



Using CipherTrace Sentry Enrichment For Anomali

September 27, 2021

<u>Introduction</u>	3
<u>Setup</u>	3
<u>Usage</u>	5
<u>When on the details page for a given IP address</u>	5

Introduction

Anomali users can utilize the CipherTrace Sentry enrichment to trace the crypto addresses associated with an IP address, along with any transactions and output destination addresses linked to them.

Setup

Users can set up the CipherTrace Sentry enrichment by clicking “Set Up” on the CipherTrace Sentry widget in the Integrations tab in the Anomali settings page.

CIPHERTRACE SENTRY

CipherTrace provides powerful and easy-to-use cryptocurrency tracing for investigators and researchers. The CipherTrace Enrichment supports the following cryptocurrencies: Bitcoin, Ethereum, Bitcoin Cash, Litecoin, and BNB. CipherTrace Enrichment allows investigators to de-anonymize crypto transactions.



Author	Version
CipherTrace	1.1.0
Source	License
https://ciphertrace.com/financial-investigations-and-blockchain-forensics/	https://ciphertrace.com/terms/
For enrichment credentials: Please contact vendor	I have Already Registered

Click “I Have Already Registered” in order to enter your API key and, optionally, the CipherTrace external URL used for Single Sign On, which will enable you to navigate directly to CipherTrace’s platform from Anomali.

CIPHERTRACE SENTRY

CipherTrace provides powerful and easy-to-use cryptocurrency tracing for investigators and researchers. The CipherTrace Enrichment supports the following cryptocurrencies: Bitcoin, Ethereum, Bitcoin Cash, Litecoin, and BNB. CipherTrace Enrichment allows investigators to de-anonymize crypto transactions.



Author

CipherTrace

Version

1.1.0

Source

<https://ciphertrace.com/financial-investigations-and-blockchain-forensics/>

License

<https://ciphertrace.com/terms/>

API Key

CipherTrace external URL

Cancel

Activate

Contact CipherTrace for more details on your external URL. If you do not enter one, you will be prompted to sign in to CipherTrace’s platform the first time you navigate there from Anomali. Once you have entered your API key and the optional external URL, you are ready to use the full features of the CipherTrace Sentry enrichment.

Usage

When on the details page for a given IP address

Right-clicking on the IP address node, a user can view all crypto addresses linked to the IP address by using the “IP to Crypto Addresses” function

Confidential & Proprietary Page 4 of 12

***.ciphertrace.com | support@ciphertrace.com | Copyright 2021 CipherTrace | DOC-SENT-CT-ANOM-20210927



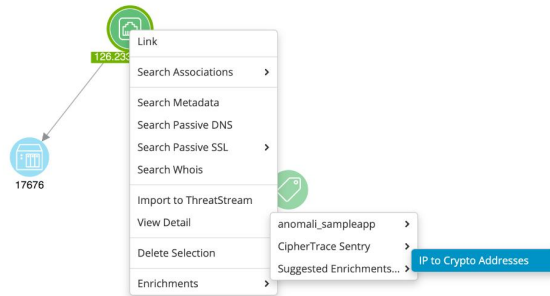
IP (1)

Tag (1)

