Consumer Risk from Piracy in Latin America

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

Consumer Risk from Piracy in Latin America

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

Executive Summary

This study examined the cybersecurity risks associated with online piracy services across six Spanish-speaking Latin American countries – Colombia, Ecuador, Mexico, Argentina, Peru, and Chile. 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 all countries and piracy service types, cyber risk was pervasive and quantifiable. Even under conservative assumptions, piracy portals were 21.77 times more likely to contain cyber threats than legitimate websites. In the worst-case model, this relative risk rose to 39.18 times higher.

- P2P and Streaming platforms were the most hazardous vectors, with regional mean detections of 84.5 and 72.8 threats per 30 sites respectively.
- Colombia's Streaming sites exhibited the single highest value recorded in the study – 131 detections!
- Scam piracy sites, which impersonate illegal streaming services but host no genuine content, acting solely as fraud and malware-delivery portals.

Even in the best-case scenario, where potentially duplicate detections are collapsed, all service types continued to show elevated risk. Although absolute threat levels varied, no country in the study exhibited a safe piracy environment.

- Colombia displayed the most severe infection density, driven by highly active streaming and IPTV retransmission services.
- Argentina, Peru, Mexico and Chile showed lower total detections but still sustained relative risks several times above legitimate baselines.

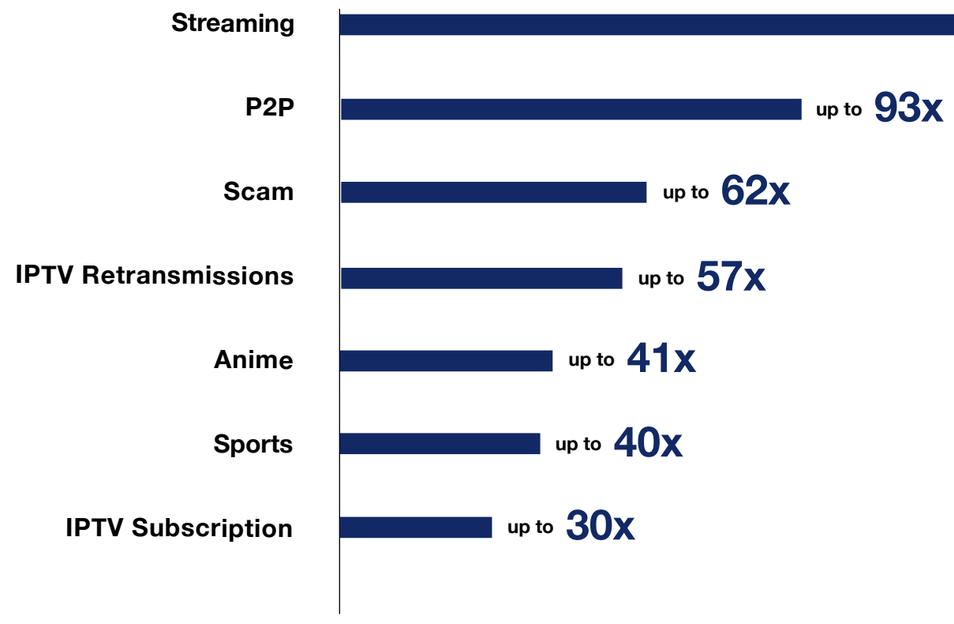
A significant proportion of identified illicit streaming devices, piracy-enabled applications, and associated malware infrastructure observed in Latin America can be traced to upstream manufacturing, software development, or hosting ecosystems concentrated in the People's Republic of China. This concentration introduces systemic supply-chain and geopolitical risk, particularly where consumer devices operate with opaque firmware, privileged network access, and persistent overseas connectivity.

In summary, the findings highlight that online piracy is no longer only an intellectual-property issue but a measurable cybersecurity threat vector. High infection densities, combined with normalized consumer behavior and easy access to illicit IPTV devices, create conditions for mass compromise.

Key Findings

Relative Risk of Encountering a Cyber Threat by Piracy Type

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



- **Relative Risk by Service Type**
  - » Streaming piracy portals: up to 131× higher risk
  - » P2P networks: up to 93× higher risk than legitimate sites
  - » Scam piracy sites: up to 62× higher risk
  - » IPTV Retransmission piracy sites: up to 57× higher risk
  - » Anime piracy portals: up to 41× higher risk
  - » Sports piracy sites: up to 40× higher risk
  - » IPTV Subscription piracy services: up to 30× higher risk
- **Overall Risk × 21.77:** In the best-case, consumers face on average more than a 21-fold increase in cyber-threat detections on piracy sites versus mainstream control sites.
- **Top-Risk Categories:** In the worst-case, P2P networks (average 84.5 detections), Streaming (average 72.8 detections), and Scam portals (average 59 detections) carry the highest relative risks over legitimate sources.
- **Market Details:** Colombia has the highest average relative risks – a 59-fold increase over legitimate sources – followed by Mexico with an exceeding 50-fold increase over legitimate sources. Argentina has the lowest average relative risks – slightly exceeding a 13-fold increase 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.
- **Cross-Country Consistency:** Every piracy service category demonstrated elevated threats in all six countries, with Streaming, P2P, and Scam sites being the most consistently risky.
- **Regional Pattern**: While legitimate sites are generally very safe, consumers using piracy services anywhere in Latin America are exposed to dramatically higher and preventable cyber risks, regardless of country.
- **Policy Implications:** These findings provide a robust evidence base for targeted policy reform, strengthened law enforcement capability in digital forensics and cyber incident response, and comprehensive public awareness campaigns tailored to local contexts. Given the stark disparity between mainstream and piracy platforms – especially in high-risk countries such as Colombia, Ecuador, and Mexico – coordinated action is strongly recommended to protect consumers from malware, phishing, and other cyber threats linked to digital piracy.

Contents

01

Introduction

Introduction

This study examines the rising consumer cybersecurity threats associated with digital piracy in Latin America, with particular attention to six key Spanish-speaking countries: Colombia, Ecuador, Mexico, Argentina, Peru, and Chile. While much discourse around piracy in the region has historically focused on economic loss[1] and intellectual property enforcement[2], this report reframes the issue through a cybersecurity and consumer protection lens – arguing that digital piracy services represent not just illicit media access points, but high-risk gateways to malware infection[3], data theft[4], financial fraud[5], and data breaches[6].

Latin America has seen historic[7] and sustained expansion in piracy services over the past decade[8], including unlicensed streaming of sports and films, anime portals, P2P networks, illicit IPTV subscriptions, and scam piracy sites. These ecosystems are evolving rapidly[9]: piracy has moved from desktop torrents and ad-saturated websites to fully featured IPTV platforms, piracy-enabled set-top boxes, and private messaging-distributed bundles[10]. In many Latin American countries, pirate streaming and IPTV services have become deeply embedded in everyday digital life, with millions of users drawn by apparent affordability, accessibility, and cultural normalization of piracy[11]. However, this apparent convenience conceals a growing consumer risk surface.

Also, a critical but underexamined dimension of piracy-related cyber risk in Latin America is the upstream concentration of infrastructure, devices, and services originating from the People's Republic of China (PRC)[12]. Empirical threat intelligence repeatedly shows that a significant proportion of illicit streaming devices (ISDs)[13], piracy-enabled Android applications, and associated command-and-control infrastructure are developed, hosted, or maintained within Chinese technology and cloud ecosystems.

Prior technical analysis[14] demonstrates that multiple high-risk ISDs and piracy APKs maintain persistent connections to PRC-based hosting providers and IP address space, including infrastructure previously linked to banking trojans, botnet frameworks, and malware loaders. This pattern mirrors findings from Asia-Pacific markets and indicates a globalized supply chain in which hardware manufacture, software development, and malware monetization converge upstream before being distributed into Latin American consumer markets.

This study analyzes cybersecurity threat data associated with a range of piracy services across six major Spanish-speaking Latin American economies, providing the basis for targeted mitigation measures – such as regulatory reform, strengthened law-enforcement capabilities, and consumer-focused education. Using an empirical and policy-relevant approach, it rigorously addresses the central question through a cyber lens: How risky are piracy platforms for consumers in Latin America, and how can those risks be reduced through strategic intervention?

Recent global and regional studies reveal the extraordinary level of cyber harm risk facing piracy users. Using threat intelligence data from over 95 security vendors, Watters (2025)[15] found that across Asia-Pacific markets, piracy services were up to 65 times riskier than legitimate sites for malware, phishing, spam, and other threats. The riskiest platforms were P2P, scam, and illicit streaming services – mirroring patterns already evident in Latin America.

Digital piracy platforms in Latin America operate not merely as copyright-infringing entities but as cybercrime distribution networks, blending deceptive branding with malicious ad delivery, credential phishing, and often outright fraud. Piracy-as-a-service offerings in the region now closely resemble legitimate streaming businesses – except that they often harvest user data, deliver hidden payloads, and directly fund organized crime. In many developing economies, piracy ecosystems represent a persistent and highly effective channel for malware distribution, driven by informal technology use and low public awareness of digital risks[16].

In this context, consumers in Latin America – many of whom are digitally active but possibly under-protected – face serious and poorly recognized cyber harms[17]. This report presents a detailed threat landscape review across the six countries, evaluating piracy modalities such as IPTV subscriptions, anime portals, P2P hubs, and fraudulent "scam" sites in Latin America[18].

The core research question is this: To what extent do piracy services in Latin America increase cyber risk to consumers, and what unique regional dynamics amplify that risk? By answering this, the report aims to inform national cybersecurity strategies, cross-border enforcement efforts, and urgently needed public education campaigns.

The International Intellectual Property Alliance (IIPA) emphasizes that copyright-based industries generate substantial employment and trade benefits – over US $1.8 trillion in output and 9.6 million U.S. jobs[19]. Extending these benefits to Latin American creative sectors depends on stronger enforcement and fair market access for legitimate content. Without these, consumers gravitate to unregulated services, exposing themselves to cyber risks while undermining domestic cultural production.

What is Digital Piracy?

Digital piracy refers to the unauthorized acquisition, reproduction, or distribution of copyrighted digital content without permission or payment to rights-holders, using a range of protocols, devices and technologies[20]. In the Latin American context, this encompasses a broad range of services that enable access to audiovisual content – including sports, films, television series, and anime – through unlicensed channels. The following categories define the primary forms of piracy under investigation in this study:

- **Sports Piracy:** Illicit platforms that stream live sports events, particularly football, by intercepting or duplicating pay-TV feeds or online broadcasts. These sites or services often attract massive regional audiences, especially during major tournaments.
- **Streaming Piracy:** Platforms that provide unauthorized access to films, series, and television content via real-time streaming, often monetized through advertising or subscriptions. These may closely resemble legal services but operate entirely without content licenses.
- **IPTV Retransmission:** The unauthorized interception and redistribution of broadcast content – via illegal IPTV servers – without a consumer subscription model.
- **IPTV Subscription Piracy:** Paid piracy services offering bundled access to hundreds of unauthorized TV channels, VOD libraries, and sports events. Consumers typically pay a flat fee for access, while operators bypass all licensing obligations.
- **Anime Piracy:** Portals that offer streaming or download access to Japanese animation without authorization, frequently using fan-created subtitles. These services often serve unmet demand where legal anime distribution is limited or delayed.
- **P2P (Peer-to-Peer):** Decentralized file-sharing networks that allow users to upload and download pirated content – including films, music, and games – directly from one another's devices, often via torrent protocols.
- **Scam Piracy Sites:** Deceptive platforms that lure users with the promise of free or discounted content but instead harvest personal data, install malware, or execute payment fraud schemes. These may mimic legitimate services or host no actual media at all.

Each of these modalities presents distinct technical and consumer-facing risks[21]. Together, they form a deeply entrenched ecosystem that facilitates the delivery of pirated content alongside malicious code, credential theft, and fraudulent payment traps[22] – placing Latin American users at significantly elevated cybersecurity risk. Importantly, these piracy ecosystems are not locally manufactured phenomena. They are downstream manifestations of a highly concentrated global supply chain, in which low-cost Android-based devices, modified firmware, and piracy applications are predominantly developed and distributed from PRC-linked manufacturing and software ecosystems. Latin American consumers therefore inherit upstream design and security decisions over which they have no visibility or control.

