YouTubeでのUSDT暗号資産詐欺の分析

Andrew Patel,
WithSecure™ Intelligence, 2023

WITH secure

コンテンツ

1. 概要

WithSecure™ Intelligenceは、暗号資産であるテザー(Tether、別名USDT) を使用した暗号資産投資スキームを装った不正なWebアプリの広告動画を数千件発見しました。これらの動画はYouTubeで公開されており、投資した通貨の量に応じたリターンを約束するものです。登録者数や視聴回数が多いYouTubeチャンネルは、こうした新しい動画を毎日のように投稿しています。参加チャンネルの中には、YouTubeの認証アカウントを持っているものもあります。

こうしたの動画の多くは、コミュニケーションアプリであるTelegramを使用する小規模詐欺グループが管理する数百のYouTubeチャンネルから、YouTubeの推薦アルゴリズムを欺くために設計された、偽物のエンゲージメントのよる増幅を受けます。これらのYouTubeチャンネルは自動化を利用し、動画にコピー＆ペーストしたコメントを投稿することで、宣伝している不正アプリを正規のものに見せかけようとしています。また、動画の説明欄には、YouTubeの検索機能を利用した独自のSEO対策が施されているようです。

本レポート執筆時点で、こうした詐欺アプリに関連する約700のURLが、データ取得・分析技術により特定されています。また、YouTubeのハッシュタグ「#usdtmining」には、3,900以上の類似動画が含まれていると報告されています。

これらの不正アプリに関連する暗号資産ウォレットのアドレスは、複数のYouTube動画から直接抽出されました。これらのウォレットに関連する取引に見られるパターンから、これらの操作に関与しているアプリや暗号資産ウォレットがさらに数千個存在する可能性があることが示唆されました。これらのウォレットの取引履歴を収集することで、900人の被害者が特定されました。被害者のウォレットとアプリのウォレット間の取引を合計すると、2022年7月から11月の間に、詐欺グループは10万米ドル強を稼いだと推定されます。

このような取引では、数百、数千の暗号資産ウォレットが使用され、これらのウォレットは互いに非常に少量かつ頻繁に送受信を行います。このような業務におけるお金の流れをマッピングすることは、非常に複雑な作業を意味します。しかし、ブロックチェーン上の少数の下流ウォレットを経由する大量の資金を特定することは可能です。

本レポートでは、この詐欺の背後にある動画とアプリの分析を詳細に説明し、関連する2つの詐欺アプリを詳細に分析し、YouTubeの#usdtminingハッシュタグを調べ、詐欺に関連する暗号ウォレットに使用されたブロックチェーン分析手法について説明し、最後にYouTubeに対する推奨事項といくつかの最終結論を提示します。

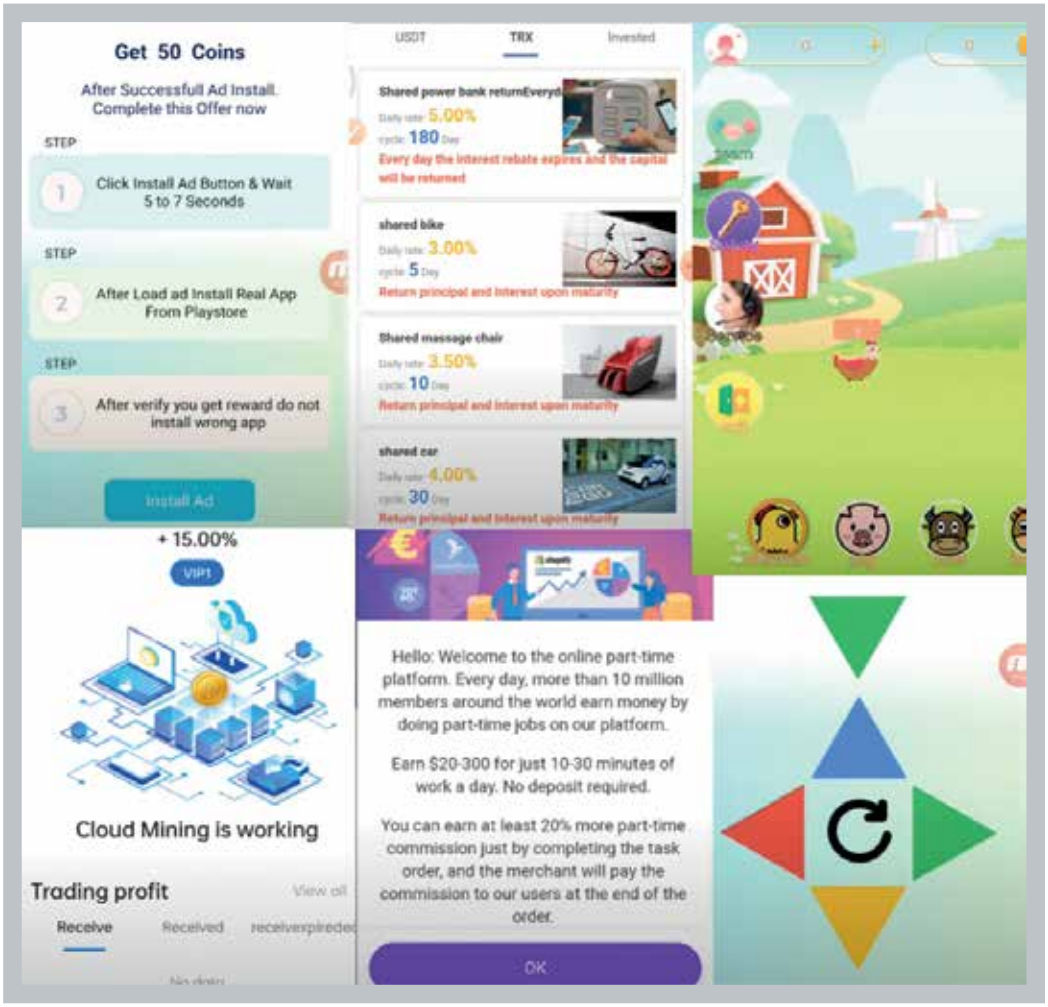
2. はじめに

サイバー犯罪者は、悪質な行為に対する支払いを受ける手段として、暗号資産をいち早く採用しています。これは、暗号資産が匿名であり、分散化されており、従来の金融規制の対象外であることが多いためです。このため、暗号資産がなければ実現しなかったであろうサイバー犯罪の活動が増加しています。

暗号資産のエコシステムには、比較的知られていない犯罪スキームが多く存在します。その一例が、マイニングプールや流動性マイニング詐欺で、暗号資産の保有者を騙して、高いリターンが得られるとされる投資をさせようとする詐欺的な行為です。このようなスキームに投資した被害者は、詐欺師にお金を渡し、そのお金は決して戻ってはきません。

大まかに言えば、テザーマイニング詐欺は次のような方法で行われます。被害者はまず、ソーシャルメディア上の広告やYouTubeのアルゴリズムからの推薦によって誘い込まれます。YouTubeには、このような「すぐにお金を稼げる」仕組みを宣伝する動画が何千本もアップされています。この種の動画は非現実的なリターンを約束することが多く、中には1日あたり2%以上のリターンを謳うものもあります。

今回分析したYouTube動画は、決まった台本に沿って作られているようです。このような詐欺アプリの作成に関与したグループが、契約したYouTuberが従うべき一定のスクリプトを提供している可能性が高い。これらのYouTuberは、このような動画を公開することで金銭的な補償を受けていると思われます。本リサーチで見つかった動画の大半は、インド地域で使用される言語で紹介されていました。



ビデオスクリプトによると、被害者は広告のアプリでアカウントを作成するよう要求されます。アプリは、Webページ、モバイルアプリケーション、場合によってはTelegramソーシャルネットワーク上でユーザーと対話するオートメーションの形で提供されます。アカウントの作成と登録のプロセスの一環として、被害者は少額 (通常は数十米ドル) の通貨をアプリに入金する必要があります。これが、詐欺師が被害者からお金を盗むポイントです。

これらの動画の多くは、被害者が友人や家族を招待するよう促し、招待を受け入れた人数に応じて少額のお金を受け取ることができると主張しています。また、アプリには、より高い投資リターンを誇るより良い「投資」オプションを解除するボーナス「VIP」構造も含まれています。これらの「VIP」制度は通常、ユーザーがより多くの通貨をアプリに入金することを要求します。YouTubeのビデオの中には、このような複雑なVIPボーナス構造について長々と説明しているものがあります。

アプリによってその仕組みは様々です。あるものは被害者に自分の投資がマイニングに使われていると思わせることを意図しており、単にお金をプールに預けておけば手数料を得ることができます。また、毎日「タスク」や「グラブ」が用意されていて、ユーザーはそれをクリックしてお金を「稼ぐ」必要があるものもあります。さらに、ニワトリや牛、馬などの動物を育てる農園ゲームもあります。

いずれの場合も、アプリのインターフェースは定期的に、あるいはアプリ特有のタスクを実行した後に、被害者の残高の増加を報告します。このような仕組みでは、一般的に、投資額が多いほど高いリターンが得られます。被害者は、少額の投資で高いリターンが得られることを知り、より多くの投資をしたくなります。

YouTubeで公開されている動画は通常、広告のアプリ内から出金機能を実演しています。これは、被害者を騙して、いつでもキャッシュアウトできると理解させるためのものです。しかし、実態はその逆であり、被害者はアプリに入金された資金を取り戻すことはできません。この事実は、これらのアプリに関連するウォレットからの取引を追跡することで確認されました。被害者がアプリのウォレットに通貨を送ったにもかかわらず、逆方向への取引は確認されませんでした。

マイニングプール投資スキームを実演するYouTubeの動画は、暗号資産のエコシステムに既に精通しており、それらの通貨の一部を既に保有している可能性が高い人々を主な対象としているように見えます。デモの対象となるアプリは、被害者がすでに作成したウォレットから資金を送金することを要求しています。ウォレットの作成方法と実際の資金投入方法を紹介するビデオもありますが、ウォレットの作成、資金投入、詐欺アプリへの登録、ウォレットへの暗号資産の投入というエンドツーエンドのプロセスは、かなり長くて手間のかかるものです。

アプリそのものも粗雑な作りで、読みにくい英文ばかりが見受けられます。これらのアプリは、真剣に投資するための手段としては明らかに説得力不足だと言えます。アプリの「業務内容」や「会社概要」をクリックして読んでみるだけで、怪しいと考えるには十分です。調査したアプリの多くは、他のアプリのリスキンバージョンであるように見えます。このため、これらの事業者は「アプリカスタマイズキット」を利用し、エンジニアでない従業員が簡単に新しいアプリを設定・展開できるようにしている可能性があります。これらのアプリを宣伝するビデオも、同様に質が低いものです。

本レポートで調査した全てのアプリは、USDT[1]暗号資産を利用しています。テザー (Tether としても知られるUSDTは、米ドルの価値に「連動 (tethered)」するとされる暗号資産です。このような通貨は「安定コイン」と呼ばれ、マイニングすることはできません。USDTでできることは、約1米ドルで購入し、ほぼ同額で売却することのみです。なお、USDTは2017年と2018年にビットコインの価値操作に使われた疑惑があるなど、大きな論争が巻き起こっています。

暗号資産を使った詐欺の研究は広く行われています。以下のリンクは、今回と同様の性質を持つ暗号詐欺に関する最近発表されたレポートへのリンクです。

- 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

本レポートでは、YouTubeの動画や「アプリ」を利用した「ハンズオフアプローチ」を採用しています。これは、現在流行している「豚の食肉解体詐欺」(長い時間をかけて豚を太らせて解体して処理するプロセスに似ていることから) で使用されている、信頼に基づくソーシャルエンジニアリングの実践的な手法とは対照的なものです。YouTubeのインフラが「ハンズオンアプローチ」よりも優先して使用される理由の1つは、動画のほとんどが英語以外の言語で表示されているため、その言語を流暢に話すことができるソーシャルエンジニアを必要とせずに被害者のプールを利用するように設計されているからかもしれません。

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

3. USDTマイニングプールの動画とアプリの解剖

YouTube見られたマイニングプール詐欺の動画のほとんどは、同じ基本構造を持っていました。このセクションでは、通常彼らが従うスクリプトの概要を説明し、paxxk[.]bizと呼ばれるアプリに関するビデオのスクリーンショットを紹介します。このURLは、私たちがこのリサーチに着手する前に、WithSecure™ Intelligenceのリサーチチームによって潜在的な詐欺サイトであることが確認されました。このアプリについては、本レポートの後のセクションで詳しく分析します。

図1は、本実施例で使用した動画のサムネイルです。この動画は、YouTubeのWeb UIで「paxxk[.]biz」を検索して最初にヒットしたもので、「Your Crypto Helper」というアカウントによって投稿されたものです。この種の動画は音声ナレーションがほとんどですが、この動画はビデオプレゼンターが参加しており、これは非常に珍しく、この動画が多くのエンゲージメントを得て、トップヒットとなった理由と考えられます。

図1: YouTubeの検索結果に表示されるサムネイル (動画サンプル)

paxxk[.]bizアプリは、スマートフォンで表示されるように設計されたシンプルなWebサイトで、どのブラウザからでもアクセスできます。スマートフォンで見ることを前提にしているため (つまり、スマホアプリのように表示される)、デスクトップのブラウザから見ると不格好に見えてしまいます (図2)。

図2: デスクトップブラウザで表示したpaxxk[.]biz

分析した動画では、まずプレゼンターがアプリの登録方法を紹介し (図3)、新規ユーザーはアカウントを作り、パスワードを設定する必要があると説明しています。また、動画内では招待コード欄があり、それを利用することでプレゼンターの収入が得られると宣伝しています。この招待コードを利用することで、プレゼンターのアカウントにお金が入る仕組みになっています。

そして、口座を持っている人が友人や家族を招待することで、無料でUSDTを獲得できることを長々と説明しています (図4)。

このアプリには、新しい人を招待したときのボーナスや、さまざまな「VIP」スキームなど、ゲーミフィケーションの仕組みが多数含まれています。その一部が図5に示されています。

