ACAMS

The Welcome to Video Case

Summary

Welcome To Video (WTV) was one of the largest child sexual exploitation dark web markets by content. The WTV case revolutionized financial crime cases involving cryptocurrency, as tracing bitcoin was the predominant mechanism for identifying and locating the dark web marketplace server, administrator, and some users.

WTV hosted approximately **250,000** unique videos, with 45% containing new imagery not previously known to exist.

About **US$353,000** worth of bitcoin was received in thousands of transactions by the administrator, Jong Woo Son.

Working in collaboration, 38 countries arrested **337 users** and rescued 23 minors from sexual exploitation.

Process

1. Using a Tor (anonymous) browser, **customers registered for an account** to access the website (typing in a specific address: mt3plrzdiyqf6jim.onion).
2. Once registered, the user would receive a **unique bitcoin address** to supply with crypto.
3. This wallet was then used to **buy "points"** on WTV marketplace.
4. Users could also **earn points by uploading unique content** of their own. The more a user's video was downloaded, the more points they would earn to watch other content.
5. All bitcoin earned from users buying points was **sent directly to the administrator's wallet.** The administrator was therefore the only person able to access the funds created by the darknet marketplace.
6. The administrator used **three different exchanges** to change the bitcoin back to fiat currency.

Notable Investigation Steps

Widgets of the videos uploaded by the administrator did not use Tor or a private connection, allowing for the unprotected IP address to be identified.

Many users populated their given WTV wallet directly from their wallet on an exchange.

Cooperation between law enforcement and crypto exchanges with proper KYC and customer identification requirements allowed perpetrators to be identified and transactions to be verified.

Key Takeaways

- Bitcoin was believed to be an anonymous form of payment, but innovative mechanisms of cryptocurrency tracing used by law enforcement enabled the wallet addresses to be identified.
- Cryptocurrency exchanges' KYC practices allowed the child predators to be identified and their wallets verified as sending the bitcoin to WTV wallets, proving their involvement in seemingly anonymous criminal activity.
- Collaboration between international law enforcement and cryptocurrency exchanges allowed for the criminals to be identified, verified, and arrested around the globe.

To find out more about the red flags and financial patterns related to child sexual abuse material (CSAM), register for our new social impact certificate – **Preventing Online Child Exploitation with Financial Intelligence: An Overview.**