Digital Content Piracy: The Free Music and Movies "Honey Trap" at the Cost of Individuals' Cybersecurity and Probable National Security Implications

Authored by
Priyanshi Rastogi
Legal Associate, IMI

Contents

Summary 2

I. Introduction 3

II. Cybercrime as an Implication of Content Piracy on the Internet 4

III. Ad-supported Model of Pirates and Ransomware 5

IV. Recommendations and Suggestions 6

1. Role of Indian Computer Emergency Response Team (CERT-In) 6

2. India's New National Cyber Security Policy 7

3. Security Guidelines for Mobile Devices and Services 7

3.1. Obligations on Network operators 8

3.2. Obligations on Service Providers 8

4. MeitY's Information Security Education and Awareness 9

5. Cyber Surakshit Bharat Initiative 9

6. Cyber Swachhta Kendra 10

Summary

With India set to have over 900 million internet users by 2025, a parallel rise in cyberthreats has become a matter of huge concern for the State and its citizens. In the first 6 months of 2022 alone, there were 6,74,021 cyber-attacks in the country. As per CERT-In, ransomware incidents in India have increased by 51% in the first half of 2022 compared to the same time last year.

With cybercrimes and cybersecurity threats reaching new heights, it is pertinent to acknowledge the ill-effects of digital piracy on user cybersecurity as well as national security. As per the Timeline to Compromise Report by Asia Video Industry Association, consumers could be exposed to cybersecurity threats within 42 seconds of clicking on a pirate website.

Malware installed through a pirate site/ app initiates financial fraud, identity theft, distributed denial-of-service attacks and lateral movement to further infect other devices on the network. Digital piracy also poses a threat to the security of the country since the money generated from disseminating pirated content is often laundered and used to finance organised crimes and terrorist activities.

Despite the cybersecurity and national security menace caused by digital piracy, it is largely overlooked in global and national debates, initiatives and policy efforts dealing with cybercrime in India and around the world. The IMI Policy Brief makes recommendations on measures that can be taken in India to acknowledge and address the cybersecurity risks stemming from digital piracy. Among the steps suggested are consumer awareness initiatives and sensitization of government officials by MeitY and the imposition of obligations on network operators and service providers under the Security Guidelines for Mobile Devices and Services.

I. Introduction

Digital content piracy continues to plague the media and entertainment sector in India causing financial losses to the industry, loss of tax revenues to the national exchequer and adversely impacting employment. The entertainment industry in India loses up to USD 2.8 billion of revenue annually due to digital piracy.[1] India ranked third in consuming pirated content in the first eight months of 2022 with 7.99 billion visits made to pirate websites[2]. The lesser-known consequence of digital content piracy, however, are the attached cybersecurity threats for both users and the nation.

As per INTERPOL's first-ever Global Crime Trend Report, more than 70% of respondents expect crimes such as ransomware and phishing attacks to increase or significantly increase in the next three to five years. It is pertinent to note that financial crime was considered the top crime threat in the APAC region, specifically financial fraud (76%).[3]

As internet penetration in India continues to increase, with the country set to have over 900 million internet users by 2025[4], a parallel rise in cyberthreats has become a matter of huge concern. There were 6,74,021 cyber-attacks in the country this year until June, which translates to around 3,700 cyber-attacks per day.[5] Cyberthreats are an expensive menace with data breaches costing an average of Rs 176 million so far in 2022.[6]

While Indian internet users tend to be extremely price conscious resulting in pirated content being used as a cheaper alternative to legitimate platforms, awareness remains minimal when it comes to cybersecurity issues stemming from content piracy.[7] Users fail to comprehend the damage that malware and other potentially unwanted programs attached to piracy sites and apps are capable of causing to their devices, data and privacy.

---

[1] https://timesofindia.indiatimes.com/blogs/voices/digital-piracy-jeopardises-indias-flourishing-creative-economy/?source=app&frmapp=yes
[2] https://www.muso.com/magazine/piracy-data-overview-january-2022-to-august-2022
[3] https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf
[4] https://www.livemint.com/news/india-to-have-around-900-million-internet-users-by-2025-report-11659063114684.html#:~:text=The%20IAMAI%20report%20titled%20'Internet,in%20the%20past%20two%20years.
[5] https://www.business-standard.com/article/technology/india-sees-sharp-rise-in-cyber-attacks-as-internet-base-continues-to-widen-122080700773_1.html
[6] *Id.*
[7] https://www.livemint.com/industry/media/piracy-on-the-rise-as-viewers-lap-up-movies-for-free-11589218957550.html

The cybersecurity and national security implications of digital piracy are largely overlooked in the debates, initiatives and policy efforts dealing with cybercrime in India. With cybercrimes and cyberthreats reaching new heights, it is imperative to acknowledge the role of digital piracy in the proliferation of data privacy, cybersecurity and national security risks.

