

Internet Quarantine: Requirements for Containing Self-Propagating Code

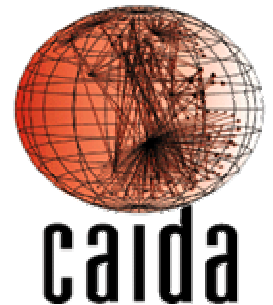
*David Moore, Colleen Shannon,
Geoffrey M. Voelker and Stefan Savage*

April 2, 2003 – INFOCOM 2003

dmoore @ caida.org

www.caida.org

www.cs.ucsd.edu



Motivation

- Internet worms increasingly common, virulent
 - Summer 2001 – CodeRed infects 360,000 in 10 hours
 - Winter 2003 – SQL Slammer infects 100,000 in 10 min
- Operational response inadequate to stop spread
- Any effective response *requires* automation

Design Issues for Automated Response

- Any reactive defense is defined by:
 - **Reaction time** – how long to detect, propagate information, and activate response
 - **Containment strategy** – how malicious behavior is identified
 - **Deployment scenario** - who participates in the system
- In this talk, we evaluate the requirements for these parameters to build **any** effective system.

Methodology

- **Simulate spread of worm across Internet topology:**
 - infected hosts *attempt* to spread at a fixed rate (probes/sec)
 - target selection is uniformly random over IPv4 space
- **Simulation of defense:**
 - system detects infection within reaction time
 - subset of network nodes employ a containment strategy
- **Evaluation metric:**
 - % of vulnerable hosts infected in 24 hours
 - 100 runs of each set of parameters (95th percentile taken)
 - Systems must plan for reasonable situations, **not** the average case
- **Source data:**
 - vulnerable hosts: 359,000 IP addresses of CodeRed v2 *victims*
 - Internet topology: AS routing topology derived from RouteViews

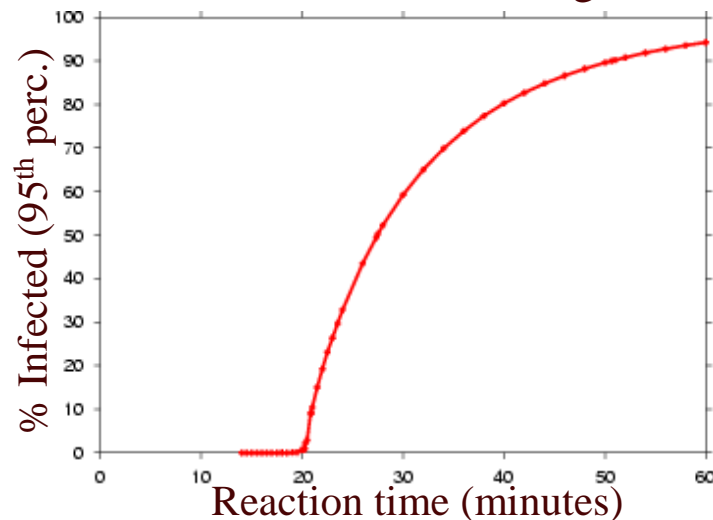
Initial Approach: Universal Deployment

- Assume **every host** employs the containment strategy
- Two natural containment strategies:
 - **Address blacklisting:**
 - block traffic from malicious source IP addresses
 - reaction time is relative to each infected host
 - **Content filtering:**
 - block traffic based on signature of content
 - reaction time is from first infection
- How quickly does each strategy need to react?
- How sensitive is reaction time to worm probe rate?

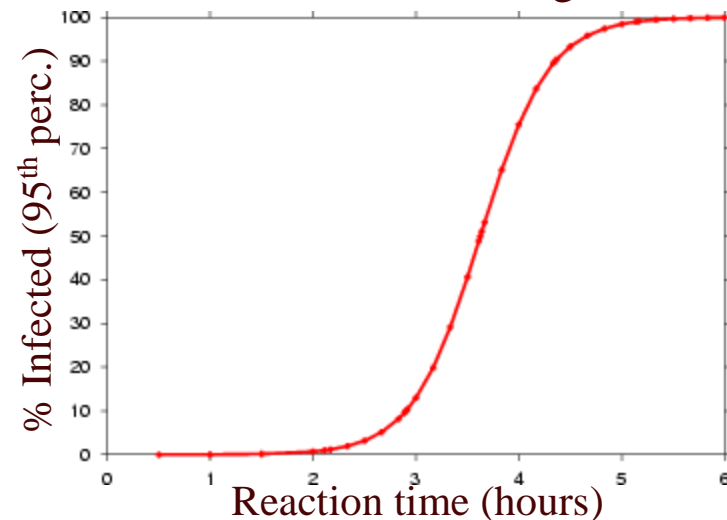


How quickly does each strategy need to react?

Address Blacklisting:

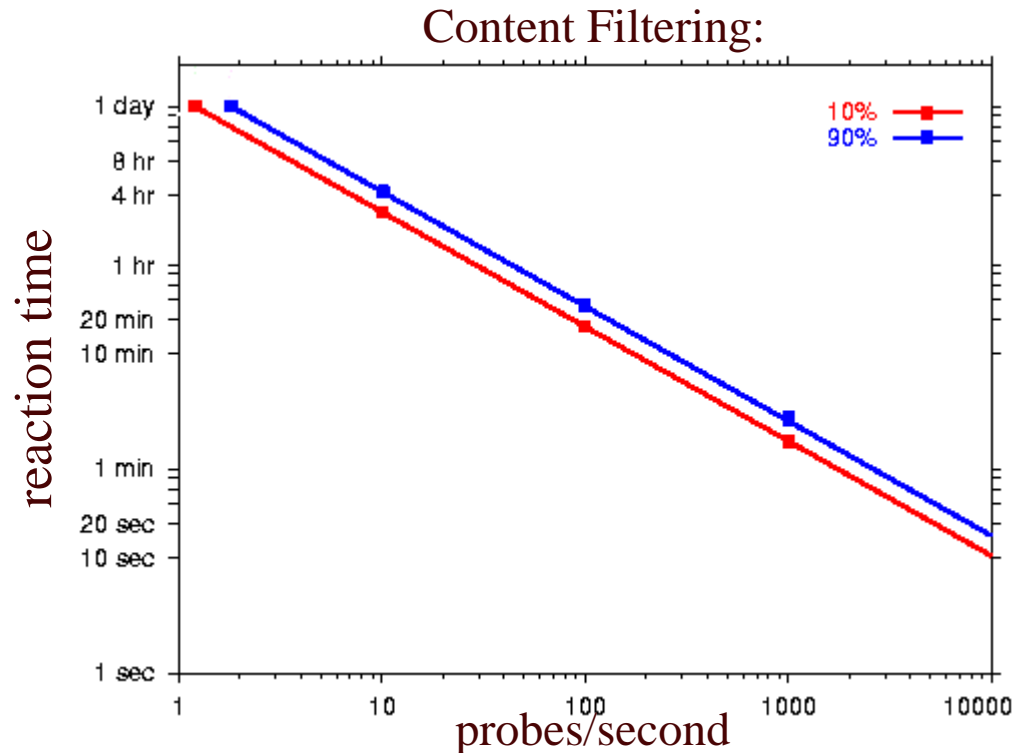


Content Filtering:



- To contain worms to 10% of vulnerable hosts after 24 hours of spreading at 10 probes/sec (CodeRed):
 - Address blacklisting: reaction time must be < 25 minutes.
 - Content filtering: reaction time must be < 3 hours

How sensitive is reaction time to worm probe rate?



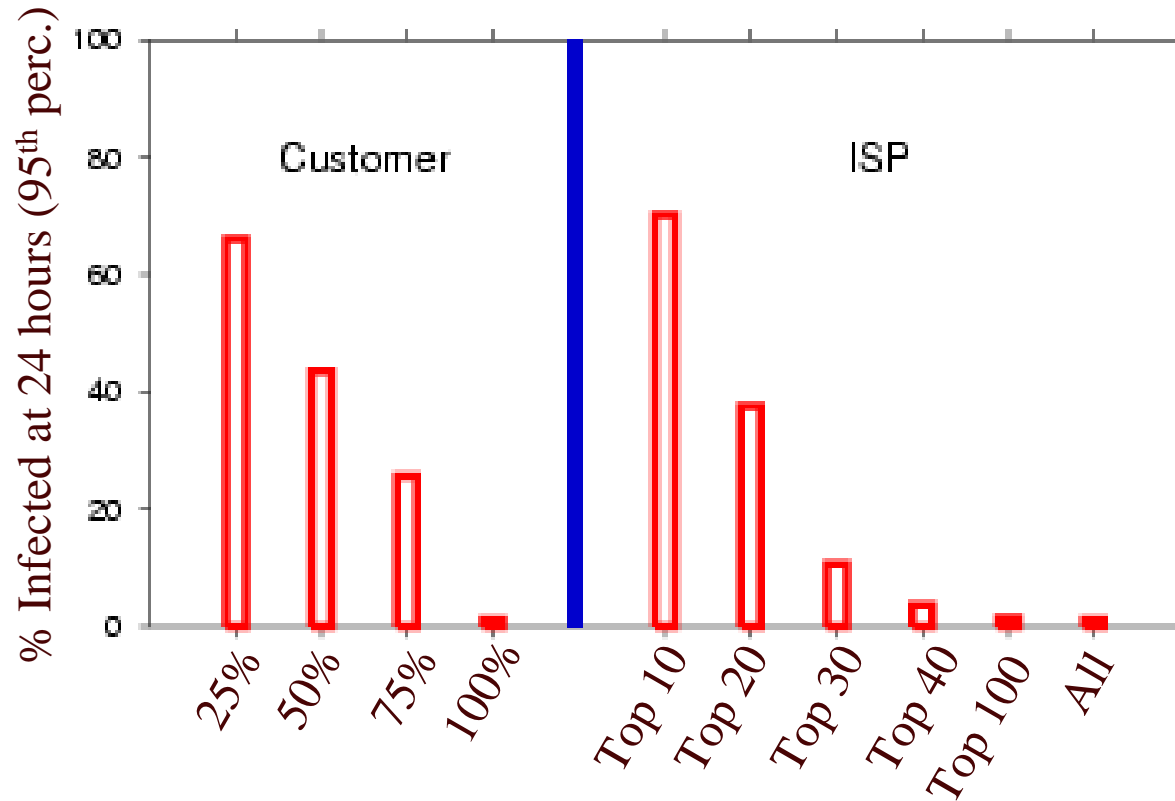
- Reaction times must be fast when probe rates get high:
 - 10 probes/sec: reaction time must be < 3 hours
 - 1000 probes/sec: reaction time must be < 2 minutes

