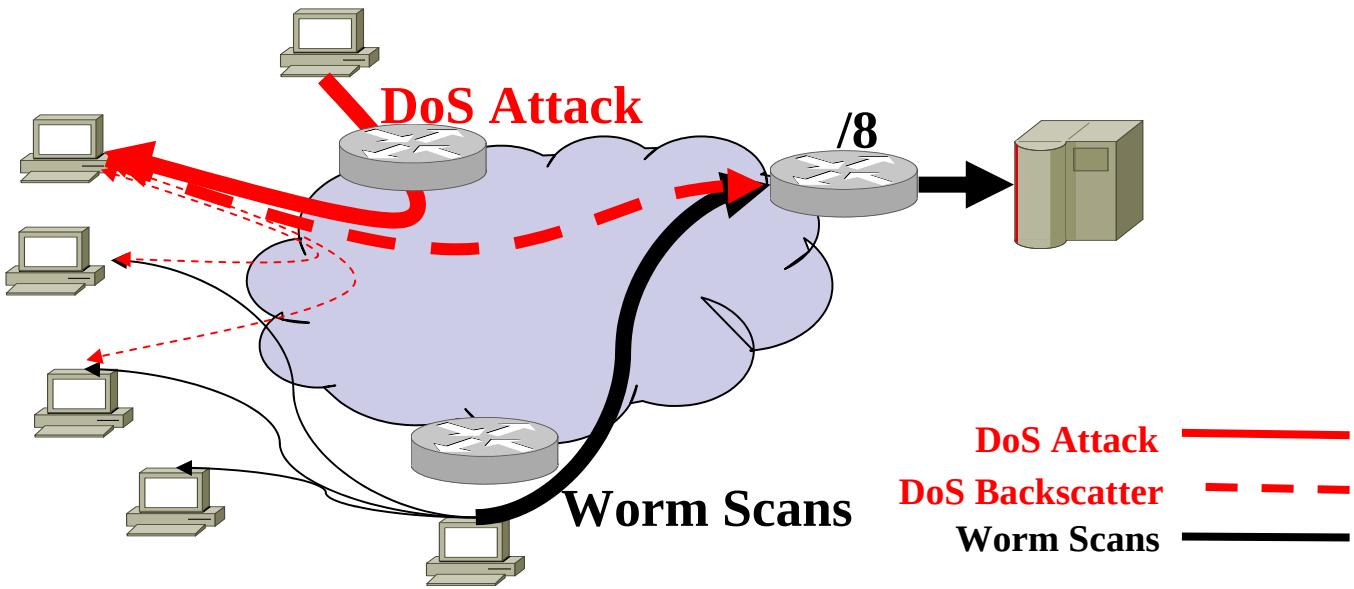
Fast and Evasive Attacks: *Highlighting the Challenges Ahead*

Moheeb Rajab, Fabian Monrose, and Andreas Terzis
Computer Science Department
Johns Hopkins University

Outline

- Background
- Related Work
- Sampling Attacks
- Malware spreading scenarios
- Promising Countermeasures
- Summary

Network telescopes



- Traffic monitors located in routable but unused IP space
  - Passive vs. Active
- Uses
  - Detect and characterize DDoS *backscatter*
  - Malware detection, collection, and forensic analysis

Network Telescopes (cont.)

- Advantages
  - No legitimate traffic *should* appear at a telescope
  - Detect unknown (zero-day) threats
- Benefits multiply by deploying distributed telescopes at a *large scale*

Thinking Ahead

- Network telescopes are invaluable assets in defending the network
- Bad News: Attackers will try to diminish their utility
  - Early indications of evolving behavior in the wild (*e.g.*, preferential scanning worms)
  - Botnets applying localized scanning
- On the Good Side: The above can be mitigated with sophisticated monitor placement strategies

Evasive Attacks

- Most popular monitoring approaches still assume that monitors can be effectively hidden from attackers merely by keeping the monitored IP space secret.
- Attackers could exploit the side-effects of monitor existence to locate and evade detection.
- Result: Evasive malware spreading with little spurious traffic

Related work

- Bethencort et al. USENIX ’05,
  - Limited to network monitors that advertise their datasets.
  - Involves long feedback loop (reaching 24 hrs.)
  - Requires excessive number of probes.
- Chen et al. WORM ’05
  - Maximizes worm scans towards densely populated /8 prefixes.
  - Can not detect network monitors.

