



Behind the Tube: Exploitative Monetization of Content on YouTube

Andrew Chu, *University of Chicago*; Arjun Arunasalam, Muslum Ozgur Ozmen, and Z. Berkay Celik, *Purdue University*

<https://www.usenix.org/conference/usenixsecurity22/presentation/chu>

This paper is included in the Proceedings of the 31st USENIX Security Symposium.

August 10–12, 2022 • Boston, MA, USA

978-1-939133-31-1

Open access to the Proceedings of the 31st USENIX Security Symposium is sponsored by USENIX.

Behind the Tube: Exploitative Monetization of Content on YouTube

Andrew Chu^{†*}, Arjun Arunasalam^{‡*}, Muslum Ozgur Ozmen[‡], and Z. Berkay Celik[‡]

[†] *University of Chicago, andrewcchu@uchicago.edu*

[‡] *Purdue University, {aarunasa, mozman, zcelik}@purdue.edu*

Abstract

The YouTube video sharing platform is a prominent online presence that delivers various genres of content to society today. As the viewership and userbase of the platform grow, both individual users and larger companies have recognized the potential for monetizing this content. While content monetization is a native capability of the YouTube service, a number of requirements are enforced on the platform to prevent its abuse. Yet, methods to circumvent these requirements exist; many of which are potentially harmful to viewers and other users. In this paper, we present the first comprehensive study on exploitative monetization of content on YouTube. To do this, we first create two datasets; one using thousands of user posts from eleven forums whose users discuss monetization on YouTube, and one using listing data from five active sites that facilitate the purchase and sale of YouTube accounts. We then perform both manual and automated analysis to develop a view of illicit monetization exploits used on YouTube by both individual users and larger channel collectives. We discover six distinct exploits used to execute illicit content monetization on YouTube; four used by individual users, and two used by channel collectives. Further, we identify real-world evidence of each exploit on YouTube message board communities and provide insight into how each is executed. Through this, we present a comprehensive view of illicit monetization exploits on the YouTube platform that can motivate future investigation into mitigating these harmful endeavors.

1 Introduction

YouTube is the world's largest video sharing platform, exceeding one billion hours of daily viewership [82]. Videos are willingly uploaded by users, who may then be rewarded through profit made via content monetization. The landscape of content creation and monetization on the YouTube platform has gone through several changes since the video host-

ing site's founding in 2005 [68]. Despite various changes to YouTube's monetization policy, content creation on the platform has remained highly profitable (e.g., *T-Series*, the most popular channel measured in YouTube subscribers nets at least \$8.5 million USD in estimated yearly income [54]). While originally allowing monetization through Participatory Video Ads (PVA) and Brand Channels, YouTube pivoted to more advanced methods that algorithmically evaluate content to determine creator payout [73, 74, 77].

With these changes, two groups of content monetization emerged: individual users and channel collectives. Individual users, known as content creators, comprise the majority userbase of YouTube, wherein any registered individual may upload content to the website that later may be monetized based on popularity. Channel collectives, more commonly known as Multi-Channel Networks or MCNs, are larger aggregates of multiple individual users that support all collective members; providing content tools in areas such as audience development, content programming, and advertisement integration [70]. Though the majority of content creators and content uploaded to YouTube abide by stated monetization policies and requirements [66, 76], a notable quantity of content violation and monetization requirement evasion techniques have been developed by either group and remain unaddressed on the YouTube platform today.

Previous technical community efforts have recently explored methods of creating deceptive content for specific demographics (i.e., children and kids [36]) as well as in-content URLs directing viewers to malicious websites [7]. However, research that examines (1) the underlying communities supporting illicit content monetization on YouTube and (2) adjacent mechanisms supporting these endeavors (e.g., account marketplaces, software) is at this time largely absent.

In this paper, we present a comprehensive review of unstudied, popular exploits used by malicious creators and MCNs to execute illicit content monetization. To accomplish this, we analyze online communities and forums that actively discuss monetization on YouTube, and filter the discussions to identify conversations between malicious creators describing their

*First authors Chu and Arunasalam have made equal contributions to this work. Work completed while Andrew Chu was at Purdue University.

methods. We also examine a number of online account marketplaces that operate with the direct purpose of facilitating the purchase/sale of YouTube accounts and analyze the attributes of active listings. Lastly, we study a number of browser-based and local software tools used to evade copyright detection and generate artificial video engagement (e.g., views, subscribers, likes, comments). From these data, we create two datasets of contextual forum comments/exchange, and marketplace listing characteristics. We perform codebook analysis on our dataset of forum comments and discover six exploits implemented by both content creators and MCNs: (1) illicit commerce of YouTube accounts, (2) artificial channel engagement, (3) in-content deception, (4) content theft, (5) withholding affiliate payment, and (6) MCN content theft. We discover these exploits have potential to both directly and indirectly harm YouTube viewers, content creators, and third-parties. Viewers are harmed via phishing and exposure to illicit or harmful content. Creators experience unfair competition and content theft, both of which harm their ability to generate revenue in the YouTube ecosystem. Third-parties that produce video content outside YouTube (i.e., movies, TV shows) become victims of piracy. Analysis of our forum comments also shed light on the abuse of software tools to perpetrate these exploits. Our findings motivate future work into user interactions and content moderation in YouTube monetization communities, and how to prevent malicious creators and MCNs from harming others on the video-sharing platform. In this work, we make the following contributions:

- We present the first study of illicit monetization operation through analyzing a wide variety of global online YouTube commerce communities complicit in supporting this operation and its economics.
- We identify and characterize six illicit content monetization exploits that harm viewers, content uploaders, and third-parties by studying discussion between exploit perpetrators and victims.
- We conduct a large-scale analysis of prohibited YouTube account listings, monetization related services, and evasion-motivated software to provide insight into how illicit content monetization exploits can be mitigated.

2 Monetization in the YouTube Ecosystem

We provide a background of the YouTube environment by defining a hierarchy of interactions between viewers and the two entities, content creators and multi-channel networks. Further, we discuss copyright and ownership on YouTube, a key matter in monetizing uploaded content at scale.

Content Creators. The term *content creator* (shortened as *creator*) describes a user who contributes media content to the YouTube platform. Creators on YouTube comprise the largest user-base of any video-sharing website, with over 44

million global users at the time of this research [46]. Creator *channels* upload created content, which falls in nine distinct categories (music, comedy, film & entertainment, gaming, beauty & fashion, sports, tech, cooking & health, and news & politics) [65]. Content 15 minutes or less in length can be uploaded to YouTube by any user with a Google account [35]. The duration can be extended to 12 hours or 128 gigabytes in file size with user verification [17]. Uploaded content must adhere to community guidelines defined by YouTube that outline policies on spam & deceptive practices, sensitive content, violent or dangerous content, and regulated goods [66]. Increasingly, content creators aim to monetize their content via various methods (e.g., advertising, partnerships) that allow content creation to be a potentially profitable process.

Multi-Channel Networks. Third-party companies called *Multi-Channel Networks* (MCNs) are external channel collectives that content creators may join to promote content monetization [70]. MCNs have become an integral part of the YouTube ecosystem, with some MCNs working with a large number of creators. For instance, Machinima is a large MCN that manages over 30,000 creators [34]. A content creator who joins an MCN is referred to as an *affiliate* creator. In exchange for a portion of the revenue generated by an affiliate creator's content, MCNs offer tools and services to guide creators in areas such as audience development, content programming, and creator collaboration. Some MCNs also provide affiliate creators with additional benefits such as copyright protection via YouTube's Content ID system. An affiliate partnership is offered by MCNs to content creators and typically cannot be started by the creator themselves (e.g., creator contacting the MCN). If an MCN finds a creator profitable, formal affiliation is set through legally binding contracts.

Copyright and Ownership. Because content uploaded to YouTube is able to generate revenue, YouTube established a copyright policy which prevents unauthorized content use or reupload. Specifically, this protects the original owners of uploaded content. Copyright policy on YouTube is enforced using *Content ID*, a system where videos are tagged as original and added to a corpus of copyrighted media [13]. All future videos uploaded to YouTube are cross-referenced against this database and are flagged upon a positive match, automating the process of detecting copyright violations and preventing others from profiting from the content of others.

Consider a music video uploaded by a musician to promote an upcoming album. Initially, they do not apply for Content ID and find a reupload of their video on a channel with more subscribers, drawing views and monetization away from their original video. The musician applies and is approved for Content ID on their video, adding their content to YouTube's database of copyrighted content. Concluding this process, the reupload is removed from YouTube, allowing the musician to receive all monetization from their original content.

Though use and approval from the Content ID system is available to individual creators, streamlined interaction with

the system often is more easily achieved via larger MCNs or business entities who may be able to more easily demonstrate alignment with YouTube's Content ID criteria [12]. For this reason, many content creators choose to affiliate with MCNs - hoping to establish stronger ownership of uploaded media.

2.1 Generating Revenue

Content monetization is the primary incentive offered by YouTube to encourage users to upload media. In the final fiscal quarter of 2019, content ads generated \$15-billion USD or 9.4% of Google's annual revenue generated for the year [69]. As a portion of this revenue is distributed to content creators, YouTube sees continuous growth of users working to become eligible for content monetization. This popularity has led YouTube to institute and revise monetization requirements for creator uploaded content. We discuss these requirements and mechanisms of monetization payout below.

2.1.1 Eligibility

Eligibility for content monetization on YouTube has evolved several times. Original conditions of monetization (i.e., prior to 2018) required that a channel obtains 10,000 lifetime views before receiving any advertising payout [71]. This method contained several flaws. While reasonable for the beginning stages of YouTube's growth, this approach was not scalable and was easily exploited by content creators. Users quickly created various paid, grey-market tools to automate and bypass the viewer threshold [8, 32, 47]. Further, companies paying to use YouTube as a means of advertising could not ensure their products were promoted to broader audiences. For instance, a video on a large channel with many viewers could equally likely show an advertisement as a video from a channel with little to no following. To address these issues, YouTube implemented new monetization standards in January 2018 that require channel videos have annual views amounting to 4,000 hours and 1,000 subscribers (dedicated viewers who choose to view more of the content [49]) before a creator can monetize their content. These standards addressed advertiser concerns of ad delivery to viewers by ensuring monetized channels have a uniform minimum audience [72]. However, we show in Section 4 that these standards harm beginner content uploaders and continue to be exploited by underground communities.

