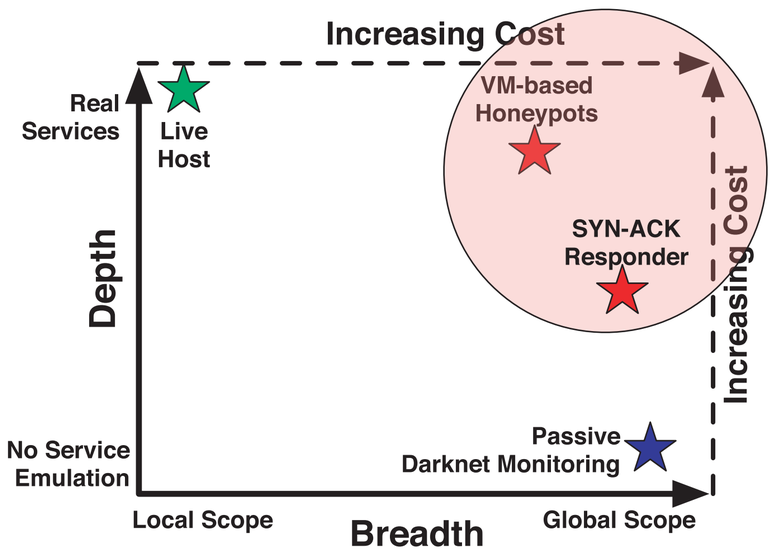
CT-ISG: Topology-Aware Internet Threat Detection Using Pervasive Darknets

Principle Investigators: Farnam Jahanian, Jignesh Patel
University of Michigan

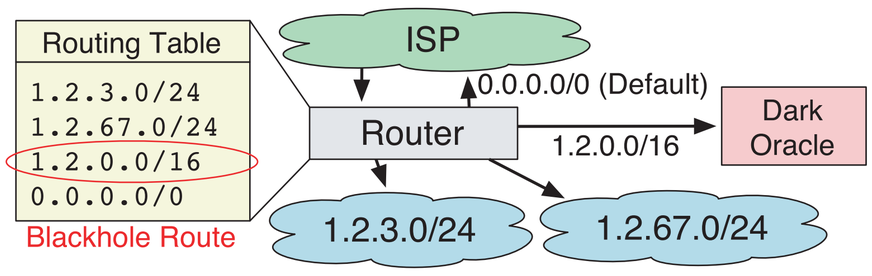
Approach:

- Automatically discover **unused** and **unreachable** addresses that contain no active hosts or services
- Deploy darknet detectors and use multi-dimentional data mining techniques to identify threats
- Enables detection of both **ingress** and **egress** infection attempts

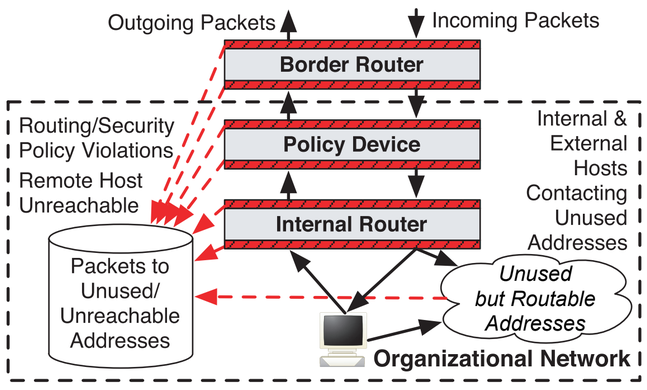


Setup:

- Darknet deployment is simple and leverages is the existing routing infrastructure
- Transparent: darknet failures do not harm the network



External routing data, internal routing data, host configuration data, and policy device configurations used to construct map of unsued and unreachable addresses



