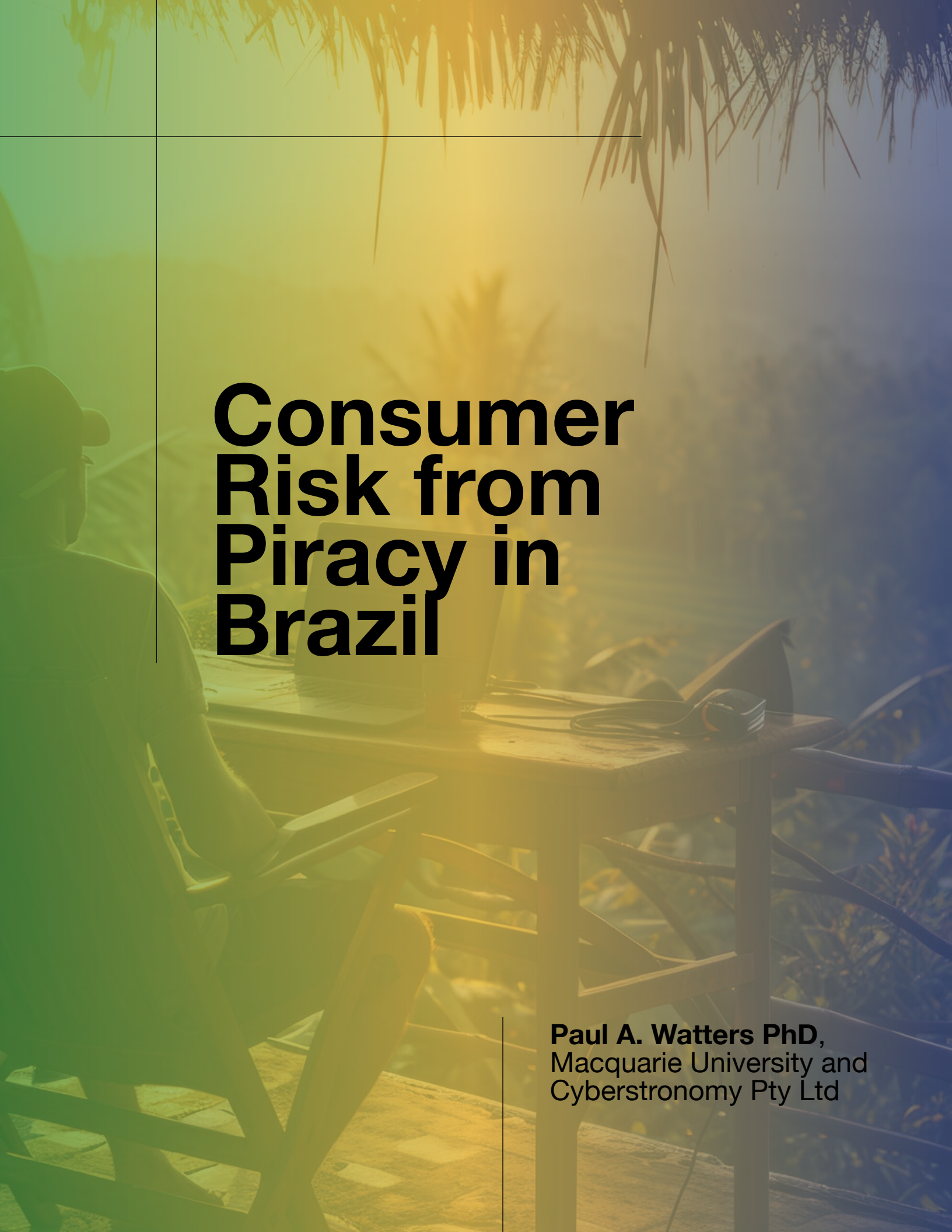


Consumer Risk from Piracy in Brazil

Paul A. Watters PhD,
Macquarie University and
Cyberstronomy Pty Ltd

Consumer Risk from Piracy in Brazil

Paul A. Watters PhD, Macquarie University and Cyberstronomy Pty Ltd

Executive Summary

This study examined the cybersecurity risks associated with digital services in Brazil. The objective was to quantify consumer exposure to malware, phishing, and fraudulent activity within piracy ecosystems, and to compare these risks with legitimate online environments. Across piracy service types, cyber risk was quantifiably pervasive. Even under conservative assumptions, Brazilian piracy portals were on average 29 times more likely to contain cyber threats than legitimate websites, and in the worst-case model, this average relative risk rose to over 54 times higher. P2P, followed by Anime and Scam sites, represented the highest-risk categories. All service types continued to show elevated risk, and none of the Brazilian piracy categories exhibited a safe or low-risk environment.

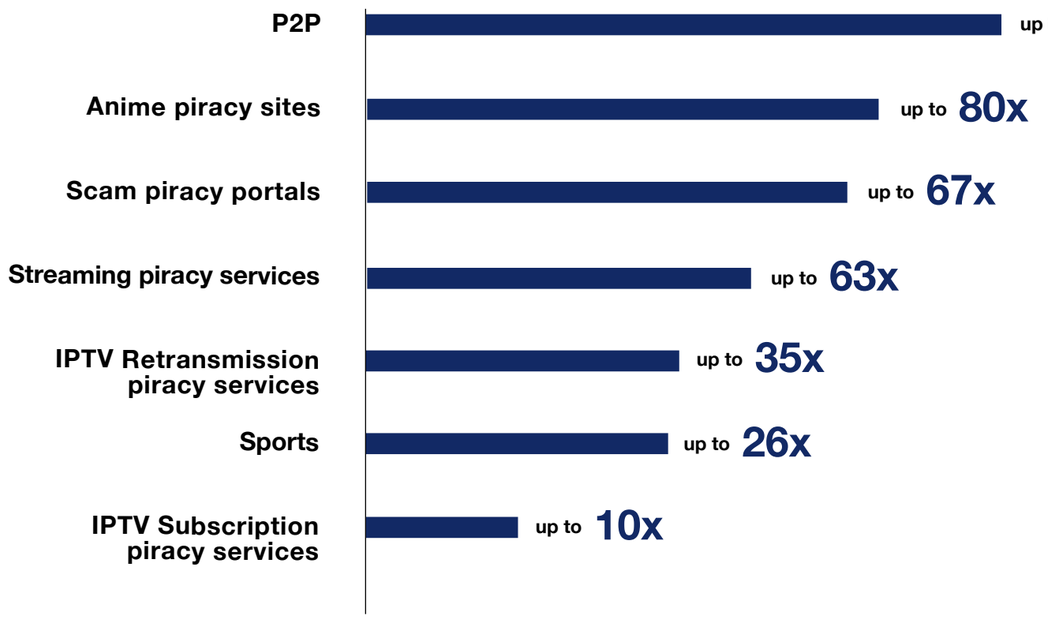
A further structural risk factor for digital piracy in Brazil is that a significant proportion of the Illicit Streaming Devices (ISDs) and associated backend services circulating in Brazil originate from China-based manufacturing and hosting hubs. Prior analyses show that many of these devices arrive with insecure firmware, backdoors, or embedded malware, creating opportunities for large-scale compromise at the point of entry into the Brazilian market. A national security risk is emerging in Brazil as a result of command and control service provision, linked to ISD and piracy websites.

The findings highlight that online piracy is no longer only an intellectual-property issue but a measurable cybersecurity threat vector, and a national security risk. High infection densities, combined with normalized consumer behavior, easy access to illicit devices, and exposure to a predominantly foreign (and frequently insecure) hardware supply chain, create conditions for mass compromise. A range of measures are proposed to reduce the impact of these risks.

Key Findings

Relative Risk of Encountering a Cyber Threat by Piracy Type

(Worst-Case, Brazil)
(All figures are 'up to x higher risk' compared to mainstream sites)



- **Relative Risk by Service Type**
  - » P2P networks: 100× higher risk than legitimate sites
  - » Anime piracy sites: 80× higher risk
  - » Scam piracy portals: 67× higher risk
  - » Streaming piracy services: 63× higher risk
  - » IPTV Retransmission piracy services: 35× higher risk
  - » Sports: 26× higher risk
  - » IPTV Subscription piracy sites: 10× higher risk
- **Overall Risk × 29.14:** In the best-case, consumers face on average more than a 29-fold increase in cyber-threat detections on piracy sites versus mainstream control sites.
- **Top-Risk Categories:** In the worst-case, P2P networks (100 detections), Anime (80 detections), and Scam portals (67 detections) carry the highest relative risks over legitimate sources.
- **Put simply:** There are almost no cyber risks on the most popular mainstream websites, but all piracy services show hugely elevated cyber risk.
- **Piracy Consistency:** Every piracy service category demonstrated elevated threats, with P2P, Anime, and Scam sites being the most consistently risky.
- **Country Pattern:** While legitimate sites are generally very safe, consumers using piracy services anywhere in Brazil are exposed to dramatically higher and preventable cyber risks.
- **Policy Implications:** These findings provide a robust evidence base for targeted policy reform, coordinated intervention, and deeper public-private collaboration. Given the stark disparity between mainstream and piracy platforms – enhanced enforcement and long-term coordinated action is strongly recommended to support legitimate commerce and protect consumers from malware, phishing, and other cyber threats linked to digital piracy.

Contents

01

Introduction

What is Digital Piracy?

Social and Economic Consequences of Piracy

Consumer Risks

A Cyber Threat Model for Digital Piracy

Cybercrime and Consumer Wealth in Brazil

Education, Capacity Building, and Public Awareness

Introduction

This research investigates the increasing consumer cybersecurity risks linked to digital piracy in Brazil. Rather than discussions centered on financial losses[1] and protecting intellectual property[2], this analysis reframes the piracy challenge primarily as a matter of consumer protection and national security. Modern digital piracy platforms serve not only as unauthorized media distribution channels, but as dangerous entry points for malicious software[3], identity theft[4], financial fraud[5], and data security breaches[6] that can impact business and government operations, often driven by Chinese infrastructure.

Over the last ten years[7], Brazil has experienced continuous expansion of piracy-related services[8], encompassing unauthorized sports and film streaming, anime websites, peer-to-peer networks, illicit IPTV subscriptions, and unauthorized software distribution. The piracy landscape has undergone substantial transformation[9] . What once involved desktop-based torrent applications and website advertisements has shifted toward feature-rich IPTV systems, piracy-based streaming memberships, and hidden distribution through private messaging platforms[10]. This swift development contributes to what experts describe as “piracy normalization” or “the cultural acceptance of piracy[11].” Yet this seeming ease of access masks increasing security risks for individual users and Brazilian society.

This research evaluates cybersecurity threat information linked to various piracy platforms operating across Brazil’s economy, establishing a foundation for focused prevention strategies – including policy changes, improved law enforcement, and public awareness campaigns. The investigation leverages empirical data collected locally and draws on previous work from a range of sources.

Previous global and regional research studies have exposed the significant extent of cyber threats confronting piracy users. Analyzing threat intelligence information from more than 95 security providers, Watters (2025)[12] discovered that throughout Asia-Pacific regions, piracy platforms were as much as 65 times more dangerous than authorized websites for malware, phishing, spam, and additional threats. The most dangerous platforms included P2P, scam, and unauthorized streaming services – reflecting trends that are clearly visible in Brazil as well.

Digital piracy services in Brazil function not simply as copyright-violating operations but as cybercrime distribution channels (often using Chinese infrastructure), merging fraudulent schemes with malicious ad delivery, credential phishing, and frequently direct fraud. Piracy-as-a-service operations in the area increasingly mimic authentic business models – though they often compromise user information, conceal malicious payloads, and actively finance organized criminal activity. In Brazil, piracy networks constitute a continuing and remarkably efficient pathway for malware dissemination, driven-by-downloads malicious software, and various forms of digital theft[13].

Within this framework, Brazilian consumers – a significant portion of whom are digitally engaged yet potentially lacking protection – encounter substantial and inadequately acknowledged cyber threats[14]. IPTV subscription services, anime websites, P2P networks, and deceptive “scam” platforms are widespread in Brazil, accounting for 56.25% of cybercrime incidents within the region[15].

The central research question is this: To what degree do piracy services in Brazil heighten cybersecurity risks to consumers, and what distinctive national factors intensify that risk? In addressing this, the report seeks to inform national cybersecurity strategies, policy and critically needed public education campaigns.

