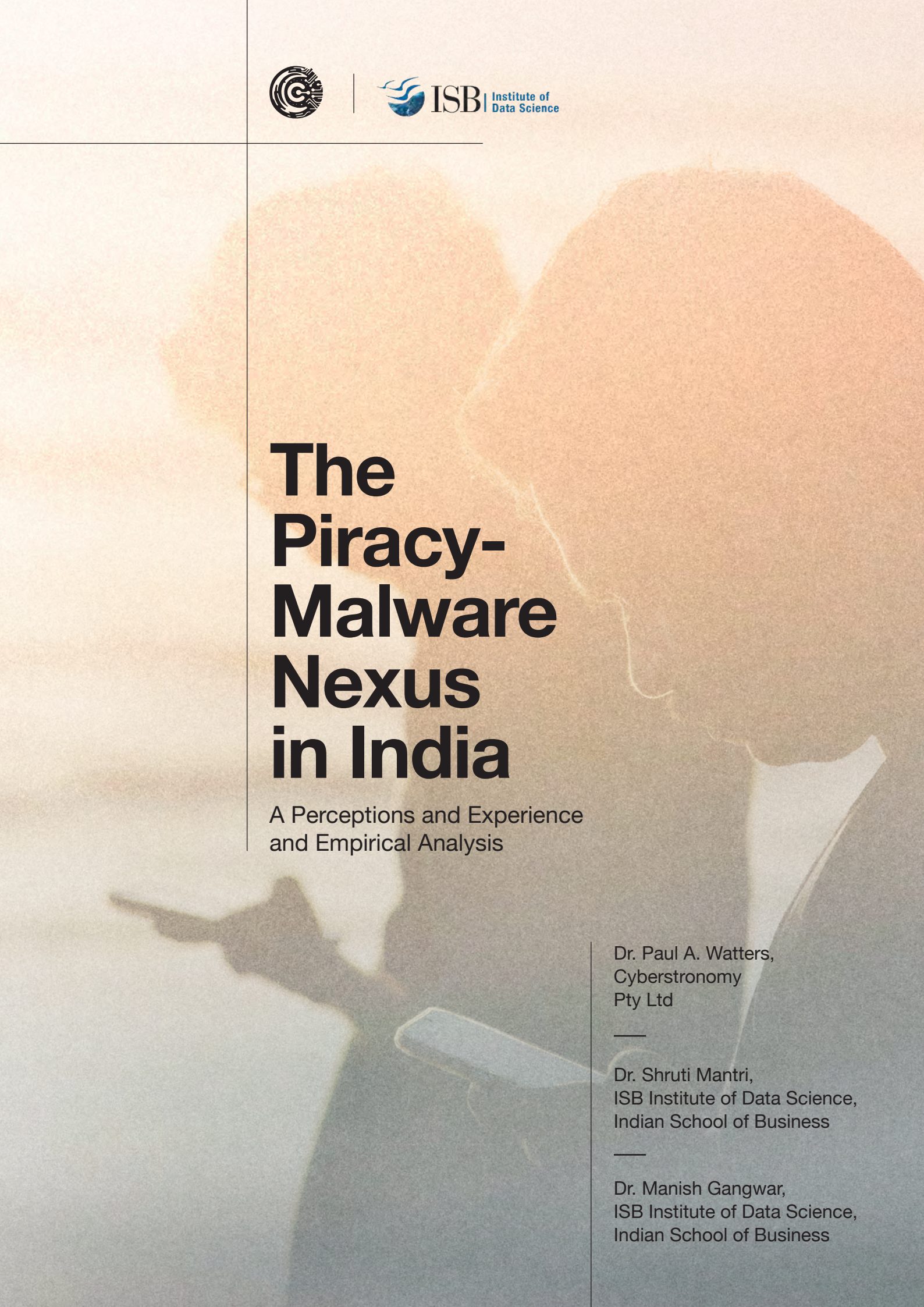


# The Piracy-Malware Nexus in India

A Perceptions and Experience and Empirical Analysis

Dr. Paul A. Watters,
Cyberstronomy
Pty Ltd

Dr. Shruti Mantri,
ISB Institute of Data Science,
Indian School of Business

Dr. Manish Gangwar,
ISB Institute of Data Science,
Indian School of Business

# Contents

# Key Findings and Recommendations

## Key Findings

**Piracy websites** pose a

**59%**

risk of malware infection for Indian consumers.

**Adult industry ads** pose a

**57%**

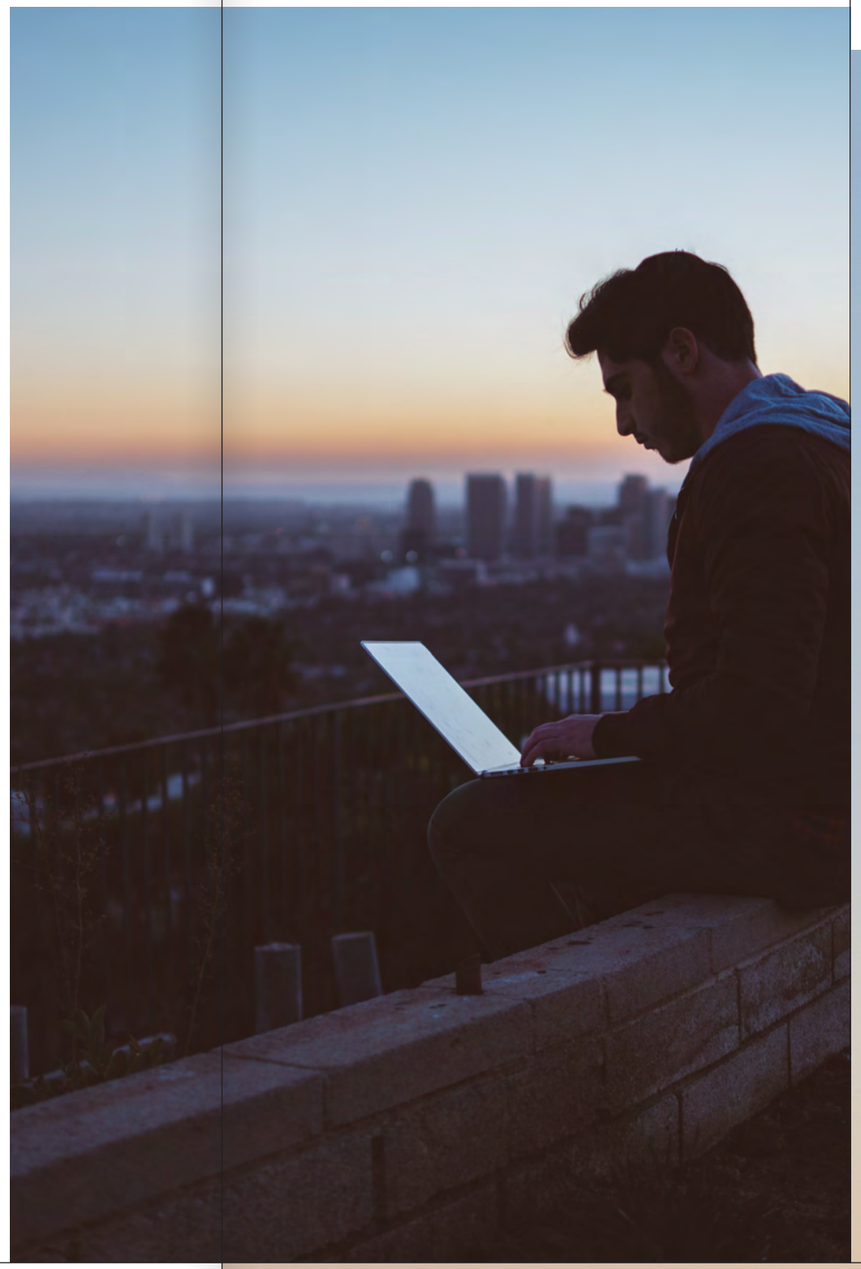
risk of malware infection for Indian consumers.

**Gambling ads** pose a

**53%**

risk of malware infection for Indian consumers.

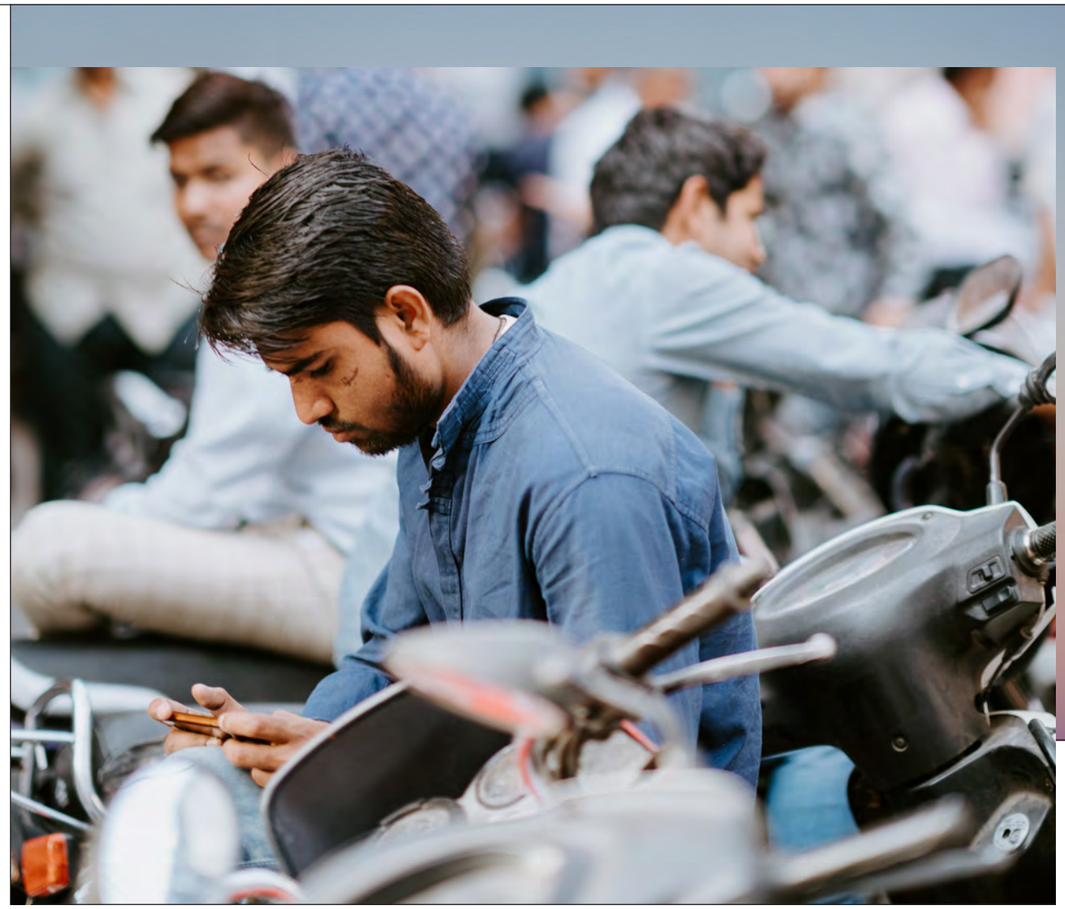
- A nationally representative Perceptions and Experience study reveals that Indian consumers ranked their relative risk of downloading malware from piracy sites at 2.03 times greater than from mainstream websites.
- Piracy websites presented the highest risk for Indian consumers of malware infection (59%) followed by accessing adult industry ads (57%) and accessing gambling ads (53%).
- Young people aged 18-24 illustrated a higher propensity of accessing piracy websites, yet also demonstrated the lowest levels of awareness of cyber risk.
- Empirical analysis using Google's VirusTotal of the top and mid-range piracy and scam sites in India reveals that the actual relative risk to consumers is 10.5 times greater for top and mid-range piracy sites, 15.5 for top scam sites, and 9 for mid-range scam sites, when compared to a set of control sites.
- The cyber risks identified – including malicious and suspicious websites, malware, and phishing – can lead to identity theft and identity fraud, as well as potentially providing remote access and opportunities for data exfiltration and other data breaches.