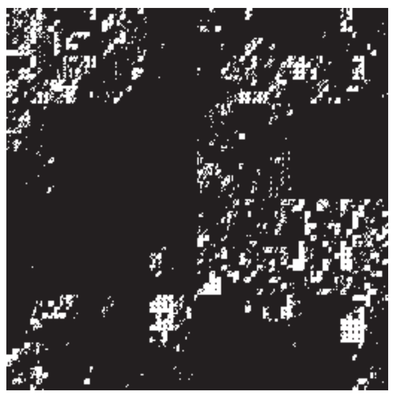
Pervasive Internal Deployment:

- Monitor unused and unreachable dark addresses **inside** the network
- Leverage other sources of address allocation data like DHCP
- Automate the process of discovering

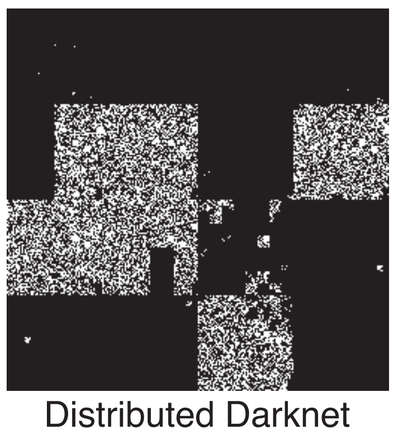
Sample report from an enterprise deployment

```
All Sources
  Total IP Packets:   59468350
  Total TCP Packets:  21950036
  Total UDP Packets:  31548715
  Total ICMP Packets: 5958197
  Unique Source IPs:  102160
  Statistics on Top 10 TCP Source IPs:
    Source IP       TCP  Pkt Cnt  Top 3 Dest Ports
    X.X.51.50       318155        tcp/445:287811 tcp/80:4836 tcp/443:4796
    X.X.221.76      185635        tcp/445:184937 tcp/5000:525 tcp/80:159
    X.X.115.81      168203        tcp/445:168185 tcp/1863:9 tcp/80:9
```

