Analysis of YouTube USDT crypto scams

Andrew Patel,
WithSecure™ Intelligence, 2023

WITH secure

Contents

1 Abstract

WithSecure™ Intelligence has discovered thousands of videos advertising fraudulent web-based apps that pose as USDT (Tether) investment schemes. These videos, hosted on YouTube, promise returns that scale on the amount of currency invested. YouTube channels with significant numbers of subscribers and view counts post new videos of this type on a daily basis. Some of the participating channels are even YouTube verified accounts.

Many videos of this nature receive inauthentic engagement boosts, designed to game YouTube's recommendation algorithms, from hundreds of YouTube channels controlled by a small group of Telegram users. These inauthentic YouTube channels also use automation to post copy-paste comments to videos in an effort to make the advertised fraudulent apps appear legitimate. Description fields attached to the videos also employ a unique style of "SEO", likely designed to game YouTube's search functionality.

At the time of writing, approximately 700 URLs associated with fraudulent apps of this nature were identified via data capture and analysis techniques. The YouTube hashtag #usdtmining also reportedly contains over 3,900 similar videos.

Cryptocurrency wallet addresses associated with these fraudulent apps were directly extracted from several YouTube videos. Patterns found in transactions associated with these wallets suggest that there may be thousands of additional apps and crypto wallets involved in these operations. By collecting transaction history for these wallets, a set of 900 victims were identified. Summing the transactions between victim wallets and app wallets provided an estimate that operations associated with these scams made just over 100,000 USD between July and November 2022.

These operations use hundreds or possibly thousands of cryptocurrency wallets, all of which make very small and frequent transfers between each other. Mapping the flow of money in these operations represents an extremely complicated endeavor. However, it is possible to identify large amounts of money flowing through a few downstream wallets in the blockchain.

This report details the anatomy of the videos and apps behind this scam, analyses two associated scam apps in detail, explores the #usdtmining YouTube hashtag, describes blockchain analysis methodology used on crypto wallets associated with the scam, and finally presents recommendations for YouTube and some final conclusions.

2 Introduction

Cybercriminals have been quick to adopt crypto currencies as a means to receive payment for their malicious activities. This is due to the fact that crypto currencies are pseudonymous, decentralized, and often not subject to traditional financial regulations. This has resulted in a proliferation of cybercriminal activities that would not have been possible without crypto currencies.

Many relatively unknown criminal schemes exist within the crypto currency ecosystem. One such example is mining pool or liquidity mining scams, which are fraudulent operations designed to trick holders of crypto currencies into investments with reportedly high returns. Victims who invest in these schemes hand money over to scammers who never give it back.

Roughly speaking, USDT mining scams work in the following manner. A victim is first lured in via advertising on social media or recommendations from YouTube's algorithm. YouTube hosts thousands of videos that advertise these "make quick money" schemes. Videos of this nature often promise unrealistic returns, with some boasting whole-number percentage points per day.

The YouTube videos analyzed in this report appear to follow a set script. It is likely that the group involved in the creation of these scam apps provide set scripts that contracted YouTubers must follow. These YouTubers are likely compensated monetarily for publishing such videos. A majority of the videos found during this research were presented in languages spoken in the Indian region.

According to the video script, victims are required to create an account in the advertised app. Apps come in the form of web pages, mobile applications, and in some cases, automation that interacts with users on the Telegram social network. As part of the account creation and registration process, the victim must deposit a small amount – normally just tens of USD – of currency into the app. This is the point where the scammer steals money from the victim.

Many of these videos encourage victims to invite friends and family in, claiming that for each person invited, they'll receive a small amount of money. The apps also include bonus "VIP" structures that unlock better "investment" options that boast higher investment returns. These "VIP" schemes usually require the user to deposit more currency into the app. Some of the videos on YouTube go into great length about these complicated VIP bonus structures.

Different apps are structured in different ways. Some are intended to make the victim believe that their investment is used for "mining" – simply leave your money in the pool and you'll earn a commission. Others contain daily "tasks" or "grabs" that the user must click on to "earn" money. We even encountered a farming game where the user invests money to raise cartoon chickens, cows, and horses, each costing different amounts of money.

In all cases, the app interface will report an increase in the victim's balance either periodically, or after performing app-specific tasks. In these schemes, higher investments typically yield higher returns. Victims, upon observing good returns on a small investment, are thus tempted to invest more.

Videos published on YouTube usually demonstrate withdrawal functionality from within the advertised app. This is to trick victims into understanding that they can cash out at any time. However, the opposite is always true. Victims will not be able to retrieve any funds deposited into the app. This fact was verified by tracking transactions from wallets associated with these apps – although victims sent currency to the app wallet, no transactions in the other direction were observed.

YouTube videos demonstrating mining pool investment schemes appear to be largely directed towards people who are already familiar with the crypto currency ecosystem and who likely already have holdings in some of those currencies. The apps that are demonstrated require a victim to transfer funds from an already created wallet. Although some videos show the viewer how to create a wallet and put real money into it, the end-to-end process of creating a wallet, populating it with money, registering with a scam app, and finally moving crypto currency into it is rather lengthy and fiddly.

The "apps" themselves are shoddily constructed and full of badly written, hardly legible English. They are clearly not convincing as vehicles for serious investment. Simply clicking through their "work description" or "company profile" sections should be enough to raise an alarm. Many of the apps investigated appear to be reskinned versions of each other. It is thus possible that these operations utilize an "app customization kit", allowing non-technical workers to configure and deploy new apps with ease. The videos that advertise these apps are of similar poor quality.

All apps studied in this report utilize the USDT[1] crypto currency. USDT, also known as Tether, is a crypto currency that is reportedly "tethered" to the value of the US dollar. Such a currency is known as a "stable coin" and cannot be mined. The only thing you can do with USDT is buy it for approximately 1 USD and sell it for approximately the same price. It is worth noting that a great deal of controversy surrounds USDT, including allegations that it was used to manipulate the value of Bitcoin in 2017 and 2018.

Research into crypto-based scams is widespread. The following links lead to recently published reports on crypto scams similar in nature to this one.

- https://news.sophos.com/en-us/2022/05/17/liquidity-mining-scams-add-another-layer-to-cryptocurrency-crime/
- https://blog.coinbase.com/security-psa-mining-pool-scams-targeting-self-custody-wallets-543ffe698724
- https://www.ic3.gov/Media/Y2022/PSA220721
- https://tbbob.com/scams/usdt-pool-mining-review-defi-mining-liquidity-scam
- https://cryptonews.com/news/hong-kong-police-publish-details-of-usdt-fraud-case-in-effort-to-raise-public-awareness-of-crypto-scams.htm
- https://news.trendmicro.com/2022/06/10/tether-usdt-phishing-fake-walletconnect-scam/
- https://www.proofpoint.com/us/blog/threat-insight/broken-dreams-and-piggy-banks-pig-butchering-crypto-fraud-growing-online

The operations detailed in this report utilize a "hands-off" approach via YouTube videos and "apps". This contrasts with the hands-on confidence-based social engineering methodology used in "pig butchering" scams that are currently popular. One reason why YouTube infrastructure is used in preference to a hands-on approach might be because most of the videos are presented in non-English languages and are thus designed to tap into a pool of victims without the need for social engineers who can fluently speak those languages.

1. https://en.wikipedia.org/wiki Tether_(cryptocurrency)

3 The anatomy of a USDT mining pool video and app

Most of the relevant mining pool scam videos observed on YouTube had the same basic structure. This section outlines the script that they usually follow and is accompanied by screenshots from a video about an app called paxxk[.]biz. This URL was identified by a WithSecure™ Intelligence researcher as a potentially fraudulent site prior to the initiation of this research effort. This app is the focus of more detailed analysis in a later section of this report.

Figure 1 shows the thumbnail of the video used in this example. It was the first hit presented by YouTube while searching for "paxxk[.]biz" in the web UI and was posted by an account called "Your Crypto Helper". Most videos of this ilk are audio narrated but this one included a video presenter, which is extremely rare, and may account for the video receiving a lot of engagement and thus showing up as the top hit.

The paxxk[.]biz app is a simple web site designed to be displayed on a mobile phone. The site can be accessed from any browser. Since it is designed to be viewed on a phone (and therefore look like a phone app), it comes over as clumsy when viewed from a desktop browser (Figure 2).

Figure 1: Thumbnail shown in YouTube search results for example vide

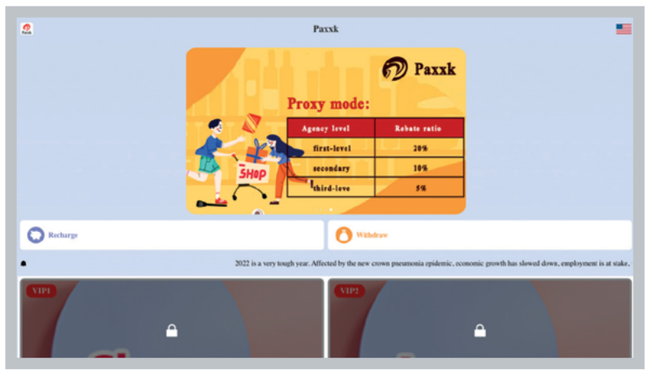


Figure 2: paxxk[.]biz displayed in a desktop browser

In the analyzed video, the presenter starts by introducing the app's registration process (Figure 3), explaining that new users must make an account and set a password. There's an invitation code field that the presenter advertises in his video. People using the invitation code will supposedly earn the presenter's account some money.

The presenter then goes into length about how account holders can earn free USDT by inviting friends and family (Figure 4).

The app contains a number of gamification mechanisms, including bonuses for inviting new people and a various "VIP" schemes. Some of these mechanisms are depicted in Figure 5.

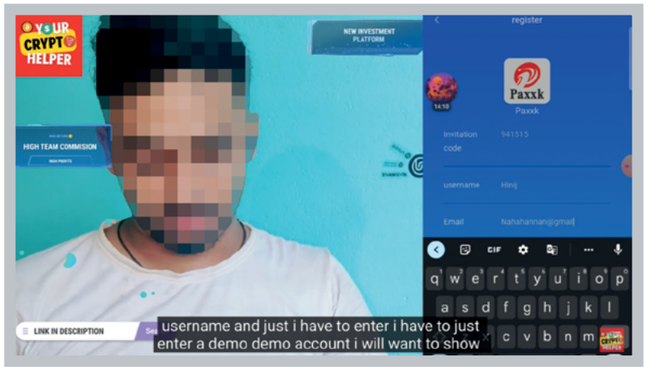


Figure 3: introducing the paxxk[.]biz registration process

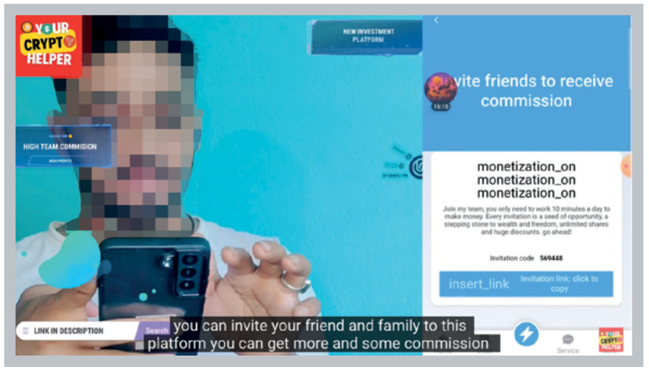


Figure 4: the presenter encourages the video's audience to invite friends and make money

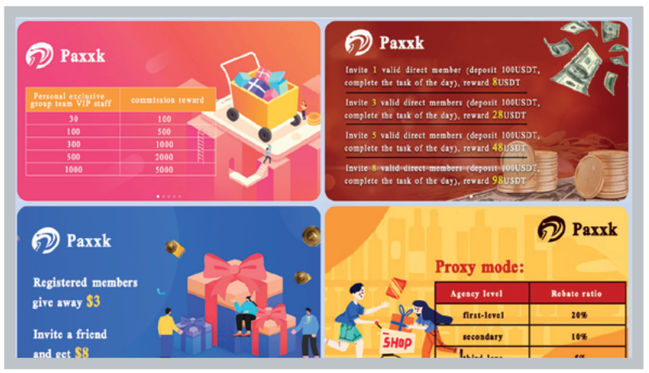


Figure 5: Thumbnail shown in YouTube search results for example vide

The app also utilizes “recharge rewards” that claim to provide monetary bonuses for adding more currency to the app (shown in Figure 6). This “recharge reward” concept is strikingly similar to “spending reward” structures commonly used in mobile games. In fact, the gamification aspects of many of these apps also mirror common mobile gaming tropes where users are incentivized to perform menial tasks to earn small rewards.

The paxxk[.]biz app includes a scrolling “tickertape” of supposedly delivered commissions (Figure 7). This part of the display is designed to make the victim think that others are reaping huge commissions (which, of course, require huge investments). Since analysis of wallets attached to these scams show very few transactions in most cases, this part of the interface is almost definitely just randomly generated.

The video continues with a brief tutorial on how to “recharge” – i.e., how to move crypto currency from your own crypto wallet to the app. The video’s presenter “transfers” 20 USDT to the app during this demo (Figure 8). This is an important part of the video since scammers need victims to perform this step in order to make money. Note how the wallet address attached to the scam app is visible in this screenshot.

Figure 6: paxxk[.]biz “recharge rewards”

Figure 7: paxx.biz commission tickertape

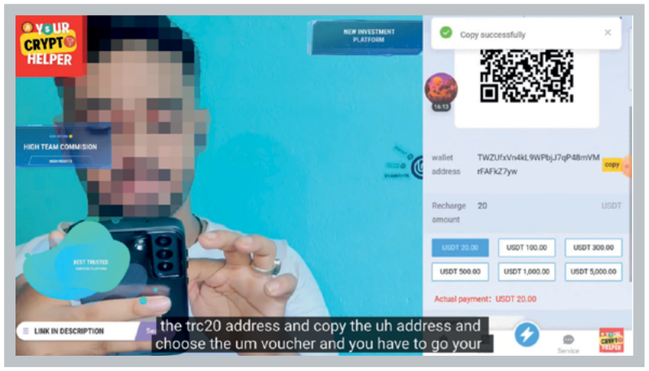


Figure 8: using paxxk[.]biz app’s “recharge” functionality

The presenter then talks about the app’s withdraw functionality, emphasizing that there are no withdrawal fees (Figure 9).

