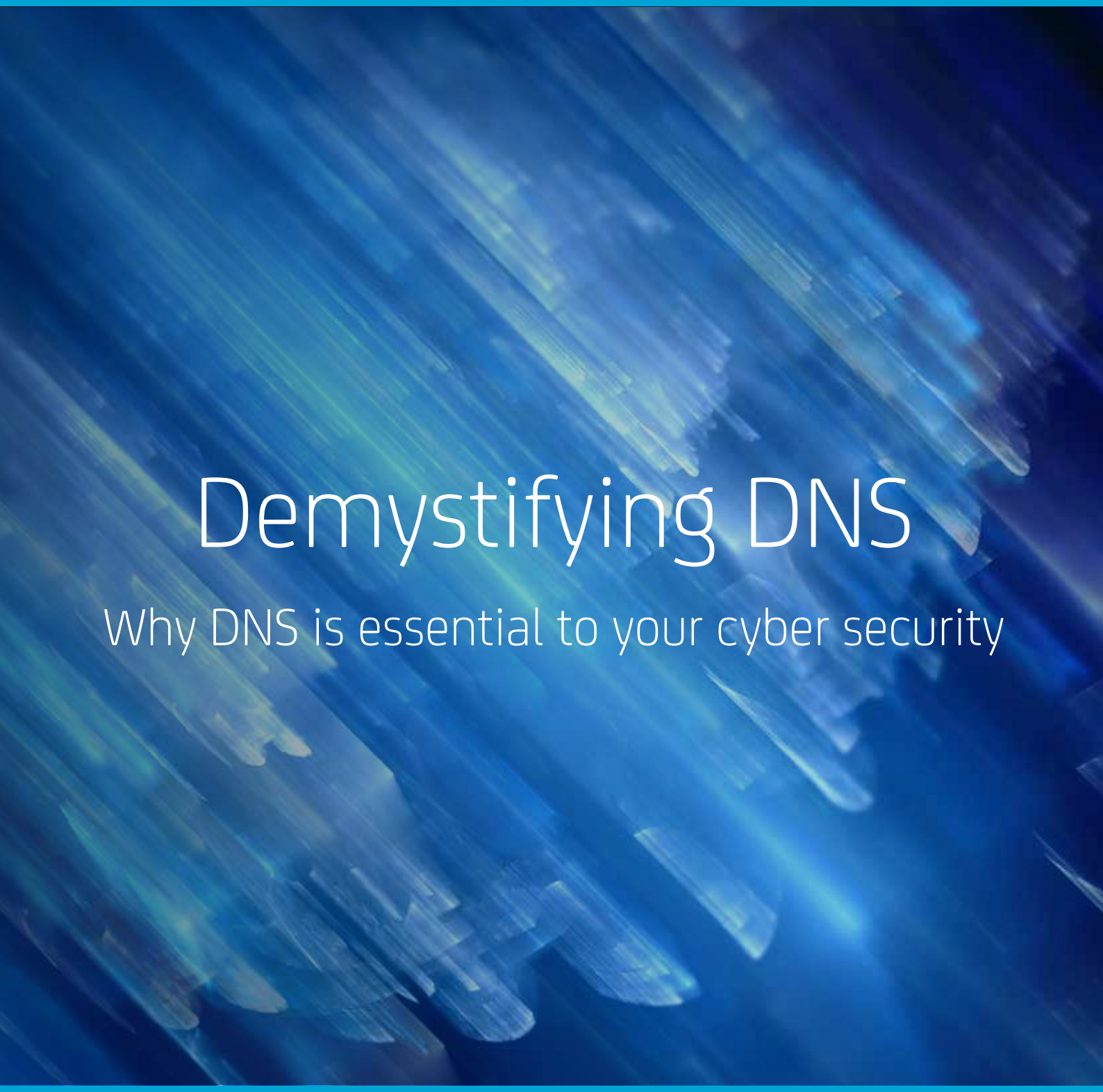


Demystifying DNS

Why DNS is essential to your cyber security

turing by NOMINET

turing by nominet

Introduction

As the cybersecurity landscape evolves, and sophisticated online criminals prey on large organisations who don't have the right defenses in place for a modern-day onslaught, cyber security is now ranked as one of the major challenges facing CEOs today.

