

Worm Propagation

Worm Propagation

- Worms propagate too fast to be controlled effectively
 - By the time we recognize its presence, it has spread all over the world
- What can we do to control?

Some worms

- Code Red - probed internet hosts for known MS Web server vulnerability
- Infected machines participated in propagation
- Infected ~400,000 hosts in 14 hours
- At peak, infected 2,000 hosts/minute
- July 2001

Some Worms

- Slammer worm -attacked known vulnerability in MS SQL server
 - Buffer overflow
- UDP Attack at port 1434
- Simple to block once detected
- Jan. 2003

Worm propagation

- Send packets to random hosts to propagate
- Some use random destinations, some use sequential scans etc.
- Once infected, that machine will help in propagation
- Exponentially fast

Warhol Worms (Weaver)

- More sophisticated methods can be employed
- Choose some target hosts to infect
- Let each of these hosts subdivide address space etc.
- No replication of effort
- Quicker propagation

Flash Worms

- Contain a complete lists of hosts to infect
- Known to have vulnerabilities from earlier analysis
- No wasted effort in infecting robust machines
- Again, quicker propagation
- Staniford, Paxon, Weaver, 2002

How fast do worms propagate?

- Hetchcote, Math of Infectious disease, SIAM '00
- Rate of infection
 - Depends on # infected machines, non-infected machines, and probing rate
- Fraction of Infected machines at a given time:
 - $i(t) = e^{\beta(t-T)} / (1 + e^{\beta(t-T)})$
 - Grows exponentially fast initially, slows down as all machines are infected

Controlling worms

- Williamson "Throttling Worms" HP Tech. Rep
- Typically, most machines don't send a lot of packets
 - Even Fewer machines
- Throttle the rate at which packets are sent to new machines
- Reduce the rate of worm propagation
 - Reduces the probing rate β

Blocking worm threads

- Liston, Labrea "Welcome to my tarpit..."
- Worms randomly send packets
- Some of the addresses unassigned
- Block threads sending packets to unassigned/unused addresses
- Will slow down TCP-based worms
- Easy to defeat

Cisco's NBAR

- Network Based Application Recognition
- Allows router to block TCP connections with specific strings in payload
- Can limit worm propagation while allowing other connections

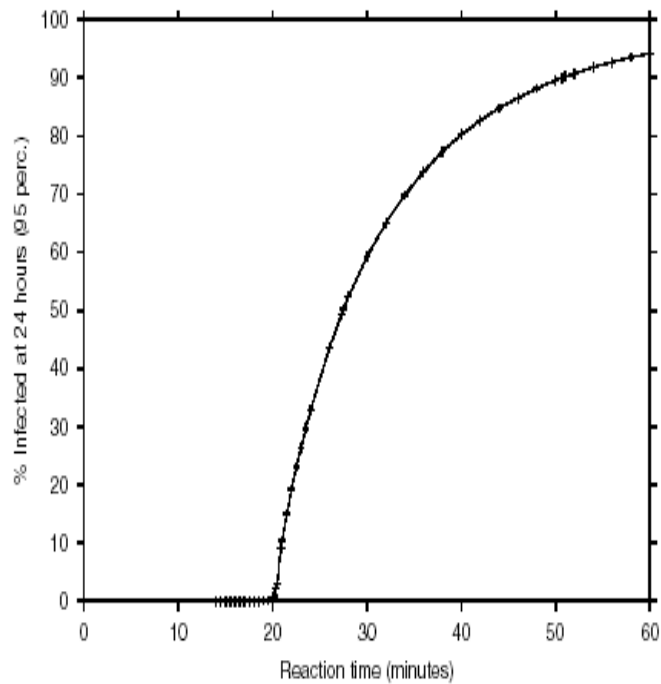
Containment Strategies

- Blacklist addresses of known infected machines
 - Don't accept connections
- Content Filtering (ala NBAR)
 - Require worm signatures
 - Drop packets with known signatures
 - Similar to AntiVirus techniques

