

報道関係者各位

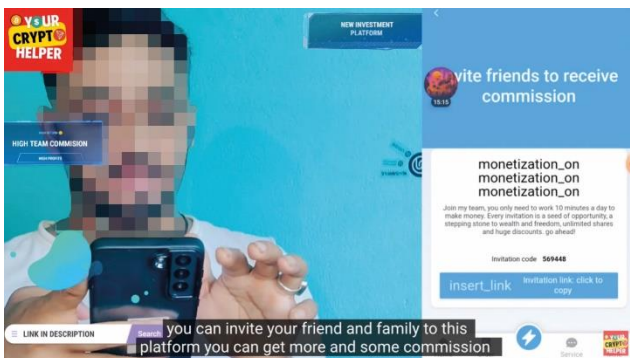
暗号通貨詐欺グループ、YouTube 動画を使って投資家を誘い出し - ウィズセキュアが調査レポート

～ 数千の勧誘動画で「いいね」や「チャンネル登録」のプーストを行い、信憑性を持たせる ～

2023 年 2 月 15 日
ウィズセキュア株式会社

先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (旧社名: F-Secure、本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、ウィズセキュア) は、同社のリサーチチームが、暗号資産である USDT (別名: テザー = Tether) を使用した暗号資産投資スキームを装った不正な Web ベース・アプリケーションへの参加を促すネットワークの発見についてまとめたレポートを発表しました。

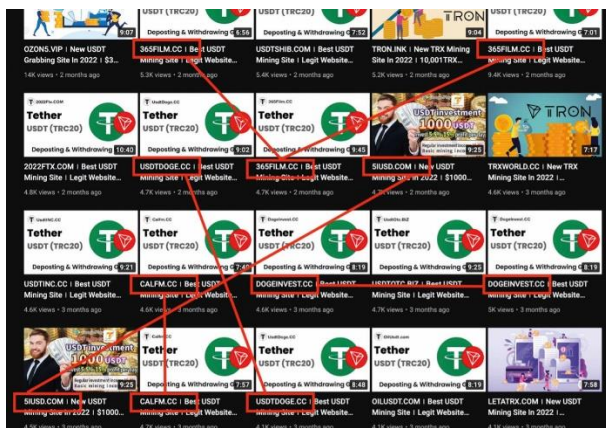
投資家を騙して資金を振り込ませることを目的とした暗号資産詐欺がインターネット、特にソーシャルメディア上で大きな問題となっています。米国連邦取引委員会によると、2021 年初頭から 2022 年 6 月までの間に 46,000 人が 10 億米ドル以上の暗号資産を詐欺で失ったと報告しており、約半数がソーシャルメディアのプラットフォームから始まったと回答しています*1。



(プレゼンターが動画の視聴者に、友達を招待してお金を稼ごうと促す)

ウィズセキュアのリサーチチームが発見した詐欺グループネットワークは数千ものオンライン動画を使用しており、その一部は、小規模の詐欺グループが管理する数百の YouTube チャンネルから「いいね」や「チャンネル登録」などの作弄的なエンゲージメントを受けています。この詐欺グループには約 30 人のメンバーがいると推定され、グループ内でのやり取りと詐欺オペレーションの手段としてメッセージアプリ Telegram を用いており、潜在的被害者に対して詐欺アプリを正当なものと思わせるために、自動化を使用して、動画にコメントをコピー&ペーストしています。

詐欺ネットワークが提供するこれらの不正な Web アプリをホストする 700 以上の URL が発見されましたが、関連する暗号資産ウォレットを分析したところ、さらに数千の URL が用いられている可能性があることが判明しました。こうした詐欺に引っかかってしまった投資家は、既存の暗号資産ウォレットからそれらのいずれかのアプリに資金を送金します。しかし、アプリからウォレットへの送金は確認されていません。



(再アップロードによる動画の複製)

ウィズセキュアのインテリジェンスリサーチャーである Andy Patel (アンディ・パテル) は、この詐欺について次のように説明しています。

「この詐欺グループは、既存の暗号資産投資家をターゲットに、複数の言語で低品質の動画を送っていますが、投資家の居住する地域ごとにビデオを翻訳／ローカライズしてはいないため、これはかなり日和見的なアプローチと言えるでしょう。一般的には、その結果、小さなトランザクションが大量に発生します。しかし、トランザクションが増えれば増えるほどその詐欺に誰かが騙される可能性が高くなり、詐欺グループを利してしまうことになるのです。」

2022 年後半にウィズセキュアのリサーチチームが収集したデータによると、発見した不正アプリは、約 900 人の被害者から 10 万米ドル強の収益を上げることができたと推定しています。

「私は、こうした手法が詐欺グループに大きな金銭的成功をもたらすものとは思いません。しかし、詐欺グループは明らかに、かなり単純な方法を用いて YouTube の推薦アルゴリズムを操作する方法を見つけ出しています。ソーシャルメディアコンテンツのモデレートはプラットフォームにとって大きな課題ですが、かなり単純でよく知られた手法を使ってコンテンツの活用がなされてしまったことは大きな懸念であり、人々をこうした詐欺から守るためにより多くの対策がなされるべきであると考えています。」と、Patel は締めくくっています。

調査レポート『YouTube での USDT 暗号資産詐欺の分析』では、これらの詐欺の背後にある動画とアプリの解剖を詳細に説明し、関連する 2 つの詐欺アプリを詳細に分析し、#usdtmining YouTube ハッシュタグを探り、詐欺に関連する暗号資産ウォレットに使用されたブロックチェーン分析手法を説明し、YouTube に対する提言を示しています。

今回の暗号資産詐欺のリサーチに関するレポート (日本語版) は、以下のページでご覧いただけます。

<https://www.withsecure.com/jp-ja/expertise/resources/cryptoscam>

*1

<https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze>

WithSecure Web サイト:

<https://www.withsecure.com/jp-ja/>

WithSecure プレスページ:

<https://www.withsecure.com/jp-ja/whats-new/pressroom>

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検出し、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、日本法人であるウイ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 でも情報の発信をおこなっています。