However, the actual withdrawal functionality is not properly demoed and watching further into the video (Figure 10) verifies that the presenter didn’t withdraw any funds. This is, of course, working as intended, since the app’s withdrawal functionality does nothing. Note the presenter’s important message in Figure 10 – if you want to make more money you have to deposit more.

The presenter finally shows viewers that the app has customer service functionality and then signs off (Figure 11).

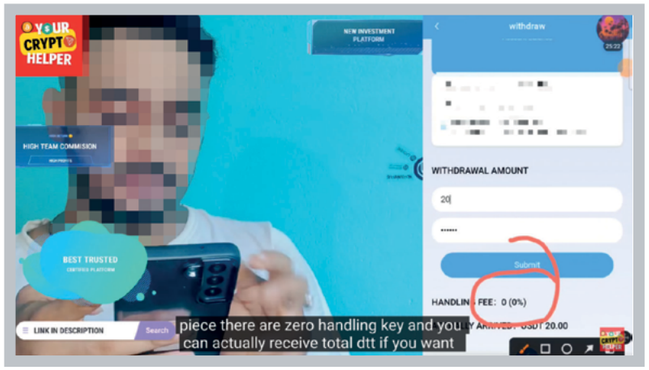


Figure 9: presenter discusses withdrawal functionality

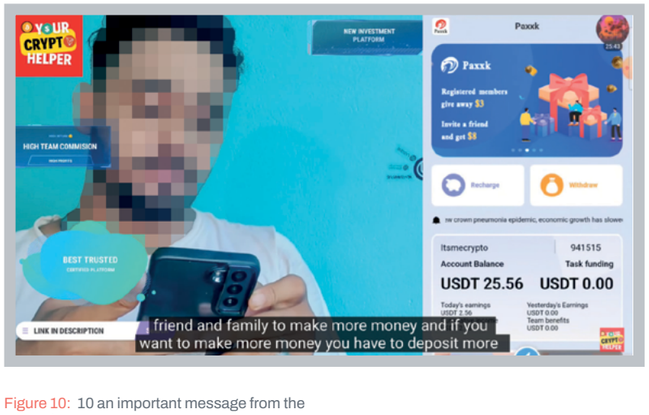


Figure 10: 10 an important message from the presenter

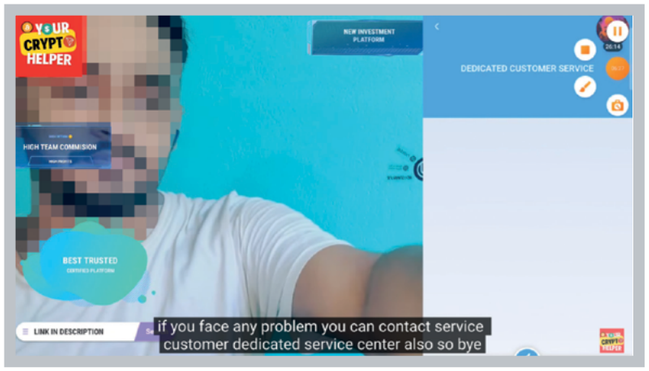


Figure 11: presenter shows viewers the existence of “dedicated customer service” functionality

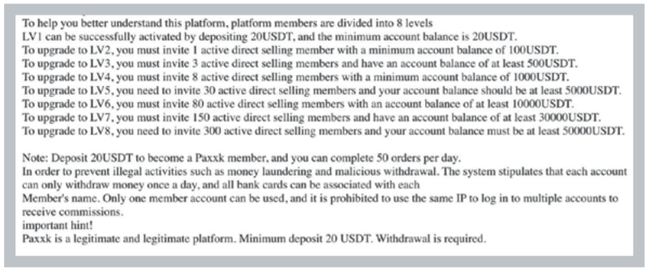
Based upon anecdotal evidence from people who have fallen for this scam, the customer service functionality does sometimes work. Supposedly, when your withdrawal doesn't go through and you contact customer service, they'll ask you to pay additional fees (which you also won't get back).

Some videos of this ilk include words from the presenter urging viewers to "do their own research and risk analysis before investing". These statements are probably designed to cover the channel owner from liability. However, such statements are moot when considering the fact that these content creators record and publish videos instructing people how to use sites that are specifically designed to steal money.

The paxxk[.]biz app contains a button labeled "Work Description" that presents the dialog depicted in Figure 12. Some interesting points in there are the fact that it costs 20 USDT to become a member and the fact that withdrawals are limited to once per day. It also states that "paxxk is a legitimate and legitimate platform" just in case you had had any doubts.

A "Company Profile" button opens the dialog depicted in Figure 13. What is written here is a guaranteed work of fiction. It is likely re-used in many other apps from the same creators.

Clicking on any item in the UI causes a troublesome "system notification" modal dialog (Figure 14) to block interaction until dismissed. This made navigation of the app tiresome after even a short amount of time.


To help you better understand this platform, platform members are divided into 8 levels
LV1 can be successfully activated by depositing 20USDT, and the minimum account balance is 20USDT.
To upgrade to LV2, you must invite 1 active direct selling member with a minimum account balance of 100USDT.
To upgrade to LV3, you must invite 3 active direct selling members and have an account balance of at least 500USDT.
To upgrade to LV4, you must invite 8 active direct selling members with a minimum account balance of 1000USDT.
To upgrade to LV5, you need to invite 30 active direct selling members and your account balance should be at least 5000USDT.
To upgrade to LV6, you must invite 80 active direct selling members with an account balance of at least 10000USDT.
To upgrade to LV7, you must invite 150 active direct selling members and have an account balance of at least 30000USDT.
To upgrade to LV8, you need to invite 300 active direct selling members and your account balance must be at least 50000USDT.

Note: Deposit 20USDT to become a Paxxk member, and you can complete 50 orders per day.
In order to prevent illegal activities such as money laundering and malicious withdrawal. The system stipulates that each account can only withdraw money once a day, and all bank cards can be associated with each
Member's name. Only one member account can be used, and it is prohibited to use the same IP to log in to multiple accounts to receive commissions.
important hint!
Paxxk is a legitimate and legitimate platform. Minimum deposit 20 USDT. Withdrawal is required.

Figure 12: paxxk[.]biz "Work Description" dialog

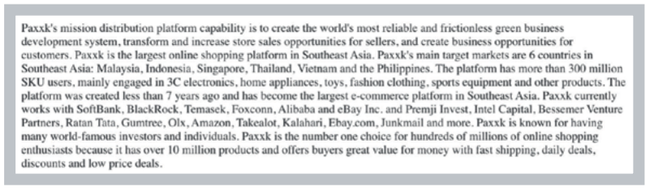

Paxxk's mission distribution platform capability is to create the world's most reliable and frictionless green business development system, transform and increase store sales opportunities for sellers, and create business opportunities for customers. Paxxk is the largest online shopping platform in Southeast Asia. Paxxk's main target markets are 6 countries in Southeast Asia: Malaysia, Indonesia, Singapore, Thailand, Vietnam and the Philippines. The platform has more than 300 million SKU users, mainly engaged in 3C electronics, home appliances, toys, fashion clothing, sports equipment and other products. The platform was created less than 7 years ago and has become the largest e-commerce platform in Southeast Asia. Paxxk currently works with SoftBank, BlackRock, Temasek, Foxconn, Alibaba and eBay Inc. and Premji Invest, Intel Capital, Bessemer Venture Partners, Ratan Tata, Gumtree, Olx, Amazon, Takealot, Kalahari, Ebay.com, Junkmail and more. Paxxk is known for having many world-famous investors and individuals. Paxxk is the number one choice for hundreds of millions of online shopping enthusiasts because it has over 10 million products and offers buyers great value for money with fast shipping, daily deals, discounts and low price deals.

Figure 13: Figure 13 paxxk[.]biz "Company Profile" dialog

Figure 14: paxxk[.]biz "system notification" modal dialog

Interestingly, this video and most others that were manually inspected during this research appear to use a form of "SEO" in their YouTube video description field. Examples from this video are presented in Figure 15. They likely represent interesting YouTube search criteria for future research around crypto scam video content.

A YouTube search for "paxxk[.]biz" retrieves dozens of videos. Figure 16 shows some descriptions which largely insinuate that the withdrawal functionality is real.

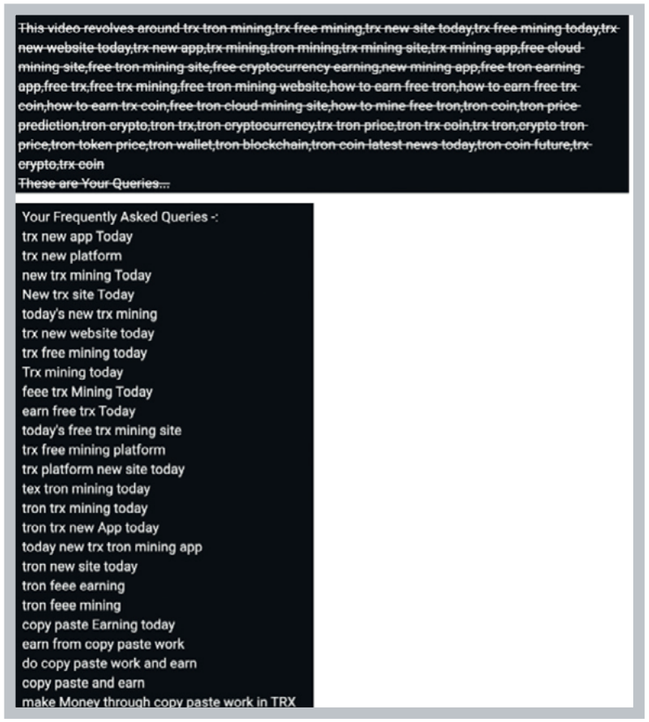


Figure 15: "SEO" embedded in video description

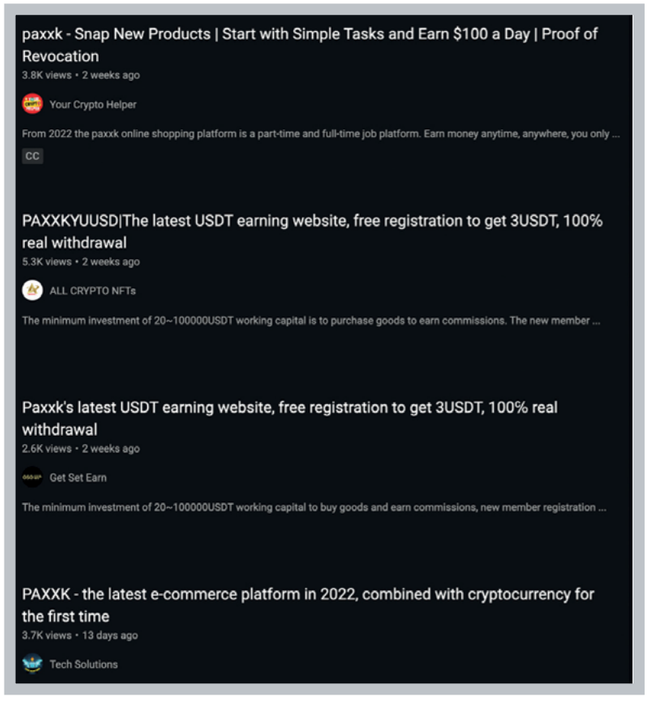


Figure 16: YouTube video descriptions pertaining to paxxk[.]biz

After scrolling past the 30 or so videos the YouTube web UI presented when searching for “paxxk[.]biz”, YouTube’s recommendation algorithm kicked in and provided a few additional suggestions, shown in Figure 17.

Similar USDT-based mining pool scams can be found by searching YouTube for the hashtag “#usdt-mining”, which reportedly contains 3.9k videos (Figure 18).

The next sections of this report will focus on analysis of YouTube videos and channels using data retrieved via the YouTube API[2] and pyyoutube[3] .

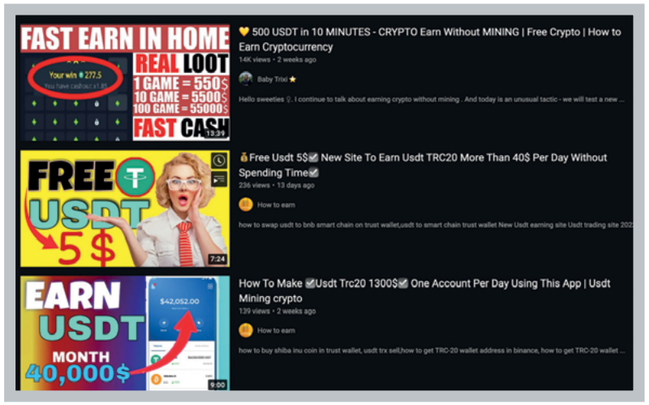


Figure 17: YouTube recommendations related to search for “paxxk[.]biz”

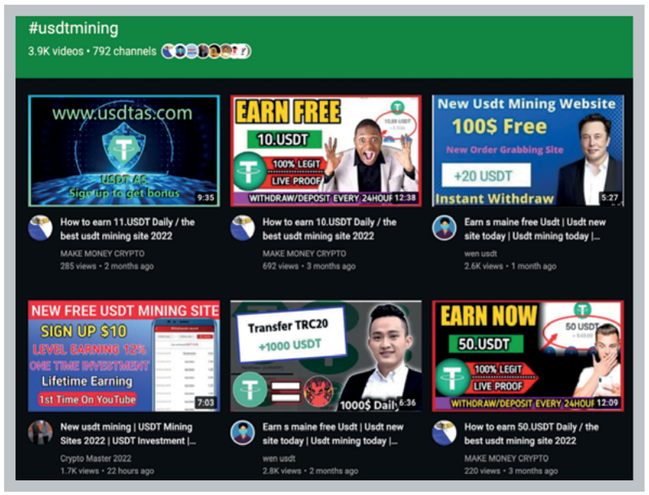


Figure 18: #usdtmining on YouTube reports 3.9k videos and 792 channels

2. https://developers.google.com/youtube/v3
3. https://github.com/sns-sdks/python-youtube

4. Analysis of YouTube activity related to paxxk[.] biz mining pool scam

Given that paxxk[.]biz is a textbook example of a USDT scam app, it seemed a perfect starting point for analysis of YouTube activity. A YouTube search (depicted in Figure 19) for “paxxk[.]biz” returns a handful of videos demonstrating how to use the app to make money.

