turing by nominet

Decoding DNS data

Introducing...

turing by Nominet

a revolutionary new tool for analysing large volumes of internet traffic

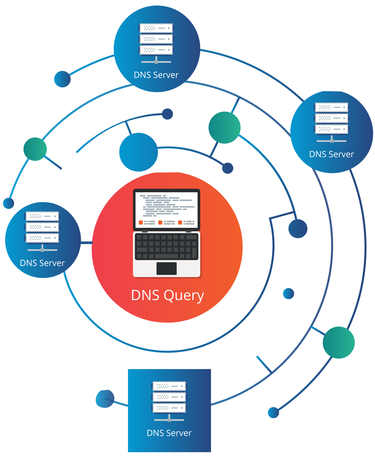
What is the Domain Name System (DNS)?

The Domain Name System (DNS) is a core component of the infrastructure of the internet. It's the equivalent of a telephone directory, storing the names of computers and their IP addresses.

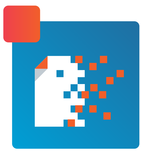
Every time someone uses a browser to look at a website or send an email, their computer generates a DNS query. The DNS translates the domain name into an IP address to find the correct computer.

The efficient operation of the DNS is crucial to any service that runs on the internet. So it makes sense for companies who manage internet infrastructure (e.g. registries, ISPs and large enterprises) to monitor the behaviour of their DNS traffic.

DNS data can be used to investigate problems, identify threats and optimise performance. Up until now, the available network management tools have not had the capability to rapidly store and anaylse DNS query data in depth.



Enter *turing*, a new breed of DNS analysis tool



Data collection at scale:

turing collects hundreds of thousands of queries per second and stores years of data.

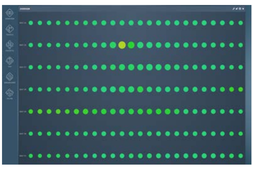
Enhanced cyber security and performance:

turing can identify botnets, sources of spam, malware index cases, man-in-the-middle attacks and network latency problems.

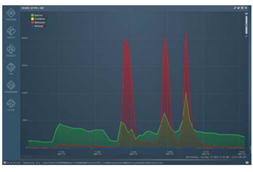
Real-time visual analysis:

turing can process terabytes of DNS traffic in seconds, rapidly summarising the data through an intuitive touch-based user interface.

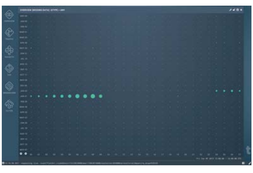
turing in action



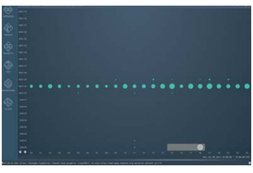
Unfiltered DNS views where each dot shows an hour's worth of traffic, colours reflect the 'health' of traffic.



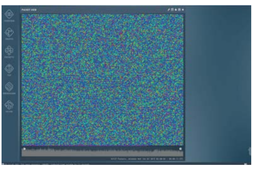
During a spam run, requests for domains that do not exist are high - this is typical of a mass mailing when the list has many invalid domains.



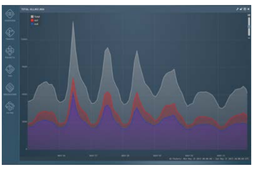
A two-year view (each dot is one day) showing a Denial-of-Service-attack (DoS) by DNS amplification.



Domain Generation Algorithms (DGA) are used by many pieces of malware and are in use for a fixed period of time, often 24 hours.



Certain aspects of a DNS query should be randomised making them hard to guess; this indicates a good, well-configured server.



One week's traffic, including a Bank Holiday, showing computers being switched on during weekdays with quieter evenings and weekend.

Find out more about *turing by Nominet* at

www.nominet.org.uk/turing

About Nominet

Domain names are one of the key building blocks of the internet – an essential component of every email address and website. Millions of businesses and consumers now depend on Nominet's services, which underpin a critical part of the UK Internet economy. Nominet is a private, not-for-profit business, responsible for the smooth and secure running of the .UK internet infrastructure. We have over 2,800 members and are committed to acting in the public interest.

With the proceeds of our successful registry business, we set up and support the Nominet Trust, an independent charitable foundation focussed on increasing access, safety and education on internet issues. As part of our commitment to making the internet a more trusted space, we have also developed an information and advice portal - www.knowthenet.org.uk - which helps internet users to get the most of being online by staying safe, legal, and informed.

nominet