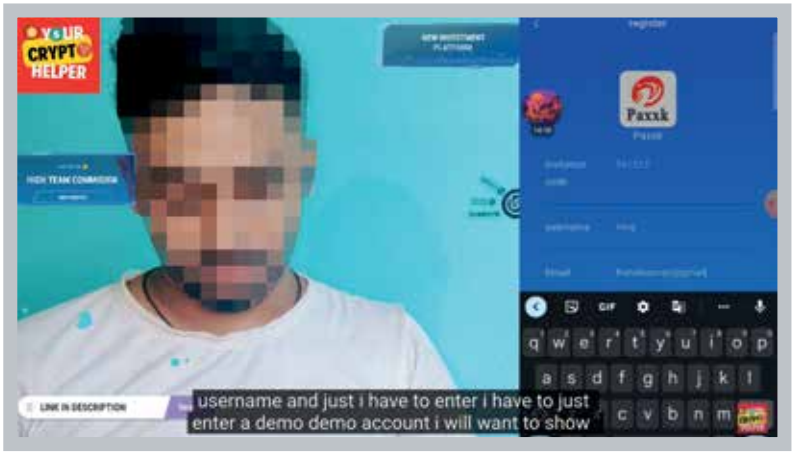


図3: paxxk[.]bizの登録方法の紹介

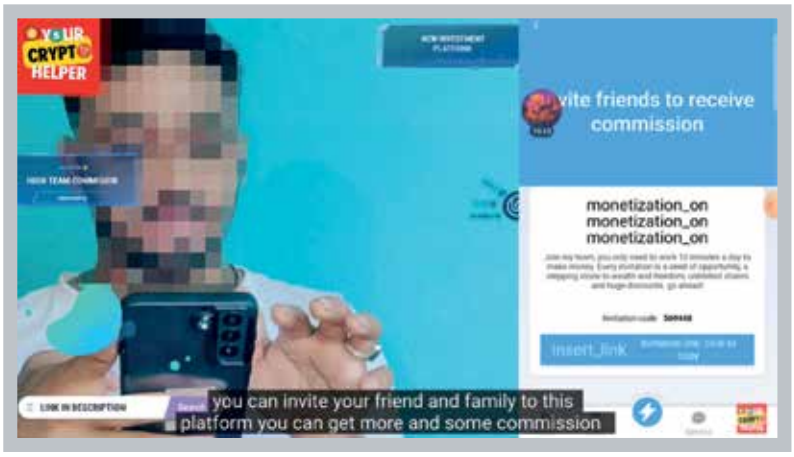


図4: プレゼンターが動画の視聴者に友達を招待し、お金を稼ぐように促す

図5: YouTube検索結果で表示されるサンプル動画のサムネイル

また、アプリに通貨を追加することで金銭的なボーナスを得られるとする「リチャージリワード」も利用されています (図6)。この「リチャージリワード」のコンセプトは、モバイルゲームでよく使われる「消費リワード」の仕組みに酷似しています。実際、これらのアプリのゲーミフィケーションの側面は、ユーザーに少額の報酬を得るために単純な作業をさせるという、モバイルゲームによくある手法を反映しています。

paxxk[.]bizのアプリには、配信されたと思われる手数料の「テロップ」がスクロール表示されます (図7)。この表示は、被害者に、他の人が巨額の手数料を受け取っていると思わせるように設計されています (もちろん、巨額の投資が必要であることは言うまでもありません)。このような詐欺の被害にあったウォレットを分析したところ、ほとんどの場合、取引はほとんど行われていないことから、この部分はほぼ間違いなくランダムに生成されたものであると考えられます。

続けて、「リチャージ」の方法、つまり自分の暗号ウォレットからアプリに暗号資産を移動させる方法について、簡単なチュートリアルが紹介されます。このデモでは、プレゼンターが20USDTをアプリに「転送」しています (図8)。詐欺師は、お金を稼ぐために被害者にこのステップを実行させる必要があるため、これは動画の重要な部分です。このスクリーンショットでは、詐欺アプリに添付されたウォレットアドレスが見えることに注目してください。

図6: paxxk[.]biz リチャージリワード

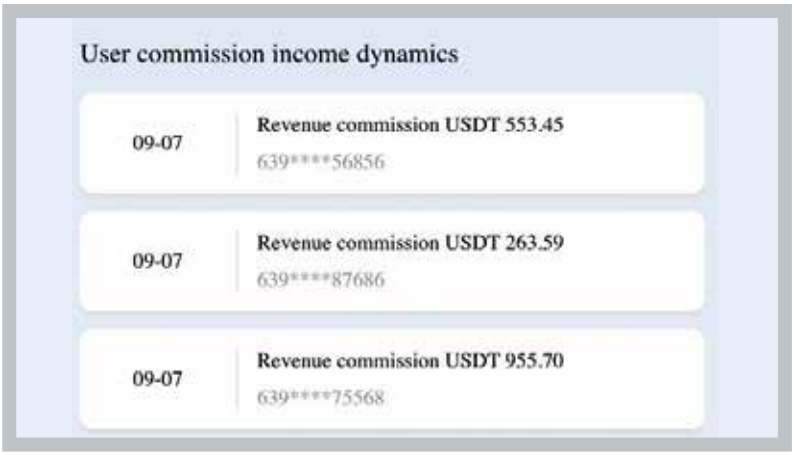


図7: paxx.bizの手数料ティッカーテープ

図8: paxxk[.]bizアプリの「リチャージ」機能を使用した場合

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).

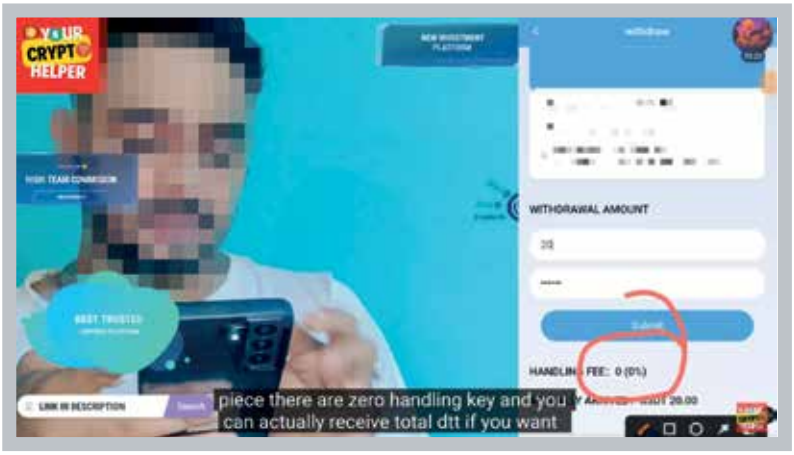


図9: 引き出し機能についてのプレゼンターの説明

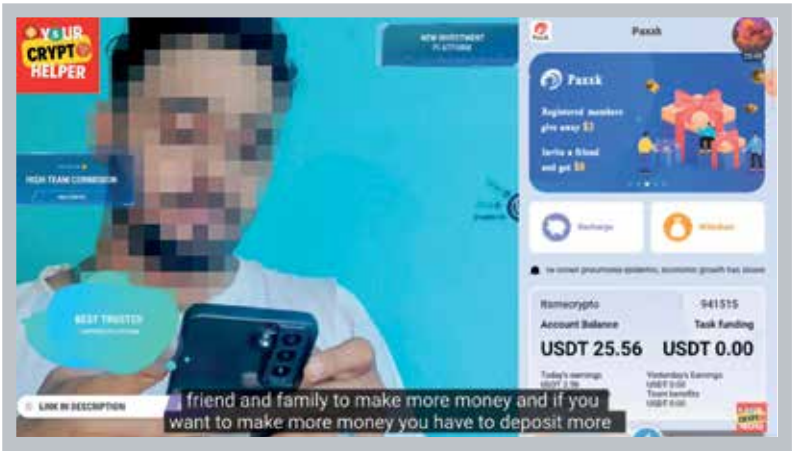


図10: プレゼンターからの大切なメッセージ

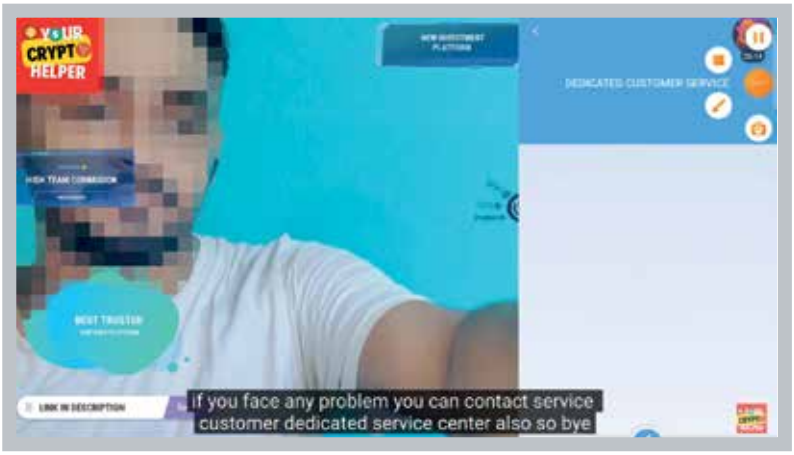


図11: 「お客様専用窓口」機能の存在を視聴者に示すプレゼンター

この詐欺に引っかかった人たちの逸話によると、カスタマーサービスの機能は時々機能するそうです。おそらく、引き出しがうまくいかずカスタマーサービスに連絡すると、追加の手数料を支払うように言われるでしょう (これも戻ってきません)。

この種のビデオの中には、視聴者に「投資する前に自分で調査し、リスクを分析するように」と促す司会者の言葉が含まれているものがあります。このような文言は、おそらくチャンネル所有者の責任を回避するために用意されたものでしょう。しかし、このようなコンテンツ制作者が、お金を盗むために特別に設計されたサイトの利用方法を指導するビデオを録画し、公開しているという事実を考慮すると、このような発言は無意味なものです。

paxxk[.]bizアプリには「Work Description」(業務内容) と書かれたボタンがあり、図12に描かれたダイアログが表示されます。その中で興味深い点は、メンバーになるには20USDTが必要であるという事実と、引き出しは1日1回に制限されているという事実です。また、疑問を持っていた場合に備えて、「paxxkは合法的で正当なプラットフォームである」とも記載されています。

「Company Profile」(会社概要) ボタンを押すと、図13のようなダイアログが表示されます。ここに書かれていることは、間違いなくフィクションです。そして、同じ制作者の他の多くのアプリで再利用される可能性があります。

UI上のどの項目をクリックしても、「システム通知」のモーダルダイアログ (図14) が表示され、解除されるまで操作ができない煩わしさがあります。このため、短時間でもアプリを操作するのに疲れてしまいます。


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.

図12: paxxk[.]biz "Work Description "ダイアログ


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, Ofx, 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.

図13: paxxk[.]biz "Company Profile "ダイアログ

図14: paxxk[.]bizの「システム通知」モーダルダイアログ

興味深いことに、この動画をはじめ、今回のリサーチで手作業で調査したほとんどの動画は、YouTubeの動画の説明欄にSEOの一種を使用しているようです。この動画の例を図15に示します。これらは、暗号詐欺の動画コンテンツに関する今後のリサーチにおいて、興味深いYouTubeの検索条件を示していると思われます。

YouTubeで「paxxk[.]biz」と検索すると、数十本の動画がヒットします。図16は、出金機能が実在することを大きくほのめかす記述の一部です。

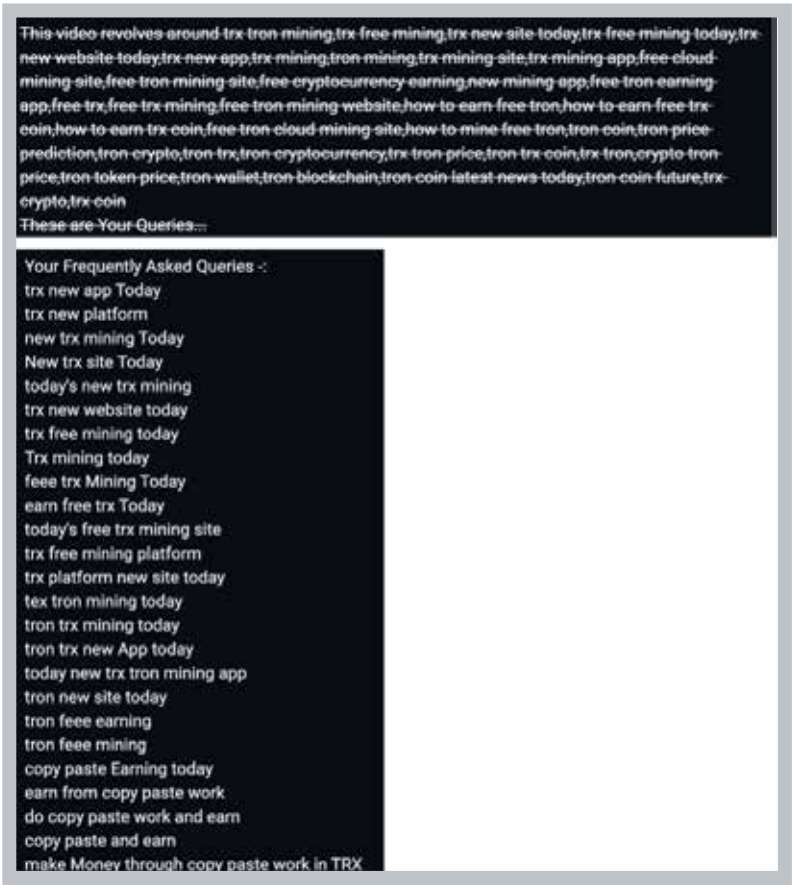


図15: 動画説明文に埋め込まれたSEO

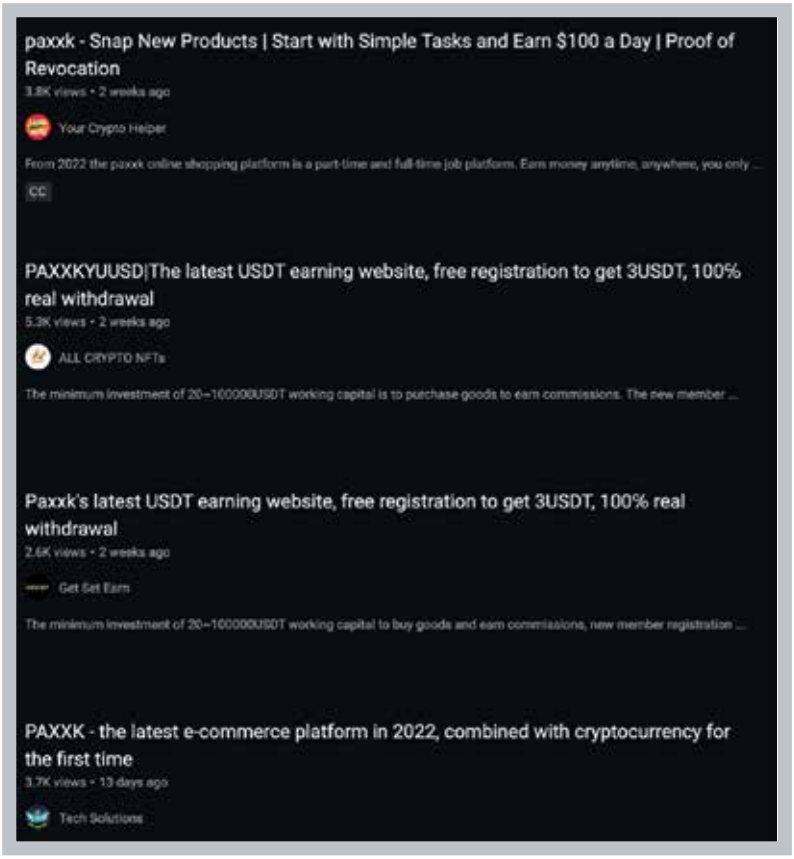


図16: paxxk[.]bizに関連するYouTubeの動画説明文

paxxk[.]biz」を検索したときにYouTubeのWeb UIが表示した30ほどの動画をスクロールして過ぎると、YouTubeの推薦アルゴリズムが作動し、図17に示すように、さらにいくつかの候補が提示されました。

