Illegal IPTV Technologies

Subjects: Others

Contributor: Adam Lockett , Ioannis Chalkias , Cagatay Yucel , Jane Henriksen-Bulmer , Vasilis Katos

Technologies providing copyright-infringing IPTV content are commonly used as an illegal alternative to legal IPTV subscriptions and services, as they usually have lower monetary costs and can be more convenient for users who follow content from different sources. These infringing IPTV technologies may include websites, software, software add-ons, and physical set-top boxes. Due to the free or low cost of illegal IPTV technologies, illicit IPTV content providers will often resort to intrusive advertising, scams, and the distribution of malware to increase their revenue.

malware analysis | cyber threat intelligence | IPTV | digital investigations

1. Introduction

As many illicit content providers supply copyright-infringing IPTV content for free, they often rely on intrusive advertising, tracking, scams, and malware to make a profit. Illicit content providers also get paid by malware authors to infect their own illicit IPTV websites or software, which are frequently malware families that can generate indirect income with ease, such as cryptocurrency-mining malware [1][2]. One study found that dozens of illicit IPTV websites contained “download now” adverts, redirecting users to landing pages with instructions for downloading malicious browser extensions [3]. Another study found that for the Australian population, 99% of advertisements on illicit content-sharing websites were categorised as high risk, with 46% of these advertisements classified as malicious [4]. Overall, this implies that using copyright-infringing IPTV technologies poses a significant risk to users’ devices, as illicit content providers cannot be trusted and may use malware to increase their revenue.

Internet Protocol Television (IPTV) is a service that provides TV programmes and on-demand video content under the TCP/IP internet protocols [5]. Most legal IPTV services supply video content as part of a TV licence, one-time purchase, or paid subscription, whereas free alternatives usually incorporate advertisements. While IPTV services each have many different genres of video content, users often need to subscribe to multiple services to view the specific films and TV programmes they want to watch. Due to the limited effort, convenience, and monetary costs of these legal IPTV services, many users instead choose to use copyright-infringing IPTV technologies to view video content illegally. A report by Sandvine estimates that “roughly 6% of all households in North America currently have a Kodi device configured to access unlicensed files and streams” [6]. This implies that many IPTV users are willing to risk compromising their home network by installing potentially infected software to access unlicensed video content in addition to possible legal action for copyright infringement.

One of the reasons why infringing IPTV users are willing to risk legal action or exposure to malware and scams is that illegal IPTV services are usually either free or have low monetary costs in comparison to legal IPTV services [7]. Additionally, applications and various software for accessing infringing content can be installed from unofficial software and application stores on physical set-top boxes, which appeals to users due to its ease of use, facilitating a “wide range of illicit content being available in one place, without the need for multiple subscriptions” [8]. Because of the lower perceived costs, these users are willing to accept the risks of trusting and potentially disclosing credit card or personal information to illicit content providers who cannot be trusted and who could be frauds.

The addition of the malware threat to this criminal environment adds another dimension to criminal activities, creating a poly-criminal environment. This was observed in the technical report on the online investigation of IP crime [9], which found that in many cases, the financial gain in one criminal activity supports the other, thus creating a vicious many-folded criminal ecosystem. Another importance in illuminating the malware ecosystem behind illegal IPTV is that it will challenge the judicial process behind the illegal IPTV ecosystem by stressing the fact that the severity of crime increases once the malware is added into the mix.

2. Illegal IPTV Technologies

Illegal IPTV technologies consist of physical set-top boxes, websites, or software in the form of standalone applications or illicit add-ons to legal software [7]. Supplying these technologies for use without paying for the content they transmit is a crime. One study identified trojan, adware, spyware, and backdoor malware from content theft websites [10], implying that illicit IPTV providers may include malware in their websites and software or advertise malware disguised as a desirable application to increase their profits. Thus, as illicit IPTV providers are already committing a crime, it appears that, in addition, many of these providers elect to distribute malware as part of the delivery to supplement their income. The following sections will define the

illegal IPTV technologies used and their risks in addition to outlining relevant malware collection and analysis techniques for these technologies.

Illicit Streaming Devices (ISDs) are physical boxes or USB sticks that connect to a TV to provide free television and film content that you would usually pay to view [8]. Many physical IPTV boxes, such as Kodi boxes, are legal, but third-party software can be installed to illegally stream IPTV content for free. Conversely, other physical IPTV boxes, often described as “fully loaded” or “jailbroken”, already include software for facilitating illegal IPTV streaming. Because ISD providers are already willing to commit copyright infringement, they are more likely to commit further breaches of law, as it could increase their profits. Therefore, ISD providers cannot be trusted, as they could supply users with ISDs infected with malware.

Overall, ISD providers are unlikely to infect the products they sell with high-impact malware when they are already making a profit from selling ISDs. However, potential users would likely purchase an ISD from a website, which itself could be a scam designed to try and get individuals to disclose their credit card details. Moreover, fake websites that advertise illegal IPTV boxes could also distribute fileless malware when visited by users. Therefore, there are other risks to purchasing and using ISDs, as the providers cannot be trusted and could be attempting to scam people.