Contributions

- Introduce a new lightweight sampling technique to detect *dark* space
  - *i.e.* Unused IP space and passive network monitors.
- Demonstrate the virulence of evasive malware spreading strategies that exploit the sampling information.
- Highlight the need to take a proactive stand and rethink current monitoring practices in light of such threats and discuss promising defense measures.

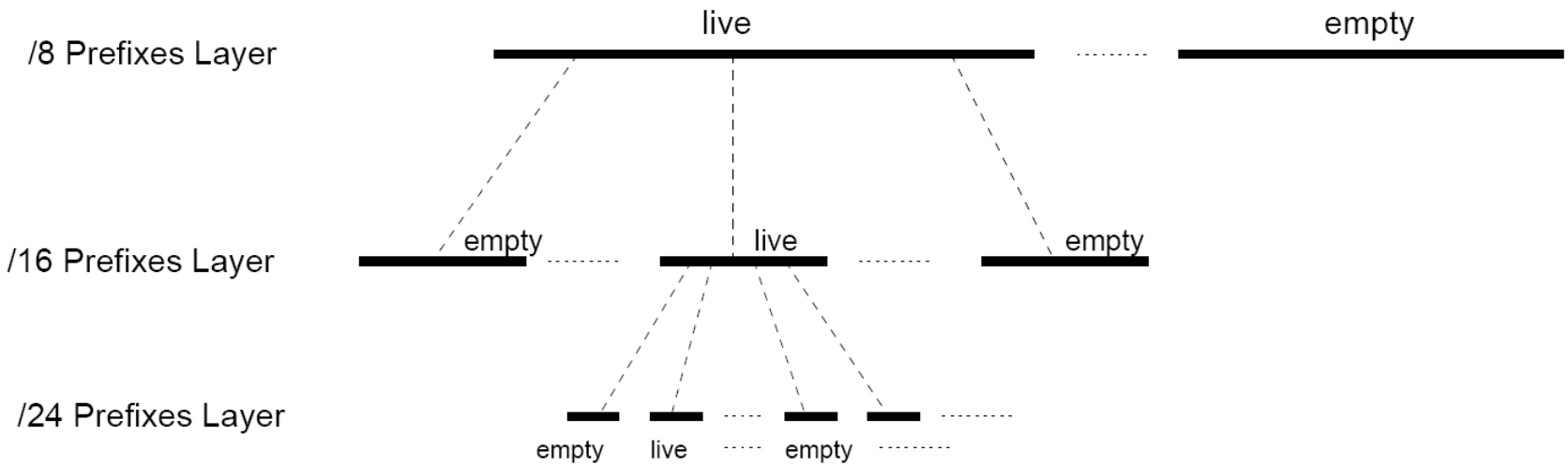
Evasive Sampling Attack

- Use sampling to probe the liveliness of address blocks with high confidence
  - TCP SYN probes, ACK probes, ICMPs, etc
  - Can be completely innocuous, using different ports from ones employed by known exploits
  - If response is received prefix is marked as *live*

Discovering the live IP space

- Requirements:
  - Fidelity and Accuracy.
  - Least number of probes.
  - Evasive sampling technique.
- Insight:
  - Exploit the clustered nature of the IP space to devise a hierarchical sampling process

Hierarchical Sampling Process



- Question: How many samples are necessary?

