Characterizing Dark DNS Behavior

Jon Oberheide, Manish Karir†,*
Z. Morley Mao, Farnam Jahanian**
**University of Michigan*
†Merit Network, Inc.

July 12, 2007

DIMVA 2007

Presentation Summary

- Sell/short/don't fly NWA ;-)
- Implications of darknet sensor evasion via DNS PTR reconnaissance
- Define dark DNS and breakdown collected dark DNS activity
- Introduce honeydns tool to complement darknet deployments

Darknet Monitoring

- Darknet sensors
  - AKA honeypots, honeynet, telescopes, etc
  - Monitor unused IP address space

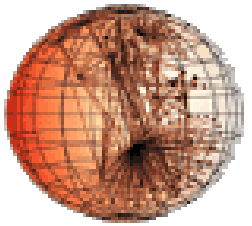
ATLAS

vmware®

nepenthes
- finest collection -

Internet Motion Sensor

The Honeynet
PROJECT®



Darknet Evasion

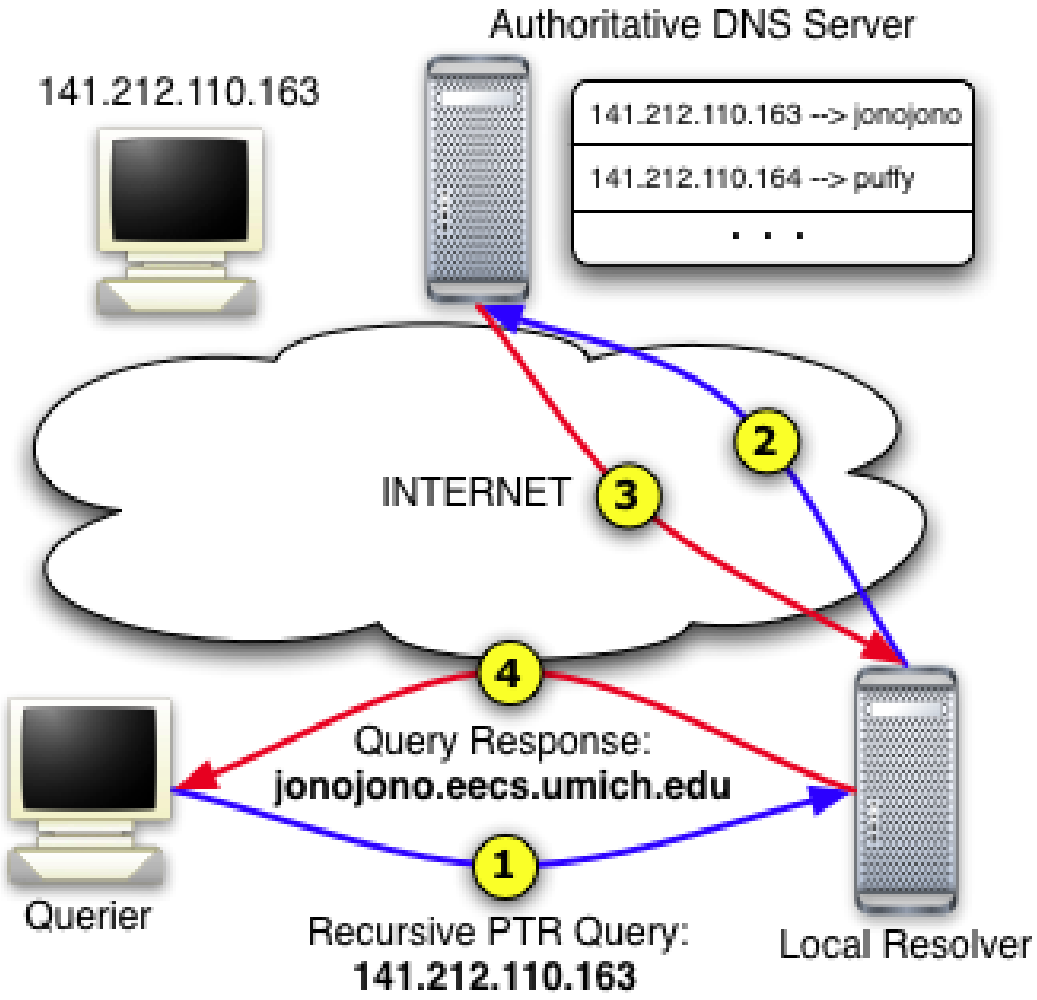
- Researcher's goals:
  - Gather threat intelligence
  - Avoid sensor fingerprinting
  - Maintain attack visibility

