

Advisory Committee on Enforcement

Eighteenth Session
Geneva, June 2 to 4, 2026

THE NEXUS BETWEEN MALWARE AND PIRACY – ENFORCEMENT TOOLS AND OPPORTUNITIES FOR GOVERNMENT TO TAKE ACTION

*Contribution prepared by Dr. Elena Blobel, Director of Global Litigation, International Federation of the Phonographic Industry, London, United Kingdom **

ABSTRACT

This contribution outlines how online piracy services routinely use the promise of free access to copyright-protected content to attract consumers to websites, apps and devices that expose them to significant risks. It highlights the type of malware used in relation to online piracy and the range of enforcement tools available to disrupt malware distribution. The contribution advocates that more attention be given at the policymaking level to the nexus between malware and piracy and the multiple associated forms of criminality. It concludes by identifying priority areas for further study, with a view to facilitating informed decision-making by policymakers.

* The views expressed in this document are those of the author and not necessarily those of the Secretariat or of the Member States of WIPO.

I. WHY IS COPYRIGHT-PROTECTED CONTENT USED IN CONNECTION WITH MALWARE DISTRIBUTION?

1. The promise of access to free, copyright-protected content through online piracy services is widely used by bad actors to lure consumers into accessing sites, apps and devices that expose them to various types of malicious threat vectors. This contribution sets out the current state of play regarding the types of malware involved, the potential scale of the issue, the types of existing enforcement actions, as well as the opportunities for governments to tackle this issue, including by raising consumer awareness.

A. TYPES OF MALWARE INVOLVED IN RELATION TO ONLINE PIRACY

2. In the experience of the International Federation of the Phonographic Industry (IFPI), there are various types of malware that can be found on music piracy sites and services. Some examples of malware connected with piracy services include:

- Ransomware delivered via deceptive pop-ups, pop-unders, click-to-play, or fake download buttons on pirate streaming and torrent sites that encrypt the files of the victim. Subsequently, payment is demanded to restore access, usually in the form of cryptocurrency.
- Crypto-jacking, where crypto-mining scripts are run covertly in the browser or device of a user, while consuming computer resources and degrading performance.
- Spyware, which covertly monitors user activity, capturing keystrokes and credentials and exfiltrating confidential or personal information such as emails, financial information and photos.
- Trojans, which comprise malware disguised as legitimate software that is downloaded through fake updates, media players or installers and creates backdoors or the installation of other malicious tools. Malvertising consists of aggressive, deceptive or intrusive ads, leading to malware downloads, harvesting of user data and redirecting users to scam pages.
- Scareware, mimicking system warnings and thereby tricking victims into downloading malicious programs. These are common on both mobile and desktop piracy services.
- Credential theft tools and fake login and payment pages focus on harvesting usernames, passwords and two-factor authentication tokens. These stolen credentials can be reused on banking or social media accounts, enabling identity theft, unauthorized fund transfers and account takeovers, and can also be resold on the illicit market. Compromised credentials can be used to access accounts for the purpose of carrying out streaming fraud (i.e. to generate fake streams of tracks on music streaming platforms which do not represent genuine fan consumption), thus diverting revenues from legitimate artists and other rights holders.
- Botnet recruitment where peer-to-peer clients, cracked network tools or illicit streaming devices pre-loaded with unlicensed add-ons are used to infiltrate local network and devices, leading them to be unwittingly recruited to botnets that coordinate distributed denial-of-service attacks, spam campaigns or additional malware distribution. Such botnets can also be used to conduct fraud, including streaming fraud.

- Domain Name System (DNS) hijackers alter DNS settings or browser configuration to redirect traffic to malicious or affiliate landing pages, re-routing the web requests of the user via attacker-controlled services.

B. THE SCALE OF THE ISSUE

3. To date, millions of Internet users access online pirate sites globally to access unlicensed copyright protected content. There is a significant body of research which assessed the potential scale of the issue and the malware risks that Internet users encounter in connection with online piracy. Overall, the reports, predominantly focused on the audiovisual sector, have highlighted that threats exist on a staggering scale worldwide. For example:

- Consumers in Southeast Asia face on average more than a 22-fold increase in cyberthreat detections on piracy sites versus mainstream control sites.¹
- In India, piracy sites carry a 59 per cent risk of malware infection, higher than adult entertainment or gambling sites, with younger users (18–24) being particularly vulnerable.²
- So-called malvertising accounted for 12 per cent of the total advertisements on piracy sites, generating a minimum of US\$ 121 million annually in revenue. Nearly 80 per cent of pirate sites investigated served malware-ridden advertisements. A visit to a piracy site leads to an attempt to serve malware to the user one in six times on average.³
- Consumers in Poland are, on average, 38.5 times more likely to encounter cyber threats on peer-to-peer sites compared to mainstream ones.⁴
- A study found that European consumers could be attacked within 71 seconds of landing on piracy sites, and on average there was a 57-per cent chance of audiovisual piracy apps coming pre-installed with embedded malware.⁵

4. Data in other sectors is less available, but the principles are broadly applicable to any rogue websites, apps and devices which offer unlicensed content to attract users, and this also bears out anecdotally in the music sector.