Estimating the sample size

- Challenge:
  - Find the minimum number of samples to detect the vast majority of the dark space with high confidence while minimizing misclassification of live space.
- Sampling Model:

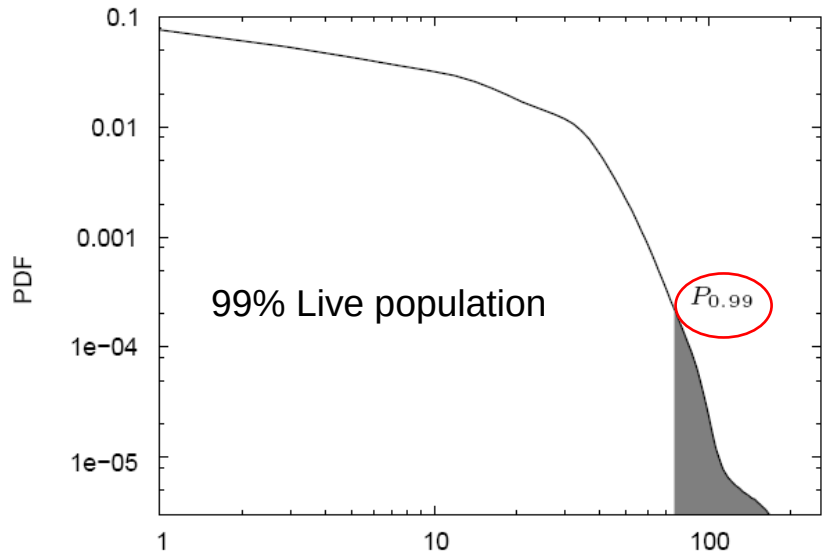
$$n = \frac{\log(1-\alpha)}{\log(1-p_{l,g})}$$

$P_{l,g}$ = Min. Number of live hosts / prefix size

- Problem: we don't know the number of live hosts in each prefix.

Estimating the sample size (ctnd.)

- Ideally, direct estimation of the live hosts distribution requires large sample size (especially for the lower layers).
- Instead, we indirectly estimate it from its marginal distribution using a small dataset.



$$L_{\min.} = P_{0.99} \cdot (total\_population)$$

$$P_{l,g} = L_{\min.} / 2^{24}$$

$$n = \frac{\log(1-\alpha)}{\log(1-p_{l,g})}$$

Evaluation

- Trace based evaluation
- Trace Summary
  - DShield large dataset (32 million sources)
  - Local Darknet trace (1.2 million sources)