2.1.2 Mechanisms of Monetization & Payout

Mechanisms to monetize content on YouTube stem from ad revenue, specifically in three categories: native advertising, external sponsors, and MCN integration.

Native Advertising. Native advertising describes advertising services offered by YouTube itself, specifically the YouTube Premium and Google AdSense services [75].

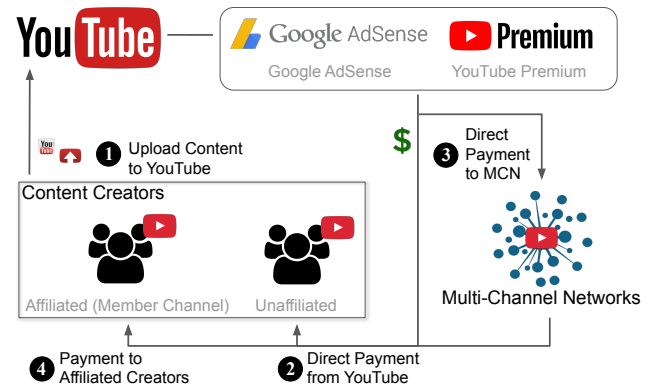


Figure 1: Overview of monetization payout on YouTube.

YouTube Premium provides a creator with revenue gained from viewers subscribed to the YouTube Premium service. Google AdSense provides a creator payout using "Cost Per Mille" (CPM), a fixed rate given for every 1,000 video views [67]. Both services provide creators with a simple means of monetizing their content but prevent several potential drawbacks for creators. The YouTube Premium service currently maintains less than 20-million active subscribers—not large enough to provide creators with notable income [78]. In Google AdSense advertising, YouTube deducts 45% of a creator's CPM rate as a service fee before payout, limiting income generated by uploaded content [3].

External Sponsors. External sponsors describe monetization stemming from indirect, supporting sources. Revenue is created from "paid promotions"—sponsored media content that endorses targeted products or services (e.g., fitness and electronics reviews) paid for by a third-party company. YouTube requires creators of external sponsor videos to disclose the nature and source of the promoted product to their viewers and specify related video metadata and media tags [79]. Payout and reimbursement from external sponsors vary broadly, often based on the sponsoring company. Smaller companies frequently compensate content creators for their promotion by allowing them to keep the reviewed product after any sponsorship duration has ended. Larger companies may structure the reimbursement of content creators contractually or on a more formal basis, similar to business transactions for conventional advertising in other mediums [14].

MCN Integration. MCNs provide creators an indirect mechanism of monetization. Affiliated channels leverage MCN tools to target specific demographics more effectively and collaborate with other affiliated creators. This process is designed to create wider viewership, gain additional subscribers, and generate more native advertising revenue/external sponsorship opportunities. MCN integration also introduces a different flow of payment for affiliated creators, one that differs from creators not tied to an MCN. The efficacy of MCNs varies largely with the level of observed community trust and

reputation. Large MCNs (e.g., AfreecaTV, Rooster Teeth Productions, ProSiebenSat.1 Media SE) may be similar to mass media and entertainment conglomerates or subsidiaries in audience reach, and manage extensive quantities of popular channels. Small, medium or lesser-known MCNs (e.g., Freedom!, ScaleLab, Talentsy) may encompass more niche collectives of content genres/creators. In the agreements between the MCN and creator, content revenue distribution is established, typically no greater than 20% for the MCN [27].

Payment Flow. Figure 1 presents an overview of how unaffiliated (native advertising) and affiliated (MCN partnered) creators receive compensation in the YouTube ecosystem. To begin, both unaffiliated and affiliated creators upload content to YouTube (❶). While unaffiliated creators receive direct payment from YouTube (❷), payment for affiliated creators is first given to their MCN (❸) before being distributed based on established contracts (❹).

3 Data Collection

Monetization is a major incentive for uploading content to YouTube, and ad revenue for this process grows every year [69, 80]. As such, we study approaches for monetization on YouTube and answer the following research questions:

- (1) What are the illicit exploits commonly used by content creators and MCNs to monetize content?
- (2) What tools/facilities are used to perpetrate such exploits?
- (3) How do these exploits harm viewers, other content creators, or third-parties?

To answer these questions, we collect and analyze data to identify illicit exploits. Figure 2 presents an overview of our identification process. We first use a simple query crawler to identify monetization-related posts and threads on online discussion boards (❶, ❷). We crawl these posts, obtain user content (e.g., comments, file uploads, embedded URLs, software tools) and apply a codebook to extract six exploits (❸-❺). Through our analysis, we additionally identify five websites used to purchase and sell YouTube accounts and build a separate crawler to extract data from these marketplaces, as well as analyze the services they offer (❻, ❼).

Ethical Considerations. The data we analyze in this work can be placed in three categories: online communications, marketplace listings, and software. Online communication data we collect contains only non-identifiable information. We examined only the text and context of messages posted by users in forum threads. We did not compile user account metrics (e.g., username, location, quantity of posts, age) that may reveal a user’s identity. Marketplace data similarly contains only metadata of public purchasable account or service listings on websites (e.g., price, subscriber count, channel genre) that cannot uniquely identify any individual. Finally, the software we examined was found through standard search terms on public online communities.

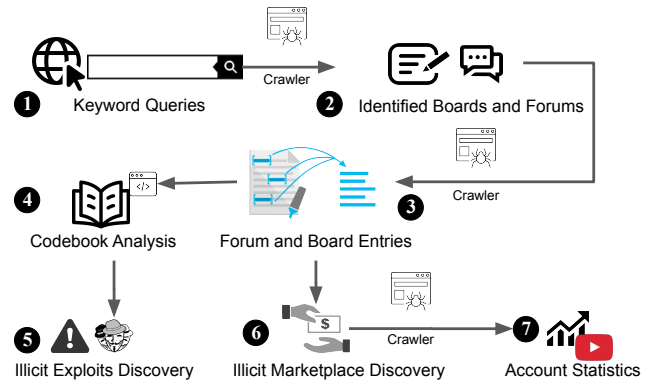


Figure 2: Procedure identifying illicit YouTube monetization discussion, services and software, and eventual exploits.

While listings and forum posts are public, we took several steps to preserve privacy in our data collection process and reduce (but not eliminate) re-identification risks. We do not make our full account marketplace/forum data public, and present only a portion of the data. For quoted forum posts, we provide only relevant fragments from original quotes. Further, we ensure quotes do not link to any YouTube video/channel.

Constructing Datasets. To understand the illicit behavior of both content creators and MCNs, we construct two datasets to analyze YouTube monetization-relevant content online; the first containing discussion board data and the second containing online marketplace data. Our dataset of discussion board data captures current creator discussion about illicit exploits and how they may be implemented. Our dataset of online marketplace data captures active online buy/sell marketplaces of services that exploit the YouTube platform. Additionally, we identify software tools used to perpetrate illicit behaviour.

3.1 Discussion Board Data

The discussion board dataset is composed of comments and posts from 11 different forums, shown in Table 1. To holistically survey the landscape of illicit YouTube monetization, we collected data from the most popular online communities from ten different countries that cover each global region. We considered only sites publicly accessible (e.g., easily found via web search) and did not require registration or prior site activity to view information. We believe this restriction is both appropriate and acceptable as it provides an accurate view of the conventional discussion of the YouTube ecosystem.

We collected data from these discussion boards with two Python web crawlers using the Scrapy web-crawling framework [43] and Zyte cloud crawling platform [87]. The first crawler (Crawler A) collects forum URLs resulting from relevant keyword searches on the Google Search API. Our second crawler (Crawler B) gathers data (user-posted text, related contextual information [e.g., screenshots, links], uploaded executables/files) from the YouTube forum/message board

Table 1: Analyzed forums and discussion boards.

# - Country	Website Name	Provided Site Description	Members	Ranking
Reddit Boards				
1 USA	Reddit /r/youtube [42]	"Discussion of YouTube as a platform - its announcements, features, bugs, and design"	471,005	805*
2 USA	Reddit /r/NewTubers [40]	"Allow[s] up-and-coming creators to improve through critiques, feedback, and cooperation among thousands of peers"	173,519	2,066*
3 USA	Reddit /r/PartneredYouTube [41]	"[Allows] creators to ask and share advice for growing their YouTube channels"	22,710	11,966*
English Forums				
4 USA	TubeBuddy [55]	"Our Mission is to make you and the rest of the YouTube Community a happier and more productive bunch"	35,362	7,183 [†]
5 USA	YTtalk [84]	"Talk about video editing, youtube gossip, branding, promotion strategies, video projects and much more!"	103,955	135,172 [†]
International Forums				
6 Mexico	ForoBeta [18]	"ForoBeta is the largest forum in Spanish for Webmasters, with discussions about SEO, bloggers, facebook among others."***	110,624	97,089 [†]
7 Brazil	Adrenaline [2]	"Adrenaline Forum - One of the largest and most active forums in Brazil"***	328,688	30,607 [†]
8 Vietnam	Dien dan Hoc Vien Youtube [28]	"Welcome to the Vietnam Youtube Academy forum"***	236,000	3,411,396 [†]
9 Cyprus	SearchEngines.guru [44]	"SearchEngines.guru is a website allowing users to discuss issues related to creating and promoting websites on the Internet."***	21,687	109,259 [†]
10 Russia	PR-CY [37]	"Self-service website promotion - Online tools for webmasters, optimizers and copywriters."***	24,630	14,420 [†]
11 Turkey	YTPara [83]	"Youtube & Webmaster Support Forum"***	79,850	39,913 [†]

* Ranking at time of writing based on number of Reddit subscribers, compared to all subreddits [39]. [†] Alexa Rank at time of writing [5]. ** Description translated to English from original language via Google Translate [25].

URLs collected by Crawler A, and discards all URLs after use. We began our investigation of illicit content monetization and data collection in December 2020 and stopped collection in May 2021. In this time frame we ran Crawler A twice, and Crawler B periodically at multiple intervals, resulting in total runtime of ≈ 101 hours. Specifically, we ran Crawler B at the middle of each month, to collect any new content posted by forum users. In our first run of Crawler A, we collected a preliminary set of forum URLs. Here, we purposefully used broad keywords (e.g., "monetization fraud", "mcn copyright") to form a starting basis of discussion for analysis.

