Recorded Future®

DATA SHEET

Crypto Data Mapping

Identify Malicious Crypto Activity

Crypto's anonymity and capacity for circumventing international borders and regulations has positioned it as a popular tool for fraudsters and criminals to store and move illegitimate funds. Recorded Future Payment Fraud Intelligence has developed a crypto solution—based on deep expertise of dark web collection and investigation methods—to find crypto wallets associated with illegal activity. With reach into both the dark web and surface web, this solution enables crypto investigation services and direct crypto exchangers to identify malicious activity happening in the crypto space.

Automated Crypto Data Collection

Recorded Future's crypto solution automatically identifies crypto wallets that are mentioned on dark web forums, Telegram channels, pastebins, "grey" forums, and social media, while also identifying whether the crypto wallets have been used for transactions or merely generated for future use.

Our enrichment of automated wallet collection provides:

- The type of crypto identified (e.g. BTC, LTC, ETH, and over 15 more)
- Validation of whether the wallet has been involved with any activity
- Attribution to the threat actors and users/individuals associated with the posting/mention of the crypto wallet
- Identification of the source where the wallet was mentioned as well as the type of mention (post/profile)
- Further enrichment of attributed posts (i.e., for dark web data this includes the thread and section of the forum where the wallet was mentioned)

KEY BENEFITS

- Identify high-profile wallets associated to services that can only be obtained through direct interaction
- Utilize Recorded Future analysts to target priority services of interest
- Map out all acceptable currencies and associated wallets for each dark web service
- Leverage manually identified wallets to identify even larger clusters associated with various services

Manually Curated Crypto Data

The top threat actors, criminal services, and dark web marketplaces devote significant effort to ensure their crypto wallets do not slip into the “public” view. With Manually Curated Crypto Data, Recorded Future infiltrates these criminal communities and attributes their crypto wallets, providing visibility into criminal activity that wouldn’t otherwise come to light. All attributions come with detailed information about the source, along with a screenshot of the transaction. Of the 700 dark web services we track, the common services targeted by manually curated wallet collection are:

- Dark Web Actors
- Drug Markets
- Gambling Services
- Ransomware Groups
- Telegram Shops
- Escrow Services
- Dark Web Markets & Forums
- Payment Card Checker Services
- DDOS Services
- PII Shops
- Proxy Services
- Spam Services
- Scam Shops
- Leak Markets