The International Intellectual Property Alliance (IIPA) highlights that industries founded on copyright produce significant employment and economic advantages – exceeding US $1.8 trillion in output and 9.6 million jobs across the wider region[16]. Expanding these advantages to Brazilian creative industries relies on more robust enforcement and equitable market access for legitimate content. In the absence of these measures, consumers turn to unregulated platforms, leaving themselves vulnerable to cyber threats while weakening domestic cultural production.

What is Digital Piracy?

Digital piracy denotes the unauthorized acquisition, reproduction, or distribution of copyrighted digital content without authorization or payment to rights-holders, utilizing a variety of protocols, devices and technologies[17]. Within the Brazilian context, this includes a broad spectrum of unauthorized content – encompassing audiovisual content – such as sports, films, television programming, and anime – obtained through unlicensed channels. The following categories identify the principal forms of piracy under examination in this study:

- **Sports Piracy:** Unauthorized platforms that broadcast live sports events, particularly football, through unregulated subscription pay-TV services or online broadcasts. These platforms frequently draw substantial regional audiences, especially during significant tournaments.
- **Streaming Piracy:** Platforms that deliver unauthorized access to films, series, and television content through ad-free streaming, frequently marketed as subscription or advertising-supported services. These may bear close resemblance to legitimate services but function entirely outside authorized frameworks.
- **IPTV Retransmission:** The unauthorized capture and redistribution of broadcast content – delivered via IPTV servers – without a consumer subscription arrangement.
- **IPTV Subscription Piracy:** Commercial piracy services providing bundled access to hundreds of unauthorized TV channels, video-on-demand libraries, and sports events.
- **Anime Piracy:** Websites that provide streaming or download access to Japanese animation without authorization, often utilizing fan-produced subtitles. These platforms frequently meet unaddressed demand in regions where authorized anime distribution is restricted or postponed.
- **P2P (Peer-to-Peer):** Decentralized file-exchange networks that enable users to upload and download pirated content – encompassing films, music, and games – directly from one user's device, frequently through torrent protocols.
- **Scam Piracy Sites:** Fraudulent platforms that entice users with offers of free or reduced-cost content but instead extract personal data, deploy malware, or conduct payment fraud operations. These may imitate legitimate – or pirate – services, and/or contain no actual media content.

Each of these modalities presents unique technical and consumer-facing dangers[18]. Collectively, they constitute a thoroughly embedded ecosystem that enables the distribution of pirated content in conjunction with malicious code, credential theft, and fraudulent payment schemes[19] – positioning Brazilian users at considerably heightened cybersecurity risk, often supported by Chinese infrastructure.

Social and Economic Consequences of Piracy

Digital piracy in Brazil reaches far beyond lost revenue – it fundamentally alters cultural expectations, disrupts creative economies, and undermines public confidence in digital services. A nation abundant in cultural production, Brazil relies on strong intellectual property frameworks to foster economic innovation and safeguard creative labor. Yet the pervasive normalization of piracy has generated systemic weaknesses, particularly among digitally engaged youth[20]. Based on the International Intellectual Property Alliance (IIPA, 2025), Brazil continues to be on USTR's Watch List due to ongoing online piracy and inadequate IP protection and enforcement[21]. Likewise, the Motion Picture Association (MPA, 2025) identifies Brazil as a market that persists in facing challenges related to IP enforcement – particularly the absence of an effective administrative site blocking mechanism – and market access constraints, such as quotas[22]. Although a new administrative site-blocking mechanism under ANCINE's authority has since been created, it has not yet entered into force.

SOCIAL CONSEQUENCES

Piracy in Brazil undermines the foundation of cultural development. When unlicensed content dominates the market, it erodes the value of local creative works, discourages domestic investment, and diminishes the perceived worth of Brazilian storytelling. The result is a distorted feedback loop: with fewer incentives to produce authentic content, creators retreat, and cultural diversity narrows[23].

Local content – ranging from indigenous-language programming to regional cinema – depends on audience engagement and commercial viability. Piracy undercuts both. The availability of unauthorized streams and downloads weakens respect for creative labor and reduces financial returns to artists, directors, and publishers. This threatens the preservation of unique cultural identities and undermines national media ecosystems[24].

Furthermore, youth surveys conducted in other regions indicate a generational transformation[25]: younger users are progressively perceiving piracy as acceptable, harmless, and even morally justified. As this mindset becomes established, it undermines public regard for copyright and legitimate digital participation. Research conducted globally has demonstrated that strong moral convictions against piracy correspond with reduced piracy rates[26]. The lack of robust ethical messaging in Brazilian digital policy may be facilitating the normalization of piracy.

ECONOMIC CONSEQUENCES

Piracy strips Brazil's creative industries of essential revenue, converting into employment losses, business failures, and reduced innovation. From musicians and animators to developers and production teams, the consequences of piracy are experienced at all stages of the content creation process. When legitimate sales decline, so does reinvestment into new and imaginative work[27].

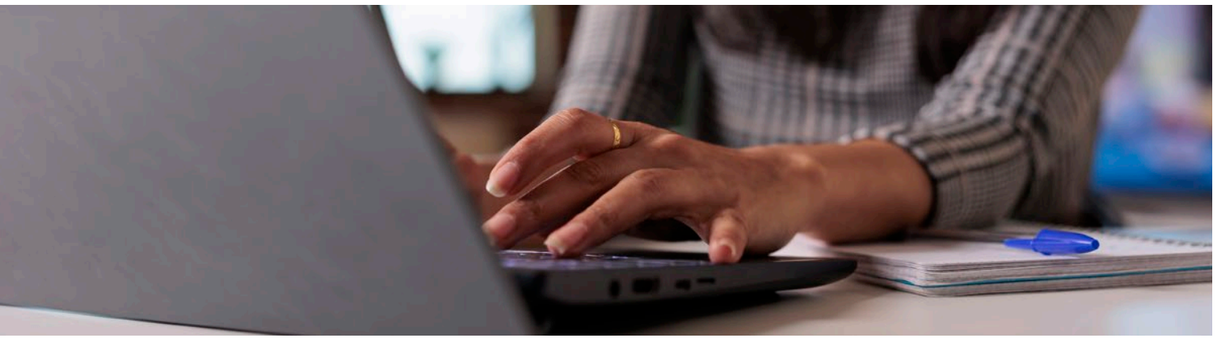
In the region, where national cinemas and music scenes are both thriving and susceptible, piracy has been connected to yearly losses extending into the billions[28]. As pirate IPTV subscriptions expand and advertising revenue moves to unlicensed platforms, governments also forfeit tax revenue – restricting funds for education, health, and cultural programs.

Legitimate services must also compete with pirate operations offering artificially low prices or "free" access. This distorts the market and disincentivizes innovation. Local entrepreneurs struggle to monetize their work, while multinational platforms may hesitate to invest in local content development in high-piracy jurisdictions[29].

In summary, digital piracy in Brazil is not merely a legal or financial challenge – it is a social and economic risk multiplier. Solutions must therefore address both enforcement and the deeper cultural norms that sustain piracy as an accepted digital behavior.

Consumer Risks

Brazilian consumers who utilize pirated services encounter significant cybersecurity dangers, particularly when processing payments or downloading content. A 2022 investigation by the Digital Citizens Alliance (DCA) in comparable markets revealed that one in ten credit card purchases on piracy platforms led to fraudulent charges within 30 days, indicating that cybercriminals frequently capture and sell card information for fraud or expensive purchases[30]. Many victims remain oblivious to the fraud until they review their financial statements – at which point they may have already experienced account freezes, chargebacks, or damage to their credit scores.



Piracy sites frequently disguise themselves as legitimate platforms, employing brand impersonation or copycat domains to establish a false impression of trustworthiness[31]. When these sites vanish or transform suddenly, users may forfeit access to purchased services and have their personal information transferred to third-party actors for spamming, scams, or other forms of harassment. The reputational harm also diminishes consumer confidence in legitimate digital services.

Based on research from multiple cybersecurity studies, the following risks are especially prevalent:

Malware & Drive-by Downloads

Simply visiting an illicit streaming site can trigger a drive-by-download, covertly installing trojans, worms, or keyloggers without user awareness. These intrusions may cause data corruption, backdoor access, or total system compromise.

Ransomware & Cryptojacking

P2P hubs and pirate APK repositories may distribute ransomware that encrypts personal files, demanding payment for release. Others secretly run cryptocurrency mining scripts, draining device performance and shortening hardware lifespan.

Phishing & Credential Theft

Fake login forms or fraudulent payment portals are deployed to harvest credentials – including banking logins, email access, and MFA codes. These can be stolen or exploited for identity theft, unauthorized purchases, and account takeovers.

Spyware & Data Exfiltration

Embedded spyware in cracked software or pirate mobile apps can monitor keystrokes, capture screenshots, or copy sensitive documents, covertly transmitting them to criminal operators or dark web brokers.

Botnet Recruitment & Network Compromise

Users who install compromised networking tools, ISDs or P2P clients may unwittingly join botnets used in cyberattacks (e.g., DDoS, malware spam), putting their own and others' devices at risk. A notable local example of this phenomenon is the Bigpanzi botnet, a Mirai-variant campaign targeting Android-based TVs and set-top boxes via *pandoraspear*. Researchers found that the botnet reached approximately 170,000 daily active bots at its peak, with the majority located in Brazil[32].

A recent technical analysis of ISDs shows how these compromised systems are also used as residential proxy nodes[33]. Devices such as EVPAD, UnblockTech 10 and SVI Cloud exhibited thousands of SOCKS5 handshakes, HTTP CONNECT tunnels, and other indicators of proxy operation, revealing that household internet connections were being silently rented out to third parties. Subsequent indicator-of-compromise analysis linked this behaviour to Chinese-hosted infrastructure associated with multiple malware operations. For Brazil, where non-approved TV boxes are widely available, similar exploitation would allow criminals overseas to “borrow” a Brazilian IP address when attacking banks, government services, or other domestic targets.

This convergence of piracy and cybercrime has been leveraged by organized crime syndicates, who progressively finance or manage piracy platforms as components of wider monetization operations[34]. These encompass ad fraud, fraudulent subscriptions, and malware distribution, frequently supported by established criminal infrastructures such as counterfeit goods networks. Earlier research in Brazil has demonstrated that advertising networks on piracy websites can directly monetize and enable criminal markets, including those connected with child exploitation material (Watters, 2015[35]). Many piracy platforms are also employed as conduits for money laundering, channeling illicit revenues through crypto mixers or shell firms.

These risks have been confirmed locally in ANATEL’s 2025 White Paper *Combate à Pirataria*[36], which provides one of the most detailed examinations of the consumer-security risks linked to unlicensed TV boxes sold in Brazil. The report’s analysis (pp. 30-36) shows that these illicit devices often come with malware already installed, hidden backdoors, and insecure update systems that let attackers take control of the device - and sometimes other devices on the same home network. ANATEL found that many of these boxes are used as part of botnets, steal passwords and personal data, and run silently even after the device is restarted. Since attackers can change the software remotely, these boxes can be used to access banking information, private documents, or photos stored on connected devices. These findings reinforce that the risks from piracy in Brazil go far beyond copyright issues and directly threaten consumer cybersecurity.

Recent Brazilian enforcement data highlight that the piracy ecosystem is embedded in a wider, largely China-centred hardware supply chain. ANATEL’s white paper notes that the great majority of illicit products originate from China, including ISDs. International network-measurement work on ISDs confirms the risk: traffic from devices such as the Unblock Tech 10 has been observed communicating directly with infrastructure operated by Chinese technology providers in Hong Kong and associated in VirusTotal with dozens of distinct malware families[37, 38]. Taken together, these findings suggest that a substantial share of the hardware and backend services enabling piracy in Brazil are tied to overseas manufacturing and hosting hubs in the People’s Republic of China, complicating purely domestic enforcement responses.

Recent enforcement patterns reveal the intensifying connection between organized crime and digital piracy. The MPA observes that these networks “capitalize on jurisdictional weaknesses and enforcement lag times to resurface under different domains within days,” leveraging cross-border infrastructure that frequently operates beyond the reach of individual national authorities[39]. Cooperative law-enforcement efforts in the region demonstrate initial success but face obstacles from varying legal definitions of online infringement and insufficient capacity for cross-jurisdictional evidence sharing.

Since these multinational criminal operations frequently span multiple jurisdictions and exploit enforcement gaps, traditional takedown and policing measures struggle to keep pace[40]. This reinforces the need for targeted consumer education, policy reform and regional cooperation on cybercrime enforcement.

A Cyber Threat Model for Digital Piracy

A cyber threat model offers a systematic approach to identifying, categorizing, and ranking how adversaries might compromise systems or services. It charts critical assets, weaknesses, attacker objectives, and probable attack pathways – allowing defenders to focus on the scenarios presenting the greatest potential harm.

Within the Brazilian piracy landscape, threat modeling reveals how criminal operators leverage unlicensed content platforms to distribute malware, harvest credentials, and penetrate users' residential and business networks. These environments merge international piracy patterns with regional characteristics including limited enforcement, elevated content pricing, and widespread adoption of inexpensive streaming hardware.

SITE OPERATORS

Site operators are the individuals or organized groups that construct and manage piracy platforms – whether web-streaming portals, IPTV services, or torrent indexes. Due to their control over the infrastructure, these operators can:

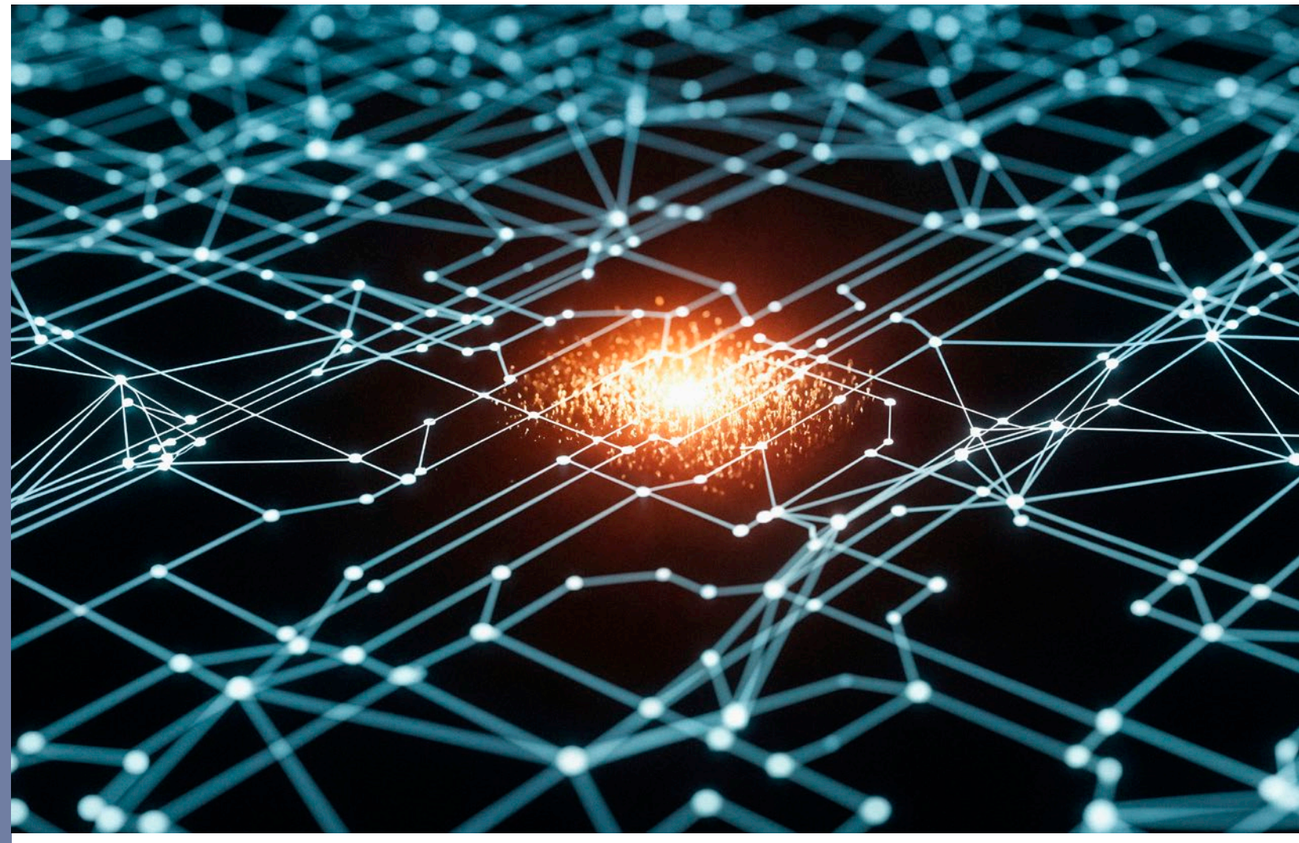
- Embed *drive-by* exploits within video players.
- Package trojans or spyware within client-side applications (such as Android TV APKs prevalent in Brazil).
- Push malicious updates via counterfeit “patches” or advertising networks.

Their command over the infrastructure provides the widest exposure: each visitor or subscriber faces potential covert payloads that deploy backdoors, cryptominers, or spyware without detection[41]. In the region, where IPTV devices and online telenovela streaming are extremely popular, these operators can impersonate legitimate local streaming services to avoid detection.

UPLOADERS

On P2P and Anime platforms, community contributors seed or host particular files. These participants may insert malware into seemingly legitimate media – inconspicuous packages, compressed archives (ZIP/RAR), or "cracked" media players – aware that users will extract and run these components on their own devices. Because users anticipate entertainment files, infections frequently remain hidden until systems are fully compromised. This indicates a substantial cognitive disconnect between perceived and genuine risk: numerous consumers view downloading or streaming pirated media as a low-stakes, everyday activity rather than a security concern. Survey data from more than 6,000 respondents across five Asia-Pacific nations revealed that while users identified piracy websites as the second-most significant source of malware risk (22.27%), substantial portions of the population continued accessing them routinely. The study additionally discovered that 31% of malware-infection variance could be accounted for by demographic and behavioral elements – especially limited risk awareness and routine access to piracy content[42].

These findings indicate that users function within mental frameworks where entertainment-related downloads seem routine and consequently perceived as harmless. Consumer behavior, influenced by expectation and habit, becomes the primary vulnerability factor – not simply the malware itself. IIPA (2025) emphasizes this behavioral aspect, encouraging governments to "invest in end-user education campaigns to strengthen consumers' understanding of the risks of accessing pirated content, including exposure to malware and phishing schemes"[43].



These conclusions correspond with the *Time to Compromise* research, which determined that users' routine interaction with piracy platforms – particularly when seeking entertainment content – generates cognitive blind zones. Consumers regard downloading or streaming pirated material as minimal-risk and commonplace, permitting infections to remain undetected until systems face compromise. Tackling these mental frameworks through digital literacy and risk-awareness initiatives would reduce the psychological distance between what users perceive and the genuine threat.

THIRD-PARTY INJECTORS

Third-party injectors are outside attackers who take advantage of shared advertising networks, widespread CMS plugins, and obsolete web frameworks employed by piracy portals. Their methods include:

- Malvertising to embed malicious advertisements.
- Cross-site scripting (XSS) to introduce JavaScript that steals cookies or diverts users to phishing pages and exploit kits.

These injectors frequently function separately from the site operators, employing automated mechanisms to breach multiple piracy portals at once. Their activities convert even relatively harmless illegal streaming platforms into delivery channels for credential theft, banking trojans, and drive-by downloads. Throughout Brazil, attackers have weaponized ad networks and cloud-hosting services to disseminate payloads or video codec updates.

SITE HACKERS

A fourth category of actors directly compromises the piracy platforms by breaching their servers to introduce or amplify harmful content. Many Brazilian piracy sites run outdated WordPress or Joomla installations with factory-default login credentials and insufficient security measures. These weaknesses create openings for hackers – whether sophisticated criminal organizations or amateur attackers – to:

- Take advantage of unpatched web application flaws (such as SQL injection and remote code execution vulnerabilities).
- Capture administrator passwords using phishing attacks or credential stuffing techniques.
- Gain elevated system access on poorly secured Linux or Windows machines to deploy rootkits or recruit servers into botnets.

The consequence is infection at the server level: even visitors accessing what appears to be an innocuous webpage may unknowingly download cryptominers, spyware, or be redirected to exploit kits. In certain scenarios, these compromised piracy platforms operate on infrastructure that is also used by legitimate ISPs or CDN providers, which creates broad attack surfaces and magnifies the threat across the region.

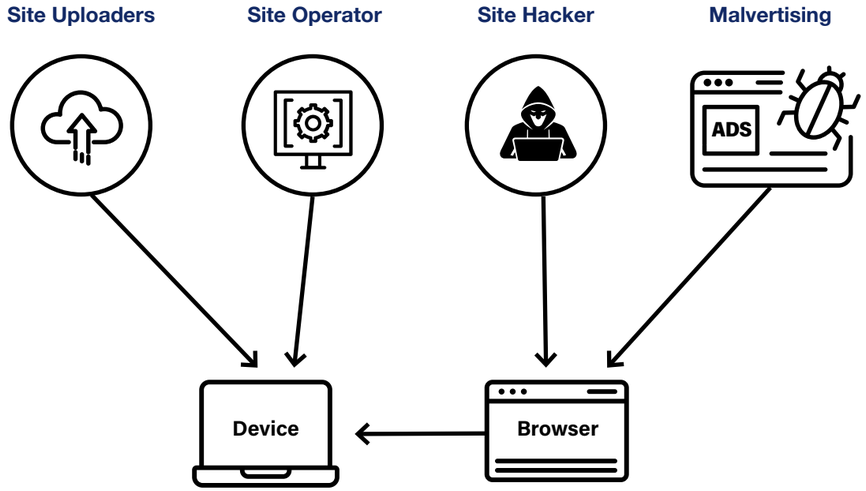
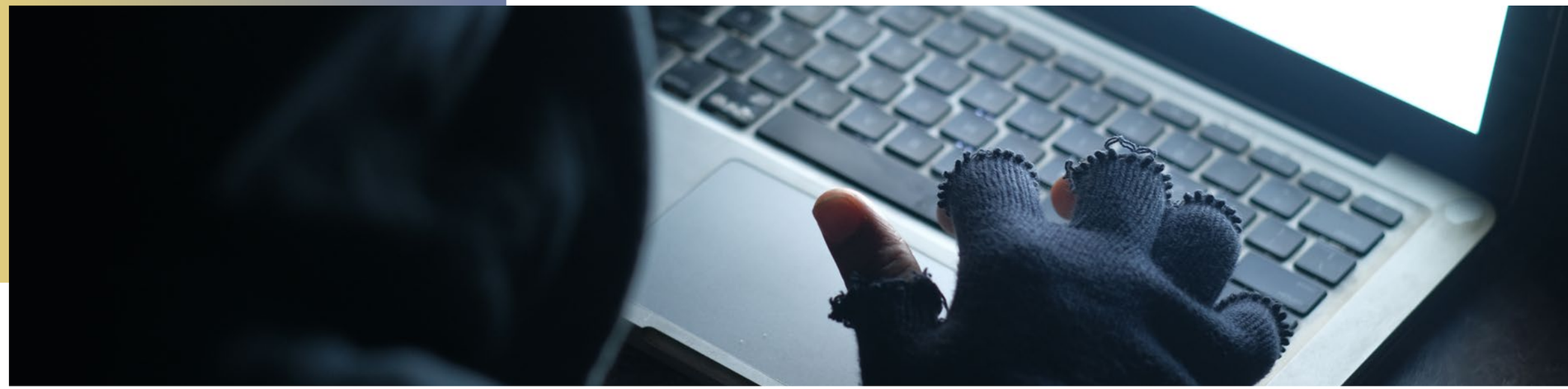


Figure 1 – Traditional Piracy Threat Model



Over recent years, Brazilian piracy has expanded from torrent swarms and advertisement-heavy websites to include ISDs – affordable “TV boxes” or USB dongles preloaded with unauthorized channels. These devices, broadly available through informal online marketplaces in Brazil, provide “direct-access” user experiences with minimal technical skills or lifetime fees, enabling access to premium sports, films, or telenovelas through what seems like a straightforward interface.

However, this ease introduces a more severe threat model (see Figure 2 - ISD Threat Model). Since ISDs run directly within home networks – frequently with administrator or root access – they can:

- Capture local network traffic and reach shared folders.
- Accept harmful code that deploys remote-access trojans or cryptojacking programs.
- Circumvent firewalls and antivirus software by appearing as legitimate devices.