## Key Recommendations

- Government to place a higher priority to digital copyright crimes in India, and train and resource appropriate law enforcement agencies. This would bring offenders to justice, and provide a clear and visible deterrent.
- Deliver demographically targeted awareness, training and education campaigns to deter consumers from accessing piracy websites and reduce risky cyber behavior, especially among the young demographic aged 18-24.
- Establish uniform, state-level cybercrime law (to include IP crimes) and enforcement procedures and state-level IP crime units across the country, to ensure proper investigation of IP crimes, including Internet piracy.

# Executive Summary



**This study investigated the link between digital piracy and cyber threats (such as malware) in India. The study used a Perceptions and Experience methodology and an Empirical analysis. The Perceptions and Experience methodology involves a consumer survey to explore questions around consumer understanding of the link between malware and piracy.**
**The Empirical analysis focuses on the relative risk of encountering cyber threats, both in terms of severity and likelihood, when compared to mainstream controls. Such analysis uses industry standard detection of suspicious and malicious sites by Google's VirusTotal product.**

In the Perceptions and Experience study, a nationally representative sample of Indian consumers aged 18+ rated the risk of getting a malware infection from piracy sites ahead of getting a malware infection from adult industry and gambling ads, and identified a relative risk of 2.03 times the rate for social media platforms and other mainstream websites. Young people aged 18-24 illustrated the riskiest behaviour, but the lowest awareness of risk.

In the Empirical study, the relative risk of malware infection and related cyber security risks was measured by conducting an experiment using Google's VirusTotal, comparing a sample of the most popular and mid-range piracy sites in India, compared to both a control group of the most popular mainstream websites, as well as to "scam" piracy sites, that actually contain no pirated content. Using the most conservative methodology, where multiple instances within each threat category were counted only once, it was found that the relative risk of encountering a cyber threat on either top-ranked or mid-range piracy sites was 10.5 times greater, rising to 15.05 for top-ranked scam piracy sites, and 9 for mid-range scam sites when compared to the control group. Comparing the actual relative risk of between 9-15.05 times from the Empirical study, with the 2.03 times greater risk of malware infection perceived by consumers in the Perceptions and Experience study, it is clear that Indian consumers are significantly underestimating their cyber risk from visiting piracy sites.

The implications of these risk findings are discussed in this report, as well as a range of recommendations provided to protect Indian consumers – including (a) government placing a higher priority on digital copyright crimes and enforcement, and taking firm action against the largest piracy syndicates and (b) implementing demographically targeted awareness, training and education campaigns to deter consumers from accessing piracy websites and reduce risky cyber behaviour, especially among the younger demographic (aged 18-24).

# Introduction

# Introduction

**“With its rich cultural heritage, talented artists, and a vast audience base, India remains a powerhouse in the world of entertainment, captivating and inspiring people around the globe.”**

In recent years, India has emerged as a vibrant entertainment powerhouse, captivating global audiences with its diverse array of cultural offerings. The Indian entertainment industry encompasses various forms of media, including film, television, music, and digital content. India’s film industry, popularly known as Bollywood, is the largest film industry in the world in terms of the number of films produced annually. Bollywood films combine elements of romance, drama, music, and dance, often delivering larger-than-life storytelling and captivating song sequences. Apart from Bollywood, India has a thriving regional and arthouse cinema scene. Different regions, such as Tamil Nadu, Telangana, Karnataka, Kerala, Maharashtra and West Bengal, have their own film industries that produce a wide range of high-quality movies. These regional industries have nurtured talented actors, directors, and technicians, contributing to the richness and diversity of Indian cinema.

It’s also important to note that Indian cultural production and consumption extends well beyond cinema. Bollywood music, with its catchy tunes, enjoys immense popularity not only within the country but also among the Indian diaspora worldwide. Beyond Bollywood music, India’s music industry is renowned for a wide range of genres, including classical, folk, devotional, and contemporary music. Indian musicians have collaborated with international artists, bridging cultures and reaching a global audience.

The Indian television industry also boasts a vast array of programming, ranging from soap operas and reality shows to comedy series and game shows. Indian television content has had a significant impact on popular culture and has launched the careers of numerous well-known actors and presenters.

The advent of digital platforms and streaming services has led to a boom in the production and consumption of web series, short films, and other digital content in India. Platforms like Netflix, Amazon Prime Video, Disney+ Hotstar, SonyLIV, Voot, Jio and Zee5 have provided a platform for Indian creators to showcase their talent and reach a global audience. Several regional-language platforms also enjoy a wide subscriber base, such as Sun NXT, Aha, Hoichoi, Koode and Planet Marathi. Indian films have gained international acclaim and recognition, with Indian actors and filmmakers making their mark on the global stage. In recent years, films such as “Masaan” and “The Disciple” have won accolades at prestigious international film festivals, while “Baahubali” and “The Elephant Whisperers” both won Oscars and “Delhi Crime” won an International Emmy. India’s entertainment industry continues to evolve, embracing new technologies and storytelling formats. With its rich cultural heritage, talented artists, and a vast audience base, India remains a powerhouse in the world of entertainment, captivating and inspiring people around the globe.

# The Threat of Piracy

**Digital piracy poses significant risks to India's cultural outputs across various entertainment sectors. It refers to the unauthorized copying, distribution, or sharing of copyrighted content, including movies, music, TV shows, books, software, and other forms of creative works. It involves obtaining and distributing copyrighted material without the permission of the rights holders, often through illegal means. There are many significant risks associated with digital piracy – mainly economic – which are outlined to the right.**

## REVENUE LOSS:

Piracy severely impacts the revenue streams of the Indian entertainment industry. Illegal distribution and sharing of copyrighted content result in substantial financial losses for filmmakers, producers, artists, and other stakeholders – estimated by consulting firm EY to be $3.08b in 2022 alone. This loss of revenue hampers the industry's ability to invest in new projects, talent development, and infrastructure (Telang and Waldfogel, 2014), and also has potential negative tax impacts.

## DIMINISHED PRODUCTION VALUE:

The financial impact of piracy may lead to a reduction in production budgets (Banerjee, 2013). As a result, the quality and production value of films, music albums, and television shows may suffer. This diminishes the overall artistic and entertainment experience for audiences.

## DISCOURAGEMENT OF CREATIVITY:

Piracy discourages creative pursuits and hampers the incentive to produce original content. Content creators invest significant time, effort, and resources into developing new ideas, scripts, music compositions, and visual effects. When their work is stolen and distributed illegally, it undermines their motivation to create, innovate and reinvest.

## THREAT TO JOBS AND LIVELIHOODS:

The entertainment industry in India provides employment to a vast number of people, including actors, directors, technicians, musicians, writers, and production crew members. Piracy can lead to reduced revenue and profitability, resulting in fewer jobs and lower wages for those working in the industry.

## STIFLED GROWTH OF THE INDUSTRY:

The prevalence of piracy can impede the growth of the Indian entertainment industry. Investors and stakeholders may become hesitant to fund projects due to the risks associated with piracy. This reluctance to invest can limit the industry's expansion, hamper technological advancements, and hinder the overall development of the sector.

## COMPROMISED AUDIENCE EXPERIENCE:

Video content available on piracy sites and services often have compromised audio and video quality as well as an enhanced risk of spreading egregious malware. Viewers who consume pirated content may have a subpar experience, as the original intent and quality of the creators may not be fully realized.

## LEGAL AND ETHICAL IMPLICATIONS:

Engaging in digital piracy is an illegal activity that violates both civil and criminal copyright laws. Engaging in or supporting piracy undermines the ethical principles of respecting intellectual property rights. It is important to foster a culture that values and supports original creative work, encouraging legal means of accessing and enjoying entertainment content.

**There have been efforts made by the Indian government, content creators, and industry stakeholders to combat piracy through stricter enforcement, awareness campaigns, and the promotion of legal distribution channels. For example, the Maharashtra Intellectual Property Crimes Unit (MIPCU). But more could be done by the government to protect intellectual property rights and curbing piracy is crucial to safeguarding India's cultural outputs, ensuring a thriving and sustainable entertainment industry for future generations. The findings of this research would also suggest that curbing piracy is crucial to safeguarding the potential risks that digital consumers may face, especially the younger demographic, when accessing piracy sites and services.**

# Piracy and Malware

**Malware, short for malicious software, refers to any software or code that is designed to disrupt, damage, gain unauthorized access to, or exploit computer systems, networks, or user devices. Malware is typically created by cybercriminals with the intent to steal information, compromise privacy, or cause harm to individuals or organizations. As outlined by Watters (2023a), some common types of malware include:**

### VIRUSES:

Viruses are malicious programs that can replicate themselves and spread by attaching to other files or programs. They can cause various damages, such as corrupting or deleting files, slowing down system performance, or even rendering a computer or network inoperable.

### TROJANS:

Trojans, named after the ancient Greek story of the Trojan Horse, are deceptive programs that disguise themselves as legitimate software or files. Once installed, Trojans can perform various malicious activities, such as stealing personal information, creating back doors for remote access, or launching other malware.

### RANSOMWARE:

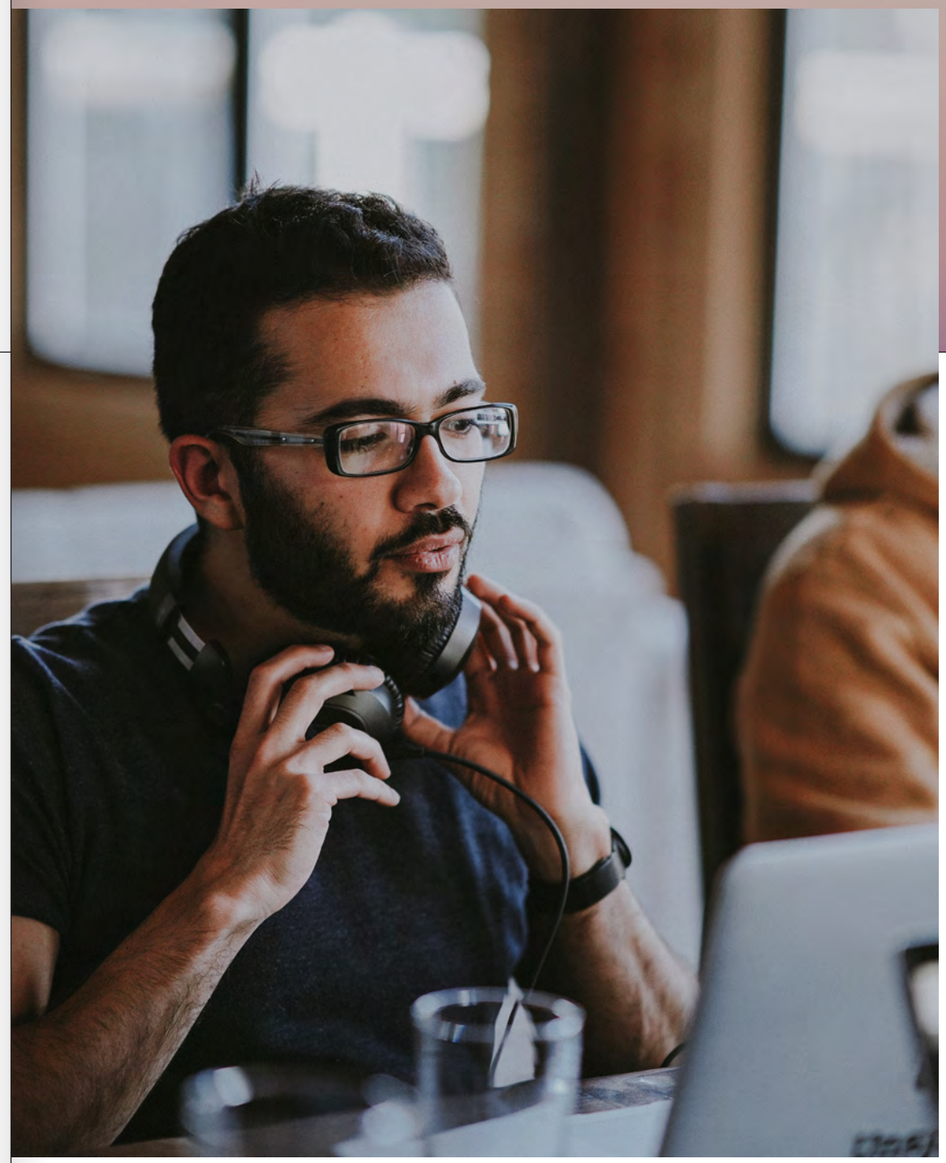
Ransomware is a type of malware that encrypts files on a victim's computer or network, making them inaccessible. The attackers then demand a ransom payment, usually in cryptocurrency, in exchange for providing the decryption key. Ransomware attacks can have severe consequences for individuals and organizations, causing data loss and financial damages.