同様のUSDTを使ったマイニングプール詐欺は、YouTubeで「#usdtmining」のハッシュタグで検索すると見つかり、3,900本の動画があるとされています (図18)。

次に、YouTube API[2]と pyyoutube[3]を介して取得したデータを用いて、YouTube の動画とチャンネルを分析することを中心に説明します。

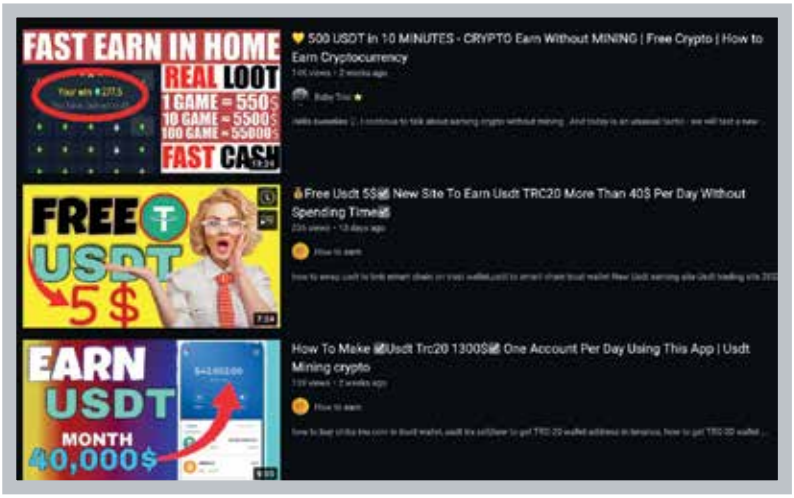


図17: paxxk[.]bizの検索に関連するYouTubeのレコメンデーション

図18: YouTubeで#usdtminingハッシュタグで検出される3,900本の動画と792のチャンネル

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

4. paxxk[.]bizマイニングプール詐欺に関連するYouTubeアクティビティの分析

paxxk[.]bizはUSDT詐欺アプリの典型例であるため、YouTubeのアクティビティを分析するには最適な出発点であると思われます。paxxk[.]biz」をYouTubeで検索すると (図19)、このアプリを使ってお金を稼ぐ方法を紹介する動画がいくつか表示されます。

api.search_by_keywords(q=keyword, count=100) を使用すると、タイトルまたは説明文のいずれかに「paxxk」という文字列が一致する動画30件を含む100件の検索項目が返されました。捕捉された動画は全て、異なるチャンネルでホストされていることが判明しました。いずれも2022年8月21日から24日の間に公開されたものです。これらの動画は英語、中東の言語、インド亜大陸の言語など、様々な言語で表示されていました。6本を除く全ての動画には、コメント欄に返信が記載されています。返信の数は1件から131件まで様々でした。図20は、その基本的な統計データです。

図20に示すように、全てのチャンネルは複数の動画を公開しており、ほとんどの場合、多くのチャンネル登録者数および視聴者数を持っています。あるチャンネルは、60万人近い登録者と400万回以上の総再生回数を誇るYouTubeの認証済みアカウントであることが確認されました。

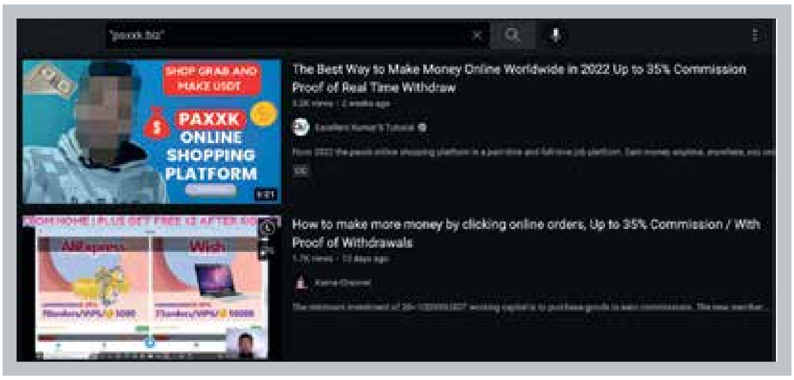


図19: paxxk[.]bizのYouTube検索の出力例

Channel ID	Video ID	Views	Cmnts	Published	Subs	Vids	Viewers
UC9TzUJ04o2GCqBPk1APBlmw	ycfUXacUi3Q	2689	63	2022-08-21	801	256	1250941
UC0VJMAJ7J_Fi6Rlfq8eWWg	oyht4skEO4M	4327	9	2022-08-21	2200	118	348488
UC7zi9zcedyAVWvV0TN0SrPA	O5cmjS0pcSY	3705	5	2022-08-22	1230	183	581544
UC7VVWue4IU7MDR0WB_CQ0DQ	3rKg3wFN_Wg	1749	7	2022-08-23	17300	776	1068504
UCDMkNUb_DzSrIcnLtx_w-gg	zDN1V_KMPOU	3879	2	2022-08-21	54600	613	3659204
UCinKKc11C60nDeiqWlVSqBA	L7D5Qg1FJww	5397	2	2022-08-21	92000	368	1124710
UCrPiL3pdXl9rvRm_DVaKhgA	OTTszbO-GDU	2549	87	2022-08-21	18200	23	43600
UCwbClWblAv5JzmmrCx7P6Ag	OfQKiA5erVA	6696	97	2022-08-24	46000	24	166559
UC4NwK9V4C6gaJo79erpd__w	ELoOH4KJNf4	762	131	2022-08-21	4150	43	84312
UCvWRQiyRF7qlDJQYSqjHGCA	Yik-Lbxvohk	2566	2	2022-08-21	19200	271	612303
UC6tPgTOz8koRq2-6u81RTVQ	2NjcmaPEoyg	9263	26	2022-08-22	599000	1957	41720461
UC0B9btAY_keFi_nuy4u893Q	ertocmgAbus	1150	20	2022-08-21	2160	285	363153
UCRnJ6PxRbIOceMCV6U8QtLw	2CoNfwQp_SI	7495	35	2022-08-21	45700	155	1869339
UCtzZo8aGES050ked8-WIQiA	UMQ-x-2vG74	3347	0	2022-08-21	74600	38	209963
UCpuv8_j_nBiIP8rlbzUIvhg	sXrq0S83DoA	10197	122	2022-08-22	33200	47	344526
UCx_txqMNu07mF-pvrQ_MDKg	qbhMX0YkULO	1941	0	2022-08-21	1040	111	347476
UCr--3Y7-CWuyyMW7aE_ZUoQ	Ep5NQKFKK7U	9881	41	2022-08-22	43500	54	1558230
UCmPfag1FiSWiTFR8DXoz4lg	PffFCmgp6EQ	3592	5	2022-08-22	3790	539	1417526
UCrQW4gmEBlo6YHsqnHGbBPQ	C1lmZne5KAE	3341	None	2022-08-23	3500	56	185280
UC-9CNfWoj56dKpiFekiTO9w	65uqHTJq9LM	10753	1	2022-08-22	2150	56	234597
UCHIn2099wWSbeKBE_GrHVNA	rLFgb1fC2JQ	5528	27	2022-08-22	47900	99	1385162
UCQLGOQhXGhSbe_9kRBB2LJw	ooCgFYGLWeM	3522	0	2022-08-23	101	167	562811
UCo5uIhofG2M5EJXY_oqblQw	nNmWX4g8T3k	1055	0	2022-08-21	31900	50	196462
UCauYiJbJa-nPBI7UPZ188QA	YGT6drSW5Ow	3638	8	2022-08-23	37500	29	62512
UC2OwRM8lrs8rke-MDeqitvA	jRw6xaHkfrQ	1399	0	2022-08-22	1220	206	271099
UClo-PKOirfwL5KglK8lVwKA	GQhoI935EF8	1582	27	2022-08-23	5740	337	405888
UCMPoJI8e3_qRC84STOnsLQw	j66VM2dORoc	1298	12	2022-08-22	12500	727	1544504
UCwKmqux1lIWs04Kc0xZPttQ	VdMrsl_StvA	4753	28	2022-08-23	48200	250	6343548

図20: paxxk[.]bizのYouTube検索で見つかった動画の基本統計量

次に、YouTube APIを使用して、事前の検索で特定された各チャンネルの全動画のリストを取得しました。このプロセスで、30のアカウントから合計8,338本の動画が見つかりました。続いて、APIを使用して、8,338本の動画に返信された全てのトップレベルのコメントを取得しました。このようにして、合計8,016のスレッドがトップレベルの返信を含み、61,048のユニークなチャンネルによって投稿された125,362のコメントが取得されました。図21は最も多くのコメントを得た10チャンネルのリストを含む、いくつかの統計を示したものです。

最も多くのコメントが寄せられたチャンネルは、図22に表されています。アカウント名は「Excellent Kumar'S Tutorial」で、YouTubeで認証されたアカウントです。よく調べてみると、「Excellent Kumar'S Tutorial」と「Your Crypto Helper」の両チャンネルの動画は、同じ人物によって公開されていることがわかりました。「Excellent Kumar'S Tutorial」チャンネルに投稿されたビデオのほとんどは合法的に見えますが、「Your Crypto Helper」に投稿されている動画は、ほとんどこれらの詐欺に関連したものばかりです。同様に、これらの動画を投稿している他のYouTubeチャンネルの多くは、大量に公開しているものの、他のことについてはあまり投稿していませんでした。

大量のコメントを投稿しているYouTubeチャンネルを分析した結果、それらのアカウントの多くにTelegramのユーザー名を含むタイトルが含まれていることが判明しました。図23は、そのチャンネル名の一例です。

```
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/UC7VVNue4IU7MORJWE_CQ6DQ       Kama Channel
11944   https://www.youtube.com/channel/UC97zUJD6o2GCqBPklAP8lmw       Get Set Earn
11485   https://www.youtube.com/channel/UCnJEBjuwQG5bk-9dnYbodfw       Kwarta Online
4664    https://www.youtube.com/channel/UCr--3YT-GNuyyMN7aE_8UoQ       BAER YT
4406    https://www.youtube.com/channel/UCGN5btAY_keFi_nuy4u893Q       DONI-HTS
4299    https://www.youtube.com/channel/UCwKmquxJ1lWeO4KcDxIPttQ       TECS HAGE
4069    https://www.youtube.com/channel/UCMPoJI8c3_qBCE4ST0neLQw       EARNING CHOICE
3429    https://www.youtube.com/channel/UCmPXeg1FiIW1TFN8DXos4lg       Nice Tech
3277    https://www.youtube.com/channel/UCDMKHGb_DzSrlenLtx_w-gg       Your Crypto Helper
```

図21: paxxk[.]bizについて投稿しているアカウントからのYouTubeコメントに関する統計情報

図22: paxxk[.]bizに関連するコメント上位のチャンネル

```
Found 1029 channels mentioning telegram
29      UCTTVkLpcRpgw-ODna7q8_tg        Javier (REDDITHACKS ON TELEGRAM)
3       UCzMQWarCttgDp04fRK6eh4g        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       UCYjXEIOh0sYUSDs_t5kg4Jg        HACKERTHURAM ON TELEGRAM
4       UCGMHXpEc8qT6wWAzr1QcJUA        HACKERTHURAM ON TELEGRAM
2       UCe_beSr1IiY5mI7i2vlePoQ        Text UNIVERSALTECH on Telegram
1       UCpMR4276kKededpG7X_0IVA        HACKG401 ON TELEGRAM
15      UC6Ynq2f5QVL0KvPlPb5xQiQ        Sheila. Philip_Hack on Telegram
4       UCNaZb0DDe675KPbuNWozj0A        Beng Hackercena on telegram
4       UC0W636Vu_LfTcYh5HxfBICg        Hackercena on telegram
4       UClQ0_sRJQkLREEqFRU4HuOw        James Reamlee on telegram
6       UCgPL4HsHxycTakVKgNDX9oQ        Jiban Clifweb on telegram
12      UCovRt28jl_hp0q4EPAP6xKA        Text stockcryptohack on telegram
3       UCK9Rwz-OCW1lcmSfmY_bhsg        Text VCminers ON TELEGRAM
4       UC-Hf7fHeaPR2cK_md2IgFVg        Netto*REALLY HACKER VINCENT02 ORIGINA ON TELEGRAM
```

図23: paxxkデータセットからTelegramに言及しているチャンネル名

簡単なテキスト処理と正規表現のトリックを使って、このリストから合計144のTelegramユーザーネームを抽出しました。ほとんどの場合、1つのTelegramユーザー名が、数十の個別のYouTubeチャンネルにリンクしている可能性があります。その一例が図24に描かれています。

