Memory Forensics Methodology for Investigating Cryptocurrency Protocols

Shaimaa S. Ali [1], Ahmed ElAshmawy[2], and Ahmed F. Shosha[3]
[1]Department of Information Security, Nile University, Giza, Egypt
[2]Principal Consultant, Axenic Limited, Wellington, New Zealand
[3]Assistant Professor at Department of Information Security, Nile University, Giza, Egypt

Abstract - *The growing market of cryptocurrencies and subsequently the relevant cyber-attacks, raises the importance of digital forensics in this domain.*

The proposed digital forensics methodology extracts digital evidence and forensic artifacts from system memory to assist investigations involving cryptocurrency. In addition, case studies are presented to explain the proposed methodology using developed Volatility [1] plugins.

Our cryptocurrency memory forensics investigation methodology extracts a series of forensically valuable cryptocurrency protocols' methods/calls. The first case study involves analyzing two legitimate processes working under two cryptocurrency network protocols; Bitcoin and CryptoNote. The second case study analyzes three different malicious Monero mining processes.

Currency transactions and revealing malicious identity are the most important findings of this paper. Other findings are listed in the results section.

Keywords: Digital Forensics, Memory Analysis, Cryptocurrency, Bitcoin, Monero.

1. Introduction

Nowadays, many countries and businesses accept cryptocurrency as a form of monetary, while their central banks cannot control or regulate its blockchain. Exploring the cryptocurrencies world from a digital forensics perspective becomes a vital issue due to its fast growing economics' dependence and the usual race of cybercriminals with money stealing intentions. Volatile memory forensics offers a great source of evidence for the wallet state, supporting the investigation of suspicious wallets.

Many forensics researches explain cryptocurrency in terms of found addresses and wallet files/folders, without paying attention to the underlying cryptographic protocols. Our proposed algorithm covers this gap.

Cryptocurrency network protocols incorporate all the cryptographic structure of a digital coin and any communication between its nodes. It is updated mostly by a group of volunteers, who make continuous improvements by releasing new versions to cover any deficiencies in coin operation.

This research aims at creating a volatile memory parser for Bitcoin and CryptoNote network protocols, and Stratum mining protocol for a group of chosen messages. Those messages reveal a lot of digital forensics information that can be correlated to the corresponding cryptocurrency community. The developed Volatility plugins were successful in extracting important parameters of certain messages exchanged between a node running Microsoft Windows 8.1 64-bit operating system with other nodes/pools.

Contributions and Findings. The following summarizes our contributions and findings:

(1) Present a generic methodology that helps investigators extract digital evidence and forensic artifacts for any cryptocurrency protocol (including mining protocols) from system memory.

(2) Apply this methodology to forensically analyze cryptocurrency protocols. The first case study illustrates the idea with two legitimate cryptocurrency processes. Results show how the methodology helps perform forensic analysis of the currency transactions, blocks and connected nodes in P2P network through parsing corresponding messages in Bitcoin and CryptoNote protocols.

(3) The second case study illustrates the application of the methodology to analyze three different mining malicious processes. Results show how the methodology helps reveal the identity of malicious miners, malicious pools and their communication method by parsing corresponding messages in Stratum mining protocol.

This research is divided into:

Section 1 - Introduction to the research problem, contribution and finding; Section 2 - Demonstration of the structure of Bitcoin protocol and the Bitcoin forensically interesting messages while listing some of the previous forensics researches for Bitcoin wallet; Section 3 - Similar literature for the CryptoNote protocol from Monero perspective; Section 4 - Briefly introduces the Stratum mining protocol while shedding light on chosen JSON-RPC methods;