FACTSHEET

Passive DNS: Trusted real-time threat intelligence from Deteque

Passive DNS allows you to uncover patterns of malicious activity from networks across the world. Global threat data that's a powerful boost to your SIEM and security analysis.

What it is

Passive DNS is a constantly updated dataset showing in real-time which host names have been resolving to which IP addresses, and when. Single data points with this essential information are combined from different information suppliers around the world, giving you the power to build a picture of potential threats across global networks that cannot be seen from monitoring a single network.

Using the combined data from Deteque's global network of Passive DNS data collectors, you can reveal patterns in DNS resolution showing the pathways used by cyber criminals to operate malicious domains used for spamming, phishing and malware insertion including ransomware.

How it works

Subscribers can query the Passive DNS database via Deteque's API to see domains and IP addresses which are suspects in Security & Incident Event Management (SIEM) investigations. The data sets produced from a query can be further analyzed by users' own tools to show whether these domains/IP addresses exhibit unusual behavior or are associated with suspicious activity.

In the case of domains, this could include recently registered domains that show a sudden burst of activity, or host names which switch between IP addresses or IP addresses that frequently switch associated host names.

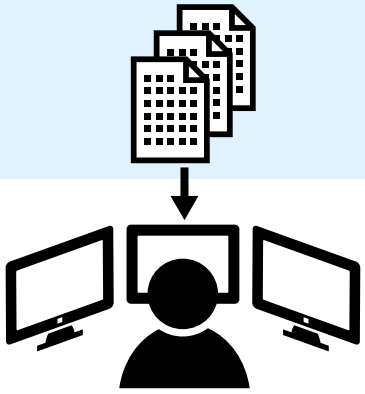
Studying Passive DNS data allows researchers to track which domain names are hosted by particular name servers. They can also see where domain names previously pointed and which subdomains exist below a certain domain name.

Deteque users can also receive data as a constant data feed, for continuous integration into existing SIEM and analytics tools and their own proprietary products.

Sample data point received by Deteque

Hostname: www.example.com
Resolves to: `IP 93.184.216.34`
When: Time and date
First seen: Time and date

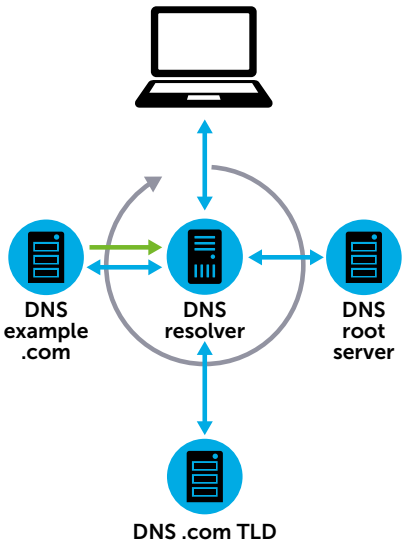
Data points collated from contributors around the world and de-duplicated



Refined data available as real-time intelligence, by querying or as a continuous data feed, for your research

Privacy and compliance

Data received from subscribers contains no Personally Identifiable Information (PII) so you can be sure that working with Deteque won't compromise your organization, customers or employees. All data is transported to Deteque with encryption in place and once processed on our side immediately deleted.



A client queries a local DNS resolver and if the IP address for that domain is not included in its cache, it will query in turn an external root server, the Top Level Domain server and the name server itself to get access to the site.

Client gets a match for domain/IP address and the result of only the recursive segment is automatically sent to Deteque. We do not see who made the query.

Global intelligence to secure your organization

Passive DNS empowers your research, enabling you to make active decisions to protect your organization including blocking certain domains from connecting to your network and evaluating risks associated with your hosting environment.

Use Passive DNS to:

- Reveal the health of your hosting network by discovering what other domains and organizations are associated with the IP blocks and name servers used by your hosting provider.
- Investigate suspicious domains by revealing their history and IP address associations
- Analyze lookalike domains to evaluate their threat potential.
- Detect infringement of your copyright and brands by lookalike and spoofed domains.
- Incorporate Deteque datasets into your own automated and reputation-based tools.

Choosing the Passive DNS that's right for you

User type	Type of use	How to obtain
Information security professionals and cyber incident response analysts	Digital forensics and investigation of activity of specific IP ranges, or analysis of the relationships between DNS queries and responses	Web portal
SOC/SIEM teams, security vendors and expert users	Multiple, frequent queries and integration of raw datasets into software and security platforms	Query via API
Large enterprises, security researchers and law enforcement agencies	Continuously monitoring live recursive DNS traffic to aid the identification of new malicious domains, emerging threats or cybercriminal trends	Continuous data feed

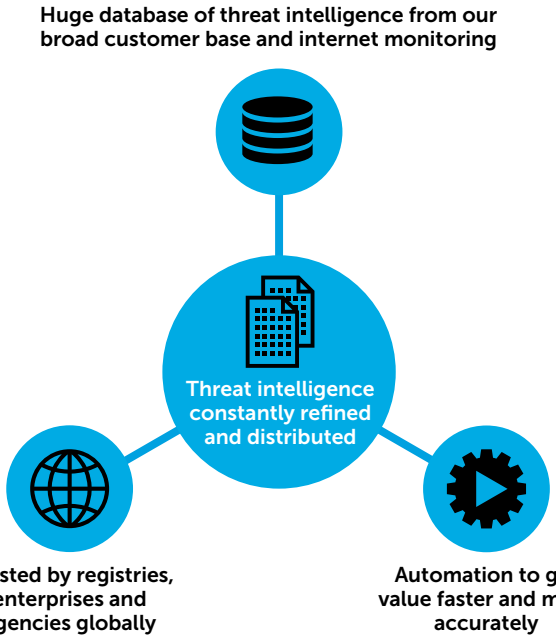
About Deteque

Deteque is a division of Spamhaus and integrated with a global network of service providers and a community of security researchers who are dedicated to combating DNS abuse. Since 2008, Deteque has been at the forefront of securing networks by collecting, collating and delivering DNS-related threat intelligence to protect organizations in real-time. In addition to Passive DNS, Deteque also collates and delivers Response Policy Zones (RPZ) threat intelligence to block malicious domains and IPs used by cyber criminals to steal data, carry out fraud and exploit legitimate systems.

A division of Spamhaus

Spamhaus works as a trusted third party where a variety of networks and organizations from all over the world contribute data that helps protect everyone.

This model sees Spamhaus currently protecting three billion user mailboxes, blocking the vast majority of spam and malware sent on the Internet. Spamhaus data is used by the majority of the Internet's ISPs, email service providers, corporations, universities, governments and military networks.



Follow Deteque:

@deteque-llc
@deteque
'Deteque' channel

www.deteque.com

Your contact:

deteque | A division of SPAMHAUS