We next executed Crawler B multiple times and gathered data from the YouTube forum/message board URLs collected by the first crawler. We examined the collected data and developed more exploit-specific keywords (e.g., "youtube link farming", "youtube movie piracy") for use in a second run of Crawler A. While we initially attempted using NLP techniques to extract keywords, we determined that such methods were impractical and insufficient in accurately capturing exploit-specific phrases. We thus used manual analysis.

We then ran Crawler A a second time using our manually generated exploit-specific keywords to collect a new set of YouTube discussion forum URLs. To complete the discussion board data collection process, we inputted the URLs resulting from this second Crawler A execution once more to Crawler B, and collected these sites' content through multiple runs. From this, we obtained 8,481 unique posts, all discussing monetization on YouTube. We then analyzed these websites by sorting them into three groups:

Reddit Boards- Multiple communities or *subreddits* that facilitate YouTube related dialogue exist on the discussion and news aggregation platform. Of these subreddits, we looked specifically at /r/youtube, /r/NewTubers, and /r/PartneredYouTube. Collectively, these three communities have over 665,000 members and facilitate user conversation about a wide variety of YouTube creator processes.

English Forums- Several forums explicitly dedicated to discussing the YouTube ecosystem exist online. We chose to analyze YTtalk and TubeBuddy, as they were the two largest

English-speaking and YouTube oriented discussion boards. These two forums host 30 distinct sub-forums dedicated to content creation, 18 of which discuss YouTube content.






International Forums- To extensively evaluate the YouTube ecosystem, we analyzed forums based in several additional countries (Mexico, Brazil, Vietnam, Cyprus, Russia, Turkey) in various global regions. In total, these six message boards contain 2,327,409 distinct threads (at the time of writing) discussing internet monetization mechanisms.

Our resulting findings from analyzing this data are presented in the form of six illicit content monetization exploits employed by content creators (Section 4.1) and MCNs (Section 4.2). A complete list of keywords used by both the first and second crawlers is presented in Appendix Table 1.

3.2 Account Marketplace Data

The online marketplace data consists of metadata from online marketplace listings of YouTube accounts on five different websites offering exclusively this service. We found these five websites by following user exchanges in our examined forum data that linked these marketplaces. Table 2 provides an overview of these websites (e.g., types of accounts sold, listing quantity, and ranking). To collect this data, we created an additional Python web crawler to deploy on these five websites. This crawler collects a number of YouTube channel specific attributes from each marketplace website listing (e.g., number of subscribers, channel genre, date of posting). While all sites additionally list accounts from platforms other than YouTube, we did not collect this data as it is not relevant to our study. Similar to our discussion board data collection process, our marketplace crawler collected data at the middle of each month from January 2020 to May 2021, with total runtime of ≈ 98 minutes. From this process, we collected data from 1,352 unique YouTube account listings, spanning over three years (March 2018 to May 2021). We then used this data to understand the landscape of YouTube accounts being sold—an action potentially harmful to viewers, other creators, and in violation of YouTube's policies.

Table 2: Analyzed social media account marketplaces.

# - Country	Website Name	Accounts Offered	# of Listings	Alexa Ranking*
1  Poland	SWAPD [50]	F, I, M, Tw, Tt, Y	21,637	26,915
2  Russia	Accs-Market.com [1]	F, I Tw, Y	1,118	41,546
3  Panama	Fameswap [16]	I, Tt, Y	3,112	13,162
4  Spain	Trustiu [52]	M, Y	277	74,827
5  Panama	ViralAccounts [59]	F, I, Tt, Y	—	292,047

Accounts: F := Facebook, I := Instagram, M := Misc., Tw := Twitter, Tt := TikTok, Y := YouTube.

* Alexa Ranking at time of writing

3.3 Software Tools

We discovered references to software tools used to execute exploits through our forum data. Creators recommend either using benign software to accomplish illicit monetization exploits, or provide links to, or even file uploads of tools marketed for illicit use. The software tools we found can be categorised as (1) web based tools: software accessed via a web page or internet browser extension, or (2) local software: applications that run on a creator’s own laptop or computer. We identified five web based tools and five local software commonly discussed among creators (mentioned many times across multiple threads). These tools are used to simulate channel engagement by generating fake likes, views, or subscribers, or are used to perform video editing techniques proven successful in evading YouTube copyright detection.

4 Discovering Illicit Behaviour on YouTube

After sorting our crawled data, we performed manual examination using codebook analysis. Specifically, we use thematic analysis [53] to understand and extract key takeaways from conversation surrounding illicit forms of monetization. Three authors jointly developed a codebook by manually analyzing every post collected by our crawler, generating initial codes, and reiterating until all authors achieved codebook stability. The authors met over multiple sessions to refine codes and reconcile disagreements. We do not present inter-coder agreements as the coded posts were reviewed as a group [33].

Non-English posts were translated to English before analysis using the Python library `googletrans` [24]. We then performed a manual analysis of translated content to confirm that translations were coherent. Our final codebook contains six high-level categories representing illicit content monetization exploits executed by either content creators or MCNs. These exploits harm viewers, other content creators, or third parties that produce and upload video content outside YouTube. Table 3 lists six distinct, illicit exploits we identified along with the malicious party involved and the party harmed. Broadly, these exploits fall into four categories:

- (1) Non-permitted sale of YouTube accounts and content-related services
- (2) Deceitful media content
- (3) Theft of copyrighted content
- (4) Theft of revenue

Table 3: Our six identified exploits, their perpetrators, and groups harmed.

Exploit	Malicious Party		Party Harmed		
	Creator	MCN	Viewer	Creator	Third Party
Illicit Commerce of YouTube Accounts	✓	✗	✓	✓	✗
Artificial Channel Engagement	✓	✗	✓	✓	✗
In-Content Deception	✓	✗	✓	✗	✗
Content Theft	✓	✗	✗	✓	✓
Withholding Affiliate Payment	✗	✓	✗	✓	✗
MCN Content Theft	✗	✓	✗	✓	✗

In the non-permitted sale of YouTube accounts and services, users on underground communities and marketplaces sell active YouTube accounts, inorganic views, subscribers, and comments. The sale of all such items is prohibited by YouTube’s terms of service [15] and is potentially harmful to viewers and other content creators. In deceitful media content, content creators exploit YouTube viewers and other content creators by directing them to external sites to monetize user activity or collect Personally Identifiable Information (PII). In theft of copyrighted content, both malicious creators and MCNs generate profit through illicit content created by other channels. In theft of revenue, MCNs deny their affiliates payment, thereby harming their source of income.

These exploits violate YouTube policy, infringe on the property of other creators, and present viewers unwelcome and even harmful content. Additionally, they have direct and indirect consequences that may harm YouTube viewers and other content creators. While YouTube has taken steps to address these issues, we observed recent discussion in our crawled forum data exploring exploit revisions and workarounds that persist on the platform. We detail exploits executed by malicious content creators in Section 4.1, and exploits executed by malicious MCNs in Section 4.2.

4.1 Malicious Content Creators

In this section, we discuss our findings regarding illicit exploits as facilitated by individual content creators on the YouTube platform. We present a motivating scenario to provide a high-level overview of how our described illicit exploits may work in tandem. We then discuss each exploit in detail, describing its functionality and impact on viewers, other creators, MCNs, and the YouTube platform.

Motivating Scenario. We consider a YouTube content creator with no previous content or experience who wants to create income via YouTube monetization quickly. To begin, the user decides that meeting YouTube’s monetization requirements is too tedious, and instead purchases a YouTube account with 3,700 subscribers and 730,000 views from the marketplace website for \$50 USD. Browsing popular videos on YouTube, the content creator observes that videos containing full-length movies and movie highlights are popular, attracting a high number of views. The content creator also realizes they can leverage viewers to promote an external website they own and earn ad revenue from.

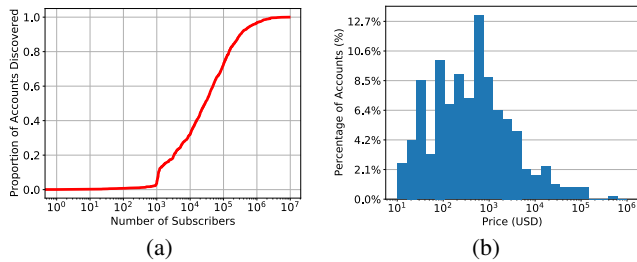


Figure 3: (a) Distribution of subscribers and (b) histogram of prices for our crawled YouTube account listings.

Next, the creator creates their first video, a short clip from a popular action film, and includes in the video content a text link to their external site. Although untrue, the creator also writes in the video description that visiting the address will allow viewers to see the full movie. The creator does not request permission from the film studio that created the movie and instead immediately uploads the video.

Lastly, to further promote their content, the content creator buys 30,000 views from a service and directs them to their upload for \$8.40 USD. The content creator continues this process for several videos of the same format (i.e., movie clips, including their external website link) and successfully gains income from YouTube monetization. In this scenario, YouTube viewers, other content creators, and third parties are harmed. Below, we explain how each of these exploits are conducted and how the mentioned parties are affected.

4.1.1 Illicit Commerce of YouTube Accounts

We discovered five websites dedicated to the illicit purchase and sale of YouTube accounts (Table 2). This exploit describes the first decision made by the user in the motivating scenario. All five websites share a similar transaction procedure. First, a user creates a listing for the YouTube account to be sold, including various information (e.g., sale price, subscriber count, monthly views, content genre). Second, other users reply to the listing with buy offers or message the selling user directly to gain more information about the account. Upon finding a paying buyer, the original poster removes the listing and provides the buyer with account credentials.

Listed Youtube Account Attributes. We examined the attributes of all account listings in our dataset to complete our profile of YouTube account sales on online marketplace platforms. To begin, we examined the distribution of channel subscribers across all account listings on our five crawled sites. Figure 3a shows the subscriber count distribution across our crawled listings on our five marketplace platforms. We found a minimum listing subscriber count of 24, a maximum of 9,220,000, and a mean of 155,785. Notably, we observe a spike in listings beginning at 1,000 subscribers, the minimum quantity required by YouTube to begin content monetization.

Supporting this quantity, such listings are frequently ac-

companied by descriptions that highlight this capability. For instance, a listing with 6,000 subscribers has the description, “No copyright or community strikes... The channel monetization criteria [is] already more than enough for monetization,” to advertise that the channel has not violated YouTube copyright or content guidelines and may quickly begin to create profit. Further, descriptions for accounts in our data similarly emphasize the origin of their views and subscribers. For example, a listing with 17,600 subscribers states “The subscribers are all organic... not bottled, not scam.” Yet, we find there is no way to verify claims of “organic” viewers or subscribers.