5. Research conducted by IFPI in Latin America found that 33 per cent of a sample of 174 MP3 download sites operating in the region were connected to malware distribution. Among those illegal music sites, 17 per cent were directly distributing malware, while another 26 per cent were indirectly distributing suspicious malware files via secondary pages under different domain names. The same research also showed that 10 per cent of those illegal music sites distributing malware had proprietary infringing mobile apps, raising the risks of abusive access and theft of personal data, as well as other types of cybercrimes. More generally, Internet users in Brazil suffered a 408 per cent increase in online fraud since 2018, with 2.1 million cases reported in 2024.⁶

¹ <https://www.alliance4creativity.com/wp-content/uploads/2025/07/Watters-PiracyInSEA-071025-v2.pdf>.

² https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4766797.

³ <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Unholy-Triangle-Report.pdf>.

⁴ https://www.mpa-emea.org/wp-content/uploads/2024/09/Watters-Consumer-Risk-from_Piracy-in-Poland.pdf.

⁵ <https://www.aapa.eu/study-on-malware-and-audiovisual-piracy-highlights-significant-risks-to-european-consumers>.

⁶ <https://forumseguranca.org.br/publicacoes/anuario-brasileiro-de-seguranca-publica/>.

C. WHICH ENFORCEMENT TOOLS ARE AVAILABLE TO ADDRESS THIS ISSUE?

6. Several initiatives exist to address malware distribution, including the following:

- The Europol Operation Endgame, a large-scale initiative focused on disrupting botnets and associated criminal infrastructures.⁷
- The National Cybercrime Forensic Laboratory within the Indian Cyber Crime Coordination Centre, which provides specialized malware forensics and analysis services to law enforcement authorities.⁸
- The Central Consumer Protection Authority of India, which has issued advice stating that digital platforms should identify and eliminate dark patterns from their interfaces, including rogue malware.⁹

7. Similar tools should be readily available in other countries to tackle malware in the context of piracy, as seen in the initiatives coordinated by the Ministry of Justice and Public Security and the Cyber Operations Laboratory in Brazil:

- Operation 404, which targeted more than 3,000 infringing sites and mobile apps in seven rounds in the last six years, some featuring direct malware distribution and personal data theft.¹⁰
- Operation Redirect, which specifically targeted piracy sites associated with malware distribution (including illegal linking music sites, stream ripping sites and torrent search engines).¹¹ The coordinated operation seized domains, blocked sites and shut down illegal websites through the combined application of disruptive measures.¹²

8. In addition to criminal remedies, civil remedies may also be available. For example, Google recently announced the launch of a lawsuit against the operators of the Badbox 2.0 botnet, which it claims has infected over 10 million devices running the Android open-source software.¹³

9. Online platforms and intermediaries must also play a role in disrupting these activities. Devices pre-loaded with infringing content and malware are sold on e-commerce platforms; mobile applications featuring malware are available on official and unlicensed app stores; rogue websites distributing malware can be discovered by search; and domain and hosting intermediaries provide the infrastructure that enables these sites. Even if this activity is prohibited under their respective terms and conditions, malicious actors are able to continue operating. As such, proactive steps are required, coupled with a scalable reporting mechanisms and expeditious and effective removal. There are also independent organizations that offer reporting channels.¹⁴

⁷ <https://www.europol.europa.eu/operations-services-and-innovation/operations/operation-endgame>.

⁸ <https://education.vikaspedia.in/viewcontent/education/digital-literacy/information-security/indian-cyber-crime-coordination-centre?lgn=en>.

⁹ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2134765>. This follows the 2023 Guidelines for Prevention and Regulation of Dark Patterns of the Central Consumer Protection Authority.

¹⁰ <https://www.gov.br/mj/pt-br/assuntos/noticias/operacao-internacional-contra-pirataria-tira-do-ar-675-sites-e-14-aplicativos-de-streaming>.

¹¹ <https://www.ifpi.org/brazilian-authorities-launch-operation-redirect-targeting-illegal-music-sites-responsible-for-malware-distribution/>.