II. Cybercrime as an Implication of Content Piracy on the Internet

Audiovisual piracy apps and sites engage in targeted delivery and installation of malicious software (malware) onto consumer devices under the guise of offering free or cheap content to unsuspecting consumers. Malware can be downloaded through malicious advertising, malicious popups, fake browser extension installations, browser notification hijacking, blocking notifications, adware, malicious software installation and banner ads.

As per the Timeline to Compromise Report by Asia Video Industry Association, consumers could be exposed to cybersecurity threats within 42 seconds of clicking on a pirate website.[8] Moreover, consumers using pirate websites and apps are 3 times more likely to be exposed to malware.[9]

Malware installed through a pirate site/ app can be used for capturing network traffic and banking credentials typed into a browser to commit financial fraud, facilitating identity theft by capturing personal data stored on a device, and moving laterally within a network to reconnoitre and further infect other, higher-value devices on the network, such as finance and payment systems.[10] Given the prominence of work from home after the pandemic, piracy becomes a national security concern when the ability of malware to infect all devices on a network is taken into account for government employees working remotely. GroupSense, a cyber intelligence firm, found evidence on the Dark Web that some hackers are discussing creating malware to modify piracy apps to steal consumer data stored on the device including photographs, usernames and passwords, and credit card information.[11]

[8] https://avia.org/how-cyber-criminals-use-ads-to-compromise-devices-through-piracy-websites-and-apps/
[9] https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf
[10] https://www.aapa.eu/study-on-malware-and-audiovisual-piracy-highlights-significant-risks-to-european-consumers
[11] https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf

Malware in piracy apps and websites can also be used to launch distributed denial-of-service attacks (DDoS), which are cyberattacks that use multiple compromised computer systems to target and attack an online service causing a denial of service for users of the targeted service. For instance, the developer of the popular Kodi media player[12] add-on Exodus which provides access to pirated content, inserted malware into the software enabling the developer to initiate DDoS attacks with the help of the infected devices against threats of his identity being exposed.[13]

Pirated content is sold to rogue websites in exchange for monetary consideration and such consideration is often exchanged using crypto-currencies such as bitcoins and/or e-wallets which are difficult to trace. Such unaccounted monies are generally laundered, used for financing organised crimes and terrorist activities, and generally form part of a larger organised crime racket. The offence of digital piracy, therefore, is not a stand-alone offence of copyright infringement but is a threat to the security of the country.

III. Ad-supported Model of Pirates and Ransomware

Legitimate content providers rely on either advertising or subscription models to generate revenues because both creating and hosting content are not free from costs. While providing content illegally, pirate apps and websites not only incur no costs but also use advertisements to generate revenues. The top 10 highest-earning pirate operators (combined top five piracy websites and top five piracy apps) collectively generated over $229 million in global annual revenues from advertising between June 2020 to May 2021.[14] Advertisements on pirate apps and websites accord an element of legitimacy to the pirate app or website. In doing so, they not only give a boost to piracy by increasing site/app traffic but also expose consumers to cybersecurity threats while making money off of cybercrimes.

The modus operandi of pirate operators is taking advantage of the complexity of the digital advertising ecosystem and the lack of audit transparency to hide among billions of legitimate ad placements and earn profits off ads that were never meant to be placed on their website using various techniques to elicit ads. Pirates also use “malvertising” or malicious advertising for ad revenues which involves fake or misrepresentative ads and promotions triggering the

[12] Free and open-source media player software application
[13] https://itif.org/publications/2019/04/25/both-consumers-and-content-creators-lose-piracy-apps/
[14] https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf

onloading of malware on the user's device with each malware infection resulting in payment to the pirate platform in addition to payment for the ad placement.[15]