Trace Based Evaluation

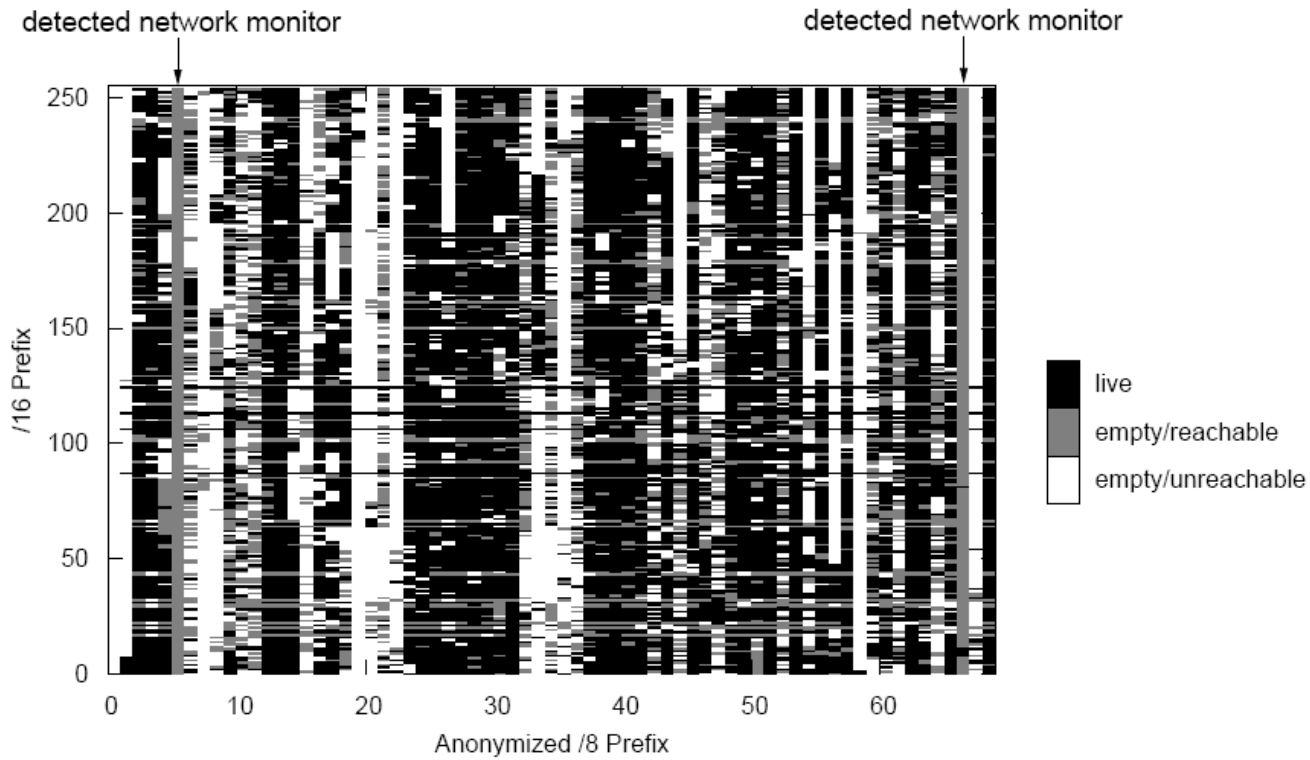
- Finding 1:
  - 400 samples/prefix enough to achieve classification accuracy 99.9 % of /16 prefixes
- Finding 2:
  - On average sampling less than 5% of the IP space accurately located 98% of the live population and 96% of the vulnerable population (from our datasets).

Sampling: results from the wild

- One might expect firewalls would thwart the accuracy of sampling by hiding parts of the IP space.

- Sampling in the wild
  - Probed 69 /8 prefixes, using 256 PlanetLab nodes

Sampling in the wild



- Detected two well known network monitors

Sampling in the wild

- Finding 1:
  - Mean number of samples = 50
- Finding 2:
  - Detected live prefixes containing 88% of the live population in the Dshield trace.
- Validation:
  - BGP tables from Routeviews show that 63% of the prefixes classified as empty were not advertised.

Why is this bad?

- Sampling knowledge can be exploited to produce evasive malware spreading.

- Two example scenarios:
  - Offline Sampling
  - Online Sampling

Offline Sampling Malware

- Sampling is done *offline* and knowledge is disseminated to the infected population through and encoded bitmap
- Each nodes scans the IP space uniformly and sends scans to live prefixes only
- However, choose your favorite scanning strategy