Using api.search_by_keywords(q=keyword, count=100), 100 search items were returned that included 30 videos that string-matched “paxxk” in either title or description. All captured videos were found to be hosted on different channels. All were published between the 21st and 24th August 2022. These videos were presented in a variety of languages including English, languages from the Middle East, and languages from the Indian subcontinent. All but 6 of the videos included replies in their comments sections. The number of replies varied from 1 to 131. Basic statistics are depicted in Figure 20.

As depisicted in Figure 20, all channels involved have published multiple videos and have, in most cases, high numbers of both subscribers and viewers. One of the channels was identified to be a YouTube verified account with close to 600,000 subscribers and over 4 million total views.

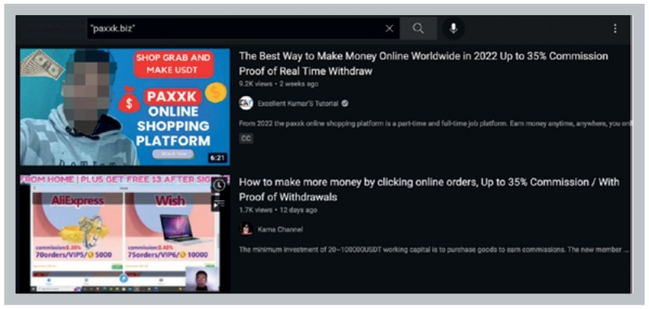


Figure 19: An example of the output of a YouTube search for “paxxk[.]biz”

Channel ID	Video ID	Views	Cmnts	Published	Subs	Vids	Viewers
UC9TzUJ06o2GCqBPk1AP8lmw	ycfUXscUi3Q	2689	63	2022-08-21	801	256	1250941
UCGVJMAJ7J_Pi6RlfqESeWWg	oyht4skBD4N	4327	9	2022-08-21	2200	118	348488
UC7si9rce8yAVRvV9TN0SrPA	O5cmj50pcSY	3705	5	2022-08-22	1230	183	581544
UC7VVNue41U7NOR0WZ_CQ0DQ	3rKg3wFW_Wg	1749	7	2022-08-23	17300	776	1068504
UCDMkHGb_DzSrIcnLtx_w-gg	zDN1V_KMPOU	3879	2	2022-08-21	54600	613	3659204
UCinKKc1lC50nDeigwlVSq8A	L7D5QglFJww	5397	2	2022-08-21	92000	368	1124710
UCrP1LJpdX19rvRm_DVsKhgA	OTTzzbO-GDU	2549	87	2022-08-21	18200	23	43600
UCwhC1WbLAv5JzmxrCx7P6Ag	OfQXiA5erVA	6696	97	2022-08-24	44000	24	166559
UC4NvK9V4C6qaJo79erpd__w	EioUN4KJNf4	762	131	2022-08-21	4150	43	84312
UCvWRQiyRF7qlDJQYSqjHGCA	Y1k-Lbxvohk	2566	2	2022-08-21	19200	271	612303
UC6tPgTOz8koRg2-6u8IKFVQ	2NjcmaPEoyg	9263	26	2022-08-22	599000	1957	41720461
UC0B9btAY_keFi_nuy4u893Q	ertucmgAbus	1158	20	2022-08-21	2160	285	363153
UCRn36PxKbIOceMCV6U8QtLw	2CoNfwQp_SI	7495	35	2022-08-21	45700	155	1869339
UCtcZoBa0ES050ked8-WIQiA	UMQ-k-2vG74	3347	0	2022-08-21	74600	38	209943
UCpuv8_j_nBiIP8rlbsUIvhg	sXrq0S8JDoA	10197	122	2022-08-22	33200	47	344526
UCs_txgMMuO7mF-pvrQ_MDKg	qbhMX0YkUL0	1941	0	2022-08-21	1040	111	347476
UCr--3YT-GWuyyMW7aE_IUoQ	Ep5NQEFKK7U	9881	41	2022-08-22	43500	54	1558230
UCmPzsglFiZW1TFR8DXoz4lg	PffFCmgp6EQ	3592	5	2022-08-22	3790	539	1417526
UCzQW4gmEBlo6YHsgnHGbBPQ	C1lmZne5KAE	3341	None	2022-08-23	3500	56	185280
UC-9CNfWoj56dKpiFckiTO9w	65ugHYJg9LM	10753	1	2022-08-22	2150	56	234597
UCHEn2099wK5beKBE_GrBVNA	rLFgb1fC2IQ	5528	27	2022-08-22	47900	99	1385162
UCQLODQhXGhSbe_9kKB8ZLJw	ooCqFYGLWeM	3522	0	2022-08-23	101	167	562811
UCo5uThofG2M5EJXY_oqblQw	nNnWE4q0T3k	1055	0	2022-08-21	31900	50	196462
UCauYiJbJa-nPBI7UPZ188QA	YGT6drSW5Gw	3638	8	2022-08-23	37500	29	62512
UC2OwRN8lrs8rke-MDegitvA	jRw6xaNkfrQ	1399	0	2022-08-22	1220	206	271099
UCic-PKOirfwL5KglKSlVwKA	GQhoI935EF8	1582	27	2022-08-23	5760	337	405888
UCMPcJI8c3_qRCS4ST0meLQw	j66VN2d0Roc	1298	12	2022-08-22	12500	727	1544504
UCwKmqux3lIWaC4Kc0xZPtrQ	YdMrs1_StvA	4753	28	2022-08-23	48200	250	6343548

Figure 20: Basic statistics of videos found using a YouTube search for “paxxk[.]biz”

The YouTube API was then used to obtain a list of all videos on each of the channels identified during the prior search. A total of 8,338 videos were found across the 30 accounts during this process. The API was subsequently used to obtain all top-level comments posted in reply to all 8,338 videos. A total of 8,016 of the threads included top-level replies, and 125,362 comments posted by 61,048 unique channels were obtained in this fashion. Figure 21 presents some statistics, including a list of the ten channels that received the most comments.

The channel that received the most comments is depicted in Figure 22. The account's name is "Excellent Kumar'S Tutorial". It is a YouTube verified account. Upon closer inspection it was determined that videos on both the "Excellent Kumar'S Tutorial" and "Your Crypto Helper" channels are presented by the same person. Most of the videos posted on "Excellent Kumar'S Tutorial" channel appear to be legitimate. However, videos posted on "Your Crypto Helper" are almost exclusively related to these scams. Likewise, many of the other YouTube channels posting these videos published at high volume and did not post about much else.

Analysis of YouTube channels that posted large numbers of comments led to the discovery that many of those accounts contained titles that included Telegram usernames. Figure 23 depicts a sample of those channel names.

```
Number of unique commenters 61048

Most received comments
Rcvd    Channel
44717   https://www.youtube.com/channel/UC6tPgTOz8koRg2-6u8IRTVQ      Excellent Kumar'S Tutorial
16918   https://www.youtube.com/channel/UC7VVNue4IU7MOR0WZ_CQ0DQ      Kama Channel
11944   https://www.youtube.com/channel/UC9TuUJ06o2GCqBPk1AP8lmw      Get Set Earn
11485   https://www.youtube.com/channel/UCkJZBjuwQGSbk-0dnYbodZw      Kwarta Online
4664    https://www.youtube.com/channel/UCr--3YT-GWuyyMW7aE_ZUoQ      BAKR YT
4406    https://www.youtube.com/channel/UC0B9btAY_keFi_nuy4u893Q      DONI-HTS
4299    https://www.youtube.com/channel/UCwKmqux3lIWsO4Kc0xZPttQ      TECH RAGE
4069    https://www.youtube.com/channel/UCMPcJI8c3_qRCS4ST0neLQw      EARNING CHOICE
3429    https://www.youtube.com/channel/UCnPZsg1FiZW1TFR8DXoz41g      Nice Tech
3277    https://www.youtube.com/channel/UCDMkHGb_DzSrIcnLtx_w-gg      Your Crypto Helper
```

Figure 21: statistics related to YouTube comments from accounts posting about paxxk[.]biz

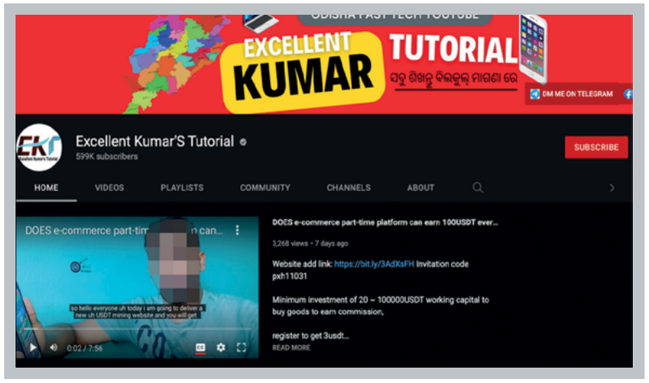


Figure 22: Top most commented channel related to paxxk[.]biz

```
Found 1029 channels mentioning telegram
29      UCTTVkLpcRpqw-ODna7q8_tg        Javier (REDDITHACKS ON TELEGRAM)
3       UCzNQWarCttgDp04fRK6oh4g        richard:::(fastcryptominings via telegram)
19      UCKHqocsCoY6FO-NVMPt-90g        ALI BRAINSCOTT001 ON TELEGRAM ]
23      UCphVv8D8_6AcV2z3iE616zg        *Wendytrad45*on telegram
33      UCGsCBfBwhK66237vNkT2Vvw        James Helped ME ..... Wendytrad45 ON TELEGRAM % A
1       UCX2-tedOn3JT90bMmLV2-1A        This stockcryptohack ON TELEGRAM
4       UCYjXZIOh0sYUSDs_t5kg4Jg        HACKERTHURAM ON TELEGRAM
4       UCGMHXpEc8qT6wWAzr1QcJUA        HACKERTHURAM ON TELEGRAM
2       UCe_beSrlIiY5mI7i2v1ePcQ        Text UNIVERSALTECH on Telegram
1       UCpMR4276kKededpG7X_0ZVA        HACKG401 ON TELEGRAM
15      UC6Ynq2f5QVL0KvP1Pb5xQiQ        Sheila.Philip_Hack on Telegram
4       UCNaZb0DUe675KPbuNWozj0A        BengHackercena on telegram
4       UC0W636Vu_LfTcYh5HxfBICg        Hackercena on telegram
4       UC1Q0_sR3QkLRHZqFRU4HuOw        James Reamlee on telegram
6       UCgPL4HsHxycTakVKqNDX9oQ        Jiban Clifweb on telegram
12      UCovRt28jl_hp0q4EPAP6xXA        Textstockcryptohack on telegram
3       UCK9Rwz-OGW1lcsSfmY_bhsg        Text VGminers ON TELEGRAM
4       UC-Hf7fHeaPR2cK_md2IgPVg        Netto*REALLY HACKER VINCENT02 ORIGINA ON TELEGRAM
```

Figure 23: Channel names from paxxk dataset that mention Telegram

Using some simple text processing and regular expression tricks, a total of 144 telegram usernames were extracted from this list. In most cases, a single Telegram username could be linked to dozens of individual YouTube channels. An example is depicted in Figure 24.

The number of posts on individual channels and videos for each set of accounts corresponding to a Telegram username was also counted. The results are depicted in Figure 25.

For the five most active Telegram users identified, a count of which channels they most frequently engaged with was then performed. A sample of the output is shown in Figure 26.