A breached ISD can thus serve as a continuing entry point for attackers, turning laterally to laptops, NAS storage, or even children’s tablets connected to the same Wi-Fi network. The danger is especially pronounced: the Mirai botnet in 2016 demonstrated how devices globally, including ISDs, were enrolled into botnets, espionage operations, or ransomware attacks. This “camouflage” tactic – hiding malicious code within everyday firmware or update channels – converts what appears to be an innocent entertainment device into a dangerous cyber-threat vector. Table 1 provides a summary of threat actors.

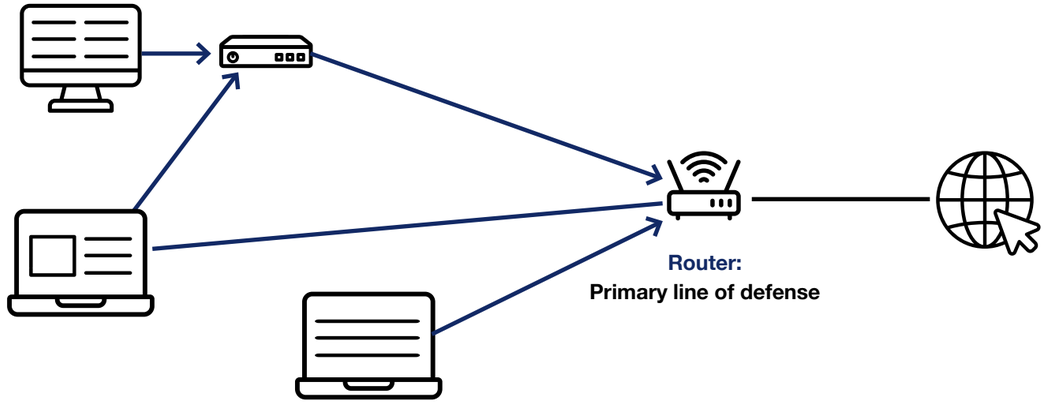


Figure 2 – ISD Threat Model – Undermining Bastion Defenses

Threat Actor	Primary Role	Attack Vectors	Consumer Impact
Site Operators	Develop, administer, and host piracy ecosystems (e.g., streaming portals, illicit IPTV services, torrent indexes).	• Drive-by exploits embedded in video players • Malicious APK files and forged update packages • Ad-network manipulation and injected scripts	System compromise through trojans, spyware, and cryptominers; high risk to all users accessing or subscribing to the service.
Uploaders	Provide and distribute files across P2P networks, anime sites, and torrent platforms.	• Malware hidden inside subtitle packs and compressed ZIP/ RAR archives • Compromised or cracked media players	Silent infections triggered during extraction or playback; delayed detection significantly increases overall risk.
Third-Party Injectors	Leverage advertising, affiliate networks, and plugin ecosystems connected to piracy sites.	• Malvertising campaigns • Multi-stage redirect chains leading to phishing sites • Bundled installers masquerading as legitimate tools	Credential theft, fraudulent payments, and unwanted software installations; exposure possible even without downloading piracy content.
Site Hackers	Breach piracy sites or seize control of their domains to weaponize them.	• SQL injection and cross-site scripting attacks • Domain takeover or DNS hijacking • Site defacement embedding malware payloads	Data breaches, deceptive phishing overlays, and forced botnet enrollment; victims rely on seemingly legitimate but compromised domains.

Table 1: Threat Actors in the Brazilian Piracy Ecosystems

Beyond simple malware behaviours, many ISD applications demonstrate capabilities associated with direct account compromise. Evidence from Malaysia[44] shows that numerous popular streaming apps engage in network discovery, credential access, log harvesting, and other MITRE ATT&CK–aligned techniques. In practical terms, this means that the same software used to stream pirated channels may also intercept authentication tokens, scan home networks, and exfiltrate sensitive data. When streaming services, payment details, or single-sign-on credentials are stored on an ISD, compromise of the device effectively grants attackers remote access to the user’s account environment, bypassing browser-level protections and multifactor prompts.

Cybercrime and Consumer Wealth in Brazil

As Brazil's digital connectivity and consumer purchasing power continue to grow, the country's online population has become an increasingly attractive target for cyber-criminal activity[45]. Several underlying factors amplify this vulnerability[46]:

- **High Internet and Mobile Penetration** - smartphone use in Brazil is exceptionally widespread, with 88.9% of residents aged over 10 owning a device[47]. The expansion of 4G- and increasingly 5G-coverage has positioned mobile phones as the dominant channel for digital access. This constant connectivity exposes users to a wide range of threats through banking apps, e-commerce platforms, and social networks, creating ideal conditions for phishing attempts, fraudulent promotions, and malicious links.

- **Rapid Digital Finance Adoption** - Brazil has emerged as a global leader in mobile payments and fintech adoption, driven by its large digital-banking customer base, the rapid nationwide uptake of the PIX instant-payments system, and a regulatory environment that actively encourages financial-technology innovation[48], but these advances also introduce new vulnerabilities. Criminals exploit cloned payment pages, counterfeit banking applications, and credential-stealing malware to intercept or divert financial transactions.

- **Expanding Middle Classes and Disposable Income** - Expanding wages, increasing online purchasing, and the widespread availability of digital marketplaces have made Brazilian consumers attractive targets for investment fraud, cryptocurrency scams, and subscription-based or "tech-support" cons. Organized crime groups routinely localize their schemes using Portuguese-language branding and references to trusted Brazilian institutions. Consequently, Brazil ranks 11th globally in consumer cyber-fraud complaints, according to FBI reporting[49].

- **Uneven Cybersecurity Awareness and Regulation** - Although Brazil has introduced several important data-protection and cybersecurity frameworks, implementation and public literacy remain inconsistent. Regional differences in institutional capacity and digital-hygiene education provide fertile ground for phishing campaigns, ransomware distribution, and identity-theft operations – particularly in communities with fewer resources or weaker local governance. Despite national initiatives such as the LGPD and the E-Ciber strategy, gaps in awareness and inconsistent enforcement continue to undermine Brazil's overall cyber-resilience.

- **High Use of Pirated and Unlicensed Services** - The persistent popularity of illicit streaming apps, IPTV devices, cracked software, and P2P platforms normalizes unsafe online practices. These ecosystems frequently distribute malware, spyware, and credential-harvesting adware, making them prime attack vectors for cybercriminal groups[50]. For example, Magis TV – one of many high-risk IPTV services – was targeted for blocking as part of Brazil's Operation 404, the country's flagship anti-digital-piracy initiative led by the Ministry of Justice and Public Security[51].

Operation 404 is the most extensive coordinated anti-piracy initiative in Latin America, with a particularly strong operational focus on Brazil[52]. Since its launch in 2019, successive phases have led to the blocking or dismantling of more than 3,000 piracy websites, mobile apps, and illicit IPTV services, often in partnership with law-enforcement agencies in the UK and the United States. In parallel, ANATEL has intensified its crackdown on *gatonet* ISDs, seizing more than one million uncertified TV boxes and tightening technical standards for all network-connected equipment imported into the Brazilian market[53].

In effect, piracy in Brazil not only undermines legitimate creative industries but also functions as a major conduit for cybercrime, erasing the boundary between casual consumer infringement and organized digital exploitation.

PROTECTIVE FACTORS IN BRAZIL'S CYBER POLICY AND REGULATORY RESPONSES

Governments and regulatory bodies have made considerable progress in establishing cybersecurity frameworks and data-protection regimes, yet the maturity and enforcement of these measures continue to vary substantially. These differences reflect uneven institutional capacity, shifting political priorities, and inconsistent regional cooperation. Brazil's most recent framework – the Estratégia Nacional de Cibersegurança (E-Ciber) – was formalized under Decree No. 12.573 on 4 August 2025[54]. This updated strategy builds on the earlier Política Nacional de Cibersegurança (PNCiber) and the Estratégia Nacional de Segurança Cibernética 2020-2023, providing continuity while setting new national priorities for cyber resilience.

E-Ciber is organized around four strategic pillars: strengthening citizen protection and digital awareness; enhancing the security and resilience of essential services and critical infrastructure; promoting public–private cooperation and systemic integration; and advancing national sovereignty and governance in cyberspace. Its priorities include improving Brazil's overall cyber-resilience, developing domestic technological capabilities, reducing reliance on foreign technologies, and expanding regulatory oversight of critical sectors. Implementation of the strategy is supported by the *Comitê Nacional de Cibersegurança* (CNCiber), a multi-stakeholder body comprising government agencies, civil society, academia, and industry representatives.

Collectively, these initiatives mark an important step toward institutionalizing cybersecurity governance in Brazil, even though challenges related to resourcing and consistent nationwide implementation remain.

LEGAL AND REGULATORY SAFEGUARDS

Brazil has introduced – and continues to refine – legislation aimed at criminalizing unauthorized system access, malware distribution, and online fraud. The country's Computer Crime and Cybercrime provisions are embedded within the Penal Code and associated laws:

- Lei No. 12.737/2012 ("Lei Carolina Dieckmann"[55]) criminalizes unlawful access to a computer device/network (art. 154-A of the penal code), installing vulnerabilities, and selling devices/programs to permit such access.
- The penal code (Decreto-Lei No. 2.848/1940) was amended by Law 12.737/2012 among others to include cybercrime-related offences (e.g., intrusion, sabotage).
- Additional Brazilian norms and regulatory instruments cover offenses such as illicit access to devices, system interference, denial-of-service attacks, and related forms of digital misconduct.

Despite this legislative progress, enforcement remains inconsistent. Many agencies still lack specialized cyber-forensics units, technical investigative capabilities, or judicial expertise needed to effectively pursue and prosecute cybercrime cases.

INSTITUTIONAL COLLABORATION AND CERT NETWORKS

Brazil has established a broad cybersecurity response architecture centered on CERT.br, the national CSIRT responsible for coordinating incident handling and issuing security advisories across both public and private sectors. Complementing this is CTIR Gov, the federal government's incident-response center, which monitors federal networks, manages cyber incidents affecting government systems, and supports the implementation of the national cybersecurity strategy (E-Ciber). Brazil also maintains several sector-specific CERTs and security operations centers – including in telecommunications, finance, and critical infrastructure – alongside the Cyber Defense Command (ComDCiber), which directs military cyber operations and national-level defensive activities. Collectively, these entities form a multi-layered cybersecurity ecosystem that strengthens incident response, resilience, and operational coordination across the country.

Regional cooperation is further supported through OAS-led initiatives, such as the Inter-American Cybersecurity Program, and through participation in the FIRST Latin America and Caribbean (FIRST-LAC) network, which promote capacity-building, joint exercises, and coordinated domain-takedown efforts.

Education, Capacity Building, and Public Awareness

Brazil's National Cybersecurity Strategy (E-Ciber) places substantial emphasis on strengthening the national cyber workforce through education, training, and professionalization. Human-capital development is identified as a central pillar of the strategy, which calls for the expansion of cybersecurity curricula, deeper partnerships with universities, increased investment in research, and the establishment of specialized training centers for professionals across both the public and private sectors. E-Ciber also underscores the importance of public-awareness campaigns and digital-citizenship initiatives to improve society's overall security posture. By pairing skills development with broader regulatory reforms, Brazil positions human capability as a critical foundation for long-term national cyber resilience.

