

REN-ISAC Passive DNS Data Collection - Background

Created by Doug Pearson (admin acct) just a moment ago



TLP: GREEN / REN-ISAC: LIMITED

The information on this page may be shared within your organization; however the information may not be published or posted publicly.

- [Summary](#)
- [DNS background](#)
- [What is passive DNS data?](#)
- [Passive DNS information is important for security operations](#)
- [What are the data sensitivity concerns? Does pDNS data link persons to the requests they make?](#)
- [How is the pDNS data collected?](#)
- [How is the REN-ISAC pDNS data shared?](#)
- [What is the value of being a contributor?](#)
- [Who do I contact to learn more or to become a contributor?](#)
- [Referenced resources](#)

Summary

DNS request and response data is collected at recursive resolving DNS servers of participating REN-ISAC members. The aggregate data, stripped of sensitivity concerns, is contributed to global collection and analysis projects operated by REN-ISAC trusted partners, such as Farsight Security's DNSDB. REN-ISAC members gain query access to processed pDNS data, improving their security protection and incident response capabilities. Global collections benefit through the improved quantity and quality of data made available.

DNS background

The Domain Name System (DNS) is a fundamental protocol of the Internet. Whenever any Internet resource, such as a web site, mail system, or Internet-connected refrigerator, is accessed by name, the name must be translated to a numeric Internet Protocol (IP) address. Under the covers, all Internet connections are IP address-to-IP address. A couple reasons for this name and number relationship are that names are much easier for most people to remember, and names stay the same while the underlying network numbers may change. DNS is the service that translates names to numbers. For example, when you visit the REN-ISAC web site www.ren-isac.net, that name must be translated to the current (as of this writing) IP address 129.79.214.150.

DNS involves:

- "clients" that make requests on behalf of users,
- "recursive resolving servers" that act on requests from clients (such as your web browser) for a domain name resolution ("what is the IP address associated to domain name X?"),
- "authoritative servers" that have the authoritative mapping of names to numbers, and
- protocols to interrelate all of that into a global system.

Authoritative servers have mappings only for the domains owned or operated by the organization running the authoritative server. Organizations operate their own server infrastructure (resolving and authoritative) or contract with a 3rd party to manage that for them. For example, Indiana University (IU) operates its own recursive resolving and authoritative DNS servers. The IU resolving server(s) respond to requests by clients (users) within the IU network. The IU authoritative servers are authoritative for all the domains that IU owns and operates (e.g. indiana.edu, iu.edu, iusb.edu, iuk.edu, ren-isac.net, etc.)

Recursive resolving servers resolve client requests by contacting the appropriate authoritative server. Recursive resolving servers usually cache answers, time-limited by a "time-to-live" (TTL) provided in the response from the authoritative server. Caching cuts down repeated requests from recursive to authoritative servers for the same name, and the TTL prevents information from persisting longer than desired, to accommodate network change.

The global DNS system makes it possible for clients relying a specific resolving server to get authoritative answers concerning any Internet resource anywhere in the world.

What is passive DNS data?

Passive DNS data (pDNS) is a collection of DNS request and response datagrams exchanged by recursive resolving DNS servers and authoritative DNS servers. The data **DOES NOT INCLUDE** datagrams exchanged between a client (user) and a resolving server. A request/response pair contains the domain name a resolution request was issued for and the IP address identified for the name. pDNS data can be collected and combined from recursive servers across many organizations and combined into an analytic resource.

Passive DNS information is important for security operations

Malware, phishing, botnets, all kinds of malicious Internet activity use domain names. Passive DNS data is extremely valuable for:

- developing threat indicators that can be applied in local security protections,
- identifying security incidents and compromised systems, e.g. malicious domains that point into your IP address space
- informing actions for incident response, and
- for global security and law enforcement teams to identify malicious infrastructure (servers, networks, botnets, etc.)

What are the data sensitivity concerns? Does pDNS data link persons to the requests they make?

There are no sensitivity considerations of note.

No personally identifiable information or otherwise sensitive information is collected. Data is collected between the contributing organization's recursive resolving DNS server(s) and external Internet authoritative servers. There is no information linking a person to a resolution request.

In the default REN-ISAC sensor configuration collected data contains the IP address of the organization's recursive resolving server as the source of a request. If that revelation is not desired, a mode can be implemented which clears the address in captured packets. By clearing the address no value is lost for global concerns; however, one order of (many) benefits to the data-contributing organization is lost wherein the organization would no longer be able to query "did a system at my site attempt to connect to <a specific> malicious site". Clearing the address is at the discretion of the contributing organization and is accomplished via local sensor configuration.

Depending on the contributing organization's DNS architecture, the sensor may see resolution requests for local domain names in addition to the desired collection of requests for external names. If the revelation of queries for local domains is not desired, that can be accomplished through local sensor configuration.

How is the pDNS data collected?

A sensor, comprised of a modest Linux server and Farsight Security, Inc's [1] sensor software, is installed and operated by the contributing organization. The sensor software is open-source, permitting inspection and privacy validation by the global security community. The sensor is given a view of DNS network traffic (port 53 UDP & TCP) at the resolving server, typically via a network span port. The sensor collects (ONLY) requests made by the resolving server to authoritative servers and the corresponding replies. The sensor sends collected data to a REN-ISAC channel on the Farsight Security Information Exchange [2].

How is the REN-ISAC pDNS data shared?

REN-ISAC shares the collected data with Farsight Security, Inc. and with other select REN-ISAC trusted partners operating under a security information sharing agreement. Farsight distributes data to vetted security researchers that maintain a contractual relationship with SIE prohibiting unauthorized redistribution, and with customers of its DNSDB service, under similar restriction.

What is the value of being a contributor?

Passive DNS data is an extremely valuable security protection and response resource, as described above. The REN-ISAC-led effort creates the conditions for REN-ISAC members to directly benefit from global collections, improves those collections by our contributions, and opens the door for REN-ISAC access to other security intelligence resources shared in partnerships.

Who do I contact to learn more or to become a contributor?

soc@ren-isac.net

Referenced resources

[1] About Farsight Security

<https://www.farsightsecurity.com/About/>

[2] Farsight Security Information Exchange (SIE)

<https://www.farsightsecurity.com/Overview/SIE/>

Additional resources

Farsight Passive DNS Sensor FAQ

https://archive.farsightsecurity.com/Passive_DNS_Sensor_FAQ/

Privacy Considerations for ISC Passive DNS

<https://archive.farsightsecurity.com/Passive-DNS-Privacy.pdf>

Passive DNS: improving security and privacy

article by Andrew Cormack, Chief Regulatory Adviser at JANET(UK)


<https://community.jisc.ac.uk/blogs/regulatory-developments/article/passive-dns-improving-security-and-privacy>

Practical Usage of Passive DNS Monitoring for E-Crime Investigations

<http://conferences.npl.co.uk/satin/presentations/satin2011slides-Rasmussen.pdf>

EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis

http://www.cs.ucsb.edu/~chris/research/doc/ndss11_exposure.pdf

 Like Be the first to like this

No labels

Powered by a free **Atlassian Confluence Community License**
granted to REN-ISAC. Evaluate Confluence today.