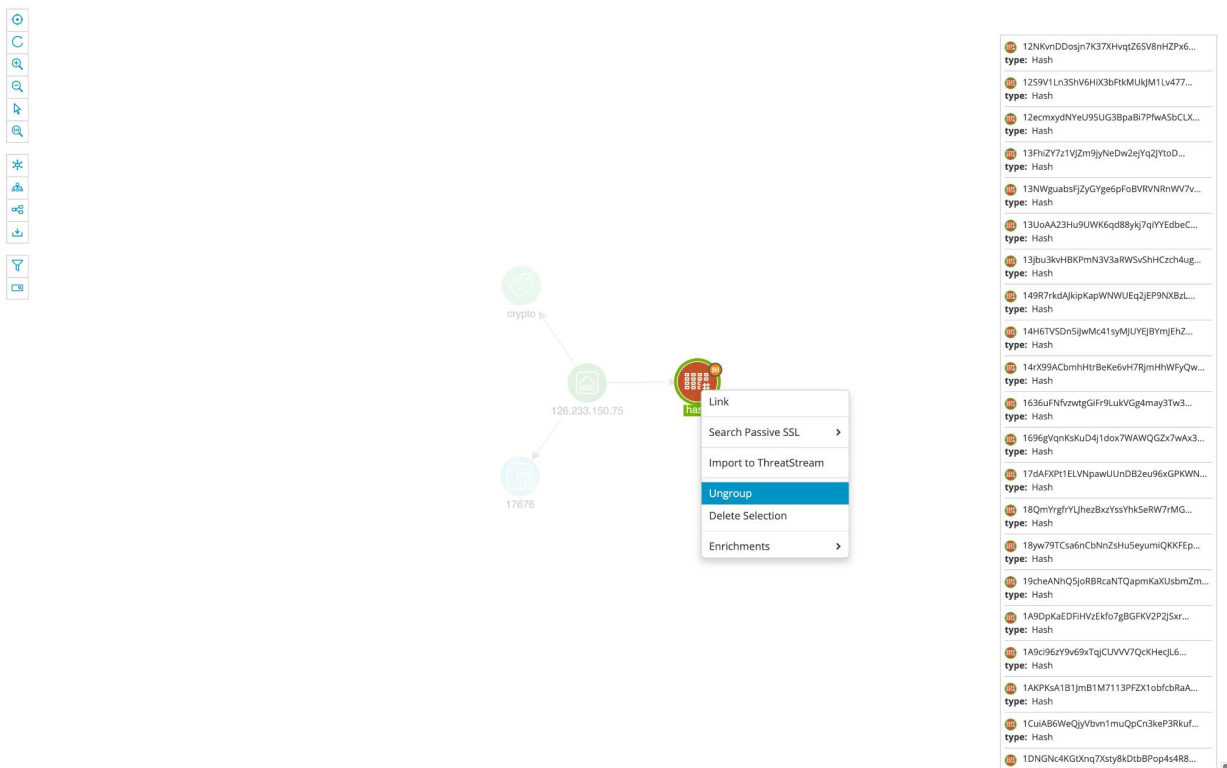
ASN (1)

