How to 0wn the Internet in Your Spare Time

Stuart Staniford, Vern Paxson, Nicholas Weaver

Daniel Suskin

Outline

- Worms
- Better worms
- Defenses
- Analysis
- Future

Present worm techniques (2001)

- Code Red I: random scanning
- Code Red II: localized random scanning
- Nimda: multiple vectors

Limitations

- Spread is exponential
  - Slow to start
- Random scanning repeats
  - A lot

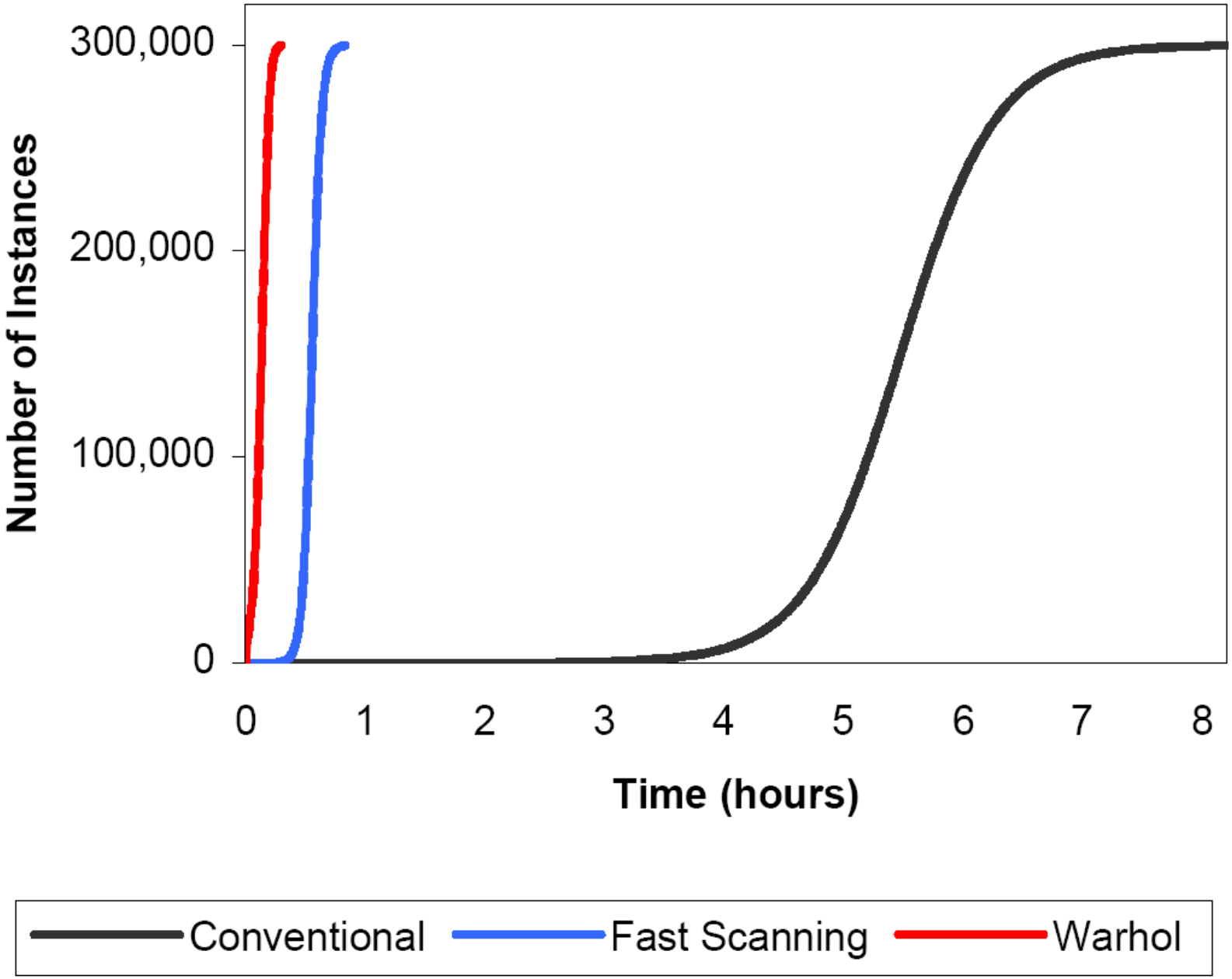
Improved worm techniques

- Hit list scanning
- Permutation scanning

Simulated effectiveness

- Complete connectivity
- Control over:
  - Number of vulnerable machines
  - Scans per second
  - Time to infect
  - Number infected by hit-list phase
  - Type of secondary scan

Simulated infection times



Projection

- Sub thirty-second near-completion times
- Example, when worm has:
  - Complete hit-list
  - Initial knowledge of host bandwidth
  - Hit-list servers
  - Up to 10^7 targets
  - 50% usage of a 256 Kbps connection
  - Limited traffic interference with itself

Contagion worms

- Slower
- Spread by application connections
- 9 million KaZaA hosts at a university involved in a one-month trace
- Seeding attack, then switch to contagion mode

Worms can be updated

- Efficiently
- Securely

Cyber CDC

- Detect
- Analyze
- Defeat
- Prevent

CCDC responsibilities

- Facilitate communications
- Research automated detection
- Analyze behavior
- Determine additional capabilities
- Propagate signatures and agents that use them to terminate or isolate
- Promote better security in internet applications

Analysis

- Balance
- CCDC practical issues
  - How

Future

- Faster and better
  - Worms
  - Countermeasures
- Founding a cyber CDC
  - How
  - Who
  - Where