また、Telegramのユーザー名に対応するアカウントのセットごとに、個別のチャンネルや動画への投稿数を集計しました。その結果は図25に示されています。

特定された最もアクティブな5人のTelegramユーザーについて、彼らが最も頻繁に関与しているチャンネルをカウントしました。出力の一例を図26に示します。

最後に、全てのTelegramユーザーのエンゲージメントを合計すると、どのYouTubeチャンネルがこのグループによって最もブーストされているかがわかります。これは、図27に描かれています。

```
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/UCSXy2_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/UCSKfgvWU9jz9ijT4DQCVDDA      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/UCV7VdcxgAiHStWR5WZWLdPw      7
https://www.youtube.com/channel/UCT6EtPtSvUiDBlW6CCSi6Ng      4
```

図24: Telegramのユーザー名「wendytrad45」に関連するYouTubeチャンネル

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

図25: paxxk[.]bizデータセットに含まれる最もアクティブなTelegramユーザー

```
wendytrad45
105 "Your Crypto Helper"   https://www.youtube.com/channel/UCDKkNGb_DzSrIcnLtx_w-gg
96 "EARNING MONEY 89"   https://www.youtube.com/channel/UCGVJMAJ7J_Fi6KlfqBSeWNg
45 "Total Trx Earning"   https://www.youtube.com/channel/UC2OwNH8lrsHrke-MDegitvA
33 "Crypto Baba"   https://www.youtube.com/channel/UCvWRQiyKF7qlDJQYSqjHGCA
32 "EARNING CHOICE"   https://www.youtube.com/channel/UCMPoJI8c3_qNC84ST0neLQw
21 "Crypto Leny"   https://www.youtube.com/channel/UCpuv8_j_nBiIP8rlbsUIvbg
17 "Crypto Earning Tricks"   https://www.youtube.com/channel/UCrPiLJpdXl8rvNn_DVsKbgA
14 "David - Nft, Crypto, Play to Earn - Defi"   https://www.youtube.com/channel/UCo5uIhofGlM5EJXY_oqblQw
13 "Excellent Kumar'S Tutorial"   https://www.youtube.com/channel/UC4tPqTOs8kn8g2-4u8IRTVQ
12 "Kama Channel"   https://www.youtube.com/channel/UC7VVNue4IUTMDMNE_CQODQ

easyworldweb
114 "Your Crypto Helper"   https://www.youtube.com/channel/UCDKkNGb_DzSrIcnLtx_w-gg
70 "Total Trx Earning"   https://www.youtube.com/channel/UC2OwNH8lrsHrke-MDegitvA
26 "EARNING MONEY 89"   https://www.youtube.com/channel/UCGVJMAJ7J_Fi6KlfqBSeWNg
19 "EARNING CHOICE"   https://www.youtube.com/channel/UCMPoJI8c3_qNC84ST0neLQw
18 "ALL CRYPTO NFTs"   https://www.youtube.com/channel/UCinKKc1lC60nDeiqwlVSqBA
11 "Crypto Baba"   https://www.youtube.com/channel/UCvWRQiyKF7qlDJQYSqjHGCA
8 "Kama Channel"   https://www.youtube.com/channel/UC7VVNue4IUTMDMNE_CQODQ
6 "Excellent Kumar'S Tutorial"   https://www.youtube.com/channel/UC4tPqTOs8kn8g2-4u8IRTVQ
6 "Kwarta Online"   https://www.youtube.com/channel/UCmJ8BjuwQGEbk-8dnYbodBw
4 "David - Nft, Crypto, Play to Earn - Defi"   https://www.youtube.com/channel/UCo5uIhofGlM5EJXY_oqblQw

omlhacks
34 "Total Trx Earning"   https://www.youtube.com/channel/UC2OwNH8lrsHrke-MDegitvA
20 "Crypto Baba"   https://www.youtube.com/channel/UCvWRQiyKF7qlDJQYSqjHGCA
13 "TECH RAGE"   https://www.youtube.com/channel/UCwEmguxJ1IWsO4Kc0aIPttQ
9 "Your Crypto Helper"   https://www.youtube.com/channel/UCDKkNGb_DzSrIcnLtx_w-gg
9 "ALL CRYPTO NFTs"   https://www.youtube.com/channel/UCinKKc1lC60nDeiqwlVSqBA
8 "Kama Channel"   https://www.youtube.com/channel/UC7VVNue4IUTMDMNE_CQODQ
8 "EARNING CHOICE"   https://www.youtube.com/channel/UCMPoJI8c3_qNC84ST0neLQw
```

図26: 最もアクティブなTelegramユーザーのYouTubeチャンネルで
最もエンゲージメントの高いアカウント

```
Telegram boosted
321 "Your Crypto Helper"   https://www.youtube.com/channel/UCDKkNGb_DzSrIcnLtx_w-gg
164 "EARNING MONEY 89"   https://www.youtube.com/channel/UCGVJMAJ7J_Fi6KlfqBSeWNg
152 "Total Trx Earning"   https://www.youtube.com/channel/UC2OwNH8lrsHrke-MDegitvA
76 "Crypto Baba"   https://www.youtube.com/channel/UCvWRQiyKF7qlDJQYSqjHGCA
59 "EARNING CHOICE"   https://www.youtube.com/channel/UCMPoJI8c3_qNC84ST0neLQw
34 "Kama Channel"   https://www.youtube.com/channel/UC7VVNue4IUTMDMNE_CQODQ
33 "David - Nft, Crypto, Play to Earn - Defi"   https://www.youtube.com/channel/UCo5uIhofGlM5EJXY_oqblQw
32 "ALL CRYPTO NFTs"   https://www.youtube.com/channel/UCinKKc1lC60nDeiqwlVSqBA
22 "Crypto Leny"   https://www.youtube.com/channel/UCpuv8_j_nBiIP8rlbsUIvbg
21 "Excellent Kumar'S Tutorial"   https://www.youtube.com/channel/UC4tPqTOs8kn8g2-4u8IRTVQ
```

図27: paxxkデータセットでTelegramユーザーのアカウントによって最もブーストされたチャンネル

これらのTelegramユーザーが「ブースト」した動画の「返信」セクションをスクロールすると、動画で実演されていることが正当なものであると視聴者に思わせるようなコメントがたくさん表示されます。これらのコメントの多くは、チャンネル名にTelegramのユーザー名を含むアカウントによって投稿されています。その一例を図28に示します。

これらのTelegramユーザーがブーストしているアカウントにアクセスすると、YouTubeには同じ作者による他のアップロード済み動画のリストが表示されます。これらは、他の詐欺アプリにリンクされた動画であることが多いです。「PSEB STUDY HALL」チャンネルからの例を図29に示します。スクリーンショットでわかるように、このようなアプリのリストは延々と続いており、毎日新しいものが追加されています。このように回転率が高いため、潜在的な被害者は、既知の詐欺を検出するサービスでこれらのURLを調べることができません。

図29に示すURLについてTwitter検索を行いました。その結果、図30に示すようなツイートが1件のみ見つかりました。今回のリサーチでは、Twitter上で悪意のあるリンクが見つかることは稀でした。

図31に、データセットに含まれる全てのコメントのやりとりのノードエッジグラフを示します。

図28: 特定されたTelegramユーザーに関連するアカウントが公開したコメントのサンプル

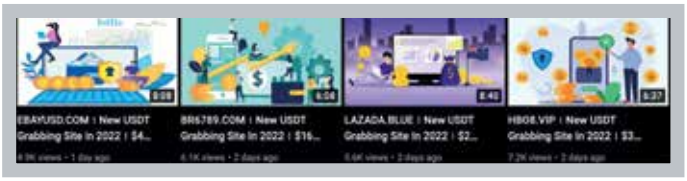


図29: PSEB STUDY HALL」チャンネルでのその他のアップロード作品

図30: ebayusd.com USDT マイニング詐欺アプリにリンクするツイート

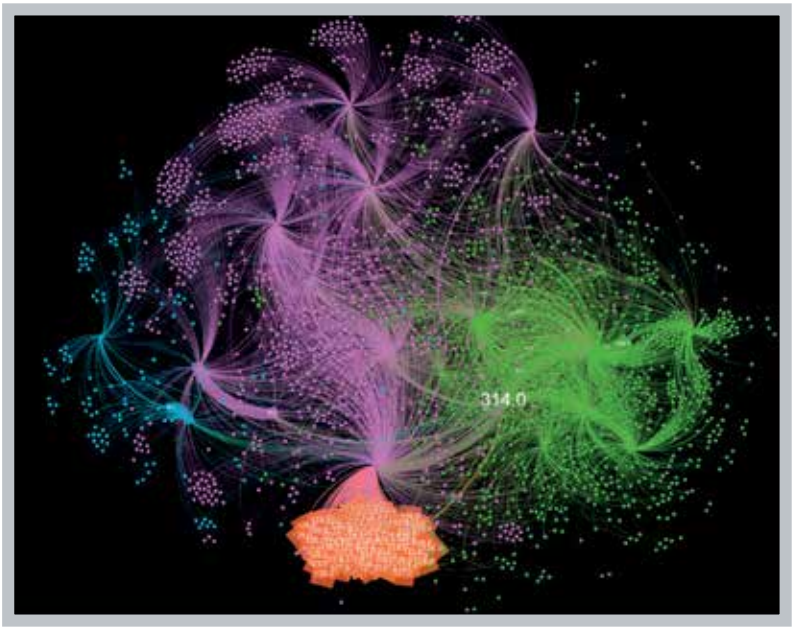


図31: paxxkデータセットにおける相互作用のノードエッジグラフ。ノードは重み付けされた次数によってラベル付けされている。数値が高いほど、そのアカウントが公開したコメント数が多い。

314.0と書かれた緑色のノードは，このデータセットで最も多くのコメントを投稿したアカウントである．図32に描かれている。このチャンネルは動画をホストしておらず、コメントを公開するためにのみ使用されている。

コメント数が110から140のオレンジ色のクラスタは、図33に描かれている「Get Set Earn」と「EARNING STORE」という2つのチャンネルにほとんどのコメントを公開しているYouTubeチャンネルの小グループを表しています。

このブースト行為に関与したアカウントは、先に確認したTelegramユーザーのものではありませんでした。YouTubeのチャンネル名の一覧を図34に示します。

Telegramユーザーのブーストアクティビティは高度に分散しているため、特定されたTelegramユーザーに関連するノードをグラフビズ上で明確に可視化することはできません。

図32: paxxkデータセットで最も活発にコメントされているYouTubeチャンネル

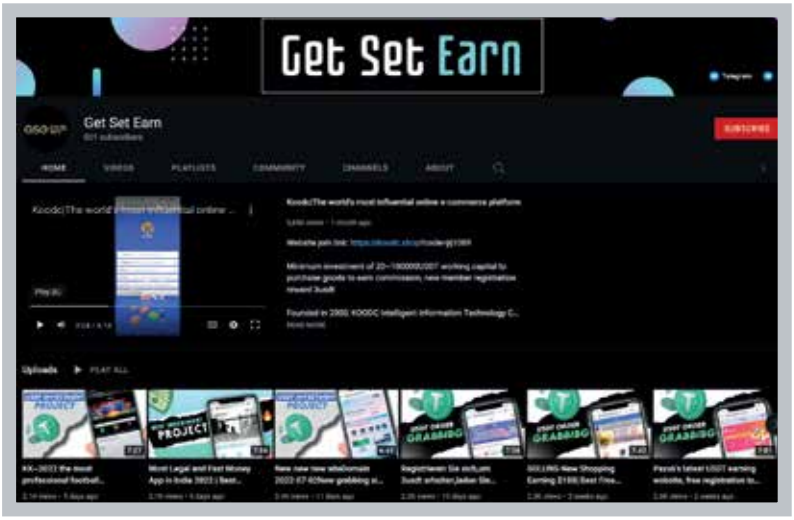
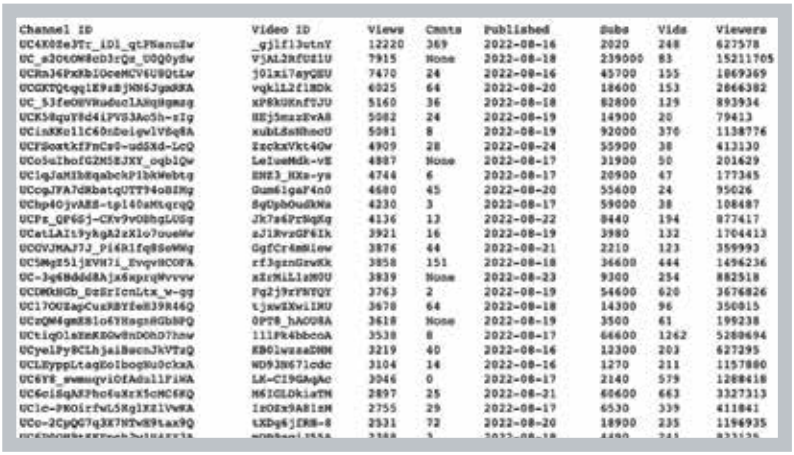


図33: Get Set Earnチャンネル、少数のアカウントからの数百のコメントでブースト

図34: Get Set EarnとEARNING STOREのチャンネルをブーストしたアカウント

5. ocitt[.]siteマイニングプール詐欺に関連するYouTubeアクティビティの分析

同様の詐欺は、ocitt[.]siteというURLを使用して確認されました。paxxk[.]bizと同じ分析方法を使用して、一連の観察結果が記録されました。api.search_by_keywords(q=keyword, count=100)を使用すると、73のチャンネルが投稿した、タイトルまたは説明文に「ocitt」の文字列が一致する77の動画を含む100の検索項目が返されました。全ての動画は、2022年8月16日から24日の間に公開されたものです。これは、paxxk[.]bizアプリで実施されたキャンペーンよりも若干ボリュームがあり、長期間に渡って実施されたことを意味します。図35は、最も視聴回数の多い動画から収集した統計のサンプルです。コメント数が視聴回数と意味のある形で相関していないことに注目してください。