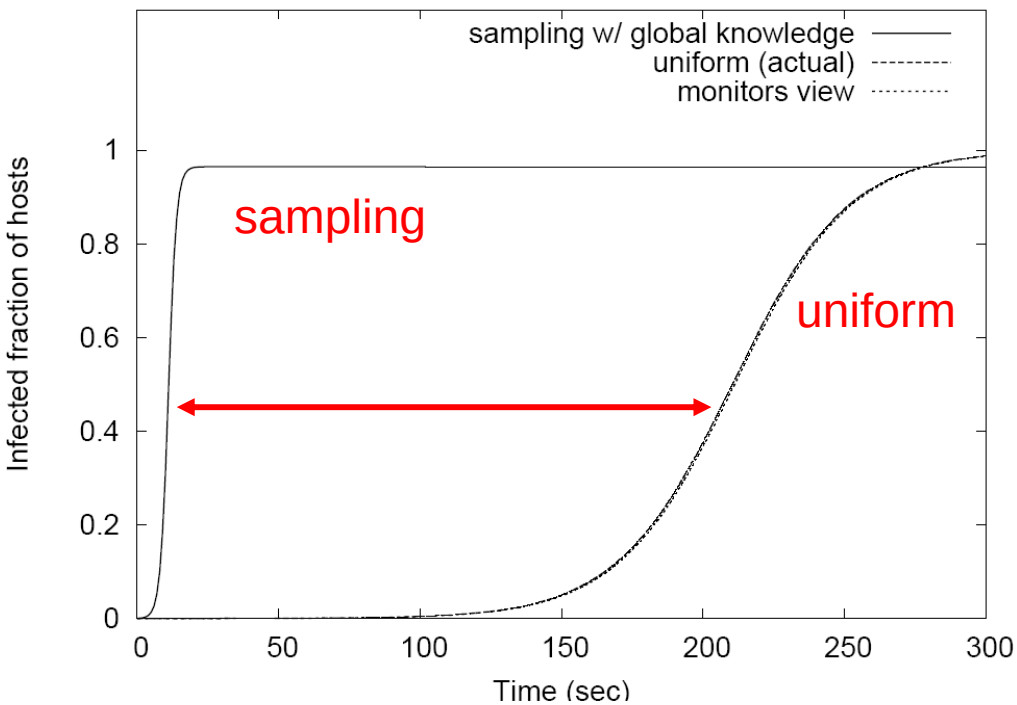
Offline Attack model

- Given:
  - V : total vulnerable population
  - I : total infected population
  - P: probability of contacting a host
  - s: average scanning rate

