

执法咨询委员会

第十八届会议
2026 年 6 月 2 日至 4 日，日内瓦

恶意软件与盗版之间的联系——执法工具及政府采取行动的机会

撰稿：国际唱片业协会全球诉讼部主任埃琳娜·博贝尔（Elena Blobel）博士，联合王国伦敦*

摘 要

本文概述了在线盗版服务通常如何通过承诺免费提供受版权保护的内容，吸引消费者访问相关网站、应用程序和设备，从而使消费者面临重大风险。本文重点介绍了在线盗版中使用的恶意软件类型，以及可用于阻断恶意软件分发的各种执法工具。本文还主张在政策制定层面更加关注恶意软件与盗版之间的联系以及多种相关犯罪形式，并在最后确定了进一步研究的优先领域，以助力政策制定者做出知情决策。

* 本文件中表达的观点为作者的观点，不一定代表产权组织秘书处或成员国的观点。

一、为什么受版权保护的内容会被用于恶意软件分发？

1. 不良行为体普遍借由在线盗版服务可免费受版权保护内容的承诺，诱使消费者访问相关网站、应用程序和设备，从而使消费者暴露于各种类型的恶意威胁载体。本文介绍了当前相关情况，包括所涉恶意软件类型、问题的潜在规模、现有执法行动的类型，以及各国政府解决该问题（包括通过提高消费者认识）的机会。

A. 在线盗版涉及的恶意软件类型

2. 根据国际唱片业协会（IFPI）的经验，音乐盗版网站和服务中可以发现各种类型的恶意软件。与盗版服务有关的恶意软件举例如下：

- 通过盗版流媒体和种子网站上的欺骗性弹出窗口、隐性弹窗广告、点击播放或虚假下载按钮传播的勒索软件，此类软件会对受害者的文件进行加密。随后，通常要求以加密货币的形式支付赎金，以恢复文件访问权限。
- 加密劫持，即在用户的浏览器或设备中秘密运行加密挖矿脚本，同时消耗计算机资源并降低性能。
- 间谍软件，该类软件暗中监控用户活动，记录键盘输入内容和账户凭证，并窃取电子邮件、财务信息和照片等机密信息或个人信息。
- 木马程序，包括伪装成合法软件的恶意软件，通过虚假更新、媒体播放器或安装程序下载，并会创建后门或安装其他恶意工具。恶意广告，包括攻击性、欺骗性或侵入性广告，会导致恶意软件下载、用户数据被窃取以及将用户重定向至诈骗网页。
- 恐吓软件，模仿系统警告，从而诱骗受害者下载恶意程序。这些在移动端和桌面端的服务中均很常见。
- 凭证窃取工具和虚假登录及支付页面的重点是窃取用户名、密码和双因素身份验证令牌。这些被盗凭证可在银行账户或社交媒体账户上重复使用，从而实现身份盗用、未经授权的资金转移和账户接管，还可以在非法市场上转售。被盗凭证可被用于访问账户，以进行流媒体欺诈（即在音乐流媒体平台上生成并不代表真正粉丝消费的虚假曲目播放量），从而转移合法艺术家和其他权利人的收入。
- 僵尸网络招募，即利用点对点客户端、破解的网络工具或预装未经许可附加组件的非法流媒体设备，侵入局域网及设备，使其在用户不知情的情况下被招募到僵尸网络，从而参与协调分布式拒绝服务攻击、垃圾邮件活动或进一步分发恶意软件。此类僵尸网络还可用于进行欺诈，包括流媒体欺诈。
- 域名系统（DNS）劫持者，通过篡改 DNS 设置或浏览器配置，将流量重定向至恶意或关联登陆页面，从而通过攻击者控制的服务对用户网页请求重新路由。

B. 问题的规模

3. 迄今为止，全球有数百万互联网用户访问在线盗版网站，以获取未经许可的版权保护内容。有大量研究对该问题的潜在规模以及互联网用户在在线盗版方面遇到的恶意软件风险进行了评估。总体而言，这些主要针对视听领域的报告强调，全世界存在的威胁规模惊人。例如：

