REGIONAL CYBERCRIME UNIT INVESTIGATES £20 MILLION CRYPTOCURRENCY THEFT WITH SELF-DEVELOPED NUIX BITCOIN EXTRACTION SCRIPT

SUMMARY

As cryptocurrencies became increasingly common in organized crime activity, the South West Regional Cyber Crime Unit needed a thorough, efficient way to identify Bitcoin addresses and keys in seized digital evidence. It created the Nuix Bitcoin Extractor, a scripting tool that extracts and validates Bitcoin addresses from any data indexed by Nuix Workstation. In the recent case of a £20 million cryptocurrency theft, this allowed the investigative team to:

- Extract cryptocurrency addresses from mobile device images, PCs, laptops and cloud storage, scanning millions of items per hour
- Quickly identify and act on leads extracted from these evidence sources
- Connect Bitcoin addresses to suspects and recover some of the stolen currency.

CHALLENGE

Cryptocurrencies are a growing element of criminal activity. Research firm Chainalysis estimated US$14 billion in cryptocurrencies were received by addresses linked to illegal activity in 2021, up 79% from 2020. As a result, Bitcoin investigation is increasingly becoming the norm in cybersecurity and other large-scale criminal investigations.

The South West Regional Cyber Crime Unit (SWRCCU) is a specialist team within the South West Regional Organised Crime Unit, one of nine regional units that target serious and organized crime across England and Wales. More than three-quarters (77%) of the cybercrime unit's investigations in 2021 involved cryptocurrencies.

Finding cryptocurrency addresses or public keys in seized evidence can assist with attribution and facilitate follow-the-money processes to identify new suspects or victims. Finding private keys can help authorities recreate digital wallets and retrieve stolen funds.

Extracting these artifacts from digital exhibits is challenging because seized evidence often runs into terabytes of data. Traditional techniques such as keyword searches, filters and analysis by cybercrime specialists are an expensive and inefficient use of highly trained human resources, often with incomplete results. In addition, existing cryptocurrency search tools don't work with modern Bitcoin protocols or mobile device extractions, making them less useful in light of the widespread use of mobile cryptocurrency wallets and trading apps.

SOLUTION

The regional organized crime unit had used Nuix software for many years as part of its digital forensics workflow. The team's forensic specialists used Nuix Workstation to ingest, process and cull digital evidence before presenting it in Nuix Investigate® for easy review by investigating officers and analysts.

Harry F, a Digital Forensic Investigator at SWRCCU, created the Nuix Bitcoin Extractor, a series of scripts to extract and validate Bitcoin addresses and keys from any Nuix case. The Nuix Bitcoin Extractor uses a Ruby script to extract plain text from each item in a Nuix case, apply regular expression searches to identify potential Bitcoin addresses and keys, and apply a mathematical checksum to eliminate false positives. A Python script, running on an internet-connected machine, validates the addresses on Blockchain.com and extracts open-source intelligence such as wallet balance, number of transactions and value of throughput.

"The ability of Nuix to ingest almost all data types – including mobile device extractions, PCs, laptops and cloud storage – has been invaluable," said Harry F. "Combined with the extensive Nuix application programming interface, the script can interact with hundreds of millions of items, allowing us to exhaustively traverse entire operational datasets in minutes."

> "The ability of Nuix to ingest almost all data types – including mobile device extractions, PCs, laptops and cloud storage – has been invaluable."

RESULTS

SWRCCU used the Nuix Bitcoin Extractor to investigate a cryptocurrency theft of more than £20 million (US$27 million), which affected thousands of victims worldwide, helping to identify suspects in the southwest of England. Following warrants and subsequent searches, the investigation team recovered many digital evidence sources containing thousands of Bitcoin addresses and forensic artifacts that were relevant to the case.

Using Nuix for the Bitcoin address extraction ensured the investigators could identify and act on opportunities in a timely manner. This helped the team identify previously unknown addresses connected to the UK suspects and recover some of the stolen currency.

“Because the script uses Nuix as source, the breadth of data it can search is only limited by what Nuix can support and process,” said Harry F. “This includes mobile phones, unallocated data and complex forensic artifacts. The tool can be run at the click of a button for any case, at speeds of roughly 5–10 minutes per million items on data that has already been indexed by our standard digital forensic workflows.”

> “The tool can be run at the click of a button for any case, at speeds of roughly 5–10 minutes per million items on data that has already been indexed by our standard digital forensic workflows.”

ABOUT THE SOUTH WEST REGIONAL ORGANISED CRIME UNIT

The South West Regional Organised Crime Unit (swrocu.police.uk) is a police unit responsible for delivering specialist and niche capabilities across the South West region, supporting Avon & Somerset, Devon & Cornwall, Dorset, Gloucestershire, and Wiltshire Constabularies. Its mission is to target and disrupt serious and organized crime.

GET THE NUIX BITCOIN EXTRACTOR

Thanks to the innovative work of SWRCCU, Nuix Bitcoin Extractor is now available to the Nuix user community. Nuix Bitcoin Extractor supports:

- P2PKH, P2SH and bech32 address protocols
- xPub/xPrv (BIP32 HD), zPub/zPrv (BIP84) and yPub/yPrv (BIP49) wallet keys.

Download the Ruby and Python scripts from the Nuix GitHub at https://github.com/Nuix/Bitcoin-Extractor.

For more information, visit **nuix.com/demo**

Nuix (www.nuix.com, ASX:NXL) creates innovative software that empowers organizations to simply and quickly find the truth from any data in a digital world. We are a passionate and talented team, delighting our customers with software that transforms data into actionable intelligence and helps them overcome the challenges of litigation, investigation, governance, risk and compliance.

APAC
Australia: +61 2 8320 9444

EMEA
UK: +44 203 934 1600

NORTH AMERICA
USA: +1 877 470 6849