02

Methods

Sample Design

Piracy Categories

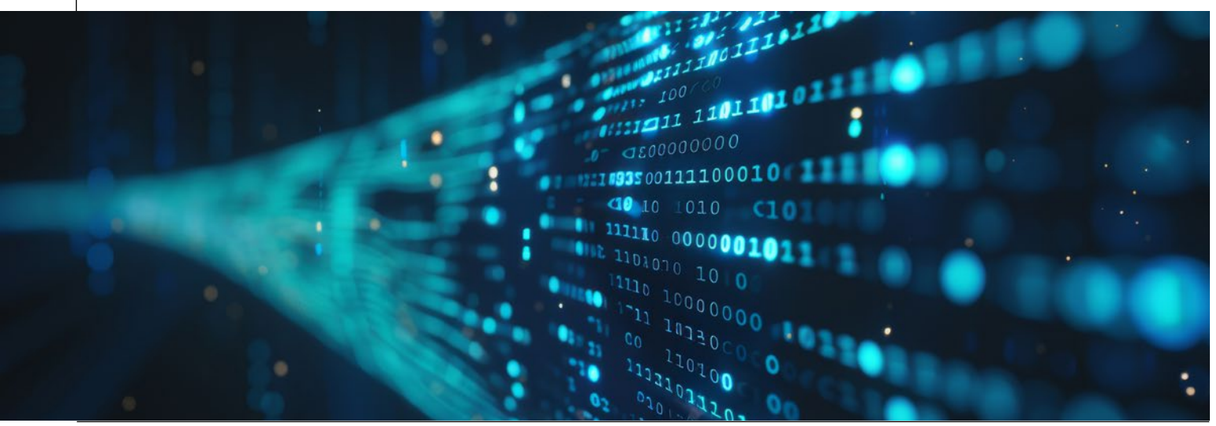
Data Collection and Analysis

Statistical Framework

Quality Assurance and Reproducibility

Methods

Data were collected from Brazil to assess consumer cybersecurity risks across major categories of piracy-related websites. The study employed VirusTotal, a Google-owned platform aggregating data from over 90 antivirus, sandbox, and threat-intelligence providers, to quantify and compare cyber risk indicators. VirusTotal's[56] multi-vendor analysis allows for a consistent, replicable approach to detecting malware, phishing, and other cyber activity across multiple jurisdictions.



Sample Design

The Alliance for Creativity and Entertainment (ACE)[57] and regional partners provided verified lists of active piracy websites operating in Brazil. These included both long-standing and emerging platforms known to distribute or promote unauthorized audiovisual content, IPTV services, and scam portals mimicking legitimate brands.

A sample of 30 piracy sites per category was selected from this list. Selection criteria emphasized verified operational status, accessibility from within Brazil, and sufficient user traffic (as observed through independent monitoring tools and ACE datasets).

For comparison, a control sample of 30 mainstream websites from Brazil was compiled using web-traffic data (via SimilarWeb, and other analytics sources) to represent the most-visited legitimate domains in each market, such as national portals, news outlets, e-commerce platforms, and government websites. Where overlap occurred between piracy and control samples, the next-ranked legitimate site was substituted. Domains associated with unrelated illicit activity (e.g., online gambling, adult content, or dark web services), or advertising networks, were excluded to preserve the integrity of the piracy–cyber risk comparison.

Piracy Categories

To reflect Brazil's distinctive piracy landscape, the study examined seven site categories:

1. **Sports** - Sites or streams rebroadcasting live sporting events (e.g., football, motorsport, boxing, or regional leagues such as CONMEBOL and Liga MX) without authorization.
2. **Streaming** - Portals offering unauthorized access to movies, TV series, or telenovelas via embedded players or direct-download links.
3. **IPTV Retransmission** - Sites distributing live broadcast feeds rebroadcast without rights, often using offshore servers or CDN-based delivery.
4. **IPTV Subscription** - Fee-based services selling channel bundles and VOD content through web dashboards or Android TV applications.
5. **Anime** - Portals hosting Japanese animation dubbed or subtitled in Portuguese without permission from rights-holders.
6. **P2P** - Peer-to-peer and torrent networks that enable downloading of unlicensed media files directly from other users.
7. **Scam** - Fake or deceptive sites impersonating legal streaming or IPTV services to harvest login credentials or payment details.

These seven categories represent a broad range of piracy distribution models and content foci active in Brazil and allow comparative measurement of consumer exposure to cyber threats.

Data Collection and Analysis

In total, 240 URLs were analyzed: 210 piracy URLs (30 per category across seven categories) and 30 control URLs. Each domain was scanned through VirusTotal's URL Analysis API, and the resulting detections were recorded across five standardized threat classifications:

- **Malicious** – Confirmed malicious behavior verified by one or more vendors.
- **Suspicious** – Heuristic detections of potential, but unverified, threat activity.
- **Phishing** – Credential-harvesting or impersonation attempts.
- **Spam** – Presence of intrusive pop-ups, adware, or unsolicited communications.
- **Not Recommended** – Distribution of potentially unwanted or unsafe applications.

For each site, vendor detections were consolidated, and results were aggregated by category, allowing computation of both absolute detection rates and relative comparisons.

Two bounding scenarios were applied:

- Best-Case Estimate: All detections from different vendors reflect the same underlying threat.
- Worst-Case Estimate: Each vendor detection represents a unique and independent threat event.

Statistical Framework

For each piracy category and control group, the mean number of detections were calculated. To measure comparative risk, a Relative Risk (RR) ratio was computed by dividing the mean detection count for piracy sites by that of the corresponding control sample. Where control samples recorded zero detections, a continuity correction (pseudo-count = 1) was applied to prevent infinite or undefined RR values – consistent with epidemiological and cybersecurity risk analysis standards.

Quality Assurance and Reproducibility

All scanning and data collection occurred during a fixed two-week period in November 2025 to minimize temporal variation in threat reporting. URLs returning HTTP errors (e.g., 404 or timeout) were replaced with the next most popular functioning domain within the same category and jurisdiction. Manual validation was conducted for both piracy and control samples to confirm domain categorization and accessibility prior to analysis.

03

Results

Cyber Threat Detections by Piracy Service Type (Tables 2 and 3)

Average Likelihood of Encountering a Cyber Threat (Tables 4 and 5)

Relative Risk of Encountering a Cyber Threat (Tables 6 and 7)

Results

To assess the cyber risk landscape associated with piracy services across Brazil, three complementary metrics were used: (1) Cyber Threat Detections, (2) Average Likelihood of Encountering a Cyber Threat, and (3) Relative Risk of Encountering a Cyber Threat.

- Cyber Threat Detections (Tables 2-3) quantify the total number of malicious, suspicious, or unwanted indicators identified across sampled piracy sites in both *worst-case* and *best-case* scenarios.
- Average Likelihood (Tables 4-5) normalizes these detections to the number of sites sampled, estimating the probability that a typical user will encounter one or more active threats during normal browsing activity.
- Relative Risk (Tables 6-7) compares the infection density of piracy sites with that of mainstream control sites, revealing how much more likely it is that a consumer will encounter malware or phishing content when visiting piracy portals rather than legitimate platforms.

Together, these measures provide a multi-layered understanding of cyber exposure in piracy ecosystems – capturing both *absolute threat volume* (Detections), *user-level exposure probability* (Likelihood), and *comparative safety differentials* (Relative Risk).

In summary, across all piracy categories, the average relative risk ranged from 29.14× in the best-case scenario to 54.43× in the worst-case scenario. This demonstrates that, regardless of modeling assumptions, piracy sites consistently expose users to markedly higher levels of malicious activity than mainstream websites.

Cyber Threat Detections by Piracy Service Type (Tables 2 and 3)

Across Brazil, all categories of piracy services displayed measurable levels of malicious activity (Tables 2-3). In the worst-case scenario, which treats every antivirus or reputation-vendor detection as a distinct threat, the highest average detections per 30 sites were recorded for P2P (100), Anime (80) and Scam sites (67). When adjusted to the best-case assumption, where multiple vendor detections on the same site are treated as a single underlying incident, the ordering of risk remained consistent. P2P, Anime and Scam sites continued to dominate the threat landscape (57, 39 and 34 respectively). Even under this conservative interpretation, all service types produced non-zero detection counts, confirming that the presence of active cyber threats is endemic in the Brazilian piracy ecosystems.

Piracy Service Type	Detections
Sports	26
Streaming	63
IPTV Retransmission	35
IPTV Subscription	10
Anime	80
P2P	100
Scam	67

Table 2 – Cyber Threat Detections by Piracy Service Type (Worst-Case)

Piracy Service Type	Detections
Sports	21
Streaming	29
IPTV Retransmission	18
IPTV Subscription	6
Anime	39
P2P	57
Scam	34

Table 3 – Cyber Threat Detections by Piracy Service Type (Best-Case)

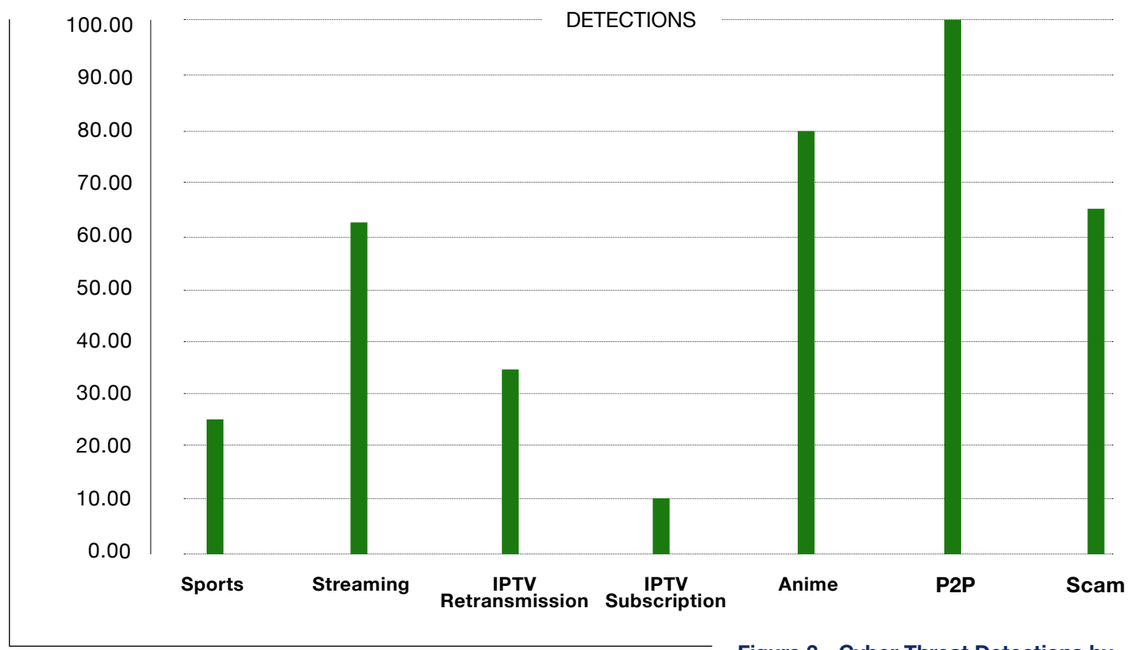


Figure 3 - Cyber Threat Detections by Piracy Service Type (Worst-Case)

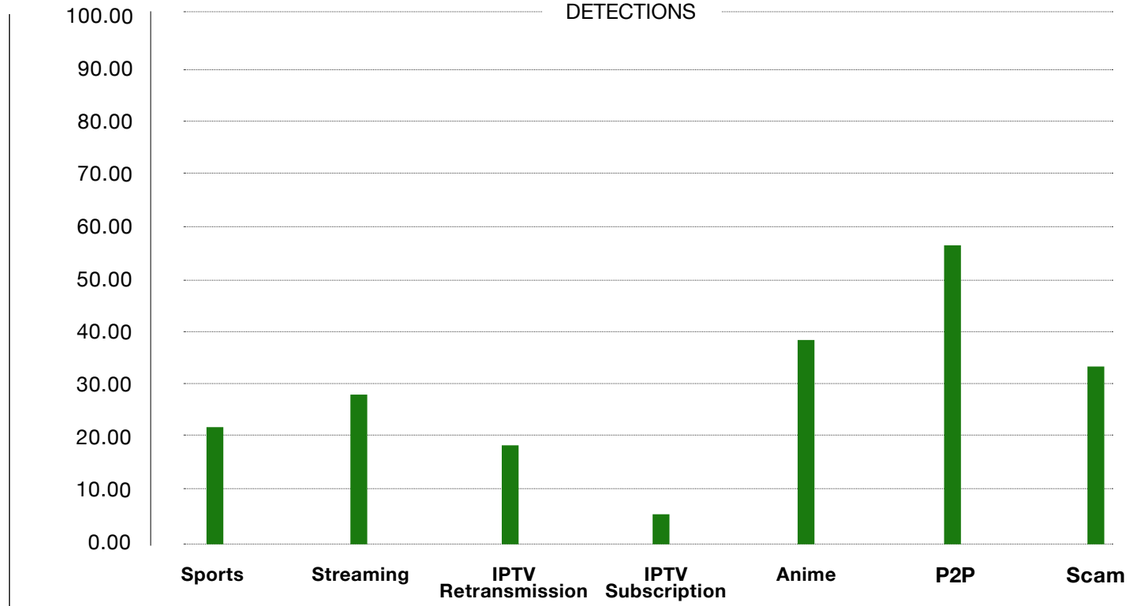


Figure 4 - Cyber Threat Detections by Piracy Service Type (Best-Case)

Average Likelihood of Encountering a Cyber Threat (Tables 4 and 5)

Normalizing detections by the number of sites sampled yields the average likelihood of encountering one or more flagged threats per 30 sites. In the worst-case analysis, users visiting P2P, Anime or Scam sites could expect an average likelihood of 3.33, 2.67 or 2.23 respectively. Even lower-volume categories such as IPTV Subscription (0.33) and Sports (0.87) displayed non-trivial exposure levels.

