DeepMalware: Deep Models and Mechanisms for Malware Detection and Defense

Xiaoyong Yuan*, Ruimin Sun*, Pan He, Qile Zhu, Aokun Chen, Daniela Oliveira, Xiaolin Li

Large-scale Intelligent Systems Laboratory, University of Florida

* equal contribution

Motivation

- Malware attacks: a major threat to personal and intellectual properties
  - Over half a billion personal information records are stolen or lost (last year);
  - a total estimated cost of $315 billion comes from cyber attacks;
  - With the rising of APTs, malware attacks today are becoming more and more sophisticated.
- We design ***DeepMalware*** with two-stream deep detection models and multi-stage online defense mechanisms in a spectrum-behavior OS.

Theory and Background

- **Conventional Malware Detection**
  - **Signature-based** malware detection:
    - efficient when detecting known attacks
    - a slight code obfuscation can evade
  - **Behavior-based** malware detection:
    - find zero-day attacks
    - instruction sequences
    - computation trace logic
    - system call sequences
- **Drawbacks** in conventional behavior detection:
  - pseudo-dynamic behavior
  - handcrafted feature engineering
  - low accuracy
  - limited datasets for training
  - no remedy for real-world online detection
- **Deep learning Detection** algorithm has achieved:
  - the state-of-the-art results in a broad spectrum of applications, such as vision, speech, text/NLP (natural language processing), recommendation, complex games, self-driving, precision medicine.

DeepMalware Method

- ***DeepMalware*** with two-stream deep detection models and multi-stage online defense mechanisms:
  - **Naïve detector** detects malware fast but inaccurate;
  - **Deep detector** performs well but needs long-term knowledge;

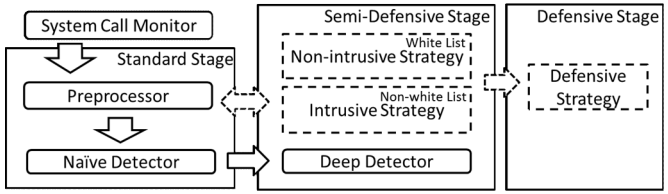

Figure 1. A workflow of the *DeepMalware* detection system

  - ***DeepMalware*** lets them contribute on their merits and make an online solution for malware detection.

Two-stream Deep Models

- Two key modules: *filter-reconstruction module* and *deep learning module.*

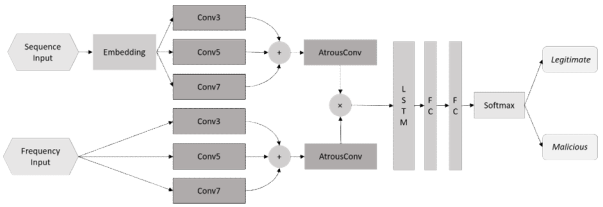

Figure 2. Two-stream deep model

- ***Filter-reconstruction module:***
  1) system-call filter
  2) n-gram model reconstruction
- ***Deep learning module*:**
  1) n-gram word embedding to convert n-gram indices into dense representation;
  2) multi-scale spatial models with inception multi-scale CNN to extract local and global information, Atrous convolution layers to broaden the receptive span, and two streams of sequence inputs and frequency inputs;
  3) temporal models with LSTM layers to extract temporal features between system calls.

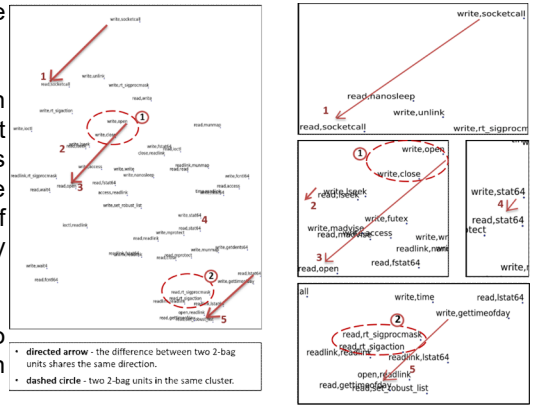

Figure 3. The distribution of "read" and "write" related 2-tuple of system calls in the Embedding Outputs. Difference between "read" and "write" related bags shares the similar direction.

Spectrum Online Defense Mechanism

- Deploy naïve detector in the *standard stage*
  - If it detects suspicious behaviors, the system will be transferred to se*mi-defensive stage.*
- For applications in the white list, a non-intrusive strategy is proposed in *semi-defensive stage*, otherwise, an intrusive strategy.
- *Semi-defensive stage* helps deep detector have enough time to gain long-term knowledge and decide to transfer the system to *standard stage* or *defensive stage.*

Expereiment Setup

- We choose 100 malware from Virustotal of six families and 400 workloads from CoreUtils Test Suite and conduct experiments with 20 virtual machines with four categories of blended attack and workload traces.

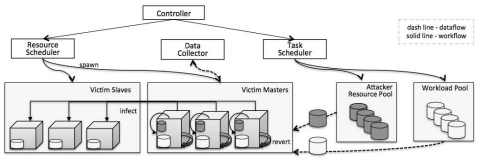

Figure 4. Data Set Generation System

Conclusion and Future Work

- Our deep learning model with the 2-tuple input performed best and achieved a 94.83% accuracy and a 94.66% F1 score.
- We conducted experiments in the Linux system as our preliminary efforts. We will contribute more in the Windows and Android system in the future work.