Finally, summing up all engagement from all Telegram users shows which YouTube channels are boosted the most by this group. This is depicted in Figure 27.

```
Found 144  telegram users responsible for 2370 comments.
463     wendytrad45
https://www.youtube.com/channel/UCmoPtPiV9dWAu0wYYVDnaXg       3
https://www.youtube.com/channel/UCFz5Xix5s9u0kk8efyCfZ6A       5
https://www.youtube.com/channel/UCqQTdvnDEb2LCh-oveoFR-A       20
https://www.youtube.com/channel/UCGExO0gm29ZHH9zbhQ-L6XA       22
https://www.youtube.com/channel/UCSXyZ_rPMaLb7ycnzbmSFyg       7
https://www.youtube.com/channel/UCSYByEL240jWeq3X_4cMZAg       23
https://www.youtube.com/channel/UCfaIShno43fd7aJRJh43t3w       3
https://www.youtube.com/channel/UCGsCBfBwhK66237vNkT2Vvw       33
https://www.youtube.com/channel/UCnIJ70iv9cQL9aTS7WA12qg       32
https://www.youtube.com/channel/UCg0SqHCCCy2Ju3csWwaKL3A       32
https://www.youtube.com/channel/UClzsxe177_3Kc_TtVuhHrIw       11
https://www.youtube.com/channel/UCWDweEH79dXhvJkz6LFQqTg       10
https://www.youtube.com/channel/UCTmpXGzDHpcidnjAyWPTbKA       39
https://www.youtube.com/channel/UCN2Axi_xArqq2VOA8K8-diw       26
https://www.youtube.com/channel/UCFvfS39cWYGpyto4TgbHMvA       19
https://www.youtube.com/channel/UCTFAvbJBWdQqzDvgvRIdHFQ       52
https://www.youtube.com/channel/UCx5gAmkjHh-pvT2-n6GXc-g       19
https://www.youtube.com/channel/UCZKfgvWU9jZ9ijT4DQCVDDA       20
https://www.youtube.com/channel/UCphVv8D8_6AcV2z3iE616zg       23
https://www.youtube.com/channel/UCr9CF_C9HfrddJGiR7hkz9A       28
https://www.youtube.com/channel/UCLxw5kFlWlU-2rRn6jpLbVQ       25
https://www.youtube.com/channel/UCV7VdcxgAiHStWR5W2WLdPw       7
https://www.youtube.com/channel/UCT6EtPtSvUjDB1W6CCSi6Ng       4
```

Figure 24: YouTube channels associated with Telegram username 'wendytrad45'

Telegram user	posts	chnls	vids
wendytrad45	463	25	257
easyworldweb	298	15	125
omlhacks	117	15	72
astrahack01	101	4	6
hackerrambosmart1	98	10	37
hackerpratik	90	7	27
brainscott001	69	13	65
vgminers	47	7	11
melley_hacks	46	13	35
kriptosai	35	8	13

Figure 25: Most active Telegram users in the paxxk[.] biz dataset

```
wendytrad45
105 "Your Crypto Helper"    https://www.youtube.com/channel/UCDMkHGb_DzSrIcnLtx_w-gg
96 "EARNING MONEY 89"    https://www.youtube.com/channel/UCGVJMAJ7J_Pi6R1fq8SeWWg
45 "Total Trx Earning"    https://www.youtube.com/channel/UC2OwRM8lrs8rke-MDegitvA
33 "Crypto Baba"    https://www.youtube.com/channel/UCvWRQiyRF7qlDJQYSqjHGCA
32 "EARNING CHOICE"    https://www.youtube.com/channel/UCMPcJI8c3_qRCS4ST0neLQw
21 "Crypto Leny"    https://www.youtube.com/channel/UCpuv8_j_nBiIP8rlbzUIvhg
17 "Crypto Earning Tricks"    https://www.youtube.com/channel/UCrPlLJpdXl9rvRm_DVsKhgA
14 "David - Nft, Crypto, Play to Earn - Defi"    https://www.youtube.com/channel/UCo5uIhofG2M5EJXY_oqblQw
13 "Excellent Kumar'S Tutorial"    https://www.youtube.com/channel/UC6tPgTOz8koRg2-6u8IRTVQ
12 "Kama Channel"    https://www.youtube.com/channel/UC7VVNue4IU7MOR0WZ_CQ0DQ

easyworldweb
114 "Your Crypto Helper"    https://www.youtube.com/channel/UCDMkHGb_DzSrIcnLtx_w-gg
70 "Total Trx Earning"    https://www.youtube.com/channel/UC2OwRM8lrs8rke-MDegitvA
26 "EARNING MONEY 89"    https://www.youtube.com/channel/UCGVJMAJ7J_Pi6R1fq8SeWWg
19 "EARNING CHOICE"    https://www.youtube.com/channel/UCMPcJI8c3_qRCS4ST0neLQw
18 "ALL CRYPTO NFTs"    https://www.youtube.com/channel/UCinKKc1lC60nDeigwlVSq8A
11 "Crypto Baba"    https://www.youtube.com/channel/UCvWRQiyRF7qlDJQYSqjHGCA
8 "Kama Channel"    https://www.youtube.com/channel/UC7VVNue4IU7MOR0WZ_CQ0DQ
6 "Excellent Kumar'S Tutorial"    https://www.youtube.com/channel/UC6tPgTOz8koRg2-6u8IRTVQ
6 "Kwarta Online"    https://www.youtube.com/channel/UCkJZBjuwQGSbk-0dnYbodZw
4 "David - Nft, Crypto, Play to Earn - Defi"    https://www.youtube.com/channel/UCo5uIhofG2M5EJXY_oqblQw

omlhacks
34 "Total Trx Earning"    https://www.youtube.com/channel/UC2OwRM8lrs8rke-MDegitvA
20 "Crypto Baba"    https://www.youtube.com/channel/UCvWRQiyRF7qlDJQYSqjHGCA
13 "TECH RAGE"    https://www.youtube.com/channel/UCwKmqux3lIWsO4Kc0xZPttQ
9 "Your Crypto Helper"    https://www.youtube.com/channel/UCDMkHGb_DzSrIcnLtx_w-gg
9 "ALL CRYPTO NFTs"    https://www.youtube.com/channel/UCinKKc1lC60nDeigwlVSq8A
8 "Kama Channel"    https://www.youtube.com/channel/UC7VVNue4IU7MOR0WZ_CQ0DQ
8 "EARNING CHOICE"    https://www.youtube.com/channel/UCMPcJI8c3_qRCS4ST0neLQw
```

Figure 26: Accounts most engaged by most active Telegram users' YouTube channels

```
Telegram boosted
321 "Your Crypto Helper"    https://www.youtube.com/channel/UCDMkHGb_DzSrIcnLtx_w-gg
164 "EARNING MONEY 89"    https://www.youtube.com/channel/UCGVJMAJ7J_Pi6R1fq8SeWWg
152 "Total Trx Earning"    https://www.youtube.com/channel/UC2OwRM8lrs8rke-MDegitvA
76 "Crypto Baba"    https://www.youtube.com/channel/UCvWRQiyRF7qlDJQYSqjHGCA
59 "EARNING CHOICE"    https://www.youtube.com/channel/UCMPcJI8c3_qRCS4ST0neLQw
34 "Kama Channel"    https://www.youtube.com/channel/UC7VVNue4IU7MOR0WZ_CQ0DQ
33 "David - Nft, Crypto, Play to Earn - Defi"    https://www.youtube.com/channel/UCo5uIhofG2M5EJXY_oqblQw
32 "ALL CRYPTO NFTs"    https://www.youtube.com/channel/UCinKKc1lC60nDeigwlVSq8A
22 "Crypto Leny"    https://www.youtube.com/channel/UCpuv8_j_nBiIP8rlbzUIvhg
21 "Excellent Kumar'S Tutorial"    https://www.youtube.com/channel/UC6tPgTOz8koRg2-6u8IRTVQ
```

Figure 27: Channels most boosted by accounts belonging to Telegram users in the paxxk dataset

If you scroll through “reply” sections on any video “boosted” by these Telegram users, you’ll see many comments designed to make viewers think that what is being demonstrated in the video is legitimate. Most of those comments are posted by accounts that mention Telegram usernames in their channel name. An example is shown in Figure 28.

When visiting accounts that are boosted by these Telegram users, YouTube displays a list of other uploaded videos from the same author. These are often videos linked to other scam apps. An example from the “PSEB STUDY HALL” channel is shown in Figure 29. As you can see in the screen-shot, the list of such apps goes on and on. New ones are added daily. This high rate of turnover prevents potential victims from looking up these URLs on “known scam” services.

A Twitter search for URLs shown in Figure 29 was performed. Only one tweet was found, depicted in Figure 30. During the period in which this research was performed it was rare to find malicious links on Twitter.

A node-edge graph of all comment interactions in the dataset is presented in Figure 31.

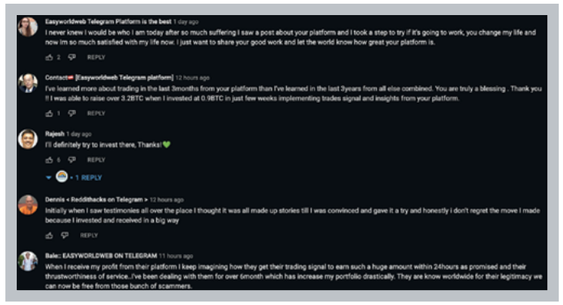


Figure 28: A sample of comments published by accounts associated with identified Telegram users

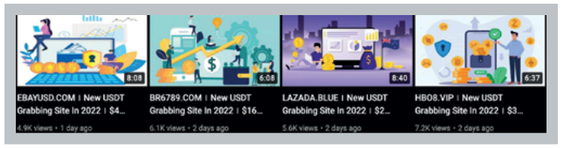


Figure 29: Other uploads on the “PSEB STUDY HALL” channel

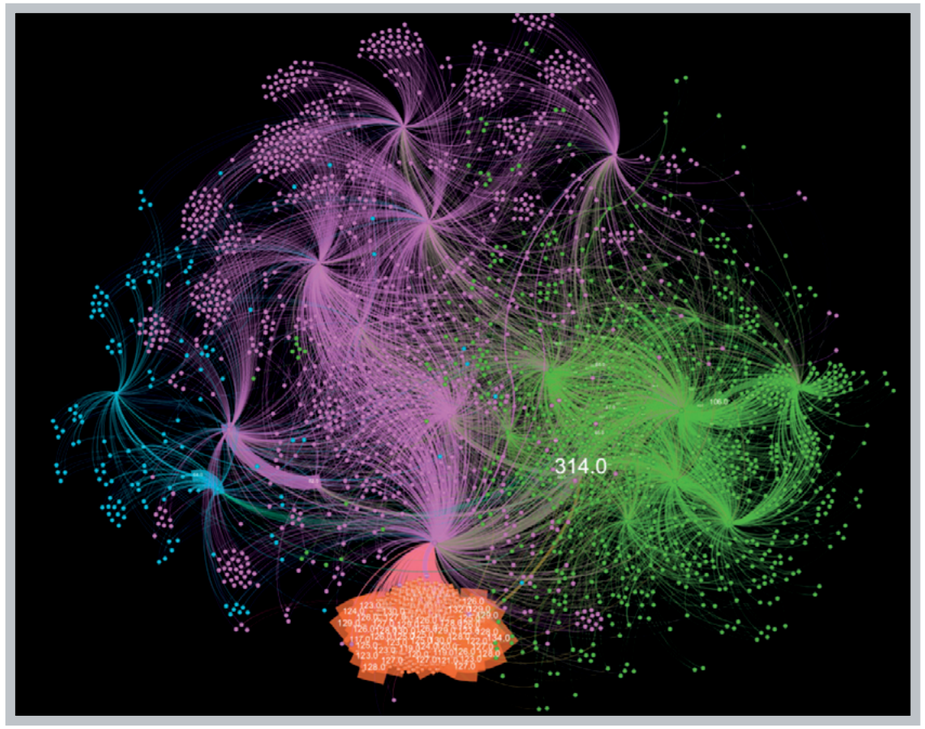


Figure 31: Node-edge graph of interactions in the paxxk dataset. Nodes are labelled by weighted out degree. The higher the number, the more comments the account published.

The green node labelled 314.0 is the account that posted the most comments in this dataset. It is depicted in Figure 32. The channel hosts no videos and was only used to publish comments.

The orange cluster of accounts with comment counts between 110 and 140 represent a small group of YouTube channels that published most of their comments to two channels, one called “Get Set Earn” – depicted in Figure 33 and another called “EARNING STORE”.

The accounts involved in this boosting behavior did not belong to the previously identified Telegram users. A list of YouTube channel names is presented in Figure 34.

It is not possible to clearly visualize nodes on the graphviz related to identified Telegram users due to the highly distributed nature of their boosting activities.

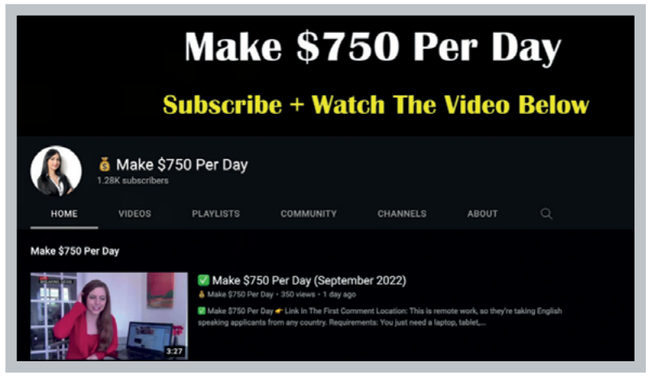


Figure 32: Most actively commenting YouTube channel in the paxxk dataset

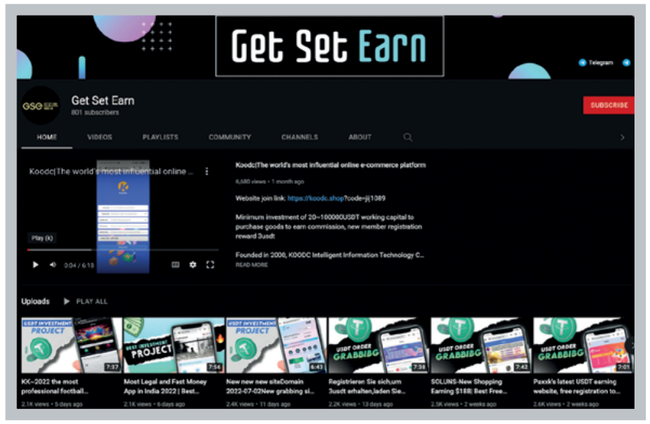


Figure 33: Get Set Earn channel, boosted by hundreds of comments from a handful of accounts

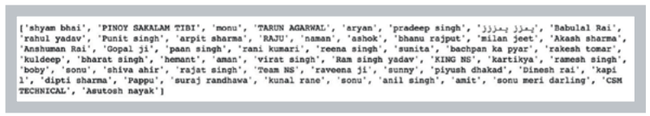


Figure 34: Accounts that boosted Get Set Earn and EARNING STORE channels

5 Analysis of YouTube activity related to ocitt[.] site mining pool scam

A similar scam was identified using the url: ocitt[.]site. Using the same analysis methodology as for paxxk[.]biz, a set of observations were recorded. Using api.search_by_keywords(q=keyword, count=100), 100 search items were returned that included 77 videos posted by 73 channels that string-matched "ocitt" in either their title or description. All videos were published between the 16th and 24th August 2022. This represents a slightly larger volume and longer-run campaign than the one that ran for the paxxk[.]biz app. A sample of gathered statistics from videos with the highest view counts is depicted in Figure 35. Note how comment counts do not correlate with view counts in any meaningful way.

As with the paxxk example, all channels involved in pushing this scam have published multiple videos and have, in most cases, high numbers of both subscribers and view counts.

The YouTube API was then used to obtain a list of all videos on each of the 73 channels identified during the prior search. A total of 15,221 videos were found during this process. The API was subsequently used to obtain all top-level comments posted in reply to all 15,221 videos. A total of 264,277 comments from 130,106 unique channels were obtained in this fashion. Figure 36 presents some statistics, including a list of the ten channels that received the most comments.

Channel ID	Video ID	Views	Cmnts	Published	Subs	Vids	Viewers
UC4K0Ze3Tr_iDl_qtPNanuZw	_gjlfl3utnY	12220	369	2022-08-16	2020	248	627578
UC_s2OtON8cD3rQz_U0Q0ySw	VjAL2RfUZlU	7915	None	2022-08-18	239000	83	15211705
UCRn36PxKbIOceMCV6U8QtLw	j0lxi7ayQEU	7470	24	2022-08-16	45700	155	1869369
UCGKTQtqqlE9zBjWN6JgmRKA	vqklL2f1HDk	6025	64	2022-08-20	18600	153	2866382
UC_53feOHVRuduclAHqHgmzg	xP8kUKnfTJU	5160	36	2022-08-18	82800	129	893934
UCK58quY8d4iPVS3Ao5h-zIg	NEj5mzzXvA8	5082	24	2022-08-19	14900	20	79413
UCinKKc1lC60nDeIgwlvSqBA	xubL5snhncU	5081	8	2022-08-19	92000	370	1138776
UCF8oxtkfrnCs0-udSXd-LcQ	zzckxVkt4Gw	4909	28	2022-08-24	55900	38	413130
UCo5uIhofG2M5EJXY_oqblQw	LeIueMdk-vE	4887	None	2022-08-17	31900	50	201629
UClqJaMIbEqabckP1bkWebtg	ENZ3_HXs-ys	4744	6	2022-08-17	20900	47	177345
UCcgJFA7dRbatqUTT94oBZMg	Gum6lgaF4n0	4680	45	2022-08-20	55600	24	95026
UChp4OjvAES-tpl40sMtqrqQ	SgUphOudkWs	4230	3	2022-08-17	59000	38	108487
UCPz_QP68j-CKv9vOBhgLUSg	Jk7s6PrNqKg	4136	13	2022-08-22	8440	194	877417
UCatIAIt9ykgA2xlo7ueWw	zJ1RvzGP6Ik	3921	16	2022-08-19	3980	132	1704413
UCGVJMAJ7J_Pi6R1fq8SeWWg	GgfCr4mNiew	3876	44	2022-08-21	2210	123	359993
UC5MgZ5ljEVH7i_EvqvHCOFA	rfJgznGzwKk	3858	151	2022-08-18	36600	444	1496236
UC-Jg6Hddd8Ajx6xprqWvvvw	xZrMiL1zN0U	3839	None	2022-08-23	9300	254	882518
UCDMkHGb_DzSrIcnLtx_w-gg	Fg2j9rFNYQY	3763	2	2022-08-19	54600	620	3676826
UCl7OU5apCuzRBYfeHJ9R46Q	tjxwZXwiIRU	3678	64	2022-08-18	14300	96	350015
UCzQW4gmBBloGYHsgnKGbBFQ	OPT8_hAOUBA	3618	None	2022-08-19	3500	61	199238
UCtiqOlsEmKZGw8nDOhD7hnw	111Pk4bbcoA	3538	8	2022-08-17	66600	1262	5280694
UCyelPy8CLhjaiBscnJkVTzQ	KB0lwzzaDNM	3219	40	2022-08-16	12300	203	627295
UCLEyppLtagEolbogNuOckxA	WD93N671cdc	3104	14	2022-08-16	1270	211	1157880
UC6Y8_swmuqviOfAdullFiWA	LK-CI9GAgAc	3046	0	2022-08-17	2140	579	1288418
UC6ciSqAKPhc6uXrX5cMC6KQ	M6lGLDkiaTM	2897	25	2022-08-21	60600	663	3327313
UCic-PKOirfwL5KqlKIlVwKA	IsOIx9A81zM	2755	29	2022-08-17	6530	339	411841
UCc-2CpQG7q3X7NTwH9tax9Q	tXDq6jf8H-8	2531	72	2022-08-20	18900	235	1196935
UC6P0OH9tKKFpch2wlH4ZY3A	nDB9cmiI55A	2388	3	2022-08-18	4480	241	823135

Figure 35: Statistics on videos related to ocitt[.]site with high view counts

```
Total videos: 15221
Total comments: 264277
Number of unique commenters 130106

Most received comments
Rcvd    Channel
68814   https://www.youtube.com/channel/UCvSz-jc007bzJ4Bo5ZwlYkA
30623   https://www.youtube.com/channel/UCtiqOlsEmKZGw8nDOhD7hnw
16945   https://www.youtube.com/channel/UC7VVNue4IU7MOR0WZ_CQ0DQ
13439   https://www.youtube.com/channel/UC5MgZ5ljEVH7i_EvqvHCOFA
10010   https://www.youtube.com/channel/UChc1UCPKf206lD_KDoOsAWg
9994    https://www.youtube.com/channel/UCM3YZaateudYcTCvROAE7Ig
7882    https://www.youtube.com/channel/UC6ciSqAKPhc6uXrX5cMC6KQ
7295    https://www.youtube.com/channel/UCc-2CpQG7q3X7NTwH9tax9Q
7162    https://www.youtube.com/channel/UC4K0Ze3Tr_iDl_qtPNanuZw
6534    https://www.youtube.com/channel/UCoNGK1ktBEU5rn3fIGT-uDA
```

Figure 36: statistics related to YouTube comments from accounts posting about ocitt[.]site degree. The higher the number, the more comments the account published.

The channel that received the most comments in this dataset was "Offer Tricks", a YouTube verified account, depicted in Figure 37.

A set of 177 Telegram users was found from commenters in this dataset. The list of most active ones closely resembled the list gathered from the paxxk dataset and is shown in Figure 38.

Channels that were most commented on by Telegram users is displayed in Figure 39. This list has significant overlap with the one extracted from the paxxk dataset. "Your Crypto Helper" is on the top in both, and one might at this point extrapolate that the person behind that channel is one of the Telegram users.

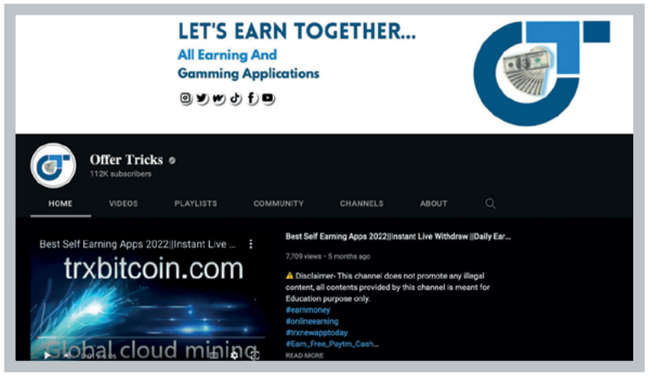


Figure 37: "Offer Tricks" account, the most commented on account in the ocitt dataset

Telegram user	posts	chnls	vids
wendytrad45	962	42	520
easyworldweb	654	39	243
brainscott001	472	45	349
hackerrambosmart1	351	23	110
omlhacks	288	29	165
hackerpratik	256	21	77
astrahack01	247	10	14
reddithacks	135	24	89
vgminers	78	12	18
melley_hacks	71	25	51

Figure 38: Most active Telegram users in the ocitt dataset

```
Telegram boosted
671 "Your Crypto Helper"   https://www.youtube.com/channel/UCDMkHGb_DzSrIcnLtx_w-gg
529 "NIXON Cryptofy"   https://www.youtube.com/channel/UCotXIHQmD9s5NrFiexyBUXQ
486 "TIGER EARNING"   https://www.youtube.com/channel/UC5MgZ5ljEVH7i_EvqvHCOFA
463 "Crypto Master 2022"   https://www.youtube.com/channel/UCtiqOlsEmKZGw8nDOhD7hnw
451 "SV Earning"   https://www.youtube.com/channel/UC6P0OH9tKKFpch2wlH4ZY3A
427 "Tricky Boss"   https://www.youtube.com/channel/UCc-2CpQG7q3X7NTwH9tax9Q
370 "EARNING MONEY 89"   https://www.youtube.com/channel/UCGVJMAJ7J_Pi6R1fq8SeWWg
216 "The School Crypto"   https://www.youtube.com/channel/UCoNGK1ktBEU5rn3fIGT-uDA
207 "Crypto Deniz"   https://www.youtube.com/channel/UChjIB17ZoIOOxrf29mnjlvw
204 "Intelligent AJK"   https://www.youtube.com/channel/UCXfEPYOQTb8vwEbgCefADUA
```

Figure 39: Channels most boosted by accounts belonging to Telegram users in the ocitt dataset

6 Analysis of YouTube activity related to #usdtmining YouTube hashtag

A YouTube page containing the hashtag #usdtmining can be displayed via the web UI. The page, which is depicted in Figure 40, reports that the hashtag represents 3.9k videos and 792 channels. This page can be displayed using the url: https://www.youtube.com/hashtag/usdtmining

Unfortunately, the YouTube API cannot be used to list items on a hashtag page, so search functionality had to be used to obtain results. Our results significantly differ from those shown in Figure 40. The YouTube API imposes a daily usage quota of 10,000 operations. A single search query consumes 100 operations, and via experimentation it was determined that 25 search results use up that 100-quota block. This restricts searches to a maximum of 2,500 results. Given that the hashtag page displayed in the web UI reported 3.9k videos, it was assumed that it would not be possible to retrieve them all via the API. A test search in the form api.search_by_keywords(q=keyword, count=1000) was performed which returned 527 videos of which 520 included the term “usdt” in either the video title or description. A total of 269 channels were identified during this search. Given the large number of channels found, additional videos for each channel were not harvested. However, top-level comments on all videos returned by the initial search were captured using the API.

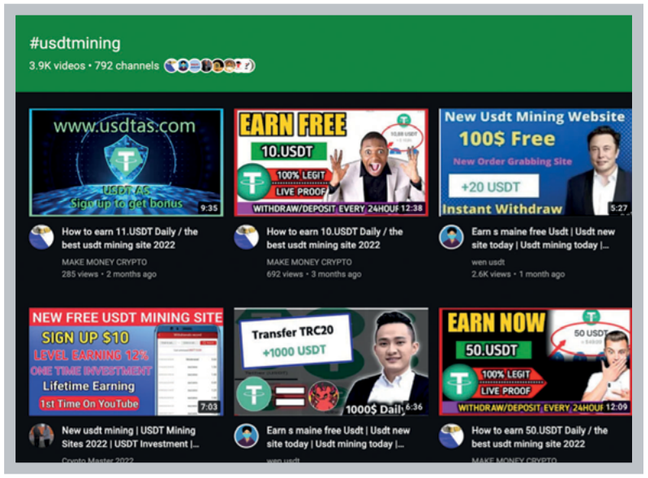


Figure 40: YouTube #usdtmining results page as shown by the web UI

Channel ID	Video ID	Views	Cmnts	Published	Subs	Vids	Viewers
JC4Yd3QgrLqdbGJDpc3hicuA	Lk5F8jtW2PM	50613	401	2022-05-27	162000	53	15742568
JCF0LLOE6RD6Dsha9a2dP41Q	iNT9a_HprFc	30811	342	2021-11-27	45500	82	1299686
JCjlhT4MaDflPnjL52VtNMfg	pd83osrNG-U	22822	102	2022-08-03	612000	59	21040671
JCnJaUeiea9qfaKTj4Ihsq3Q	4AukcWwQ9C4	22284	143	2022-05-07	566000	730	15419718
JCUwsqySjGexPTBcshNPYO-w	CBlznZGKMxA	20847	285	2022-08-25	95100	31	494666
JCgsbpLB2440VD2LpNmIv_kg	OI4O3xKdx_k	20648	1	2022-06-17	22800	90	928720
JCJOPyaxbwGbjaEYjynuDm6Q	Y6jOuENLzs	17130	103	2022-01-23	15600	545	1066668
JCSonJpwwfq0sRX_Wge384NQ	zlPC2zbh4mY	16121	180	2022-09-01	104000	82	47987935
JCvBhujfY4vmNyMVLOEv8Bdw	GLqRj6eoI20	16015	141	2022-09-03	117000	49	1187093
JC3jK2nntdzF88CXGOljxC8Q	gJCOAcn4aic	14762	114	2022-09-01	44700	143	2135235
JCe8N6UGOfByC5gSzizakk7w	f-NrfWB8R8Q	13511	30	2022-07-12	252000	68	50615198
JCvJCo6Kct9VCIh5eSi9k5vA	Yuimo99otjo	12479	68	2022-09-01	16000	22	4499616
JC4tPgYOz8koRgJ-6u8IRTVQ	h42N5MKk5Yg	11452	142	2022-08-04	599000	1957	41723231
JChB3zI7XRpPcbjRk5J87gKg	XjBGCC_a2x8	11431	0	2022-03-16	289000	205	1011777
JCXMdcXX0cVR0IvGQaxAgD2w	nHCmj2W9uu4	10075	28	2022-07-02	105000	62	764818
JCh1VxSowMoBvLgSdcLiLWOA	LjNBSb7gWNE	9032	105	2022-06-21	102000	292	6909772
JCODOAYz6tjpC-T0ZIKl7hsQ	VrS-_lxcocQ	8728	3	2022-03-20	1570000	929	44130437
JCtyTfyxD_mJ_XCyB26qmavg	Y2NBPi5GuqQ	8256	4	2022-04-14	219000	822	26061880
JCHs3YP9163VlvBPQPnWARrw	_ZlvZ26emHA	8090	83	2022-09-03	79800	101	512036
JCAw66QhuMDQ3T3hH5bS1bjA	Gi2zgOxadhw	8029	3	2022-05-14	54000	109	1576043
JCVKGHYD5pUE7poBFUcRXF9A	AobR_AKLIh0	8014	14	2022-04-20	5440	23	154419
JCNpS8YopW8gjoaNpQnl1yRA	7XpviE33Jns	7727	8	2022-05-03	1070	69	428691
JCa9NnloM5rkKaObMlUhw9Lg	tjsjTqJ46sI	7463	74	2022-04-24	3790	131	128545
JCRQ4EAAkCb09SXzU8U2QDlg	UJWVdgskG7o	7295	15	2022-06-29	46200	59	432784
JCexDgaONEXi0Gzy1dhZAPSw	mjF579B-mGO	7267	5	2022-07-21	368	197	829907

Figure 41: Statistics on videos related to #usdtmining with high view counts

A total of 11,710 comments were harvested. Statistics are presented in Figure 41.