- 东南亚消费者在盗版网站遭遇的网络威胁检出量，相较于主流对照网站平均高出 22 倍以上。¹
- 在印度，盗版网站感染恶意软件的风险高达 59%，高于成人娱乐或赌博网站，年轻用户（18-24 岁）尤其易受侵害。²
- 所谓恶意广告占盗版网站广告总量的 12%，每年至少产生 1.21 亿美元的收入。在所调查的盗版网站中，有近 80% 的网站充斥着恶意软件广告。平均每访问盗版网站六次，就会出现一次向用户推送恶意软件的行为。³
- 波兰消费者在点对点网站上遭遇网络威胁的几率平均是主流网站的 38.5 倍。⁴
- 一项研究发现，欧洲消费者在登陆盗版网站的 71 秒内就可能遭遇攻击，平均有 57% 的盗版视听应用程序预装内嵌恶意软件。⁵

4. 其他领域可获取的数据较少，但上述原则广泛适用于提供未经许可内容以吸引用户的任何流氓网站、应用程序和设备，这在音乐领域更有实例佐证。

5. 国际唱片业协会在拉丁美洲进行的研究发现，在该区域运营的 174 个 MP3 下载网站样本中，有 33% 与恶意软件分发有关。在这些非法音乐网站中，有 17% 直接分发恶意软件，另有 26% 通过不同域名下的二级页面间接分发可疑的恶意软件文件。同一研究还显示，在分发恶意软件的非法音乐网站中，有 10% 拥有专有侵权移动应用程序，从而增加了滥用访问权、窃取个人数据以及其他类型网络犯罪的风险。更广泛来看，自 2018 年以来，巴西网民遭遇的网络欺诈增加了 408%，2024 年报告的案件达 210 万起。⁶

C. 有哪些执法工具可用于解决这一问题？

6. 为解决恶意软件分发问题采取的若干举措包括：

- 欧洲刑警组织的“终局行动”，这一项大型行动，重点是捣毁僵尸网络和相关的犯罪基础设施。⁷

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/>。

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

- 印度网络犯罪协调中心内的国家网络犯罪法医实验室，为执法当局提供专门的恶意软件法证和分析服务。⁸
- 印度中央消费者保护局，该局已提出建议，指出数字平台应识别并消除其界面中的黑暗模式，包括流氓恶意软件。⁹

7. 正如巴西司法和公共安全部与网络行动实验室协调开展的以下举措所显示的那样，其他国家也应具备类似的工具，以应盗版方面的恶意软件：

- 404 行动，在过去六年中分七轮针对 3,000 多个侵权网站和移动应用程序开展，其中一些侵权网站和移动应用程序直接分发恶意软件和窃取个人数据。¹⁰
- 重定向行动，专门针对与恶意软件分发有关的盗版网站（包括非法链接音乐网站、流媒体翻录网站和种子搜索引擎）。¹¹该协调行动通过综合运用多种捣毁措施，查封域名、屏蔽网站并关停了非法网站。¹²

8. 除刑事补救措施外，还可能民事补救措施。例如，谷歌最近宣布对 Badbox 2.0 僵尸网络的运营商提起诉讼，谷歌声称该网络已经感染了超过 1,000 万台运行安卓开源软件的设备。¹³

9. 在线平台和中介也必须在捣毁这些活动方面发挥作用。预装侵权内容和恶意软件的设备在电子商务平台上销售；官方和未经许可的应用程序商店都提供带有恶意软件的移动应用；通过搜索可以发现分发恶意软件的流氓网站；域名和托管服务中介提供了支持这些网站的基础设施。即使根据各自的条款和条件，此类活动是被禁止的，恶意行为体仍能继续运作。因此，需要采取积极主动的措施，同时建立一个可扩展的举报机制，并迅速有效地清除。还有一些独立组织提供举报渠道。¹⁴

D. 为什么这对各国政府而言很重要？

10. 必须使在线盗版与恶意软件之间的联系问题以及该领域不断演变的趋势应引起全球当局和各国政府的注意。利用盗版网站分发恶意软件是多重犯罪的一个例子，可能对全球消费者造成极大危害。加上盗版造成的危害，这不仅对权利人，而且对整个社会都构成了风险。

