Mingzhe Gao

mzgao@njnet.edu.cn · (+86) 151-5053-2663 · Blog

Research Interests

My current research focuses on algorithm-assisted solutions to security problems. More specifically, my research interests include areas such as binary malware/webshell detection, static program analysis (AST / opcode), and adversarial attacks against learning systems.

Education

Southeast University (SEU), Nanjing, China 2019 – 2022

Master student in Cyberspace Security (CS)

Shandong University of Technology, Shandong, China 2015 – 2019

B.S. in Software Engineering (SE)

Research Publication

Rectify the Malware Family Label via Hybrid Analysis 2023

Computer & Security(SCI JCR 2) Corresponding Author

Brief introduction: Rectify the Malware Label bias

- Propose a malware label correction tool called RecMaL. It employs hybrid analyses for malware label rectifying;
- Figure out the core reasons for mislabeling issues and summarize them into 3 types, including error, ontology and multi-label;
- With the same features and models used, rectifying the label can lead to a 1.9% improvement in accuracy;

A Malicious Code Static Detection Framework Based on Multi-Feature Ensemble Learning 2021

Journal of computer research and development(EI) Corresponding Author

Brief introduction: Propose a static malware detection framework based on multi-feature ensemble learning.

- Implemented 5 feature, including non-PE (Portable Executable) structure feature, visible string feature, assembly code sequences feature, PE structure feature and function call relationship feature;
- Use Bagging and Stacking ensemble algorithms to reduce the risk of overfitting;
- Achieved 97% accuracy rate;

Experience

Alibaba Cloud Inc. Hangzhou, China 2022 – Present

Security engineer Basic Security

Brief introduction: Reduce False Positives from Webshell Detection Engines.

- A cross-language solution was implemented to detect benign samples by parsing the intermediate language ASTs of PHP, JSP, and ASP/ASPX
- Recall Rate 98% for php language on public cloud
- Greatly reduce the False Positive rate of AV engine

Qi Anxin Technology Research Institute 2020 – 2022

Malware research based AI collaborated with Lingyun Ying

Brief introduction: Malware family classification, Conception shift, Adversarial attack

- Malware family classification via hybrid analysis
- Concept drift detection based on malware classifier
- Malware adversarial sample construction based on static feature

Skills

- Programming Languages: Python > C++ > Java
- Platform: Linux, Mac, Windows
- Tools: Sklearn, IDA Pro, Tensorflow
- Development: Binary, Web

Honors and Awards

To recommend the excellent graduation paper of master in Jiangsu Province — Apr. 2023
4th Prize, Award on DataCon Big Data Security Competition — Jan. 2023
1st Prize, Award on QiangWang Cup Artificial Intelligence Challenge — Nov. 2021
9th Prize, Award on DataCon Big Data Security Competition — Nov. 2021
2nd Prize, Award on ZongHeng Cup Network Security Innovation Competition — Nov. 2021
4th Prize, Award on Artificial intelligence-based malware family classification Competition — Sep. 2021

Miscellaneous

- Blog: https://mzgao.blog.csdn.net/
- Languages: English - Fluent, Mandarin - Native speaker
- Research interest: Malware analysis, Static program analysis, System and software security, Software Compostition Analysis, Vulnerability Exploitation and etc