Malvertising is used to initiate ransomware attacks, which is a cyberattack that encrypts data on the targeted device with criminals demanding payments to make the data accessible again. While targeting government entities, criminals may also threaten to leak sensitive information from the data in case of failure to make payment.[16]

According to INTERPOL's Global Crime Trend report, cyber threats like ransomware are expected to increase in the future according to 79% of enforcement respondents from the APAC region.[17] Ransomware is predicted to cost its victims around $265 billion (USD) annually by 2031, with a new attack every 2 seconds.[18] As per CERT-In, ransomware incidents have increased by 51% in the first half of 2022 compared to the same time last year and drive by download[19] is the common tactic in citizen-centric ransomware cases.[20] The fact that even piracy advertising researchers were hit by ransomware further highlights the capability and reach of ransomware prevalent on piracy websites and apps.[21]

IV. Recommendations and Suggestions

Despite the cybersecurity menace that digital piracy causes, it is largely overlooked in policies and initiatives dealing with cybercrime in India. The following recommendations address key steps that can be taken in India to acknowledge and address the cybersecurity risks stemming from digital piracy.

1. Role of Indian Computer Emergency Response Team (CERT-In)

The Indian Computer Emergency Response Team (CERT-In) is responsible for tracking and monitoring cybersecurity incidents in India. CERT-In also issues advisories regarding the latest

[15] https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Unholy-Triangle-Report.pdf
[16] https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Unholy-Triangle-Report.pdf
[17] https://www.interpol.int/en/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf
[18] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
[19] A drive-by download attack refers to the unintentional download of malicious code to your computer or mobile device that leaves you open to a cyberattack.
[20] https://www.csk.gov.in/documents/RANSOMWARE_Report_Final.pdf
[21] https://torrentfreak.com/piracy-advertising-researchers-fall-victim-to-ransomware-attacks/

cyber threats and countermeasures regularly; it has issued 68 advisories for data security and mitigating fraudulent activities so far.[22]

Recently, CERT-In issued an advisory on festival-themed scams that promise users offers and prizes but end up stealing sensitive information like bank account details and OTP.[23] Similarly, CERT-In must issue an advisory specifically dealing with digital piracy to apprise users of the cybersecurity risks stemming from accessing content on pirate websites and apps. While CERT-In has issued advisories on mobile based malware[24] and securing mobile devices and applications[25], there is no mention of digital content piracy. Given that roughly 1 in 3 pirate apps carry malvertising[26], it is pertinent that CERT-In explains to users that pirate apps are usually embedded with malware and provide guidance on identifying such rogue apps.

2. India's New National Cyber Security Policy

India's National Cyber Security Policy is due for an update. The currently applicable National Cyber Security Policy 2013[27] aims to prevent and respond to cyber threats through a combination of institutional structures, people, processes, technology and cooperation. While the Policy mentions development of effective public-private partnerships and creation of cyber awareness, it fails to make any reference to digital piracy. In order to safeguard privacy of citizens' data and reduce economic losses incurred from cybercrime and data theft, it is pertinent that the new National Cyber Security Policy, which is reportedly in the works since 2019[28], address the link between digital piracy, cybersecurity threats and cybercrimes.

3. Security Guidelines for Mobile Devices and Services

The Ministry of Electronics and Information Technology (MeitY) initiative to put out Draft Security Guidelines for Mobile Devices and Services[29], with the aim to protect sensitive data and provide security to mobile service users, is highly appreciable. However, given that pirate websites and apps expose mobile phone users to security threats of sensitive information loss

[22] https://loksabhaph.nic.in/Questions/QResult15.aspx?qref=35987&lsno=17
[23] https://www.medianama.com/2022/10/223-cert-in-advisory-festival-scams/
[24] https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2022-0014
[25] https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0013
[26] https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf
[27] https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf
[28] https://www.medianama.com/2020/10/223-cybersecurity-policy-to-have-cyber-insurance-framework/
[29] https://www.medianama.com/wp-content/uploads/2022/09/MSG_Guidelines_Draft_V1.0_July_22-2.pdf

and misuse of personal data by adversaries, the following obligations should be included under the Security Guidelines for Mobile Devices and Services.