We found 239 unique genre categories in our crawled data, with 488 listings in the most popular genre of “Gaming & Entertainment”. This aligns with conventional statistics of YouTube viewership, with “Gaming” and “Entertainment” combined accounting for 41% of total YouTube video content globally [60]. Figure 3b presents a histogram of prices for account listings. Pricing structures across our five studied marketplace sites varied in regard to providing a static price or only a “best offer” format. Across original poster static prices and prospective buyer best offers, we found a minimum listing price of \$10 USD, a maximum listing price of \$512,925 USD, and mean listing price of \$5,405 USD.

The minimum priced account listing uploaded videos in genre “Movies & Music,” had 226,462 total views, and maintained 3,840 subscribers; above YouTube’s threshold for monetization. Examining channel screenshots attached to the listing, we observe a spike in views beginning in August 2018 and ending in December 2019, with less than ten monthly views from January 2020 to the present. We posit this drop in popularity supports the low listing price. The maximum-priced account listing also uploaded videos in genre “Movies & Music,” had 102,143,576 total views, and maintained over 124,000 subscribers. Channel screenshots attached to the listing show a consistent viewership of at least 500,000 viewers per month, providing annual revenue of \$108,157.35 USD.

Viewer and Creator Harm. The commerce of YouTube accounts both directly and indirectly harms viewers on the platform. For example, a content creator previously banned by YouTube may purchase an account for \$35 USD, with 650 subscribers. This creator is not obligated to continue uploading content consistent with that of the prior creator and may upload harmful content. Viewers already subscribed to the account are directly deceived as they unknowingly view undesired content when notified of a new video.

The presence of YouTube account marketplaces may also indirectly harm other content creators on the platform. Standard users attempt to grow their channel organically, creating consumable content for viewers to enjoy and share to meet YouTube’s minimum requirements for content monetization. However, a content creator who purchases a channel from an account marketplace evades these requirements and may immediately benefit from monetizing content, harming standard users who aim to compete on the same platform.

Table 4: Websites offering artificial engagement services.

#	Website Name	Service Offered	Services	Alexa Ranking*
1	USA SubPals [48]	S, L, V	37	14,469
2	USA QQTube [38]	S, L, V	38	15,803
3	Turkey YoutubeAboneKas [64]	S, V	2	36,634
4	Panama SonukEr [47]	S, V	32	337,981

Services: S := subscribers, L := likes, V := views. * Ranking at time of writing

4.1.2 Artificial Channel Engagement

We discovered discussion on several forums related to *artificial channel engagement*, illicit methods creators use to simulate views, subscribers, likes and comments to make their channel appear more popular. Specifically, creators use these methods to circumvent YouTube’s monetization requirements (i.e., 4,000 annually viewed hours of channel videos, and 1,000 subscribers). We observed two main methods of facilitating artificial channel engagement: (1) purchasing artificial engagement services on online marketplaces and (2) software bots tailored for mimicking views, likes, and/or subscribers.

Underground Channel Engagement Marketplaces. Table 4 shows a summary of the four most frequently mentioned artificial engagement service marketplaces in our forum data. On these websites, various services are available for purchase, with pricing ranging from free to \$180 USD. We observed two primary services: view-botting and community exchange. *View-botting* describes purchasable automated services that use unique network addresses to increase view counts on YouTube videos. SubPals [48] and QQTube [38] are the two most mentioned view-botting services in our dataset. *Community exchange* describes purchasable and free services that use a network of genuine users to mutually increase account metrics. YoutubeAboneKas [64] and SonukEr [47] are the most mentioned community exchange services in our dataset.

Creators opt to use these services, hoping that artificially inflating numbers will persist on YouTube. One creator claimed that they “... [bought] views on QQTube. It took 3 months. After that time, [their] channel started having organic views.” Creators purchase these services through a simple transaction process. They first create an account, specifying the channel or video purchased services will be applied to. After selecting their desired service and paying the corresponding fee, the service effect is applied to the specified content.

Engagement Bot Software. We also observe discussion of artificial engagement bot software—both paid and open-sourced. Table 5 shows the bot software mentioned in our dataset. These software differ in their functionality (e.g., some provide creators the ability to generate views while others generate subscribers or comments) and required technical ability for use (e.g., preloaded Google Chrome extension, Python script with user provided arguments, local software with a graphical interface). For example, a user interacts with a GUI interface to provide a video-ID for the video they wish to generate views for. The user is also able to specify the number of views generated, and computing resources the software uses.

Table 5: Studied artificial channel engagement software.

#	Software Name	Engagement Type	Software Type
1	YouTube Subscribers Generator [23]	S, L, V	Chrome Extension
2	YouTube View Bot [26]	V	Chrome Extension
3	Goyral Youtube Bot [20]	C	Chrome Extension
4	Youtube-viewer [63]	V	Python Code (Github)
5	YouTube-SubBot [61]	S	Python Code (Github)
6	Youtube-video-viewer-bot [62]	V	Python Code (Pip Package)

Engagement Type: S := subscribers, L := likes, V := views, C := comments.

The application then queries this video using computer instances from various IP addresses, gathering “unique” views for this content. (See Figure 1a in Appendix for an example of a \$249 USD YouTube view bot with these features).

To contrast, another software we examined leverages participating forum members to “crowd-source” views and comments. Used via a browser extension, a user simply installs the extension, logs into a portal using their forum credentials, and inputs the link of the content they wish to gather views and comments on. Finally, we observe discussion between users that support their use in illicit content monetization. For instance, one forum creator suggested supplementing bot software with an IP proxy list, “if ... your software queries a lot on your own IP, YouTube will detect [your account] and delete it, so find a proxy list and add it to the list on the side...”.

Viewer and Creator Harm. Artificial engagement on YouTube presents several problems that concern viewers, other creators, and the YouTube platform. Consider a user who queries YouTube for a video on the top stock investment apps and first sees two results: the desired video with 20,000 true views, and a similarly titled video with 60,000 view-botted views. The user chooses the higher viewed, view-botted video, assuming it is the desired content, as it appears more popular at first glance. To illustrate, one creator justifies his/her decision to purchase views by stating “...people will more likely watch a video [that has] 20k views vs. 800.”

In the event that the view-botted video contains harmful content, the user is lured into watching this harmful video due to the high view count. At scale, such inauthentic activity may negatively impact other creators as it may draw views and revenue away from legitimate content. For YouTube, this situation may drive away both viewers and creators.

4.1.3 In-Content Deception

Malicious creators leverage uploaded content to implement in-content deception, an exploit that allows them to promote external content for monetary gain or harvest user personally identifiable information. Specifically, we observe discussions on our analyzed forums describing creators redirecting viewers from YouTube content to external websites. We found this method frequently used alongside videos containing shortened or irrelevant content to the video search query.

Deceptive External Content. Figure 4 shows an overview of how malicious creators execute in-content deception. Malicious creators deceitfully place links in either the descrip-

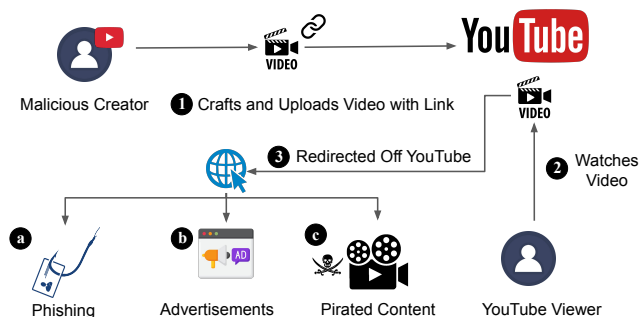


Figure 4: In-content deception used by malicious creators.

tion of their videos or in the video media itself and upload the video to YouTube (1). A benign YouTube viewer clicks on the video to watch it (2). The viewer is redirected off YouTube and to an external site via the link (3). Upon arriving at the external site, viewers encounter further “requirements” for viewing the desired content (e.g., account creation, payment/subscription, completing surveys). Viewers interacting with these websites may gain ad revenue for the creator or have their personal information collected when following any stated steps. In this way, malicious creators both monetize their content on YouTube and redirect traffic to sources where they can gain further profit through problematic methods.

To develop a better sense of the types of external content delivered to viewers, we list destination websites that malicious creators redirect viewers to. First, we observe websites that require users to provide additional financial information (a). For example, viewers are directed to click on a video description link to view a film. This link redirects them to an external website where viewers need to create an account to watch the film. Account creation is hidden behind a paywall. (An example can be found in Figure 1b in Appendix.)

Second, we observe another use case where malicious creators advertise services or other content on external websites (b). To illustrate, we find a website that viewers are redirected to via a link shown directly in video media from a channel that focuses on Movie & Music content. Accompanying the link is text promising users they will be able to watch a full length version of a specified film. However, following this link deceitfully directs a viewer to a website advertising a pay-per-click URL shortening service (See Figure 1c in Appendix for an image of this website).

Third, we found this exploit also promotes distribution of pirated content (c). Viewers are redirected to Google Drive folders containing unauthorized film uploads, or are directed to join groups to download pirated content. Appendix Figure 1d presents one such example where YouTube video content redirects viewers to a page advertising a Telegram group called *Moviez Corner Group* that promotes pirated content.

Viewer Harm. Consider a malicious content creator who maintains a popular YouTube channel that contains short movie clips eligible for monetization. The creator decides

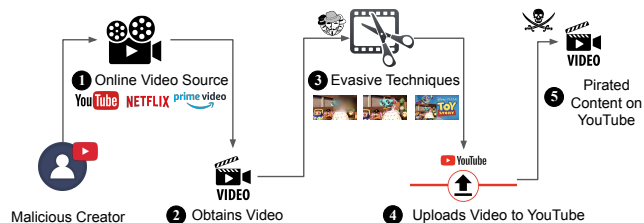


Figure 5: Content theft procedure used by malicious creators.

to leverage the popularity of their channel and promote an external website that they also own. This website entices visitors to submit a web form of PII information (i.e., phishing) to “gain access” to the website’s contents. To attract YouTube viewers, the creator uploads videos promising users a full-length version of a movie if they follow a link to the creator’s external website and fill out a short form. Upon arriving at the external site, users encounter heavy ad presence for yet another domain hosting pirated content. Here, we observe the malicious creator profiting off advertisements and promoting piracy. If a viewer is deceived into filling out the short form, their sensitive information may also be exploited.