### SPYWARE:

Spyware is designed to secretly monitor and gather information about a user's activities without their consent. It can track keystrokes, capture screenshots, record online browsing habits, and collect sensitive information like passwords or credit card details. The gathered information is often sent to the attacker, compromising user privacy and security.

### ADWARE:

Adware, short for advertising-supported software, is malware that displays unwanted advertisements on infected systems. It often comes bundled with legitimate software and displays intrusive or misleading ads, redirects web browsers, and collects user information for targeted advertising. While adware is primarily an annoyance, it can also slow down system performance and compromise user privacy.



**Malware plays a significant role in facilitating identity theft and identity fraud by enabling cybercriminals to gain unauthorized access to personal and sensitive information in the following ways (Watters, 2023b):**

### DATA THEFT:

Malware can be designed to collect personal information, such as usernames, passwords, credit card details, social security numbers, or other sensitive data. This information can then be transmitted to the attackers, who can misuse it for identity theft or fraud purposes.

### KEYLOGGING:

Some types of malware, such as keyloggers, record keystrokes on infected devices. This allows cybercriminals to capture usernames, passwords, and other confidential information entered by the victim. The recorded data is then used to gain unauthorized access to online accounts or commit identity theft.

### PHISHING ATTACKS:

Malware can be utilized in phishing attacks, where victims are deceived into revealing their personal information or login credentials through fake websites, emails, or messages. Malicious software can be embedded in these phishing attempts to collect the entered data and compromise the victim's identity.

### REMOTE ACCESS:

Certain malware, like Remote Access Trojans (RATs), allows cybercriminals to gain remote control of infected devices. This enables unauthorized access to personal files, financial information, or sensitive data stored on the victim's system, potentially leading to identity theft or fraud.

### IDENTITY SPOOFING:

Malware can be employed to create fake or malicious websites that mimic legitimate organizations, such as banks, e-commerce platforms, or government agencies. Victims unknowingly enter their personal information on these fake sites, believing them to be genuine, thereby exposing themselves to identity theft or fraud.

Once cybercriminals acquire personal and sensitive information through malware, they can engage in various fraudulent activities within India (Ghosh, 2021; Pillai, 2023; Saluja, 2022), including:

- Opening fraudulent bank accounts or credit cards in the victim's name
- Making unauthorized financial transactions or purchases using stolen payment details
- Filing false tax returns to fraudulently obtain refunds
- Applying for loans or mortgages using stolen identities
- Committing healthcare fraud by using stolen medical information for insurance claims
- Engaging in identity cloning to assume the victim's identity for various illegal purposes

The link between malware and identity theft/fraud underscores the importance of robust cybersecurity measures, such as using reputable antivirus software, regularly updating systems and applications, practicing safe online browsing habits, and being cautious of suspicious emails or websites. Additionally, being vigilant about monitoring financial statements, credit reports, and taking immediate action if any signs of identity theft or fraud are detected is crucial.



**As demonstrated by extensive past research (Aldriwish, 2021; Blancaflor et al, 2021; Bowman et al, 2022; El Fiky, 2020; Kumari and Chen, 2022; Lee et al, 2019; Suwa, 2021; Watters, 2021), there is a strong relationship between piracy and malware, with piracy often serving as a vector for the distribution of malicious software. Some key ways in which malware and piracy interact include:**

### UNTRUSTED SOURCES:

When users engage in piracy, they often seek out unauthorized channels or websites to download or stream copyrighted content. These sources are typically unregulated and lack proper security measures. As a result, users are more likely to encounter malware-infected files or malicious websites during their piracy activities.

### MALICIOUS DOWNLOADS:

Pirated content, such as movies, music, software, or books, is often bundled with malware or infected with viruses. When users download or access such content from unauthorized sources, they run the risk of inadvertently downloading and installing malware onto their devices. These malicious downloads can compromise system security, privacy, and functionality.

### STREAMING AND TORRENTS:

Piracy is often facilitated through streaming sites and torrent platforms, where users can share and download copyrighted content, often using a mobile platform. These technologies, while not inherently malicious, can be abused by cybercriminals who upload infected files or create fake torrents that entice users into downloading malware-infected content.

### ADWARE AND POP-UPS:

Websites and platforms that host pirated content often rely on advertisements as a source of revenue. However, these ads can be conduits for malware, including adware, spyware, or ransomware. Users accessing pirated content may be bombarded with intrusive ads that contain malicious code, leading to malware infections.

### FAKE/SCAM SITES:

These sites purport to host pirated content, but in fact, they are simply scam sites. Typically, after visiting the site, the first 20 seconds of a pirated movie will be played, and then the user will need to register. Initially, the user will need to enter their credit card details to register, but then in the "fine print" is a billing agreement for a monthly fee in the order of $60. Most users will not be aware that they are being charged a fee in the order of ten times what it would cost to subscribe to a legitimate site.

### PHISHING SITES:

Piracy sites can be setup to collect email and password details from users. These credentials can then be bundled and on-sold in the hope that they will be reused from the user's own email accounts, providing the perfect attack vector for identity theft.

# Risks

**What are the levels of risk for those Indian consumers who access piracy sites and services?**

Accessing piracy sites is risky for Indian consumers on a number of levels, including potential legal consequences, as well as major cybersecurity risks, notably from malware infection. Given the serious risks outlined above, this report aims to further explore and understand the digital piracy-malware nexus and how these cybersecurity risks might impact Indian consumers, and also to quantify the risks faced by Indian consumers online. These are not hypothetical or historical risks – in 2023, ReasonLabs looked at pirated versions of Oscar-nominated films, and found thousands of instances of threats that were detected by their Endpoint Detection and Response (EDR) and Anti-Virus (AV) products. Over 6 weeks, researchers monitored thousands of cyber threat instances being linked to pirated content, including malware, spyware and keyloggers. A good example was a document stealer associated with a “Top Gun: Maverick” download. This code searched the victim’s hard drive for Word documents, Excel sheets, and PDF files, and would then email them to the attackers e-mail address. The research question for this study is to specifically examine the cyber risks that Indian consumers would encounter when visiting these sites, and how does this risk level link to consumer understanding of the threat.

The report is divided into two main sections – a Perceptions and Experience study, and an Empirical study. Perceptions and Experience studies offer several benefits and are valuable for exploring complex phenomena like the link between piracy and malware, providing in-depth insights, and capturing the richness of human experiences. On the other hand, Empirical studies are best suited to examining large-scale trends, establishing statistical relationships, and providing objective and generalizable findings. By combining both approaches, we hope to achieve a comprehensive understanding of cybercrime risks to Indian consumers when accessing piracy sites and services.

Our Perceptions and Experience study explored questions around consumer understanding of the link between malware and piracy, using a nationally representative sample, while the Empirical study focused on the actual risk of encountering malware, using industry standard detection of cyber risks by Google’s VirusTotal product, including identification of suspicious and malicious sites, malware, and spam and phishing activity.

# Methods & Data

## 02

**Perceptions and Experience Study**
**Empirical Study**

# Perceptions and Experience Study

**The Perceptions and Experience study measured Indian consumers attitudes and understanding of the malware-piracy nexus.**

International research data and analytics group YouGov were commissioned to seek responses (in English) to an online survey from a representative sample of the Indian population (N=1,037) to answer a range of questions about their understanding of piracy, engagement in piracy (if any), understanding of malware, and the link between the two. The survey was conducted in June 2023. The full questions and range of responses are shown in Appendix A, but the knowledge dimensions are summarized right.

Alongside these questions, demographic data was also collected, to allow deeper insights to be developed, including factors relating to age, sex, and location.

1. **Knowledge of malware**, including bots, ransomware and spyware
2. **Experience of malware attack**, including family members, colleagues and friends
3. **Accessing pirated content**, including family members, colleagues and friends
4. **Perception of the relationship between malware and access of pirated content**, from Very Unlikely to Very Likely
5. **Activities with malware risk**, when comparing piracy activities to social media, gambling ads, adult industry ads, and so on

# Empirical Study

**The approach to measuring cyber risk on piracy sites was developed using VirusTotal – a Google product that visits websites and determines whether they have host malware, phishing, suspicious, malicious or spam content.**

VirusTotal uses hash matching against a database provided by more than 70 anti-virus vendors, as well as a sandbox to actually execute and profile malicious code. It is the "gold standard" for anti-virus research globally. The data collected using VirusTotal was used to develop metrics for risk, such as the average likelihood of a consumer encountering a threat, across all or any type, including where multiple vendors have identified those threats. Importantly, when using these metrics, they can be used to compute relative when compared to a benign set of mainstream sites that are likely to have very low levels of cyber risk.

A list of piracy sites which illegally provided access to film and TV content, as well as scam piracy sites, that were popular amongst Indian consumers, was provided by the Alliance for Creativity and Entertainment (ACE), the world's largest non-profit anti-piracy association representing film, TV series and live sports rightsholders. The list included sites based on data about copyright removal request levels, copyright-related site blocking in various countries, and other sources. Within the list, a number of samples were identified for comparison. A control sample based on the top 30 most popular overall websites in India was also assessed to ensure that a valid comparison could be made between users visiting piracy sites versus a typical website. A sample size of 30 was chosen for each sample, which allows us to make inferences about populations, since we can use the sample standard deviation to compute standard error. In short, we have selected samples to be representative of their respective populations, and used an experimental design with a control to allow for inferences to be validly drawn.

**SAMPLES WERE COLLECTED FOR THE FOLLOWING CATEGORIES BASED ON TRAFFIC TO SITES BY INDIAN CONSUMERS IN MAY 2023:**

## Top 30

- Piracy sites in India
- "Scam" piracy sites in India
- Mid-range piracy sites in India
- Mid-range "scam" piracy sites in India
- Websites in India

The "Top 30" were the most popular sites during the sampling period, while the mid-range sites provided a validation that the results for the "Top 30" were broadly representative of the population, given that the Pareto Principle suggests that a relatively small number of sites would likely attract the most traffic. The mid-range sample was drawn from the mid-point of the entire sample list provided based on ranking by visits, comprising the top 1,000 sites. The "scam" piracy sites were those independently verified by the Alliance for Creativity and Entertainment (ACE) as not hosting actual pirated content.

Why have we drawn a distinction between piracy and "scam" piracy sites in India, and between the top sites and the mid-range sites? A "scam" piracy site is one which actually hosts no content at all – it tries to fool the user into purchasing a subscription for a highly-inflated price, after the user provides their credit card details. While noting that all piracy sites are risky, it was predicted that these "scam" sites would be even riskier, since they never have any intention of showing any real product. Also, it was hypothesized that mid-range sites may be riskier for consumers than the most popular sites, since they would not be attracting as much illicit advertising. Thus, the site operators may need to supplement their income by other means, such as scams or malware.