¹² <https://www.gov.br/mj/pt-br/assuntos/noticias/operacao-redirect-bloqueia-oito-sites-piratas-de-musica-1>.

¹³ <https://www.securityweek.com/google-sues-operators-of-10-million-device-badbox-2-0-botnet/>.

¹⁴ For example, Netbeacon offers a channel for the reporting of DNS abuse: <https://netbeacon.org/>.

D. WHY SHOULD THIS BE IMPORTANT FOR GOVERNMENTS?

10. It is important that the issue of the link between online piracy and malware, as well as evolving trends in this area, are brought to the attention of authorities and governments globally. Using piracy sites to distribute malware is an example of poly-criminality which can be extremely harmful to consumers worldwide. Together with the harm caused by piracy, this constitutes a risk not only for rights holders but also for society at large.

11. Recent trends also demonstrate that piracy ecosystems increasingly intersect with broader forms of cybercrime and poly-criminality. In particular, unofficial application ecosystems, unauthorized app stores, APK download sites and other side-loading channels are frequently used to distribute applications associated with malware, spyware, credential theft, fraud and other malicious activity.

12. Consumers seeking unauthorized access to music, audiovisual or live-streaming content may unknowingly install applications outside of trusted distribution environments, exposing devices and personal data to significant cybersecurity risks.

13. Such activities illustrate how piracy services can act not only as mechanisms for copyright infringement, but also as gateways for wider criminal conduct including phishing, financial fraud, botnet recruitment, advertising fraud and large-scale credential harvesting.

14. In some cases, malicious actors exploit demand for popular content or content that has been removed from mainstream app stores to lure consumers into downloading infected applications or interacting with deceptive links and fake software updates.

15. The growing prevalence of sideloaded mobile applications and unlicensed app distribution channels further increases these risks, particularly where bad actors can rapidly repackage and redistribute infringing or malicious applications outside established review and security processes. This reinforces the need for coordinated engagement between governments, cybersecurity authorities, law enforcement, online intermediaries and app ecosystem operators to address the broader societal harms associated with piracy-linked malware distribution.

16. It is expected that the risks posed by malware on piracy sites and apps will continue to grow, facilitated by artificial intelligence (AI). A recent report recognized that AI could augment and facilitate certain crime types, including malware distribution, through its ability to combine more realistic looking content with automated delivery at scale.¹⁵ Cybercrime and fraud have a detrimental effect on victims, which was the subject of a recent study published by the United Kingdom Home Office.¹⁶

II. CONCLUSION

17. The nexus of malware and online piracy should be studied further, including by the World Intellectual Property Organization, to gather relevant data and information to facilitate informed decision-making by policymakers, with a view to developing the necessary tools to tackle any emerging issues.

18. There are a number of areas which could be studied further, for instance:

- The threat arising from piracy in mobile applications, including popular content-sharing applications such as Discord and Telegram, particularly given the growth of content consumption via mobile, and the broader availability of such mobile

¹⁵ https://cetas.turing.ac.uk/sites/default/files/2025-03/cetas_research_report_-_ai_and_serious_online_crime_0.pdf.

¹⁶ <https://www.gov.uk/government/publications/understanding-the-cyber-crime-and-fraud-victim-journey/understanding-the-cyber-crime-and-fraud-victim-journey>.

applications from unauthorized app stores/Android Package Kit download sites (i.e. side-loading).

- The potential new threat vectors posed by emerging technologies, for example, using AI to generate fake pre-release or other deepfake content that can be used as bait for malware distribution.
- The role of malware in poly-criminality, including the distribution of malware via devices offering access to unlicensed content, which can then be used to harvest credentials or establish botnets for other nefarious purposes such as streaming fraud.

19. There are already a number of enforcement tools and actions being taken which can serve as a starting point for the establishment of global best practices, and which should foster discussions and engagement with intermediaries, encouraging them to take more voluntary actions.

20. Furthermore, ongoing awareness-raising and education of consumers in connection with the harm caused by online piracy should be paired, where applicable, with appropriate warnings related to malware risk.¹⁷

[End of contribution]

¹⁷ For example, a 2023 study by the European Union Intellectual Property Office found that 82 per cent of European citizens agree that illegally obtaining online content entails a risk of exposure to harmful practices such as scams or inappropriate content for minors. Nonetheless, it was considerably less common for people to avoid illegal sources because of bad experiences for themselves or others (13 per cent and 19 per cent, respectively). However, these reasons were more compelling to motivate intentional users of illegal services to stop using online pirated content (31 per cent and 29 per cent, respectively). See: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2023_IP_Perception_Study/2023_IP_Perception_Study_FullR_en.pdf.