Limited Network Deployment

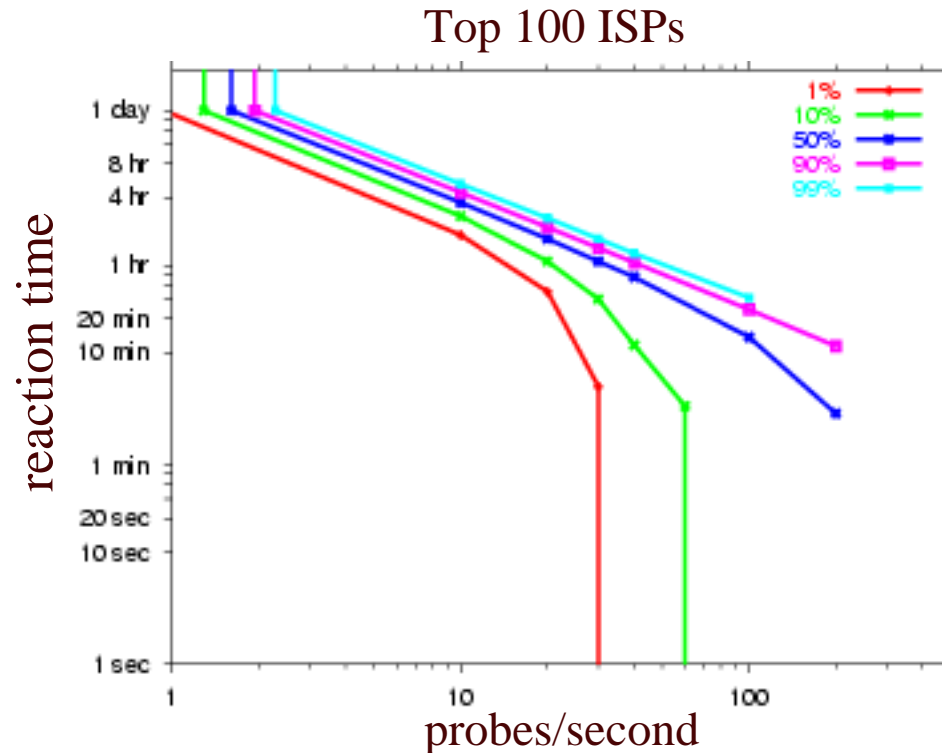
- Depending on every **host** to implement containment is not feasible:
 - installation and administration costs
 - system communication overhead
- A more realistic scenario is limited deployment in the **network**:
 - Customer Network: firewall-like inbound filtering of traffic
 - ISP Network: traffic through border routers of large transit ISPs
- How effective are the deployment scenarios?
- How sensitive is reaction time to worm probe rate under limited network deployment?

How effective are the deployment scenarios?

CodeRed-like Worm:



How sensitive is reaction time to worm probe rate?



- Above 60 probes/sec, containment to 10% hosts within 24 hours is impossible even with *instantaneous* reaction.

Summary

- Reaction time:
 - required reaction times are a couple minutes or less
- Containment strategy:
 - content filtering is more effective than address blacklisting
- Deployment scenarios:
 - need nearly all customer networks to provide containment
 - need at least top 40 ISPs provide containment



Conclusions

Reactive systems can contain some worms

...however...

Building such a system entails enormous engineering and administrative challenges.