The best-case scenario produced similar relative ordering, though at reduced magnitudes. P2P remained the most hazardous (1.9 detections per 30 sites), followed by Anime (1.30) and Scam sites (1.13), demonstrating that even superficially inactive piracy portals pose ongoing infection risks. These findings reinforce that Brazilian consumers face a persistent baseline probability of compromise each time they access unlicensed media services.

Piracy Service Type	Average Likelihood
Sports	0.87
Streaming	2.10
IPTV Retransmission	1.17
IPTV Subscription	0.33
Anime	2.67
P2P	3.33
Scam	2.23

Table 4 – Average Likelihood of Encountering a Cyber Threat by Piracy Type (Worst-Case)

Piracy Service Type	Average Likelihood
Sports	0.70
Streaming	0.97
IPTV Retransmission	0.60
IPTV Subscription	0.20
Anime	1.30
P2P	1.90
Scam	1.13

Table 5 – Average Likelihood of Encountering a Cyber Threat by Piracy Type (Best-Case)

Relative Risk of Encountering a Cyber Threat (Tables 6 and 7)

Comparing piracy sites to matched control sets of the top 30 mainstream websites in Brazil highlights the magnitude of risk differentials. In the worst-case analysis, piracy platforms were many more times more likely to contain malicious or phishing payloads than legitimate sites. The highest relative risks were recorded for P2P (100×), Anime (80.00×), and Scam (67.00×).

Even in the best-case formulation, which assumes substantial duplication among vendor detections, the average relative risk remained much greater than that of control sites. P2P (57.00×), Anime (39.00×) and Scam sites (34.00×) persisted as the dominant risk categories. Scam piracy sites – domains that mimic the appearance of piracy portals but contain no genuine media content – exhibited risk ratios comparable to active distribution hubs, suggesting that these fraudulent sites now operate primarily as malware-delivery and credential-harvesting vectors rather than conduits for unlicensed streaming.

Piracy Service Type	Relative Risk
Sports	26.00
Streaming	63.00
IPTV Retransmission	35.00
IPTV Subscription	10.00
Anime	80.00
P2P	100.00
Scam	67.00
Average	54.43

Table 6 - Relative Risk of Encountering a Cyber Threat by Piracy Threat (Worst-Case)

Piracy Service Type	Relative Risk
Sports	21.00
Streaming	29.00
IPTV Retransmission	18.00
IPTV Subscription	6.00
Anime	39.00
P2P	57.00
Scam	34.00
Average	29.14

Table 7 - Relative Risk of Encountering a Cyber Threat by Piracy Threat (Best-Case)

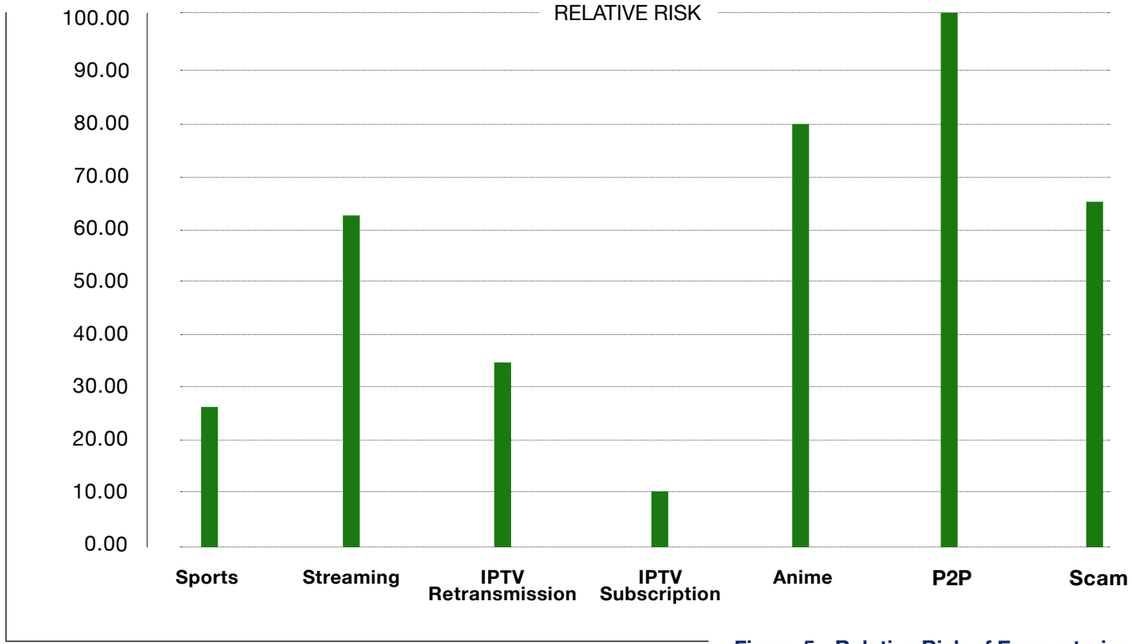


Figure 5 - Relative Risk of Encountering a Cyber Threat by Piracy Type (Worst-Case)

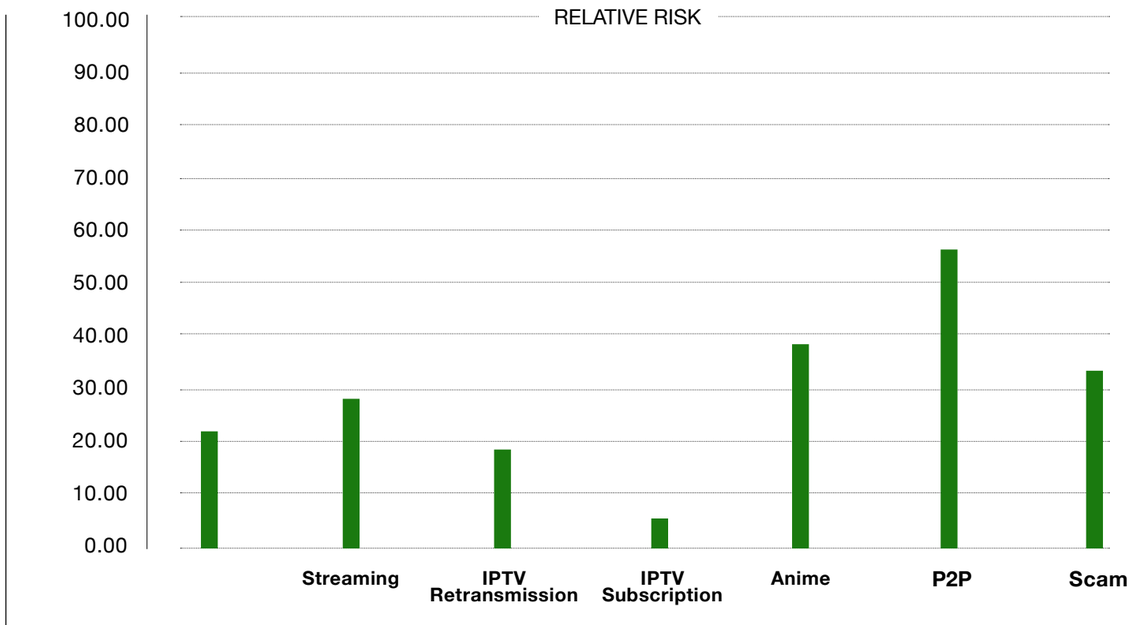


Figure 6- Relative Risk of Encountering a Cyber Threat by Piracy Type (Best-Case)

04

Discussion and Conclusions

Threat Composition and Attack Surface

Socio-Economic and Behavioral Drivers

Comparative Risk, Global Convergence, and the Role of Website Blocking

Behavioral Interventions and Demand-Side Mitigation

Consumer Risk and Policy Implications

Limitations and Future Work

Summary

Discussion and Conclusions

The findings demonstrate that Brazil's piracy ecosystem poses systemic and sustained cybersecurity risks to consumers. Across all service types examined, each category exhibited active or latent threats. Even under conservative, best-case modeling, users remained significantly more likely to encounter malware or phishing material on piracy platforms than on legitimate services. These patterns closely align with results observed in Southeast Asia, suggesting a common and globally converging threat landscape in which piracy and cybercrime are increasingly inseparable.

Threat Composition and Attack Surface

The prominence of P2P and Streaming platforms as high-risk vectors reflects both their underlying technical design and their widespread consumer adoption. P2P networks inherently expose users to executable files, unverified archives, and community-distributed content, creating ideal conditions for malware insertion. Streaming portals, meanwhile, depend on embedded media players and advertising-exchange frameworks that enable malvertising, drive-by exploits, and credential-harvesting mechanisms.

Equally important is the growth of Scam piracy sites-domains that mimic illicit streaming services but provide no actual content. These sites function instead as lures for payment fraud, data extraction, and forced malware redirection. Their elevated risk ratios illustrate how cybercriminals increasingly weaponize user expectations of “free” access, turning deception itself into a scalable mode of cybercrime. Free, ad-free piracy services create an illusion of safety, but their lack of visible monetization often signals more opaque - and harmful - business models. When a device or service presents no advertising and no subscription fees, the operator frequently monetizes users through hidden channels such as residential proxying, data harvesting, or pre-installed malware. In this sense, the absence of ads should be treated not as a reassurance but as a red flag indicating that the user’s bandwidth, data, or device integrity may be the product being sold.

Previous research into piracy-linked advertising networks has shown that these ecosystems often intersect with criminal infrastructures responsible for distributing exploitative material, reinforcing the conclusion that piracy services now operate as multi-purpose cybercrime platforms (Watters, 2015)[58].

Socio-Economic and Behavioral Drivers

Piracy in Brazil operates within a landscape shaped by strong consumer demand for entertainment and near-universal mobile connectivity. For many users, the cost of licensed streaming services remains prohibitive, while the widespread use of Android-based smart TVs and smartphones facilitates the rapid installation of unlicensed applications. These factors collectively sustain a large and receptive market for IPTV and P2P alternatives.

Behavioral norms further amplify these risks. The widespread social acceptance of piracy – coupled with a perception that accessing unlicensed content carries minimal personal consequence – reduces user attention to site legitimacy and file provenance. Many individuals disable security protections, disregard browser warnings, or install “cracked” applications that surreptitiously deliver malware. As a result, even brief or low-level exposure can escalate into full system compromise, particularly in contexts where endpoint security and patching practices are weak.

Comparative Risk, Global Convergence, and the Role of Website Blocking

The relative-risk ratios identified in Brazil closely mirror those documented in Southeast Asia, indicating that piracy-linked cybercrime has evolved into a globalized illicit service economy. The recurrence of identical hosting infrastructures, advertising-network identifiers, and malware signatures across regions suggests extensive cross-border reuse – and potentially common operator groups.

These patterns underscore the value of network-level disruption as a defensive strategy. As demonstrated by Herps et al. (2025)[59], rapid and systematic blocking of piracy domains – coordinated among rights holders, ISPs, and cybersecurity regulators – can produce measurable cybersecurity gains. Their analysis showed that sustained blocking of high-risk piracy sites corresponded with significant reductions in national malware infections and phishing incidents.

In the Brazilian context, similar interventions could yield comparable benefits. Proactive, targeted blocking of scam and malware-serving domains would reduce user exposure while complementing traditional copyright enforcement. Strengthened regional cooperation between CERTs and telecommunications regulators could further enhance resilience, reframing what is often viewed as a copyright measure into a broader public-interest cybersecurity initiative.

Behavioral Interventions and Demand-Side Mitigation

While technical controls can restrict access to harmful domains, behavioral interventions are equally important for addressing the underlying demand for piracy. Emerging findings from deterrence research and human–computer interaction indicate that real-time, context-aware messaging – such as pop-up warnings, interstitial notices, and automated chatbots – can meaningfully influence user decision-making at moments of heightened risk[60].