3.1. Obligations on Network operators

While the Draft Guidelines contains a provision on the obligation of network operators to deploy network and edge intelligence to eliminate rogue mobile apps, the term "rogue mobile apps" has not been defined and it is important that the same be defined to include all kinds of content piracy within its ambit, taking into consideration the factors laid down in UTV Software Communication Ltd. and Ors. v. 1337X.TO and Ors. (2013)[30] for determining whether a website is a rogue website.

Moreover, network operators should have the obligation to implement robust detection systems for malware and other cybersecurity threats for displaying warnings to users similar to browsers providing an intermediate warning page, that prevents the user from proceeding, until they click a button, acknowledging the detected risks.

3.2. Obligations on Service Providers

3.2.1. App stores

Service providers such as mobile app stores must be obligated to have technological measures in place to scrutinize mobile apps and prevent the listing of rogue apps that provide pirated content embedded with malware. Furthermore, social media and mobile apps must work with network operators to ensure that links to pirate websites and apps that pose threat to mobile security are not being circulated amongst users.

3.2.2. Ad-tech companies

Ad-tech companies are intermediaries whose services are used by brands or ad agencies for ad placement on publishing spaces available in the market. Take for instance, Google's advertising technologies, which include its content delivery network and advertising delivering systems, appears to have provided 51% of ads to piracy apps.[31] The Guidelines must obligate ad-tech service providers to conduct due diligence before

[30] 2019 SCC OnLine Del 8002
[31] https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf

purchasing ad-space on apps/ websites to ensure that they are not exposing users to security threats by using ad-space on pirate websites/ apps.

4. MeitY's Information Security Education and Awareness

MeitY is implementing the Information Security Education and Awareness (ISEA) Phase-II project to train government personnel and create mass information security awareness for various users.[32] The awareness workshops being conducted under this initiative and the self-paced three module e-learning course on Cyber Hygiene Practices[33] should also include material on digital piracy and related cybersecurity threats.

InfoSec Awareness website provides information on various topics such as mobile security, cyber stalking, phishing attacks, OTP frauds, dangerous malware found in Android Apps, QR Code scams, etc. but fails to address digital content piracy. Even the webpages on 'Dangerous Malware found in Android Apps'[34] and 'Mobile Security'[35] fail to explain the link that pirate apps have with malware and cybersecurity of users. Moreover, the advisory on 'Dangerous Malware found in Android Apps'[36] does not apprise users to be cautious of apps providing copyrighted audio-visual content free of cost and instead suggests avoiding installing mobile applications containing advertisements, which is an impractical solution. It is suggested that MeitY use the InfoSec Awareness website as a platform to spread awareness about cybersecurity risks of digital piracy, particularly in relation to malware and mobile devices.

5. Cyber Surakshit Bharat Initiative

MeitY's Cyber Surakshit Bharat initiative aims to spread awareness about cyber-crime and build capacities across all government departments, in order to ensure adequate safety measures to combat the growing menace of cybercrimes. It is disappointing, to say the least, that the Course Overview of the upcoming Training Programme[37] mentions various topics like darknet and darkweb, social media management, and D-DOS attack but makes no mention of digital piracy. Given the well-established association between digital piracy and cybersecurity threats, it is imperative that law enforcement authorities are sensitized to the issue and therefore, a

[32] https://pib.gov.in/PressReleasePage.aspx?PRID=1885363
[33] https://infosecawareness.in/cybhyg
[34] https://www.infosecawareness.in/topic/dangerous-malware-found-in-8-android-apps
[35] https://www.infosecawareness.in/concept/mobile-security?lang=en
[36] https://www.infosecawareness.in/topic/dangerous-malware-found-in-8-android-apps
[37] https://www.meity.gov.in/writereaddata/files/Cyber%20Surakshit%20Brochure_.pdf

module on “Digital piracy: A cybercrime and a cybersecurity threat” must be included in the training programme under the Cyber Surakshit Bharat initiative.

6. Cyber Swachhta Kendra

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre), operated by CERT-In, provides cyber security tips and best practices for citizens and organisations, in addition to its function of detection of malicious programs and free tools to remove the same. Under ‘Security for personal computer’ in Security Best Practices, the ‘Internet Security’ section states that copyright issues must be checked before using the internet and only original websites should be used for downloading files.[38] While these security best practices are appreciated, it would be more practicable to refer to digital piracy apps and websites that disseminate free content illegally to enable better user understanding.

[38] https://www.csk.gov.in/documents/Desktop_security.pdf