Websites for streaming IPTV content illegally are available over the surface web, with examples including PutLocker and FlixTor. IPTV content is usually freely available on these websites, which is attractive to users who are not willing to pay for a streaming service or risk purchasing an ISD. However, as the illicit content provided is often free, IPTV websites are untrustworthy, as they are more likely to rely on trackers, scams, and malware to gain a profitable income.

Illegal IPTV websites have different strategies for providing infringing IPTV content. Many sites host and potentially live-stream IPTV content on their website, although these websites are more likely to be detected by anti-piracy organisations. To reduce the risk of legal action, some websites collect and contain lists of hyperlinks to websites for accessing IPTV content illegally, known as “link aggregators” [9]. Link aggregators can also be found on legitimate websites, such as GitHub repositories and forum posts.

Once more, using illegal IPTV websites or aggregators is risky, as they cannot be trusted. In comparison to ISDs, IPTV websites are potentially riskier because they receive no income for providing free IPTV content, whereas ISDs are purchased. Hence, IPTV websites rely on intrusive advertising and malware to gain a profit, with adverts often redirecting users to malicious or scam websites when clicked on [7]. This is known as malvertising (malicious advertising), which distributes malware by injecting online advertisements with malicious code [11]. Cybersecurity company RiskIQ found that 1 in 3 content theft websites expose visitors to malware, with hackers paying the providers USD 70 million to add malware to their websites [1]. This implies there is a significant chance of users obtaining infected with high-severity malware, especially if hackers are willing to pay a total of USD 70 million.

Malware can be distributed to users of illegal IPTV websites when users download video files for watching IPTV content, such as MP4 files. When an infected file is opened, the malware will execute on the user’s device, which could be anything from ransomware to a remote access trojan (RAT). Although users may not realise the risks of downloading files from an untrustworthy source, technically proficient users will be aware of the risks and are likely to mitigate the risk of infecting their devices by using an antivirus that scans files or a virtual machine (VM).

However, this is not the only risk of using IPTV websites. Another risk is fileless malware. Fileless malware does not require a user to download a malicious file; rather, it exploits vulnerable applications on a victim’s device to enable the injection of malicious code into its main memory [12]. Fileless malware is a high risk to users, as it is unlikely to be detected by antivirus signatures and could potentially infect a user as soon as they visit a website [13].

One study analysed the malicious codes in embedded PDFs. Moreover, malicious codes embedded into the PDF files present a prevalent way of infecting the main memory and using malicious JavaScript codes [14]. There are several recent data-dependent malicious URL identification and classification studies in the literature based on machine learning, deep learning, or an ensemble of classification algorithms [15][16][17][18][19][20].

Furthermore, many threat intelligence platforms, such as VirusTotal and AlienVault Open Threat Exchange (OTX), do not recognise these sites as malicious. To illustrate, researchers scanned 1555 illicit IPTV websites and aggregators gained from an IPTV GitHub repository in VirusTotal. Of these websites, only 34 were identified as malicious or had an association with malware for both VirusTotal and AlienVault OTX even though many of these websites contained intrusive advertisements attempting to scam users into downloading potentially unwanted programs (PUPs) that may have been malicious.

Infringing IPTV (Pro v7.0.6) software includes standalone desktop and mobile phone applications in addition to add-ons or plugins for legitimate IPTV software, such as Kodi. Using standalone applications to access IPTV content illegally often requires paid subscriptions. A study found that a business, SET TV, offered infringing IPTV content to over 180,000 users with

a USD 20 monthly or USD 200 annual subscription via a standalone software application [7]. Again, it is less likely that providers will infect IPTV applications with malware if they are already making a profit. In comparison to using websites for IPTV, there is more incentive for IPTV website providers to include malware, as the content provided is usually free. However, downloading and executing an application infected with malware could have a greater impact if users do not have antivirus software installed.

While studies suggest that standalone infringing IPTV applications have a considerable number of users, another study found that 26 million Kodi users (68% of the total user base) were pirating illegal IPTV content using Kodi (20.2) software add-ons [21]. Although these add-ons are often downloaded from likely benign GitHub repositories, the Digital Citizens Alliance found that third-party Kodi add-ons were used to distribute cryptocurrency-mining malware [2]. Similarly, Warrior et al. found that 1.4% of Kodi add-ons resolved to domain IP addresses found on malicious blacklists (131 out of 9146 add-ons studied) [22]. This implies that add-ons facilitating the streaming of illicit IPTV content are more widely used than standalone applications and may be more likely to be infected with malware.

