A Moving Target Approach to Enhancing Machine Learning-Based Malware Defense

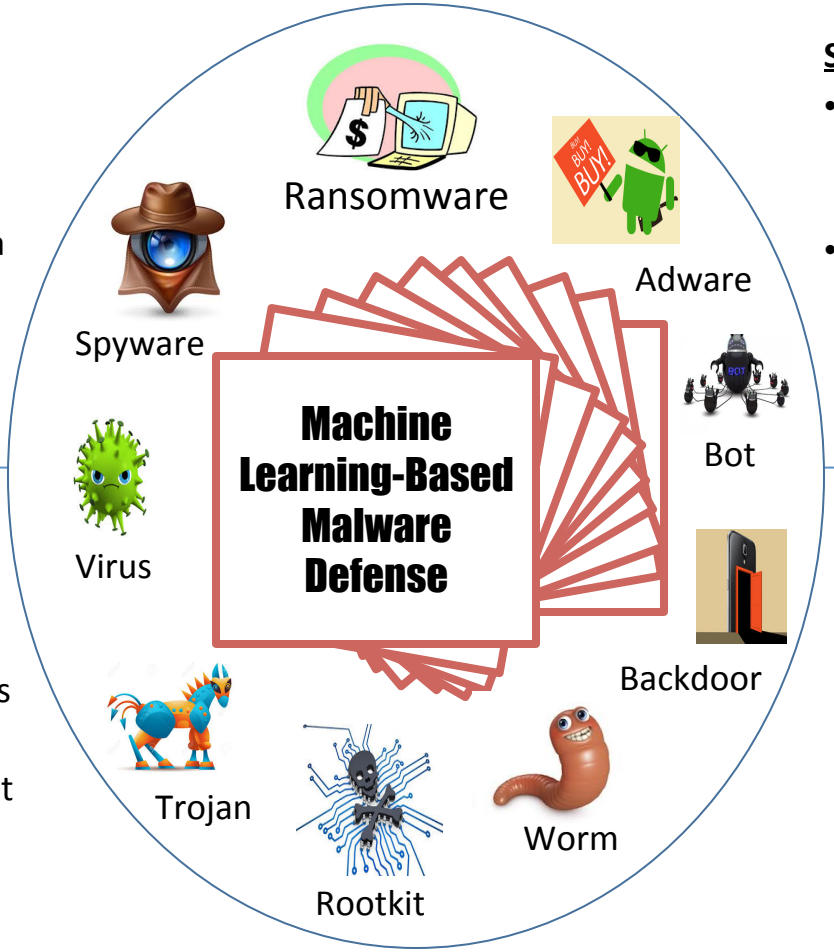
BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK

Challenge:

- Malware attacks are constantly evolving and getting more sophisticated
- Machine learning offers a promising approach to automating malware defense, but is not immune to adversarial manipulation

Solution:

- We propose a proactive strategy to enhance machine learning-based malware defense systems
- Our key innovation is to introduce a moving target into the attack surface of machine learning-based malware defense



Scientific Impact:

- Enhance robustness of machine learning-based malware defense systems
- Help the community gain deep insights into the security concerns associated with machine learning-based cyber defense

Broader Impact:

- Mitigate malware attacks that are behind a majority of cyber crimes
- Proposed methods can be deployed in practical malware defense systems
- Two female Ph.D. students are trained from this project; one undergraduate student is participating in this project

NSF Proposal 1618631
PI: Dr. Guanhua Yan
Binghamton University
State University of New York
Email: ghyan@binghamton.edu