# Results

## 03

**Perceptions and Experience Study**
**Empirical Study**
**Focus on Mobile**

# Perceptions and Experience Study

**Piracy websites** pose a

**59%**

risk of malware infection for Indian consumers.

**Adult industry ads** pose a

**57%**

risk of malware infection for Indian consumers.

**Gambling ads** pose a

**53%**

risk of malware infection for Indian consumers.

The most significant result from the study was the finding that the websites which presented the highest risk of malware infection for Indian consumers was accessing piracy websites (59%), compared to accessing adult industry ads (57%) and accessing gambling ads (53%). At the lower end of the spectrum, consumers rated accessing social media platforms and clicking on known branded advertising at 29%. In other words, Indian consumers themselves rated the relative risk for piracy at 2.03 times the rate for malware risk, supported by the net "likely" relationship between malware and access of pirated content of 56%. This relative risk value was calculated by dividing the proportion of respondents who identified piracy websites as the top risk compared to clicking on known-branded advertising, i.e., 0.59/0.29=2.03. As we will see from the Empirical study, it is quite likely that this is a significant underestimate of the actual relative risk, posing a policy challenge for governments and industry and emphasizing the need for greater awareness and education of the piracy-malware nexus.

The second most significant result was that 64% of consumers had experienced a malware attack, and that 62% had accessed pirated content. Both of these values are high, and presumably relate to potentially a lifetime of experience using the internet, rather than a fixed time window. From Question 1, we know that 78% of consumers had knowledge of cybersecurity threats, and presumably, the gap between knowledge and experience (78%-64%=14%) may be due to better informed decision-making and countermeasures employed by those consumers, including avoiding piracy sites (a gap of 78%-62%=16%). Again, from a population perspective, this provides a very useful set of insights into the links between knowledge, behavior, risk perception and risk mitigation. A further breakdown of the data is provided in Appendix B.

The final significant finding was that an understanding of the relationship between age and an understanding of the relationship between malware and piracy increases linearly with age. Thus, young people rate the relationship less likely than any other cohort. Yet, worryingly, they also cite that 42% of their peers use piracy services. Based on these results, it seems that young people aged 18-24 may need to be the focus on policy or education initiatives. This is consistent with psychological research showing that adolescents tend to engage in risk-taking behaviors.

# Empirical Study

The URLs for the 150 websites in the sample across all five categories (Top 30 Piracy, Top 30 Scam, Mid-Range Piracy, Mid-Range Scam and Control) were uploaded to VirusTotal, and the results tabulated across five cyber risk categories (malicious, malware, suspicious, phishing and spam). These categories can be defined as follows:

- **Malicious** – human confirmation that a site contains cyber threats
- **Suspicious** – machine detection that a site contains cyber threats
- **Malware** – malware distributed from the site
- **Phishing** – site used to steal users' credentials
- **Spam** – site used for unsolicited email, popups and automatic commenting

These categorizations are based on reports from more than 70 partners comprising the worlds' largest cybersecurity threat detection companies, and represent a community-based effort to identify sites which are actively engaged in delivering cyber threats. For each detection company only one category per site is reported, based on their assessment of the risks on the site.

Table 1 shows the results for the average chance of all detected cyber threats, while Table 2 shows the results for the average chance of any detected cyber threats. The former is a broader measure, since we assume that the different antivirus companies may be identifying different threats, while the latter is a narrower measure, where the presence of any threat is counted only once. In summary, the former is the worst case, and the latter is the best case. The full tables are given in Appendix C.

The results indicate – at best – that the average likelihood of encountering a cyber threat on a Top 30 or Mid-Range piracy site was 0.7, whereas it was 1.03 for a Top 30 scam site, falling to 0.8 for a mid-range scam site. The control site had a 0.06 chance of encountering a cyber threat. These results support the hypothesis that scam piracy sites are more likely to expose users to cyber threats when compared to piracy sites. It was interesting to note that there no differences between the Top 30 and Mid-range piracy sites, suggesting the level of cyber threat is fairly uniform. However, for scams, the most popular sites were the ones most likely to represent a threat to their users.

The worst case data supports a similar pattern of results to the best case: for the Top 30 and Mid-range piracy sites, the average likelihood was 1.00 and 0.96 respectively, while the average likelihood for Top 30 scam and Mid-range scam sites jumped to 1.8 and 1.06 respectively. The average likelihood for the control sites remained the same at 0.06.

Table 3 shows the relative risk calculation, that takes the average detections data, and divides by the detections value of the control group, for the worst case and best case scenarios respectively. This provides a mechanism to compare the self-report relative risk from the Perceptions and Experience study (of 2.04) with the Empirical results. Whether we consider the best case or worst case scenarios, consumers in India are significantly underestimating the risk of cyber threats from visiting piracy or "scam" sites.



**Table 1 –** Worst Case Scenario – Average Likelihood of All Cyber Threats

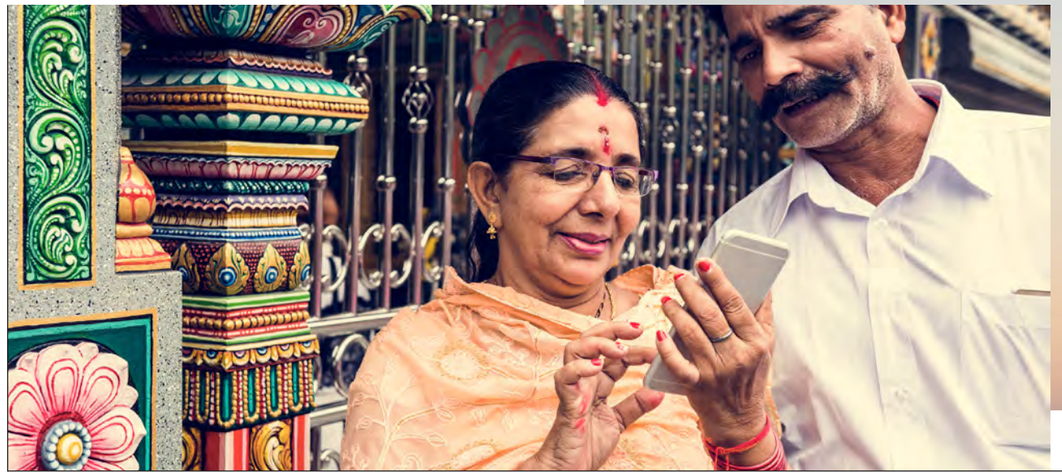
| Category | N | Detections | Likelihood |
|---|---|---|---|
| Top 30 Piracy | 30 | 30 | 1.0 |
| Top 30 Scam | 30 | 54 | 1.8 |
| Mid-range Piracy | 30 | 29 | 0.96 |
| Mid-range Scam | 30 | 32 | 1.06 |
| Control | 30 | 2 | 0.06 |

**Table 2 –** Best Case Scenario – Average Likelihood of Any Cyber Threat

| Category | N | Detections | Likelihood |
|---|---|---|---|
| Top 30 Piracy | 30 | 21 | 0.7 |
| Top 30 Scam | 30 | 31 | 1.03 |
| Mid-range Piracy | 30 | 21 | 0.7 |
| Mid-range Scam | 30 | 24 | 0.8 |
| Control | 30 | 2 | 0.06 |

**Table 3 –Relative Risk Calculations**

| Category | Worst Case | Best Case |
|---|---|---|
| Top 30 Piracy | 15 | 10.5 |
| Top 30 Scam | 27 | 15.5 |
| Mid-range Piracy | 14.5 | 10.5 |
| Mid-range Scam | 16 | 9 |



# Focus on Mobile

It is noted that 74.05% of all internet traffic in India is generated by mobile users. For the Perceptions and Experience survey, this means that the responses should be interpreted in the context of this usage level vis-à-vis a nationally representative sample. For the Empirical Study, the interpretation regarding mobile usage is more complex. VirusTotal, as a platform, is able to scan URLs which are available for both mobile and desktop users, and it is able to analyse malware samples from mobile and desktop sources. However, the domain statistics do not provide a further breakdown of whether the threats posed target mobile or desktop platforms specifically. In this study, we provided a generic URL for analysis by VirusTotal, and did not provide a site-specific URL; not all domains provide them, although user experience may suffer, because the default globally is typically to develop sites for desktop use. Most modern web development toolkits using a Model-View-Controller (MVC) architecture which can provide the appropriate experience for different platforms. In the Empirical Study, though, analysing the domains using VirusTotal provides aggregated results. In some cyber threat categories, there will be no difference – scams and phishing, for example, will be available to users on all platforms. However, any platform-specific code, such as installation of mobile-specific malware, will obviously only impact malware users. This is one drawback of using aggregated cyber threat data.

## TO FURTHER UNDERSTAND MOBILE-SPECIFIC ISSUES, WE PROVIDE AN ILLUSTRATIVE EXAMPLE BELOW.

First, we choose a site that has been flagged as malicious by VirusTotal. Second, we visit the site using an Android device. When any link on the page is clicked, a popup is launched, as shown in Figure 1.

A popup asks the user to confirm “QR Reader” for installation in order to continue watching. When the user clicks “Confirm,” another popup is launched showing a warning message that the file may be harmful, as shown in Figure 2.

A malicious .apk file is then downloaded to the device. When launched, the file could infect the device. Furthermore, the user may be requested to allow notifications from each popup, or from each application.

As popups were permitted from the “QR Reader” app, a fake malware notification is displayed with a malicious link, as shown in Figure 3, asking the user to install third-party antivirus, as shown in Figure 4.

We checked this .apk file using VirusTotal, and it was flagged as malicious by Trustlook as Android. Malware.General (score 4), and matched three crowd-sourced Intrusion Detection System (IDS) rules from two different providers, including truncated ethernet header, stream packet with invalid ack, and shutdown rst invalid ack.

It also sought the following Android permissions: MANAGE_ACCOUNTS, READ_EXTERNAL_STORAGE, USE_CREDENTIALS, AUTHENTICATE_ACCOUNTS, CAMERA, WRITE_EXTERNAL_STORAGE, GET_ACCOUNTS and INSTALL_SHORTCUT. Based on a number of consumer reviews, it seems that another dimension to the enterprise is a scam, with very frequent billing reported, and the BBB flagging that the business only a mail forwarding address in the United States (which is forwarded to a residential block in Dubai), and unresponsive customer support.

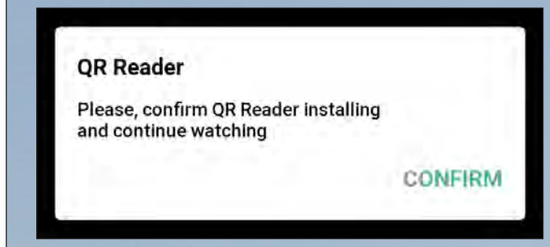



Figure 1 – Install prompt

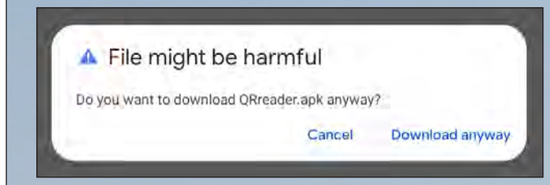



Figure 2 – Harm warning


Figure 3 – False alarm for notifications

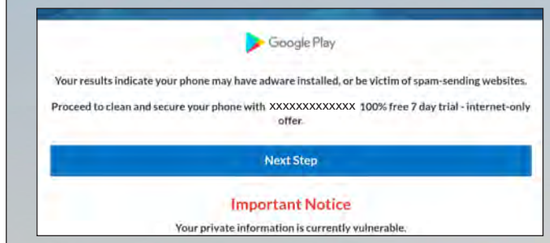



Figure 4 – Fake malware prompt

What this example demonstrates is that piracy sites use a combination of tactics, including popups, malicious notifications, scams and fake malware warnings to entice users into installing malware onto their mobile devices. In much the same way as desktop users are vulnerable to these tactics, mobile users must also be aware that websites can deliver tailored malicious messaging and code which is specific to their platform.