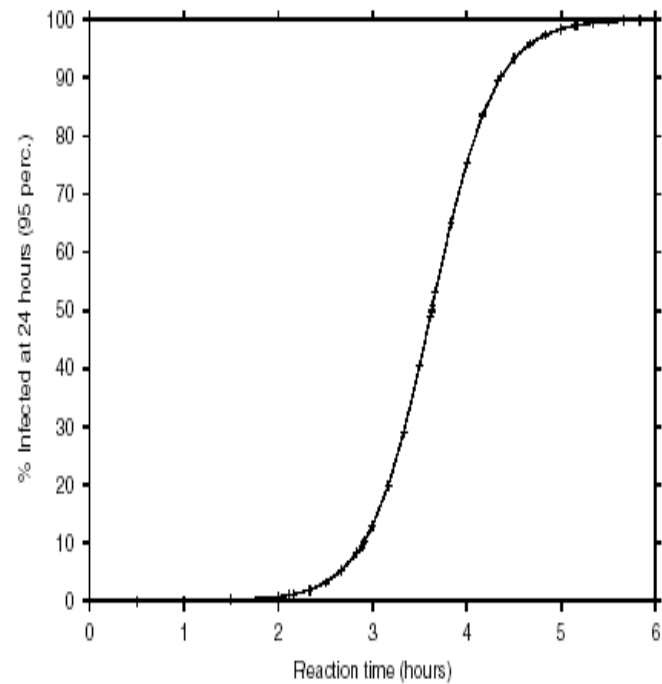
Containment speed

- Reaction time: How long does it take to detect, identify and characterize the worm?
 - During this time, the worm is free to do what it wants to do
- Deployment –is everyone ready to fight worms
- Faster reaction times better
- “Internet Quarantine” Moore, et al, Infocom 2003

How effective(CodeRed)?