Channel ID	Video ID	Views	Cmts	Published	Subs	Vids	Viewers
UC4K0Ze3Tr_iDl_qtPNanuZw	_gjlfl3utnY	12220	369	2022-08-16	2020	248	627578
UC_s2OtON8eD3rQz_U0Q0ydw	VjAL2RfUIlU	7915	None	2022-08-18	239000	83	15211705
UCRnJ6PxKblOceMCV6U8QtLw	j0lxi7ayQEU	7470	24	2022-08-16	45700	155	1869369
UCGXTQtqqlE9zBjKN6JgmKKA	vqkiL2flMDk	6025	64	2022-08-20	18600	153	2866382
UC_5JfeO8VNuduclAHqHgmzg	xP8kUKnfUJU	5160	36	2022-08-18	82800	129	893934
UCK54quY8d4iPVS3Ac5h-zIg	HEj5mzzEvA8	5082	24	2022-08-19	14900	20	79413
UCinKKo11C6OnDeigwlV8q8A	xubLdaNhooU	5081	8	2022-08-19	92000	370	1138776
UCFSoxtkfFnCs9-udSXd-LcQ	ZzckzVkt4Qw	4909	28	2022-08-24	55900	38	413130
UCo5ulhofGZM5EJXY_oqblQw	LeluoMdk-vE	4887	None	2022-08-17	31900	50	201629
UClqJaM3bEqabckP1bkWebtg	ENE3_HXs-ys	4744	6	2022-08-17	20900	47	177345
UCcgJYA7dRbatqUTT94oBIMg	Gum6lgaF4n0	4680	45	2022-08-20	55600	24	95026
UChp4OjvAES-tpl40aMtqrqQ	8qUpbOudkNs	4230	3	2022-08-17	59000	38	108487
UCPz_GP6Sj-CEv9vOBhgLUSg	Jk7s4PzHqXg	4136	13	2022-08-22	8440	194	877417
UCatLALt9ykgA2eXlo7oueHw	aJ1RvzGF6Ik	3921	16	2022-08-19	3980	132	1704413
UCGVJMAJ7J_Pi4R1fq8SeWWg	GqfCr6m8iew	3876	44	2022-08-21	2210	123	359993
UC5MgZ51jEVH7i_EvqvHCOFA	rf3gznGzwXk	3858	151	2022-08-18	34600	444	1496236
UC-3q6BddABAjx6xpzqWvvvw	xErMiLlsM0U	3839	None	2022-08-23	9300	254	882518
UCDMGhGb_GsErIcnLtx_w-gg	FqZj9rFNTQY	3763	2	2022-08-19	54600	620	3676826
UCl7OUIagCuxRBYfwEJ9R46Q	tjxwIXwiIMU	3670	64	2022-08-18	14300	96	350015
UCzQM4gmE8lo6YHsgnHGbBPQ	0PT8_hAOO8A	3618	None	2022-08-19	3500	61	199238
UCtiQlsEmKZGw8nDOhD7hnw	111Pk4bbcnA	3538	8	2022-08-17	64600	1262	5280694
UCyelPy9CLhjaiBwcnJkVTzQ	KB0lwzaaDNM	3219	40	2022-08-16	12300	203	627295
UCLEyppLtaqEoIbogKu0ckxA	WD9JN67lcdc	3104	14	2022-08-16	1270	211	1157880
UC6YE_wwmuqviOfAdallFiWA	LK-C19GAqAc	3046	0	2022-08-17	2140	579	1288418
UC6ciSqAKFhc6uXrX5cMC6KQ	M6ICGLbkiaTM	2897	25	2022-08-21	60600	663	3327313
UCic-PKOirfwL5Kg1XZ1VwKA	IsOZx9A8IsM	2755	29	2022-08-17	6530	339	411841
UCc-2CpQG7q3X7NTwH9tax9Q	tXDq6jfKB-8	2531	72	2022-08-20	18900	235	1196935

図35: ocitt[.]siteに関連する動画で、再生回数が多いものの統計情報

paxxkの例と同様に、この詐欺に関与した全てのチャンネルは複数の動画を公開し、ほとんどの場合、登録者数と視聴回数の両方が高くなっています。

次に、YouTube APIを使用して、事前検索で特定された73の各チャンネルの全動画のリストを取得しました。この過程で、合計15,221本の動画が発見されました。続いて、APIを使用して、全ての15,221の動画に返信するために投稿された全てのトップレベルのコメントを取得しました。このようにして、130,106のユニークなチャンネルから、合計264,277のコメントが取得されました。図36は、最も多くのコメントを受け取った10チャンネルのリストを含む、いくつかの統計情報を示しています。

```
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/UC5MgZ51jEVH7i_EvqvHCOFA
10010   https://www.youtube.com/channel/UChelUCPKf2061D_KDoOsAWg
9994    https://www.youtube.com/channel/UCM3Y2aateudYcTCvROAE7Ig
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
```

図36: ocitt[.]site度について投稿しているアカウントのYouTubeコメントに関する統計。数値が高いほど、そのアカウントが公開したコメントが多い。

このデータセットで最も多くのコメントを得たチャンネルは、図37に示すように、YouTubeの認証済みアカウントである「Offer Tricks」でした。

このデータセットのコメンターから177人のTelegramユーザーのセットが見つかりました。最もアクティブなもののリストは、paxxkデータセットから収集したリストと密接に類似しており、図38に示すとおりです。

Telegramユーザーが最もコメントしたチャンネルは、図39に表示されています。このリストは、paxxkデータセットから抽出したリストと大きく重複しています。「Your Crypto Helper」はどちらも上位にあり、この時点でそのチャンネルの背後にいる人物がTelegramユーザーの一人であると推定されるかもしれません。

図37: ocittデータセットで最もコメントされた "Offer Tricks "アカウント

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

図38: ocittデータセットに含まれる最もアクティブなTelegramユーザー

```
Telegram boosted
671 "Your Crypto Helper"   https://www.youtube.com/channel/UCDMkHGb_DzSrIcnLtx_w-gg
529 "NIXON Cryptofy"   https://www.youtube.com/channel/UCotXIBQmD9s5NrFiexyBUXQ
486 "TIGER EARNING"   https://www.youtube.com/channel/UC5Mq251jEVH7i_EvqvBCOFA
463 "Crypto Master 2022"   https://www.youtube.com/channel/UCtiqOlsEmKZGw8nDOhD7hnw
451 "SV Earning"   https://www.youtube.com/channel/UC6POOB9tKKFpch2w1H4ZYJA
427 "Tricky Boss"   https://www.youtube.com/channel/UCc-2CpQG7q1X7NTwH9tax9Q
370 "EARNING MONEY 89"   https://www.youtube.com/channel/UCGVJMAJ7J_Pi6RIfq8SeWWg
216 "The School Crypto"   https://www.youtube.com/channel/UCoNGK1ktBEU5rn3fIGT-uDA
207 "Crypto Deniz"   https://www.youtube.com/channel/UChjIBl7IoIOOxrf29mnjlvw
204 "Intelligent AJK"   https://www.youtube.com/channel/UCXfEPYOQTb8vwEbgCefADUA
```

図39: ocittデータセットでTelegramユーザーのアカウントによって最もブーストされたチャンネル

6. #usdtmining YouTubeハッシュタグに関連するYouTubeアクティビティの分析

ハッシュタグ #usdtmining を含むYouTube ページを Web UI で表示することができます。図40に示すように、このハッシュタグは3,900本の動画と792のチャンネルを表していると報告されています。このページは、https://www.youtube.com/hashtag/usdtmining というURLで表示することができます。

残念ながら、YouTubeのAPIではハッシュタグページの項目を一覧表示することができないため、検索機能を用いて結果を得る必要がありました。この結果は、図40の結果とは大きく異なっています。YouTube APIは、1日あたり10,000回という利用枠が設定されています。1回の検索クエリで100オペレーションを消費し、実験では100クォータのブロックを25件の検索結果で使い切ってしまうことが判明しました。そのため、検索結果は最大2,500件に制限されます。Web UIで表示されるハッシュタグページには3,900本の動画が報告されており、APIで全てを取得することは不可能と想定されました。api.search_by_keywords(q=keyword, count=1000)の形式でテスト検索を行ったところ、527本の動画が返され、そのうち520本は動画のタイトルか説明に「usdt」という単語が含まれていました。この検索では、合計269のチャンネルが特定されました。多くのチャンネルが見つかったため、各チャンネルの追加の動画は収穫されませんでした。しかし、最初の検索で返された全ての動画のトップレベルのコメントは、APIを使用して取得されました。

図40: Web UIで表示されるYouTube #usdtminingの結果ページ

Channel ID	Video ID	Views	Cmts	Published	Subs	Vids	Viewers
UC4YdJQqrLqdbGJDpc3hicuA	Lk5F8jIW2PM	50613	401	2022-05-27	162000	53	15742568
UCF0LL0E6RD4Deha9a2dP4lQ	1NT9m_MprFo	30811	342	2021-11-27	45500	82	1299686
UCjihT4MaDfiPnjL52VtNMfg	pd8JoarBG-U	22822	102	2022-08-03	612000	59	21040671
UCnJaUeiea9qfaKTj4Ihsg3Q	4AukcWwQ9C4	22284	143	2022-05-07	566000	730	15419718
UCUwqySjGexPTBcshNFYO-w	CE1znZGKbkA	20847	285	2022-08-25	95100	31	494666
UCgsbpLB2440VD2LpRmIv_kg	OI4OJaKdx_k	20648	1	2022-06-17	22800	90	928720
UC2OPyaxbwDbje8YjynuUm6Q	Y6jOuSXWLzs	17130	103	2022-01-23	15600	545	1066668
UCSonJpwwfq9sRX_Wge384HQ	slPC2zbb4mY	16121	180	2022-09-01	104000	82	47987935
UCwBhujfY4vnNyWVLOEv8Bdw	GLqRj6eoI20	16015	141	2022-09-03	117000	49	1187093
UC3jK2nntdaF8BCXGOljvC8Q	qJCOAcn4aic	14762	114	2022-09-01	44700	143	2135235
UCe8N6DGOfByC5gSzizakk7w	f-MrfWB8R8Q	13511	30	2022-07-12	252000	68	50615198
UCvJCo6Kot9VCIh5eSi9k5vA	Yuimo99otjo	12479	68	2022-09-01	16000	22	4499616
UC6tPgTOz8koRg2-6u8IRTVQ	h42B5NKk5Yg	11452	142	2022-08-04	599000	1957	41723231
UChB3aI7XRpPcbjRkBJZ7gKg	Xj8GCC_a2xE	11431	0	2022-03-16	289000	205	1011777
UCKMdcXX0cVR0IvGQaxAgD2w	nHCmj2M9uu4	10075	28	2022-07-02	105000	62	764818
UCh1VxBowHcBvLqSdcLiLMOA	LjWB8b7gWNE	9032	105	2022-06-21	102000	292	6909772
UCODOAYz6tjpC-T0IIKl7haQ	VrS-_lxcocQ	8728	3	2022-03-20	1570000	929	44130437
UCtyTfyxD_mJ_XCyB26qmavg	YZNBPi5OugQ	8256	4	2022-04-14	219000	822	26061880
UCHs3YP9163VlvBFQPswNAzw	_2Lv826emNA	8090	83	2022-09-03	79800	101	912036
UCAw66QhuMDQJTzhB5bd1bjA	GI2zgOxadhw	8029	3	2022-05-14	54000	109	1576043
UCVKGHYD5pUE7po8FDcRXF9A	AobR_AKLIh0	8014	14	2022-04-20	5440	23	154419
UCHp8BYopW8gjoaNpQnl1yRA	7XpviE3JJns	7727	8	2022-05-03	1070	69	428691
UCa9WnlcM5rkKaObMlUhw9Lg	tjsjTqJ46sI	7463	74	2022-04-24	3790	131	128545
UCRQ4EAAkCb09EKsU8U2QDlg	UJWVdgskG7o	7295	15	2022-06-29	46200	59	432784
UCcxDgeUNEKi0GzyIdhZAP9w	mjF579B-mG0	7267	5	2022-07-21	368	197	829907

図41: 視聴回数の多い #usdtmining 関連動画の統計データ

合計11,710件のコメントが収穫されました。統計は図41に示すとおりです。

このようにして、5,256のユニークなチャンネルから、合計11,710のコメントが得られました。なお、コメントを含む動画は485件のみです。図42は、最も多くのコメントを得た10チャンネルのリストなど、いくつかの統計情報を示しています。

図43は、#usdtminingデータセットに含まれるチャンネル間のインタラクションのノードエッジグラフを示したものです。ノードは、インディグリー (コメント受信数) でラベル付けされています。このグラフは、#usdtminingのハッシュタグの多くの動画が、全く別のアカウントグループからコメントを受け取っていることを示しています。グラフの真ん中の混乱は、コメンター間の重複が起こった場所を示しています。

```
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
```

図42: YouTubeコメントに関する統計 (#usdtmining データセットより)