Social and Economic Consequences of Piracy

Digital piracy in Latin America extends far beyond revenue loss – it reshapes cultural expectations, disrupts creative economies, and strains public trust in digital services. A region rich in cultural production, Latin America depends on enforceable intellectual property frameworks to support economic innovation and protect creative labor. Yet the widespread normalization of piracy has created systemic vulnerabilities, especially among digitally native youth[23]. According to the International Intellectual Property Alliance (IIPA, 2025), major Latin American markets – including Mexico and Colombia – remain on USTR's Watch List because of persistent online piracy and weak enforcement mechanisms[24]. Similarly, the Motion Picture Association (MPA, 2025) highlights Mexico and Colombia as key markets where "widespread availability of illegal IPTV and streaming services" continues to undermine legitimate audiovisual trade and digital-platform investment[25].

SOCIAL CONSEQUENCES

Piracy in Latin America weakens the foundation of cultural development. When unlicensed content floods the market, it erodes the value of local creative works, discourages domestic investment, and diminishes the perceived worth of Latin American storytelling. The result is a cultural feedback loop: with fewer incentives to produce authentic content, creators retreat, and cultural diversity narrows[26].

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[27].

Furthermore, youth surveys in other regions suggest a generational shift[28]: younger consumers increasingly view piracy as normal, safe, and even ethical. As this attitude takes root, it erodes public respect for copyright and lawful digital engagement. Studies globally have shown that a strong moral obligation not to pirate correlates with lower piracy rates[29]. The absence of strong ethical messaging in Latin American digital policy may be contributing to the entrenchment of piracy.

ECONOMIC CONSEQUENCES

Piracy deprives Latin America's creative industries of critical revenue, translating into job losses, business closures, and stagnant innovation. From musicians and animators to developers and production crews, the impact of piracy is felt at every level of the content creation chain. When legitimate sales falter, so does reinvestment into new content[30].

In the region, where national cinemas and music scenes are both prolific and vulnerable, piracy has been linked to annual losses reaching into the billions[31]. As pirate IPTV subscriptions rise and advertising revenue shifts to unlicensed platforms, governments also lose tax revenue – constricting 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[32].

In summary, digital piracy in Latin America is not just 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

Consumers in Latin America who access pirated services face serious cybersecurity risks, especially when making payments or downloading content. A 2022 study by the Digital Citizens Alliance (DCA) found that one in ten credit card transactions on piracy platforms resulted in unauthorized charges within 30 days, suggesting that cybercriminals often harvest and resell card data for fraud or high-value purchases[33]. Many victims are unaware of the fraud until receiving their financial statements – by which time they may have suffered account holds, chargebacks, or credit score impacts.

Piracy services that advertise themselves as “free” and “ad-free” present a distinct and heightened risk profile. Unlike ad-supported piracy sites, which at least expose their monetization mechanisms, ad-free services must extract value covertly. Empirical analysis shows that such services frequently monetize users through data harvesting, credential exfiltration, residential proxying, or direct enrollment of devices into botnets[34].

In this model, the consumer is not the customer but the commodity. The absence of visible advertising should therefore be treated as a warning signal rather than a safety feature, particularly when combined with mandatory app installation, device sideloading[35], or opaque subscription models.

Piracy sites frequently masquerade as legitimate platforms, using brand impersonation or copycat domains to create a false sense of trust[36]. When these sites disappear or change overnight, users may lose access to promised services and have their personal information sold to third-party actors for spamming, scams, or other forms of harassment. The reputational damage also reduces consumer confidence in legitimate digital services.

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

Malware & Drive-by Downloads

Merely visiting an illicit streaming site can result in a drive-by download, silently installing trojans, worms, or keyloggers without user consent. 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

Imitation login forms or fake payment portals are used to harvest credentials – including banking logins, email access, and MFA codes. These can be resold or used for identity theft, unauthorized purchases, and account takeovers.

Spyware & Data Exfiltration

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

Botnet Recruitment & Network Compromise

Users who install cracked networking tools, Illicit Streaming devices or P2P clients may unknowingly join botnets used in cyberattacks (e.g., DDoS, malware spam), putting their own and others’ devices at risk.

This convergence of piracy and cybercrime has been exploited by organized crime syndicates, who increasingly finance or operate piracy platforms as part of broader monetization schemes[37]. These include ad fraud, fake subscriptions, and malware delivery, often supported by existing criminal infrastructures such as counterfeit goods networks. Many piracy platforms are also used as conduits for money laundering, funneling illicit revenues through crypto mixers or shell firms. Recent enforcement trends confirm the deepening overlap between organized crime and digital piracy. The MPA notes that these networks “exploit jurisdictional gaps and enforcement delays to re-emerge under new domains within days,” using cross-border infrastructure that often lies outside effective national reach[38]. Collaborative law-enforcement initiatives across Mexico, Colombia, and Central America show early promise but remain constrained by inconsistent legal definitions of online infringement and limited capacity for cross-jurisdictional evidence sharing.

Since these multinational criminal operations often span multiple jurisdictions and exploit enforcement gaps, traditional takedown and policing measures struggle to keep pace[39]. Threat intelligence correlation indicates repeated connections between piracy services used in Latin America and infrastructure hosted within PRC IP address space or PRC-affiliated cloud providers. This includes command-and-control servers, update endpoints, and proxy coordination nodes previously linked to banking trojans, botnet frameworks, and malware loaders. 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 provides a structured way to identify, categorize, and prioritize how adversaries may compromise systems or services. It maps valuable assets, vulnerabilities, attacker goals, and likely attack vectors – enabling defenders to concentrate on the scenarios with the highest potential impact.

In the Latin American piracy ecosystem, threat modeling exposes how malicious actors exploit unlicensed content sites to deliver malware, steal credentials, and infiltrate users' home and corporate networks. These ecosystems – spanning Mexico, Argentina, Chile, Colombia, and other regional markets – blend global piracy trends with local factors such as weak enforcement, high content costs, and pervasive use of low-cost streaming devices.

SITE OPERATORS

Site operators are the individuals or organized groups that build and maintain piracy platforms - whether web-streaming portals, IPTV services, or torrent indexes. Because they control the infrastructure, these operators can:

- Inject *drive-by* exploits into embedded video players.
- Bundle trojans or spyware inside client-side applications (such as Android TV APKs common in Latin America).
- Distribute malicious updates through counterfeit “patches” or ad networks.

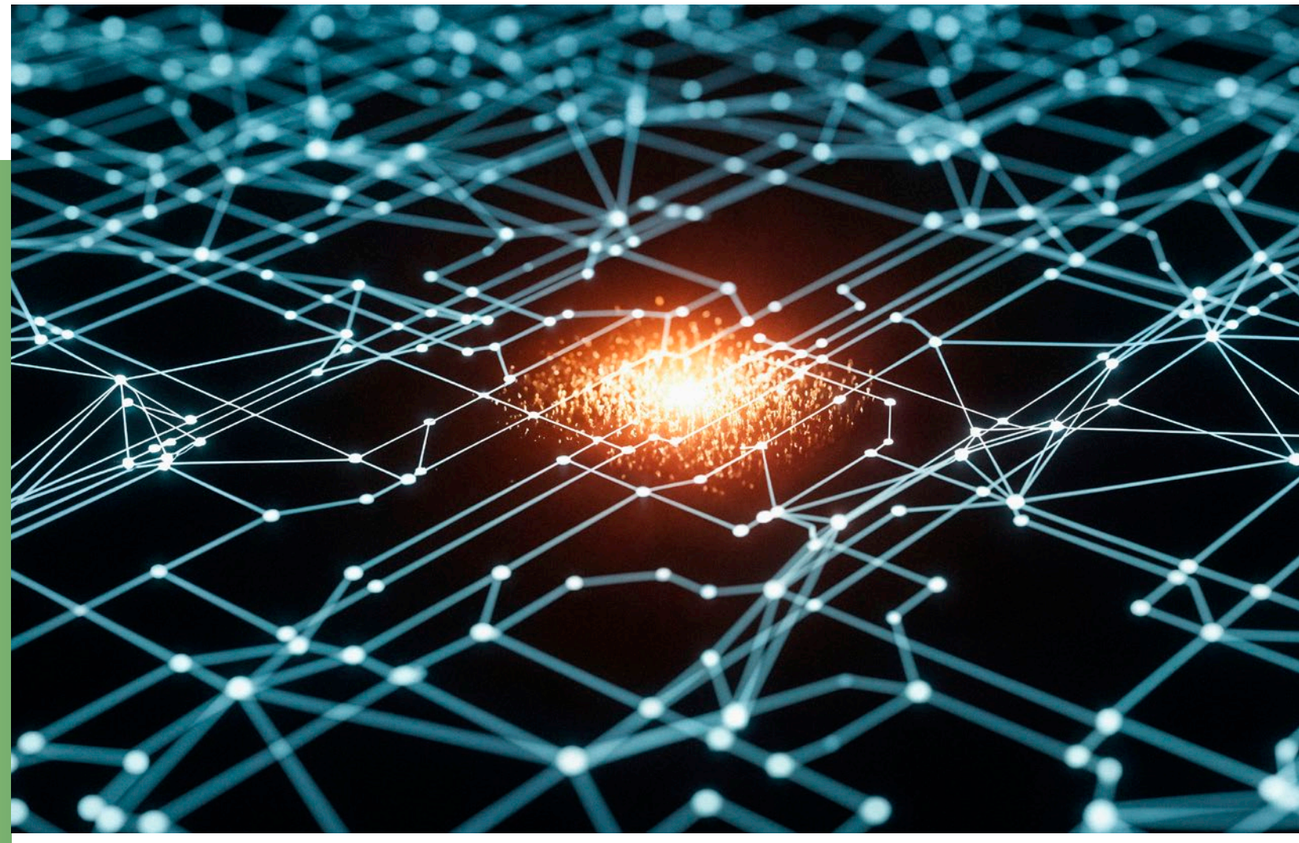
Their infrastructure-level control grants the broadest reach: every visitor or subscriber is exposed to potential hidden payloads that install backdoors, cryptominers, or spyware silently[40]. Within the region, where IPTV boxes and online telenovela streams are highly popular, these actors often mimic legitimate regional streaming services to evade detection.

UPLOADERS

On P2P and Anime sites, community uploaders seed or host specific files. These contributors may embed malware in what appears to be safe media – subtitle packs, compressed archives (ZIP/RAR), or "cracked" media players – knowing that users will decompress and execute these components locally. Since users expect entertainment files, infections often go unnoticed until systems are compromised. This reflects a wider cognitive gap between perceived and actual risk: many consumers equate downloading or streaming pirated media with a low-stakes, routine activity rather than a security threat. Survey data from over 6,000 participants across five Asia-Pacific countries showed that although users ranked piracy websites as the second-highest source of malware risk (22.27%), large segments of the population still accessed them regularly. The study also found that 31% of malware-infection variance could be explained by demographic and behavioral factors – particularly low risk awareness and habitual access to piracy content[41].

These results suggest that users operate under mental models in which entertainment-related downloads are familiar and therefore perceived as benign. Consumer behavior, shaped by expectation and habit, becomes the critical vulnerability vector – not just the malware itself. IIPA (2025) reinforces this behavioral dimension, urging governments to "invest in end-user education campaigns to enhance consumers' knowledge of the dangers of accessing pirated content, including exposure to malware and phishing schemes"[42].

These findings align with the *Time to Compromise* study, which identified that users' habitual engagement with piracy sites



– especially when seeking entertainment – creates cognitive blind spots. Consumers perceive downloading or streaming pirated media as low-risk and familiar, allowing infections to go unnoticed until systems are compromised. Addressing these mental models through digital-literacy and risk-awareness campaigns would narrow the psychological gap between perceived and actual threat.

THIRD-PARTY INJECTORS

Third-party injectors are external attackers who exploit shared advertising networks, common CMS plugins, and outdated web frameworks used by piracy portals. They use techniques such as:

- Malvertising to inject malicious ads.
- Cross-site scripting (XSS) to insert JavaScript that captures cookies or redirects users to phishing pages and exploit kits.

These injectors often act independently of the site operators, using automated tools to compromise dozens of piracy portals simultaneously. Their actions transform even relatively benign illegal streaming sites into vectors for credential theft, banking trojans, and drive-by downloads. Across Latin America, attackers have exploited regional ad networks and cloud-hosting providers to distribute payloads disguised as sports betting widgets or video codec updates.

