Towards Malware Classifiers Robust to Adversarial Malware

Phung, Andy (School: Independence High School)
Mohapatra, Suryabhan (School: Independence High School)
Baviskar, Mihir (School: Independence High School)

Malware developers actively seek vulnerabilities in computer systems and malware detectors to exploit for personal gain. Most modern malware detectors are learning-based (converting malware to images for feature extraction) and/or heuristic-based (analyzing control flow), as signature-based detection can easily be evaded through obfuscation. However, the existence of perturbations for input images such that the resulting images, known as adversarial examples, are misclassified is a critical flaw of learning-based detectors. Similarly, behavioral optimization can be deployed to evade heuristic-based detectors. We aimed to exploit these flaws to design a new adversarial attack capable of preparing modern detection systems for specialized attacks. We proposed a new, highly efficient adversarial attack for malware examples. For a given malware program, “headers” composed of adversarial bits are generated using a denoising autoencoder emulating Carlini & Wagner’s adversarial attack and appended to the malware program. The nature of our attack also allows for the application of obfuscation or metamorphism techniques in tandem. Using the results of testing five datasets of 500 examples generated by our attack on four classifiers, we proved that the accuracy reduction results of our datasets are not significantly different using the Mann-Whitney U test. We also calculated the two-sample proportion confidence interval for the accuracy reduction in our results. Our research culminated in contributing a large dataset of adversarial malware examples generated with our attack to further research on robust malware detection. Future work may include evaluating our attack in real-world settings and exploring attacks fundamentally incorporating concealment techniques.

Awards Won:
King Abdulaziz &amp
his Companions Foundation for Giftedness and Creativity: On-line Mawhiba Universal Enrichment Program
King Abdulaziz &amp
his Companions Foundation for Giftedness and Creativity: Award of $500