- Attacker's goals:
  - Evade monitored address space
    - Avoid tripping IDS alerts
    - Conceal attack techniques
  - Attack live, high-value targets

DNS Reconnaissance

- The Domain Name System (DNS)
  - Provides lucrative characteristics
    - Extensive source of information
    - Recursive queries -> ***Source cloaking***
    - Authoritative servers -> ***Out-of-band queries***
- DNS PTR queries
  - Translate IP address to hostname
  - Potential for large-scale reconnaissance
    - Live targets likely to have associated hostnames
    - Scanning target range with mass PTR querying

PTR Query Example

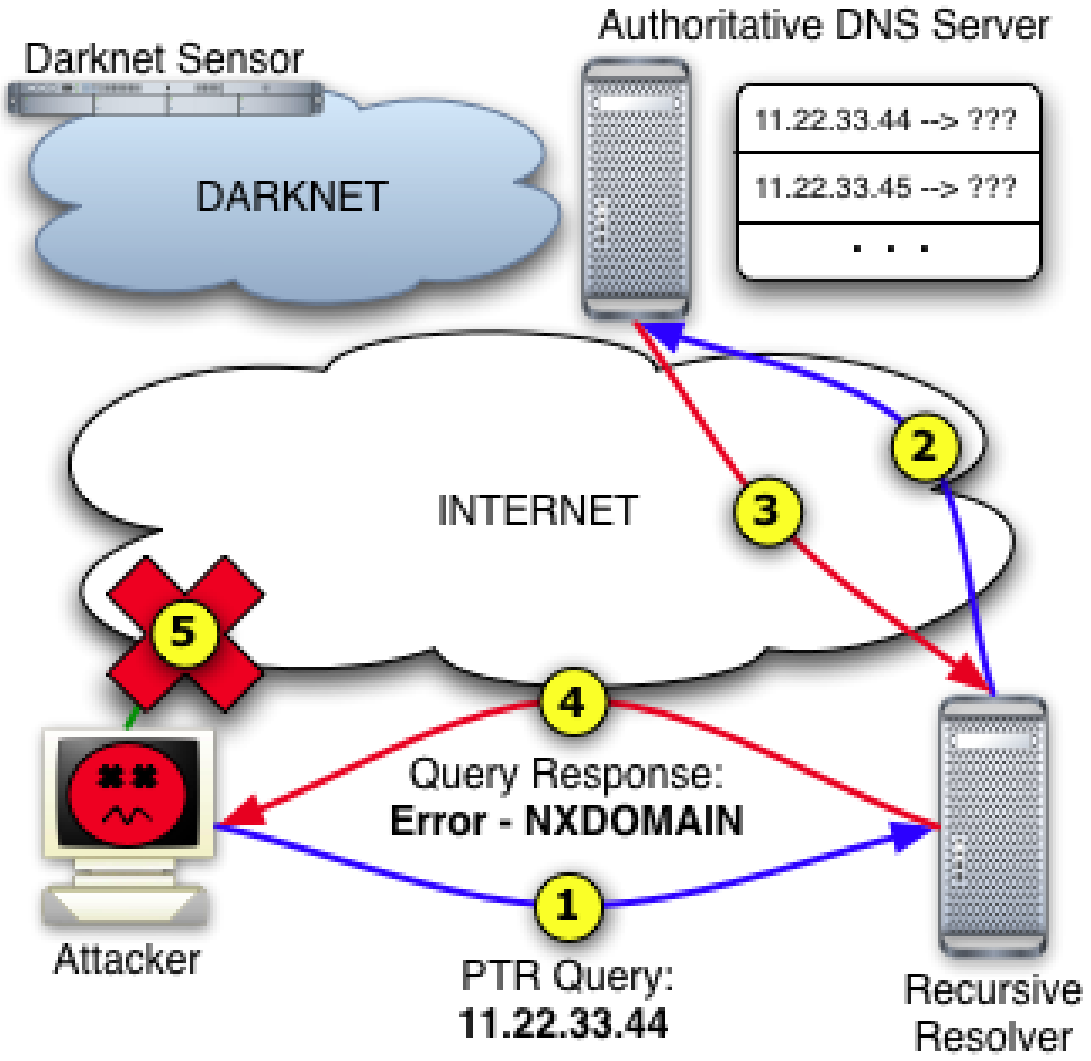


PTR Reconnaissance Feasibility

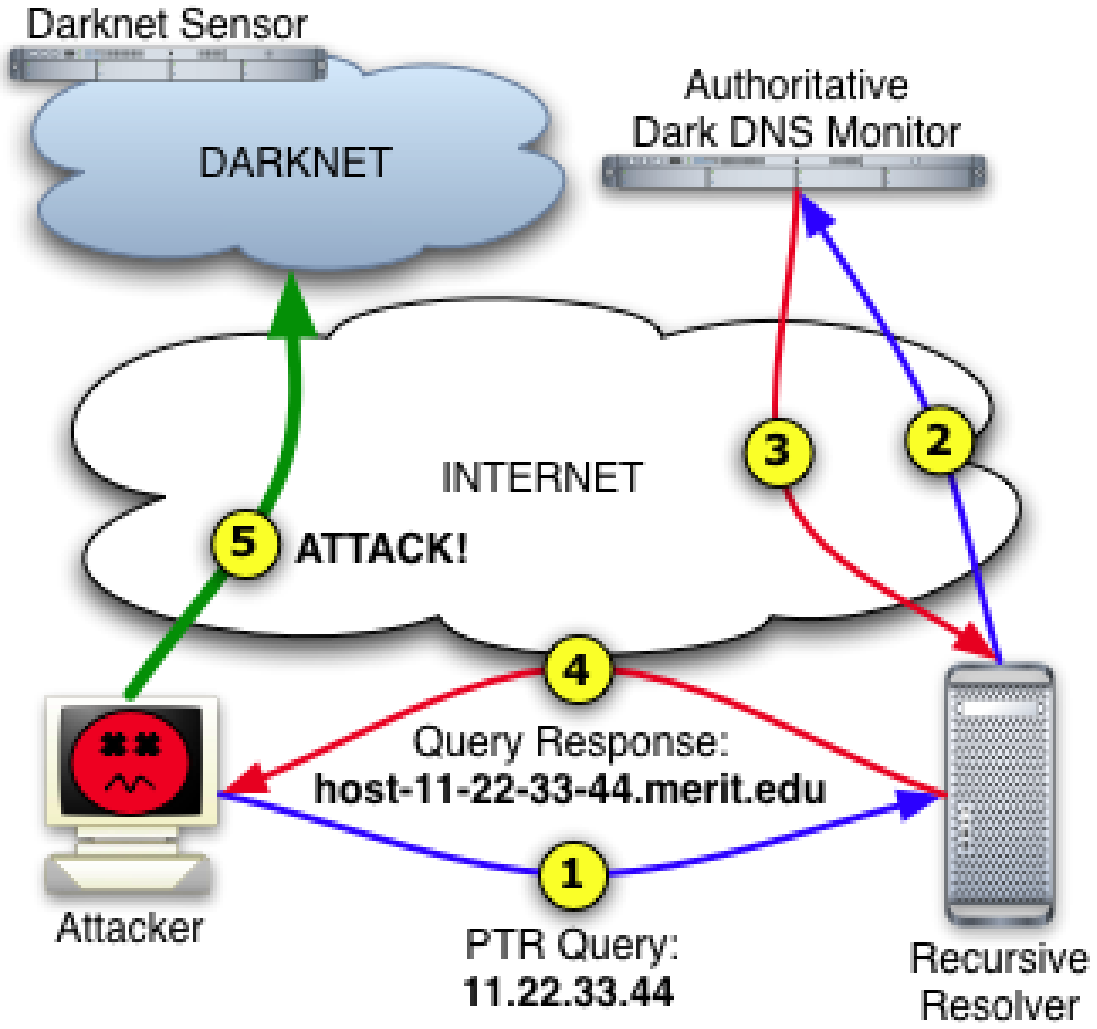
- Sensors frequently improperly deployed
  - Lacking proper reverse DNS delegation
  - Ex: large-scale, distributed darknet sensor system
    - >17 million routable addresses
    - PTR recon evaded **99.9985%** of address space
- Distribution of legitimate hosts with PTRs
  - 24 hours of NetFlow from regional provider
  - ~1.2 million unique IPs involved in TCP flows
    - ~981k have valid PTR records **(79.43%)**