SITE HACKERS

A fourth actor class – site hackers – targets the piracy platforms themselves, breaching servers to plant or amplify malicious content. Many piracy portals in Latin America operate on unpatched WordPress or Joomla CMSs, with default credentials and weak security settings. These vulnerabilities allow hackers – ranging from organized cybercriminal groups to opportunistic "script kiddies" – to:

- Exploit known web vulnerabilities (e.g., SQL injection, remote code execution).
- Steal admin credentials through phishing or credential stuffing.
- Escalate privileges on under-secured Linux or Windows hosts to install rootkits or botnet agents.

The result is server-side malware injection: every visitor, even to a seemingly harmless page, can be served cryptominers, spyware, or links to exploit kits. In some cases, compromised piracy sites share infrastructure with legitimate ISPs or CDN nodes, creating lateral movement opportunities and amplifying the regional impact.

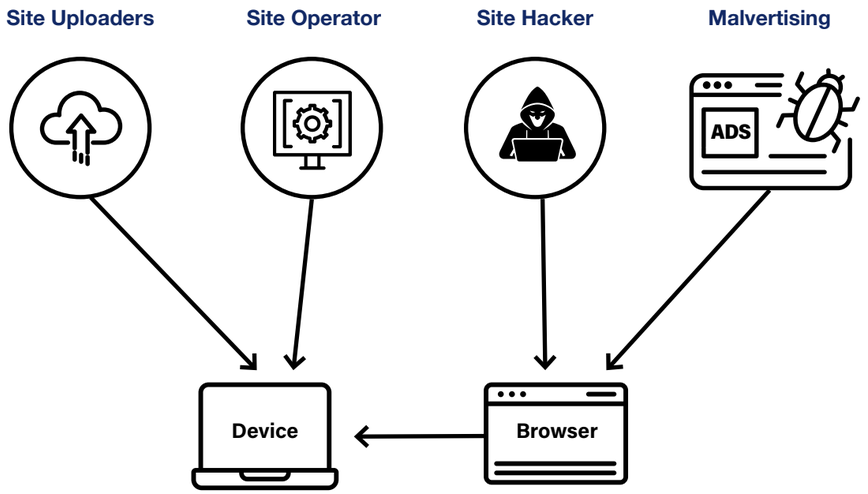
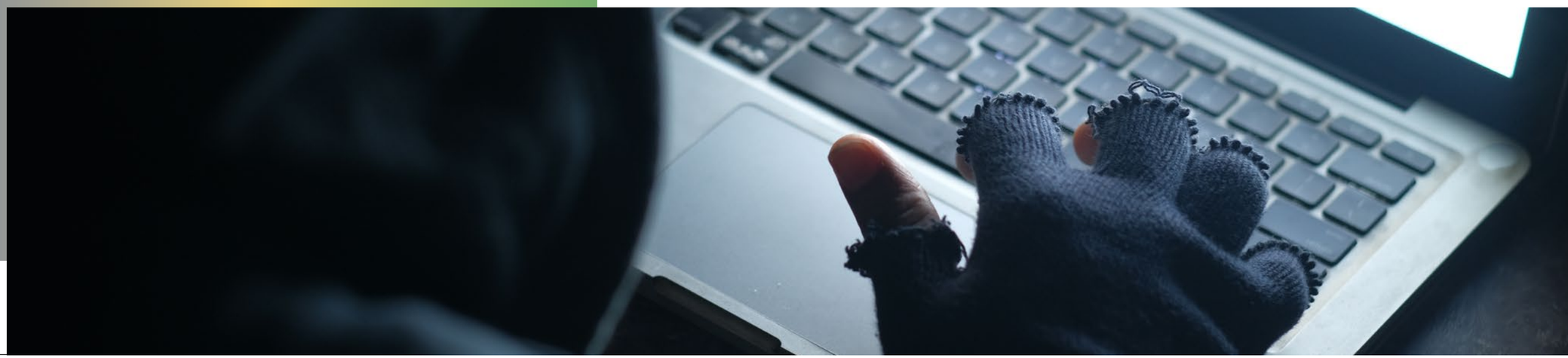


Figure 1 – Traditional Piracy Threat Model



In recent years, Latin American piracy has evolved from torrent swarms and ad-saturated websites to Illicit Streaming Devices (ISDs) – low-cost TV boxes and USB dongles pre-loaded with unlicensed channels. These devices, widely sold through informal online marketplaces in Mexico and Colombia, deliver "piracy-as-a-service": users plug them in, pay a flat monthly or lifetime fee, and access premium sports, movies, or telenovelas through what appears to be a legitimate interface.

Yet this convenience introduces a new and more dangerous threat model (see Figure 2 – ISD Threat Model).

Because ISDs operate directly on the home network – often with administrator or root privileges – they can:

- Intercept local traffic and access shared folders.
- Receive malicious firmware updates that install remote-access trojans or cryptojacking scripts.
- Bypass firewalls and antivirus protections by masquerading as trusted devices.

A compromised ISD can therefore act as a persistent foothold for attackers, pivoting laterally to laptops, NAS drives, or even children's tablets on the same Wi-Fi network. The risk is not hypothetical: like how Mirai hijacked IoT devices globally in 2016, weaponized ISDs could be recruited into botnets, espionage, or ransomware campaigns. This "camouflage" strategy – embedding malicious code inside routine firmware or update channels – turns what seems to be a harmless entertainment gadget into a serious cyber-crime and national-security threat for the region. A summary of threat actors is provided in Table 1.

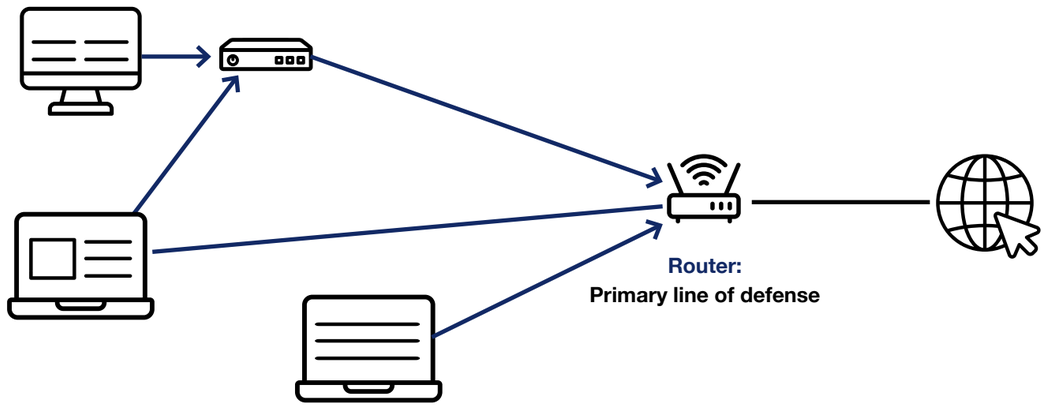


Figure 2 – ISD Threat Model – Undermining Bastion Defenses

Threat Actor	Primary Role	Attack Vectors	Consumer Impact
Site Operators	Build and maintain piracy platforms (streaming portals, IPTV servers, torrent indexes).	• Drive-by exploits in embedded players • Malicious APKs and counterfeit patches • Ad network injection	**System compromise** via trojans, spyware, cryptominers; broad exposure for all visitors/ subscribers.
Uploaders	Seed/share files on P2P and anime sites.	• Malware embedded in subtitle packs, ZIP/RAR archives • Cracked media players	**Hidden infections** during decompression or playback; delayed detection increases compromise risk.
Third-Party Injectors	Exploit advertising, affiliate, or plug in channels linked to piracy sites.	• Malvertising campaigns • Redirect chains to phishing portals • Bundled installers	**Credential theft,** payment fraud, and unwanted software installs; exposure even without downloads.
Site Hackers	Compromise piracy platforms or hijack domains.	• SQL injection, cross site scripting • Domain hijacking • Defacement with malware payloads	**Data breaches**, phishing overlays, and botnet recruitment; consumers misled by trusted-looking domains.

Table 1: Threat Actors in the Latin American Piracy Ecosystems

The enrollment of Chinese-manufactured consumer devices into piracy-linked botnets has implications that extend beyond individual harm and consumer fraud[43]. At scale, these botnets represent a latent national security risk. Devices embedded within ordinary households can be remotely coordinated to conduct distributed denial-of-service attacks, anonymized credential harvesting, and large-scale proxying of illicit traffic, significantly complicating attribution and law-enforcement response.

Prior national-level analysis in Malaysia demonstrates that ISDs can be weaponized as part of residential proxy networks, enabling foreign or criminal operators to route malicious traffic through civilian infrastructure[44]. This capability creates plausible pathways for espionage, critical infrastructure disruption, and the laundering of cyber operations through Latin American residential IP space, thereby elevating piracy ecosystems from copyright violations to matters of strategic cyber resilience[45].

Where botnet command infrastructure and update channels are concentrated in foreign jurisdictions with limited transparency and legal cooperation mechanisms, the national security implications are amplified. In the case of piracy-linked botnets with PRC-centric infrastructure, this creates asymmetric risk: Latin American consumer networks absorb the operational burden of compromise, while control and monetization remain offshore.

Recent threat research has documented the *Bigpanzi* cybercrime operation, which compromises Android-based televisions and set-top boxes using malware commonly referred to as *pandoraspear*. The campaign demonstrates how piracy-adjacent ecosystems can be leveraged to build and maintain a large botnet of consumer devices, supporting criminal monetization pathways such as distributed denial-of-service (DDoS), illicit traffic proxying, and other downstream abuse. Notably, analysis reported a substantial concentration of affected devices and observed activity in the region, illustrating the relevance of STB/ISD malware at scale in Latin American consumer networks[46].

Cybercrime and Consumer Wealth in Latin America

As digital connectivity and purchasing power expand across Latin America, consumers have become increasingly appealing targets for cybercriminals[47]. Several factors contribute to this heightened risk[48]:

- High Internet and Mobile Penetration - Smartphone penetration exceeds 80% in most markets, and 4G – and increasingly 5G – coverage has made mobile devices the primary gateway for online activity. Constant connectivity exposes users to multiple threat vectors via banking apps, e-commerce platforms, and social media channels, creating fertile ground for phishing, fake promotions, and malware-laden links.

- Rapid Digital Finance Adoption - The regional boom in mobile payments and fintech innovation – including CoDi in Mexico, and similar real-time systems in Colombia and Peru – has expanded digital finance access[49] but also introduced new vulnerabilities. Attackers exploit cloned payment interfaces, counterfeit banking apps, and credential-harvesting malware to intercept or redirect transactions.

- Expanding Middle Classes and Disposable Income - Rising wages, digital consumption, and the proliferation of online marketplaces across Mexico, Chile, and Argentina make consumers lucrative targets for investment scams, cryptocurrency fraud, and “tech support” or subscription-based cons. Organized groups frequently localize their lures with Spanish-language branding and exploit trust in local institutions, with Mexico recording the third highest losses globally according to an FBI report[50].

- Uneven Cybersecurity Awareness and Regulation - While Chile and Mexico have enacted data protection and cybersecurity laws, enforcement and digital literacy remain inconsistent across much of the region. In Ecuador, Peru, and Colombia, awareness gaps and weaker institutional capacity allow phishing, ransomware, and identity-theft campaigns to flourish.

- High Use of Pirated and Unlicensed Services - Persistent use of pirated streaming apps, IPTV boxes, cracked software, and P2P platforms continues to normalize unsafe online behavior[51]. These services often distribute malware, spyware, or credential-stealing adware, making them ideal entry points for cybercriminals, as reported in relation to Magis TV, as just one regional example[52,53].

In summary, in Latin America, piracy not only undermines creative industries – it also serves as a significant vector for cybercrime, blurring the line between casual infringement and systemic exploitation.

PROTECTIVE FACTORS IN LATIN AMERICA'S CYBER POLICY AND REGULATORY RESPONSES

Across Colombia, Ecuador, Mexico, Argentina, Peru, and Chile, governments have made significant strides in developing cybersecurity strategies and data-protection regimes. However, the level of maturity and enforcement varies widely, reflecting differences in institutional capacity, political prioritization, and regional cooperation.

NATIONAL CYBERSECURITY FRAMEWORKS

Most countries in the region have established national cybersecurity strategies that define priorities such as critical-infrastructure protection, digital trust, and interagency coordination.

