ANOMALI CIPHERTRACE

ANOMALI AND CIPHERTRACE: CRYPTOCURRENCY THREAT INTELLIGENCE

Detect, investigate, and respond to crypto-threats with CipherTrace Sentry and Anomali ThreatStream

THE CIPHERTRACE AND ANOMALI JOINT SOLUTION FEATURES:

- **Deep Blockchain Insights:** CipherTrace Sentry Enrichment for Anomali ThreatStream provides powerful and easy-to-use cryptocurrency de-anonymization and tracing to increase crypto-threat visibility, detection, and response and enhance investigations.
- **Credible Transaction Attribution:** With CipherTrace Sentry, Anomali users can leverage CipherTrace's industry-leading attribution to de-anonymize crypto-addresses and associate them with real-world entities and events, such as criminals, dark markets, ransomware events, terrorist funding, crypto-exchanges and ATMs, and more.

IMMEDIATE TIME-TO-VALUE

- **Matches Crypto Addresses with IP Addresses:** Using the CipherTrace enrichment for Anomali ThreatStream, users can view all the crypto addresses associated with an IP Address of interest, along with their associated owners and events.
- **Investigate Ransomware Payments:** Detailed blockchain analytics and cryptocurrency intelligence data to track cryptocurrency payments made to hackers.
- **Comprehensive Tracing of Transactions:** Users can easily trace a given address's input and output transactions via the Anomali ThreatStream user interface.

BOOST ANOMALI WITH SUPERIOR CRYPTO-INTELLIGENCE

The CipherTrace Sentry integration allows users to work with a vast array of data to enable detailed analysis, without leaving the Anomali ThreatStream platform. CipherTrace does this through a variety of techniques, including running transactions on 1,000 crypto-exchanges. CipherTrace analysts add over 1.5 million attribution datapoints each week.

DETAILED BLOCKCHAIN ANALYTICS AND CRYPTOCURRENCY INTELLIGENCE

Provides an end-to-end audit trail of transactions. With the information, users can distill "big data" into a view of the cryptocurrency risk landscape.

ACTIONABLE INTELLIGENCE FOR EVIDENTIARY PROCEEDINGS & REGULATORY COMPLIANCE

Trace crypto transactions to ensure compliance with Anti-Money Laundering Regulations.

REAL-TIME, ACCURATE RISK REPORTING

Discover locations and IP Addresses associated with cryptocurrency transactions as they occur so users can respond immediately to threats.

USE CASE: DETECTING AND INVESTIGATING CRYPTOCURRENCY-THREATS

TARGET MARKET:

Leading Financial Institutions and Law Enforcement agencies

CHALLENGE:

The need to identify crypto-activity associated with clients and insider transactions in order to:

- Thoroughly understand threats and suspicious activities
- Perform investigations
- Execute targeted due diligence activities

SOLUTION:

CipherTrace and Anomali connected and investigated crypto-addresses, IP addresses, and funds flows, along with their relationships to entities and events of interest.

With CipherTrace and Anomali, the security team was able to:

- Improve threat hunting by exposing hidden crypto-activity in corporate networks.
- Perform extended due diligence on client activities related to cryptocurrency.
- Assist clients and internal constituents with enhanced investigations into ransomware and malware incidents, dark market activities, and other crypto-related situations.
- Access and correlate crypto-intelligence data for investigations right from the Anomali dashboard

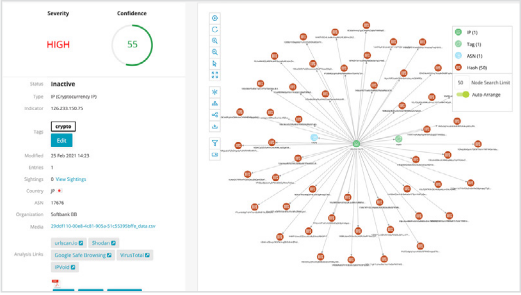
CUSTOMER BENEFIT:

- Detailed, accurate, graphical reports that can be used as evidence in legal proceedings
- Better business decision-making: increased time-to-insight for internal investigations
- Single dashboard view: provides visibility into previously hidden crypto-activities
- Collate data from multiple sources: Combines crypto-data with other information sources for deeper insights

BENEFITS:

IDENTIFY THREATS

Identify crypto-activity associated with internal and external IP addresses of interest.

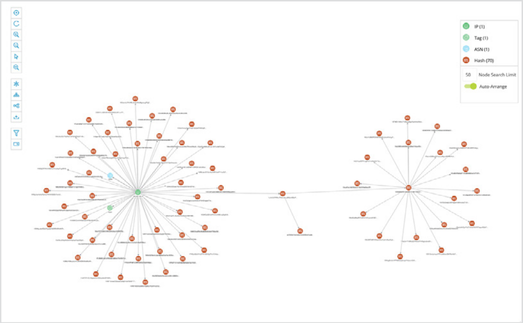


Severity: HIGH
Confidence: 55

Status: Inactive
Type: IP (Cryptocurrency IP)
Indicator: 126.233.150.75
Tags: crypto
Modified: 25 Feb 2021 14:23
Entries: 1
Sightings: 0 View Sightings
Country: JP
ASN: 17676
Organization: Softbank BB
Media: 29ddf110-00e8-4c81-905a-51c55395bffe_data.csv
Analysis Links: urlscan.io, Shodan, Google Safe Browsing, VirusTotal, IPVoid

FOLLOW THE MONEY

Trace crypto address transactions via the ThreatStream user interface to follow the money in ransomware, theft, and other investigations and find source and destination of funds.



Extend Anomali threat intelligence with seamless integration of real-time contextual crypto-ownership and movement-of-funds data tied to IP addresses and real-world events.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS