Accepted Manuscript

Title: A malware detection method based on family behavior graph

Author: Ding Yuxin, Xia Xiaoling, Chen Sheng, Li Ye

PII: S0167-4048(17)30214-6
DOI: https://doi.org/doi:10.1016/j.cose.2017.10.007
Reference: COSE 1219

To appear in: *Computers & Security*

Received date: 8-2-2017
Revised date: 18-8-2017
Accepted date: 21-10-2017

Please cite this article as: Ding Yuxin, Xia Xiaoling, Chen Sheng, Li Ye, A malware detection method based on family behavior graph, *Computers & Security* (2017), https://doi.org/doi:10.1016/j.cose.2017.10.007.

A Malware Detection Method Based on Family Behavior Graph

Ding Yuxin, Xia Xiaoling, Chen Sheng, Li Ye

Harbin Institute of Technology Shenzhen Graduate School, Shenzhen University Town, Shenzhen

Tel.: +86 755 2603 2193, Fax: +86 755 2603 2461

ABSTRACT

Graph-based malware detection methods must build a behavior graph for each known malware, and they are thus difficult to apply in practice. To solve this issue, we study how to build a common behavior graph for each malware family. We represent malware behaviors as dependency graphs. To find the dependency relations between system calls, we use a dynamic taint analysis technique to mark the system call parameters with taint tags, and we then build the system call dependency graph by tracing the propagation of the taint data. Based on the dependency graphs of malware samples, we propose an algorithm to extract the common behavior graph, which is used to represent the behavioral features of a malware family. Finally, a graph matching algorithm that is based on the maximum weight subgraph is used to detect malicious code. The experimental results show that the proposed method has a high detection rate and a low false positive rate and can detect malware variants.

Keywords

dependency graph, dynamic taint analysis, malware, security, system call

Yuxin Ding received the Ph.D. degree in computer science from Institute of Software, Chinese Academy of Sciences, in 1999. He is currently an Associate Professor in the Department of Computer Science at the Harbin Institute of Technology Shenzhen Graduate School. His current research interests are primarily in computer security and machine learning.

Xiaoling Xia received her B.S. degrees in Computer Sciences from the Hunan University in 2014. She is currently a master student in the Department of Computer Science at the Harbin institute of technology Shenzhen Graduate School. Her current research interests are in machine learning and computer security.