- Mexico's National Cybersecurity Strategy (2017) remains the region's most comprehensive, outlining a multi-stakeholder model that includes academia and the private sector[54].
- Chile has advanced toward the creation of a National Cybersecurity Agency (ANCI) and updated its cybersecurity law to align with international standards, emphasizing resilience and CERT capacity[55].
- Colombia adopted a CONPES 3995 cybersecurity policy, prioritizing digital-economy protection, while Peru and Argentina have formalized national frameworks to strengthen coordination between defense, justice, and telecommunications authorities[56].
- Ecuador is in the process of expanding its National Cybersecurity Plan (2022-2025), focused on developing incident-response capacity and public education.

Together, these frameworks have begun to institutionalize cybersecurity governance, even as resource constraints and uneven implementation persist.

LEGAL AND REGULATORY SAFEGUARDS

All six countries have enacted or proposed legislation to criminalize unauthorized access, malware distribution, and online fraud, and most maintain Computer Crime or Cybercrime Laws integrated into their penal codes.

- Mexico's Federal Law on the Protection of Personal Data Held by Private Parties[57], Chile's new Personal Data Protection Law 21.719[58], and Argentina's Data Protection Act (Law 25.326)[59] establish obligations for data controllers and processors.
- Colombia's Law 1273[60] and Peru's Law 29733[61] strengthen penalties for cybercrime and mandate transparency in data processing.
- Ecuador's Personal Data Protection Law (2021)[62] is the most recent in the region, signaling growing convergence with international privacy norms.

Despite these advances, enforcement capacity remains uneven, and many national institutions may lack specialized cyber-forensics units and judicial expertise to prosecute transnational digital offenses.

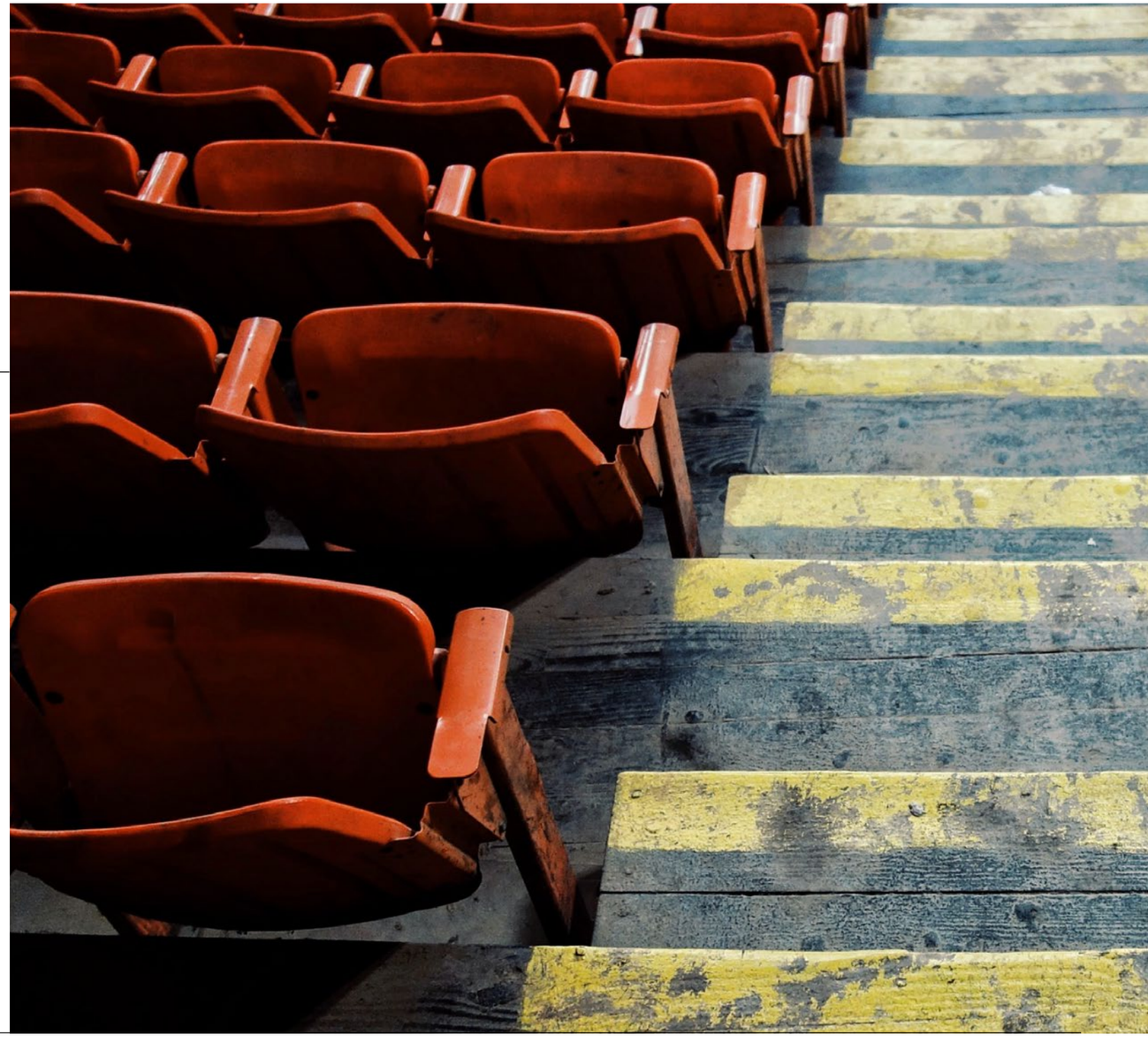
INSTITUTIONAL COLLABORATION AND CERT NETWORKS

Each country now operates at least one Computer Emergency Response Team (CERT) or Cybersecurity Operations Centre (CSOC), supporting early warning, incident coordination, and information sharing.

- CSIRT-Gov (Chile) and CSIRT Colombia maintain 24×7 monitoring and coordinate with ISPs and major platforms to respond to large-scale phishing or ransomware events.
- Peru's CSIRT-Perú, Ecuador's EcuCERT, Mexico's CERT-MX, and Argentina's CERT.AR collaborate with law-enforcement and private stakeholders to exchange threat indicators and mitigate regional campaigns.

Regional cooperation is reinforced through OAS (Organization of American States) initiatives, such as the Inter-American Cybersecurity Program, and the Forum of Incident Response and Security Teams – Latin America and Caribbean (FIRST-LAC), which facilitate capacity-building, joint exercises, and domain-takedown coordination.

Education, Capacity Building, and Public Awareness



Governments across Latin America have recognized that cyber resilience depends not only on regulation but also on human capital development. National programs such as Chile's Talento Digital[63] aim to upskill students, SMEs, and civil servants in digital hygiene and threat detection. Public-awareness campaigns – often in collaboration with telecom providers and NGOs – promote safe online behavior and warn against phishing and fraudulent streaming apps.

Regional organizations such as the OAS Cybersecurity Program also play key roles in training law-enforcement personnel and harmonizing best practices across borders. Despite this growing architecture of laws, institutions, and partnerships, specific countermeasures against the cybersecurity risks emerging from digital piracy remain underdeveloped. While national CERTs and regulators increasingly identify malware distribution through phishing and botnets, piracy-linked cyber threats – such as malicious IPTV apps, counterfeit streaming devices, and infected P2P portals – are rarely addressed explicitly in public policy.

Integrating piracy-related threat intelligence into regional CERT networks and consumer-protection frameworks would represent a critical next step in safeguarding Latin American users from these high-risk vectors.

02

Methods

Sample Design

Piracy Categories

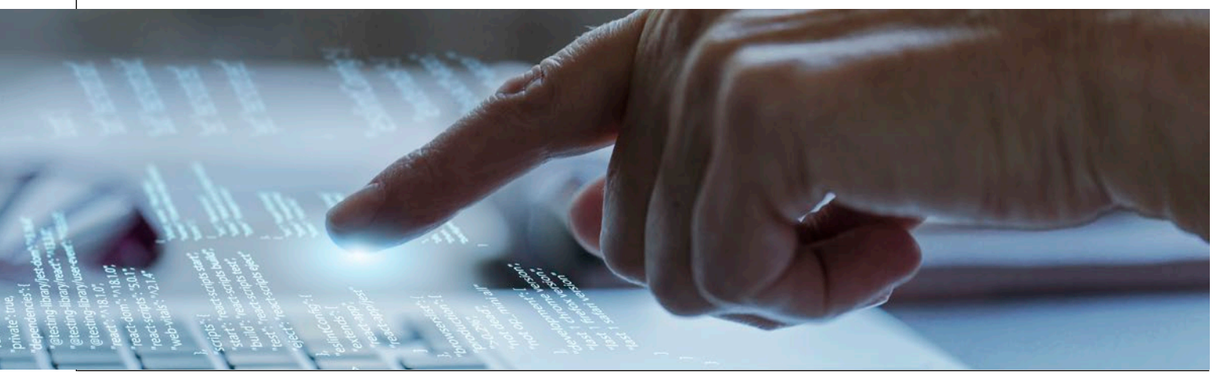
Data Collection and Analysis

Statistical Framework

Quality Assurance and Reproducibility

Methods

Data were collected from six Latin American countries – Colombia, Ecuador, Mexico, Argentina, Peru, and Chile – 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[64] 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)[65] and regional partners provided verified lists of active piracy websites operating in the six study countries. 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 per country was selected from this list. Selection criteria emphasized verified operational status, accessibility from within the target country, and sufficient user traffic (as observed through independent monitoring tools and ACE datasets).

For comparison, a control sample of 30 mainstream websites per country was compiled using web-traffic data (via SimilarWeb, and regional 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 Latin America'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 Spanish 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 Latin America and allow comparative measurement of consumer exposure to cyber threats.

Data Collection and Analysis

In total, 1,440 URLs (240 per country) 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 country and 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)

Regional Patterns

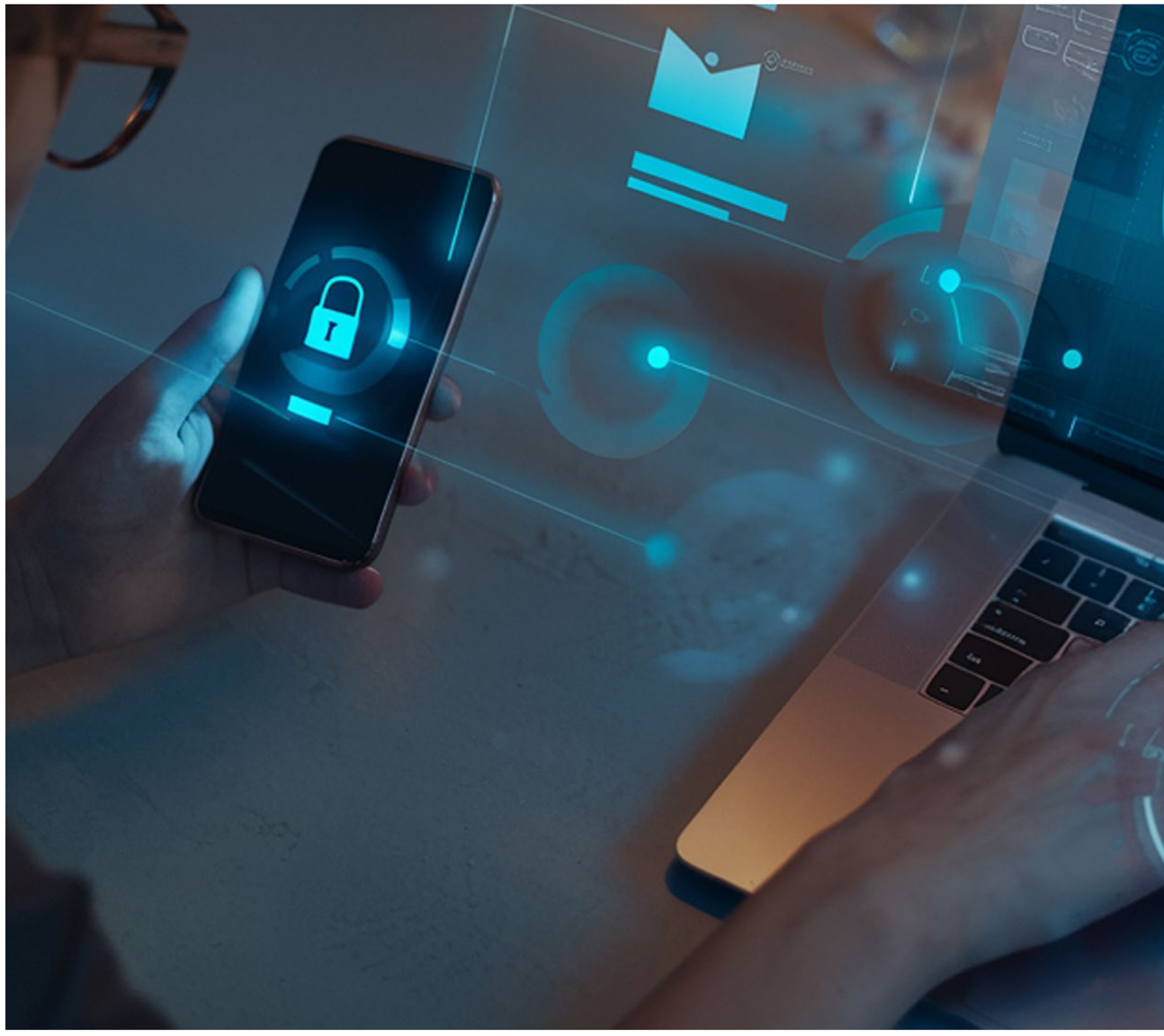
Results

To assess the cyber risk landscape associated with piracy services across Latin America, 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 21.77× in the best-case scenario to 39.18× 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 Latin America, 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 (regional mean = 84.5) and Streaming (72.8). Colombia's Streaming sites exhibited the single highest value observed in the dataset, at 131 detections, almost double the regional mean, underscoring the exceptional risk concentration in that market. Scam and Anime sites also exhibited substantial levels of malicious code, with regional averages of 59.0 and 30.5 respectively.