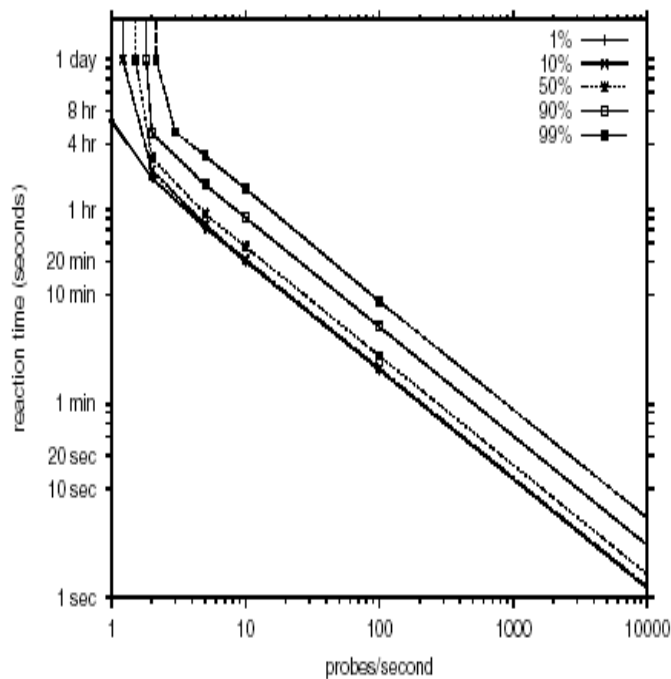


(a) Address Blacklisting

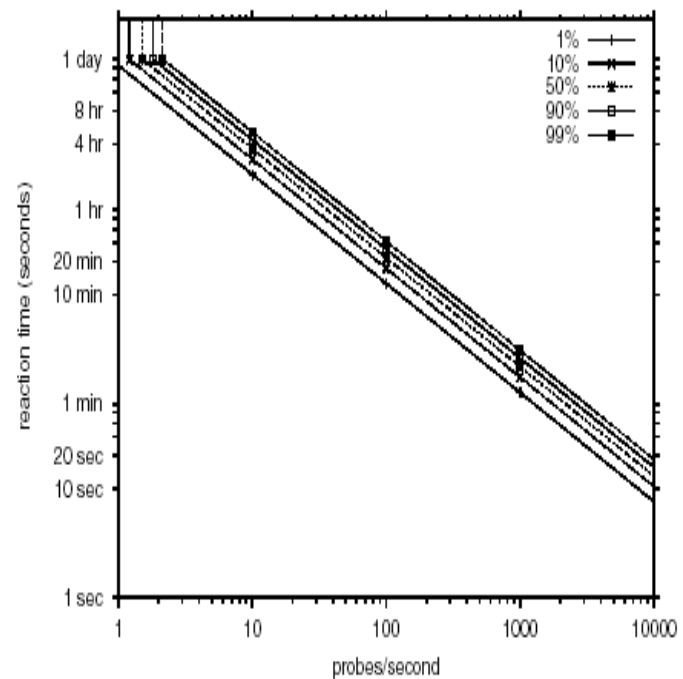


(b) Content Filtering

How Effective (general)?



(a) Address Blacklisting

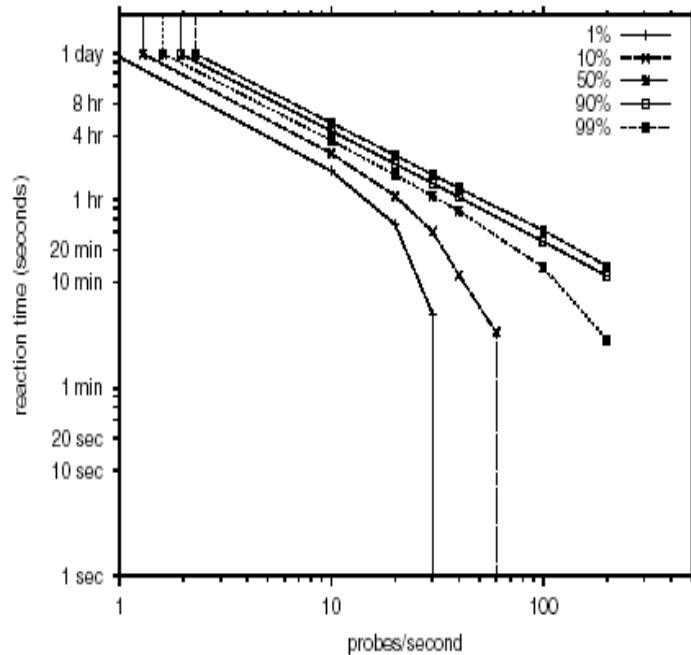


(b) Content Filtering

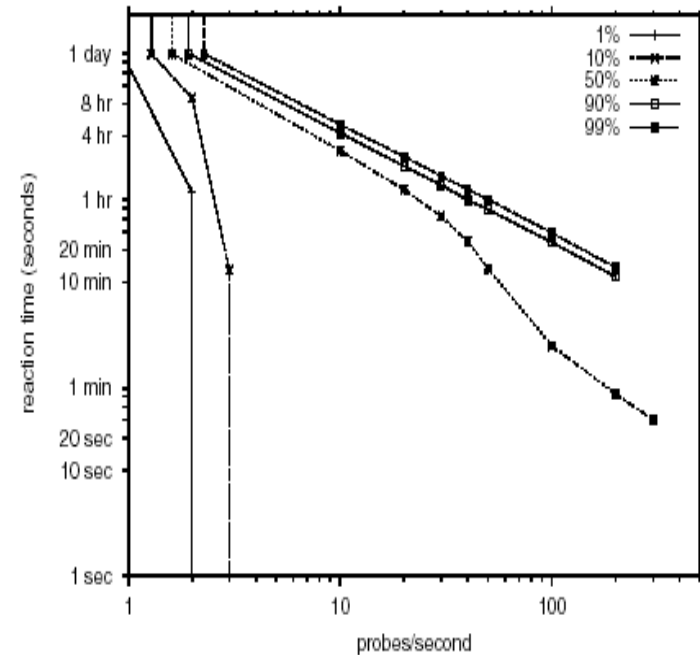
How effective(deployment)?



How effective(Deployment)?



(a) Top 100 ISPs



(b) 50% Customers

Summary of today's class

- Worms can propagate really fast
- A few known techniques slow down the rate of propagation
- Short Reaction times, wide-spread deployment necessary
 - Reaction times so short -need automatic means of worm identification
- Content filtering more effective than address blacklisting