50 Node Search Limit

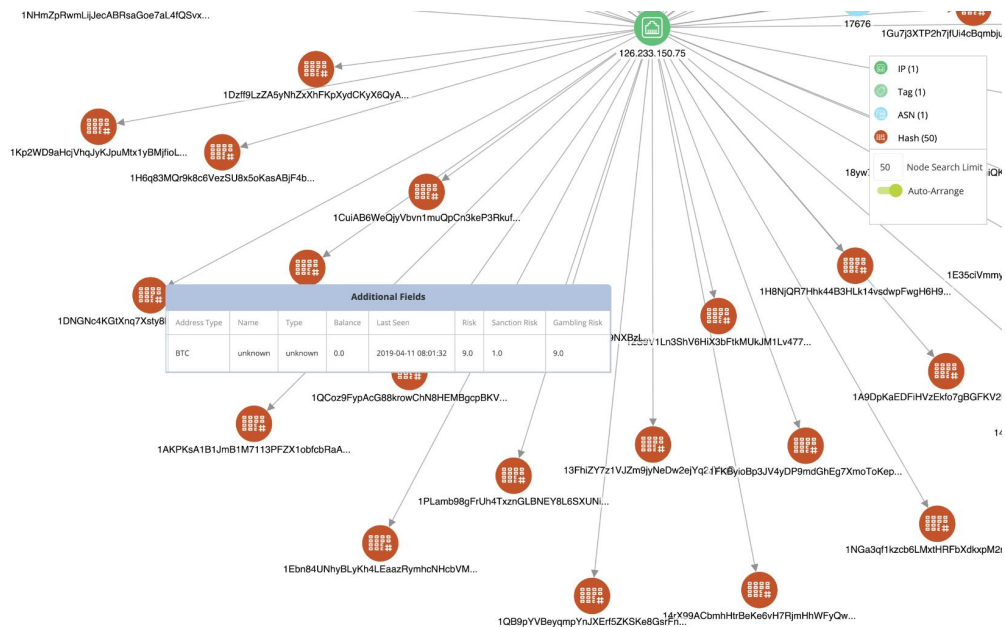
Auto-Arrange



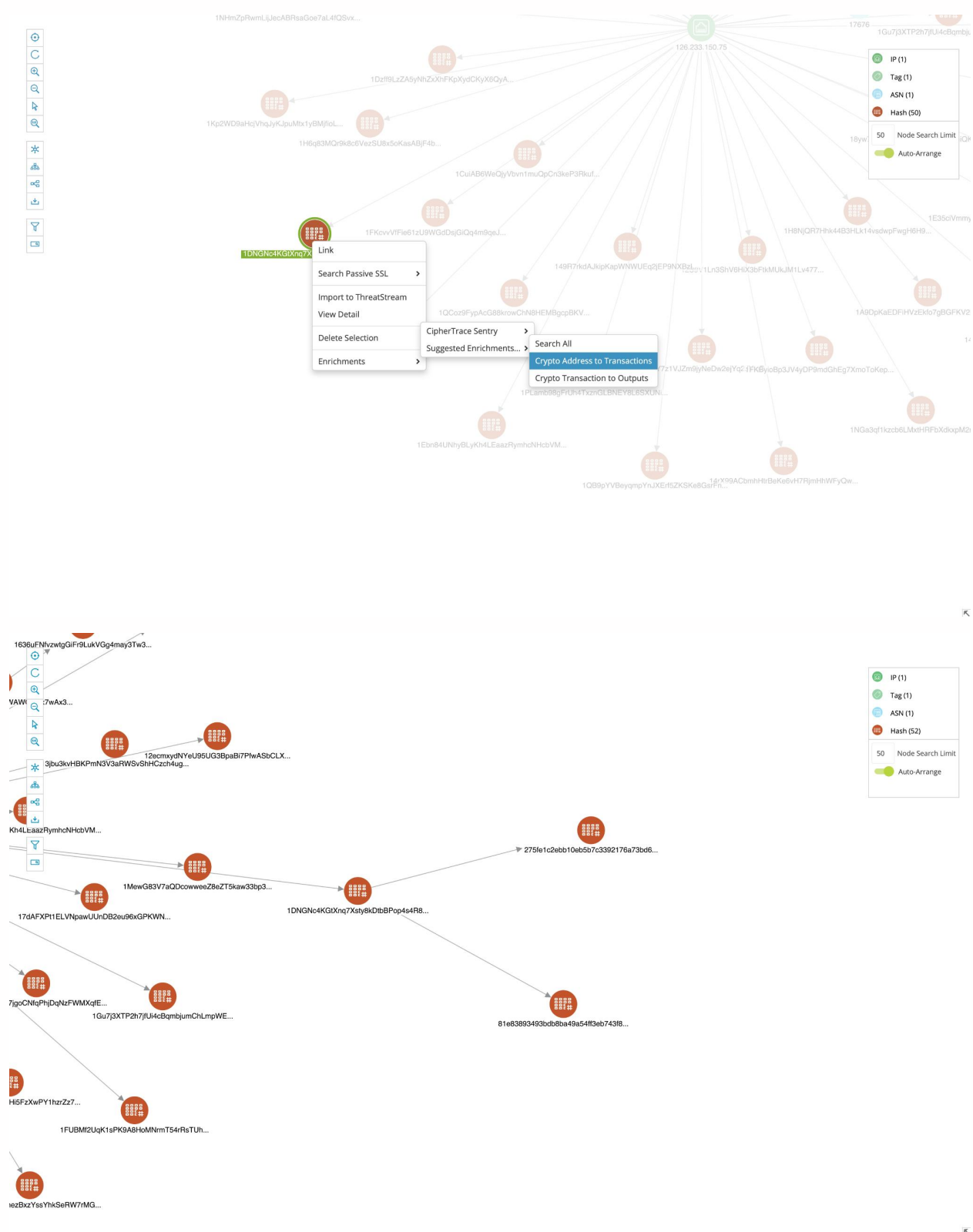
To view the crypto addresses individually, click the aggregated node's "Ungroup" option