4.1.4 Content Theft

When analyzing posts of forum users asking how they can “...upload movies to YouTube” or “...how [they can] avoid being copyright claimed by the copyright bot,” we discovered several exploits used by content creators to steal content for re-upload and personal monetization.

To begin, we observe that to evade Content ID detection and successfully monetize stolen media, malicious creators use video and audio transformation methods. Figure 5 presents an overview of how malicious creators capitalize on popular video content from other channels, popular television shows, or movies. Here, a malicious creator realizes such content is more likely to receive views, so they find and illicitly obtain/download a popular video without the original uploader’s permission (1, 2). The creator then uses evasive techniques to edit the video and re-uploads it to their own channel (3, 4). In the event their reuploaded video bypasses YouTube’s automated copyright violation detection, these creators profit on pirated content that they do not own (5). We discuss the content theft exploit steps in detail below and the different software tools used to facilitate these techniques.

Content ID Evasion Techniques. We found evidence of several evasive video editing techniques used by malicious creators to avoid detection of copyright violation. Various users propose different techniques to circumvent YouTube’s automated copyright detection [13]. For example, one user writes “...you can add frames, logos and subtitles to your video clips to make them unique with various effects, preventing account removal/suspension.” Another user claims “...you can flip a video to circumvent the copyright infringement scanner.”

Table 6: Analyzed software tools used by content creators to avoid copyright claims.

#	Software	Description	Type
1	Videonti [57]	"Make videos unique by adding frames, logos, etc."	Desktop
2	Kapwing [31]	"Edit video and create content online"	Web
3	Videoyap [58]	"Produces unique video by inserting text-to-speech audio"	Web

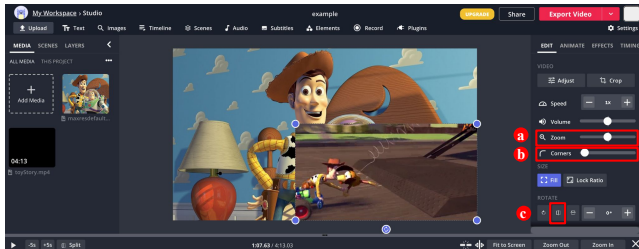


Figure 6: Embedding video into a static image using browser-based software Kapwing [31], to evade YouTube Content ID detection. Other evasive techniques marked with a red box: (a) Zooming in, (b) Adding a border, and (c) Flipping.

In total, we discovered eight video perturbation techniques creators commonly apply to successfully avoid detection of copyright violations: (1) Flipping/Mirroring, (2) Zooming, (3) Frame manipulation (static image in the background, inserting frames), (4) Adding watermarks, (5) Audio manipulation, (6) Color manipulation, (7) Adding borders/dark shadows, and (8) Blurring. To perform these techniques, creators use software to manipulate video content. To discover these software, we examine the links and images in the crawled threads, and check if they include reference to any relevant programs.

Table 6 shows an overview of the software found in our analysis. One such example is video editing software Kapwing [31], a browser-based tool allowing creators to use these techniques. Figure 6 shows the layout of the Kapwing software as well as its ability to embed a video into a static image (*frame manipulation*). Using Kapwing, we generate content that employs techniques (1), (2), (3), (7), and (8), as seen in Figure 7. Kapwing’s capability of performing these evasive techniques highlights the ease at which creators are able to evade detection of copyright violation. While Kapwing is marketed for benign and non-illicit use, we discovered software specifically catered to malicious creators evading YouTube copyright detection. For example, the software Videonti is marketed by its creator as “...able to make content unique” by providing an example of embedding an animated film in a static image (See Figure 1e in Appendix to view images found on the homepage of the Videonti software).

Further discussion in our data provides clear evidence of its use in content theft, with additional posts, screenshots, and videos demonstrating successful use of the tool. For instance, one forum user writes “...I used this software to upload a clip from the movie ‘Avengers.’ it has been uploaded now for five days and youtube has taken no action against my account.”

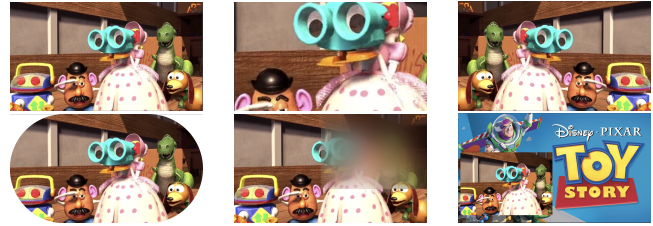


Figure 7: Techniques to avoid detection of copyright violations: From top left to bottom right; unedited video, zooming in, mirroring, adding a border, blurring a corner, adding a frame.

Creator and Third-Party Harm. When analyzing our dataset, we find creators voice their frustration on how content theft harms their channel. By having their own content stolen and re-uploaded, creators lose out on the monetization that should be rightfully theirs. This negatively affects their income and channel growth. A benign creator notes “Some [user] nicked my video just after hours of uploading. When confronted, he says, ‘it’s for a good cause.’ ‘His’ video has been receiving a lot of likes and views. Mine, on the other hand, received a number of dislikes, and I am not sure why.” YouTube creators are not the only ones harmed. When malicious creators upload stolen content that was not uploaded to YouTube, third parties who own said content have traffic redirected from their own websites. Finally, viewers in many cases are unknowingly watching pirated content and indirectly contributing to piracy in watching such content.

4.2 Malicious Multi-Channel Networks

In this section, we discuss our findings on illicit exploits facilitated by MCNs on the YouTube platform. We found three fraudulent reasons individual content creators join MCNs.

First, some creators join an MCN after being banned on Google AdSense, which prevents them from monetizing content. To detail, many unsuccessfully attempt to appeal their ban and join an MCN as a last resort. Because revenue from content is first distributed to the MCN, previously banned creators are able to earn income through affiliation. For example, one creator from our crawled forum data explained that they joined an MCN after being demonetized. “I partnered with [MCN] just so I could get at least some money from my channel (even if it is only 70% of my total).” While some MCNs audit creators who wish to affiliate, we found many have no process or description of account standards on their websites.

Second, we found creators discussing joining an MCN as a method of tax evasion. As MCNs receive an affiliate’s revenue before distributing it to their creators, income is not directly traceable to creators’ accounts. One creator noted that “...popular MCN payment methods such as Paypal and Skrill” help creators as they “[draw less attention] in filing taxes and audits.” Similarly, we observed creator demand in seeking MCNs that pay via cryptocurrency. For example, we found an MCN advertising to pay creators via a variety of



Figure 8: (a) MCN with cryptocurrency payout capabilities. (b) Translated homepage of Iranian MCN Andropay, highlighting their ability to help Iranian creators monetize content.

cryptocurrencies such as Bitcoin, Nollar and Nano, marketed via an online brochure, as shown in Figure 8a. Although cryptocurrency is not specifically mentioned as a means for tax evasion, we found creators asking for references to such MCNs in subforums where users discuss methods of evading taxes. For example, on one thread, a creator requests “...links to MCNs who pay through BitCoin or other Cryptocurrency.”

Third, creators from countries without access to Google AdSense may only be able to monetize their content via an MCN. This is because Google is a US company and thus, must “...comply with sanctions imposed by the United States Office of Foreign Assets Control (OFAC)” [22]. As such, AdSense is restricted in many countries designated as sensitive by the U.S. Department of State including Cuba, North Korea and Iran [45]. Creators from these countries bypass these sanctions by partnering with MCNs, allowing them to monetize their content. To illustrate, we identified an Iranian MCN named Andropay that claims that one of its main features is to help creators “...cash out YouTube channel revenue ... with the lowest possible fees”, as shown in Figure 8b. Andropay’s corporate office address, listed on both the company’s homepage and Google Maps, is located in Tehran, Iran. On inspection of the company’s homepage, we discovered Andropay alleges that their business is registered in multiple countries to facilitate services to Iranian creators while not violating sanctions.

Illicit MCN Practices. Fraudulent practices involving MCNs relate to unlawful interactions between an MCN and both affiliated and unaffiliated creators. We found that instances of fraud in these circumstances can be categorized into one of two categories: obscuring payment, and theft of creator content. In obscuring payment, we observed evidence of MCNs withholding or obscuring generated video revenue from affiliate creators, with extreme cases describing the total loss of deserved income. In theft of creator content, MCNs leverage Content ID privileges to steal unique content.

4.2.1 Withholding Affiliate Payment

We observed discussion across many forums describing MCNs withholding payment from their affiliate creators. To detail, affiliate creators first upload their content to YouTube. Revenue generated from their content is then distributed not to them, but to their associated MCN. However, creators allege MCNs withhold creators’ contracted split of the revenue. In

doing so, malicious MCNs retain the full profit earned by their affiliated creators. We analyzed discussion concerning such cases of MCNs withholding affiliate payment and highlight three key findings. MCNs:

- (1) provide deceptive and false justifications
- (2) sever communication with creators
- (3) coerce creators to maintain affiliation

Deceptive and False Justifications. In the event of withheld payment, most MCNs provide their affiliates justification as to why their contracted revenue has not been distributed. Although there is no method to verify if such justifications are actually false, our analysis uncovers many allegations across multiple forums and threads suggesting these justifications have no realistic basis. For example, we found discussion about an MCN that refused to pay their creators and instead suggested “...payments [were] denied by paypal.” We also observed conversation between creators alleging MCNs create false requirements for their affiliated users (e.g., reaching a minimum quantity of content views). Upon further examination, we also found examples where MCNs did not pay their creators even after achieving the agreed minimum requirements. For instance, one creator states “[they] had earned over \$2500 in the past 4 months, well over the claimed requirement for the MCN to send [them their] payment”, however “[they] had not been paid.” Finally, other reasons found in our data include “uploading repetitive content” and “content that damages the network.”

Severance of Communication. We also found many creators discussing the lack of communication received from their affiliated MCNs. For example, one creator in our crawled data complains “...[I’m] not in [an MCN] anymore, but [I] still don’t have [my] money. [I’ve] sent [so] much mail to their support, per email, and over the dashboard, but never received an answer.” Another creator states “...[the MCN] doesn’t even bother replying to my emails which clearly shows they have no intention of paying my earnings.”