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 and Streaming sites continued to dominate the threat landscape (55.5 and 40.5 detections respectively), followed by Anime (23.8) and Scam (24.3). Even under this conservative interpretation, all service types produced non-zero detection counts, confirming that the presence of active cyber threats is endemic across Latin American piracy ecosystems.

Piracy Service Type	Colombia	Ecuador	Mexico	Argentina	Peru	Chile	Average
Sports	20	25	40	17	27	21	**25.0**
Streaming	131	60	58	48	72	68	**72.8**
IPTV Retransmission	45	39	57	36	33	36	**41.0**
IPTV Subscription	30	15	10	16	15	20	**17.7**
Anime	35	31	41	26	21	29	**30.5**
P2P	90	84	85	83	93	72	**84.5**
Scam	62	62	61	56	60	53	**59.0**
Control	0	0	0	3	1	2	**1**
Average	51.63	39.50	44.00	35.63	40.25	37.63	**41.44**

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

Piracy Service Type	Colombia	Ecuador	Mexico	Argentina	Peru	Chile	Average
Sports	15	11	22	14	12	16	**15.0**
Streaming	48	37	39	44	36	39	**40.5**
IPTV Retransmission	20	19	28	19	18	16	**20.0**
IPTV Subscription	13	8	5	8	9	12	**9.2**
Anime	22	27	30	21	18	25	**23.8**
P2P	57	60	60	58	46	52	**55.5**
Scam	26	23	27	24	25	21	**24.3**
Control	0	0	0	3	1	2	**1**
Average	25.13	23.13	26.38	23.88	20.63	22.88	**23.66**

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

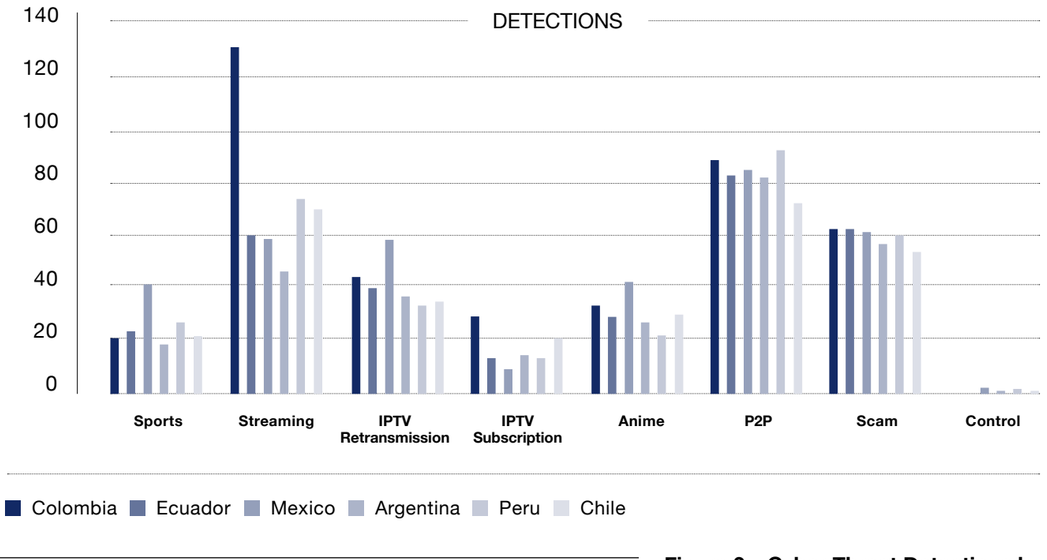


Figure 3 – Cyber Threat Detections by Piracy Service Type (Worst-Case)

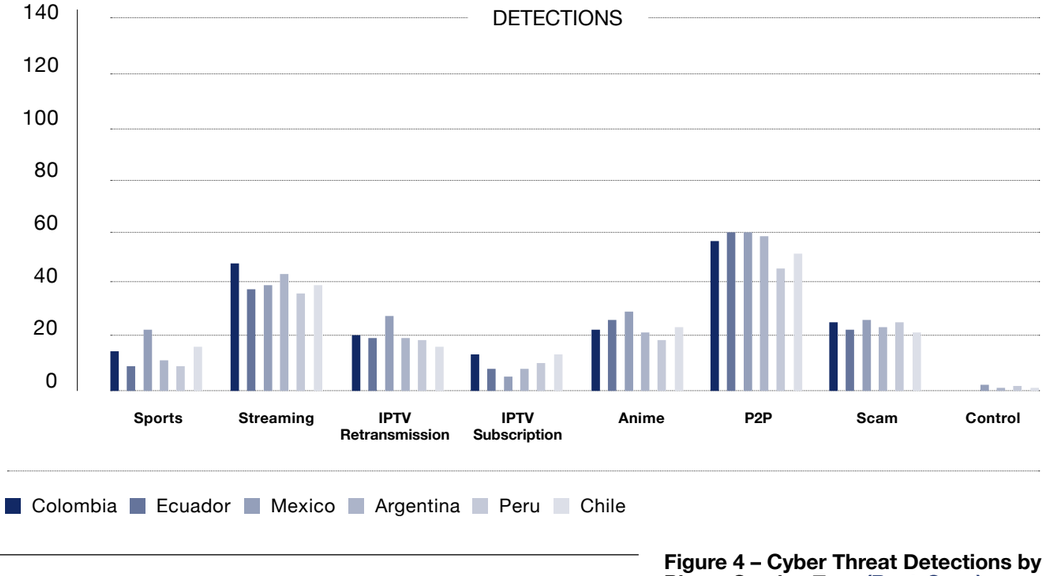
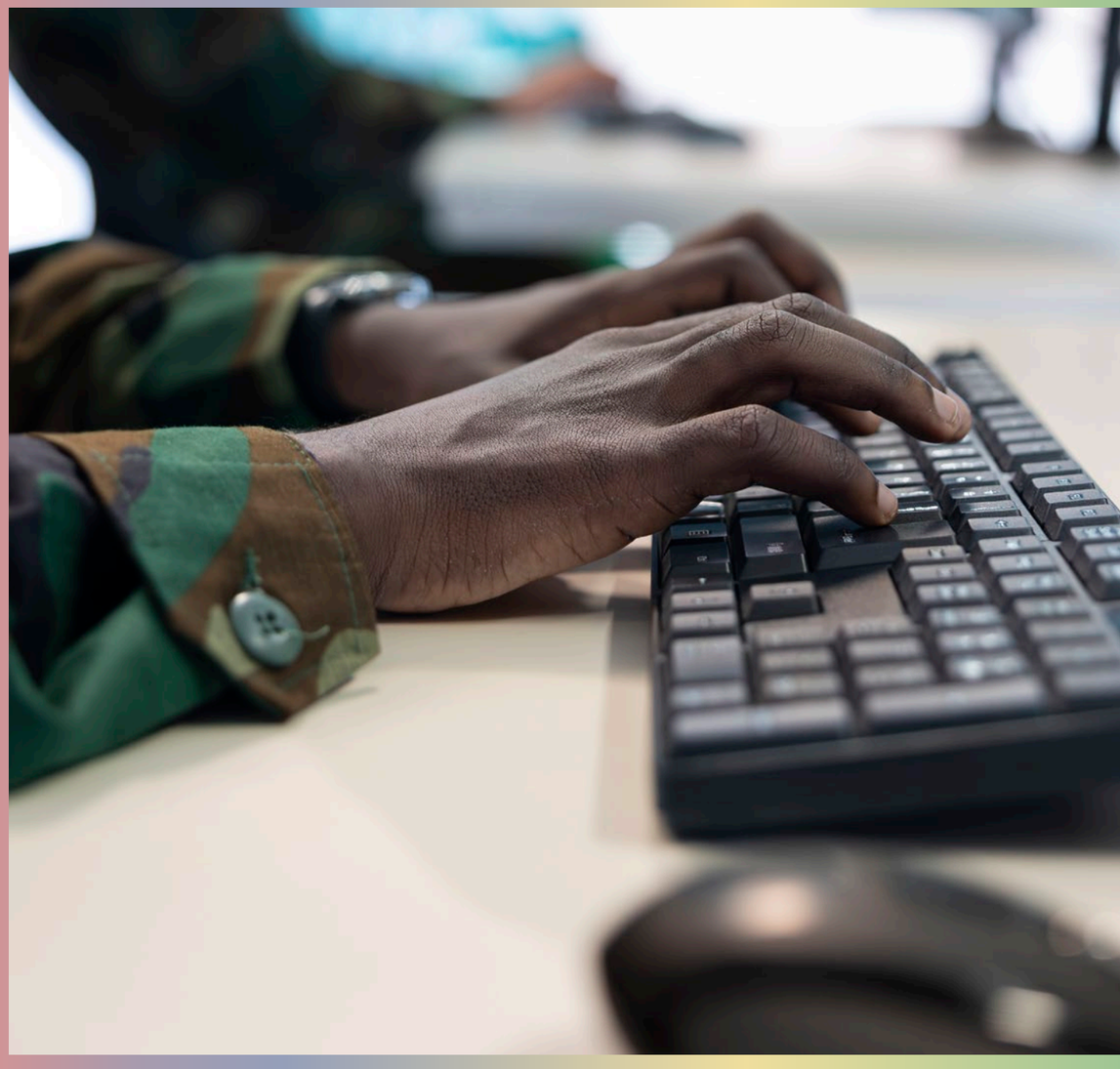


Figure 4 – Cyber Threat Detections by Piracy Service Type (Best-Case)



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 or Streaming sites could expect an average likelihood of 2.82 or 2.43 respectively. Even lower-volume categories such as IPTV Subscription (0.59) and Sports (0.83) displayed non-trivial exposure levels.

The best-case scenario produced similar relative ordering, though at reduced magnitudes. P2P remained the most hazardous (1.85 detections per 30 sites), followed by Streaming (1.35) and Scam sites (0.81), demonstrating that even superficially inactive piracy portals pose ongoing infection risks. These findings reinforce that Latin American consumers face a persistent baseline probability of compromise each time they access unlicensed media services.

Piracy Service Type	Colombia	Ecuador	Mexico	Argentina	Peru	Chile	Average
Sports	0.67	0.83	1.33	0.57	0.90	0.70	**0.83**
Streaming	4.37	2.00	1.93	1.60	2.40	2.27	**2.43**
IPTV Retransmission	1.50	1.30	1.90	1.20	1.10	1.20	**1.37**
IPTV Subscription	1.00	0.50	0.33	0.53	0.50	0.67	**0.59**
Anime	1.17	1.03	1.37	0.87	0.70	0.97	**1.02**
P2P	3.00	2.80	2.83	2.77	3.10	2.40	**2.82**
Scam	2.07	2.07	2.03	1.87	2.00	1.77	**1.97**
Control	0.00	0.00	0.00	0.10	0.03	0.07	**0.03**
Average	1.72	1.32	1.47	1.19	1.34	1.26	**1.38**

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

Piracy Service Type	Colombia	Ecuador	Mexico	Argentina	Peru	Chile	Average
Sports	0.50	0.37	0.73	0.47	0.40	0.53	**0.50**
Streaming	1.60	1.23	1.30	1.47	1.20	1.30	**1.35**
IPTV Retransmission	0.67	0.63	0.93	0.63	0.60	0.53	**0.67**
IPTV Subscription	0.43	0.27	0.17	0.27	0.30	0.40	**0.31**
Anime	0.73	0.90	1.00	0.70	0.60	0.83	**0.79**
P2P	1.90	2.00	2.00	1.93	1.53	1.73	**1.85**
Scam	0.87	0.77	0.90	0.80	0.83	0.70	**0.81**
Control	0.00	0.00	0.00	0.10	0.03	0.07	**0.03**
Average	0.84	0.77	0.88	0.80	0.69	0.76	**0.79**

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 each country 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 (69.28×), Streaming (61.83×), and Scam (48.36×). Notable extreme values included 131× for Streaming in Colombia, representing a two-order-of-magnitude increase over the background risk level of general web traffic.