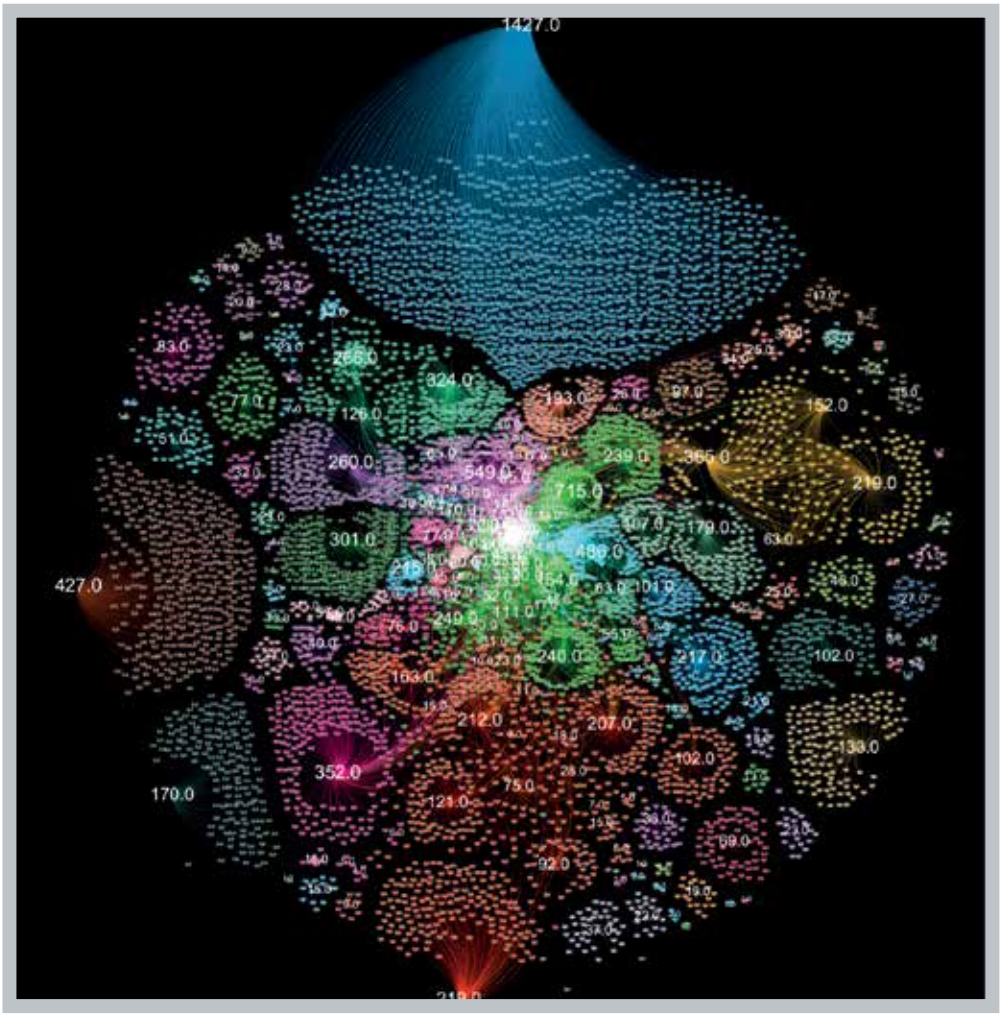


図43: usdtminingデータセットにおけるインタラクションのノードエッジグラフ。ノードは次数でラベル付けされている。

このデータセットで最も多くのコメントを得たチャンネルは、図44に描かれている「Crypto Master 2022」です。これは、認証を受けたアカウントではありません。

本データセットのYouTubeチャンネル名から、合計92のTelegramアカウント名を発見しました。彼らは1,554件のコメント投稿に関与していました。最もアクティブな10人のTelegramユーザーのリストは、図45に示されています。

Telegramユーザーから最も多くのコメントが寄せられた10アカウントのリストを図46に示します。これまでのリストと重複していることがよくわかります。

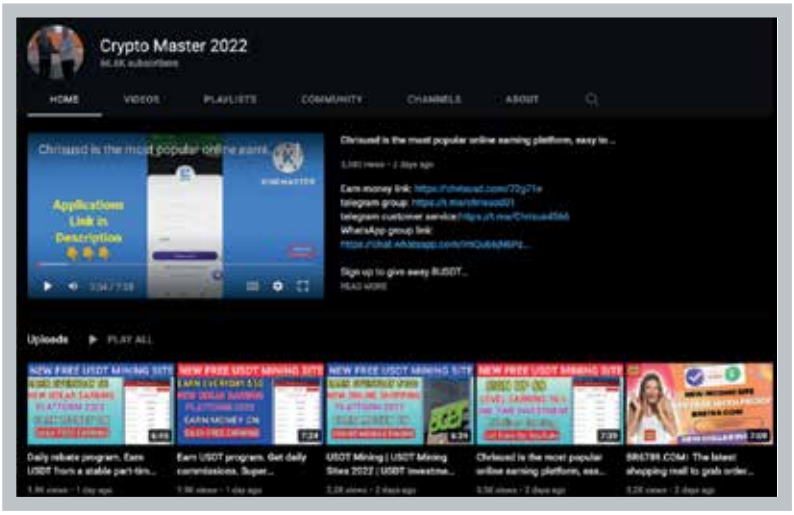


図44: Cusdtminingのデータセットで最もコメントされた「Crypto Master 2022」アカウント

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

図45: Musdtminingデータセットで最もアクティブなTelegramユーザー

```
178 "Crypto Master 2022"   https://www.youtube.com/channel/UCtiqOlsEmK3Gw8nDOhD7hmw
172 "MINING BOI"   https://www.youtube.com/channel/UCJNGmfXWw3THnI0Vt4ExhFw
101 "PSEB STUDY HALL"   https://www.youtube.com/channel/UCRpItF2j5jeWfstw4hLwJGg
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_Iw
52 "Earning day"   https://www.youtube.com/channel/UCNeByWhsQ9CHIIF-C54VWVw
47 "Golden Crypto"   https://www.youtube.com/channel/UCDWftLCMxVViH9urcoEKK8Q
47 "Earning Mantra"   https://www.youtube.com/channel/UCwBhujfY4vmNyMVLOEv8Bdw
45 "TIGER EARNING"   https://www.youtube.com/channel/UC5Ng75ljEVH7i_EvqvHCOFA
42 "EARNING MONEY 89"   https://www.youtube.com/channel/UCGVJMAJ7J_Pi6K1fq8SeWWg
```

図46: usdtminingデータセットでTelegramユーザーのアカウントによって最もブーストされたチャンネル

7. その他の分析

Telegramユーザーがブーストしたアカウントは、これらの詐欺に関連する動画を大量に投稿していることが容易に観察されます。図47は、「PSEB STUDY HALL」チャンネルがホストしている動画のサンプルです。スクリーンショット内の各ビデオの再生回数が似ていることに注目してください (6,000回～10,000回の間)。エンゲージメントを高めるために、Telegramユーザーによって投稿されたコメントに加えて、他の形の非正規アクティビティ (偽のいいね、ビュー、チャンネル登録など) が使用されていると推測されます。このような行為によって、これらの動画はYouTubeのアルゴリズムによって推奨される可能性が高くなります。

図47: PSEBSTUDYHALLのYouTubeチャンネルにアップロードされた動画

図48は、「Crypto Master 2022」がホストしている動画のサンプルです。Crypto Master 2022はPSEB STUDY HALLよりもブーストされていますが、スクリーンショット内の動画の再生回数にはかなり大きなばらつきがあります。

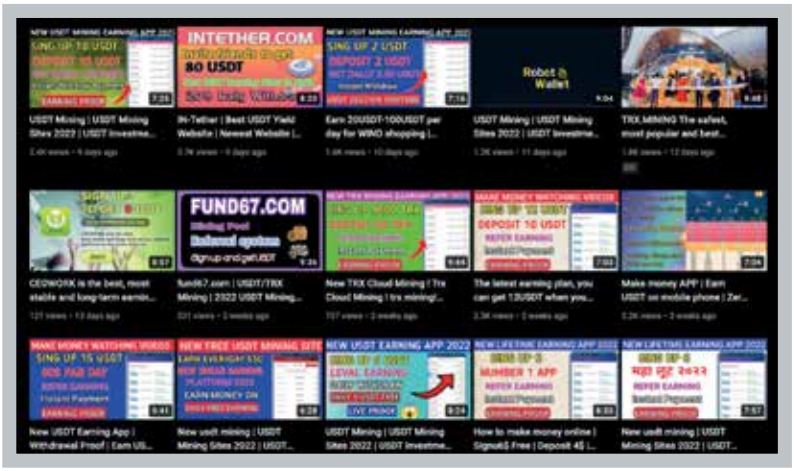


図48: VCryptoMaster2022のYouTubeチャンネルにアップロードされた動画

また、図49に示すように、これらのチャンネルは、同じ詐欺アプリの宣伝動画を複数投稿していることも注目すべき点です。サムネイルと動画の時間から、これらは常に元の動画の再アップロードであることがわかります。

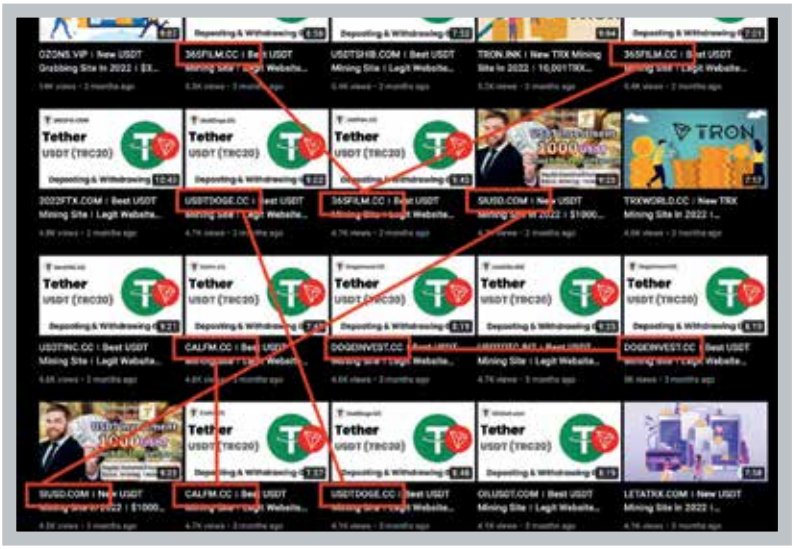


図49: 再アップロードによる映像の複製 (PSEB STUDY HALLチャンネル)

このリサーチを行っている間、多くの関係チャンネルが定期的にチャンネル名を変えていることが明らかになりました。例えば、「TIGER EARNING」チャンネルは「Crypto With Earning」に改名しています。YouTubeのchannelIdを使用してこれらのチャンネルを追跡すると、名前の変更を追跡することができます。

3つのデータセット全てから得られた動画のタイトルと説明文からURLを抽出しました。このようにして、合計700のユニークなアプリのURLを取得しました。図50は、取得したURLのトップサンプルについて、キャンペーンの開始日と終了日、日数、投稿された動画数などの統計情報を示しています。リストの約3分の1から15本の動画数が一貫しているのは、新しい詐欺アプリが作成されたときに動画を投稿する通常のチャンネルグループの規模を表していると思われます。

Telegramユーザーに関連するチャンネルに関連するコメントが採取されました。各ユーザーについて、最初に見つかった40文字でコメントをグループ化しました。これにより、ほぼ同一のコメントを発見することができました。全てのTelegramユーザーは、複数の動画に渡ってほぼ同一のコメントを何度も公開していました。同じ動画に対して、同じコメントが複数回投稿されていることもありました。図52と図53は、2人のTelegramユーザーが投稿したコメントのコピペ性を示しています。

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
trx1.love	2022-04-04	2022-04-29	25	13
earnshope.com	2022-08-29	2022-09-06	8	13

図50: 3つのデータセットでキャプチャされた動画のタイトルと説明文から、最も多く見られたURL

図51: 各詐欺アプリのURLに関連するチャンネル

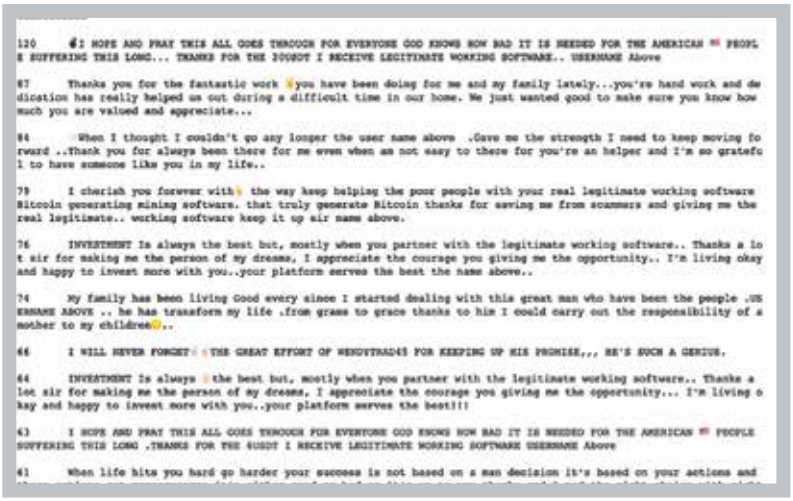


図52: wendytrad45 からのコメント (最初の40文字の類似性による)。左の数字は、そのコメントがデータ上で何回見られたかを示している。

余談ですが、Twitterで#USDTMINING というハッシュタグが発見されました。これはUSDTマイニングプールの詐欺を間接的に宣伝するために使われていたのです。女性アバターのアカウントが投稿したツイートは、USDTのマイニング方法を知るためにダイレクトメッセージを送るよう求めています。全てのツイートはほぼ同時刻に公開され、内容も同一であることから、自動化が利用されていることが示唆されました。図54にそのようなツイートのサンプルを示します。Twitterには#miningusdtというハッシュタグも存在します。

図53: brainscott001 からのコメント (最初の40文字の類似性による)。左の数字は、そのコメントがデータ上で何回見られたかを示す。

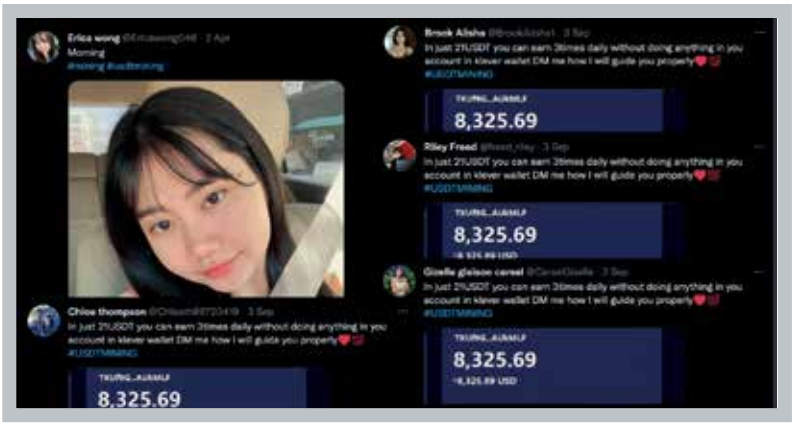


図54: USDTMININGのハッシュタグを含むツイート例

8. 暗号資産トランザクションの分析

この詐欺に関連するYouTube動画では、個人の暗号資産ウォレットからアプリに資金を移動する方法を視聴者に指示しているため、動画を手動で検査することにより、各アプリに関連するウォレットアドレスを特定することが可能です。ウォレットアドレスは、アドレスを書き写す方法と、ビデオに表示されたQRコードをスキャンする方法の2つの方法でビデオから抽出することができ、後者が望ましいとされています。このプロセスを用いて、これらの業務に関連する様々なYouTubeチャンネルから投稿された動画から、合計30個のウォレットアドレスを抽出しました。なお、YouTubeのメタデータを解析した結果、合計700のユニークなURLが見つかりましたが、この30個のアドレスは、関係する全てのウォレットのごく一部であることがわかります。