Coerced Affiliate Relationship. In an additional circumstance, some creators who are denied payment are further unable to *unlink* themselves; the process of dissolving the MCN-to-creator affiliation. For instance, one creator from our crawled data claimed “...[the MCN] never provided me with good opportunities or helped me, and [has] just been taking my money, so I decided to leave last year. They said I could not leave until December because it was a breach of contract.” Another creator who tried obtaining a copy of their contract noted that “...the [MCN] dashboard doesn’t seem to allow [me] to get copies of them,” highlighting access to contracts is limited by MCNs. Inability to unlink results in coerced affiliation and continuous loss of revenue, with MCNs keeping almost all content monetized profit generated by creators.

Many creators are reluctant to name the MCNs they are affiliated with when making these allegations. We posit this is due to fear of legal action from their prior association with

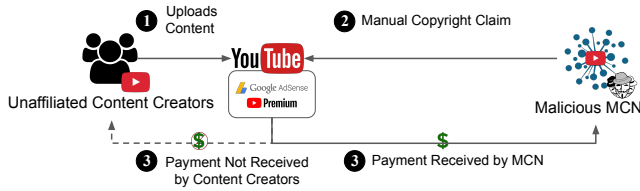


Figure 9: Overview of how malicious MCNs abuse their Content ID privileges.

an MCN. For example, one creator states they “...can’t reveal the name of their network due to potential contract troubles.”

However, we identified six MCNs that are repeatedly mentioned in the discussion surrounding this exploit¹. Upon further investigation, we observe that all six are still operational, with one resuming offered services in January 2021 after a short hiatus. Our findings indicate that MCNs are able to continue with their operations despite refusing to pay their affiliates, highlighting that public allegations and complaints are unable to negatively impact an MCN’s business ability.

Creator Harm. When MCNs withhold payment, creators are directly harmed as they are refused income generated by their original content. This, in turn, can affect their ability to create content. For instance, one creator noted that withheld payments “...affect the financial security of partners who rely on this platform and steady ongoing payments to maintain their product or channel.” Creators in these situations also cite that withheld payments have negatively impacted their quality of life, with many content creators depending on YouTube revenue as their sole source of income. For example, one creator who “...makes [his/her] living off YouTube and [has] a family” expressed frustration when experiencing withheld payments since “[they] could be going broke.”

4.2.2 MCN Content Theft

In addition to affiliated content creator harm, we found evidence of unaffiliated creators’ harm inflicted by malicious MCNs. Because Content ID privileges are typically more widely available to MCNs, we discovered that access to these privileges leads to abuse. Figure 9 presents an example Content ID abuse case. Individual content creators who upload their content to YouTube find their content to be falsely claimed by a malicious MCN (①, ②). Here, these creators do not earn revenue from their content, and in some cases have revenue stolen by the offending MCN (③).

Abuse of Copyright Claim. We observe broad discussion of MCNs leveraging their Content ID privileges to claim ownership of videos falsely. False claims are primarily carried out via YouTube’s manual claiming tool [21]. This tool enables MCNs to claim ownership of videos and operates on an honor code (users of the tool are responsible for not making false claims). We observed many complaints from creators whose

¹To prevent this paper from encouraging prospective malicious MCNs, MCN names are available for research on request.

uploaded original content was later claimed by an MCN. For example, one creator alleges “...[an MCN] is abusing their access to Content ID (particularly the manual claiming tool) and working in tandem with [another MCN] to siphon millions from songs they do not have any rights to claim.”

Dispute of False Copyright Claims. Individual content creators may dispute Content ID claims. During the dispute process, the disputed video may either be monetized or blocked from being viewed, depending on the claim. For the former, YouTube holds the revenue generated from the date of the dispute separately (in escrow), and upon resolution, revenue is paid to the appropriate party. However, this process is tedious and does not guarantee corrected action, or content restoration. One post in our dataset claims “...[I’ve] had multiple content ID disputes rejected in the past few months for using royalty-free music.” Additionally, we also observed numerous allegations of MCNs acknowledging a copyright claim was incorrectly filed but fail to drop the said claim. One creator claims when talking with a malicious MCN that “...they acknowledged [the claim] was a mistake and removed it...[but that] months later my video had a claim again.” Dissatisfaction with the dispute system and frustration with unfairness when dealing with claims were common themes presented by creators when discussing malicious MCNs applying Content ID to original content. For example, one creator noted “YouTube’s Copyright Claim Dispute System is so [expletive] biased towards the Big Corps / Holders (MCNs), and that they might as well already remove it because it’s useless anyway.”

Creator Harm. Due to MCN abuse of Content ID privileges and difficulty in disputing false copyright claims, creators are harmed as they find their videos demonetized. Even in the case of a successful Content ID claim dispute, creators may lose monetization for up to 30 days, the maximum time the owner of claimed copyright content has to respond [19]. For instance, one creator in our data states “I’ve lost 1 month [of revenue] because an MCN decided to claim copyright.”

5 Discussion and Limitations

Content creators and MCNs leveraging illicit monetization exploits on YouTube are a persistent problem. Our work primarily uses qualitative methodology to analyze publicly available forums. Similar to previous work [53], we note that themes present in our dataset may differ from private forums and groups. As mentioned in Section 3.1, we focus on publicly accessible forums to capture public conversation amongst creators, and in turn, resources most available to creators.

We also note that our findings do not focus on the frequency of occurrence for each specific exploit, as we instead aim to provide a review of the most popular illicit monetization exploits on YouTube. Our analysis presents three observations that provide insight into potential solutions against illicit monetization and future work in the area. First, we highlight the

emergence of online forums as a source of information for malicious creators. Second, we note how the incentive to monetize YouTube content creates online marketplaces that cater to malicious creators aiming to implement illicit monetization exploits. Third, we examine the hierarchical MCN-creator relationship and detail how it may lead to creator harm.

5.1 Online Illicit Monetization Communities

Analyzing data from our 11 crawled forums, we discovered conversation spreading illicit monetization tactics of stealing original content and directing traffic to external sites. For instance, manual examination of forum threads found using relevant keywords resulted in the unexpectedly straightforward discovery of illicit content monetization services, software, and guides. While we observed posting guidelines for a number of these forums prohibiting discussion of deceitful or evasive practices on YouTube, we found this rule poorly enforced; likely due to ambiguity in YouTube policy interpretation. As such, the existence of these forums acts as a potential gateway for illicit content monetization, further contributing to the existence of harmful content on YouTube.

Mitigation. Consistent moderation of various third-party websites is a likely difficult, impractical, and contentious task for YouTube to address. Although exhaustive moderation is impractical, we believe YouTube would significantly benefit from periodically crawling/evaluating sentiment on public forums and analyzing conversations from creators to detect the emergence of new illicit strategies. Additionally, we posit that improved moderation of community content and/or more accessible policies outlining YouTube monetization policy would help protect YouTube viewers and other benign creators, while simultaneously limiting loopholes that allow malicious tactics to flourish. We plan to continue monitoring these communities and their discussion to examine how these groups organize and construct illicit monetization exploits.

5.2 Illicit Content Monetization Economy

Our analysis of crawled forum data and marketplace listings shows an active service market that profits off facilitating illicit monetization on YouTube. We discovered nine online marketplaces providing the illicit sale of YouTube accounts and content-related services (e.g., purchasable views, subscribers, comments). We found evidence of malicious creators successfully using these services to purchase accounts and generate artificial channel engagement, allowing them to immediately monetize their content and reach an audience.

We also observed discussion around content editing software tailored for evading YouTube policy and copyright detection. On websites such as YTPara, we found entire forum threads dedicated to the commerce of tools that allow creators to manipulate uploaded content or self-host mechanisms of artificial engagement. Although unintentional, benign software

also contributes to this economy with many video editing software leveraged for illicit content monetization. Lastly, we observed MCNs themselves as a component of this economy, with malicious creators joining MCNs to illicitly work around inability to monetize, or country-specific law/tax restrictions.

Mitigation. Current methods of countering YouTube account abuse (e.g., sale of accounts, use of services/evasion software) rely on tracking account IP addresses and taking action on mismatches in login sessions, or flagged accounts [81]. However, this action occurs *after* transactions are completed for these items, with no current methods proactively preventing users from leveraging these illicit resources.

We plan to explore how online forums can enact strict guidelines to prevent the promotion of the for-profit illicit monetization economy and how developers of benign software used in monetization exploits can work with YouTube to prevent abuse of their software. Further efforts should also be conducted to detect artificial engagement and purchased accounts. For example, an anomaly detector can be implemented to identify abnormal/malicious behavior in creator accounts and their related content. To detail, if an uploaded video has (as compared to previous uploads from an account): (1) lack of community engagement (e.g., likes, comments), (2) disparity in content genre/video length, and (3) irregularities in upload location, this may collectively flag a creator account as potentially purchased from a marketplace.

5.3 Contentious MCN-Creator Relationships

The MCN-creator relationship has become an integral part of the YouTube ecosystem. Although the relationship between both parties is posed as mutually beneficial, we found evidence of common circumstances that harm creators. Specifically, MCN withheld creator payment and abuse of Content ID privileges are highlights of such points of contention. We also found that many creators feel YouTube is not the appropriate mediator between MCNs and individual creators, noting power imbalance improperly handled by YouTube.

Mitigation. Our findings highlight the need for improved oversight of MCN-creator relationships on the YouTube platform as well as relevant resources to protect creators from MCN harm. We suggest adding creator-oriented features for reporting or acting against malicious MCNs, as current YouTube guidelines do not provide such resources. Such a capability would mitigate abuse of creators and promote improved content quality. Policy revisions that emphasize creator protection in the MCN-affiliate relationship could also mitigate such concerns. In future work, we will reach out to YouTube for potential collaboration in examining internal data (e.g., patterns of wide distribution of Content ID for uploaded content matched with reports of malicious MCNs, payout to a single MCN account from multiple channels) that can identify malicious MCNs via affiliated creators.

6 Responsible Disclosure

Our findings are unconventional in regard to security and user protection concerns on YouTube. That is, we do not highlight any code or present new exploits of the YouTube backend that may harm users. Existing reporting methods provided by YouTube for our type of findings only extend to individual accounts and/or uploaded content, but do not provide an option for reporting wide-scale malicious activity. For example, while a YouTube viewer may flag an individual YouTube channel for deceptive external content (e.g., phishing personal information), there is no option to submit a security risk that describes such an exploit/concern at scale (e.g., “bug-bounty” style form that allows high-detail description for a concern).