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 (44.72×) and Streaming (32.36×) persisted as the dominant risk categories, followed by Scam (19.92x) and Anime (19.42x). 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	Colombia	Ecuador	Mexico	Argentina	Peru	Chile	Average
Sports	20.00	25.00	40.00	5.67	27.00	10.50	**21.36**
Streaming	131.00	60.00	58.00	16.00	72.00	34.00	**61.83**
IPTV Retransmission	45.00	39.00	57.00	12.00	33.00	18.00	**34.00**
IPTV Subscription	30.00	15.00	10.00	5.33	15.00	10.00	**14.22**
Anime	35.00	31.00	41.00	8.67	21.00	14.50	**25.20**
P2P	90.00	84.00	85.00	27.67	93.00	36.00	**69.28**
Scam	62.00	62.00	61.00	18.67	60.00	26.50	**48.36**
Average	59.00	45.14	50.29	13.43	45.86	21.36	**39.18**

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

Piracy Service Type	Colombia	Ecuador	Mexico	Argentina	Peru	Chile	Average
Sports	15.00	11.00	22.00	4.67	12.00	8.00	**12.11**
Streaming	48.00	37.00	39.00	14.67	36.00	19.50	**32.36**
IPTV Retransmission	20.00	19.00	28.00	6.33	18.00	8.00	**16.56**
IPTV Subscription	13.00	8.00	5.00	2.67	9.00	6.00	**7.28**
Anime	22.00	27.00	30.00	7.00	18.00	12.50	**19.42**
P2P	57.00	60.00	60.00	19.33	46.00	26.00	**44.72**
Scam	26.00	23.00	27.00	8.00	25.00	10.50	**19.92**
Average	28.71	26.43	30.14	8.95	23.43	12.93	**21.77**

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

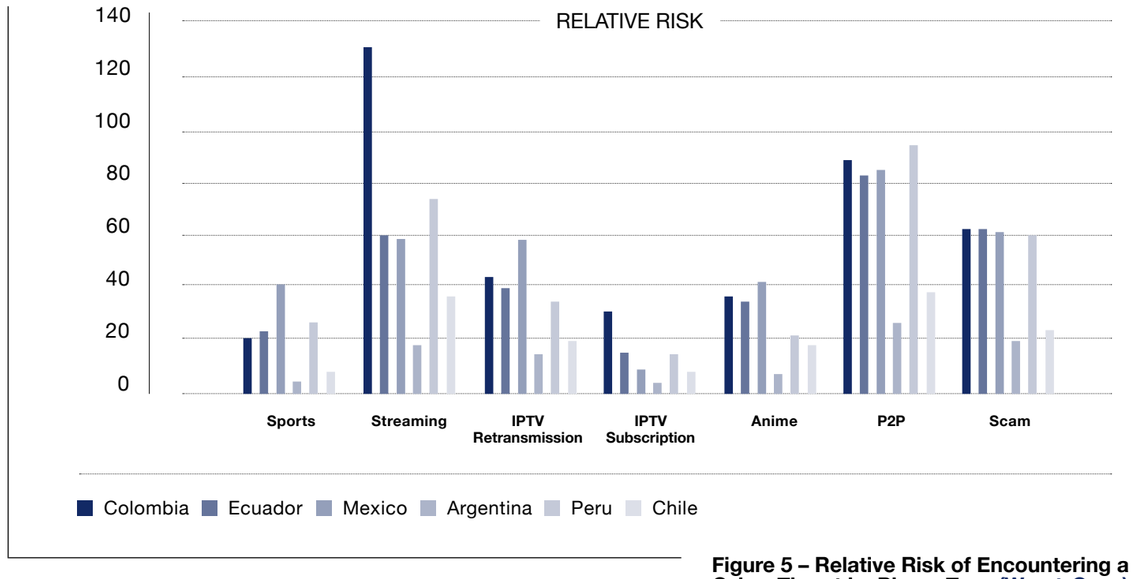


Figure 5 – Relative Risk of Encountering a Cyber Threat by Piracy Type (Worst-Case)

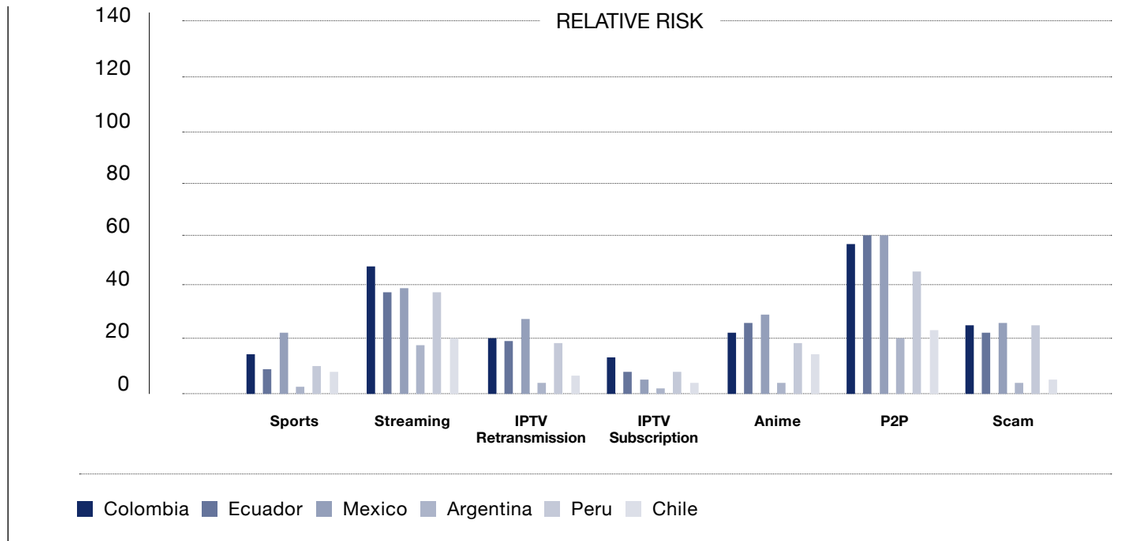


Figure 6 – Relative Risk of Encountering a Cyber Threat by Piracy Type (Best-Case)

Figure 7 shows a heatmap to summarize the worst-case results. The heatmap provides a powerful visual overview of the relative cyber risk associated with different piracy modalities across six Latin America countries. Compared to the raw data table, the heatmap quickly highlights several key patterns:

- P2P piracy consistently presents the highest risk across all countries, with exceptionally high values in Peru and Colombia.
- Colombia exhibits elevated risks across almost all piracy types and exhibited the single highest value record in the study for Streaming – 131 detections.
- Argentina stands out for its uniformly low risk levels in every modality, as clearly reflected by the lighter colors throughout its column.
- IPTV Subscription generally poses lower risks relative to other piracy types, with the exception of a marked spike in IPTV Subscription risk for Colombia.
- Scam sites represent a significant risk in Colombia, Ecuador, Mexico and Peru, reinforcing the need for targeted consumer protection strategies.

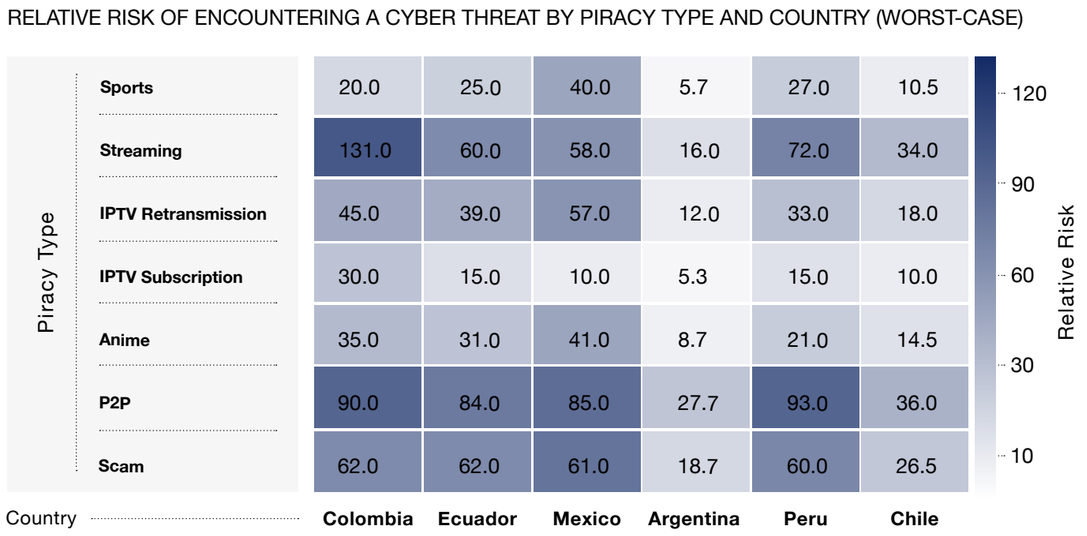


Figure 7 – Relative Risk of Encountering a Cyber Threat by Piracy Type (Worst-Case)

Regional Patterns

Colombia recorded the highest overall exposure across multiple categories, particularly Streaming and IPTV Subscription services, reflecting a dense ecosystem of aggregation sites with minimal security hardening. Argentina, Peru and Chile showed lower absolute detection counts yet still maintained relative risks well above background web baselines, demonstrating that no market in the study presented a “cyber safe” piracy environment.

