On the Effectiveness of Distributed Worm Monitoring

Moheeb Abu Rajab   Fabian Monrose   Andreas Terzis
Computer Science Department
Johns Hopkins University
Monitoring Internet Threats

- Threat monitoring techniques:
  - Intrusion detection systems monitoring active networks
  - Monitoring routable unused IP space [Moore et al, 2002]

- Monitoring unused address space is attractive
  - No legitimate traffic
  - Forensic analysis and early warning

- CAIDA deployed the first /8 telescope
Single Monitor Case

DoS Attack

Worm Scans

/8

DoS Attack

DoS Backscatter

Worm Scans
Size Matters!

- Size of the monitor is an important factor in providing an accurate view of a worm breakout [Moore et al, 2002]

- But there are several other factors yet to be explored
Single monitor view is too limited

DoS Attack

Worm Scans

Non-uniform scanner
Goals

- Provide a model to evaluate the performance of distributed monitoring systems in terms of:
  - Number of monitors?
  - Sizes of monitors and the overall IP space requirements?

- Provide guidelines for better design and monitor deployment practices.
Outline

- Problem and Motivation

- A Worm Propagation Model
  - Population Distribution
  - Extended worm model

- Distributed Worm Monitoring
  - Distributed Telescope Model
  - Design parameters

- Summary
Why another worm model?

- Previous worm models assumed that the vulnerable population is **uniformly** distributed over the whole IP space.

- Sources of non-uniformity in population distribution
  - Un-allocated address space
  - Highly-clustered allocated space
  - Usage of the allocated space
The distribution of Vulnerable population over the IP space is far from uniform. Best fits a Log-normal distribution.
Extended Worm Propagation Model

- Worm propagation models must incorporate population density distribution.

- Especially Non-uniform scanning worms:
  - Probability of scanning a host depends on its location relative to the infected scanner
Non-uniform worm propagation model

- Expected number of scans per /16 subnet

\[ k_i^j = p_{16} s b_i^j + p_8 s b_i^{(/8)} \frac{2^{16}}{2^{24}} + p_0 s n_i \frac{2^{16}}{2^{32}} \]
Non-uniform worm propagation model

- The expected number of infected hosts per /16 subnet (AAWP Model [Chen et al, 2003])

\[ b_{i+1}^j = b_i^j + (v_i - b_i^j) \left[ 1 - \left( 1 - \frac{1}{2^{16}} \right)^{k_i^j} \right] \]

Vulnerable non-infected hosts

- The expected total infection

\[ n_{i+1} = \sum_{j=1}^{2^{16}} b_i^j \]
Impact of population distribution

Number of Infected hosts vs time, for a Nimda-like worm

\[ s = 100 \text{ scans/time tick}, P_{16} = 0.5, P_{8} = 0.25, P_0 = 0.25 \]

\( N = 10^6 \) hosts uniformly distributed
Over the IP space

\( N = 620,000 \) hosts extracted from
DShield data set
Outline

- Problem and Motivation

- Better Worm Model
  - Population Distribution
  - Extended worm model

- Distributed Worm Monitoring
  - Distributed monitoring system model
  - Design parameters

- Summary
Using the Model---
Distributed Monitoring:

- What do we want to evaluate?

  - System detection time: the time it takes the monitoring system to detect (with particular confidence) a new scanner.
Assumptions

- Single scan detection

- Information sharing and aggregation infrastructure among all monitors.
Monitors Logical Hierarchy

\[ S^{(0)} = M + M_A + M_B + M_C \]

\[ S^{(8)} = M_B + M_C \]

\[ S^{(16)} = M_C \]
Evaluation

- Nimda-like scanner

- Three Monitor deployment scenarios:
  - Random monitor deployment
  - Full knowledge of population distribution
  - Partial population knowledge
Evaluation (Random monitor placement)

Random Monitor placement  
$P_r = 0.999$, $s = 10$ scans/time tick  
Nimda-like scanning

with only 40 hosts per /16, 7100 more scans will cause infecting 2 victims before being detected
Evaluation (Full vulnerable distribution knowledge)

Monitors deployed in top populated prefixes

512 /17 $\rightarrow$ 9 time ticks

/8 $\rightarrow$ 940 time ticks
Evaluation (Partial Knowledge)

Monitors deployed randomly over the 5000 most populated /16 prefixes (contain 90% of the vulnerable population)

Example: 512 monitors with 2048 IP addresses/monitor → 160 time ticks
Practical Considerations

- Monitors will be deployed at different administrative domains.

- How many domains are needed to deploy these 512 monitors?

- Mapping the monitors to AS space, only 130 AS’s among the top address space owners are required to achieve detection time of 160 time ticks
Summary

- Population distribution has a profound impact on worm propagation speed.

- Distributed Monitoring provides an improved detection time (three times faster than a single monitor of equivalent size).

- Even partial knowledge of the population distribution can improve detection time by roughly 30 times.

- Effective distributed monitoring is possible with cooperation among top address space owners.
Questions?