We have thus contacted Google researchers with experience researching YouTube to disclose our findings and for potential future collaborations. We received acknowledgment from one researcher in the area of Google product user experience, who then forwarded our disclosure to a principal engineer responsible for YouTube ad monetization. This individual then directed us to the Strategic Partnership team at YouTube, who told us they would route our research to members of the team for review before deciding on next steps to proceed.

7 Related Work

Analysis of Malicious Behavior on Online Forums. The security community has long explored online forums to expose conversations surrounding malicious activity. Tseng et al. [53] and Bellini et al. [6] underscore how forums such as Reddit serve as platforms to discuss methods to perpetrate intimate partner violence and how these forums advertise tools to aid in such behavior. Similarly, abuse, cyberbullying, and online harassment on online platforms like Twitter have also been studied [10, 30]. A line of work has explored the online economy or marketplace that aims to aid illegal transactions [9, 29, 56, 86]. In contrast, we present the first study on how content creators use online forums as a means of exchanging information concerning illicit monetization and as an avenue to express contention with MCNs.

Detecting Illicit Activity on YouTube. The YouTube ecosystem has been studied to identify harmful content. Recent works have analyzed metadata and shared features (i.e., keywords, hashtags) across spam videos on YouTube [7, 51]. Another line of work focused on the automated classification of harmful activity on YouTube. Motivated by *Elsagate*, a controversy where YouTube videos categorized as children’s content contained inappropriate themes (e.g., Elsa from Disney film *Frozen* performing suggestive acts), Papadamou et al. developed a binary classifier for detecting YouTube videos potentially disturbing/harmful for toddlers [36]. Similarly, several efforts have identified spam and click-bait type videos by studying video metadata, comments, user

activities, and video attributes [4, 11, 85]. In contrast, we provide a broad overview of the different types of methods exploited by creators to monetize content while also shedding light on how MCNs exploit creators when monetizing content.

8 Conclusions

In this paper, we describe the landscape of illicit content monetization exploits used by content creators and MCNs on YouTube. We crawled 11 forums and discussion boards and studied conversations surrounding illicit monetization, examining online account and service marketplaces, and software. We identify six distinct illicit and exploitative methods perpetrated by creators and MCNs. These exploits harm viewers, other creators, and third-parties. We present a comprehensive review of how online communities are sources of intelligence for illicit content monetization activity, and how the economy surrounding illicit monetization further operates in the scope of relationships between content creators and MCNs.

Acknowledgment

We thank our shepherd Elissa Redmiles and our anonymous reviewers for providing us with valuable comments and feedback used to improve our paper. This work is supported by startup funding from Purdue University.

References

- [1] YouTube channels for sale | buy & sell YouTube channel. <https://tinyurl.com/yyvny6oz>, 2020. [Online; accessed 22-December-2020].
- [2] Fórum adrenaline - um dos maiores e mais ativos fóruns do brasil. <https://tinyurl.com/y3kwmfdv>, 2020. [Online; accessed 21-December-2020].
- [3] Payments faqs. <https://tinyurl.com/y6n8rcza>, 2020. [Online; accessed 20-December-2020].
- [4] Tulio Alberto, Johannes Lochter, and Tiago Almeida. Tubesppam: Comment spam filtering on YouTube. In *IEEE 14th international conference on machine learning and applications (ICMLA)*, 2015.
- [5] Alexa - competitive analysis, marketing mix, and website traffic. <https://tinyurl.com/y9k4se8k>, 2020. [Online; accessed 22-December-2020].
- [6] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. “So-called privacy breeds evil” narrative justifications for intimate partner surveillance in online forums. *Proceedings of the ACM on Human-Computer Interaction*, 2021.

- [7] Elijah Bouma-Sims and Brad Reaves. A first look at scams on YouTube. In *Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb)*, 2021.
- [8] Buy YouTube views. <https://tinyurl.com/y5sgz427>, 2020. [Online; accessed 21-December-2020].
- [9] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. In *IEEE Symposium on Security and Privacy (SP)*, 2018.
- [10] Despoina Chatzakou, Nicolas Kourtellis, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini, and Athena Vakali. Measuring #GamerGate: A tale of hate, sexism, and bullying. In *Proceedings of international conference on world wide web companion*, 2017.
- [11] V. Chaudhary and A. Sureka. Contextual feature based one-class classifier approach for detecting video response spam on youtube. In *Eleventh Annual Conference on Privacy, Security and Trust*, 2013.
- [12] YouTube help - copyright management tools. <https://tinyurl.com/kzzwcgo>, 2020. [Online; accessed 22-December-2020].
- [13] YouTube help: How Content ID works. <https://tinyurl.com/kzzwcgo>, 2020. [Online; accessed 21-December-2020].
- [14] YouTube stars are blurring the lines between content and ads. <https://tinyurl.com/y2ktb8t5>, 2020. [Online; accessed 22-December-2020].
- [15] Fake engagement policy. <https://tinyurl.com/vmc4vr9b>, 2021. [Online; accessed 20-September-2021].
- [16] Buy instagram accounts & YouTube channels - fameswap. <https://tinyurl.com/y6lxqxa9>, 2020. [Online; accessed 20-December-2020].
- [17] Upload videos longer than 15 minutes - computer - YouTube help. <https://tinyurl.com/y2bg3nop>, 2020. [Online; accessed 20-December-2020].
- [18] Foro de YouTube. <https://tinyurl.com/yxhomcl8>, 2020. [Online; accessed 20-December-2020].
- [19] Dispute a Content ID claim - YouTube help. <https://tinyurl.com/39h75axw>, 2021. [Online; accessed 17-May-2021].
- [20] Goyral YouTube bot. <https://tinyurl.com/ejxdsc>, 2021. [Online; accessed 3-March-2021].
- [21] What is a manual claim? - YouTube help. <https://tinyurl.com/yefukb43>, 2021. [Online; accessed 17-May-2021].
- [22] Understanding adsense country restrictions - adsense help. <https://tinyurl.com/tftbwa6>, 2021. [Online; accessed 17-May-2021].
- [23] Free YouTube subscribers generator app 2021. <https://tinyurl.com/3ck6x278>, 2021. [Online; accessed 3-March-2021].
- [24] googletrans 3.0.0. <https://pypi.org/project/googletrans/>, 2021. [Online; accessed 3-March-2021].
- [25] Google translate. <https://tinyurl.com/7adadfe>, 2020. [Online; accessed 22-December-2020].
- [26] YouTube view bot. <https://tinyurl.com/25k7z5yu>, 2021. [Online; accessed 3-March-2021].
- [27] YouTube networks for small channels, the ultimate guide! <https://grow.grin.co/youtube-networks-for-small-channels/>, 2019. [Online; accessed 3-March-2021].
- [28] Dien dan hoc vien YouTube - hvyt. <https://tinyurl.com/y6x5upy5>, 2020. [Online; accessed 21-December-2020].
- [29] Thomas J Holt. Examining the forces shaping cyber-crime markets online. *Social Science Computer Review*, 2013.
- [30] Yiqing Hua, Mor Naaman, and Thomas Ristenpart. Characterizing twitter users who engage in adversarial interactions against political candidates. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2020.
- [31] Kapwing - edit video and create content online. <https://www.kapwing.com/>, 2020. [Online; accessed 3-March-2021].
- [32] What are your options when buying YouTube views? <https://tinyurl.com/y6rbrwy8>, 2020. [Online; accessed 21-December-2020].
- [33] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction*, 2019.
- [34] What are the top YouTube mcns up to now? <https://tinyurl.com/2hvfbszm>, 2021. [Online; accessed 3-March-2021].
- [35] Create a new YouTube channel - youtube help. <https://tinyurl.com/mx9fyc9>, 2020. [Online; accessed 22-December-2020].

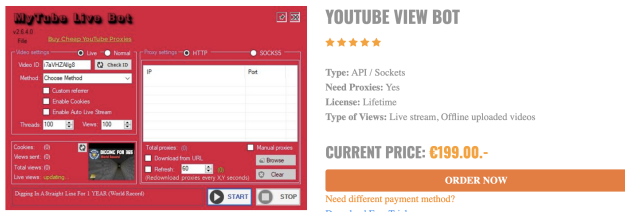
- [36] Kostantinos Papadamou, Antonis Papasavva, Savvas Zannettou, Jeremy Blackburn, Nicolas Kourtellis, Ilias Leontiadis, Gianluca Stringhini, and Michael Sirivianos. Disturbed YouTube for kids: Characterizing and detecting inappropriate videos targeting young children. In *Proceedings of the International AAAI Conference on Web and Social Media*, 2020.
- [37] PR-CY service of independent website promotion - online tools for webmasters, optimizers and copywriters. <https://tinyurl.com/y62cr2m2>, 2020. [Online; accessed 22-December-2020].
- [38] Buy instant YouTube views, subscribers & likes - qq-tube.com. <https://tinyurl.com/y52xykzq>, 2020. [Online; accessed 21-December-2020].
- [39] Metrics for reddit - discover the fastest growing subreddits & reddit stats. <https://tinyurl.com/yy6yukqk>, 2020. [Online; accessed 20-December-2020].
- [40] Newtubers - the premiere small content creator community. <https://tinyurl.com/y88a27cs>, 2020. [Online; accessed 21-December-2020].
- [41] Reddit partnered YouTube content creators. <https://tinyurl.com/y6sjc3u6>, 2020. [Online; accessed 22-December-2020].
- [42] YouTube. <https://tinyurl.com/lkvx5gz>, 2020. [Online; accessed 22-December-2020].
- [43] Scrapy - a fast and powerful scraping and web crawling framework. <https://tinyurl.com/grs6vxx>, 2020. [Online; accessed 22-December-2020].
- [44] Searchengines.guru - it news and forum focused on digital marketing, seo optimization and website development. <https://tinyurl.com/yxbv3oob>, 2020. [Online; accessed 21-December-2020].
- [45] Bureau of counterterrorism - state sponsors of terrorism. <https://tinyurl.com/72y8w3ww>, 2021. [Online; accessed 1-June-2021].
- [46] YouTube, Twitch, Twitter, & Instagram statistics - socialblade.com. <https://tinyurl.com/zjxn7kw>, 2020. [Online; accessed 20-December-2020].
- [47] Sonuker. <https://tinyurl.com/yalkrd2x>, 2020. [Online; accessed 21-December-2020].
- [48] Free YouTube subscribers - grow your YouTube channel quicker than ever before! <https://tinyurl.com/y2wddqf4>, 2020. [Online; accessed 20-December-2020].
- [49] YouTube basics - the quickstart guide to YouTube. <https://tinyurl.com/y4pty6m>, 2020. [Online; accessed 22-December-2020].
- [50] SWAPD: Buy, sell, & trade virtual properties. <https://tinyurl.com/qwgtxz5>, 2020. [Online; accessed 20-December-2020].
- [51] Ashutosh Tripathi, Kusum Kumari Bharti, and Mohona Ghosh. A study on characterizing the ecosystem of monetizing video spams on YouTube platform. In *Proceedings of the 21st International Conference on Information Integration and Web-based Applications & Services*, 2019.
- [52] Buy and sell websites. <https://tinyurl.com/y68pg9zm>, 2020. [Online; accessed 19-December-2020].
- [53] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *USENIX Security*, 2020.
- [54] T-series's YouTube stats (summary profile) - social blade stats. <https://tinyurl.com/2692bt3h>, 2021. [Online; accessed 5-June-2021].
- [55] Tubebuddy forums. <https://tinyurl.com/ybsnlhgd>, 2020. [Online; accessed 20-December-2020].
- [56] Rolf Van Wegberg, Samaneh Tajalizadehkhoob, Kyle Soska, Ugur Akyazi, Carlos Hernandez Ganan, Bram Klievink, Nicolas Christin, and Michel Van Eeten. Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In *USENIX Security*, 2018.
- [57] Videonti - advanced batch rendering solutions. <https://tinyurl.com/5yxukh4k>, 2013. [Online; accessed 3-March-2021].
- [58] Videoyap. <https://www.videoyap.com/>, 2020. [Online; accessed 3-March-2021].
- [59] Buy & sell your viral social media account influence - viralaccounts.com. <https://tinyurl.com/y7fkxxd4>, 2020. [Online; accessed 20-December-2020].
- [60] Distribution of total YouTube video content worldwide as of december 2018, by category. <https://tinyurl.com/2js7svt9>, 2021. [Online; accessed 1-June-2021].
- [61] YouTube-subbot. <https://tinyurl.com/2j725nsp>, 2019. [Online; accessed 3-March-2021].
- [62] youtube-viewer-bot. <https://tinyurl.com/2w3ccsz8>, 2020. [Online; accessed 3-March-2021].
- [63] youtube-viewer. <https://github.com/soumyadityac/youtube-viewer>, 2020. [Online; accessed 3-March-2021].

- [64] YouTube abone hilesi,youtube abone kasma. <https://tinyurl.com/y45s925j>, 2020. [Online; accessed 20-December-2020].
- [65] YouTube guide builder. <https://tinyurl.com/tz6weet>, 2020. [Online; accessed 21-December-2020].
- [66] YouTube community guidelines (rules and policies). <https://tinyurl.com/ycy54tev>, 2020. [Online; accessed 22-December-2020].
- [67] Media shark - the 2020 guide to YouTube CPM. <https://tinyurl.com/y5jx9a6v>, 2019. [Online; accessed 20-December-2020].
- [68] USATODAY: Video websites pop up, invite postings. <https://tinyurl.com/yxrz78lv>, 2005. [Online; accessed 22-December-2020].
- [69] Alphabet announces fourth quarter and fiscal year 2019 results. <https://tinyurl.com/y4uoh3q8>, 2020. [Online; accessed 22-December-2020].
- [70] Multi-channel network (mcn) overview for YouTube creators. <https://tinyurl.com/yy36hmuy>, 2020. [Online; accessed 20-December-2020].
- [71] YouTube's new monetization rules are controversial, painful and necessary. <https://tinyurl.com/yy38b5b9>, 2018. [Online; accessed 22-December-2020].
- [72] YouTube partner program overview & eligibility. <https://tinyurl.com/y7w22auk>, 2020. [Online; accessed 21-December-2020].
- [73] YouTube5Year: History of monetization at YouTube. <https://tinyurl.com/y379ru4x>, 2010. [Online; accessed 22-December-2020].
- [74] Infographic: The history of video advertising on YouTube. <https://tinyurl.com/y3q33d7p>, 2011. [Online; accessed 22-December-2020].
- [75] Youtube Help: Choose how you want to monetize. <https://tinyurl.com/orr5qe3>, 2020. [Online; accessed 20-December-2020].
- [76] YouTube Help: Youtube channel monetization policies. <https://tinyurl.com/v5by48w>, 2021. [Online; accessed 5-June-2021].
- [77] The Verge: The golden age of YouTube is over. <https://tinyurl.com/y6h5zyyy>, 2019. [Online; accessed 21-December-2020].
- [78] YouTube premium and music have 20 million subscribers. <https://tinyurl.com/yypdjquf>, 2020. [Online; accessed 22-December-2020].
- [79] Add paid product placements, sponsorships & endorsements. <https://tinyurl.com/yyync92x>, 2020. [Online; accessed 20-December-2020].
- [80] YouTube revenue and usage statistics (2021). <https://www.businessofapps.com/data/youtube-statistics/>, 2020. [Online; accessed 3-March-2021].
- [81] YouTube community guidelines enforcement. <https://tinyurl.com/y8ubf8zx>, 2021. [Online; accessed 08-June-2021].
- [82] YouTube Official Blog: You know what's cool? a billion hours. <https://tinyurl.com/wha4sj9f>, 2017. [Online; accessed 3-March-2021].
- [83] Ytpara.com - YouTube & webmaster destek forumu - vbuletin. <https://tinyurl.com/y6pqosqy>, 2020. [Online; accessed 20-December-2020].
- [84] YouTube forum, the #1 YouTube community, video editing, branding & YouTube help. <https://tinyurl.com/yxvzkscr>, 2020. [Online; accessed 20-December-2020].
- [85] S. Zannettou, S. Chatzis, K. Papadamou, and M. Sirivianos. The good, the bad and the bait: Detecting and characterizing clickbait on YouTube. In *IEEE Security and Privacy Workshops (SPW)*, 2018.
- [86] Gengqian Zhou, Jianwei Zhuge, Yunqian Fan, Kun Du, and Shuqiang Lu. A market in dream: the rapid development of anonymous cybercrime. *Mobile Networks and Applications*, 2020.
- [87] Zyte - world leading web scraping services, & developer tools. <https://tinyurl.com/y33j3weu>, 2020. [Online; accessed 20-December-2020].

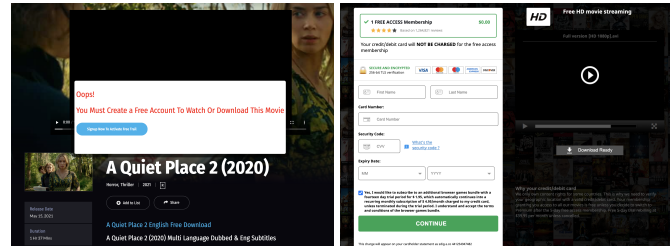
Appendix

We provide images pertaining to the exploits we have discovered. Figure 1a is a sale listing of a view bot application that was advertised on a forum. Figure 1b,1c,1d are examples of websites that malicious creators redirect benign viewers to. Figure 1e presents two images from the homepage of the software *Videonti*, which markets itself as a means to avoid detection of copyright violation.

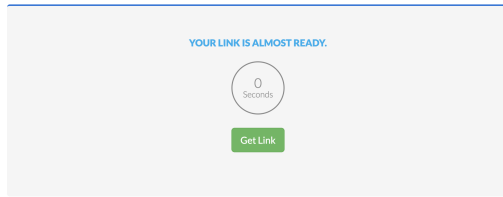
Table 1 lists all keywords used in the Google Search API crawler (Crawler A), described in Section 3.1.



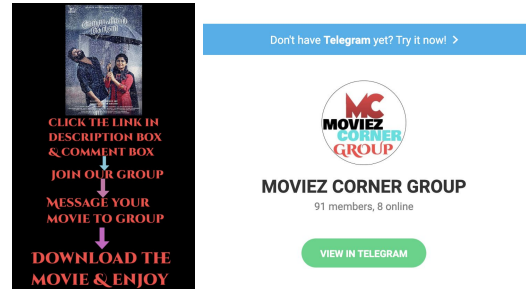
(a)



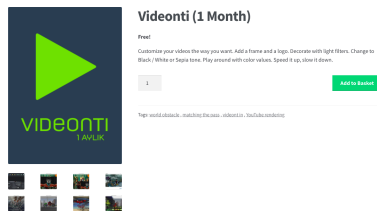
(b)



(c)



(d)



(e)

Figure 1: (a) Sale listing of a view bot application that costs 199.00 Euros (242.63 USD) that runs on a local computer. (b) Example of a website advertised via a link, where watching a movie requires account creation. (c) Example of website advertising a URL shortening service while a user waits for a link to download a movie. (d) Video that redirects users to join a *Telegram* (messaging app) group where members exchange pirated content. (e) Description and images of *Videonti* from its website, highlighting that the software is intended to evade copyright violation detection.

Table 1: Keywords used in Google crawler (Section 3.1).

Initial Discovery Keywords				
monetization fraud	mcn copyright	mcn scam	mcn fraud	mcn danger creator
mcn creator interaction	mcn creator scam	youtube copyright policy	youtube scam	youtube fraud
youtube affiliate	youtube affiliate scam	youtube content policy	youtube creator	youtube monetization policy
youtube advertising policy	youtube ad scam	youtube partner	youtube partner fraud	youtube partner scam
Exploit-specific Keywords				
youtube reupload	illegal reupload	youtube movie piracy	youtube movie site	link farming
youtube third-party affiliate	youtube fake views	youtube fake comments	youtube fake likes	youtube fake subscribers
youtube buy channel	youtube buy account	youtube buy monetized account	youtube sell channel	youtube sell account
youtube sell monetized account	youtube advertise link	youtube link in description	youtube go to link	youtube channel stealing
youtube channel content theft	youtube channel copyright	youtube channel stealing videos	youtube buy likes	youtube buy subscribers
youtube buy comments	youtube instant subscribers	youtube instant comments	youtube instant likes	youtube guarantee subscribers
youtube guarantee comments	youtube guarantee likes	MCN breach of contract	MCN not paying	MCN withholding payment
MCN content id theft	MCN stealing content	MCN theft	MCN claim copyright	MCN copyright infringement
MCN claim content id	MCN fake			