A total of 11,710 comments from 5,256 unique channels were obtained in this fashion. Note that only 485 of the videos contained comments. Figure 42 presents some statistics, including a list of the ten channels that received the most comments.

A node-edge graph of interactions between channels captured in the #usdtmining dataset is presented in Figure 43. Nodes are labelled by in-degree – the number of incoming comments. This graph illustrates that many of the videos in the #usdtmining hashtag received comments from entirely separate groups of accounts. The mess in the middle of the graph shows where overlap between commenters happened.

```
Total videos: 485
Total comments: 11710
Number of unique commenters 5256

Most received comments
Rcvd    Channel
716     https://www.youtube.com/channel/UCtiqOlsEmKZGw8nDOhD7hnw
549     https://www.youtube.com/channel/UCJNGmfZWw3TBnI0Vt4ExhFw
486     https://www.youtube.com/channel/UCRpItF2j5jeWfstw4hLw3Gg
365     https://www.youtube.com/channel/UCwBhujfY4vmNyMVLOEv8BdW
352     https://www.youtube.com/channel/UC5-o_QDw3BB_yQkmJuDa_Zw
324     https://www.youtube.com/channel/UCUwsqySjGexPTBcshNPYO-w
301     https://www.youtube.com/channel/UCAFv7ueHe3lBixUDw-uaeHA
266     https://www.youtube.com/channel/UCODOAYz6tjpC-T0ZIKl7hsQ
260     https://www.youtube.com/channel/UCSonJpwwfq0sRX_Wge384NQ
249     https://www.youtube.com/channel/UCDMkHGb_DzSrIcnLtx_w-gg
```

Figure 42: Statistics related to YouTube comments from the #usdtmining dataset

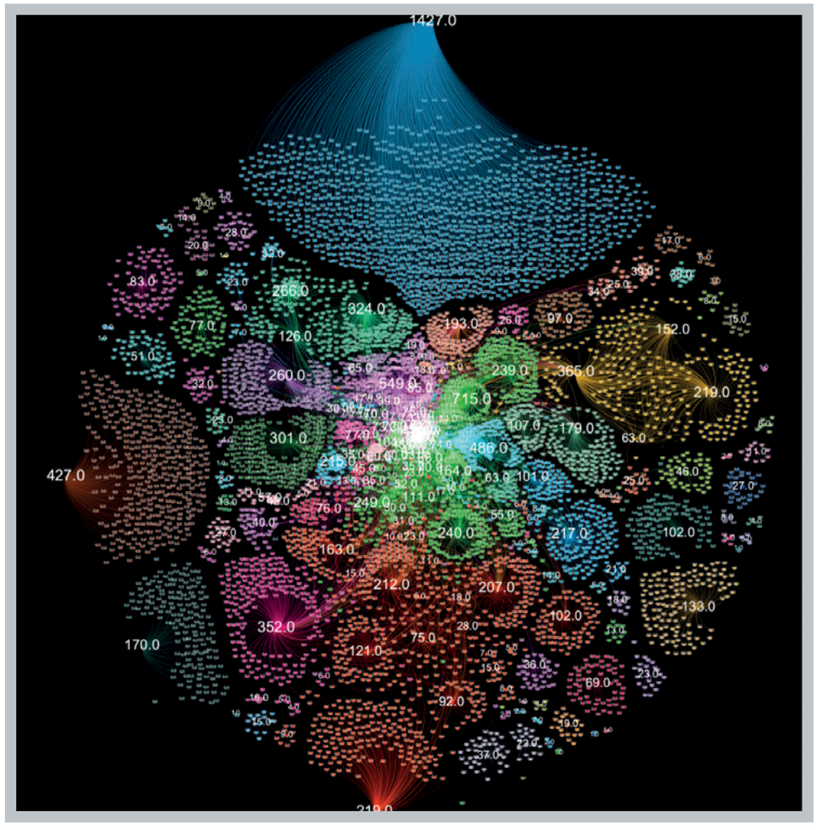


Figure 43: Node-edge graph of interactions in the #usdtmining dataset. Nodes are labelled by in-degree

The channel that received the most comments in this dataset was “Crypto Master 2022”, depicted in Figure 44. Not a verified account this time.

A total of 92 Telegram account names were found from YouTube channel names in this dataset. They were responsible for posting 1,554 comments. A list of the ten most active Telegram users is presented in Figure 45.

A list of the ten accounts that received most comments from Telegram users is shown in Figure 46. The overlap with previous lists is quite evident.

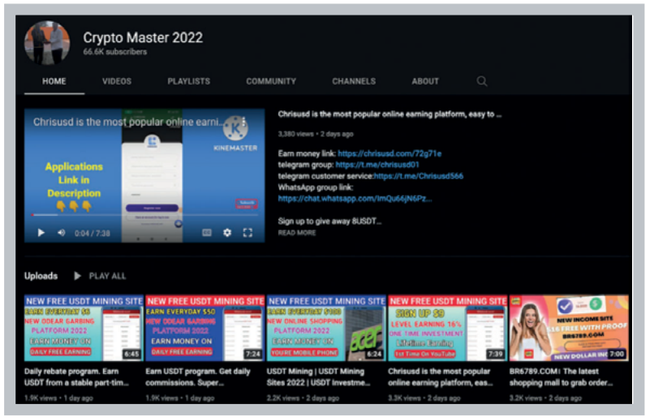


Figure 44: Crypto Master 2022” account, the most commented on account in the usdtmining dataset

Telegram user	posts	chnls	vids
wendytrad45	350	92	170
hackerrambosmart1	270	51	83
hackerpratik	185	31	50
easyworldweb	159	32	56
omlhacks	69	28	47
astrahack01	62	3	3
reddithacks	49	27	39
rightsidehack	39	14	20
crypto_topzy	38	17	20
cirominginghack	37	2	3

Figure 45: Most active Telegram users in the #usdt-mining dataset

```
178 "Crypto Master 2022"   https://www.youtube.com/channel/UCtiqOlsEmKZGw8nDOhD7hnw
172 "MINING BOI"   https://www.youtube.com/channel/UCJNGmfZWw3TBnI0Vt4ExhFw
101 "PSEB STUDY HALL"   https://www.youtube.com/channel/UCRpItF2j5jeWfstw4hLw3Gg
86 "Your Crypto Helper"   https://www.youtube.com/channel/UCDMkHGb_DzSrIcnLtx_w-gg
56 "Inside Earner"   https://www.youtube.com/channel/UC5-o_QDw3BB_yQkmJuDa_Zw
52 "Earning day"   https://www.youtube.com/channel/UCNeByWhsQ9CHIfP-C54VwVw
47 "Golden Crypto"   https://www.youtube.com/channel/UCDWftLCMxVViH9urcoEXK8Q
47 "Earning Mantra"   https://www.youtube.com/channel/UCwBhujfY4vmNyMVLOEv8Bdw
45 "TIGER EARNING"   https://www.youtube.com/channel/UC5MgZ51jEVH7i_EvqvHCOFA
42 "EARNING MONEY 89"   https://www.youtube.com/channel/UCGVJMAJ7J_Pi6R1fq8SeWWg
```

Figure 46: Channels most boosted by accounts belonging to Telegram users in the usdtmining dataset

7. Additional analysis

It is easy to observe that the accounts boosted by Telegram users post a great deal of videos related to these scams. Figure 47 shows a sample of videos hosted by the “PSEB STUDY HALL” channel. Note how the number of views on each video in the screenshot is similar (between 6k and 10k). It can be assumed that other forms of inauthentic activity (such as fake likes, views, and subscribes) are being used, in addition to the comments posted by Telegram users, to boost engagement. Such actions make these videos more likely to be recommended by YouTube’s algorithms.

Figure 48 shows a sample of videos hosted by “Crypto Master 2022”. Although Crypto Master 2022 was “boosted” more than PSEB STUDY HALL, the number of views on videos in the screen-shot varied quite dramatically.

Also of note is the fact that these channels post multiple videos advertising the same scam apps as shown in Figure 49. Thumbnails and video durations indicate that these are always re-uploads of the original video.

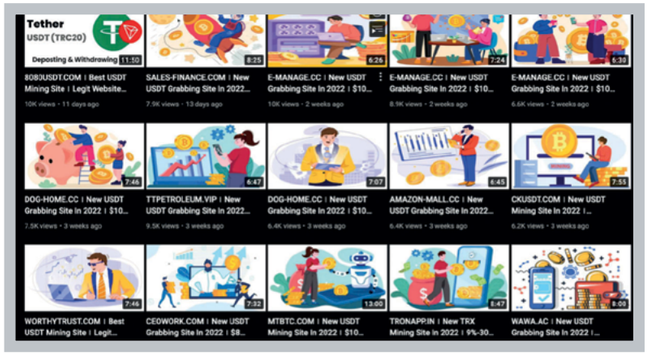


Figure 47: Videos uploaded to the PSEBSTUDYHALL YouTube channel

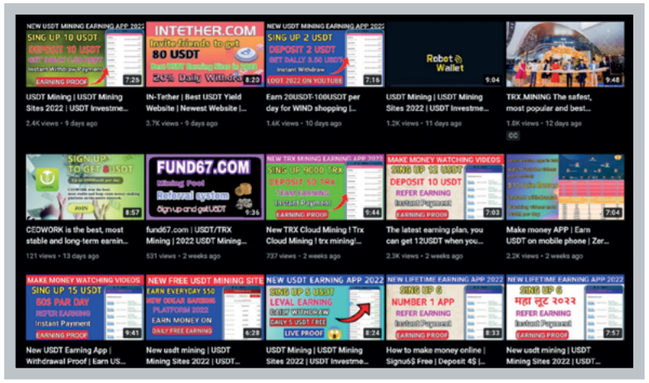


Figure 48: Videos uploaded to the CryptoMaster2022 YouTube channel

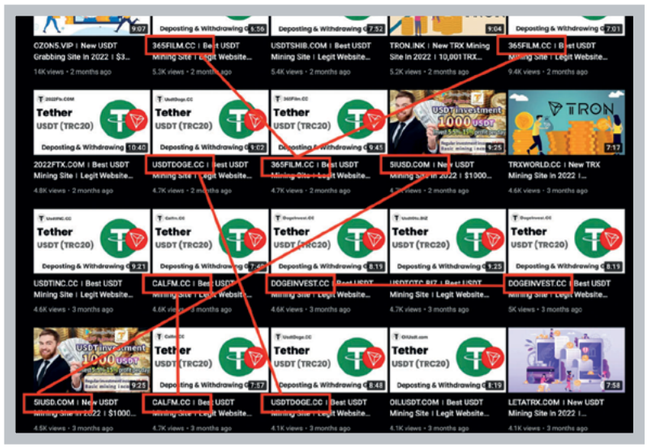


Figure 49: Video duplication via re-uploading (PSEB STUDY HALL channel)

While performing this research it was evident that many channels involved changed their channel name regularly. For instance, the “TIGER EARNING” channel renamed to “Crypto With Earning”. Tracking these channels using their YouTube channelId allows name changes to be followed.

URLs were extracted from titles and descriptions of videos obtained from all three datasets. A total of 700 unique app URLs were obtained in this way. Figure 50 presents statistics for a top sample of the obtained URLs that includes campaign start and end dates, duration in days, and number of videos posted. The consistency in number of videos from about a third of the way down the list – fifteen give or take a few – likely indicates the size of the regular group of channels posting videos as new scam apps are created.

Comments associated with channels associated with Telegram users were harvested. For each user, comments were grouped by the first 40 characters found. This allowed near-identical comments to be discovered. All Telegram users published near-identical comments over and over across multiple videos. Sometimes the same comment was posted multiple times in response to the same video. Figure 52 and Figure 53 depict the copy-paste nature of comments posted by two Telegram users.

URL	Start	End	Duration	Videos
898trx.com	2021-01-23	2022-05-20	481	154
trxzdh.com	2022-03-19	2022-06-12	84	69
mallusdt.com	2022-08-21	2022-09-03	13	40
usdtrr.org	2022-06-23	2022-08-06	44	35
usdtgroup.top	2022-07-24	2022-08-31	38	34
paxxk.biz	2022-08-20	2022-08-23	3	25
peacetrx.com	2022-07-10	2022-07-31	21	22
ebayusd.com	2022-08-30	2022-09-05	6	22
usdt67.com	2022-08-30	2022-09-05	6	21
saweria.co	2022-08-24	2022-09-05	12	18
5iusd.com	2022-05-20	2022-07-13	54	17
trxroom.com	2022-06-29	2022-07-04	5	17
trxmux.com	2022-05-07	2022-06-12	36	16
trxfh.cc	2022-04-27	2022-05-22	25	15
br6789.com	2022-09-01	2022-09-04	3	15
gbostore.com	2022-08-29	2022-09-06	8	15
bvtron.com	2022-09-04	2022-09-05	1	15
trxcft.com	2022-03-23	2022-05-09	46	14
trxrain.com	2022-07-10	2022-07-17	7	14
vcvtrx.com	2022-06-20	2022-06-23	3	14
trx.lol	2022-04-10	2022-05-06	26	14
trx.online	2022-03-15	2022-04-22	37	14
trxl.love	2022-04-04	2022-04-29	25	13
earnshope.com	2022-08-29	2022-09-06	8	13

Figure 50: Most seen URLs from video titles and descriptions captured in all three datasets

Figure 51: Channels associated with each scam app URLt

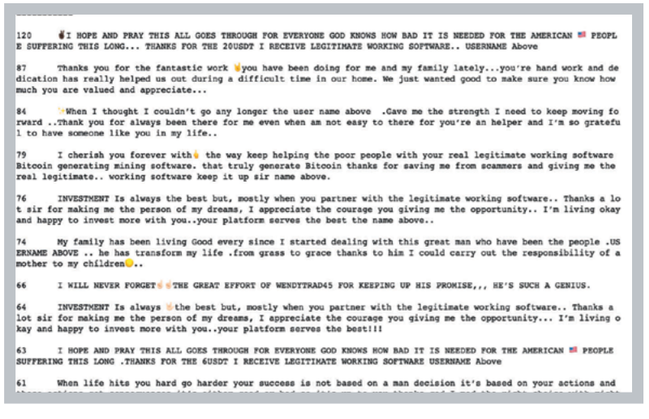


Figure 52: Comments from wendytrad45 by similarity of first 40 characters. The number to the left indicates how many times that exact comment was seen in the data

As an aside, the hashtag #USDTMINING was found on Twitter. It was being used to indirectly advertise USDT mining pool scams. Tweets posted by accounts with female avatars ask people to direct message them to learn how to mine USDT. All tweets were published at about the same time, and were identical in content, suggesting that automation was used. A sample of such tweets is presented in Figure 54. A #miningusdt hashtag also exists on Twitter.

