Method for Malware Detection and Classification using Image Processing Techniques

Tech ID: 21993 / UC Case 2012-085-0

BRIEF DESCRIPTION

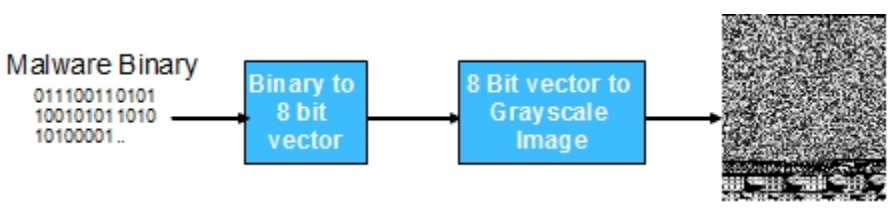
A novel method for visualizing and classifying malware using image processing techniques, applicable to malware detection and anti-virus software.

BACKGROUND

Existing approaches for analyzing malware include static code analysis (which looks at the structure of the code) and dynamic code analysis (which runs the code in a virtual environment), both of which have specific strengths. However, static analysis suffers from code obfuscation due to the need to unpack and decrypt the code, while dynamic analysis may overlook malicious behavior due to an inadequate virtual environment. Both approaches are computationally heavy and time intensive.

DESCRIPTION

Researchers at the University of California, Santa Barbara have developed SARVAM, a novel method for visualizing and classifying malware using image processing techniques, applicable to malware detection and anti-virus software. Initial experiments show that this technique has a classification accuracy of 98%, which is on par with the state of the art. However, this method avoids many of the drawbacks of current methods and thus exhibits improved performance. In particular, this technology has a lower computational cost for malware analysis, has a faster response to threats, is resilient to popular obfuscation techniques such as section encryption, and does not require disassembly or code execution for classification.



ADVANTAGES

- 98% classification accuracy (matching state-of-the-art methods), but with improved performance:
  - o Lower computational cost for malware analysis

CONTACT

Pasquale S. Ferrari
ferrari@tia.ucsb.edu
tel: .

INVENTORS

- Jacob, Gregoire
- Manjunath, Bangalore S.
- Nataraj, Lakshman
- Vigna, Giovanni

OTHER INFORMATION

KEYWORDS

Malware, indsoftw

CATEGORIZED AS

- **Computer**
  - Security
  - Software

RELATED CASES

2012-085-0

o Faster response to threats

o Resilience to popular obfuscation techniques such as section encryption

o Neither disassembly nor code execution needed for classification

APPLICATIONS

- Malware Detection
- Anti-Virus Software

This technology is available for licensing.

OTHER INFORMATION

An online demo of SARVAM is available at this link: http://sarvam.ece.ucsb.edu/

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- A Video Fingerprinting Method For Duplicate Detection

University of California, Santa Barbara
Office of Technology & Industry Alliances
342 Lagoon Road, ,Santa Barbara,CA 93106-2055 |
www.tia.ucsb.edu
Tel: 805-893-2073 | Fax: 805.893.5236 | padilla@tia.ucsb.edu