Article Information

Author: Michael Bacina
Service: Anti-money Laundering & Corruption, Blockchain

Blockchain helps bust bad guys in darkweb shutdown

The US Department of Justice has revealed a massive international operation which has led to the shutdown of a child exploitation website hosting more than 8 terabytes of child pornography, making it one of the largest illegal website shutdowns ever.

The investigation has led to hundreds of arrests over the US, United Kingdom, South Korea, Germany, Saudi Arabia, the United Arab Emirates, the Czech Republic, Canada, Ireland, Spain, Brazil and Australia. Further details of the investigation and arrests are available in the unsealed complaint, titled "United States of America v Twenty-four cryptocurrency accounts".

Known as "Welcome to Video" (WTV), the website was a child pornography marketplace operating out of South Korea that allowed users to buy content with Bitcoin or upload their own content. Users received a unique Bitcoin address when they signed up, which was used to send funds to buy content. More than 1.3 million Bitcoin addresses were associated with the website. Between 2015 and 2018, the website had received over USD$350,000 worth of Bitcoin over thousands of individual transactions.

While this story has been reported on in The Australian (paywall), Daily Telegraph and various other outlets in the mainstream media, almost all references have missed the key point:

this bust would not have been possible without the transparent, immutable register inherent in the Bitcoin blockchain.

In the words of Internal Revenue Service (IRS) Chief Don Fort:

"Through the sophisticated tracing of bitcoin transactions, IRS-CI special agents were able to determine the location of the Darknet server, identify the administrator of the website and ultimately track down the website server's physical location in South Korea"

Blockchain analysis company Chainalysis announced that it was involved with the investigation and identified some of the methods by which they were able to identify the website's users, and ultimately enable police departments to make arrests.

In short, using the publicly listed Bitcoin wallet address on the website, Chainalysis was able to analyse transaction activity associated with that account to build the following graph showing the flow of funds associated with the website address:

View Large Image: Credit: Chainalysis Inc.

After identifying the addresses associated with cryptocurrency exchanges which had sent funds to WTF, government agencies contacted exchanges and obtained information relating to the accounts. Thanks to industry driven regulation requiring cryptocurrency exchanges to perform Know Your Customer (KYC) and Anti-Money Laundering (AML) processes, (facilitated by the AML/CTF Act in Australia) the identity of the account holders at the exchanges could be provided to police.

Chainalysis stated that for the most part, the information which agencies obtained from the exchanges was enough to identify WTV users. Where it was not, the information provided by exchanges was able to be aggregated with other publicly available data or agency intelligence which led to the international agencies being able to identify the remaining users of this abhorent website.

The past focus of the "dark side" of cryptocurrency completely misses that cryptocurrency with immutable public ledgers is the worst system for illegal value transfer and this takedown is a perfect example of why. Had the users of this website pay

in cash or another means, the analysis which was available in this case would never have been possible.

Financing criminal activity with an system which leaves an immutable, irreversible and publicly accessible record is a terrible way to commit crime, and provides an accessible and low-cost resource for regulators to investigate illegal activities.