91% of CEOs say breaches of data privacy and ethics will have a negative impact on stakeholder trust in the next five years.
Source: 20th CEO Survey, PwC, 2017

Gartner research shows that IT-related changes are the number two business priority for CEOs, ranking second only to growth. This is due to a shift away from outsourcing with 57% of CEOs preferring to build up digital capabilities in house, the reinternalization of IT. And with the General Data Protection Regulation (GDPR) due to be implemented in May 2018, businesses need to ensure they have a robust security solution – policy, resources and tools in place or they could be at risk of significant fines.

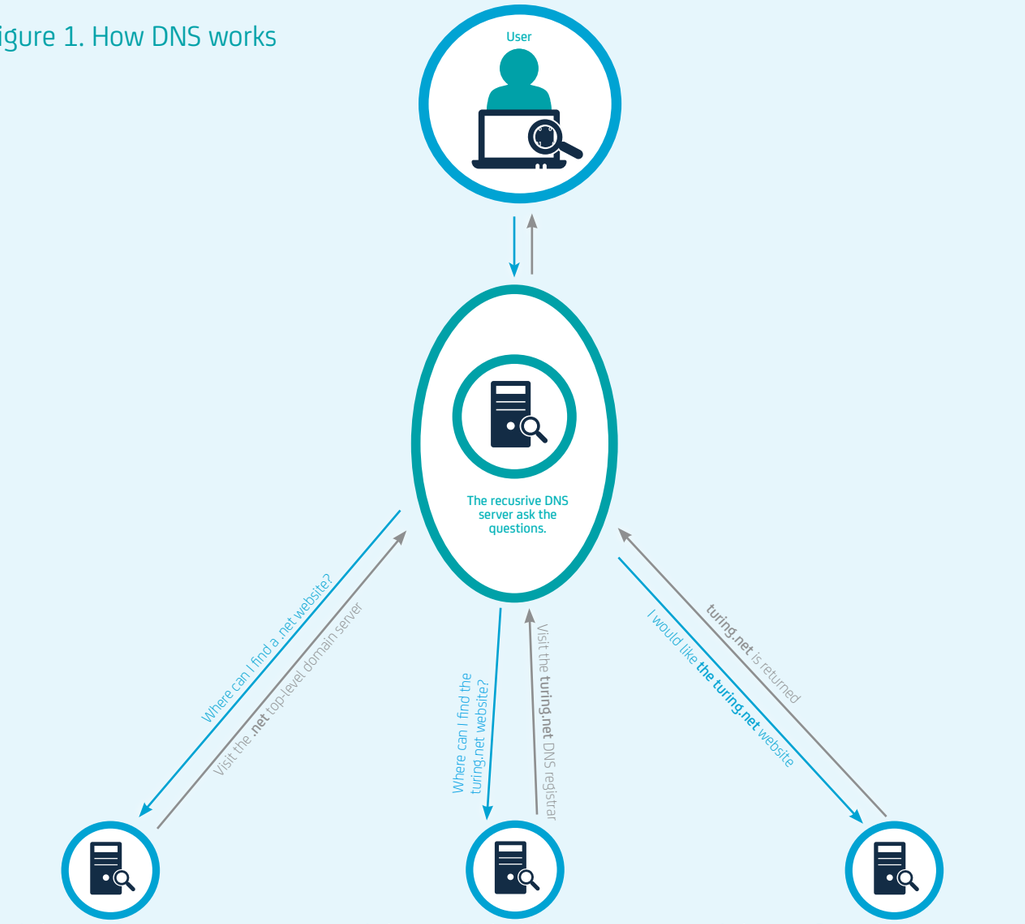
turing by nominet

The role of DNS

DNS plays a critical role in every network – it is the technology standard used to turn humanly understandable domain names into internet protocol (IP) addresses understood by machines.

For example, when someone types in the website **www.turing.net**, this is converted into IP address **52.210.24.201** and a data lookup takes place to ensure the right site is returned. This makes it quick and simple to access websites, applications and devices on the internet, do business online, socialize, learn, and collaborate.

Figure 1. How DNS works



Authoritative Root server

The root server handles requests for information about top-level domains only and does not have the information about where the lower-level domains (or full domain name e.g. turing.net) are hosted The job of the root server is to direct the requester to the name servers that specifically handle the requested top-level domain.

Authoritative Top-level domain server

These servers give answers to queries about the domains under their control (e.g. .com, .net, .uk). There are multiple top-level domain servers so your query for .com will be directed to a different location than your query for .uk. The top-level domain servers are authoritative as they provide the address of the requested domain's DNS registrar or private DNS server.

Authoritative Domain-level name servers

These servers contain the details for the requested domain, usually known as zone files. The zone file holds both the domain name (e.g. www.turing.net) and the machine readable IP address for that host. This returns the final answer – the IP address – to the requester and is the last stage of the domain name system.

DNS is easily accessible to everyone - users with good intentions and, unfortunately, the criminally-minded alike. Several factors make DNS especially attractive to cyber criminals. Due to its ubiquitos, always-on but behind-the-scenes nature, DNS is often overlooked by system administrators. It has some inherent vulnerabilities coming from its design, to be an open and easy-to-operate system. Most firewalls whitelist DNS. This results in DNS becoming a path for many cyber attacks.

For example, cyber criminals can easily manipulate a targeted company's domain name for malicious purposes. They can also easily register domains that differ only slightly from an organization's legitimate domain name (known as 'typosquatting') or redirect traffic that's navigating to the company's website to a rogue server by altering the IP address mapped to that domain in DNS records. Criminals use these techniques routinely to carry out scams, such as phishing, click fraud or brandjacking.

Two-thirds of DNS traffic logs analyzed showed signs of malicious activity
Source: Infoblox survey 2016

The number of attacks exploiting DNS are on the rise. Organizations worldwide are facing an immediate need to pay closer attention to DNS, to detect and respond to attacks, in order to keep their business secure and protected. Fortunately, due to the pervasiveness of DNS it's a great place for plugging in a defense layer that offers protection from threats that traditional security solutions, such as antivirus or network firewalls, would miss.

With the growth of the internet and more and more people and devices getting online every hour of every day, there are billions of packets of data to monitor, track and analyze. Traditionally it has been very difficult to gain insight into DNS traffic and to detect cyber threats or identify network misconfigurations that affect performance. There is now a business need to tap into this wealth of data and make sense of it.

turing by nominet

DNS on your corporate network

Corporate recursive DNS server

If your organization has a significant online presence, you're probably running your own DNS server. For example, a recursive DNS resolver which intercepts all outgoing queries to the internet from your organization's users, such as a user clicking on a link to connect to to a website.

Then, to find the IP address of the server that hosts the requested website, the recursive DNS resolver either forwards the query on to other servers or, if it has received the answer previously and cached it, it replies to the user right away.

These servers can be targeted by cyber criminals in several ways:

- Altering the answers to the queries that the server stores can redirect users to a malicious website and lead to a malware infection or loss of confidential data, for example, through phishing (see figures 2 and 3).
- Unauthorized copying and transfer of confidential data can be leaked through DNS, this is known as data exfiltration (see figure 4).
- Denial of Service (DoS) attacks can overload the DNS servers and shut down DNS resolution for a network, so that queries coming from real users trying to connect would not resolve and the website would not be displayed, thus disrupting business (see figure 5).

By analysing traffic that goes through the recursive servers, *turing* (Nominet's DNS analytics tool) can tell you a lot about the health of your network. For example, by monitoring traffic while cross-referencing the security lists it can reveal infected machines on your network, such as machines that have become part of a botnet and are sending spam, or those contacting a command-and-control domain after they've been infected with malware that uses that domain to establish a communication channel.

Figure 2. Phishing

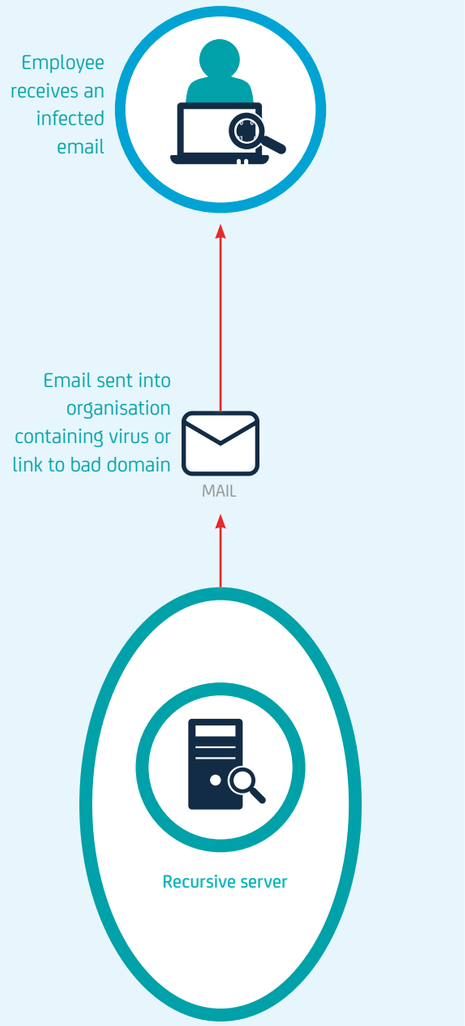
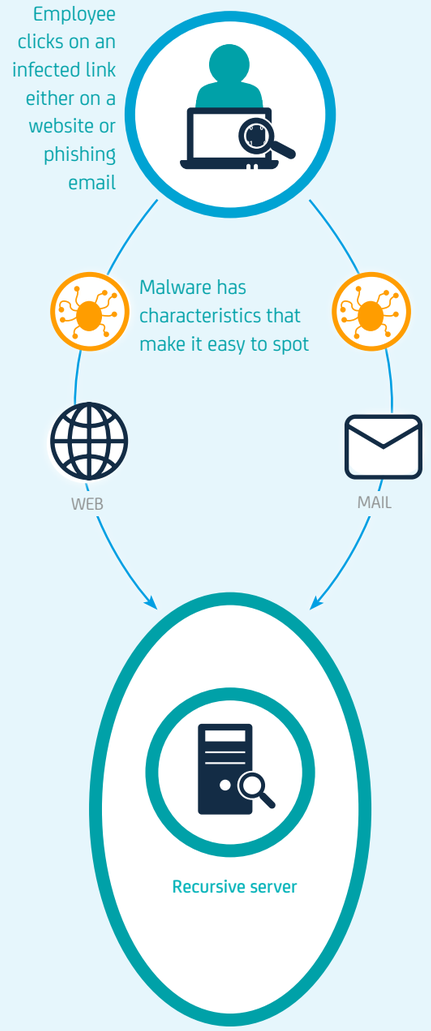


Figure 3. Malware



turing by nominet

Figure 4. Data Exfiltration

Corporate authoritative DNS server

As an organization you have an external audience, they will be asking your website questions:

where can i find the latest product?
what are the details of your service offering?
how much does it cost?'

Providing them with the right answers is authoritative DNS.

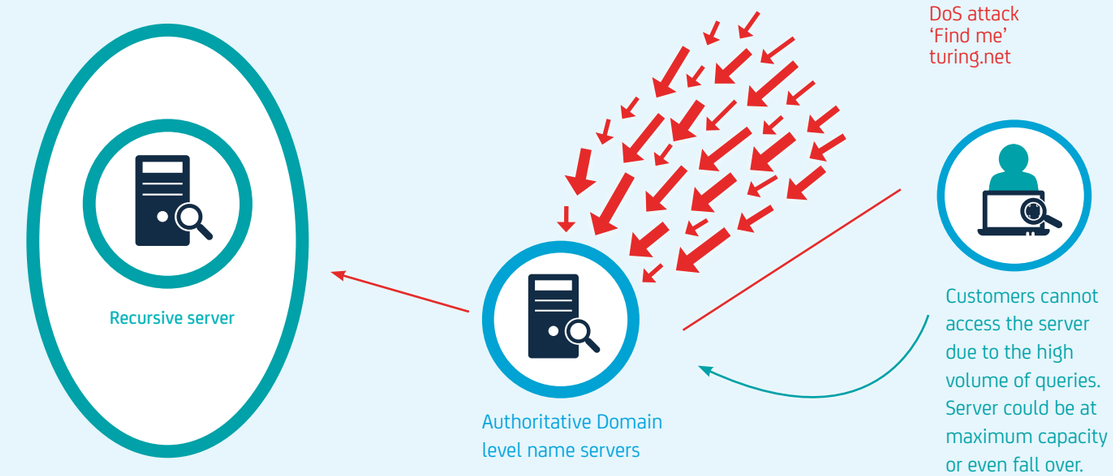
You will be running an authoritative nameserver, this server is responsible for answering these questions, mapping your domain names to IP addresses of the servers that host them and returning the right results to your customers. Tampering with the records the nameserver holds or its load and availability can seriously harm your business. Protecting this asset is of paramount importance to your business's operation, security and reputation.

A DoS attack against an authoritative DNS server may shut down resolution for a specific domain name or a group of domain names, so that no users can access them. An example of such an attack and the impact it may have is a DDoS attack, a type of DoS on Dyn which took place in November 2016 (see figure 5). **(https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/).**

During a DNS hijack, cyber criminals redirect traffic intended for a company's website to their web server with a replica of the site's content. Once on the fake site, users could enter user accounts, passwords, or even credit card numbers. In April 2017 hackers redirected all traffic intended for a Brazilian bank to a phishing replica of the website, and stole users' bank account details **(https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/).**

turing can detect suspicious traffic, as well as unfolding DoS attacks right from the start. It also provides you with all the details of a security event that enable you to act promptly and mitigate the threat - for example, IP addresses responsible for a DoS attack that you'd want to block, stopping your servers from falling over.

Figure 5. DoS



Delivering DNS services to your customers

ISP recursive DNS server

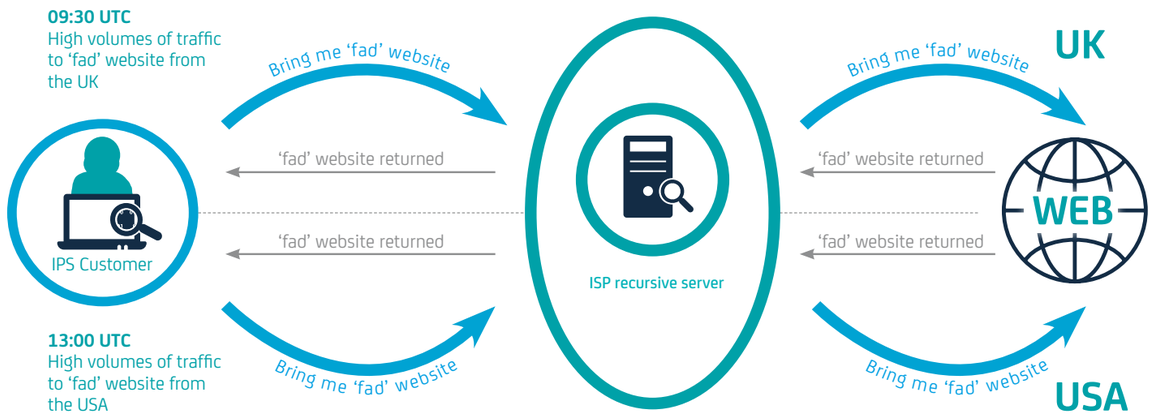
If you are an Internet Service Provider running a recursive DNS name server for your customers, making and caching queries on their behalf, then adding a security and analytics layer to this service can enhance your proposition, helping to protect your customers and your own organisation.

In addition to identifying threats and other events discussed in the previous sections of this paper, *turing* can also provide invaluable insight into your customers' business and browsing habits. For example, the list of top domain names can help you to better understand what people are most often looking for. If you are hosting websites, identifying the most popular hosted websites can help you allocate your resources so that those sites always have enough bandwidth. You can spot the latest fad website or see this information at different times or days of the week, to help you identify patterns and manage resources allocated to hosted sites to improve load balancing (see figure 6).

The top source IP addresses can help you to better understand who your users are. By identifying where your traffic is coming from, you can, for example, reduce your internal costs by setting up appropriate peering arrangements that would allow you to manage the traffic in the most cost-efficient way to you.

turing can give you insight into this customer behavior as well as helping you identify and mitigate against security risks.

Figure 6. Load balancing



turing by nominet

Glossary of threats specific to DNS

- **Amplification** - a distributed denial-of-service attack in which the attacker exploits the ability of DNS to return large responses to small queries; a large number of such responses are used to overload and bring down the victim's server.
- **App-based attack** - an attack targeted at a specific application and designed either to overwhelm the application or its components or to take advantage of vulnerabilities in the application.
- **Brute-force attack** - a trial-and-error method used to obtain information, often using automated software to guess the value of the desired data as many times as needed. For example, the attackers could force DNS servers to leak information about their mail servers, IP addresses, subdomains, etc. by constantly querying them for their possible subdomains.
- **Cache poisoning** - also known as DNS spoofing, is a form of computer hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect IP address. This results in traffic being diverted to the attacker's server.
- **DNS DDoS** - a distributed denial-of-service attack in which the attackers try to make the victim's server unavailable by overloading it with DNS requests from a large number of endpoints under their control (e.g. a botnet).
- **Domain generation algorithms** - algorithms used by various families of malware to periodically generate a large number of domain names that can be used as rendezvous points with their command and control servers.
- **DNS hijack -** queries are redirected to a domain name server (DNS). This could be via the use of malicious software or unauthorized modification of a server.
- **Fast flux** - an attack by a botnet that hides its phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.
- **Flood attack** - a denial-of-service attack in which the attacker sends a very large number of DNS requests to the server, trying to overload it so that it becomes unavailable to legitimate users trying to reach it.
- **OS and application vulnerabilities** - system flaws and application weaknesses that could be exploited to compromise the security of the system.
- **Pharming** - an attack in which the attackers redirect a website's traffic to another, fake site, often by exploiting a vulnerability in DNS server software.
- **Phishing** - an attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity, and often by directing users to enter sensitive information at a fake website that looks identical to the legitimate one.
- **Reflection** - a distributed denial-of-service attack in which the attackers replace the source address in their requests with that of their victim, thus causing a great number of large responses to be sent to the victim.
- **Semantic attack** - a social engineering attack that bypasses technical defences by altering electronic information in such a way that it still looks correct to the user, but the result is incorrect. It aims to deceive rather than directly attack the user and thus obtain valuable information (such as passwords, financial details, etc.).
- **Tunnelling** - transferring data over DNS by encapsulating it into DNS queries, often to illegally exfiltrate sensitive data out of an organisation.
- **UDP DrDOS attack** - a distributed reflection denial-of-service attack that uses UDP (User Datagram Protocol) spoofing (the attacker's source address in a request is replaced with the victim's one) and amplification (small requests generate large responses).

What is turing?

turing is a DNS cyber intelligence and analytics tool. It provides real-time insights into your organization's network traffic patterns, threats and events through the lens of DNS. turing uses machine learning algorithms and third-party feeds to identify and alert about anomalous behavior.

The ***turing*** software can be implemented on your network for your IT teams to use as part of their security solution or you can utlilize our expertise through our DNS services. **www.turing.net**

About Nominet

We protect, promote and support the online presence of more than 10 million domain names and handle around 3 billion DNS requests each day. With 20 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. We work closely with Internet Corporation of Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF) and law enforcement. Nominet is also part of the Active Cyber Defence (ACD) programme, being run as part of UK Government's National Cyber Security Strategy to help protect governmental and Public Service Networks (PSNs) from malware, phishing, botnets and other threats.

turing
by NOMINET