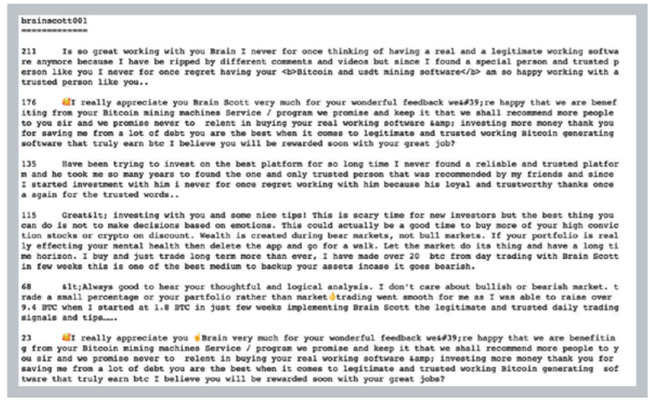


Figure 53: Comments from brainscott001 by similarity of first 40 characters. The number to the left indicates how many times that exact comment was seen in the data

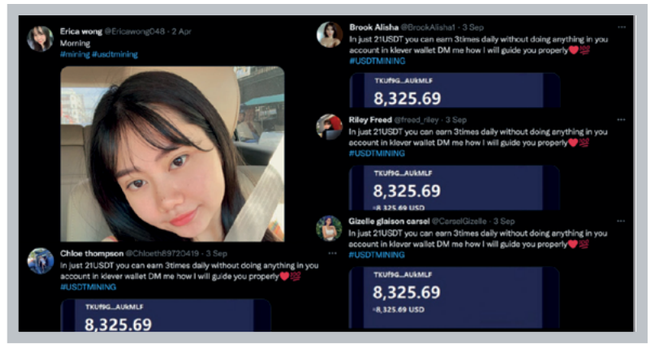


Figure 54: Example tweets containing the #USDTMINING hashtag

8 Crypto transaction analysis

Since YouTube videos associated with this scam instruct viewers on how to move funds from their personal crypto currency wallets into the app, it is possible to determine wallet addresses associated with each app by manually inspecting videos. Wallet addresses can be extracted from videos in two ways – either by transcribing the address or by scanning a QR code shown in the video. The latter is preferable. Using this process, a total of 30 wallet addresses were extracted from videos posted from a variety of YouTube channels associated with these operations. Note that a total of 700 unique URLs were found via analysis of YouTube metadata, and, as such, these 30 addresses represent a tiny fraction of all wallets involved.

Manually extracting wallet addresses from the YouTube videos in question was a cumbersome process. Videos must be opened in an incognito browser window, since opening them while logged into your own account will cause YouTube to start heavily recommending such content, even after viewing only a small number of videos. Nowadays, YouTube shows advertisements, that cannot be blocked, for every few minutes of video content viewed. As such, while manually extracting wallet addresses from these scam videos, we were forced to sit through many, many ads. Having to sit through hours of ads was the reason we stopped after extracting only 30 wallet addresses.

Wallet addresses extracted from all associated videos were part of the Tron cryptocurrency scheme. Tron can be used to facilitate USDT transactions, and wallet addresses of this type can be examined on sites such as tronscan.org. An example of tronscan.org's web interface is shown in Figure 55. Tronscan also exposes a free API that can be used to query up to the last 10,000 transactions for any valid wallet address.

For the purposes of this research, data was collected on Friday 28th October 2022 for transactions going back a maximum of 120 days.

All 30 wallet addresses extracted from YouTube videos were queried using tronscan. Of those, 29 were valid. The wallet address associated with paxxk[.]biz could not be queried on tronscan, suggesting that it may have been made up. This wallet address appears in multiple videos on YouTube, where the app's functionality is demonstrated on-camera. The fact that the wallet address is invalid conclusively proves that the app demonstrated in paxxk[.]biz videos is a special build created for demonstration purposes.

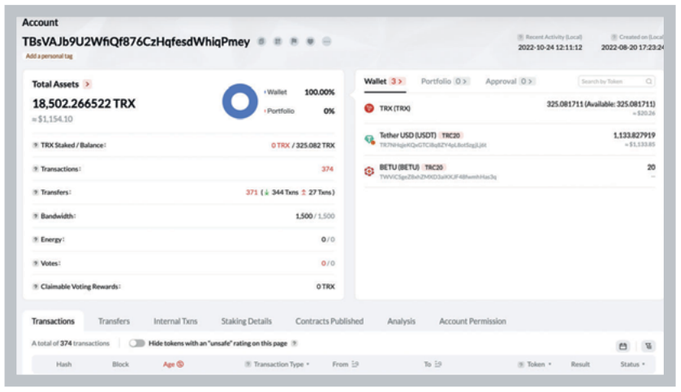


Figure 55: Statistics on videos related to ocitt[.]site with high view counts

Some wallets had no activity on them whatsoever (0 transactions). This includes wallets associated with apps that were advertised on YouTube over a month prior to the investigation. This further supports the idea that the apps being demonstrated in these YouTube videos are custom demo builds with no real functionality. It can thus be concluded that those YouTubers are knowingly and willingly lying when they claim to be demonstrating withdrawal functionality, and hence are fully aware that they are participating in a criminal endeavor.

Some of the queried wallets received a small whole-number sum of USDT from one wallet and subsequently sent the same amount to a different wallet. In the case of videos published by the "PSEB STUDY HALL" YouTube channel, the sending wallet address was always identical. For other channels, such as "Crypto Master 2022" and "EARNING MONEY 89", seeding was performed by a different wallet address each time. A total of 5 seeding wallets were found in this manner. Further manual extraction of app wallets from videos posted by those YouTube channels may reveal further seeding wallets, and possibly an overlap of addresses.

The "PSEB STUDY HALL" seeding account was observed sending money to six app wallet addresses extracted from YouTube videos. The wallet, TKnN-86vWQtz3PyjfTGbgurGZvSTtdJKKVW, had performed 7832 transactions at the time of capture. Over its lifetime it received a total of 12,950 USDT and sent a total of 12,473 USDT. A thorough analysis of this wallet could be the basis of an entire report.

Wallets that received small (<100) whole-number USDT payments from each seeding wallet were identified in an attempt to discover additional app wallets. For each wallet identified, transaction data was collected only if the wallet had a history of 500 or less total transactions. This methodology was based on an observation that active wallets associated with these scam apps tended to not have a great deal of transactions associated with them. A total of 1,576 potential app wallets were discovered across the five seeding accounts using this methodology. Note how this number exceeds the number of URLs extracted from YouTube videos (700). This may mean that either (i) there exist a lot more videos on YouTube that weren't captured by recursing channels involved in paxx[.]biz, ocitt[.]site, and #usdtmining (i.e. the YouTube API didn't return all possible results) or (ii) half of those potential app wallets were misidentified. It is likely that both hypotheses are correct to a certain extent, and the true explanation lies somewhere in between.

From manually inspecting wallets associated with successful scam apps, the following was observed:

- Victim wallets sent USDT to app wallets. No USDT was sent back to any victim wallet, verifying that the "withdraw" functionality is indeed fake.
- App wallets that received payments from victims periodically sent USDT to "receiving" wallets, where it was then sent on to other wallets, and so on. Most payments made in this manner were for small amounts, and on a frequent basis.

To gather a list of potential victim wallets, transactions related to each of the 1,576 app wallets were analyzed as follows: (i) a list of wallets that made a payment of at least 10 USDT to any app wallet was collected, (ii) of those, any wallet that received a payment from any wallet in the dataset was discarded, and any wallet that made a payment to any wallet other than potential app wallets was also discarded. This analysis yielded a total of 915 potential victim wallets.

During a cursory examination of potential victim accounts, it was observed that some had millions of US dollars in holdings and had a history of millions of transactions. For the purposes of brevity, accounts of this type will be denoted as "whales".

One example of such a whale account is TJDENsfB-Js4RFETt1X1W8wMDc8M5XnJhCe. This wallet had performed over 8 million USDT transactions and had holdings in excess of 74 million USD at the time of analysis. This account interacted with TBsVAJb9U2WfiQf-876CzHqfesdWhiqPmey, the wallet associated with the ocitt[.]site app, and TExJShP2ZFR4zEKnvzoc2ZcRmd-9FbBbPjA, the wallet associated with wstrustfund.com. This 'whale' wallet appeared in a list of the top 175 accounts based on its TRX holdings. Given the large number of transactions associated with this wallet, it is possible that it is an automated trading bot.

Each of the 7,251 wallet addresses in the dataset were queried for transaction count. Those with over 1 million transactions were denoted as whales. A total of 28 such accounts were found. Interactions between whale accounts and other wallets in the dataset is depicted in Figure 56.

The fact that these whale accounts interact with such an obscure scam, especially one that requires manually registering for, and interacting with a shoddy and clearly fraudulent web “apps” seems highly illogical. It was not possible to correlate any of the whale addresses with known trading platforms or crypto exchanges via lookups on tronscan.org. As such, this phenomenon remains a mystery, and one that cannot be solved with our current understanding of the TRON ecosystem.

After filtering whale accounts from the previously determined potential victim wallets, the number was reduced to 900. Figure 57 depicts all USDT-related financial interactions between active potential app wallets, victims, and receiving wallets. As you can see, the situation is quite a mess, and untangling any further inferences would be highly problematic. However, clusters of potential victim wallets, and their connections to potential app wallets are easily observable, even in such a complex graph representation.

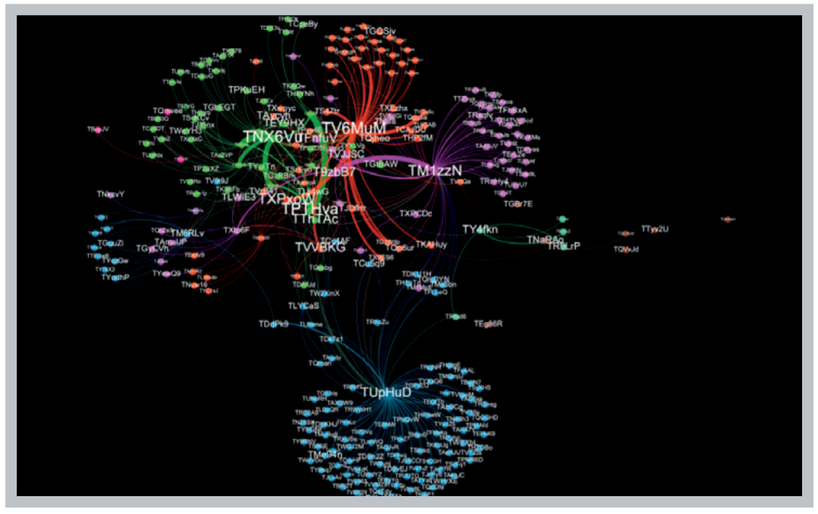


Figure 56: Interactions between whale accounts and other wallets in the collected data. Wallet addresses are truncated to the first six characters..

Figure 57: Interactions between active potential app wallets, victims, and receiving wallets. Wallet addresses are truncated to the first six characters.

```
TFnfuVcSbXsc2beaTeYgkLsHoKpUwVJ38m gained 9748.802958000002 USDT from 27 victims
TS4ZtrM18N5CzJhsXwTbLxmQe6kqUU3meu gained 5375.5143 USDT from 8 victims
TVVBKGk4p7KEnYRa7ANUTiMA1BsFvqzzQu gained 4751.028827000001 USDT from 28 victims
TYQq6cLDMqewcD9Wm2HvbdcBMa6yw3JcMS gained 3929.1000000000004 USDT from 6 victims
T9zbB7FTaPbi3YKu1Rj55SNNazV3vBUnMZ gained 3586.5299999999997 USDT from 11 victims
TLzijSAvFPhg2fM6kafcQ39ZkLW51DV76k gained 3199.898 USDT from 24 victims
TPye4E4DbP5YeJquz7tfCGg9nlLVzv6Y47 gained 3100.7182470000007 USDT from 39 victims
TVJJSCWQU1lgFHZCz3VGale1PH5VYV7fPb gained 2571.21212900001 USDT from 31 victims
TQp6urHGztfuuHwdxhlRAyYNWimuDyAYKt gained 2410.632818999999 USDT from 28 victims
TPAdpTzd2qv3SdYA6raZxq9EwxeWDL6G41 gained 1764.1493860000003 USDT from 11 victims
TX9E963g7f67Dq86UadJCQ6CtX1pWrmxjR gained 1706.6325970000003 USDT from 35 victims
TLWiE3AnHYNzxeRftvPqj4kGLrVrS2wG9 gained 1672.7752550000002 USDT from 13 victims
TKAHuyToMdDMgkSbEL1qni64QLrgwjxuQ3 gained 1542.09 USDT from 4 victims
TNLj3pu5qmzv6u2uQDpHXp9dr5WnoMBhv8 gained 1406.6360530000002 USDT from 12 victims
TG3WdpuanzKBbWxNFekRRavitt3FPDBAmH gained 1373.031025 USDT from 47 victims
TEY9HXF4mWutnK2PCvBdspLVU42d5TdeTa gained 1304.894 USDT from 8 victims
TThTAcKHgJqF7ftAg5vKWR4dWsvhwf6aFR gained 1279.7009999999998 USDT from 40 victims
TVGfbSaSszsGxPwnGGinXJS8gUUaiJ3BSN gained 1247.815 USDT from 20 victims
THP2fM5hNfyZwsCcwwSzWGZorpvwi489oh gained 1180.9282349999999 USDT from 22 victims
TRnLWU24iB279seN9AxBNu4pHY3NFXR31k gained 1062.743637 USDT from 5 victims
TQgg5ayq7CSyR68LLvNSiYXFpeF6KQjaWW gained 1055.45 USDT from 11 victims
TUi4wG76LKBxPJRLWm8Wvjr6a6QtJBt73T gained 990.814916 USDT from 18 victims
TXGn5BeEjGzEUnLrnERLA8bnGhpr8z3ZUz gained 971.2777649999998 USDT from 16 victims
TCQSjv7U97aABsRsgNhB1WFGXExWAZfDjc gained 890.0 USDT from 5 victims
TCqvHFxDwo9MtLBFPU7iVJ48D8EXghE5mH gained 867.823383 USDT from 27 victims
TSxjsq5AhnriJet5wG5TdGTmLzd59w6CrJ gained 849.044 USDT from 24 victims
TDbKHJ2NjEFR8udAhmqCH4hkq8cwazYgKK gained 837.0 USDT from 3 victims
```