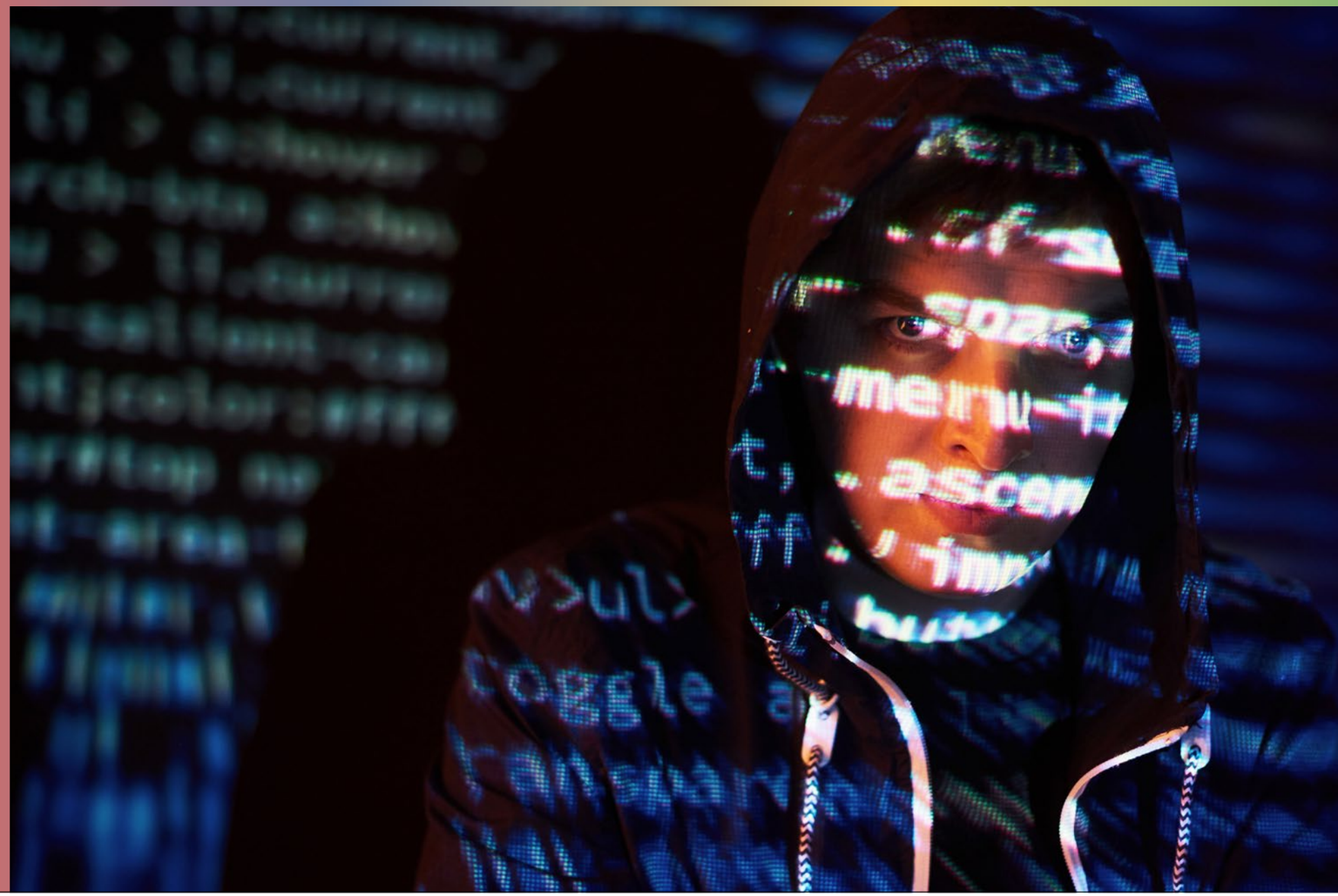
Despite economic and infrastructural differences across the six countries, the risk hierarchy by service type – P2P > Streaming > Scam > Anime > IPTV > Sports – remained relatively stable. This alignment with Southeast Asian patterns[66] indicates a global convergence in the operational and technical structures of piracy-linked cybercrime. The same monetization mechanisms – malvertising networks, drive-by downloads, and fraudulent “piracy-as-a-service” models – appear to underpin both regions’ ecosystems, suggesting coordinated or at least shared threat infrastructures spanning multiple continents.

04

Discussion and Conclusions

Discussion and Conclusions

The results confirm that piracy ecosystems across Latin America present systemic and persistent cybersecurity risks to consumers. Regardless of country or service type, every piracy category analyzed contained active or potential threats. Even under conservative best-case assumptions, users were over twenty times more likely to encounter malware or phishing content on piracy sites than on legitimate platforms. These findings mirror those observed in Southeast Asia, indicating a shared and globally convergent threat architecture in which piracy and cybercrime have become functionally intertwined.



Threat Composition and Attack Surface

The dominance of P2P and Streaming platforms as high-risk vectors reflects both their technical architectures and their widespread popularity. P2P networks inherently expose users to executable file transfers and unverified archives, while streaming portals rely heavily on embedded media players and ad-exchange monetization frameworks that enable malvertising, drive-by exploitation, and credential harvesting.

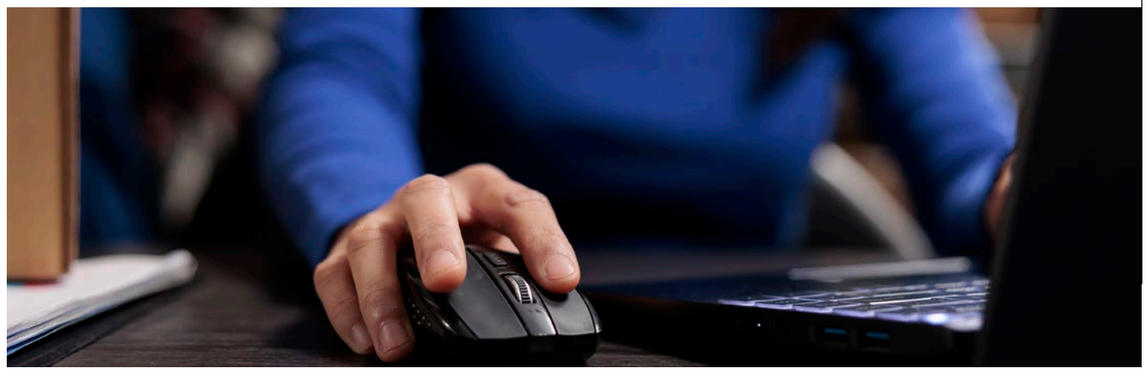
Equally significant is the proliferation of Scam piracy sites – domains that imitate illicit streaming portals but deliver no genuine content. Instead, these sites serve as bait environments for payment fraud, data harvesting, and forced malware redirects. Their high relative-risk ratios confirm that cybercriminals increasingly exploit the *expectation* of free content, transforming deception itself into a scalable cybercrime strategy.

Recent technical analysis of illicit streaming devices used to access pirated Premier League content demonstrates systematic residential proxy behavior[67]. Network traffic analysis identified thousands of SOCKS5 handshakes, high client fan-in, and encrypted tunnel negotiation consistent with commercial residential proxy services. These findings indicate that piracy ISDs are not passive endpoints but active nodes in global proxy networks, allowing third parties to route arbitrary traffic through Latin American households. Such proxying enables fraud, credential stuffing, malware distribution, and evasion of geoblocking and law-enforcement controls, while exposing consumers to reputational and legal risk.

Socio-Economic and Behavioral Drivers

Piracy in Latin America exists within an environment characterized by strong consumer demand for entertainment, and near-universal mobile connectivity. For many users, legitimate streaming platforms remain unaffordable, while Android-based smart TVs and smartphones enable the rapid installation of unlicensed apps. These conditions create a fertile market for IPTV and P2P alternatives.

Behavioral norms compound these risks. Widespread piracy normalization – the perception that accessing unlicensed content carries little consequence – reduces user vigilance regarding site authenticity or file provenance. Many users disable protective features, ignore browser warnings, or install “cracked” applications that silently install malware. As a result, even low-level exposure rapidly scales into genuine compromise, particularly where endpoint protection and patching discipline are weak.



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

Relative-risk ratios observed across Latin America align closely with those documented in Southeast Asia, suggesting that piracy-linked cybercrime now operates as a globalized illicit service economy. The replication of hosting infrastructure, ad-network identifiers, and malware signatures across regions indicates significant cross-border reuse and possibly shared operator groups.

These findings highlight the importance of network-level disruption as a defensive measure. As demonstrated by Herps et al. (2025)[68], *swift, systematic website blocking* – implemented through coordinated action between rights holders, ISPs, and cybersecurity regulators – can achieve measurable cybersecurity benefits. Their analysis showed that persistent blocking of known piracy domains led to a sustained reduction in national malware infection rates and phishing incidents.

Applied to the Latin American context, this approach could deliver similar dividends. Timely, targeted blocking of high-risk domains – especially scam and malware-serving portals – would reduce exposure while complementing traditional copyright enforcement. Regional collaboration between CERTs and telecommunications regulators could further enhance resilience, converting what is often perceived as a copyright measure into a public-interest cybersecurity intervention.

Behavioral Interventions and Demand-Side Mitigation

While technical countermeasures can limit access to harmful sites, behavioral interventions are equally essential to address the demand side of piracy. Emerging evidence from deterrence research and human–computer interaction suggests that real-time, context-aware messaging – including pop-up warnings, automated chatbots, and interstitial notices – can measurably influence user decisions at the moment of risk[69].

Automated systems have been used to interrupt harmful online behaviors in domains ranging from fraud to child exploitation, by combining legal reminders, moral framing, and referral pathways to legitimate alternatives. In the context of piracy, these interventions could warn users when they attempt to access or download from known high-risk domains, providing information about the cyber and privacy dangers rather than moral or punitive appeals.

Chatbots, for example, could engage users conversationally to redirect them toward legitimate streaming options or public awareness resources, a model currently under evaluation in cyber-safety initiatives targeting youth audiences[70]. Deployed alongside blocking and takedown programs, such “soft deterrence” mechanisms could reduce repeated exposure while avoiding punitive enforcement, aligning with a harm-reduction approach to online safety.

Consumer Risk and Policy Implications

The evidence positions piracy exposure not as a passive by-product of copyright infringement but as an active cyber-safety hazard. High detection densities in Colombia and the other nations correspond to large-scale consumer exposure to credential theft, spyware, and payment fraud. The persistence of scam piracy sites – essentially fake portals masquerading as content sources – illustrates that this ecosystem now functions as a malware distribution infrastructure rather than a cultural or moral issue alone.

Policy frameworks in Latin America should therefore expand from intellectual property enforcement to encompass consumer protection and digital resilience. Following the approach validated by Herps et al. (2025), rapid blocking of verified malicious piracy domains should be classified as a cybersecurity measure. Complementary behavioral interventions – including warnings, chatbots, and educational messaging – should be integrated into national digital literacy strategies, helping users recognize that accessing pirated content exposes them to measurable cyber harm.

The consistently high levels of risk identified across Latin American markets underscore the urgent need for coordinated responses at both national and regional levels. In line with findings from Asia-Pacific, proportionate and transparent site blocking regimes should be considered as part of government responsibility, alongside strengthened law enforcement capability in digital forensics and cyber incident response, and comprehensive public awareness campaigns tailored to local contexts. By implementing these measures, policymakers can help reduce consumer exposure to malware, phishing, scams, and other cyber harms linked to piracy - ultimately protecting digital citizens and supporting the region's growing digital economies.

Furthermore, evidence from technical analysis of ISDs in Southeast Asia shows that many devices establish persistent, privileged connections to overseas servers, enabling direct remote access to the device and, in some cases, the surrounding local network[71]. These connections bypass normal user authentication and operate independently of consumer awareness or consent. While this behavior was documented in the Malaysian market, the same device families and application ecosystems are widely distributed in Latin America. As a result, similar risks - including covert surveillance, data exfiltration, and unauthorized network access - should be considered present by default in Latin American piracy ecosystems, absent evidence to the contrary.

Many piracy-enabled devices and applications maintain persistent outbound connections to servers located in China, raising additional concerns regarding data sovereignty, cross-border data transfer, and the absence of meaningful consumer recourse. Consumers may have their viewing habits, credentials, network metadata, or device fingerprints transferred offshore without consent or regulatory protection.

Limitations and Future Work

This study, like prior regional analyses, relies on VirusTotal detection aggregates as a proxy for active compromise. While effective for large-scale comparison, vendor heterogeneity and sampling bias may influence precision. Furthermore, the analysis excludes closed IPTV subscription networks, encrypted messaging channels, and private social media groups, which represent an additional component of the piracy landscape in Latin America.

Future research should integrate behavioral data collection, including user response to warning messages and chatbots, to evaluate intervention effectiveness in situ. Longitudinal measurement of national blocking outcomes – following the Herps et al. (2025) methodology – could quantify reductions in infection prevalence and phishing victimization. Coupled with dynamic malware execution studies, such research would provide a holistic view of both technical and human factors shaping piracy-related risk.

Summary

Latin America's piracy ecosystem exhibits the same structural vulnerabilities, monetization models, and infection vectors observed globally. The results demonstrate that cyber risk in this environment is predictable, preventable, and addressable through coordinated interventions. Research confirms that decisive, systematic blocking can meaningfully reduce consumer exposure, while behavioral deterrence tools – such as warning systems and chatbots – offer scalable, non-punitive means of influencing user choices. Collectively, these strategies underscore that effective piracy mitigation is not merely a copyright objective but a cybersecurity and public-safety imperative.

Both IIPA and MPA stress that enforcement coordination[72] – particularly among Mexico, Colombia, and other Pacific Alliance members – has yielded early progress[73]. However, sustainable deterrence will depend on harmonized legal frameworks, stronger judicial follow-through, and public–private collaboration. The MPA argues that "light-touch regulation of digital services," paired with dynamic site-blocking and notice-and-stay-down systems, offers an effective balance between legitimate trade and consumer protection. Integrating these models within broader cybercrime and consumer-protection policies could help Latin American governments frame anti-piracy enforcement as a digital-resilience issue, rather than solely a copyright or trade concern.

Policymakers should treat the concentration of piracy device supply chains and malware infrastructure in PRC-linked ecosystems as a strategic risk factor when assessing consumer cybersecurity, device importation, and site-blocking regimes. Ultimately, the cybersecurity risks faced by Latin American consumers are not confined to local piracy behavior. They reflect structural dependencies on opaque global supply chains, with a disproportionate reliance on PRC-manufactured devices, software, and infrastructure. Addressing piracy-related cyber risk therefore requires not only enforcement and education, but a clear-eyed assessment of upstream geopolitical and supply-chain exposure.

