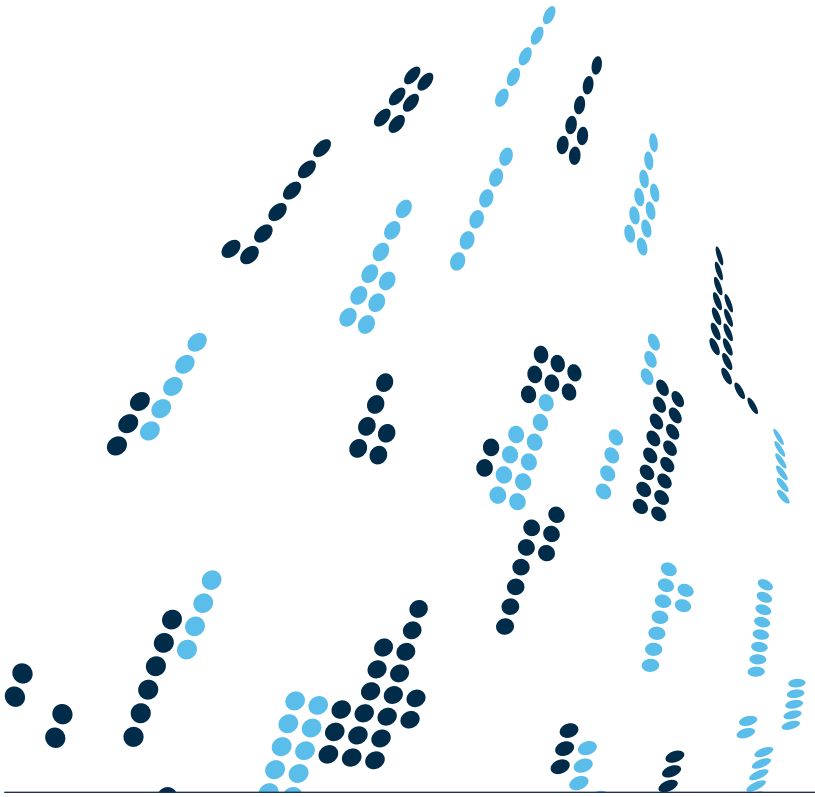
turing by NOMINET

Decoding DNS data

turing by Nominet:

decoding your DNS traffic to provide new insights and help you better manage your cyber security.



If you have a large DNS infrastructure, understanding what is happening with your real-time and historic traffic is difficult, if not impossible. Until now, the available network management tools have only been able to provide slow snapshots of a small window of the data.

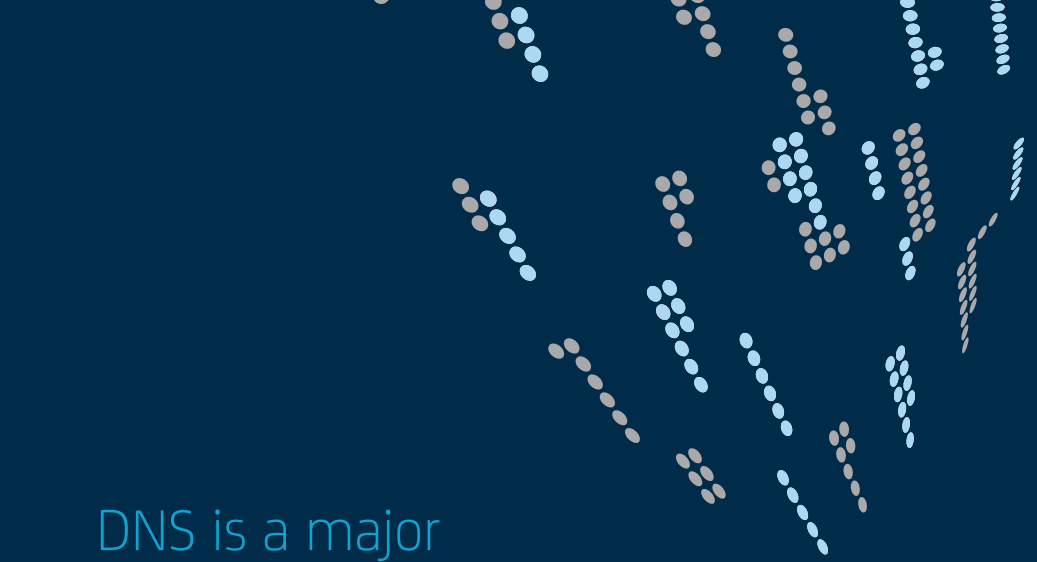
turing provides a new way of working with this data. This innovative DNS analytics and visualisation solution delivers rapid insight to identify patterns of use and cyber security problems.

Analysis of historic DNS data will help you to understand what normal traffic patterns look like and so identify any unusual activity and take action, mitigating any cyber security incidents before they have chance to embed themselves in your system.

This level of insight into what's happening on your business critical networks makes for more efficient planning, more economic live operation and more effective decisions.

With *turing* you can:

- Identify, locate and mitigate the effects of botnets or other malware abusing your infrastructure
- Locate and fix network misconfigurations
- Immediately recognise attempts to make unauthorised changes to your DNS records
- Understand your DNS traffic which can lead to improved business intelligence
- Ensure compliance with preventative security good practice, maximising availability of business-critical systems
- Collate an evidential data trail to support any legal action



DNS is a major vector of cyber attack and occurrences are on the rise as cyber criminals exploit inherent vulnerabilities within the system.

With billions of packets of data to monitor, track and analyse, identifying these attacks has historically been like finding the proverbial needle in a haystack. *turing* is a ground-breaking solution that helps turn the tables on cyber criminals by delivering near real-time analysis of all the detailed DNS traffic on your systems.

By collating DNS metadata and correlating request and response messages at the point of capture, *turing* enables you to identify, investigate and act on any unusual activity to mitigate any damage before it has chance to embed itself in your system.

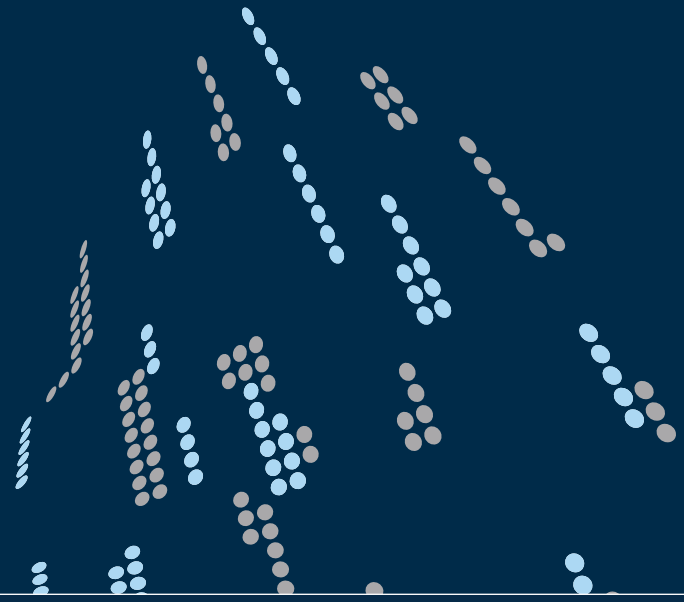
Speed is of the essence when dealing with any cyber security attack and *turing* has been designed to enable detailed analysis of terabytes of data in seconds. As well as providing near real-time visualisation and analysis of your DNS data you can also manipulate the data with ease, rapidly zooming in and out from seconds to years of data.

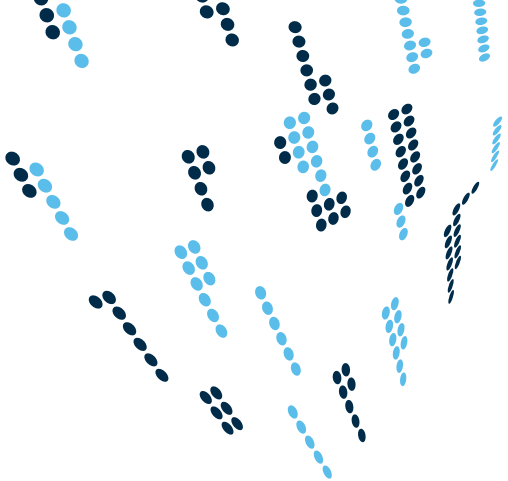
turing captures and stores all DNS messages including UDP, TCP, IPv4, IPv6 and EDNS packets.

The system also collects and stores advanced DNS metadata in detail so that as well as recording every single query and response you can also view information such as the resolver's IP address, port number and latency.

As well as being able to rapidly zoom in and out of packet level detail you can also filter the results with this metadata so you can focus on specific query or response types, individual DNS flags, individual domains or IP addresses in order to isolate specific issues.

This means that specific queries can be accessed and analysed and you can develop an understanding of your DNS traffic that was previously impossible.





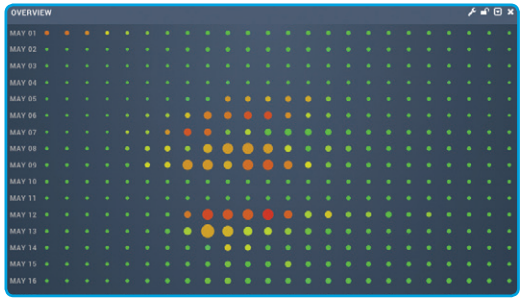
turing has a rich analysis environment which enables simple and intuitive interaction with a clear visual representation of DNS data.

turing has been built specifically for dealing with DNS data using a bespoke patent-pending architecture that out-performs other Big Data alternatives.

turing has a purpose-built storage and retrieval system that means that manipulating vast quantities of data is simple and fast.

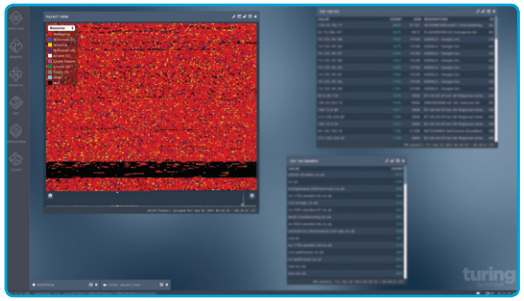
The system has been built using HTML5 which means it can be viewed on any browser on any device – so no need to invest in bespoke hardware. An intuitive touch and gesture based user interface helps you to easily interact with your data.

The solution also features a rich API so you can integrate the feed into other network management systems.



Analysing your DNS traffic with *turing* begins with an overview window which shows a summary of your traffic – you can choose a time scale from a whole year down to a single day. Traffic information is shown in a simple graphical format where the size and colour of each dot represents the query volume and the ratio of error responses for each time segment.

The size and colour of the dots on the Overview window help identify particular time periods of interest where the DNS traffic shows anomalies. These time periods can then be investigated further using a traffic window that shows types of query and response. Within this window information can be filtered according to data type and the time period visualised can be filtered from a month's worth of traffic down to a single millisecond, allowing for detailed analysis of key points of interest.



Individual packet data can be clearly visualised and segmented with a simple colour-code to identify specific query/response types. Data sorting is made simple using assorted filters that can be used individually or in combination and interactive legends make this filtering simple and intuitive. Packet data can also be listed and sorted according to Query name or Source IP.

turing has already made big steps in improving the health of the Internet.

Botnet identification

turing has been used to create a unique fingerprint that can quickly identify infection by a prevalent botnet. This was done by analysing spikes in MX responses and zeroing in on the characteristics of non-resolving requests, identifying and diagnosing spam patterns. With the ability to identify such infections almost immediately, this discovery can drastically reduce the amount of spam across name servers.

Latency issues identification

turing can identify latency issues that can result in crippling transmission and processing delays. By identifying and analysing re-query traffic, Nominet has pinpointed issues with specific servers so that solutions could be found.

Long domain name bugs and errors

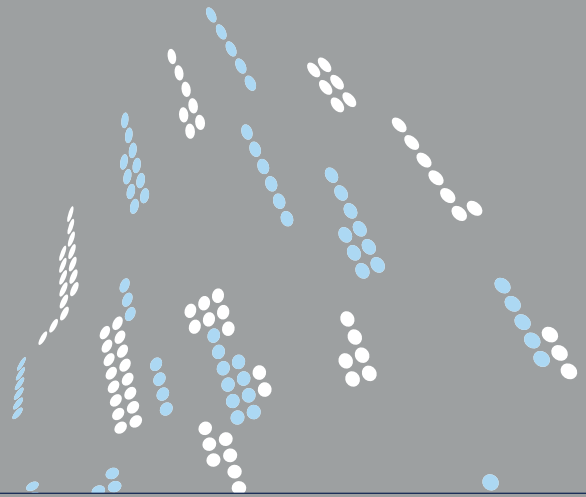
turing has been used to isolate and analyse an increase in SERVFAIL responses, identifying that they were the result of non-protocol compliant, long domain names (255+ bytes). This was causing problems with Google's Public DNS and also highlighted a hidden bug within BIND. Both problems have subsequently been resolved.

Malware Index Case detection

The processing power of *turing* enabled the identification of the Index Case of a particularly aggressive piece of malware by tracking back from infected machines which were using the Domain Generation Algorithm. This has enabled the prediction and identification of subsequent infections, severely limiting the spread of this particular malware.

Man-in-the-middle attack detection

Through analysis of source ports, *turing* can identify Kaminsky-style blind spoofing/caching attacks, detecting when resolvers are not choosing ports at random. By identifying non-random resolvers, Nominet has detected and prevented Man-in-the-middle attacks.



Future development

turing is already being used to help the Internet to become more stable by identifying abuse, misconfigurations and software bugs. As we continue to develop it, look out for a cloud hosted version (making it easier to start analysing your data), further integration with 3rd party management tools and a wealth of new features like spike detection, additional queries, smart heuristics and BGP monitoring.

About Nominet

Nominet is a public purpose not-for-profit company that is responsible for running the .uk, name registry since 1996 and the .cymru and .wales domains from September 2014. This includes protecting, promoting and supporting the online presence of more than 10 million domain names and handling around 4 billion DNS requests each day. With over 18 years experience in running one of the busiest and most successful Internet registries in the world, Nominet is one of the leading authorities on DNS. Nominet works closely with Internet Corporation of Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF) and is responsible for authoring the DNSSEC and other DNS standards.

Find out more:

If you would like any more information about turing please contact us:

nominet.uk/turing
turing@nominet.uk
+44 (0) 1865 332255