Figure 58: A sample of top-grossing potential app wallets identified

Summing all USDT payments from all potential victim wallets to potential app wallets discovered during this process yields a value of roughly 115,628 USDT. Given that only 700 URLs were discovered during analysis of YouTube channels involved in these operations (from data gathered via the YouTube API), it is possible that some of the wallets included in this calculation didn’t belong to scam apps. Conversely, it is possible, given the analysis of just five “seeding” wallets, that the number of actual app wallets identified in this capture represents only a fraction of all wallets involved. As such, the profit value calculated here is likely to be highly inaccurate in both directions. Unfortunately, there is no way to map app wallet addresses back to YouTube videos. In order to accurately verify that potential app wallet addresses uncovered in this analysis are really part of this scam, manual inspection of all possible YouTube videos would be required. This represents an infeasible task (especially due to the number of ads that one would need to suffer through). The profit value calculated here is also subject to change – it was calculated at the time of analysis, and it is possible that scams, especially freshly published ones, bring in new victims, and thus new revenue. To properly track these operations, analysis of both YouTube and wallet activity should be performed on a regular basis over an extended period of time.

The wallet associated with the ocitt[.]site app - TBsVAJb9U2WfiQf876CzHqfesdWhiqPmey - received at total of 7504.200462999997 USDT and sent a total of 6370.372544 USDT during its lifetime. Not all of these transactions can be attributed to victim payments, and it can be assumed that this wallet was used for other, additional purposes. Of note, TP8ojbCEoV25KSB75iVYK9MNXtH1ApwtkA received a total of 2892 USDT from it. By analyzing transactions associated with TP8ojbCEoV25KSB75iVYK9MNXtH1ApwtkA, a great deal of currency can be seen changing hands. Figure 59 shows a sample of the top summed transactions to and from this account.

The wallet TNR8hnL8EGei35yxYJtWHb2PJW5hPQao6D that received close to 60,000 USDT from TP8ojbCEoV25KSB75iVYK9MNXtH1ApwtkA is not a whale account. At the time of capture, the account was holding approximately 8,000 USD worth of currency and had performed just over 1,300 transactions. However, analysis of transactions on this address shows even more money being moved around. This is depicted in Figure 60. Note that this activity happened over a 120-day period at the time of query. By gathering all transactions over this wallet’s entire lifetime, it is possible to determine that over 1.4 million USD moved through this account. Whether the money flowing through this wallet is attached just to these particular crypto scams or if it includes other “business ventures” is currently a point of speculation.

```
TP8ojbCEoV25KSB75iVYK9MNXtHlAPwtkA received at total of 103420.05 USDT
TNR8hnL8EGei35yxYJtWHb2PJW5hPQao6D received at total of 59881.380000000005 USDT
TSezDwTKJjgPAyl7CpahVdn6mhUE7FCNDe received at total of 16709.0 USDT
TGvxkn9xugbpy241W4CL8pSloWX6j9dADz received at total of 5422.0 USDT
TJzz6t8eXcSjGyQa2Vxgr574WGeVM9QCUs received at total of 3648.5 USDT
TNYGLTRgcPpbhm3SXJvQzDjKh9Lu4SPiQv received at total of 2467.17 USDT
TCRTQCPdd4vHqGHxoSbQaFesyQxkQKBYDa received at total of 2419.0 USDT
TJgEfSfpwCnMaqUsabp5GsRujoj4TiGP6n received at total of 2000.0 USDT
TZ1GE4ZxrCzNZSnzGnWhzlfB5uxzCPu4mh received at total of 2000.0 USDT
TALuuveYAJGbX3qxhpJVnWNSUuWEEVjBHK received at total of 2000.0 USDT
TXePC5KygFnxZyoEGDzlaB4hhrMnY7yFTD received at total of 2000.0 USDT
TGVwxEfJifJVDsHSJGYEAmbMx5PA5RUXz4 received at total of 1300.0 USDT
TT7vRhAUXUSxEDYeBy6CYTbikQVoGfvoat received at total of 1271.0 USDT
TB1mAPJ764Aj9xz58vkfL2Q6MZh4pFuhZz received at total of 1000.0 USDT

TP8ojbCEoV25KSB75iVYK9MNXtHlAPwtkA sent a total of 103174.05 USDT
TPW4ByRd7iU9XmZXzTrW4N8CH8E5iz8xQi sent a total of 22232.3 USDT
TCtaEmc477VFfPE5EoHMcMrFlJTcDe9Q4l sent a total of 15635.0 USDT
TUzfXSGDdtvu45P3aEsLFcXXjL2hwbHR9f sent a total of 10987.5 USDT
TCRTQCPdd4vHqGHxoSbQaFesyQxkQKBYDa sent a total of 6802.5 USDT
TNSQYGSyR4eGntGyCYQJJN977WQgPJqq3F sent a total of 4569.0 USDT
```

Figure 59: Top summed transactions associated with TP8ojbCEoV25KS-B75iVYK9MNXtH1ApwtkA

```
TNR8hnL8EGei35yxYJtWHb2PJW5hPQao6D received at total of 840966.2421400001 USDT
TR2FWAQxcSLW7GoVBcytdVwSePtT9TpU2t received at total of 226801.0 USDT
TX6cDrFGhPXkndoEaePwPY4sVuzhajiReL received at total of 218706.0 USDT
TNgJjmXee8TxroBJLN2VHZcbH4UMAGMWls received at total of 197922.0 USDT
TSezDwTKJjgPAyl7CpahVdn6mhUE7FCNDe received at total of 113892.0 USDT
TPDkx8NbC6876L7nUEE6kzZEjjUXjdzdKB received at total of 30726.0 USDT
TB8miN24Y4ZMq3ArYisvmX8ED3SAs5KjQl received at total of 22976.0 USDT
TELprXRRYib8jAfo8BfUn3rvbwdQlWVdBo received at total of 10059.0 USDT
TA2TJv6dnScXBu1X4coGuMBqjVytF8vVJ6 received at total of 5080.0 USDT
TP8ojbCEoV25KSB75iVYK9MNXtHlAPwtkA received at total of 4429.0 USDT

TNR8hnL8EGei35yxYJtWHb2PJW5hPQao6D sent a total of 840809.71 USDT
TGbF5MHaMWEZuAs2i6VEjpxB4BYnncSwF1 sent a total of 281787.95 USDT
TSezDwTKJjgPAyl7CpahVdn6mhUE7FCNDe sent a total of 187670.4 USDT
TM1zzNDZD2DPASbKcgdVoTYhfmYgtfwx9R sent a total of 72493.3663 USDT
TP8ojbCEoV25KSB75iVYK9MNXtHlAPwtkA sent a total of 59881.380000000005 USDT
TU4TXN4SfTYckqCSSEtVR5iK8mLa2Sv9VV sent a total of 30035.5 USDT
TT9qEmQSbYdrUXy3WJ79xQS64ghgfqJUoD sent a total of 27933.0 USDT
TJNRreD5dtwd7mTVMgtqzsQV9aMjpoKG2J sent a total of 22195.0 USDT
TKN98KhmJyojCzXfBtA47YqujthYY6FiD2 sent a total of 18344.0 USDT
TCQMSq5Niaj82FHuxeNpPiPKJaC5VMrQtD sent a total of 16616.0 USDT
```

Figure 60: Top summed transactions associated with TNR8hnL8EGei35yxYJt-WHb2PJW5hPQao6D

Although it is possible to continue following this trail of money, the obfuscated nature of crypto currency wallets makes it impossible to associate accounts with individuals or businesses. It was generally observed that these operations moved small amounts of currency through multiple accounts, an observation that is backed by the complex node-edge graph depicted in Figure 57. The only definite associations we have are a small number of wallets associated with apps advertised on YouTube. As far as who might be running these operations, how large they are, whether they are associated with other crypto scams (such as “pig butchering”), or anything else would require a great deal of further investigation.

9 Recommendations for YouTube

The research involved in this report was straightforward to perform and was seeded with the discovery of a single scam app (paxxk[.]biz). Discovering hundreds of channels and URLs associated with these fraudulent schemes was trivial, and only limited by the speed at which data could be gathered. Independent researchers constantly find examples of malicious and inauthentic activity on social media platforms. Those investigations work with rate-limited APIs and a limited set of metadata, and yet they’re able to discover phenomena unnoticed by the owners of those sites. It is the responsibility of those platforms to act upon such findings by utilizing additional metadata only available with employee access.

YouTube’s free API rate limits are quite restrictive, especially with regards to search functionality. However, the YouTube API web user interface is very informative in that it allows tracking of rate-limit usage in almost real-time. We would welcome functionality in the YouTube API to allow videos listed under a hashtag to be fetched without the need to use search queries.

Given the number of channels discovered that were posting fraudulent content, the frequency at which they published, and the length of time at which these operations had been running, it is highly surprising that they weren’t already spotted and taken down. Now that we know about these operations, videos of this nature should be thoroughly enumerated and removed by the YouTube safety team, along with any other channels participating in similar operations (both those publishing videos and those automated to post comments and boost engagement). If this isn’t something YouTube is willing to do, they should, at the very least, suppress their algorithm’s recommendation of these videos. YouTube should also make an effort to understand how the “SEO” text found in the description fields of these videos might affect YouTube’s search and recommendation algorithms.

A cursory glance at results returned by an Internet search for “buy YouTube views” illuminates the existence of many services selling YouTube likes, views, comments, and subscribes. It is clear that inauthentic amplification is being used to boost engagement numbers on many of the videos highlighted in this report (such as videos published on the PSEB STUDY HALL channel). While we're aware that detecting inauthentic activity on social networks is a difficult endeavour, with regards to the videos highlighted in this report, determining patterns and channels involved in their actions was a straightforward task that required very little API usage. It would be nice to know that YouTube’s administrators take inauthentic amplification seriously and are devising more generic methods to detect and counter such activity in the future.

The fact that YouTube verified accounts have participated in the advertising of these scams is worrying. It conveys the idea that verified status isn’t something that can be trusted and that verified badges are issued far too easily.

10 Conclusions

Although many “USDT mining” scam videos have been created by many YouTubers, one group involved in this scam likely consists of a tightly coordinated team containing around thirty members. This hypothesis is supported by examination of the overlap between unique URLs and the channels that actively promote them (Figure 50 and Figure 51) and an overlap across Telegram users that comment on videos (Figure 25, Figure 38, and Figure 45).

Analysis of transactions performed on wallets associated with these scam apps proves that they are fake. (i) some app wallets have no transactions on them (despite videos demonstrating otherwise), (ii) victim wallets have not been seen to receive transfers from the app wallets.

By extracting wallet addresses from YouTube videos of this nature, it was possible to map out a potential network of “seeding” accounts, app wallets, victims, and receiving addresses. Estimates suggest that these various operations earned as much as 100,000 collectively USD between July and November 2022. However, analysis of crypto transactions involved in these operations was limited and may have simply missed a large number of additional wallets.

Given that the running costs of these operations must include registering domains, creating apps, paying content creators to publish and boost videos, and managing the flow of currency through potentially thousands of crypto wallets, they don’t appear to be very lucrative. One must wonder how YouTube content creators are incentivized to create endless videos of this nature. This is especially the case for verified accounts with hundreds of thousands of subscribers. Perhaps YouTube’s lax policies and inability to find and shut down such content emboldens them even if incentives are meagre.

Crypto currency of significant dollar value can be observed flowing through wallets further along the payment chain, suggesting that these scam apps may be part of one or more larger cyber criminal operations. An article from The Times of India published on 9th September 2022[4] suggests that operations similar to those detailed in this report can be attributed to Chinese operators. However, no details regarding attribution methodology are given in the article. Additionally, our research didn’t uncover any data or indicators that could be used for attribution purposes.

These scams rely on victims finding and watching YouTube videos. Although most videos analyzed in this research have thousands of views, activity on wallets associated with their scam apps suggests that either the schemes themselves are not very convincing, or that all those views come from inauthentic sources designed to boost the video’s chances of being recommended. The poor quality of videos and the apps associated with them is probably a contributing factor behind the lack of success of such operations. That said, the entities behind these various operations continue to create new apps and post new videos on a daily basis. This suggests that they are playing a numbers game and hoping that, every now and then, they hook a whale that will deliver them huge profits. It is quite possible that these groups will modify certain aspects of their operations going forward. If the accounts and videos detailed here do end up being taken down by YouTube, we fully expect the entities behind these operations to rebuild and continue doing what they’re doing.

4. https://timesofindia.indiatimes.com/city/lucknow/uttar-pradesh-cops-unearths-rs-4200-crore-frauds-linked-to-chinese-operators/article-show/94103428.cms

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure