

ABSTRACT OF THE DISCLOSURE

【Invention Title】 CYBER THREAT INFORMATION PROCESSING APPARATUS, CYBER THREAT INFORMATION PROCESSING METHOD, AND STORAGE MEDIUM STORING CYBER THREAT INFORMATION PROCESSING PROGRAM

Provided are a cyber threat information processing apparatus, a method thereof, and a storage medium storing a cyber threat information processing program. It is possible to provide a cybersecurity threat information processing method including disassembling an input executable file to obtain disassembled code, and reconstructing the disassembled code to obtain reconstructed disassembled code, into a hash function, and converting the hash function into N-gram data (N being a natural number), and performing ensemble machine learning on block-unit code of the converted N-gram data to profile the block-unit code by an identifier of an attack technique performed by the block-unit code and an identifier of an attacker generating the block-unit code. It is possible to detect and address a variant of malware, and identify malware, an attack technique, an attacker, and an attack prediction method within a significantly short time even for a variant of malware.

(FIG. 35)