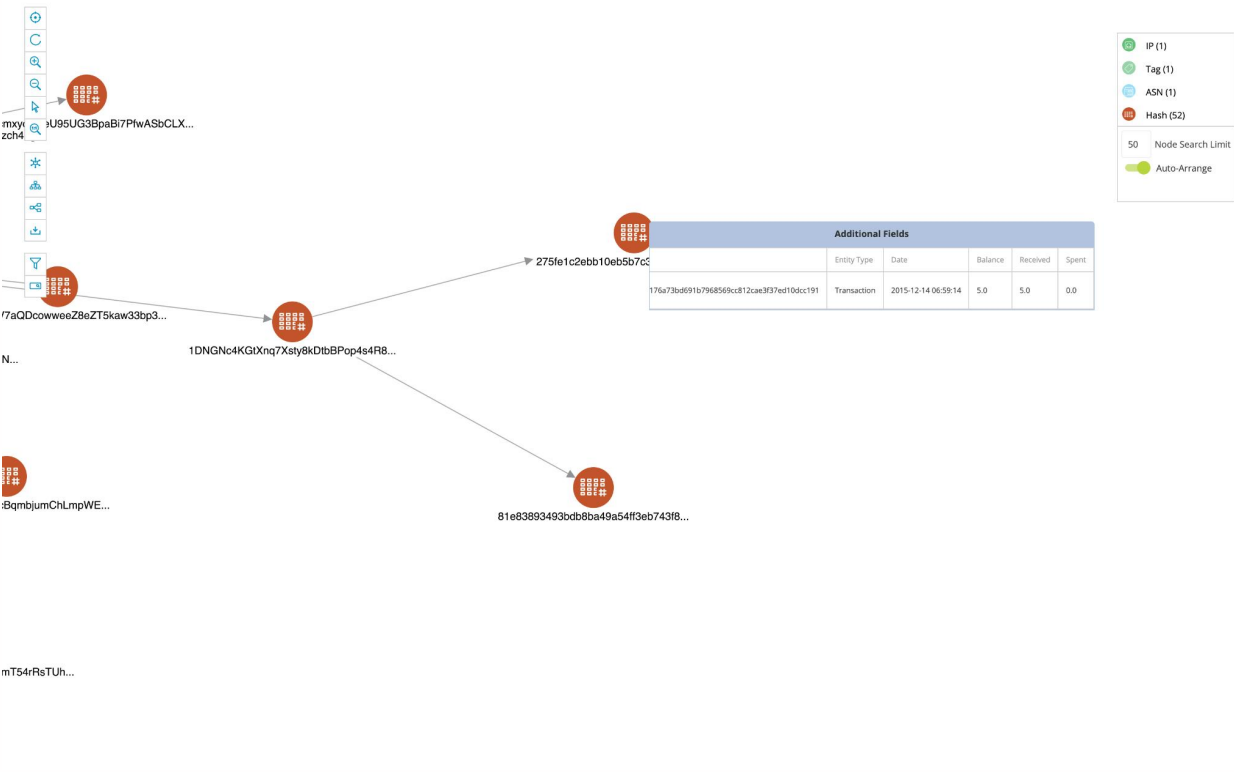
By hovering over the crypto address nodes, users can view associated information gathered by CipherTrace