Automated systems have been deployed in other online-harm contexts, including fraud and child-exploitation prevention, where they combine legal cues, moral framing, and pathways to legitimate alternatives to interrupt harmful behavior. Applied to piracy, similar interventions could notify users when they attempt to access or download from known high-risk domains, highlighting the associated cybersecurity and privacy risks rather than relying on moral or punitive messaging.

Chatbots, for instance, could engage users in brief conversational prompts that redirect them toward legitimate streaming options or public-awareness resources – a model currently being evaluated in cyber-safety initiatives for adolescent users[61]. When deployed alongside blocking and takedown measures, such “soft-deterrence” strategies may reduce repeated exposure to malicious piracy environments while avoiding punitive enforcement, aligning with a harm-reduction approach to digital safety.

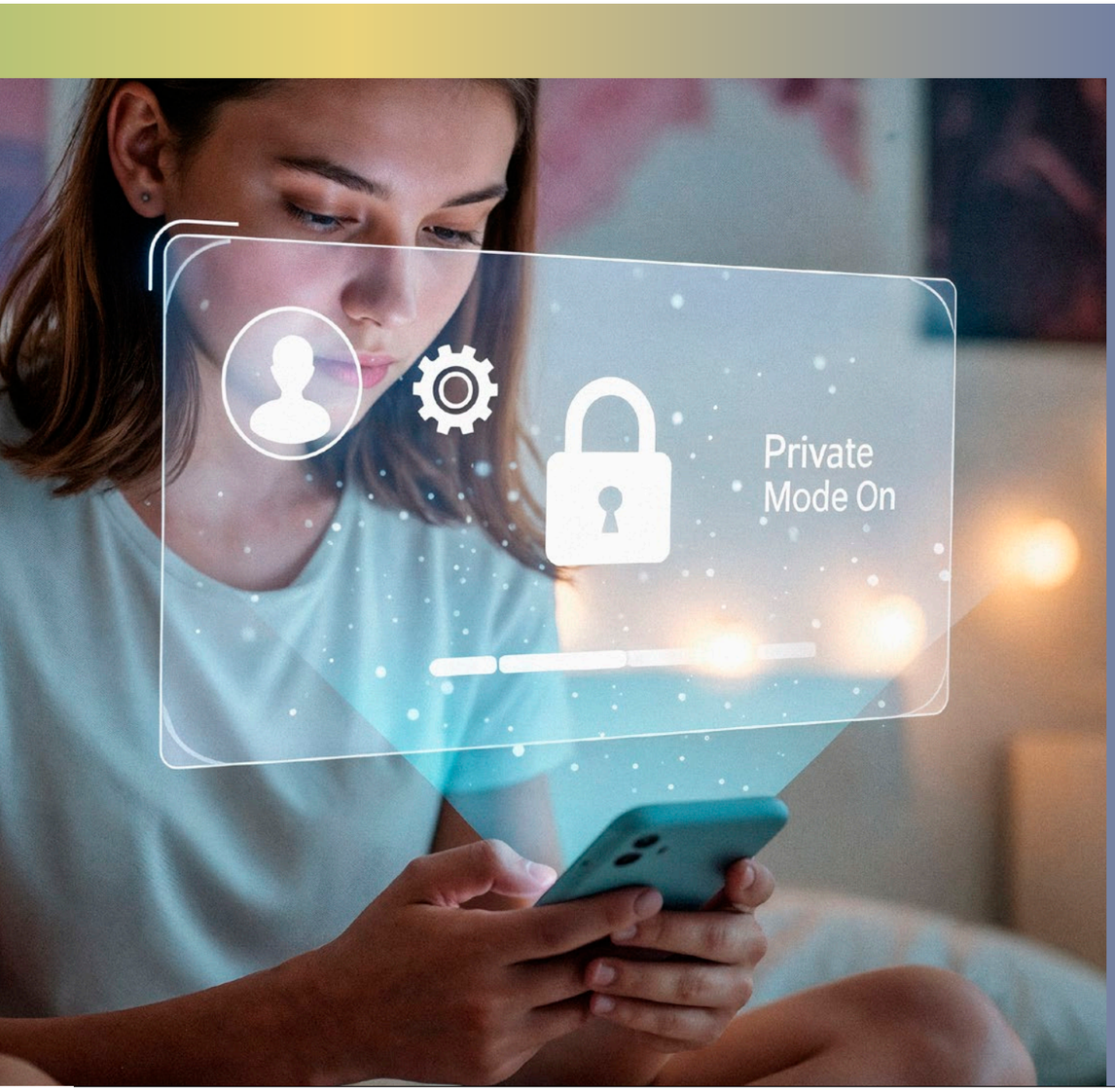
Consumer Risk and Policy Implications

The consistently high levels of cyber risk observed across Brazilian piracy ecosystems provide a strong rationale for treating site blocking not only as a copyright-enforcement tool but also as a consumer-protection and cybersecurity measure. Evidence from APAC markets demonstrates that proportionate and transparent site-blocking regimes can materially reduce national exposure to malware, phishing, and scam infrastructure. Although Brazil has established an administrative site-blocking mechanism under ANCINE, it has not yet entered into force; activating and embedding this capability within a broader cybersecurity strategy would substantially enhance consumer safety and reduce systemic risk.

The findings show that piracy exposure is not merely incidental to copyright infringement but constitutes a direct and significant cyber-safety threat. High threat densities across Brazilian piracy categories translate into widespread exposure to credential theft, spyware, financial fraud, and scam portals designed solely to harvest data or distribute malware. This evolution indicates that much of the piracy ecosystem now functions primarily as a cybercrime distribution infrastructure rather than a cultural or moral phenomenon.

Accordingly, Brazil's policy framework should expand beyond intellectual-property enforcement to incorporate consumer protection, digital resilience, and national security objectives. Consistent with Herps et al. (2025), rapid

blocking of verified malicious piracy domains should be recognized as a cybersecurity intervention, supported by strengthened digital-forensics and cyber-incident-response capabilities. Complementary behavioral measures - such as warning messages, chatbots, and targeted digital-literacy initiatives - can further reduce harm by making cyber risks salient to users. Collectively, these measures would lower exposure to malware, phishing, fraudulent payment capture, and large-scale device compromise, thereby protecting digital citizens and supporting Brazil's expanding digital economy.



Limitations and Future Work

As with previous regional studies, this analysis uses VirusTotal detection aggregates as a proxy for active compromise. Although this approach is effective for large-scale comparative assessment, variations in vendor signatures and sampling biases may affect measurement precision. In addition, the study does not examine closed IPTV subscription ecosystems, encrypted messaging channels, or private social-media groups, all of which constitute important components of Brazil's broader piracy environment.

Future research should incorporate behavioral data – such as user reactions to warning messages or chatbot interventions – to assess the real-world effectiveness of deterrence mechanisms. Longitudinal evaluation of national blocking initiatives, following the methodology employed by Herps et al. (2025), could further quantify reductions in malware infection rates and phishing victimization. When complemented by dynamic malware-execution analyses, such work would offer a more comprehensive understanding of both the technical and human factors that shape piracy-related cyber risk.

Summary

Brazil's piracy ecosystem reflects the same structural vulnerabilities, monetization patterns, and infection vectors seen globally. The findings show that the associated cyber risks are predictable and, importantly, reducible through coordinated intervention. Prior research demonstrates that decisive and sustained domain blocking can substantially limit consumer exposure, while behavioral deterrence mechanisms –such as warning systems and chatbots – provide scalable, non-punitive tools for influencing user behavior. Together, these approaches reinforce that effective piracy mitigation is not solely a copyright concern but a broader cybersecurity and public-safety priority.

Both the IIPA and MPA note that enhanced enforcement coordination across the region has produced early gains. However, long-term deterrence will require more harmonized legal frameworks, stronger judicial follow-through, and deeper public–private collaboration. The MPA contends that "light-touch regulation of digital services," combined with dynamic site-blocking and notice-and-stay-down mechanisms, offers an efficient balance between supporting legitimate commerce and protecting consumers. Embedding these models within Brazil's wider cybercrime and consumer-protection policies would allow authorities to reposition anti-piracy enforcement as an integral component of national digital resilience, rather than treating it solely as an intellectual-property or trade matter.

