CIPHERTRACE

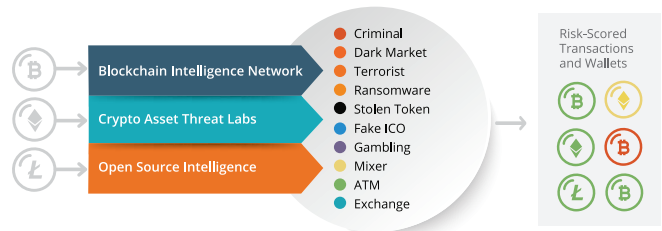# CipherTrace Transform – Cryptocurrency Tracing for Maltego

CipherTrace Enhanced Bitcoin Blockchain Intelligence and Forensics Enable More Successful Maltego Investigations

CipherTrace provides powerful and easy-to-use cryptocurrency tracing for investigators and researchers. A library of "transforms" seamlessly integrates CipherTrace Cryptocurrency Intelligence data feeds from open source and private intelligence into Maltego. Investigators use this enhanced platform to de-anonymize transactions and obtain solid evidence on individuals who use Bitcoin to launder money, finance terrorism, or carry out drug dealing, extortion and other crimes.

Seamless Maltego Integration

The intuitive CipherTrace Transform allows even non-technical agents and analysts to easily identify and trace criminals who attempt to use Bitcoin on the internet to conceal their illicit activities. CipherTrace Active Attribution applies advanced big data analytics–which leverages machine learning algorithms–to cluster data points within the expansive CipherTrace attribution repository. The result is a broad, cataloged, high-resolution view of the cryptocurrency transaction landscape.

Using this CipherTrace Cryptocurrency Intelligence, Maltego transforms allow users to easily risk-rate bitcoin addresses and trace tainted transactions. The seamless Maltego integration also offers a powerful data mining tool for investigators, allowing them to combine disparate forensics sources, perform a deeper analysis, and gain a more comprehensive perspective.

Blockchain Intelligence Network
Crypto Asset Threat Labs
Open Source Intelligence

- Criminal
- Dark Market
- Terrorist
- Ransomware
- Stolen Token
- Fake ICO
- Gambling
- Mixer
- ATM
- Exchange

Risk-Scored Transactions and Wallets

The Maltego transforms access advanced CipherTrace blockchain intelligence, which combines millions of new attribution data points each day. This Cryptocurrency Intelligence identifies risky transaction characteristics and locations, including known criminal, dark market and gambling sites as well as mixers.

# Maltego Transforms for Addresses, Transactions and Wallets

The integrated Maltego transforms operate at three levels: bitcoin address, bitcoin transaction and bitcoin wallets. Bitcoin Address and Bitcoin Transaction transforms enable investigators to calculate the current state of a coin or transaction including risk level and potentially location.

Bitcoin Address Transforms

Users can explore bitcoin addresses using the CipherTrace Bitcoin Address Transform, and a Detail View explains why a transaction received a particular risk rating. Users can also enhance these results with additional details gleaned from IP addresses, inbound and outbound transactions, and wallet transaction data.
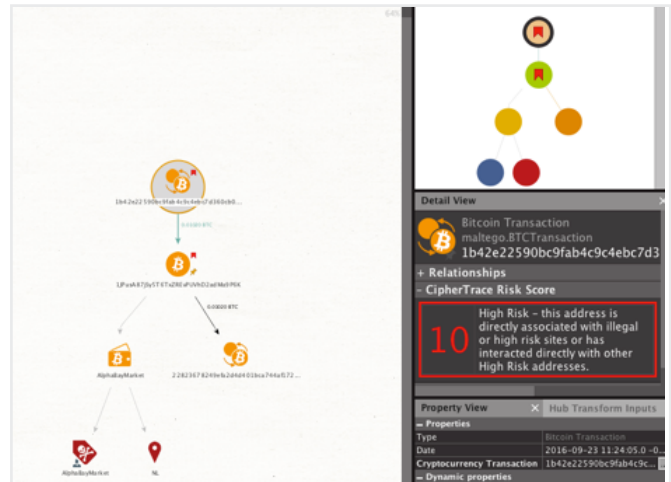
A high-risk transaction with a known dark market
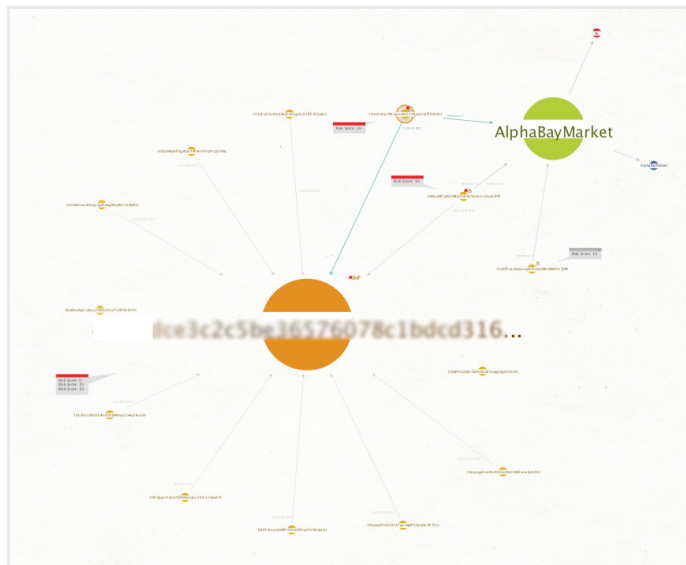
The "To Inbound transaction [CipherTrace]" and "To outbound Transaction [CipherTrace]" transforms allow users to move back and forth through time in forensics data derived from the bitcoin blockchain. This capability enables investigators to trace the addresses to see if they have been tainted by association with known bad bitcoin addresses, transaction, and wallets.

Bitcoin Transaction Transforms

Users can also perform a trace based on a transaction—a record in the public bitcoin blockchain that records the movement of bitcoins, or portions of them, from one address to another. A transaction has one or more outputs, and can be looked up in the CipherTrace Transaction transform screen.

The CipherTrace Maltego integration transaction tracing options include destination addresses, source addresses, and risk scoring. Users can get wallet information by tracing the addresses of the transactions. All of the data provided can easily integrate into other Maltego transforms to make investigations and research as seamless and intuitive as possible.

Bitcoins Wallet Transforms

A wallet address provides a way to group bitcoin addresses into one group that is likely to be controlled by a single user or service. The Wallet Transform can be used to identify exchanges, locations, and other associations.