Metamorphic Worm Detection

Douglas S. Reeves      N.C. State University
http://modusoperandi.csc.ncsu.edu  NSF Grant CNS-0627505

The Problem

- Most infectious software has hundreds of variants; constantly mutating
- Examples of mutation techniques: register reassignment, code motion, instruction substitution, “junk” code insertion, etc.
- Rapid rate of mutation requires simplistic signatures to be continually updated & disseminated

Research Objective

Automatically create functional signatures not affected by such mutations

Approach

- Statically analyze binaries to extract system calls + parameters
- Use maximum weighted matching to identify similar patterns

Evaluation Results

1. Tested on programs with randomized memory address layouts. Most cases readily identifiable as variants.
2. Tested on hundreds of examples of malware mutants, and on examples of unrelated malware. Excellent ability to discriminate. See figure.
3. Tested on different releases of GNU software tools. Accurately identifies similarities.

Publication

“MetaAware: Identifying Metamorphic Malware”, in ACSAC 2007