05

Appendices

Appendix A – Colombia Results by Piracy Service Type

Appendix B – Ecuador Results by Piracy Service Type

Appendix C – Mexico Results by Piracy Service Type

Appendix D – Argentina Results by Piracy Service Type

Appendix E – Peru Results by Piracy Service Type

Appendix F – Chile Results by Piracy Service Type

Appendix A – Colombia
Results by Piracy Service Type

BEST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	9	4	0	2	0
Streaming	16	22	7	2	1
IPTV Retransmission	6	10	2	2	0
IPTV Subscription	4	7	0	2	0
Anime	7	9	2	0	4
P2P	23	23	3	0	8
Scam	7	15	3	0	1
Control	0	0	0	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	10	8	0	2	0
Streaming	29	83	15	3	1
IPTV Retransmission	8	29	5	3	0
IPTV Subscription	5	22	0	3	0
Anime	9	20	2	0	4
P2P	38	41	3	0	8
Scam	8	45	8	0	1
Control	0	0	0	0	0

Appendix B – Ecuador
Results by Piracy Service Type

BEST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	7	2	1	1	0
Streaming	15	19	1	1	1
IPTV Retransmission	6	9	2	2	0
IPTV Subscription	3	4	0	1	0
Anime	9	11	1	1	5
P2P	23	24	4	0	9
Scam	6	14	3	0	0
Control	0	0	0	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	7	13	4	1	0
Streaming	23	34	1	1	1
IPTV Retransmission	6	26	5	2	0
IPTV Subscription	4	9	0	2	0
Anime	10	14	1	1	5
P2P	26	45	4	0	9
Scam	7	47	8	0	0
Control	0	0	0	0	0

Appendix C – Mexico
Results by Piracy Service Type

BEST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	10	8	2	1	1
Streaming	14	22	0	1	2
IPTV Retransmission	9	13	3	3	0
IPTV Subscription	1	3	0	1	0
Anime	13	8	2	1	6
P2P	24	23	4	0	9
Scam	7	16	4	0	0
Control	0	0	0	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	11	22	5	1	1
Streaming	20	35	0	1	2
IPTV Retransmission	11	35	7	4	0
IPTV Subscription	2	6	0	2	0
Anime	16	16	2	1	6
P2P	28	44	4	0	9
Scam	8	44	9	0	0
Control	0	0	0	0	0

Appendix D – Argentina
Results by Piracy Service Type

BEST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	8	4	1	1	0
Streaming	16	22	3	1	2
IPTV Retransmission	6	9	2	2	0
IPTV Subscription	3	4	0	0	1
Anime	7	8	1	0	5
P2P	23	23	4	0	8
Scam	7	15	2	0	0
Control	0	2	1	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	9	6	1	1	0
Streaming	16	26	3	1	2
IPTV Retransmission	8	23	2	3	0
IPTV Subscription	5	9	0	0	2
Anime	8	12	1	0	5
P2P	26	45	4	0	8
Scam	8	42	6	0	0
Control	0	2	1	0	0

Appendix E – Peru Results by Piracy Service Type

BEST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	7	3	2	0	0
Streaming	11	20	3	1	1
IPTV Retransmission	6	8	2	2	0
IPTV Subscription	3	4	0	2	0
Anime	6	7	0	1	4
P2P	19	18	3	0	6
Scam	9	14	2	0	0
Control	1	0	0	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	8	14	5	0	0
Streaming	17	47	6	1	1
IPTV Retransmission	8	21	2	2	0
IPTV Subscription	4	8	0	3	0
Anime	7	9	0	1	4
P2P	23	55	9	0	6
Scam	11	43	6	0	0
Control	1	0	0	0	0

Appendix F – Chile Results by Piracy Service Type

BEST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	9	5	0	2	0
Streaming	15	19	2	1	2
IPTV Retransmission	5	8	2	1	0
IPTV Subscription	4	6	0	2	0
Anime	11	8	1	0	5
P2P	22	22	1	0	7
Scam	4	14	3	0	0
Control	0	1	1	0	0

WORST-CASE

Service Type	Suspicious	Malicious	Phishing	Spam	Not Recommended
Sports	10	9	0	2	0
Streaming	22	39	4	1	2
IPTV Retransmission	5	25	5	1	0
IPTV Subscription	5	12	0	3	0
Anime	12	11	1	0	5
P2P	26	38	1	0	7
Scam	5	40	8	0	0
Control	0	1	1	0	0

06

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. BankInfoSecurity. (2025). *FBI warns of BADBOX 2.0 botnet surge in Chinese devices*. BankInfoSecurity. https://www.bankinfosecurity.com/fbi-warns-badbox-20-botnet-surge-in-chinese-devices-a-28616
13. Dark Reading Staff. (2023). *Badbox operation targets Android devices in fraud schemes*. Dark Reading. https://www.darkreading.com/vulnerabilities-threats/badbox-operation-targets-android-devices-in-fraud-schemes
14. 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.
15. Watters, P. (2025). *Consumer risk from piracy in Southeast Asia*. SSRN. https://ssrn.com/abstract=5371543
16. 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
17. 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
18. 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
19. International Intellectual Property Alliance. (2025, January). *2025 Special 301 Report on copyright protection and enforcement*. Washington, DC: IIPA. https://www.iipa.org/reports/special-301-reports
20. 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.
21. 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).
22. 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.
23. Alex, P. (2013). *Piracy and the digital revolution in Latin America: Cultural consumption and resistance. International Journal of Cyber Criminology*, 7(1), 1–15.
24. 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
25. Motion Picture Association. (2025). *Submission for the 2026 National Trade Estimate Report on Foreign Trade Barriers*. Washington, DC: MPA
26. Belchior-Rocha, A., et al. (2024). Unveiling the Ethical Dilemmas of Digital Piracy. *Social Sciences, 13*(11), 579.
27. Inter-American Development Bank. (2022). *Intellectual Property Rights and Public Policies for the Creative Economy in Latin America and the Caribbean: Recommendations*. Washington, DC
28. Yoon, C. (2011). Theory of planned behavior and ethics theory in digital piracy: An integrated model. *Journal of Business Ethics*, *100*(3), 405–417.
29. 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
30. Terra, A. (2016). Copyright law and digital piracy: an econometric global cross-national study. *NCJL & Tech.,18*, 69.
31. 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
32. Parks Associates. (2023). *Consumer attitudes toward piracy* [Research report]. Parks Associates. https://www.parksassociates.com/storage/medias/7574f23a52abca4389d60fff00ff78ac10553e131f93f9fd6f06.pdf
33. 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
34. Toulas, B. (2024). *Free VPN apps on Google Play turned Android phones into proxies*. BleepingComputer. https://www.bleepingcomputer.com/news/security/free-vpn-apps-on-google-play-turned-android-phones-into-proxies
35. Broadband TV News. (2025). *ACE steps up campaign against piracy via sideloaded apps.* https://www.broadbandtvnews.com/2025/12/04/ace-steps-up-campaign-against-piracy-via-sideloaded-apps/
36. Fortra. (2023). *2023 Domain Impersonation Report*. Fortra. https://static.fortra.com/corporate/pdfs/other/fta-domain-impersonation-report-2023.pdf
37. 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
38. Motion Picture Association. (2025). *Submission for the 2026 National Trade Estimate Report on Foreign Trade Barriers*. Washington, DC: MPA
39. 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
40. 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
41. 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
42. 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
43. Federal Bureau of Investigation. (2025). *Home internet connected devices facilitate criminal activity (PSA250605)*. Internet Crime Complaint Center (IC3). https://www.ic3.gov/PSA/2025/PSA250605
44. Watters, P. (2025). *Cybersecurity harms and illicit streaming devices* (SSRN Scholarly Paper No. 5800843). Social Science Research

Bibliography

Network. https://doi.org/10.2139/ssrn.5800843

45. Chan, E. (2025). *Singapore police, cybersecurity agency warn of malware in non-certified Android TV boxes*. CNA. https://www.channelnewsasia.com/singapore/police-cyber-security-agency-warn-illegal-streaming-devices-android-tv-set-top-box-hacking-malware-5462401
46. Turing, A., Acey9, & rootkiter. (2024). *Bigpanzi exposed: The hidden cyber threat behind your set-top box*. Qianxin XLab. https://blog.xlab.qianxin.com/bigpanzi-exposed-hidden-cyber-threat-behind-your-stb/
47. 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
48. Tsang, A. (2025). *Latin America: Evolving e-commerce market landscape.* HKTDC Research. https://research.hktdc.com/en/article/MTkwNzk4MDYyMQ
49. Gallagher, T., Navajas, S., Herrera, D., & Zárate Moreno, A. (2025). Five drivers reshaping finance in Latin America and the Caribbean. IDB Invest. https://www.idbinvest.org/en/blog/digital-economy/five-drivers-reshaping-finance-latin-america-and-caribbean
50. 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
51. Lockett, A., 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
52. Neira, S. (2025). *Por qué usar Magis TV en el PC es un riesgo de espionaje: así acceden a la información.* Infobae. https://www.infobae.com/tecno/2025/05/28/por-que-usar-magis-tv-en-el-pc-es-un-riesgo-de-espionaje-asi-acceden-a-la-informacion/
53. Melo, Y. (2025). *MagisTV en Perú: la moda del streaming gratuito expone a usuarios a graves riesgos de seguridad. Infobae Perú.* https://www.infobae.com/peru/2025/09/27/magistv-en-peru-la-moda-del-streaming-gratuito-expone-a-usuarios-a-graves-riesgos-de-seguridad
54. Gobierno de México. (2017). *Estrategia Nacional de Ciberseguridad (ENCS) – Executive Summary*. Secretaría de Gobernación. https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf
55. Política Nacional de Ciberseguridad 2023-2028 (Chile). (2023). *Política Nacional de Ciberseguridad 2023-2028.* Agencia Nacional de Ciberseguridad (ANCI). Retrieved from https://anci.gob.cl/pncs-2023-2028/
56. Consejo Nacional de Política Económica y Social [CONPES]. (2020). *CONPES 3995: Política Nacional de Confianza y Seguridad Digital.* Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf
57. Vela-Treviño, C., Villanueva-Plasencia, D., & Bojalil-Warth, P. (2025). *Mexico: From 2010 to 2025 – Evolution of the new Federal Law on the Protection of Personal Data Held by Private Parties.* Baker McKenzie InsightPlus. https://connectontech.bakermckenzie.com/mexico-from-2010-to-2025-evolution-of-the-new-federal-law-on-the-protection-of-personal-data-held-by-private-parties-2/
58. Biblioteca del Congreso Nacional. (2024). *Ley N.° 21.719 que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.* https://www.leychile.cl/leychile/Navegar?idNorma=1209272&idVersion=2026-12-01
59. Observatorio Legislativo CELE. (2020). *Law 25.326 – Personal Data Protection Act (PDPA) of Argentina.* https://observatoriolegislativocele.com/en/personal-data-a/
60. Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.* Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492
61. Congreso de la República. (2011). *Ley N.° 29733 – Ley de Protección de Datos Personales.* https://www.gob.pe/institucion/pcm/normas-legales/243470-29733
62. Ecuador: Asamblea Nacional. (2021). *Ley Orgánica de Protección de Datos Personales (Registro Oficial Suplemento No. 459, 26-V-2021).* https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf
63. Fundación Chile. (2024). *Talento Digital para Chile.* https://fch.cl/iniciativa/talento-digital-para-chile/
64. For more details of how VirusTotal works, see https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works
65. 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
66. Watters, P. (2025). *Consumer risk from piracy in Southeast Asia.* Cyberstronomy Pty Ltd. SSRN. https://doi.org/10.2139/ssrn.5371543
67. 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
68. 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
69. 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
70. 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.
71. 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
72. Motion Picture Association. (2025). *Submission for the 2026 National Trade Estimate Report on Foreign Trade Barriers.* Washington, DC: MPA
73. López-Leyva, S., & Martínez, J. G. (2024). *Isomorphism: A pathway to institutionalize intellectual property in the Pacific Alliance*. Management Dynamics in the Knowledge Economy, 12(3), 285–301. https://doi.org/10.2478/mdke-2024-0017

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*-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