$$I_{t+1} = I_t + (V_t - I_t)\left[1 - (1 - p)^{sI_t}\right]$$

$$p = \frac{1}{2^{32}} \quad \text{total\_live\_space}$$

Simulation results

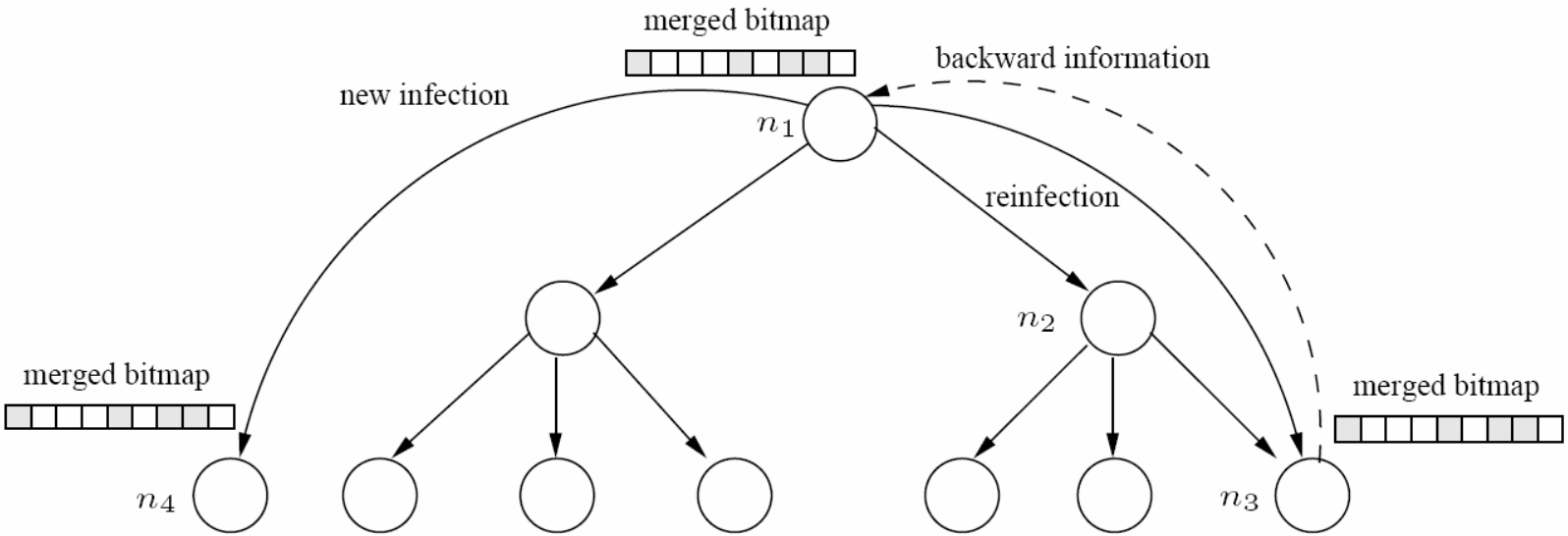


- 1024 /24 monitors + /8 monitors mapped with 100% accuracy.
- Average spurious traffic rate received at the monitors **<1 %** average background noise

Spreads 10 times faster than classic uniform spreading worm

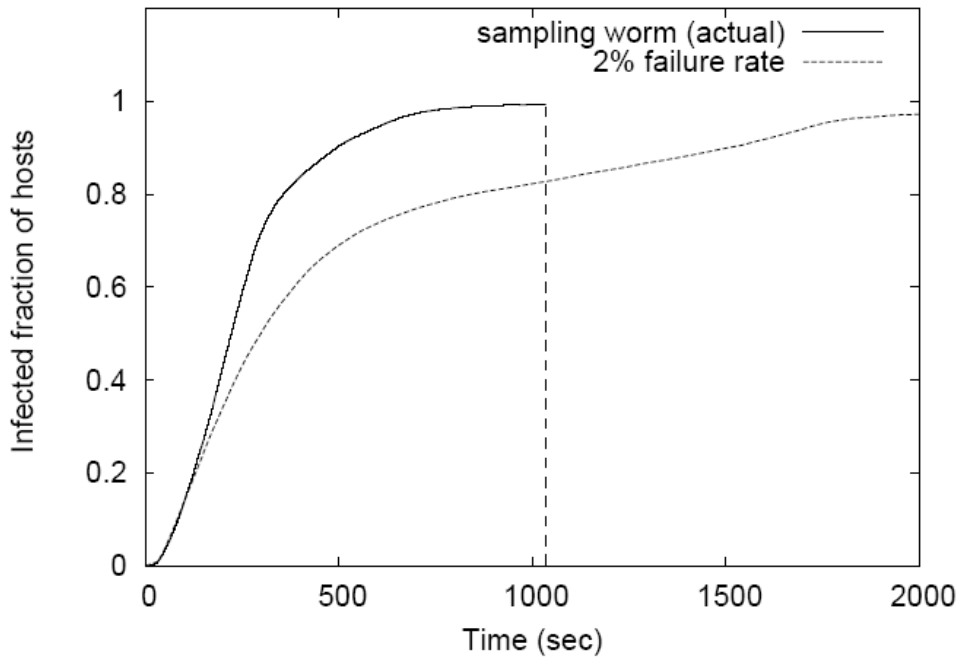
Online Spreading

- Combine sampling and scanning phases
- Forward and backward sampling progress sharing



Online Spreading

- Reduced payload (only 256 bits required)
- Online sampling does not hinder malware spreading speed
- Imperfect redundancy reduction serves to compensate for end-host failures



Promising Defenses

- **Active Responders**
  - Attract malware, by luring the attack into the monitor space.
  - However, active responders are not immune against simple variants of the sampling attacks.
  - Responding to all ports and all addresses looks equally suspicious
  - To be effective responder need to mimic the persona of actual operational networks
- Roaming the monitored Space.
- Use smaller monitors.

Summary

- We show the credible threat from a simple evasive strategy that undermines the effectiveness of widely adopted monitoring technique
- We highlight the need to be proactive and discuss promising directions to counter such threats.

Acknowledgements

- DShield.
- Hopkins Information Technology Services (HITS).
- We thank the anonymous reviewers.

THANK YOU !

Defenses: What does not work

- 1024 /24 monitors + /8 monitors mapped with 100% accuracy
- Increasing monitor deployment, does not help even when population aware placement strategy is used.