The Global Phenomena of Pig Butchering

Overview

Crypto investment scams have overtaken all other cyber frauds, totalling **$3.3 billion** in losses in 2022, according to a recent Federal Bureau of Investigation (FBI) report.

An innovative romance investment scam making headlines, called **pig butchering,** is proliferating globally.

With elements including **human trafficking, fabricated websites, targeted social engineering**, and ties to other organized crime, it is vital for financial institutions to be aware of this fraud scheme.

Global Touchpoints

Red Flags

Human Trafficking

- A customer recently moved to Asia for a new job opportunity.
- An IP address accesses an account from a known region for hosting scam compounds.
- The customer does not have recurring activity, like regular bills, store receipts, etc.
- A third-party attempts to open an account for an individual but they do not know critical details about the individual.

Industrial Scale Scam Centers

- A business has a physical address in Asia, including Cambodia, Laos, Myanmar.
- A business is listed as a casino, luxury hotel or type of first-class amenity (as many switched from these semi-legitimate businesses to full-time scam centers post-COVID).
- Scam center uses complex ownership structures to disguise actual activity.

Cash to Crypto Services

- The victim is asked to withdraw cash from bank accounts and then deposit it into crypto ATMs.
- Multiple payments are made to a single address from different ATMs around the globe and vice versa.
- Depositing cash to a service with no 'know your customer' (KYC) requirements.
- When questioned, 'crypto investments' is the reason given for deposits/withdrawals.
- Payments are sent to services in high-risk jurisdictions.

Fake Investment Platforms

- A customer asks to withdraw funds repeatedly, in gradually larger amounts, for a new crypto investment, specifically when the client has no previous known history in crypto trading.
- A customer sends funds directly to a flagged wallet or a hot wallet that is then moved quickly.
- Customer withdrawal activity is significantly different than normal practices with no explanation.
- A customer notes significant gains in crypto investments.

Open-Source Intelligence (OSINT)

- An unsolicited job offer via messaging apps, social media, etc. that promises high pay with very little time commitment or effort.
- A job offer that includes free accommodation, higher than average salary or travel stipends/budget.
- Telegram groups advertising people for sale using the word "cyber slaves" and bounties for escaped "workers."
- An investment platform's customer service appears to be conducted via WhatsApp.
- A message from a SMS number that can be traced back to a phony account, spam, or a platform offering online SMS.
- The investment platform has minor mistakes that mismatch known crypto investment platforms (like a domain missing a letter).
- The scammer says they have insider trading information to make high returns.

To learn more, check out the CORNERSTONE newsletter by Homeland Security Investigations (HSI), which can be found here, and ACAMS previous infographic detailing the crime.

V11052023