Passive DNS

A Tool that is Making a Difference in Tracking Down Criminal Activity On The Internet

Merike Kaeo
merike@isc.org
Passive DNS – What Is It?

• Passive DNS replication is a technology invented in 2004 by Florian Weimer
• Inter-server DNS messages are captured by sensors and forwarded to a collection point for analysis
• After being processed, individual DNS records are stored in a database where they can be indexed and queried
Questions that can be answered using a Passive DNS Database

• Where did this domain name point to in the past?
• What domain names are hosted by a given nameserver?
• What domain names point into a given IP network?
• What subdomains exist below a certain domain name?
Passive DNS – Tool to Find the Badness
End User & Operator Privacy Protected

Client 1

O1: www.isc.org./A
R1: www.isc.org./A

Q2: www.isc.org./A
R2: org./NS

Q3: www.isc.org./A
R3: isc.org./NS

Q4: www.isc.org./A
R4: www.isc.org./A

RD=0

Content 1 (Root)

Content 2 (org)

Content 3 (isc.org)

Sensor

Q2,R2,Q3,R3,Q4,R4

SIE

Not Collected

Collected
ISC DNSDB UI

Internet Systems Consortium

DNSDB Search

Search mode:  RRset  Rdata
Record type:  ANY
Domain name:  
TLD:  

Search  Reset

© 2010 Internet Systems Consortium, Inc.
Contact us by sending email to info@sie.isc.org.
Who Gets DNSDB Access?

• Two Types of Access
  - DNSDB User Interface
  - DNSDB API

• Who Gets Access
  - Vetted Member of the Operational Security Community
  - Passive DNS Contributors
  - SIE Peers
Participation

• Add a Passive DNS sensors to your DNS infrastructure
  - Only recursive DNS replies from authoritative servers are of interest
  - All data is aggregated, obscuring the source
• Participants get access to the aggregate data for your own investigations
• Contributing to ISC’s Passive DNS
  - Send email to passivedns@isc.org
• Applying for DNSDB access
  - https://dnsdb.isc.org
Questions?