# Discussion

## 04

**Discussion**
**Law Enforcement**
**Regulatory Reform**
**Education**
**Broader Risks**

# Discussion

**By combining the results of both the Perceptions and Experience study and the Empirical analysis, it is clear that Indian consumers underestimate their actual cyber risk when using piracy sites.**

In the Perceptions and Experience study, Indian consumers identified using piracy sites more than twice as likely as mainstream sites as the #1 source of malware, with a relative risk of 2.03. However, even using the most conservative analysis of cyber risk on the most popular piracy sites, as well as piracy “scam” sites, indicates that the relative risk is likely to be in the range of 9-15.5, when compared to a control baseline of mainstream sites. The cyber risks identified through the use of Google’s VirusTotal system included malicious and suspicious websites, malware, and phishing carry individual risks to Indian consumers of identity theft and fraud, as well as broader exposure for the population at large.

Given these high levels of cyber risk, and the potential financial consequences for consumers, what can Indian authorities do to reduce this risk? We make three key recommendations that flow directly from this result:

### LAW ENFORCEMENT:

Government to place a higher priority to digital copyright crimes in India, and train and resource appropriate law enforcement agencies. This would bring offenders to justice, and provide a clear and visible deterrent.

### REGULATORY REFORM

Initiate stakeholder discussions on effectiveness of anti-piracy and anti-malware takedown rules, to make responding to piracy sites that host malicious content fast and effective..

### EDUCATION:

Deliver demographically targeted awareness, training and education campaigns to deter consumers from accessing piracy websites and reduce risky cyber behavior, especially among the young demographic aged 18-24.

In the following discussion, these recommendations are explored, and the likely outcomes of action – or inaction, by authorities are examined.

# Law Enforcement

**Digital piracy can be a profitable crime which stifles creativity, undermines investment, reduces tax contributions to governments and, as demonstrated by the findings of this study, puts Indian consumers at risk of egregious malware.**

Online piracy in India will probably continue to thrive as long as it is profitable, and it is worth noting that the placing and dissemination of malware is now a revenue stream for many piracy site operators. As such law enforcement plays a critical role in reducing the levels of cyber risk faced by Indian consumers who access piracy websites and services. This may involve raising the priority afforded to IP crimes nationally; for example, the Ministry of Information and Broadcasting in India had established the Committee on Piracy, which submitted its report in 2010. The Committee identified piracy as "the biggest threat" to the growth of the entertainment industry, and correctly hypothesized:

> **"With increasing speeds of broadband and wider broadband connectivity, if effective steps are not taken to check Internet piracy, both the film and music industry would suffer huge losses."**

The Committee observed that countering piracy was unfortunately "very low in terms of priority in the radar of law enforcement agencies," and that copyright laws needed "to be enforced more effectively." Further, that it "is very important that the Internet Service Providers (ISPs) are also roped in to fight piracy." In 2016, the Indian government's National IPR Policy called for better "legal and enforcement mechanisms," along with consumer awareness, to combat piracy. In 2021, the bipartisan Department-Related Parliamentary Standing Committee on Commerce, in a report reviewing the IPR regime in India, called for better collaboration, co-ordination and capacity-building, with respect to state-level and national-level agencies, to effectively fight piracy. Here the Committee suggested involving the powerful Central Bureau of Investigation (CBI). The Committee also stated that the enactment of specific anti-piracy legislation was "the need of the hour," and that the Indian government should "consider establishing a Central Coordination Body on IP Enforcement for undertaking coordinative efforts by involving various Ministries, Departments, and Governmental agencies" to bolster enforcement.

Furthermore, given the clear linkages between piracy sites and malware, the National Cyber Coordination Centre of India (NCCC), headed by the National Cyber Security Coordinator (NCSC), may also be requested to lend its assistance and expertise.

The NCCC is tasked with coordinating with various national-level agencies on matters pertaining to cybersecurity, providing inputs that may be used by law enforcement agencies. Here, it is significant that, in 2022, Lt. General (retd.) Rajesh Pant, the then NCSC, identified malware as "the starting point" of all cybersecurity threats in India and acknowledged that malware may be spread, by "clickbaiting" internet users to click on pirated content.

At the state police level, National IPR Policy had called for "the strengthening of IPR cells in State police forces." There is, however, only one state in India, Maharashtra, with an operational unit specifically dedicated to fighting digital piracy: the Maharashtra Intellectual Property Crimes Unit (MIPCU), previously known as the Maharashtra Cyber Digital Crime Unit (MCDCU). The establishment of similar units in other states, especially in states with a high number of internet users, is likely to be beneficial in curbing piracy. Such units can prioritize the disruption of piracy networks linked to websites and apps that expose internet users to malware and unsafe third-party sites. Further, although the MIPCU was established in 2017 (as the MCDCU), reports suggest that it has not undertaken many significant anti-piracy operations, and that its parent division, Maharashtra Cyber, may be understaffed. Therefore, improving the quantity and quality of staff at the MIPCU is also desirable.

# Regulatory Reform


Further stakeholder discussions on effectiveness of anti-piracy and anti-malware takedown rules need to occur, to make responding to piracy sites that host malicious content fast and effective. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 require online intermediaries, including social media intermediaries, to exercise “due diligence” and prevent the hosting of “information” that “infringes any patent, trademark, copyright or other proprietary rights, as well as well as “information” that “contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource.” Intermediaries are also required to remove copyright-infringing material, within stipulated time-frames, on the receipt of directions from government agencies or courts. Further, intermediaries are required to appoint “Grievance Officers” to hear complaints from “an individual or any person.” Given the vast prevalence of pirated content, including content linked to malware, it may be desirable to investigate the actual effectiveness of the present rules and regulations and consider improvements to the law and its implementation. A first step towards this would be to initiate stakeholder discussions.

# Education

**The results suggest that targeted education, awareness and training programs need to focus on the 18-24 cohort. This demographic had the least knowledge of cybercrime and malware dissemination yet had the highest propensity to take risks and access piracy websites.**


Awareness of the risks involved when accessing online pirated content as well as the promotion of consumer tools and technologies that can reduce cyber risk, such as anti-malware and anti-phishing tools, would be of benefit to these “digital natives.”

We provide some detailed suggestions below for how cyber risk awareness could be achieved for this group in India:

## IDENTIFY TARGET AUDIENCES:

Determine the key target audiences for the program, including the general public, students, industry professionals, content creators, and policymakers. Each group may require tailored messaging and approaches to address their specific needs and challenges. The results of this study clearly indicate 18-24 year-olds should be a key focus on any education programs.

## DEVELOP EDUCATIONAL MATERIALS:

Create informative and engaging educational materials, such as brochures, videos, infographics, and online resources, that explain the risks associated with piracy sites and cyber threats. These materials should emphasize the importance of legal content consumption, online safety, and the consequences of engaging with pirated content.

## PUBLIC AWARENESS CAMPAIGNS:

Launch a comprehensive public awareness campaign utilizing various media channels to reach a wide audience. This can include television and radio advertisements, social media campaigns, public service announcements, and collaborations with influencers or celebrities. The campaign should highlight the dangers of piracy sites and promote legal alternatives.

## SCHOOL AND UNIVERSITY PROGRAMS:

Integrate educational modules on digital citizenship, copyright, and online safety into school curricula and university programs. Provide teachers and educators with training resources and materials to facilitate discussions and activities on responsible digital behavior, copyright awareness, and the impact of piracy.

## INDUSTRY WORKSHOPS AND TRAINING:

Organize workshops, seminars, and training sessions for industry professionals, including filmmakers, musicians, content creators, and distributors. These sessions can educate them about copyright laws, licensing, digital rights management, and legal distribution platforms. Encourage industry stakeholders to adopt best practices that discourage piracy and protect their own content.

## GOVERNMENT AND POLICYMAKER ENGAGEMENT:

Engage with government bodies, policymakers, and law enforcement agencies to raise awareness about the link between cyber threats and piracy sites. Advocate for effective legislation, effective enforcement actions against the largest piracy site operators, as well as advocating for the importance of collaboration between different stakeholders in combating piracy and protecting consumers from cyber threats.

## PARTNERSHIPS AND COLLABORATIONS:

Collaborate with ISPs, content industry associations, cybersecurity organizations, and consumer advocacy groups to jointly develop and deliver awareness initiatives. Pool resources, expertise, and networks to reach a broader audience and amplify the program’s impact.

## EVALUATION AND FEEDBACK:

Continuously evaluate the program’s effectiveness through surveys, feedback mechanisms, and data analysis. Measure the awareness levels, behavioral changes, and perceptions of the target audiences. Use this feedback to refine and improve the programme over time.

# Broader Risks

**If cyber risk is not reduced, and malware continues to be disseminated via piracy sites, what are the broader consequences for India? We have documented some key considerations below:**

### CYBER ESPIONAGE:

Malware on piracy sites, especially when accessed from within a work environment and via work computers and devices, could be used as a tool for cyber espionage, enabling unauthorized access to sensitive information, government networks, or critical infrastructure. Nation-state actors or other malicious entities may exploit vulnerabilities in pirated software, compromised downloads, or embedded malware to gain unauthorized access to confidential data, government systems, or defence networks.
In an increasingly hostile Indo-Pacific, malware distributed through piracy sites offers the perfect “bait,” especially among the 18-24 year cohort.

### DATA BREACHES AND LEAKS:

Malware can facilitate data breaches, leading to the leakage of sensitive information. Such breaches can compromise national security by exposing sensitive information, disrupting government operations, or providing adversaries with valuable intelligence. Government workers accessing piracy sites could inadvertently introduce malware into sensitive networks.

### CRITICAL INFRASTRUCTURE ATTACKS:

Malware distributed through piracy sites can target critical infrastructure systems, including power grids, transportation networks, or communication systems. By compromising these systems, adversaries can disrupt essential services, cause widespread chaos, or create vulnerabilities that compromise national security. Malicious nation states could use malware distributed through piracy sites to gain a widespread foothold and initiate lateral movement within national infrastructure, as per the MITRE ATT&CK framework.

### MALICIOUS CODE PROPAGATION:

Malware on piracy sites can serve as a vector for the widespread propagation of malicious code. If users unknowingly download infected files or visit compromised websites, the malware can spread across networks, infecting government systems, private organizations, or individual devices.
This can lead to large-scale disruptions, financial losses, and potential threats to national security.

### EXPLOITATION OF SUPPLY CHAINS:

Malware on piracy sites can infiltrate supply chains, particularly software supply chains, leading to compromised systems or unauthorized access to critical infrastructure. Attackers can exploit vulnerabilities in host operating systems, compromising their integrity and introducing backdoors or malicious functionality that can be used for nefarious purposes, including surveillance, sabotage, or espionage.

### MALWARE-AS-A-SERVICE (MAAS):

Piracy sites can serve as platforms for the distribution of malware-as-a-service, where cybercriminals offer malware or hacking tools to other threat actors. This can contribute to a thriving underground cybercrime ecosystem, enabling a range of malicious activities that can pose national security risks, such as cyberattacks, data breaches, or information warfare.

**So while consumers are impacted personally, the collective consequences of cyber threats remaining unchecked are very serious for the entire nation.**

# Bibliography

# Bibliography


Agnihotri, A., & Bhattacharya, S. (2019). Unethical consumer behavior: The role of institutional and socio-cultural factors. *Journal of Consumer Marketing*, 36(1), 124-135.