問題のYouTube動画からウォレットアドレスを手動で抽出するのは、かなり面倒な作業でした。自分のアカウントにログインした状態で動画を開くと、わずかな数の動画を見ただけで、YouTubeがそのコンテンツを強く推奨するようになるため、動画はシークレットブラウザで開く必要があります。現在、YouTubeでは、数分間の動画視聴ごとにブロックできない広告が表示されます。そのため、詐欺動画からウォレットアドレスを手動で抽出する際には、何度も何度も広告を見ることを余儀なくされました。何時間も広告を見続けなければならないことが、30個のウォレットアドレスを抽出しただけで作業を中断した理由です。

関連する全ての動画から抽出されたウォレットアドレスは、トロン暗号資産スキームの一部でした。トロンはUSDTの取引を促進するために使用することができ、この種のウォレットアドレスはtronscan.orgなどのサイトで調べることができます。tronscan.orgのWebインターフェースの例を図55に示します。TRONSCANはまた、任意の有効なウォレットアドレスの過去10,000トランザクションまで照会するために使用できる無料のAPIを公開しています。

本リサーチでは、2022年10月28日(金)に、最大120日前にさかのぼる取引についてデータを収集しました。

YouTube動画から抽出したウォレットアドレス全30個をTRONSCANで照会し、そのうち29個が有効でした。paxxk[.]bizに関連するウォレットアドレスはTRONSCANで照会できず、作り物である可能性が示唆されました。このウォレットアドレスは、YouTubeの複数の動画に登場し、アプリの機能がカメラで実演されています。このウォレットアドレスが無効であることは、paxxk[.]bizのビデオで実演されているアプリが、実演のために作成された特別なビルドであることを決定的に証明するものです。

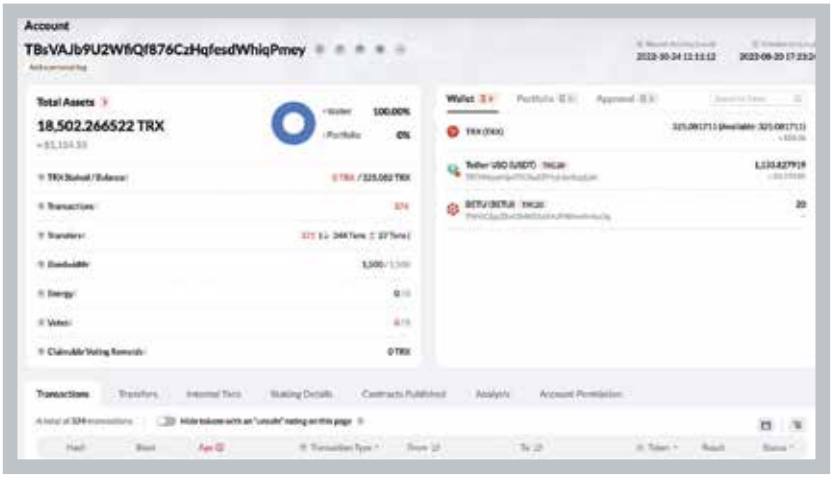


図55: ocitt[.]siteに関連する動画で、再生回数が多いものの統計情報

一部のウォレットでは、アクティビティが全くありませんでした (トランザクション数0)。これには、調査の1ヶ月以上前にYouTubeで宣伝されたアプリに関連するウォレットが含まれています。このことは、これらのYouTube動画で実演されているアプリは、実際の機能を持たないカスタムデモのビルドであるという考えをさらに裏付けるものです。このことから、これらのYouTuberは、引き出し機能を実演していると主張するとき、故意に嘘をついており、したがって、犯罪行為に加担していることを十分に認識していると結論付けることができます。

照会されたウォレットの中には、あるウォレットから整数倍の少額のUSDTを受け取り、その後、別のウォレットに同額を送信しているものがありました。YouTubeチャンネル「PSEB STUDY HALL」が公開した動画の場合、送信側のウォレットアドレスは常に同一でした。「Crypto Master 2022」や「EARNING MONEY 89」など他のチャンネルでは、毎回異なるウォレットアドレスでシード (種まき) が行われました。このような方法で合計5つのシードウォレットが見つかりました。これらのYouTubeチャンネルが投稿した動画からアプリのウォレットをさらに手動で抽出すると、さらなるシードウォレットや、アドレスの重複が判明する可能性があります。

「PSEB STUDY HALL」のシードアカウントは、YouTube動画から抽出した6つのアプリウォレットアドレスへの送金が確認されました。ウォレット「TKnN86vWQtz3PyjfTGbgurGZvSTtdJKKVW」は、キャプチャ時に7,832件のトランザクションを実行していました。その寿命の間に、それは合計12,950 USDTを受信し、合計12,473 USDTを送信しました。このウォレットの徹底的な分析が、レポート全体の礎となるものなのです。

各シードウォレットから少額 (100未満) の整数USDTの支払いを受けたウォレットは、追加のアプリウォレットを発見する目的で特定されました。特定された各ウォレットについて、そのウォレットの取引履歴が合計500件以下の場合のみ、取引データを収集しました。この方法は、これらの詐欺アプリに関連するアクティブなウォレットには、あまり多くのトランザクションが関連付けられていない傾向があるという観察に基づいています。この方法を用いて、5つのシードアカウントで合計1,576個の潜在的なアプリウォレットが発見されました。この数は、YouTubeの動画から抽出されたURLの数 (700) を上回っていることに注目してください。これは、(i) paxx[.]biz, ocitt[.]site, および #usdtmining に関わる再帰的チャンネルによって捕捉されなかった多くの動画がYouTubeに存在する (つまり、YouTube APIが全ての可能な結果を返さなかった) か、または (ii) それらの潜在的アプリウォレットの半分が誤って認識されたかを意味しているのかもしれません。どちらの仮説もある程度は正しく、真の説明はその中間にあると思われます。

成功した詐欺アプリに関連するウォレットを手作業で検査したところ、以下のことが確認されました。

- 被害者のウォレットはアプリのウォレットにUSDTを送信しました。どの被害者ウォレットにもUSDTは送り返されておらず、「引き出し」機能が本当に偽物であることが検証された。
- 被害者から支払いを受けたアプリのウォレットは、定期的にUSDTを「受信」ウォレットに送り、そこから他のウォレットに送られるといった具合です。このような方法で行われる支払いのほとんどは少額で、頻繁に行われるものでした。

潜在的な被害者ウォレットのリストを収集するために、1,576の各アプリウォレットに関連するトランザクションを以下のように分析しました。(i) いずれかのアプリウォレットに10 USDT以上の支払いを行ったウォレットのリストを収集し、(ii) その中で、データセット内のいずれかのウォレットから支払いを受けたウォレットは破棄し、潜在的アプリウォレット以外のウォレットに支払いを行ったウォレットも破棄した。この分析により、合計915の潜在的な被害者ウォレットが得られました。

被害者となりうる口座をざっと調べたところ、数百万米ドルを保有し、数百万回の取引履歴があるものがあることが確認されました。簡潔さを期すため、この種の口座を「クジラ」と表記することにする。

このようなクジラアカウントの一例として、TJDENsfBJs4RFETt1X1W8wMDc8M5XnJhCeが挙げられます。このウォレットは、分析時点で800万USDT以上の取引を行い、7,400万USDを超える保有量を持っていました。このアカウントは、ocitt[.]siteアプリに関連するウォレットであるTBsVAJb9U2WfiQf876CzHqfesdWhiqPmeyや、wstrustfund.comに関連するウォレットのTExJShP2ZFR4zEKnvzoc2ZcRmd9FbBbPjAとやり取りしています。このクジラウォレットは、TRXの保有量に基づく上位175口座のリストに登場しました。このウォレットに関連する大量の取引を考えると、自動取引ボットである可能性があります。

データセットに含まれる7,251のウォレットアドレスそれぞれについて、取引回数を問い合わせました。100万件を超える取引は「クジラ」と呼ばれ、そのようなアカウントは合計28個見つかりました。データセット内のクジラアカウントと他のウォレット間の相互作用を、図56に示しています。

これらのクジラアカウントがこのような不明瞭な詐欺、特に手動で登録し、粗悪で明らかに詐欺的なウェブ「アプリ」とやり取りする必要があるという事実は、非常に非論理的であるように思われます。tronscan.orgのルックアップを通じて、クジラのアドレスを既知の取引プラットフォームや暗号資産取引所と関連付けることは不可能でした。このように、この現象は謎のままであり、現在のTRONエコシステムの理解では解決できないものなのです。

先に特定された潜在的被害者ウォレットからクジラアカウントをフィルタリングした後、その数は900に減少しました。図57は、アクティブな潜在的アプリウォレット、被害者、受信ウォレット間の全てのUSDT関連の金融取引を示しています。ご覧のように、状況はかなり混乱しており、これ以上の推論を解くことは非常に問題があります。しかし、潜在的な被害者ウォレットのクラスタと潜在的なアプリウォレットへの接続は、このような複雑なグラフ表示でも容易に観察することができます。