05

Bibliography

Bibliography

1. Rodriguez Ovejero, J. M., Stammati, L., & Torres Figueroa, M. P. (2019). The impact of piracy on the structure of the Pay TV market: a case study for Latin America. *Journal of Media Business Studies, 16*(1), 40-57.
2. Robertson, C. J., Gilley, K. M., Crittenden, V., & Crittenden, W. F. (2008). An analysis of the predictors of software piracy within Latin America. *Journal of Business Research, 61*(6), 651-656.
3. Kumar, Svrana, et al. “Malware in pirated software: Case study of malware encounters in personal computers.” *2016 11th International Conference on Availability, Reliability and Security (ARES)*. IEEE, 2016.
4. Telang, R. (2018). Does online piracy make computers insecure? evidence from panel data. *Evidence from Panel Data (March 12, 2018)*.
5. Creative Content Australia & SARA (2024). *Australian piracy behaviours and attitudes 2023: Wave 15 adults* (Anti-Piracy Tracker 2023). Creative Content Australia. https://creativecontentaustralia.org.au/wp-content/uploads/2024/07/SARA-CCA-Anti-Piracy-Tracker-2023_Published.pdf
6. Putman, P. (2025). *The consequences of digital piracy*. US CyberSecurity Magazine. Retrieved November 8, 2025, from https://www.uscybersecurity.net/digital-piracy/
7. Kigerl, A. C. (2013). Infringing nations: predicting software piracy rates, BitTorrent tracker hosting, and P2P file-sharing client downloads between countries. *International Journal of Cyber Criminology, 7*(1). http://www.cybercrimejournal.com/IJCC-January-June-2013-Vol7-No1.php
8. BB Media. (2025, February 18). More than 24 million homes watch pirated content in LatAm. *TodoTVNews*. Retrieved from https://www.todotvnews.com/en/more-than-24-million-homes-watch-pirated-content-in-latam/
9. Office of the United States Trade Representative. (2024, January). *2023 Review of Notorious Markets for Counterfeiting and Piracy*. https://ustr.gov/sites/default/files/2023_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy_Notorious_Markets_List_final.pdf
10. Locke, L., Chalkias, I., Yucel, C., Henriksen-Bulmer, J., & Katos, V. (2023). *Investigating IPTV malware in the wild. Future Internet, 15*(10), 325. https://doi.org/10.3390/fi15100325
11. Belchior-Rocha, H., Arslan, A., & Yener, S. (2024). *Unveiling the ethical dilemmas of digital piracy: A comprehensive exploration of motivations, attitudes, and behaviors. Social Sciences,* 13(11), 579. https://doi.org/10.3390/socsci13110579
12. Watters, P. (2025). *Consumer risk from piracy in Southeast Asia*. SSRN. https://ssrn.com/abstract=5371543
13. Danaher, B., Smith, M. D., & Telang, R. (2020). *Piracy Landscape Study: Analysis of existing and emerging research relevant to intellectual property rights (IPR) enforcement of commercial-scale piracy* (USPTO Economic Working Paper No. 2020-02). SSRN. https://ssrn.com/abstract=3577670
14. Diao, H., & Vergara Cobos, E. (2024). *Cybersecurity Economics for Latin America and the Caribbean (Preliminary Version)*. The World Bank. https://documents1.worldbank.org/curated/en/099011925184519084/pdf/P179481-5515e6c4-1d69-444d-a057-744edce07402.pdf
15. Flor-Unda, O. (2023). *A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America*. Informatics, 10(3), 71. https://doi.org/10.3390/informatics10030071
16. International Intellectual Property Alliance. (2025). *2025 Special 301 Report on copyright protection and enforcement.* Washington, DC: IIPA. https://www.iipa.org/reports/special-301-reports
17. Huang, K., Zhang, K., Chen, J., Sun, M., Sun, W., Tang, D., & Zhang, K. (2021). Understanding the Brains and Brawn of Illicit Streaming App. *In International Conference on Digital Forensics and Cyber Crime* (pp. 194-214). Cham: Springer International Publishing.
18. Delos Santos, M. S. V., Etorma, A. D., Ocampo, H. A., Panjaitan, A. E., Romualdo, J. M. B., & Blancaflor, E. B. (2022). Risk Analysis of Home User’s Vulnerability to Illegal Video Streaming Platform. In *Proceedings of the 4th International Conference on Management Science and Industrial Engineering* (pp. 365-372).
19. Ntsama, J. E., Tchakounte, F., Tchakounte Tchuimi, D., Faissal, A., Fotso Kuate, F. A., Effa, J. Y., Udagepola, K. P., & Atemkeng, M. (2023). *Determinants of Cybercrime Victimization: Experiences and Multi-stage Recommendations from a Survey in Cameroon*. In R. A. Saeed, A. D. Bakari & Y. H. Sheikh (Eds.), *Towards new e-Infrastructure and e-Services for Developing Countries* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 499, pp. 317-337). Springer.
20. Alex, P. (2013). *Piracy and the digital revolution in Latin America: Cultural consumption and resistance. International Journal of Cyber Criminology*, 7(1), 1–15.
21. International Intellectual Property Alliance. (2025). *2025 Special 301 Report on copyright protection and enforcement*. Washington, DC: IIPA. https://www.iipa.org/reports/special-301-reports
22. Motion Picture Association. (2025). *Submission for the 2026 National Trade Estimate Report on Foreign Trade Barriers*. Washington, DC: MPA
23. Belchior-Rocha, A., et al. (2024). Unveiling the Ethical Dilemmas of Digital Piracy. *Social Sciences, 13*(11), 579.
24. Inter-American Development Bank. (2022). *Intellectual Property Rights and Public Policies for the Creative Economy in Latin America and the Caribbean: Recommendations*. Washington, DC
25. Yoon, C. (2011). Theory of planned behavior and ethics theory in digital piracy: An integrated model. *Journal of Business Ethics, 100*(3), 405–417.
26. Phau, I., Lim, A., Liang, J., & Lwin, M. (2014). *Engaging in digital piracy of movies: a theory of planned behaviour approach. Internet Research, 24*(2), 246-266
27. Terra, A. (2016). Copyright law and digital piracy: an econometric global cross-national study. *NCJL & Tech., 18*, 69.
28. ConvergenciaLatina. (2024). Online content distributors miss out on up to US $1.3 billion a year due to piracy in the region. ConvergenciaLatina. https://www.convergencialatina.com/Section-Analysis/360046-3-52-Online_content_distributors_miss_out_on_up_to_US_1_3_billion_a_year_due_to_piracy_in_the_region
29. Parks Associates. (2023). *Consumer attitudes toward piracy* [Research report]. Parks Associates. https://www.parksassociates.com/storage/medias/7574f23a52abca4389d60fff00ff78ac10553e131f93f9fd6f06c80183158588.pdf
30. Digital Citizens Alliance. (2023). *Giving piracy operators credit: How signing up for piracy subscription services ratchets up the user risk of credit-card theft and other harms*. https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Giving-Piracy-Operators-Credit.pdf
31. Fortra. (2023). *2023 Domain Impersonation Report*. Fortra. https://static.fortra.com/corporate/pdfs/other/fta-domain-impersonation-report-2023.pdf
32. Qi An Xin X-Lab. (2023). *Bigpanzi exposed: The hidden cyber threat behind your set-top box*. Qi An Xin X-Lab. https://blog.xlab.qianxin.com/bigpanzi-exposed-hidden-cyber-threat-behind-your-stb/
33. Watters, P. (2025). *Residential proxying and illicit streaming devices* (SSRN Scholarly Paper No. 5767282). Social Science Research Network. https://doi.org/10.2139/ssrn.5767282
34. Robertson, H., & Fooks, J. (2021). *Taking the profit out of intellectual property crime: Piracy and organised crime networks and individual offenders*. Royal United Services Institute. https://static.rusi.org/whr_ip_crime_web_version_0.pdf
35. Watters, P. A. (2015). *An analysis of piracy website advertising in Brazil and its linkages to child exploitation material.* Bangkok, Thailand: ECPAT International. Retrieved from https://ecpat.org/wp-content/uploads/2021/05/Piracy-Website-Advertising-in-Brazil_ENG.pdf
36. Agência Nacional de Telecomunicações. (2025). *White paper: Combate à pirataria – Riscos, impactos e ações regulatórias*. ANATEL. https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-lanca-white-paper-e-reforca-compromisso-com-a-seguranca-dos-usuarios
37. Watters, P. (2024). Cybersecurity risks from illicit streaming devices in Taiwan (SSRN Scholarly Paper No. 4986107). Social Science Research Network. https://doi.org/10.2139/ssrn.4986107
38. Watters, P. (2025). *Residential proxying and illicit streaming devices* (SSRN Scholarly Paper No. 5767282). Social Science Research Network. https://doi.org/10.2139/ssrn.5767282
39. Motion Picture Association. (2025). *Submission for the 2026 National Trade Estimate Report on Foreign Trade Barriers.* Washington, DC: MPA
40. For an example, see INTERPOL. (2024). *Project I-SOP: Illegal streaming, digital piracy & money-laundering*. https://www.interpol.int/Crimes/Illicit-goods/Projects/Project-I-SOP
41. Watters, P. A. (2021). *Time to compromise: How cyber criminals use ads to compromise devices through piracy websites and apps*. Social Science Research Network. https://doi.org/10.2139/ssrn.4536943
42. Watters, P. A. (2021). *Consumer risk and digital piracy – Where does malware come from?* Social Science Research Network. https://doi.org/10.2139/ssrn.4536938
43. International Intellectual Property Alliance. (2025). *2025 Special 301 Report on copyright protection and enforcement*. Washington, DC: IIPA. https://www.iipa.org/reports/special-301-reports

Bibliography

44. Watters, P. (2025). *Cybersecurity harms and illicit streaming devices* (SSRN Scholarly Paper No. 5800843). Social Science Research Network. https://doi.org/10.2139/ssrn.5800843
45. World Bank Group. (2024). *Cybersecurity economics for emerging markets.* World Bank Group. https://documents1.worldbank.org/curated/en/099011925184519084/pdf/P179481-5515e6c4-1d69-444d-a057-741edce07402.pdf
46. Tsang, A. (2025). Latin America: *Evolving e-commerce market landscape*. HKTDC Research. https://research.hktdc.com/en/article/MTkwNzk4MDYyMQ
47. Instituto Brasileiro de Geografia e Estatística. (2024). *In Brazil, 88.9% of the population had a mobile phone in 2024*. Agência de Notícias IBGE. https://agenciadenoticias.ibge.gov.br/en/agencia-news/2184-news-agency/news/44045-in-brazil-88-9-of-the-population-had-a-mobile-phone-in-2024
48. Business Development Director for Brazil, JuicyScore. (2025). *Brazil's fintech revolution built access at scale. Now it faces the cost of speed*. JuicyScore. https://juicyscore.ai/en/blog/brazil-fintech-revolution-pix-digital-payments-fraud
49. Jimenez Romero, K. (2024). *Brazil, Mexico y España entre los que más reclamaron por fraudes cripto en el FBI durante 2023*. Cointelegraph. https://es.cointelegraph.com/news/brazil-mexico-and-spain-led-in-fbi-crypto-fraud-claims-in-2023
50. Barbosa, F. (2024). *TV boxes são usadas para ataques de negação de serviço na América Latina.* TELETIME. https://teletime.com.br/26/01/2024/tv-boxes-sao-usadas-para-ataques-de-negacao-de-servico-na-america-latina/
51. Blog do Valente. (2025). *Operação derruba 14 plataformas ilegais de IPTV que tinham mais assinantes que grandes TVs por assinatura no Brasil.* Blog do Valente. https://blogdovalente.com.br/noticias/brasil/2025/11/operacao-derruba-14-plataformas-ilegais-de-iptv-que-tinham-mais-assinantes-que-grandes-tvs-por-assinatura-no-brasil/
52. International Data Spaces Association. (2024, September 26). *In a new phase of the operation against digital piracy, the Brazilian Ministry of Justice and Public Security takes down websites and streaming apps with illegal content.* Retrieved from https://ids.org.br/en/news-post/in-a-new-phase-of-the-operation-against-digital-piracy-the-brazilian-ministry-of-justice-and-public-security-takes-down-websites-and-streaming-apps-with-illegal-content
53. InSight Crime. (2022). "*Clandestine TV connections": The new criminal economy in Brazil*. Retrieved from https://insightcrime.org/news/clandestine-tv-connections-new-criminal-economy-brazil/
54. OECD. (2025). *National cybersecurity strategy (E-Ciber) – Brazil* (Policy No. BRA2214). Digital Economy Policy Platform. https://depp.oecd.org/policies/BRA2214
55. Observatório Legislativo CELE. (2012). *Brazil – Law 12.737 (typification of computer-crimes 2012*). https://observatoriolegislativocele.com/en/brazil-law-12-737-typification-of-computer-crimes-2012/
56. For more details of how VirusTotal works, see https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works
57. The Alliance for Creativity and Entertainment (ACE) is the world's leading coalition dedicated to protecting the legal creative market and reducing digital piracy. Driven by a comprehensive approach to addressing piracy through criminal referrals, civil litigation, and cease-and-desist operations, ACE has achieved many successful global enforcement actions against illegal streaming services and unauthorized content sources and their operators. Drawing upon the collective expertise and resources of more than 50 media and entertainment companies around the world-including sports channels and associations-and reinforced by the Motion Picture Association's content protection operations, ACE protects the creativity and innovation that drives the global growth of core copyright and entertainment industries. The current governing board members for ACE are Amazon, Apple TV+, Netflix, Paramount Global, Sony Pictures, Universal Studios, The Walt Disney Studios, and Warner Bros. Discovery. Charles Rivkin is Chairman and CEO of the Motion Picture Association and Chairman of ACE. For more information, visit www.alliance4creativity.com
58. Watters, P. A. (2015). *An analysis of piracy website advertising in Brazil and its linkages to child exploitation material.* Bangkok, Thailand: ECPAT International. Retrieved from https://ecpat.org/wp-content/uploads/2021/05/Piracy-Website-Advertising-in-Brazil_ENG.pdf
59. Herps, A., Watters, P. A., Simone, D., & Foster, J. L. (2025). When does website blocking actually work? *Laws, 14*(6), 81. https://doi.org/10.3390/laws14060081
60. Hunn, C., Watters, P., Prichard, J., Wortley, R., Scanlan, J., Spiranovic, C., & Krone, T. (2023). *How to implement online warnings to prevent the use of child sexual abuse material* (Trends & issues in crime and criminal justice No. 669). Australian Institute of Criminology. https://doi.org/10.52922/ti78894
61. Roehrer, E., Pokawinkoon, P., Watters, P., Sauer, J. D., & Scanlan, J. (2024). Adolescent-centric design of an online safety chatbot. *Journal of Computer Information Systems,* 1-14.

06

Appendix

Appendix – Results by Piracy Service Type.

BEST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	9	8	2	1	1
Streaming	7	19	3	0	0
IPTV Retransmission	5	11	1	1	0
IPTV Subscription	2	3	1	0	0
Anime	12	18	3	2	4
P2P	20	24	5	0	8
Scam	10	19	5	0	0
Control	1	0	0	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	9	13	2	1	1
Streaming	8	50	5	0	0
IPTV Retransmission	7	26	1	1	0
IPTV Subscription	2	7	1	0	0
Anime	15	44	15	2	4
P2P	23	58	11	0	8
Scam	12	49	6	0	0
Control	1	0	0	0	0

Notes

RESEARCHER BIOGRAPHY

Professor Watters is a trusted cybersecurity researcher and thought leader at Cyberstronomy Pty Ltd. He is the author of *Counterintelligence in a Cyber World* (Springer - ISBN 978-3031352867) and *Cybercrime and Cybersecurity* (CRC Press - ISBN 978 - 1032524511). Professor Watters is Honorary Professor of Security Studies and Criminology at Macquarie University, and Professor of Information Systems at Holmesglen Institute. His work has been cited 13,385 times, with an *h*-index of 53, and an *i*-10 index of 156. He was ranked within the top 0.5% of researchers worldwide (all fields) by ScholarGPS in 2024.

Professor Watters was awarded the Order of Australia Medal in 2026 for services to tertiary education, including research, teaching and service.

ACKNOWLEDGEMENTS

Funding for this research was provided by the Motion Picture Association. The work was produced independently by Dr Paul Watters, Macquarie University (Sydney).

Photo Credits: Freepik.com