Aldriwish, K. (2021). A deep learning approach for malware and software piracy threat detection. *Engineering, Technology & Applied Science Research*, 11(6), 7757-7762.

Banerjee, A. (2013). The Indian Film Industry's Battle Against Piracy: Some Reflections. *WIPO-WTO Colloquium Papers*, 4, 35-44.

Başeskioğlu, M. Ö., & Tepecik, A. (2021, June). Cybersecurity, computer networks phishing, malware, ransomware, and social engineering anti-piracy reviews. In *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1-5). IEEE.

Blancaflor, E., Esguerra, C., Fandiño, C., Gonzales, A. L., Nisperos, B., & Pono, L. (2021, March). A. Assessment of Student Vulnerability on the Download of Malware Disguised as Cracked Software. In *Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management Singapore*.

Bowman, A., Sharma, M., & Biros, D. (2022). Too good for malware: Investigating effects of entitlement on cybersecurity threat assessment and piracy behavior.

Dastidar, S. G., & Elliott, C. (2020). The Indian film industry in a changing international market. *Journal of Cultural Economics*, 44, 97-116.

Eisend, M. (2019). Explaining digital piracy: A meta-analysis. *Information Systems Research*, 30(2), 636-664.

El Fiky, A. H. (2020). Deep-droid: Deep learning for android malware detection. *Int. J. Innovative Technol. Explor. Eng*, 9(12), 122-125.

Fitzgerald, S. (2019). Over-the-top video services in India: Media imperialism after globalization. *Media Industries Journal*, 6(2), 00-00.

Ghosh, U. (2021). Online financial frauds and cyber laws in India-an analysis. *FINANCIAL FRAUDS AND CYBER LAWS*, 10.

Grover, M., Sharma, N., Bhushan, B., Kaushik, I., & Khamparia, A. (2020). Malware threat analysis of IoT devices using deep learning neural network methodologies. *Security and Trust Issues in Internet of Things*, 123-143.

Jha, A. K., & Rajan, P. (2021). Movie piracy: Displacement and its impact on legitimate sales in India. *The Journal of World Intellectual Property*, 24(3-4), 237-252.

Kumari, N., & Chen, M. (2022). Malware and piracy detection in Android applications. In *2022 IEEE 5th International Conference on Multimedia Information Processing and Retrieval (MIPR)* (pp. 306-311). IEEE.

Lee, B., Jeong, S., & Paek, S. Y. (2019). Determinants of digital piracy using deterrence, social learning and neutralization perspectives. *International Journal of Comparative and Applied Criminal Justice*, 43(4), 295-308.

Lee, S. J., & Watters, P. A. (2016). Gathering intelligence on high-risk advertising and film piracy: A study of the digital underground. *Automating open source intelligence*, 89-102.

Martin, J., & Whelan, C. (2023). Ransomware through the lens of state crime. *State Crime Journal*, 12(1), 4-28.

Mishra, S., Rout, D., Kantha, R. K., & Jha, M. (2021). A CASE STUDY ON PERCEPTION OF PEOPLE OF BHUBANESWAR CITY TOWARDS OTT APPLICATIONS. *Journal of Emerging Technologies and Innovative Research (JETIR),* 8(3).

Nagaraj, S., Singh, S., & Yasa, V. R. (2021). Factors affecting consumers' willingness to subscribe to over-the-top (OTT) video streaming services in India. *Technology in Society*, 65, 101534.

Pillai, S. (2023). Identity Theft: Prevention of Modern Crimes in the Era of Internet. *Issue 2 Indian JL & Legal Rsch.,* 5, 1.

Salgado, J. (2022). Modern Piracy: Fighting Ransomware with a Universal Foundation and Why an International Cybercrime Treaty Must Follow in the Footsteps of the Paris Agreement. *Conn. J. Int'l L.,* 37, xiv.

Saluja, S. (2022). Identity theft fraud-major loophole for FinTech industry in India. *Journal of Financial Crime*.

Shah, U. (2019). Digital music piracy in India: Issues and Challenges. *International Journal of Research in Social Sciences*, 9(6), 709-721.

Singh, P. (2019). New Media as a Change Agent of Indian Television and Cinema: A study of over the top Platforms. *Journal of Content, Community and Communication*, 9(1), 131-137.

Singh, V. K., Srichandan, S. S., & Bhattacharya, S. (2021). What do Indian researchers download from sci-hub? An analytical introspection. *Journal of Scientometric Research*, 10(2), 259-264.

Sundaravel, E., & Elangovan, N. (2020). Emergence and future of Over-the-top (OTT) video services in India: An analytical research. *International Journal of Business, Management and Social Research*, 8(2), 489-499.

Suwa, R. (2021). Detecting Cybersecurity Threats from Online Digital Piracy Websites.

Telang, R. & Waldfogel, J. (2014). Piracy and new product creation: A Bollywood story. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2478755

Vaijayanthee, S. (2022). Combating the Threat of Piracy in the Indian Music Industry. *Journal of Legal Studies & Research*, 8(5), 21-28.

Watters, P. (2021). Consumer Risk and Digital Piracy–Where Does Malware Come From?. *Available at SSRN 4536938*.

Watters, P.A. (2023a). *Cybercrime and Cybersecurity*. CRC Press.

Watters, P. A. (2023b). *Counterintelligence in a Cyber World*. Springer Nature.

Watters, P. A., Layton, R., & Dazeley, R. (2011). How much material on BitTorrent is infringing content? A case study. *Information Security Technical Report*, 16(2), 79-87.


## Acknowledgements

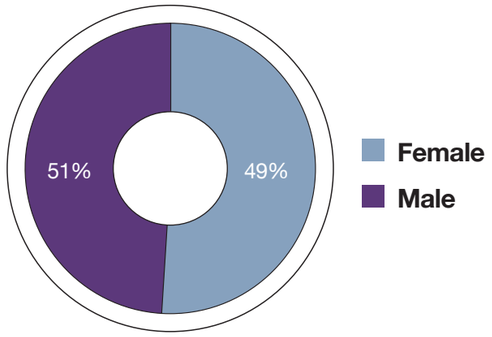
Funding for this research was provided by the Motion Picture Association (MPA). The work was produced independently by Cyberstronomy Pty Ltd and the ISB Institute of Data Science, Indian School of Business. The researchers acknowledge the assistance of YouGov in seeking responses to an online survey from a representative sample of the Indian population.

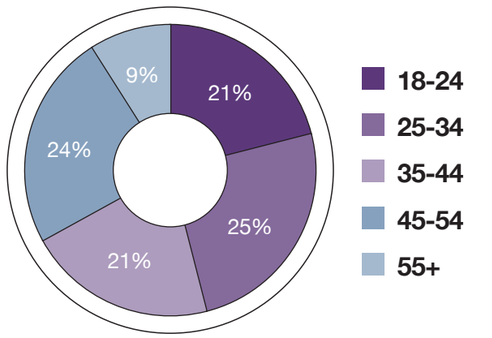
# Appendices

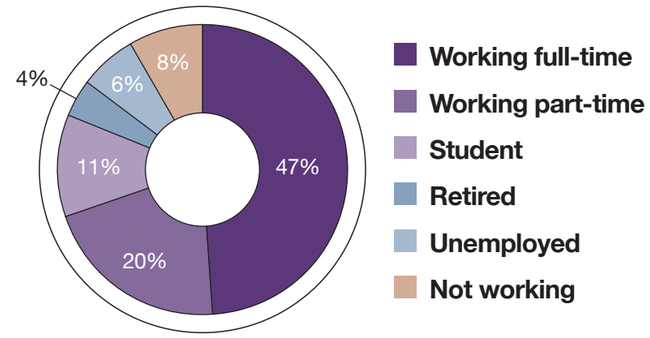
# Appendix A

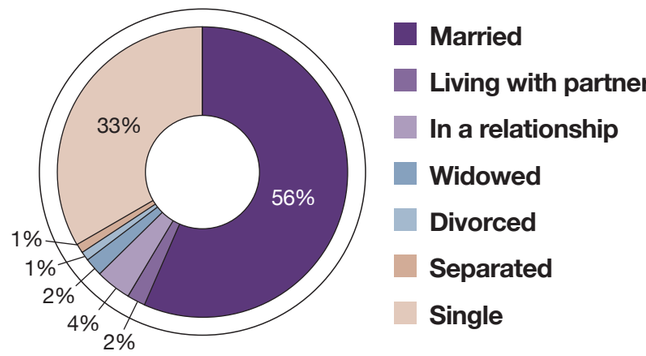
YouGov Survey Demographic and Questions

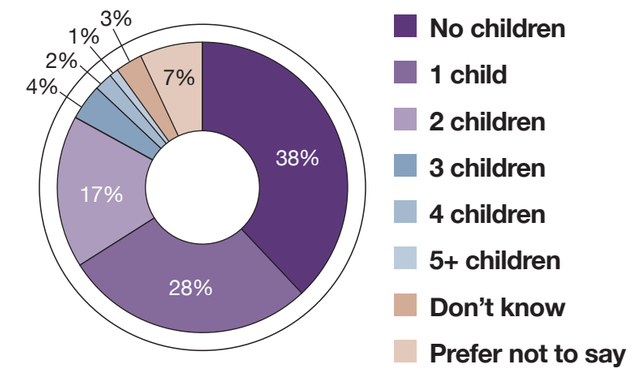
**The survey was conducted between 23 May - 29 May 2023, with a total of 1,037 respondents interviewed in India, as part of the nationally representative YouGov National Omnibus. Figures are weighed in related to online population aged 18+. Respondents are invited to participate in the National Omnibus based on their demographic characteristics, in proportion to the frequency of adult citizens in India.**



## Q1.

**Have you ever heard of any of the following types of malware (tick all that apply):**

- Bots
- DDoS attacks
- Ransomware
- Remote Access Trojans that steal private and financial information
- Spyware that remotely activates and records via a computer's video and audio functionality
- None of the above

## Q2.

**Do you know of anyone who has ever experienced a malware attack/ ever experienced a computer/device malfunction that they think could have been caused by malware?**

- Myself
- A family member
- A member of my household
- A friend
- An office colleague
- Others
- None

## Q3.

**Do you know of anyone who ever accessed pirated content via any piracy service (e.g. torrent sites, streaming sites, use of TV boxes or other physical devices)?**

- Myself
- A family member
- A member of my household
- A friend
- An office colleague
- Others
- None

## Q4.

**From your understanding, how likely do you think a malware attack or computer/ device malfunction caused by malware is related to the access of pirated content?**

- 5 – Very Likely
- 4
- 3
- 2
- 1 – Very Unlikely

## Q5.

**Which of the following activities do you think would put you and your household at the most risk of downloading malware or experiencing a malware attack? Please rank "1" for the activity with the most risk and "7" refers to activity with the least risk.**

- Social media platforms (such as Facebook, Instagram etc)
- Clicking on known branded advertising
- Clicking on gambling ads
- Clicking on adult industry ads
- Piracy websites
- Piracy devices (such as Piracy TV boxes)
- E-Game websites
- None of the above present any risk

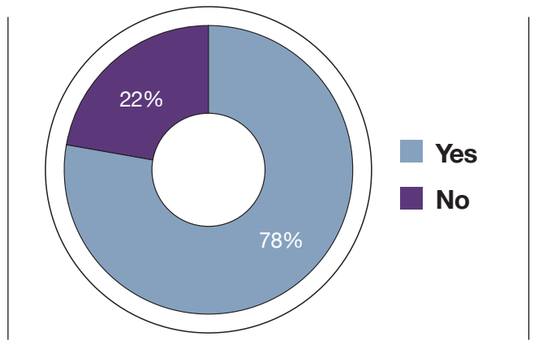
# Appendix B

YouGov Survey Results

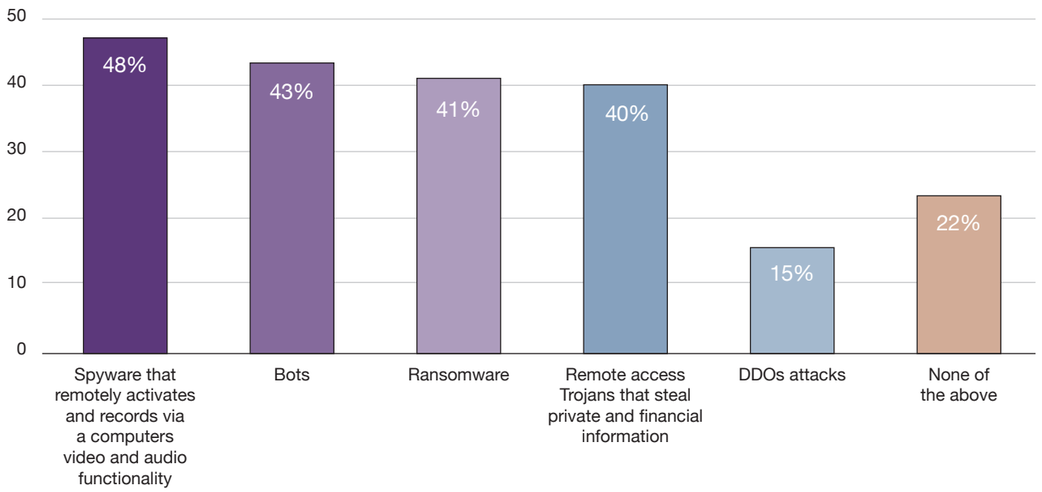
## Q1.