PTR reconnaissance is feasible

Improperly Delegated



Properly Delegated



Dark DNS

Current darknet sensors:

Only analyze traffic targeted ***at*** monitored addresses and fail to consider OOB probes ***about*** addresses.

Dark DNS:

Inquiries ***about*** dark address space via PTR queries performed in the DNS namespace.

Goals:

- Explore characteristics of dark DNS activity collected via authoritative monitoring infrastructure
- Improve ability of sensors to prevent PTR reconnaissance via lightweight honeydns tool

Measurement Datasets

- Delegated reverse authority for two class B darknets
  - Monitored and collected dark DNS activity
- 3 Response Types
  - No Response (NR) – baseline
  - NXDOMAIN (NX) – non-existent domain
  - Valid Response (VR) – spoofed PTR reply
    - *host-a-b-c-d.merit.edu* for IP address a.b.c.d
- Collection Period
  - Week of collection for each darknet and response type

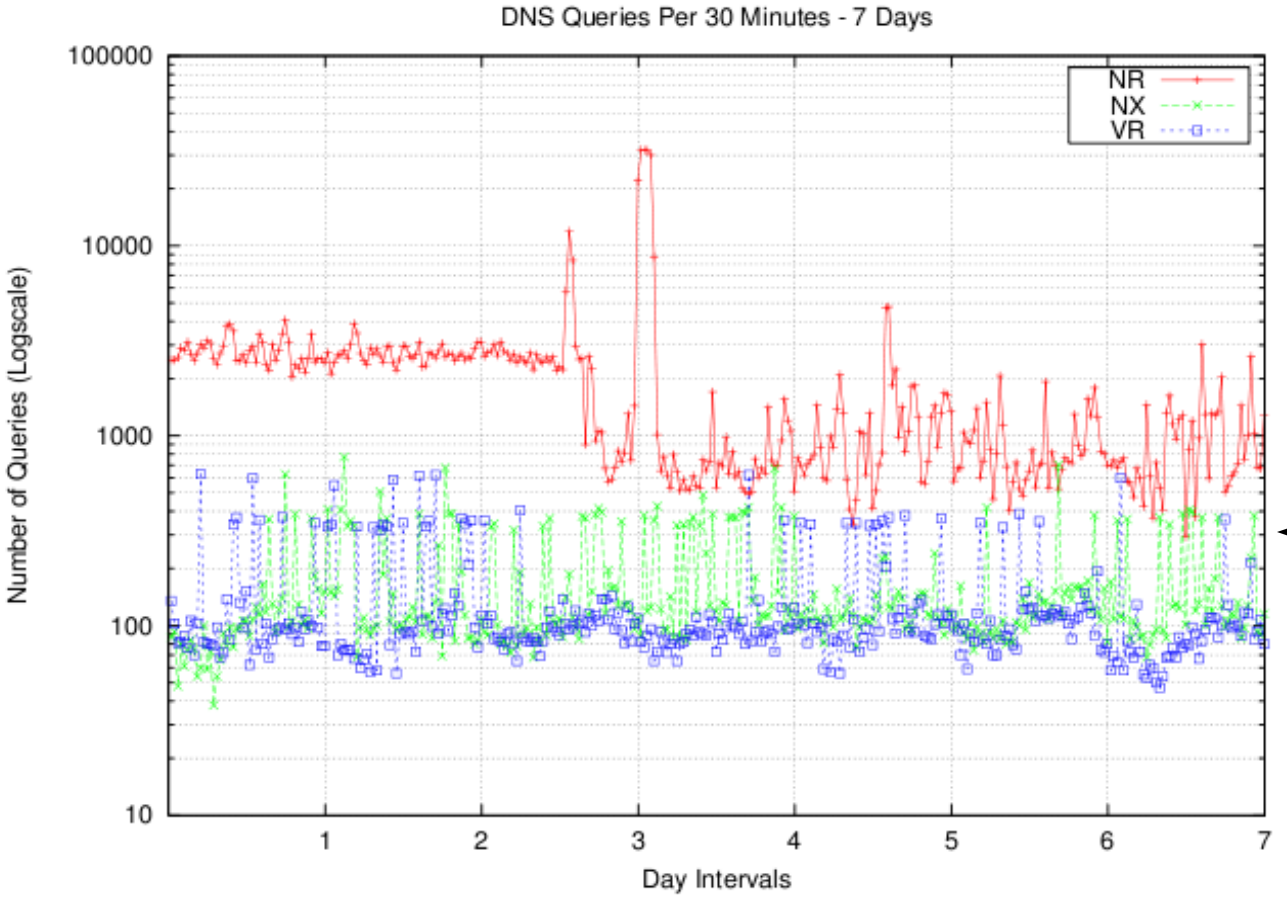
Dataset Characteristics

Dataset	Queries	Unique Sources	Unique Targets	Avg Query Rate	Max Query Rate
NR_A	714K	11.2K	64.1K	353.70	5501
NR_B	606K	11.8K	52.2K	300.34	2725
NR_Total	1.32M	17.0K	116K	654.8	5553
NX_A	57K	8.59K	28.9K	27.56	552
NX_B	58K	9.09K	29.4K	28.79	560
NX_Total	115K	13.1K	58.4K	57.1	825
VR_A	45K	7.45K	24.2K	22.35	321
VR_B	-	-	-	-	-
VR_Total	45K	7.45K	24.2K	22.35	321

- Categories of dark DNS
  - Misconfiguration
  - DDoS backscatter
  - “Legitimate” PTR mapping
  - Malicious reconnaissance

Query Code	Query Type	Count	Percentage
1	A	81	0.0704%
6	SOA	683	0.5937%
12	PTR	114214	99.2846%
15	MX	4	0.0035%
33	SRV	32	0.0278%
255	ANY	23	0.0199%

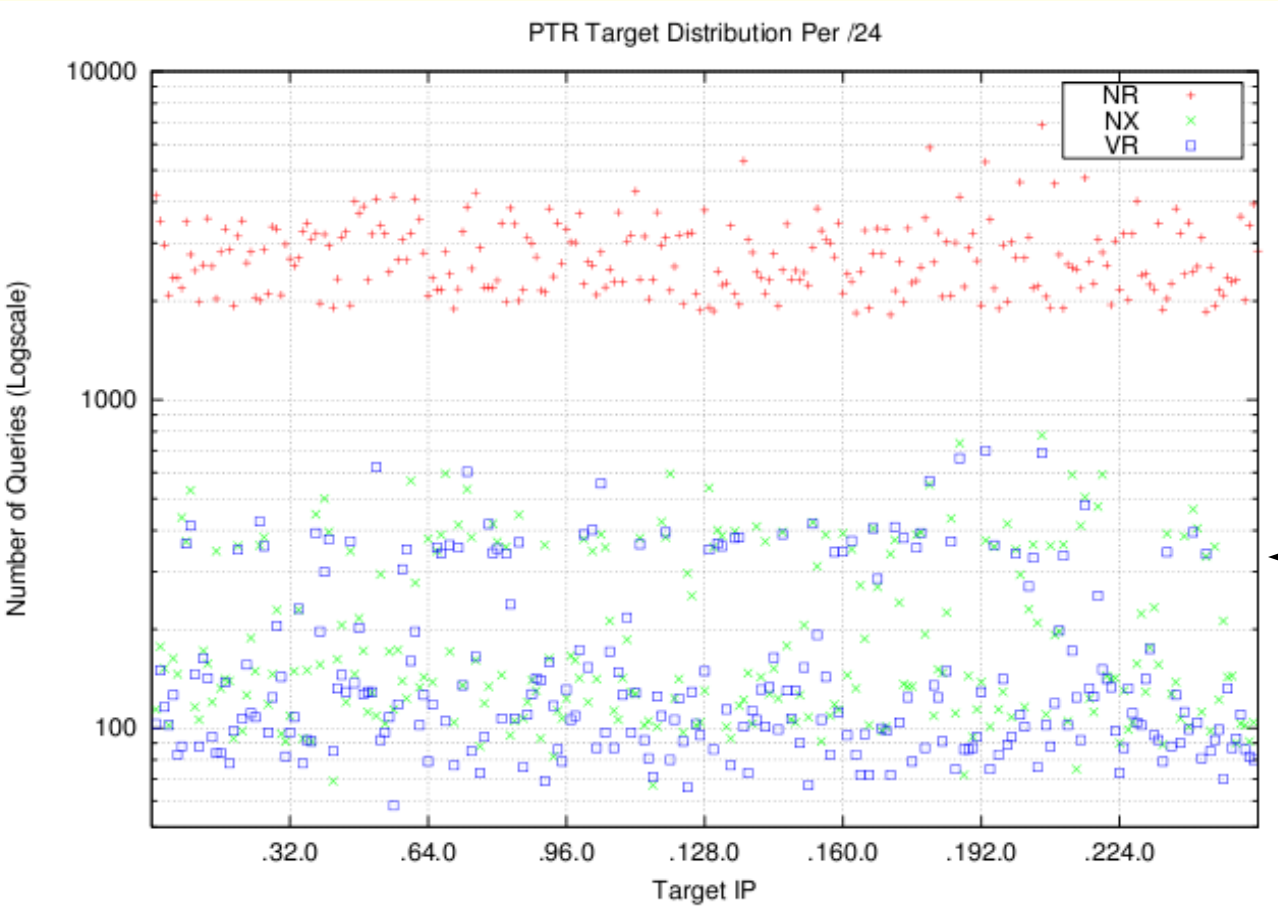
Query Rate



mini-spikes

Consistent flow of dark DNS activity

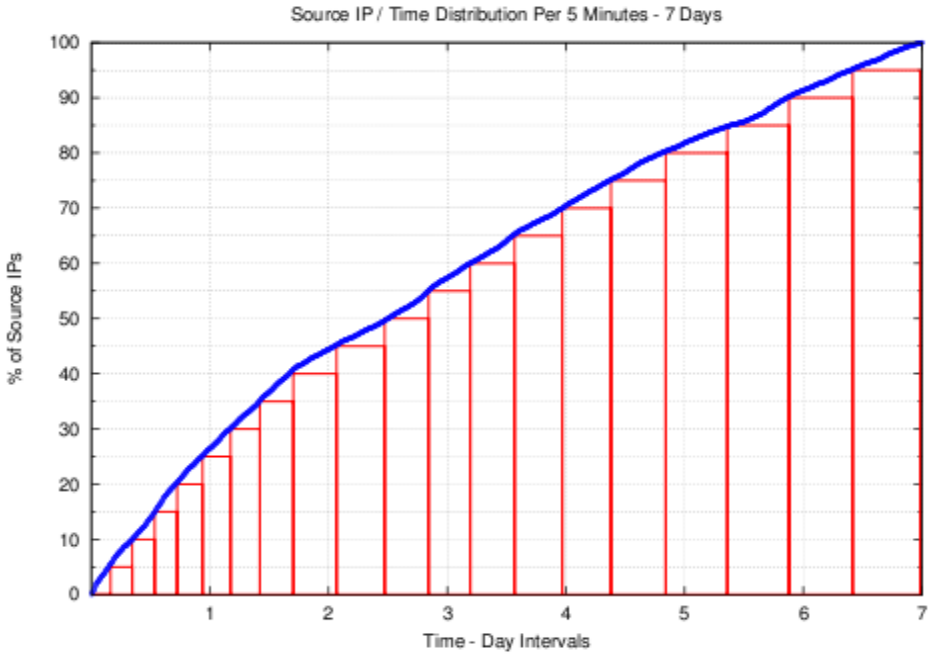
Query Targets

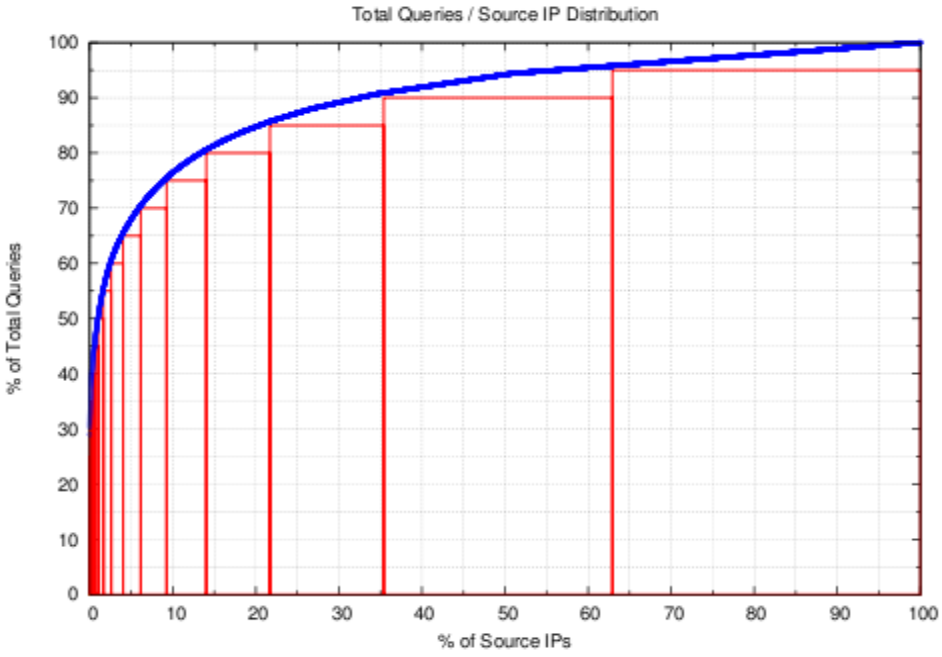


mini-spikes

Query targets evenly distributed across subnet

Query Sources





New query sources continually observed

10% hosts -> 75% queries
50% hosts -> 95% queries

Query Sources

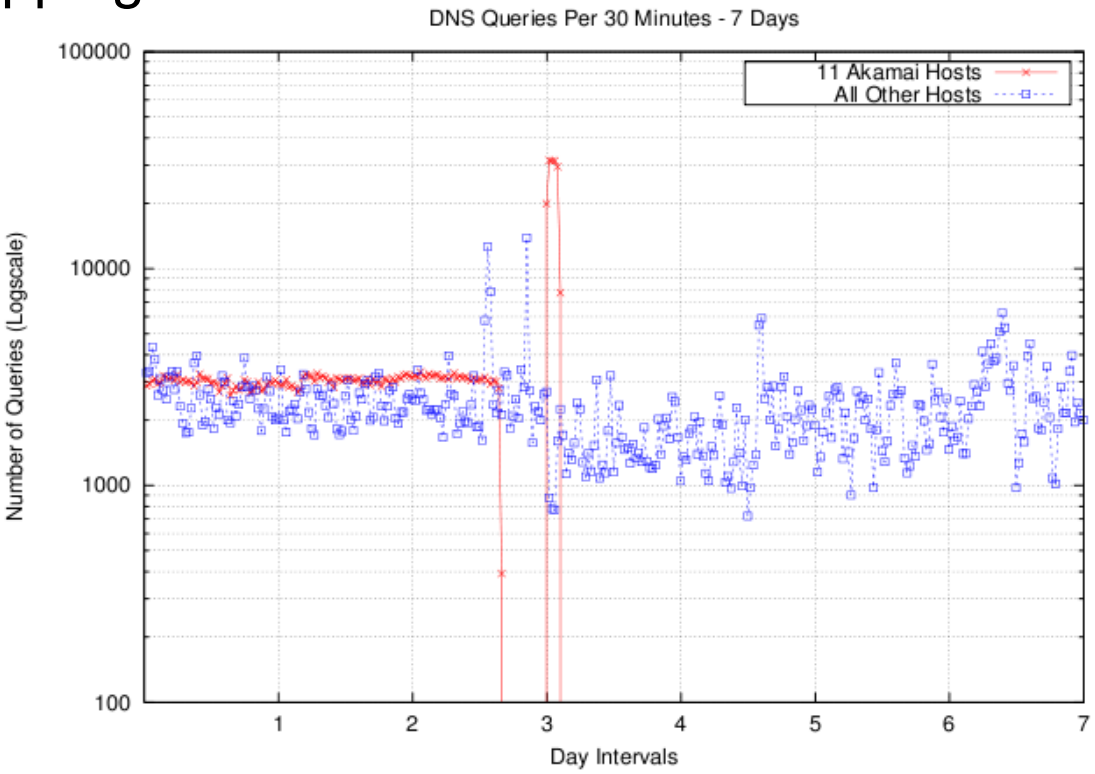
Rank	Source IP	Percentage
1	69.15.35.X	29.0315%
2	156.45.232.X	1.2431%
3	24.93.41.X	0.5537%
4	65.24.7.X	0.4198%
5	200.169.8.X	0.4172%
6	24.92.226.X	0.4085%
7	212.27.54.X	0.3833%
8	212.27.54.X	0.3712%
9	24.25.5.X	0.3694%
10	216.219.254.X	0.3659%

Operating System	Initial TTL	Unique Sources	Percentage
Linux/BSD	64	10480	72.93%
Windows	128	1043	7.26%
Solaris/Other	255	2846	19.81%

Rank	Unique Sources (% of total)	ASN	Name
