CAREER: Automatic Learning of Adaptive Network-Centric Malware Detection Models

Challenge:

- Malware infections are at the origin of most modern cyber-crime
- Despite much research, reliably detecting malicious software remains very challenging

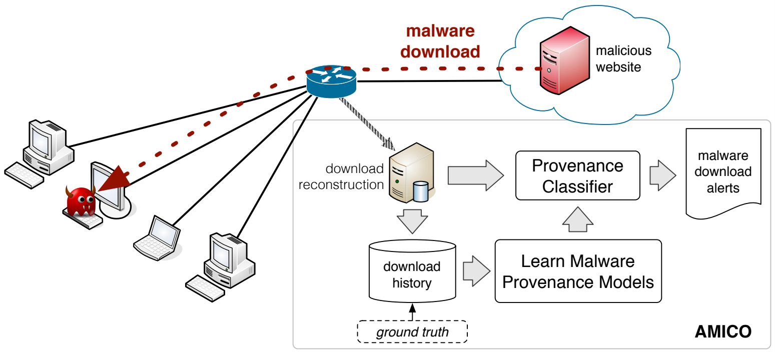
Solution:

- Automatically learn malware behavior from two points of view: (1) how malware behaves after it infects a machine; and (2) how malware is distributed to new victims

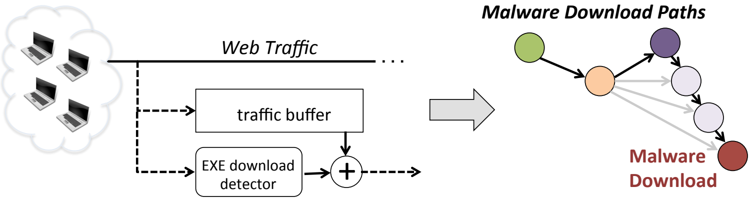
Award # CNS-1149051

PI: Roberto Perdisci (perdisci@cs.uga.edu)
University of Georgia - Athens, GA

Malware Download Detection



Reconstructing and Learning from Malware Download Paths



Scientific Impact:

- By studying malware behaviors and automatically learning new detection models from large numbers of real-world malware instances, this project aims to greatly improve our ability to defend computers from malware injections

Broader Impact:

- Improve Internet security, by creating new and more effective network-based malware defenses
- Creation of open-source malware detection software that is currently in use through the UGA campus network, and has been also funded by DHS via a transition to practice program