### AWARENESS OF MALWARE

The majority of respondents are familiar with at least one type of malware attack (78%). Among the various malware types, Spyware stands out with the highest awareness, being recognized by 48% of respondents. Awareness levels of Bots, Ransomware and Remote Access Trojans are similar at around 40%. On the other hand, DDoS attacks are the least familiar type, possibly due to their narrower target selection of specific organizations or websites. The limited reach reduces overall visibility of DDoS attacks.




**Have you ever heard of any of the following types of malware? Please select all that apply.**

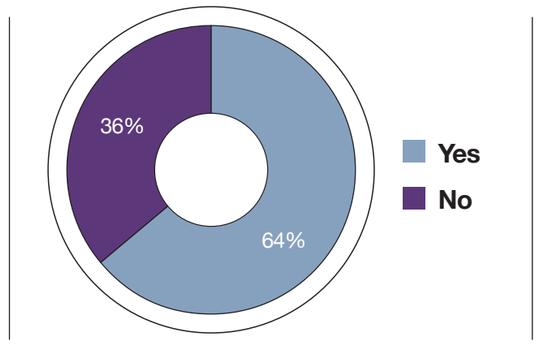




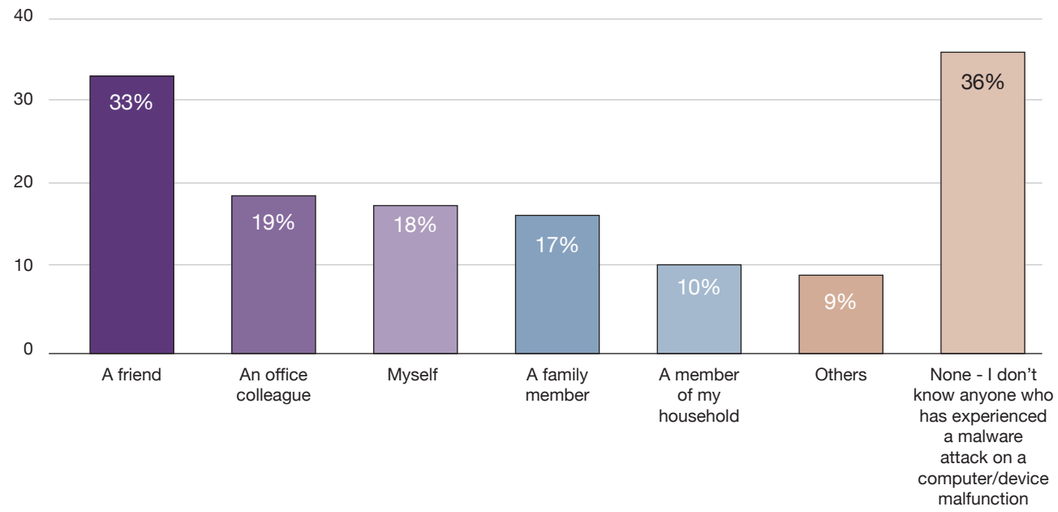

## Q2.

### EXPERIENCE OF MALWARE ATTACK

Malware attacks are fairly common in India, about 2 in 3 respondents have encountered malware attacks personally or know someone within their circle suffered from these attacks.



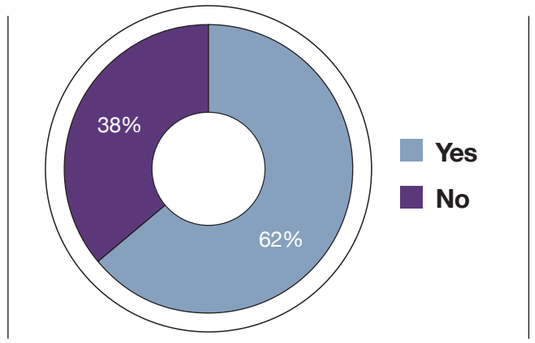

**Do you know if anyone who has experienced a malware attack or a computer/ device malfunction that you think could have been caused by malware?**



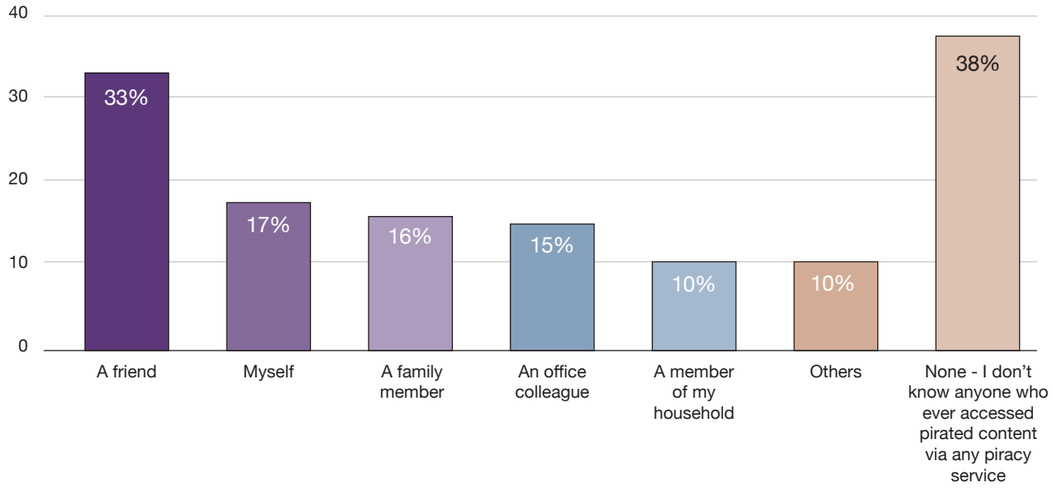
# Q3.

## ACCESSING PIRATED CONTENT

62% of respondents who know someone or personally have accessed pirated content before, which could be the reason for such common Malware attack experience in India.




**Do you know anyone who ever accesses pirated content via any piracy service (e.g. torrent sites, streaming sites, use of the TV boxes or other physical devices)?**

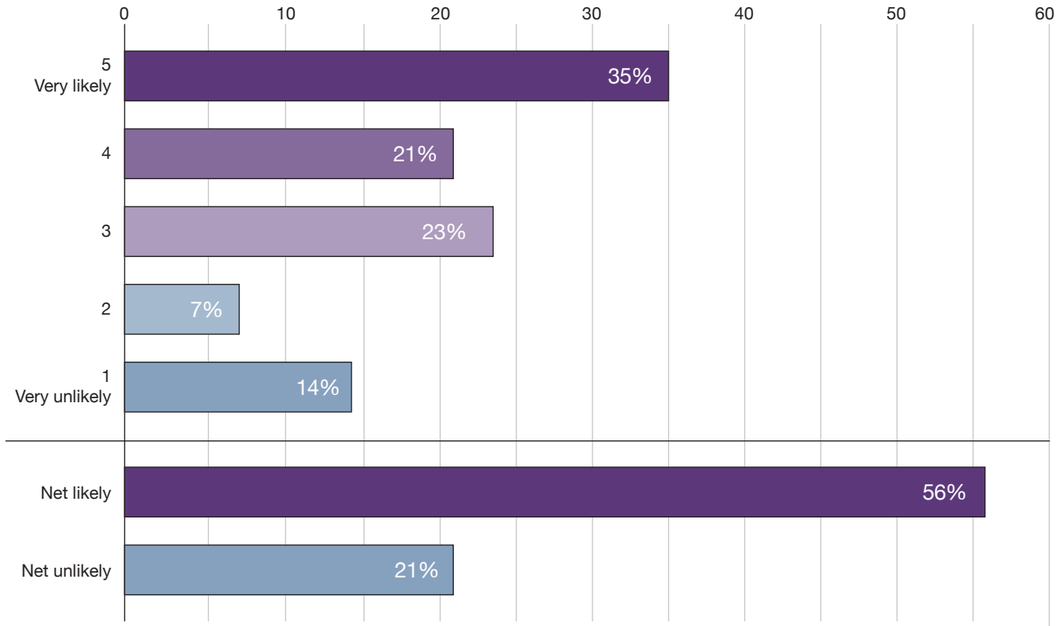





# Q4.

## RELATIONSHIP BETWEEN MALWARE AND ACCESS TO PIRATED CONTENT

**From your understanding, how likely do you think a malware attack or computer/ device malfunction caused by malware is related to the access of pirated content?**



From your understanding, how likely do you think a malware attack or computer/ device malfunction caused by malware is related to the access of pirated content?

| Do you know anyone who ever accesses pirated content via any piracy service? | Very likely 5 | 4 | 3 | 2 | Very unlikely 1 | Net likely | Net unlikely | All |
|---|---|---|---|---|---|---|---|---|
| Myself | 22 | 21 | 13 | 21 | 6 | 21 | 11 | 17 |
| A family member | 19 | 19 | 15 | 13 | 8 | 19 | 10 | 16 |
| A member of my household | 13 | 12 | 8 | 16 | 1 | 13 | 6 | 10 |
| A friend | 38 | 37 | 32 | 25 | 19 | 38 | 21 | 33 |
| An office colleague | 20 | 20 | 10 | 12 | 6 | 20 | 8 | 15 |
| Others | 8 | 11 | 8 | 9 | 15 | 9 | 13 | 10 |
| None | 32 | 32 | 41 | 34 | 60 | 32 | 50 | 38 |
| Unweighted N | 358 | 222 | 241 | 77 | 139 | 580 | 216 | 1,037 |

Despite 56% of respondents believe that accessing a piracy site may result in a malware attack or a computer/device malfunction caused by malware, 21% of them still have accessed piracy sites themselves.

