Join The Global Passive DNS (pDNS) Network Today & Gain Effective Tools To Fight Against Cyber Crime

Why contribute passive DNS data to ISC?

ISC - *the Public Benefit Company that works to sustain the spirit of the Internet* - is expanding the capacity of our ***Passive DNS System***. Passive DNS provides the industry greater insight into how the cyber-criminals are using DNS to violate the Internet.

Vetted organizations are invited to join the pDNS network by configuring their DNS infrastructure to be a passive DNS sensor (pDNS). Once you join, your system becomes a part of the global pDNS network, helping to fight against cybercrime, and gaining your team access to effective DNS visibility tools.

Passive DNS is a very scalable network design and has minimal operational impact. ***As an additional bonus for participating, all vetted organizations that contribute Passive DNS will have access to the DNS Database (DNSDB) at the ISC Security Information Exchange (SIE)*** – an investigative tool that we use to analyze the cyber-criminal's use of DNS. By participating in this effort, you are expanding the data collected, thereby enabling greater insights into how the cyber-criminals are using DNS to exploit the Internet.

Passive DNS

"Passive DNS" or "passive DNS replication" is a technique invented by Florian Weimer in 2004 to opportunistically reconstruct a partial view of the data available in the global Domain Name System into a central database where it can be indexed and queried.

Passive DNS databases are extremely useful for a variety of purposes. Malware and e-crime rely heavily on the DNS, and so-called "fast flux botnets" abuse the DNS with frequent updates and low TTLs. Passive DNS databases can answer questions that are difficult or impossible to answer with the standard DNS protocol, such as:

- *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?*

Joining the network by operating a passive DNS sensor is an effective and easy way to contribute to the global online anti-abuse effort. The data is 'aggregated', thus not linkable to the specific devices making the query.