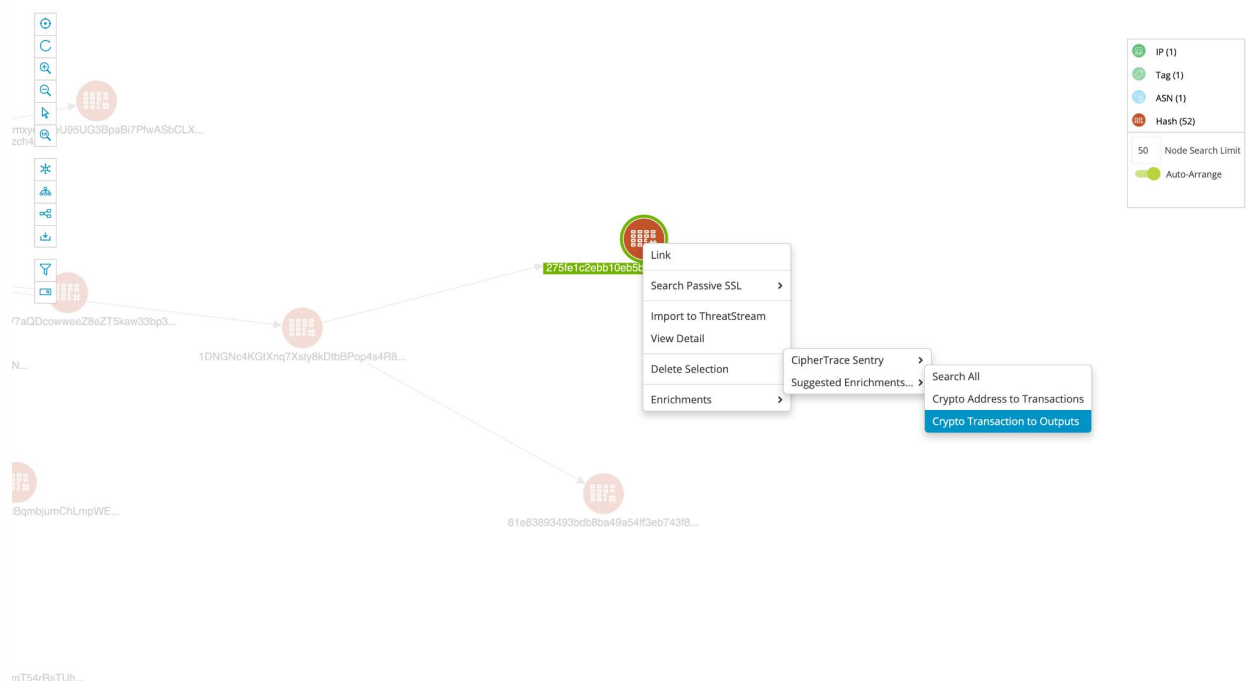
Right clicking on the crypto address node yields the “Crypto Address to Transactions” function, which will reveal all transactions associated with this address.



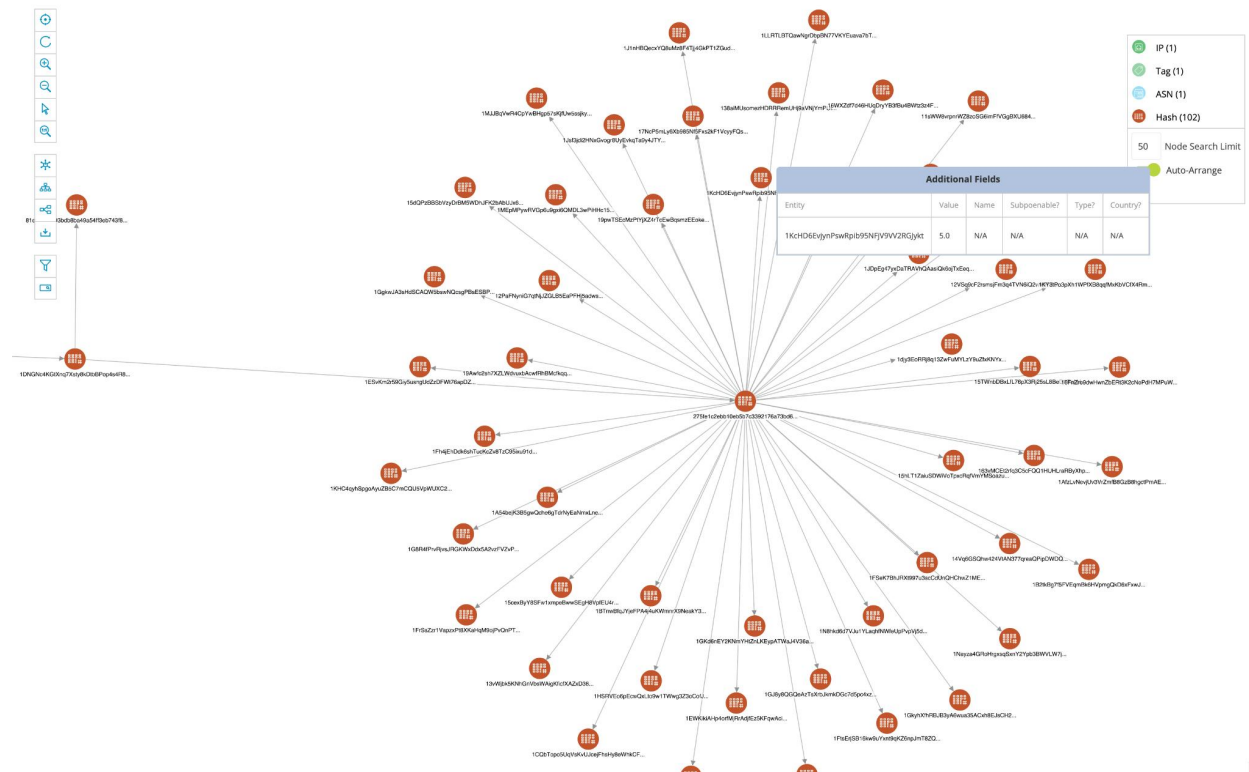
Users can view information associated with each transaction by hovering over the node



After right clicking on the transaction node, users can reveal all of the transaction's output destination addresses using the function "Crypto Transaction to Outputs"



Once again, hovering over each output reveals information linked to it from the CipherTrace system.



13 Oct 2020
10:51

25 Feb 2021
14:23
[View details](#)

Cryptocurrency
IP

126.233.150.
75

[jp](#)

zachary.kreiser@ciphertancelabs.com

My Organization

N/A

55

50

Inactive

962

Anonymize

Assign to Workgroups

Delete

Enrichments

PASSIVE DNS (0)

WHOIS

ANOMALI_SAMPLEAPP

SAMPLEAPP ENRICHMENT

CIPHERTRACE SENTRY

SUGGESTED ENRICHMENTS...

25 ▾

Source

Domain

Record Data

Record Type

First Seen

Last Seen

⚙️

No data available

Associations

OBSERVABLES (0)

THREAT BULLETINS (0)

ACTORS (0)

ATTACK PATTERNS (0)

CAMPAIGNS (0)

COURSE OF ACTION (0)

IDENTITIES (0)

INCIDENTS (0)

INFRASTRUCTURE (0)

INTRUSION SET (0)

MALWARE (0)

SIGNATURES (0)

TOOLS (0)

TTPs (0)

VULNERABILITIES (0)

CUSTOM THREAT MODELS (0)

INVESTIGATIONS (0)

No associated investigations.

Comments

Add a comment

Red ●

↶ ↷

B i U ⌂ x₂ x² A ~ AA~ Aₐ - ¶*

¶ • ≡ ∴ ∵ ∶ “ ” ⌕ 📄 🗉 — ✎ ☰

Type something

Enrichments

PASSIVE DNS (0)

WHOIS

ANOMALI_SAMPLEAPP

SAMPLEAPP ENRICHMENT

CIPHERTRACE SENTRY

SUGGESTED ENRICHMENTS...

Address Information for 126.233.150.75

View IP Address in CipherTrace Inspector

Wallet Addresses

25

1 - 25 of 58 items

Address	Address Type	Wallet Balance	Last Seen	CipherTrace Risk Score	Entity Type	Entity	View in CipherTrace	
12NKvnDDosjn7K37Xhv...	BTC	0	2019-04-11 08:01:32	9	unknown	unknown	Link	
1259V1Ln35hV6HX3bFt...	BTC	0	2019-04-11 08:01:32	2	exchange	SpectroCoin.com	Link	
12ecmxydNYeU95UG3B...	BTC	0	2019-04-11 08:01:32	1	unknown	unknown	Link	
13PhiZY7z1VjZm9jyNeD...	BTC	0	2019-04-11 08:01:32	1	services	BitPay.com	Link	
13NWguabsFjZyGyGe6p...	BTC	0.00000546	2019-04-11 08:01:32	1	unknown	unknown	Link	
13UoAA23Hu9UWK6qd...	BTC	0	2019-04-11 08:01:32	2	exchange	Poloniex.com	Link	
13jbu3kvH8KPMn3V3a...	BTC	0	2019-04-11 08:01:32	1	unknown	unknown	Link	
149R7rkdAJkipKapWNW...	BTC	0.0049647	2019-04-11 08:01:32	1	unknown	unknown	Link	
14H6TV5Dn5ijwMc41sy...	BTC	0	2019-04-11 08:01:32	1	unknown	unknown	Link	