Abstract

A new generation of attacks called as polymorphic attacks - where malware repeatedly mutates to deceive regular malware detection - are continuing to drive the growth in complexity of malware. Polymorphic malwares are using far more sophisticated approaches that may include editing its own source code to avoid signature-based detection. There is increasing necessity to handle this level of unprecedented polymorphism. Especially, scripts have been exploited to
widespread polymorphic malwares. In this paper, we propose a modified Hybrid detection model based dependency analysis. Every script malware can be represented by a dependency graph and then the detection can be transformed to the problem finding maximum subgraph isomorphism in that polymorphism still maintains the core of logical structures of malwares. We also present threshold selection and priority level management approaches which can be used to improve detection accuracy and reduce computational cost.

References

- A Survey on Techniques in Detection and Analyzing Malware Executables, IJARCSSE Volume 3, Issue 4, April 2013
- Arini Balakrishnan, Chloe Schulze "Code Obfuscation Literature Survey";
- Keehyung Kim, Byung-Ro Moon "Malware Detection based on Dependency Graph using Hybrid Genetic algorithm";
- Dinabandhu Bhandari, C. A. Murthy, Sankar K. Pal "Variance As A Stopping Criterion For Genetic Algorithms With Elitist Model";
- J. Ferrante, K. J. Ottenstein, and J. D. Warren "The program dependence graph and its use in optimization,";
- Thomas B’arecke and Marcin Dety niecki "Combining Exhaustive and Approximate Methods for Improved Sub-Graph Matching";
- Jacobo Toran´ "on the hardness of graph isomorphism";
- Thomas B’arecke and Marcin Dety niecki "Memetic Algorithms for Inexact Graph Matching";
Adaptation of Memetic Algorithm for detecting Polymorphic forms of Script Malware

**Index Terms**

Computer Science  
Memetic Algorithm

**Keywords**

Malware Detection  
Subgraph Isomorphism  
Genetic Algorithm  
Dependency Graph