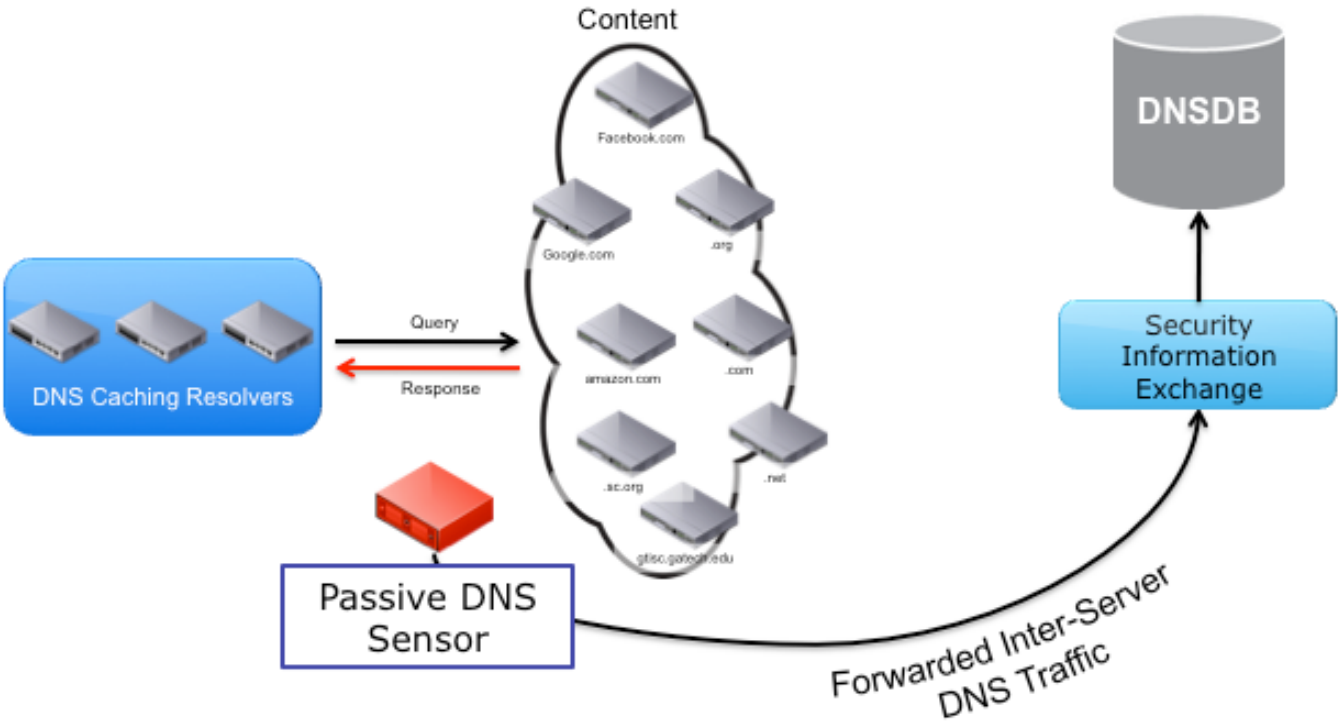

Figure 1 - Passive DNS Sensor placed between the DNS Resolvers and DNS Authoritative Servers

Passive DNS Data Collection

Passive DNS only replicates the inter-server traffic between caching recursive nameservers and authoritative nameservers. Data capture only occurs when a recursive DNS cache experiences a cache miss and must query in order to obtain needed data.

Passive DNS replication is inherently both ***efficient*** and ***privacy preserving***. Only a small portion of the network traffic generated by a DNS server needs to be captured and backhauled. This is more efficient than the traditional "DNS logging". No client IP addresses are ever captured in the data requested by the recursive DNS cache. The lack of the client IP addresses preserves privacy. In addition, the

DNS cache data is reused. Large, busy DNS caches are thus naturally very effective at protecting the privacy of individual users.

ISC has produced an easy to install passive DNS sensor program, which can be installed directly on either production DNS servers or a monitoring server connected to a "tap" or "SPAN" port. The sensor uses libpcap to collect the upstream packets generated by the recursive DNS server and then periodically uploads the data in compressed form to collection servers operated by ISC's Security Information Exchange (SIE) project. Extremely busy DNS servers typically produce only 1-5 megabytes of data per minute.

DNS Database (DNSDB)

Passive DNS data is uploaded into the SIE network, where it is distributed to vetted security researchers that maintain contractual relationships with SIE that prohibit unauthorized redistribution. ISC has invested a considerable amount of resources into analyzing and aggregating the large volumes of passive DNS data submitted to SIE. One of the results of this effort is the ISC Passive DNS Database (DNSDB), a database cluster that stores unique DNS records witnessed in the passive DNS data.

In exchange for providing passive DNS data to the ISC DNSDB project, vetted operators of passive DNS sensors are entitled to no-fee access to ISC DNSDB's easy-to-use web search interface.

As can be seen in figure 2, DNSDB provides insight to criminal activity. Using a domain from SPAM E-mail, DNSDB can trace the DNS activity to uncover associated domains which have been or will be used for future SPAM.

