom15.com
juraganfilm.name	magazinelib.com	mitom15.tv
katmoviehd.ac	malavida.com	mitom5.com
katmoviehd.bz	mamahd.ws	mitom5.tv
katmoviehd.dad	mangaesp.net	mitom7.net
katmoviehd.day	mangakakalot.com	mitomb.tv
katmoviehd.dev	mangamovil.net	mitomc.tv
katmoviehd.ma	mangaqueen.com	mitomf.tv
katmoviehd.mov	mangaread.org	mitomk.net
kazesub.com	mangathailand.com	mitomt.tv
kazetori-manga.com	mangaus.xyz	mitomv.live
keepvid.works	manga-yaoi.com	mitomv.tv
kingsmanga.net	manhuaes.com	mitomx.tv
kinox.run	manhuafast.net	mitomz.tv
kinox.top	manhuazone.org	mixdrop.ag
kiss-anime.ws	manhwalist.com	mixdrop21.net
klikmanga.id	marcianotorrent.com	mixdropjmk.pw
komiku.com	marrontorrent.com	moddroid.co

moddroid.com	nsw2u.com	readcomicsonline.ru
mp3download.to	nsw2u.net	readdorohedoromanga.com
mp3teca.info	nswrom.com	readhxh.com
mreader.co	nung2hdd.com	readjujutsukaisen.com
multicanais.bet	officialkmspico.com	readlightnovel.today
multicanais.cl	okgoals.com	readmha.com
multicanais.plus	one2ball.net	readnovelfull.com
multicanais.wf	osreformados.com	reapertrans.com
musescore.com	otakudesu.cam	reddit-soccerstreams.com
musio.net.br	otakudesu.lol	repacklab.com
mydownloadtube.net	oyasumipunpun.com	repelis.net
myfreemp3juices.cc	pakvim.net	retrostic.com
myself-bbs.com	pcgamestorrents.com	rockdownload.org
mythethao.net	pdfcoffee.com	rojadirectenvivo.me
myvidster.com	pelisonline.me	romsdl.com
nabee-manga.com	pelisplus.so	roms-download.com
naijaonpoint.com	phimtho.net	romsdownload.net
nanamovies.me	phoneky.com	romsdroid.net
necromanga.com	pirlotv.site	romsever.com
netcine.bz	pirlotvonline.org	romsfun.com
netcine.cx	playtube.pk	romslab.com
netcine.rs	pobreflix.gg	ruslar.me
netcine.to	pobreflix.io	rutracker.ru
netcine.ws	pobreflix2.com	sakamotodayschapters.com
netcine3.la	protorrent.net	savetube.app
nexus-games.net	ps3r.com	seirsanduk.com
ngoaingu123.info	qquing.net	sendspace.com
nippyspace.com	r4i-sdhc.com	sendvid.com
novel5s.com	rakball.com	series2day.com
novelfull.com	rakhoic.tv	seriesblanco.com
novel-gate.com	rakhoit.tv	sharemania.us
novelhall.com	rakhoiz.net	sharetext.me
novels.pl	ranker-manga.com	shibamanga.com
novelzzz.com	readbeastars.online	skidrowcodex.net

skidrow-games.com	torrents2download.com	webcric.com
skymoviehd.net	tubidy.blue	webtoon.xyz
speedtorrent.com	tudoaovivo.com.br	westmanga.fun
sportvshdsonlinetv.com	tv247us.com	worldof-pcgames.net
sritown.com	tvonline.global	wplocker.com
starazi.com	uniondht.org	wrapk.net
streamees.com	up-4ever.net	x2convert.cc
strikeout.nu	upload.ee	xoilac.gg
suamusica.com.br	uploaddeimagens.com.br	xoilac365q.live
suatela.com	uploadfile.pl	xoilac87.tv
suatela.net	usaupload.com	xoilacz.net
subnhanhvl.co	userscloud.com	xoilaczc.tv
superfilmes.la	usersdrive.com	xoilaczz.tv
superfilmes.ph	uwatchfree.be	y2mate.blue
superflix.biz	varioscanais.com	y2mate.info
superflix.black	vebo12.tv	yalnizmp3.ws
superflix.rip	veboc.tv	yasdl.com
superpsx.com	vebot.live	youconvert.net
supertvaovivo.co	vebov.live	youdbox.site
supertvaovivo.tv	veboz.live	youtubemp4.to
super-warez.eu	veoh.com	youtubemultiplier.com
telamix.net	verfutebol.tv	youtubnow.co
temseries.online	verfutebol1.online	yt1s.io
terbit21.tube	vertvcable.com	yt2mp3.ws
terbit21.tv	videoindirxa.net	yt5s.com
thetowerofgod.com	videoindirxo.com	yts.autos
tlnovelas.net	video-to-mp3-converter.com	yts-subs.com
tmomanga.com	vimm.net	zamusic.org
todotorrents.net	vipleague.st	zippysharedjs.com
tokyoghoulre.com	wallpapercave.com	zpaste.net
toonthe.com	waploaded.com	
topstreams.info	war-forum.net	
torlock2.com	watchseriestv.top	
torrentproject2.net	weadown.com	

About Digital Citizens Alliance

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on the importance for Internet stakeholders— individuals, government, and industry—to make the Web a safer place. Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical, and creative industries, as well as online safety experts and other communities focused on Internet safety. Visit us at www.digitalcitizensalliance.org.

About White Bullet Solutions

Founded in 2013 by a leadership team of experienced Cybersafety and Intellectual Property lawyers from the media and advertising industries, White Bullet offers companies cyber risk data and protection, brand safety solutions, and full transparency on their advertising placement and digital supply chains. Piracy and malvertising are among the cyber risks addressed by the technology and solutions offered by White Bullet.

White Bullet works collaboratively with brands, policymakers, and the advertising industry to safeguard advertising spend and prevent ad placements from appearing on IP Infringing domains and apps. White Bullet is a certified brand safety anti-piracy solutions provider under the advertising industry regulator TAG and is a stakeholder to the EU Commission Memorandum of Understanding on Advertising and IPR.

About Unit 221B

Unit 221B, LLC focuses on products and services designed for selected clients, primarily those seeking discreet advanced cyber requirements and operations. We are comprised of unique specialists in the fields of information security, cryptography, forensics, legal, investigations, law enforcement, and intelligence.

digitalcitizens alliance

whitebullet

UNIT 221B
GUIDED BY INTEGRITY | DISCREET BY DESIGN