1	594 (4.5%)	AS7132	SBIS-AS - SBC Internet Service
2	268 (2.0%)	AS3320	DTAG Deutsche Telekom AG
3	214 (1.6%)	AS7018	ATT-INTERNET4 - AT&T WorldNet
4	204 (1.5%)	AS6128	CABLE-NET-1 - Cablevision Systems
5	202 (1.5%)	AS4230	Embratel Brazil
6	194 (1.4%)	AS5617	TPNET Polish Telecom commerce
7	192 (1.4%)	AS209	ASN-QWEST - Qwest
8	190 (1.4%)	AS5089	NTL NTL Group Limited
9	174 (1.3%)	AS21844	THEPLANET-AS - THE PLANET
10	164 (1.2%)	AS577	BACOM - Bell Canada

Akamai Mapping

- 11 distinct, distributed Akamai-deployed hosts
  - Large source of PTR queries
  - Network locality mapping
- Anomalous event
  - Steady (~100/min)
  - Crash (0/min)
  - Spike (~1000/min)
  - Crash (0/min)



Discussion

- Measurements results
  - Significant amount of dark DNS traffic observed
    - Large number of originating networks/hosts
  - Verified mapping and scanning activity
  - Non-trivial random background activity
    - Difficult to track and classify
- Return to reconnaissance issue
  - How to prevent attackers from evading darknet sensors using PTR queries?

Honeydns

- Honeydns tool
  - Lightweight, flexible python daemon
  - Simple authoritative DNS response functionality
    - BIND unnecessarily complex for subset of required functionality
- Complementary to darknet deployments to prevent PTR reconnaissance
  - Includes rudimentary alerting for scan detection
  - Extensible for dynamic honeynet topologies and sampling

Future Work

- Extent of reconnaissance by attackers
  - Complicated discrimination between categories
    - Mapping, backscatter, misconfigured, malicious activity
  - Correlation of dark DNS with attack traffic
    - Difficult due to recursive queries, source cloaking
    - Amplified by availability of open resolvers

Questions

QUESTIONS???