Map of an IMS enterpise darknet deployment

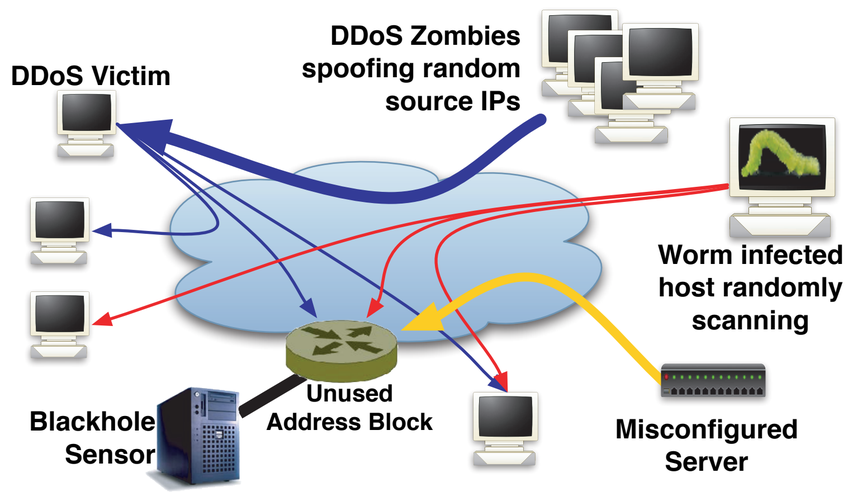


Infected/Misconfigured Sources



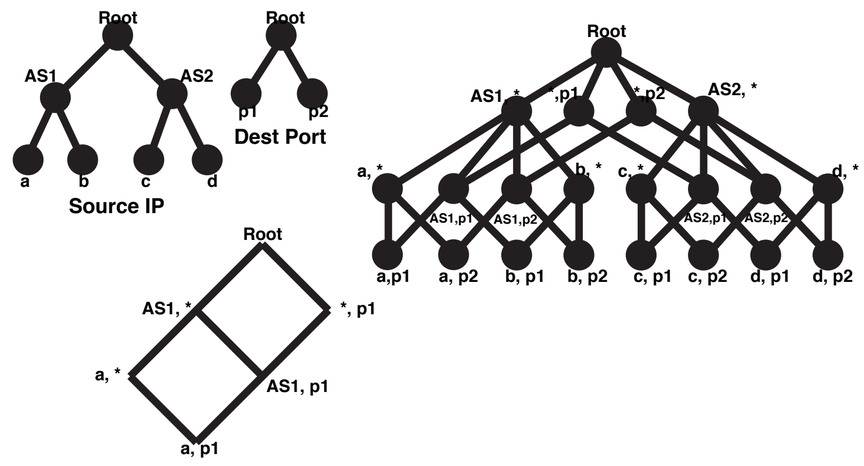
Distributed Darknet Sensors

Darknet Sensors:



- A darknet sensor monitors an unused globally advertised address block that contains **no active hosts.**
- Traffic is the result of **DDoS backscatter, worm propagation, misconfiguration,** or other **scanning.**

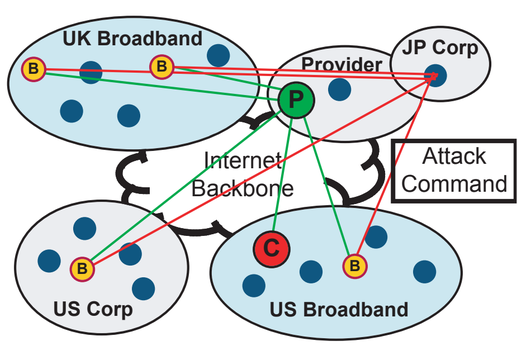
Multi-Dimentional Data Mining:



- Data at pervasive darknets systematically explored using a novel multi-dimentional data mining approach
- Semantic knowledge of packet attributes is used to cluster events and identify zero-day threats, targeted attacks, bot-recruiting, and worms

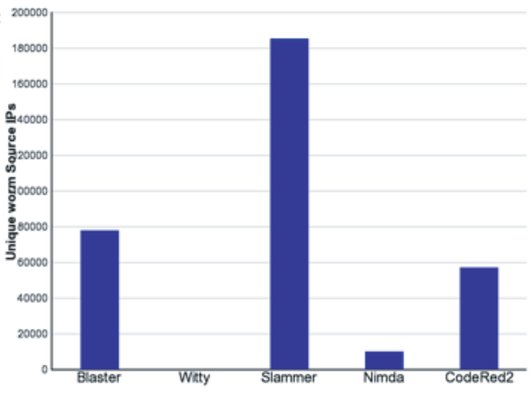
Changing Threat Landscape:

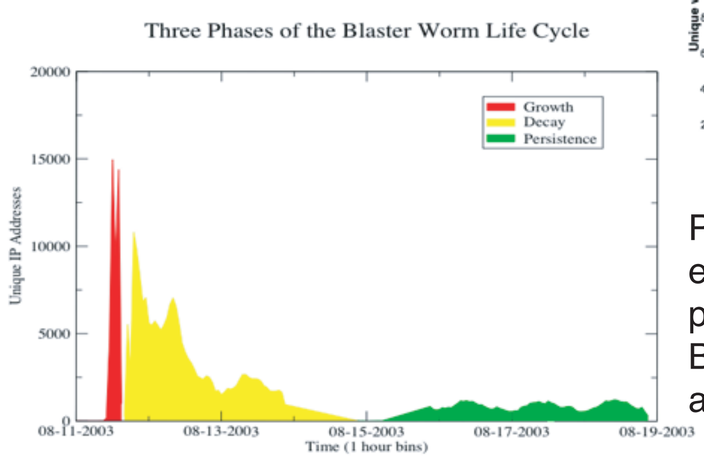
- Fundamental Change in Internet threats:
  Attackers have learned a compromised system is more useful alive than dead!
- Transformation is motivated by economic incentives
  - DoS Extortion
  - Identity Theft
  - Phishing
  - SPAM
  - Spyware



Observations:

Hundreds of thousands of unique hosts still infected after several years.





Pervasive darknets produced event analysis for numerous prevalent threats including Blaster, Sasser, Witty, Dabber, and botnets.