Age Group

| Do you know anyone who ever accesses pirated content via any piracy service? | 18-24 | 25-34 | 35-44 | 45-54 | 55+ | All |
|---|---|---|---|---|---|---|
| Myself | 22 | 16 | 20 | 16 | 10 | 17 |
| A family member | 21 | 17 | 18 | 12 | 9 | 16 |
| A member of my household | 15 | 11 | 11 | 9 | 3 | 10 |
| A friend | 42 | 33 | 29 | 34 | 19 | 33 |
| An office colleague | 15 | 13 | 17 | 18 | 10 | 15 |
| Others | 11 | 10 | 7 | 9 | 15 | 10 |
| None | 32 | 35 | 42 | 38 | 54 | 38 |
| Unweighted N | 223 | 262 | 215 | 241 | 96 | 1,037 |

Age Group

| From your understanding, how likely do you think accessing a piracy site may result in a malware attack or a computer/device malfunction caused by malware? | 18-24 | 25-34 | 35-44 | 45-54 | 55+ | All |
|---|---|---|---|---|---|---|
| 5 – very likely | 28 | 33 | 36 | 39 | 38 | 35 |
| 4 | 22 | 22 | 20 | 20 | 26 | 21 |
| 3 | 28 | 23 | 21 | 21 | 23 | 23 |
| 2 | 9 | 7 | 7 | 7 | 5 | 7 |
| 1 – very unlikely | 14 | 15 | 15 | 13 | 7 | 14 |
| Net likely | 50 | 55 | 57 | 58 | 64 | 56 |
| Net unlikely | 23 | 23 | 22 | 20 | 13 | 21 |
| Unweighted N | 223 | 262 | 215 | 241 | 96 | 1,037 |

It is worth noticing that the younger age group (aged 18-24) cites that 42% of their peers use piracy services, furthermore their understanding on related malware risk is significantly lower than general public. Hence, it is important to raise their awareness on the threats from pirated contents.

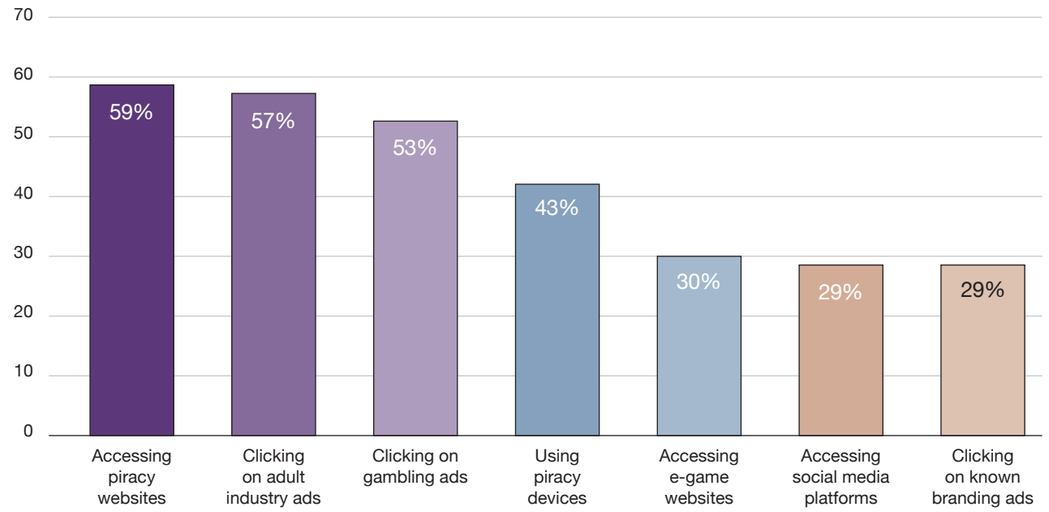


# Q5.

## ACTIVITIES WITH MALWARE RISK

Accessing piracy websites emerges as the highest malware risk activity, with 59% of respondents believing it is the riskiest activities. Clicking on adult industry advertisements comes in second place (57%) and clicking on gambling advertisements is perceived as the third one (53%).

Do you know if anyone who has experienced a malware attack or a computer/ device malfunction that you think could have been caused by malware?



# Appendix C

## Empirical Analysis Study

### Best Case Scenario

| Category | Malicious | Malware | Suspicious | Phishing | Spam | Total |
|---|---|---|---|---|---|---|
| Top 30 Piracy | 16 | 1 | 4 | 0 | 0 | 21 |
| Top 30 Scam | 20 | 2 | 6 | 2 | 1 | 31 |
| Mid-range Piracy | 16 | 0 | 4 | 1 | 0 | 21 |
| Mid-range Scam | 18 | 1 | 4 | 1 | 0 | 24 |
| Control | 1 | 0 | 1 | 0 | 0 | 2 |

### Worst Case Scenario

| Category | Malicious | Malware | Suspicious | Phishing | Spam | Total |
|---|---|---|---|---|---|---|
| Top 30 Piracy | 24 | 2 | 4 | 0 | 0 | 30 |
| Top 30 Scam | 37 | 6 | 8 | 2 | 1 | 54 |
| Mid-range Piracy | 24 | 0 | 4 | 1 | 0 | 29 |
| Mid-range Scam | 24 | 2 | 4 | 2 | 0 | 32 |
| Control | 1 | 0 | 1 | 0 | 0 | 2 |



### Best Case Scenario

| Top 30 piracy | Top 30 scam | Mid-range piracy | Mid-range scam | Control |
|---|---|---|---|---|
| vegamovies.chat | web.app | thebigheap.com | videostape.com | google.com |
| 1tamilblasters.net | amazonmovie.online | moviehunt.me | xmovies8-hd.net | youtube.com |
| dotmovies.bio | trendingnow.github.io | 560pmovie.com | moviesnet.xyz | facebook.com |
| 9animetv.to | yoursilverscreen.com | soap2day-online.com | cinema-xxi.com | instagram.com |
| zoro.to | 4khdmovies.club | seriesonlinehd.tv | onwatchly.com | aajtak.in |
| sanji.to | freemovies.cloud | jamsbase.com | mopiez.com | samsung.com |
| hdhub4u.college | megavideos.online | reqzone.com | kinohdonline.com | cricbuzz.com |
| bollyflix.cool | watchmovies.design | vivdisk.com | nazmovies.xyz | xhamster.desi |
| moviesmod.co.in | hdhub4u.run | zippyshare.com | freemovies.rodeo | whatsapp.com |
| downloadhub.tools | moviesonline4k.tv | multiup.org | yellowmovies.xyz | realsrv.com |
| ibomma.tel | epixflix.com | filmy-hit.green | bingmovies.xyz | parimatch-in.com |
| ibomma.pm | deltaflix.online | filmyzilla.vin | hdflix.club | twitter.com |
| allmovieshub.party | worldmovieshd.com | hdmp4mania2.com | gomovies.casino | amazon.in |
| gogoanimes.fi | watchmovies.racing | bollyflix.casa | flixneo.com | ssyoutube.com |
| 9xflix.qpon | allsportsflix.top | movierulzhd.to | uflix24.com | xhamster.com |
| gogoanime.cl | thepiratebay.email | moviefiz.life | filmybro.us | jiocinema.com |
| mkvmoviespoint.help | bodelen.com | thepiratebay10.org | 123moviesus.xyz | wikipedia.org |
| mkvcinemas.lat | flixmax.stream | hdhub4u.city | moviesholic.stream | quora.com |
| skymovieshd.wine | bemovies.club | 7movierulz.men | onion.ly | google.co.in |
| filmyzilla.cafe | fulltv.com.ar | mlsbd.vip | onlineflix.stream | flipkart.com |
| yts.autos | watchmovies.yachts | gomovies.sx | flixplus21.com | weather.com |
| bolly4u.cafe | popcorntime.co | secretlink.xyz | fullmoviehindidubbed.in | news18.com |
| watchmovierulz.to | movieoi.xyz | toonime.co | fooxplus.club | linkedin.com |
| filmyfly.shop | just-watch.club | moviesmod.co | streamovie.club | espncricinfo.com |
| moviesda5.com | onlineactivation.com | rarbgprx.org | watchmovies.rodeo | openai.com |
| 4funbox.com | moviesred.xyz | mirrorace.org | freemovies.golf | timesofindia.com |
| gdflix.lol | dailyeadscreen.com | jexmovie.com | regionmovie.com | indiatimes.com |
| 5movierulz.ma | fulltv.com.mx | gdrivepro.xyz | 4film.org | zoom.us |
| vegamovies.cheap | bigmoviesc.com | likewap.com | twomovies.info | xvideos2.com |
| moviesnation.vip | flixgo.me | filmyhunk.co | newtwilightzone.club | hindustantimes.com |

## Worst Case Scenario

| Top 30 piracy | Top 30 scam | Mid-range piracy | Mid-range scam | Control |
|---|---|---|---|---|
| vegamovies.chat | web.app | thebigheap.com | videostape.com | google.com |
| 1tamilblasters.net | amazonmovie.online | moviehunt.me | xmovies8-hd.net | youtube.com |
| dotmovies.bio | trendingnow.github.io | 560pmovie.com | moviesnet.xyz | facebook.com |
| 9animetv.to | yoursilverscreen.com | soap2day-online.com | cinema-xxi.com | instagram.com |
| zoro.to | 4khdmovies.club | seriesonlinehd.tv | onwatchly.com | aajtak.in |
| sanji.to | freemovies.cloud | jamsbase.com | mopiez.com | samsung.com |
| hdhub4u.college | megavideos.online | reqzone.com | kinohdonline.com | cricbuzz.com |
| bollyflix.cool | watchmovies.design | vivdisk.com | nazmovies.xyz | xhamster.desi |
| moviesmod.co.in | hdhub4u.run | zippyshare.com | freemovies.rodeo | whatsapp.com |
| downloadhub.tools | moviesonline4k.tv | multiup.org | yellowmovies.xyz | realsrv.com |
| ibomma.tel | epixflix.com | filmy-hit.green | bingmovies.xyz | parimatch-in.com |
| ibomma.pm | deltaflix.online | filmyzilla.vin | hdflix.club | twitter.com |
| allmovieshub.party | worldmovieshd.com | hdmp4mania2.com | gomovies.casino | amazon.in |
| gogoanimes.fi | watchmovies.racing | bollyflix.casa | flixneo.com | ssyoutube.com |
| 9xflix.qpon | allsportsflix.top | movierulzhd.to | uflix24.com | xhamster.com |
| gogoanime.cl | thepiratebay.email | moviefiz.life | filmybro.us | jiocinema.com |
| mkvmoviespoint.help | bodelen.com | thepiratebay10.org | 123moviesus.xyz | wikipedia.org |
| mkvcinemas.lat | flixmax.stream | hdhub4u.city | moviesholic.stream | quora.com |
| skymovieshd.wine | bemovies.club | 7movierulz.men | onion.ly | google.co.in |
| filmyzilla.cafe | fulltv.com.ar | mlsbd.vip | onlineflix.stream | flipkart.com |
| yts.autos | watchmovies.yachts | gomovies.sx | flixplus21.com | weather.com |
| bolly4u.cafe | popcorntime.co | secretlink.xyz | fullmoviehindidubbed.in | news18.com |
| watchmovierulz.to | movieoi.xyz | toonime.co | fooxplus.club | linkedin.com |
| filmyfly.shop | just-watch.club | moviesmod.co | streamovie.club | espncricinfo.com |
| moviesda5.com | onlineactivation.com | rarbgprx.org | watchmovies.rodeo | openai.com |
| 4funbox.com | moviesred.xyz | mirrorace.org | freemovies.golf | timesofindia.com |
| gdflix.lol | dailyeadscreen.com | jexmovie.com | regionmovie.com | indiatimes.com |
| 5movierulz.ma | fulltv.com.mx | gdrivepro.xyz | 4film.org | zoom.us |
| vegamovies.cheap | bigmoviesc.com | likewap.com | twomovies.info | xvideos2.com |
| moviesnation.vip | flixgo.me | filmyhunk.co | newtwilightzone.club | hindustantimes.com |


To discuss the report further, please contact:

**Dr. Paul A. Watters**
Cyberstronomy Pty Ltd
ceo@cyberstronomy.com

**Dr. Shruti Mantri**
ISB Institute of Data Science,
Indian School of Business
shruti_mantri@isb.edu

**Dr. Manish Gangwar**
ISB Institute of Data Science,
Indian School of Business

ISB | Institute of Data Science