References

1. Digital Citizens Alliance. How Digital Platforms Are Being Overrun by Bad Actors and How the Internet Community Can Beat Them at Their Own Game. 2017. Available online: https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Trouble-in-Our%20Digital-Midst%20Report-June-2017.pdf (accessed on 25 August 2023).
2. Digital Citizens Alliance. Fishing in the Piracy Stream: How Dark Web of Entertainment Is Consumers to Harm. 2019. Available online: https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf (accessed on 25 August 2023).
3. Hsiao, L.; Ayers, H. The Price of Free Illegal Live Streaming Services. arXiv 2019, arXiv:1901.00579.
4. Watters, P. A Systematic Approach to Measuring Advertising Transparency Online: An Australian Case Study. SSRN Electron. J. 2013.
5. Simpson, W.; Greenfield, H. What Is Internet Protocol, and Why Use It for Video? In IPTV and Internet Video; Elsevier: Amsterdam, The Netherlands, 2009; pp. 1–14.
6. Sandvine Subscription Television Piracy Sandvine Global Internet Phenomena Spotlight. Case Study 2 Global Internet Phenomena Spotlight. 2017. Available online: https://www.sandvine.com/hubfs/downloads/reports/internet-phenomena/sandvine-spotlight-subscription-television-piracy.pdf (accessed on 25 August 2023).
7. Pandey, P.; Aliapoulios, M.; McCoy, D. Iniquitous Cord-Cutting: An Analysis of Infringing IPTV Services. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, 17–19 June 2019; pp. 423–432.
8. Intellectual Property Office. UK Government Response to the Call for Views Regarding Illicit IPTV Streaming Devices. 2018. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/750177/Gov-Response-call-for-views-Illicit-IPTV.pdf (accessed on 25 August 2023).
9. EUIPO. Illegal Iptv in the European Union. 2019. Available online: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Illegal_IPTV_in_the_European_Union/2019_Illegal_IP (accessed on 25 August 2023).
10. EUIPO. Identification and Analysis of Malware on Selected Suspected Copyright-Infringing Websites. 2018. Available online: https://euipo.europa.eu/knowledge/course/view.php?id=3395 (accessed on 25 August 2023).
11. Xing, X.; Meng, W.; Lee, B.; Weinsberg, U.; Sheth, A.; Perdisci, R.; Lee, W. Understanding Malvertising Through Ad-Injecting Browser Extensions. In Proceedings of the 24th International Conference on World Wide Web, International World Wide Web Conferences Steering Committee, Geneva, Switzerland, 18 May 2015; pp. 1286–1295.
12. Sudhakar; Kumar, S. An Emerging Threat Fileless Malware: A Survey and Research Challenges. Cybersecurity 2020, 3, 1.

13. Sanjay, B.N.; Rakshith, D.C.; Akash, R.B.; Hegde, V.V. An Approach to Detect Fileless Malware and Defend Its Evasive Mechanisms. In Proceedings of the 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), Bengaluru, India, 20–22 December 2018; pp. 234–239.
14. Dabral, S.; Agarwal, A.; Mahajan, M.; Kumar, S. Malicious PDF Files Detection Using Structural and Javascript Based Features. In Proceedings of the Communications in Computer and Information Science, New Delhi, India, 13 May 2017; Springer: Singapore, 2017; Volume 750, pp. 137–147.
15. Aljabri, M.; Altamimi, H.S.; Albelali, S.A.; Al-Harbi, M.; Alhuraib, H.T.; Alotaibi, N.K.; Alahmadi, A.A.; AlHaidari, F.; Mohammad, R.M.A.; Salah, K. Detecting Malicious URLs Using Machine Learning Techniques: Review and Research Directions. IEEE Access 2022, 10, 121395–121417.
16. Abad, S.; Gholamy, H.; Aslani, M. Classification of Malicious URLs Using Machine Learning. Sensors 2023, 23, 7760.
17. Mahesh; Ananth; Dheepthi. Using Machine Learning to Detect and Classify URLs: A Phishing Detection Approach. In Proceedings of the 2023 4th International Conference on Electronics and Sustainable Communication Systems, ICESC 2023—Proceedings, Coimbatore, India, 6–8 June 2023; pp. 1285–1291.
18. Difaizi, T.Z.; Camille, O.P.-W.L.; Benhura, T.C.; Gupta, G. URL Based Malicious Activity Detection Using Machine Learning. In Proceedings of the 2023 International Conference on Disruptive Technologies (ICDT), Greater Noida, India, 11–12 May2023; pp. 414–418.
19. Ghaleb, F.A.; Alsaedi, M.; Saeed, F.; Ahmad, J.; Alasli, M. Cyber Threat Intelligence-Based Malicious URL Detection Model Using Ensemble Learning. Sensors 2022, 22, 3373.
20. Rafsanjani, A.S.; Kamaruddin, N.B.; Rusli, H.M.; Dabbagh, M. QsecR: Secure QR Code Scanner According to a Novel Malicious URL Detection Framework. IEEE Access 2023, 11, 92523–92539.
21. Sheppard, J. Cloud Investigations of Illegal IPTV Networks. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1942–1947.
22. Warrior, M.A.; Xiao, Y.; Varvello, M.; Kuzmanovic, A. De-Kodi: Understanding the Kodi Ecosystem. In Proceedings of the Web Conference 2020, Taipei, Taiwan, 20–24 April 2020; ACM: New York, NY, USA, 2020; pp. 1171–1181.