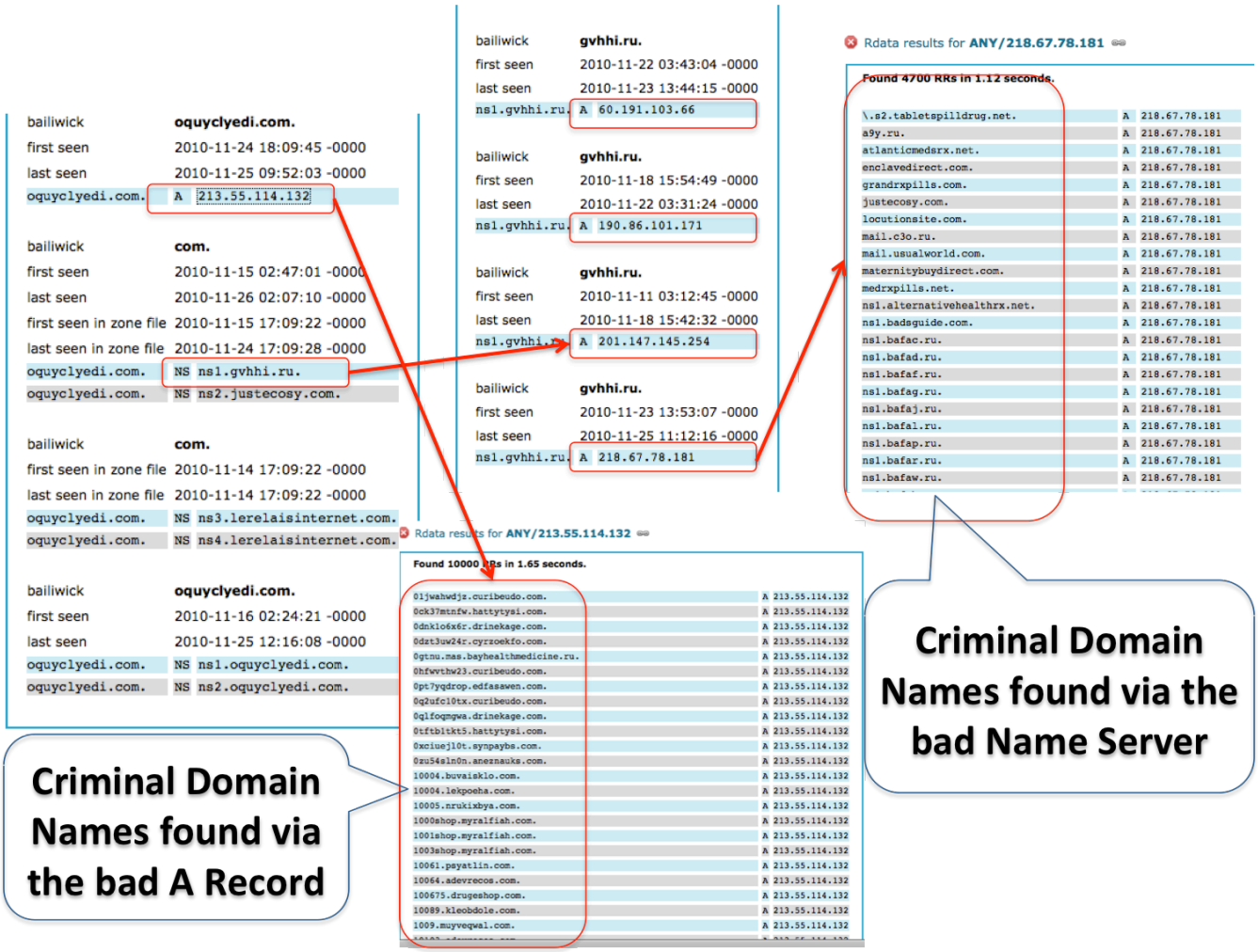

Figure 2 - Using DNSDB to track down criminal infrastructure.

How to Participate?

If you are interested in joining and operating a passive DNS sensor on behalf of ISC or have questions that are not answered by this document, please send email to <**info@sie.isc.org**>.

Further Passive DNS Reading

The ISC SIE website: https://sie.isc.org/

The ISC DNSDB website: https://dnsdb.isc.org/

SIE DNS sensor packages:

Red Hat / CentOS and Debian:
ftp://ftp.isc.org/isc/nmsg/misc/sie-dns-sensor/

FreeBSD:
ftp://ftp.isc.org/isc/nmsg/misc/sie-scripts-0.14.tar.gz

Papers and Materials:

Robert Edmonds's Defcon 18 slides:
http://users.isc.org/~edmonds/passive_dns_hardening_handout.pdf

Florian Weimer's original paper:
http://www.enyo.de/fw/software/dnslogger/first2005-paper.pdf

The Internet Systems Consortium

Internet Systems Consortium, Inc. (ISC) is a non-profit 501(c)(3) public benefit corporation dedicated to supporting the infrastructure of the universal connected self-organizing Internet—and the autonomy of its participants—by developing and maintaining core production quality software, protocols, and operations.

ISC is proud to be the producer and distributor of commercial quality Open Source software for the Internet Community and to offer world-class online and professional services based on our software. Since 1996 ISC has led the industry with the most complete reference standard implementation of DNS (BIND) software using a Managed Open Source model. ISC also provides production-quality reference implementations for other core protocols such as DHCP, and distributes other open source software.

All of our open source software is available for free download from our website, since it is free, the Software Forum is a membership program for users and integrators of ISC's software or sponsored projects. ISC depends on annual membership fees to provide funding for ongoing software maintenance, enhancement and publication.

ISC also provides a number of Operational Programs and Services that benefit users of the Internet directly and indirectly. Since 1994, ISC has operated F-Root (one of the 13 root DNS servers) as a public service to the Internet.