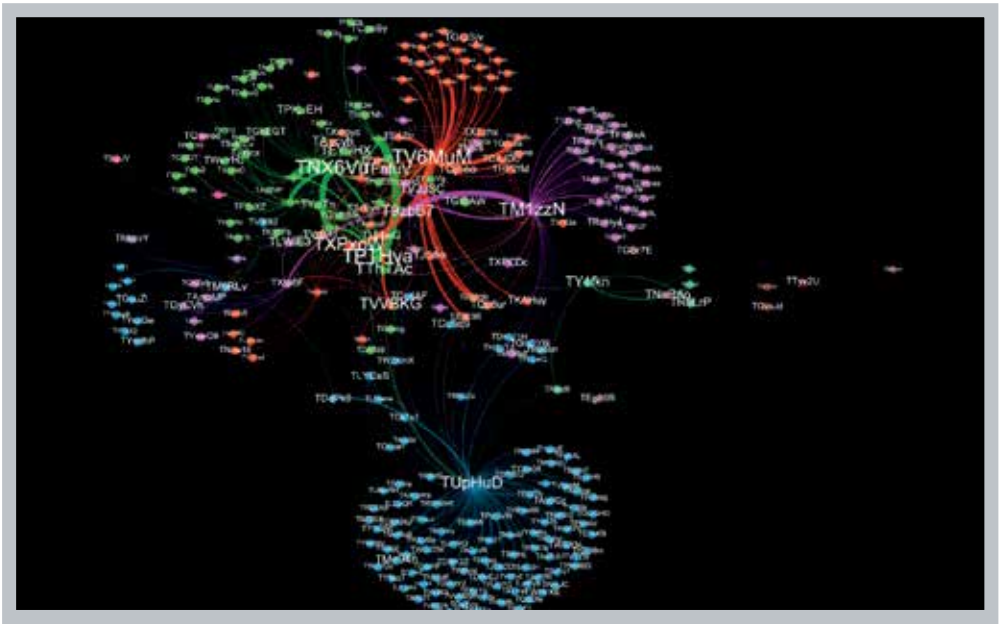


図56: 収集したデータにおけるクジラアカウントと他のウォレットとの相互作用。ウォレットアドレスは最初の6文字に省略されている。

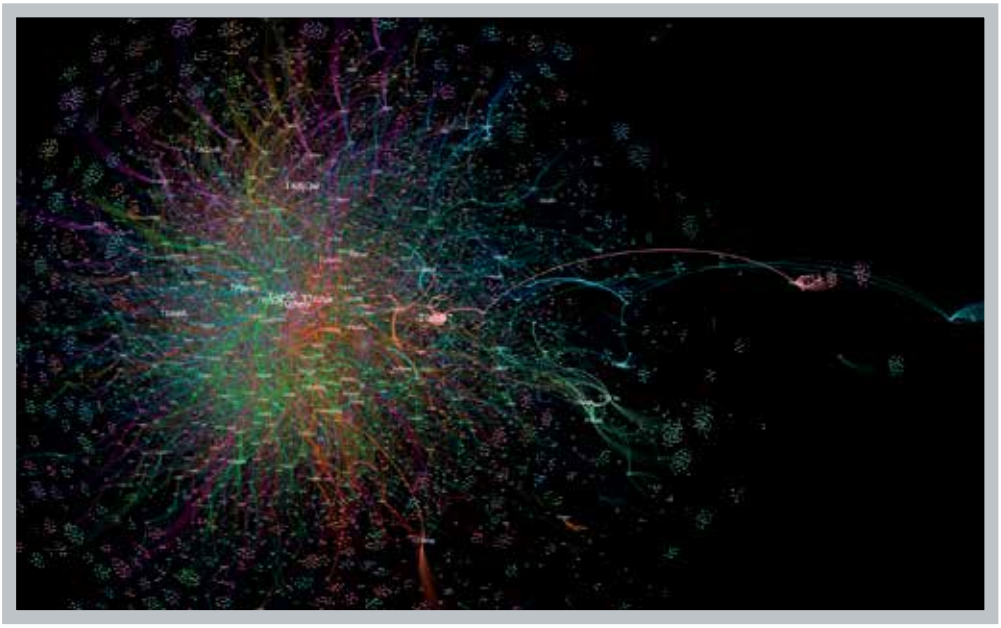


図57: アクティブな潜在的アプリウォレット、被害者、受信ウォレット間の相互作用。ウォレットアドレスは最初の6文字に省略されている。

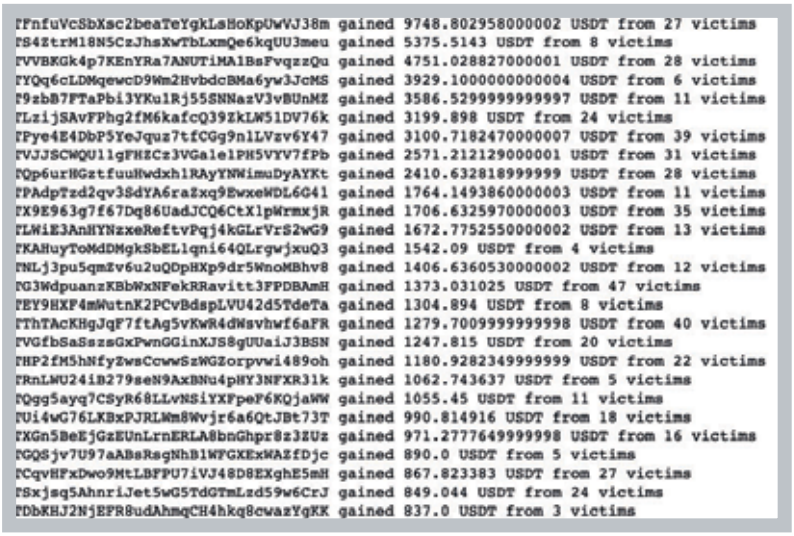


図58: 潜在的なアプリウォレットのうち、売上高が上位のものの例

この過程で発見された潜在的被害者のウォレットからアプリ候補のウォレットへのUSDTの支払いを全て合計すると、およそ115,628USDTという値になります。これらの操作に関与したYouTubeチャンネルの分析で発見されたURLはわずか700件であることから (YouTube API経由で収集したデータ)、この計算に含まれるウォレットの一部は詐欺アプリに属していない可能性があります。逆に、5つのシードウォレットの分析から、今回確認された実際のアプリウォレットの数は、関係するウォレット全体のごく一部に過ぎない可能性もあります。そのため、ここで計算された利益値は、双方向で非常に不正確である可能性が高いです。残念ながら、アプリのウォレットのアドレスとYouTubeの動画を関連付ける方法はありません。この分析で明らかになった潜在的なアプリウォレットアドレスが本当にこの詐欺の一部であるかどうかを正確に検証するには、可能性のある全てのYouTube動画を手動で検査する必要があります。これは現実的ではありません (特に、多くの広告に悩まされることになるため)。また、ここで計算された利益値は、分析時に計算されたものであり、詐欺、特に登場したばかりの詐欺は、新しい被害者をもたらし、それによって新しい収入を得る可能性があります。これらの操作を適切に追跡するためには、YouTubeとウォレットの両方のアクティビティを長期間にわたって定期的に分析する必要があります。

ocitt[.]siteアプリに関連するウォレット（TBsVAJb9U-2WfiQf876CzHqfesdWhiqPmey）は、その有効期間中に合計7504.2004629997 USDTを受け取り、合計6370.372544 USDTを送信しています。これらの取引の全てが被害者の支払いに起因するわけではなく、このウォレットは他の追加的な目的に使用されていたと推測されます。特筆すべきは、TP8ojbCEoV25KSB75iVYK9MNXtH1Ap-wtkAがそこから合計2,892USDTを受け取っていたことです。TP8ojbCEoV25KSB75iVYK9MNXtH1ApwtkAに関連する取引を分析することで、大量の通貨が取引されていることが確認できます。図59は、この口座との間で行われたトランザクションのうち、上位の合計トランザクションの例を示しています。

TP8ojbCEoV25KSB75iVYK9MNXtH1ApwtkAから60,000USDT近くを受け取ったウォレットTNR8hnL8EGEi-35yxYJtWHb2PJW5hPQao6Dはクジラアカウントではありません。捕捉時、この口座は約8,000米ドル相当の通貨を保有し、1,300件強の取引を行っていました。しかし、このアドレスのトランザクションを分析すると、さらに多くの資金が移動していることがわかります。これは図60に示されています。このアクティビティは、クエリの時点で120日間に渡って行われたことに注目してください。このウォレットの全使用期間中の全取引を収集することで、140万ドル以上がこのアカウントを通じて移動したことを判断することができます。このウォレットを経由する資金が、これらの特定の暗号資産詐欺に関連したものなのか、それとも他の「ビジネスベンチャー」を含むものなのかは、現在のところ推測の域を出ていません。

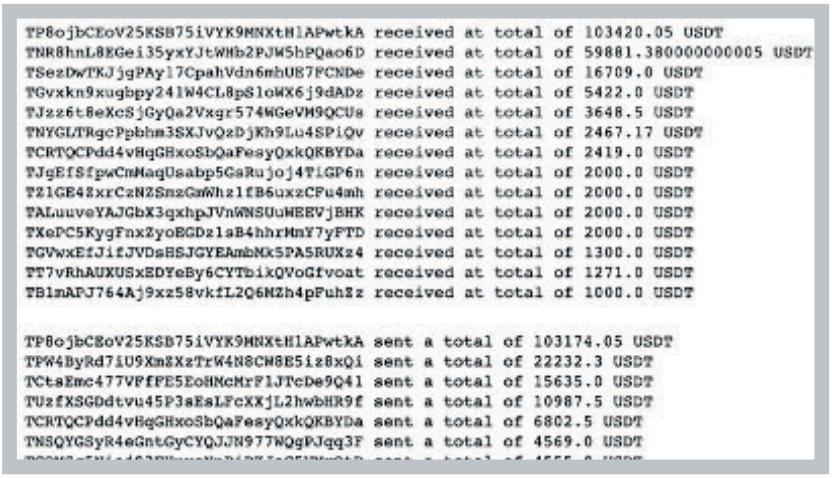


図59: TP8ojbCEoV25KS-B75iVYK9MNXtH1ApwtkAに関連する取引額合計の上位

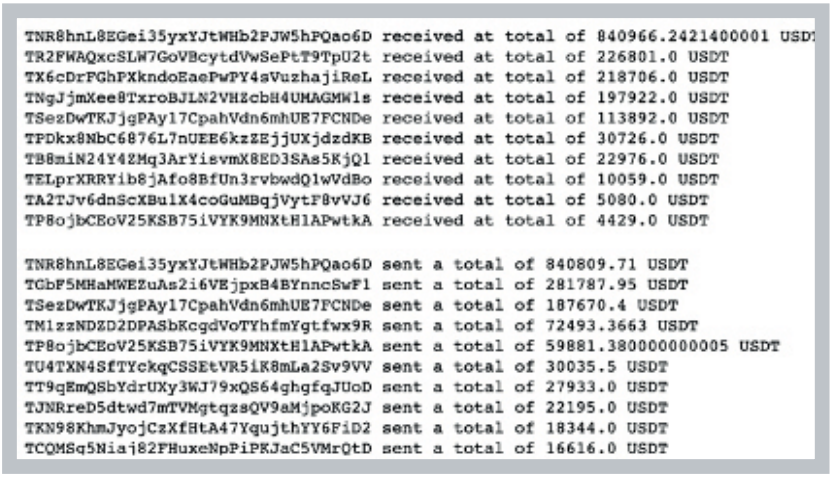


図60: TNR8hnL8EGei35yxYJtWHb2P-JW5hPQao6Dに関連するトランザクションの上位の合計値

このような資金の痕跡を追い続けることは可能ですが、暗号資産ウォレットの難読化により、個人または企業のアカウントを関連付けることは不可能です。一般に、これらの操作では、複数のアカウントを通じて少額の通貨が移動していることが観察され、この観察は、図57に示された複雑なノードエッジグラフによって裏付けられています。唯一明確な関連性があるのは、YouTubeで宣伝されているアプリに関連する少数のウォレットだけです。このようなオペレーションを実行しているのは誰か、規模はどの程度か、「豚の食肉解体詐欺」など他の暗号資産詐欺と関連しているか、などについてはさらに多くの調査が必要だと考えられます。

9. YouTubeへの提言

本レポートに含まれるリサーチは、単一の詐欺アプリ (paxxk[.]biz) の発見を種に、簡単に実行することができました。これらの詐欺行為に関連する何百ものチャンネルやURLを発見することは容易であり、データを収集するスピードに限界があっただけです。多くのリサーチャーたちは、ソーシャルメディアプラットフォームにおける悪意ある不正なアクティビティの例を常に発見しています。これらのリサーチは、制限されたAPIと限られたメタデータを使用して行われますが、サイトの所有者が気付かない現象を発見することができます。このような発見をもとに、従業員のアクセスによってのみ得られる追加のメタデータを利用して行動することは、これらのプラットフォームの責任であると言えます。

YouTubeの無料APIのレートリミットは、特に検索機能に関してかなり制限されています。しかし、YouTube APIのWebユーザーインターフェースは、ほぼリアルタイムでレートリミットの使用状況を追跡できる点で非常に有益です。YouTube APIの機能として、ハッシュタグの下に表示された動画を検索クエリなしで取得できるようになることを期待します。

不正なコンテンツを投稿していたチャンネルの発見数、公開頻度、これらの運用が行われていた期間を考慮すると、まだ発見されずに削除されていなかったことは非常に驚くべきことです。このような運用が判明した以上、この種の動画は、YouTubeの安全対策チームによって徹底的に洗い出され、削除されるべきですし、同様の運用に参加している他のチャンネル (動画を公開しているチャンネル、コメントを投稿してエンゲージメントを高めるために自動化されているチャンネルの両方) についても、削除されるべきです。もしこれがYouTubeの意思に反するものであれば、少なくとも、アルゴリズムによるこれらの動画の推奨を抑制すべきです。また、YouTubeは、これらの動画の説明欄に見られるSEOテキストが、YouTubeの検索や推薦のアルゴリズムにどのような影響を与えるかを理解する努力をする必要があります。

「YouTubeの再生回数を買う」というキーワードでインターネット検索をすると、YouTubeのいいね、再生回数、コメント、チャンネル登録を販売するサービスが多数ヒットします。本レポートで取り上げた多くの動画 (PSEB STUDY HALL チャンネルで公開された動画など) のエンゲージメント数を高めるために、作為的なブーストが利用されていることは明らかです。ソーシャルネットワーク上の不正なアクティビティを検出するのは難しいことですが、本レポートで取り上げた動画に関しては、その行動のパターンとチャンネルを特定するのは簡単な作業であり、APIの使用はほとんど必要ありませんでした。YouTubeの管理者が正規でないブーストを真剣に受け止め、そのようなアクティビティを検出し、対抗するためのより一般的な方法を将来的に考案していることを知るのは良いことでしょう。

YouTubeの認証済みアカウントがこのような詐欺の宣伝の手助けをしていることは、非常に心配なことです。認証済みというステータスが信頼できるものではなく、認証済みバッジがあまりにも簡単に発行されているのは憂慮すべき事態です。

10. まとめ

USDTマイニングの詐欺動画は多くのYouTuberによって作成されていますが、この詐欺に関与しているグループの1つは、約30人のメンバーを含む緊密な連携チームで構成されていると思われます。この仮説は、ユニークなURLとそれを積極的に宣伝するチャンネル間の重複 (図50と図51)、および動画にコメントするTelegramユーザー間の重複 (図25、図38、図45) を調べることで裏付けられています。

これらの詐欺アプリに関連するウォレットで実行されたトランザクションの分析により、詐欺アプリが偽物であることが証明されています。(i) いくつかのアプリウォレットでは、(そうでないことを示す動画があるにもかかわらず) 取引が行われていません。(ii) 被害者のウォレットでは、アプリウォレットからの送金の受け取りが確認されていません。

この種のYouTube動画からウォレットアドレスを抽出することで、シードアカウント、アプリウォレット、被害者、受信アドレスの潜在的なネットワークをマッピングすることができました。これらの様々なオペレーションは、2022年7月から11月の間にまとめて10万米ドルもの利益を得たと推測されます。しかし、これらの操作に関与した暗号トランザクションの分析は限られており、単に多数の追加ウォレットを見落とした可能性があります。

このような詐欺オペレーションのランニングコストには、ドメインの登録、アプリの作成、コンテンツクリエイターへの動画公開やブーストのための支払い、何千もの暗号ウォレットを通じた通貨の流れの管理などが含まれているはずで、とても大きな利益をあげられるものとは思えません。YouTubeのコンテンツクリエイターは、このような性質の動画を無限に作成するインセンティブをどのように得ているのか、不思議に思わざるを得ません。特に、何十万人もの購読者を持つ認証済みアカウントの場合はなおさらです。おそらく、YouTubeの緩いポリシーと、そのようなコンテンツを発見して閉鎖することができないことが、インセンティブが微々たるものであっても、彼らにモティベーションを与えているのでしょう。

このような詐欺アプリは、1つまたは複数の大規模なサイバー犯罪の一部である可能性が示唆されています。2022年9月9日に発行されたThe Times of Indiaの記事[4]は、本レポートで詳述したものと同様のオペレーションが中国のオペレーターに起因する可能性を示唆しています。しかし、この記事には、帰属方法に関する詳細は記載されていません。また、当社のリサーチでは、帰属決定に利用できるデータや指標は発見されませんでした。

これらの詐欺は、被害者がYouTubeの動画を見つけ、視聴することに依存しています。この調査で分析したほとんどの動画は数千回再生されていますが、その詐欺アプリに関連するウォレットでのアクティビティ、詐欺そのものがあまり説得力を持たないか、動画が推奨される可能性を高めるために、これらの再生が全て非正規のソースからもたらされていることを示唆しています。動画やアプリの品質が低いことが、このような詐欺オペレーションがあまり成功しない一因であると思われます。とはいえ、こうした様々なオペレーションの背後にある脅威アクターは、毎日のように新しいアプリを作成し、新しい動画を投稿し続けています。このことは、彼らが数で勝負し、時折莫大な利益をもたらす鯨を釣り上げることを望んでいることを示唆している。これらの詐欺グループが今後、アクティビティの一部を修正する可能性は十分にあります。もし、ここで紹介したアカウントや動画がYouTubeによって削除されたとしても、これらのアクティビティの背後にいるグループがさらに力をつけ、再びアクティブに活動を行うであろうと私たちは想定しています。

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

WithSecure™について

WithSecureは、ITサービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちはAIを活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を探し出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は30年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。

1988年に設立されたWithSecureは本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は www.withsecure.com をご覧ください。また、Twitter @WithSecure_JP でも情報の配信をおこなっています。

ウィズセキュア株式会社
〒105-0004　東京都港区新橋2丁目2番9号　KDX新橋ビル 2階
Tel: 03-4578-7710 / E-mail: japan@withsecure.com
https://www.withsecure.com/ja_JP/

2023.02 JP

WITH secure