11. 最近的趋势还表明，盗版生态系统日益与更广泛的网络犯罪和多重犯罪形式交织在一起。特别是，非官方应用程序生态系统、未经授权的应用程序商店、APK 下载网站和其他侧载渠道经常被用来分发与恶意软件、间谍软件、凭证窃取、欺诈和其他恶意活动有关的应用程序。

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>。这遵循了中央消费者保护局《2023 年黑暗模式防范与规范指南》。

¹⁰ <https://www.gov.br/mj/pt-br/assuntos/noticias/operacao-internacional-contrapirataria-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 例如，Netbeacon 提供了一个举报 DNS 滥用的渠道：<https://netbeacon.org/>。

12. 试图未经授权获取音乐、视听或直播内容的消费者可能会在不知情的情况下在可信的分发环境之外安装应用程序，从而使设备和个人数据面临重大的网络安全风险。
13. 此类活动表明，盗版服务不仅可以充当版权侵权的手段，还可以充当更广泛犯罪行为的网关，包括网络钓鱼、金融欺诈、僵尸网络招募、广告欺诈和大规模凭证窃取。
14. 在某些情况下，恶意行为体利用对热门内容或已从主流应用程序商店下架内容的需求，诱使消费者下载受感染的应用程序，或与欺骗性链接和虚假软件更新进行交互。
15. 侧载移动应用程序和未经许可的应用程序传播渠道的日益盛行进一步增加了这些风险，特别是当不良行为体可以在既定审查和安全流程之外迅速重新打包和重新分发侵权或恶意应用程序时。这就更加需要各国政府、各网络安全机构、执法部门、在线中介和应用程序生态系统运营商之间的协调参与，以解决与盗版相关的恶意软件分发所带来的更广泛的社会危害。
16. 预计在人工智能的推动下，盗版网站和应用程序上的恶意软件所带来的风险将继续增加。最近的一份报告认为，人工智能能够将更逼真的内容与大规模自动交付结合起来，从而增强和促进某些类型的犯罪，包括恶意软件分发。¹⁵ 网络犯罪和欺诈对受害者造成有害影响，这是联合王国国内政部最近发表的一项研究的主题。¹⁶

二、 结论

17. 应由世界知识产权组织等进一步研究恶意软件与在线盗版之间的联系，以收集相关数据和信息，助力政策制定者做出知情决策，进而开发必要的工具来解决任何新出现的问题。
18. 有许多领域可以进一步研究，例如：
- 移动应用程序（包括 Discord 和 Telegram 等热门内容共享应用程序）盗版带来的威胁，特别是考虑到通过移动设备消费内容的增长，以及从未经授权的应用程序商店/Android 软件包下载网站（即侧载）更广泛地获取此类移动应用程序。
 - 新兴技术带来的潜在新威胁载体，例如，利用人工智能生成虚假的预发布内容或其他深度伪造内容，并将其作为分发恶意软件的诱饵。
 - 恶意软件在多重犯罪中的作用，包括通过提供未经许可内容访问权限的设备分发恶意软件，然后利用这些软件窃取凭证或建立僵尸网络，以实现流媒体欺诈等其他恶意目的。
19. 目前已经有若干执法工具和行动，可以作为建立全球最佳做法的起点，并应促进与中介的讨论与协作，鼓励其采取更多自愿性行动。

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>.

20. 此外，在就在线盗版所造成的危害对消费者持续开展宣传和教育工作的同时，还应酌情就恶意软件风险发出适当警示。¹⁷

[稿件完]

¹⁷ 例如，欧洲联盟知识产权局 2023 年的一项研究发现，82%的欧洲公民认为，非法获取在线内容会带来遭遇欺诈或未成年人不宜内容等有害行为的风险。然而，由于自身或他人遭遇过不良经历而规避非法来源的情况则要少得多（分别为 13%和 19%）。不过，这些原因更能促使故意使用非法服务的用户停止使用在线盗版内容（分别为 31%和 29%）。见：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。