Understanding the threats to DNS and how to secure it

Chris Marrison

Chris Marrison, Infoblox

Essentially the address book of the Internet, the Domain Name System (DNS) is a mission-critical infrastructure used by all organisations and without which they cannot function. Yet, despite its importance, it remains a vulnerable network component that is frequently used as an attack vector by cyber-criminals, and is inadequately protected by traditional security solutions.

Catastrophic failure

It's a simple fact that, when critical DNS services are compromised, it can result in catastrophic network and system failure. An organisation's external DNS servers – those that face the Internet – that are used by its websites and email clients, may be subject to cyber-attacks such as DNS Distributed Denial of Service (DDoS) exploits, or simple reconnaissance, all of which can result in degraded performance and downtime.

"It's important for organisations to take steps to protect DNS from both external and internal threats, and take advantage of the unique position that DNS holds within the network"

But threats to an organisation's DNS will not always come from outside its firewalls; targeted attacks, representing risks to both data and infrastructure, can also come from within. An endpoint infected with malware, for example, or an advanced persistent threat (APT) could be using DNS to try to communicate with command and control (C&C) servers. Or a malicious insider could be attempting to steal sensitive information by embedding data in DNS queries or opening a DNS tunnel.

For a more complete and thorough security posture, it's important for organisations to take steps to protect DNS from both external and internal threats, and take advantage of the unique position that DNS holds within the network as an optimal enforcement point for protection and for responding to threats.

Threats to external DNS servers

Also known as 'authoritative' servers, an organisation's external DNS servers answer incoming queries from anyone attempting to connect with its network, such as sending an email or visiting its website. It's important that these authoritative servers remain available 100% of the time, or else the organisation they serve will vanish from the Internet. It's perhaps little surprise, therefore, that external DNS servers are subject to a variety of attacks, including DNS hijacking, and reflection and amplification, a form of DDoS attack involving an unwitting third party, among others.

The two most common threats, DNS reflection and amplification, led to DNS being recognised as tied for first place with HTTP as the protocol most used in all reflection/amplification attacks in the past year.[1] Targeting organisations in the gaming, software, technology, telecommunications, media, and financial services industries, these attacks exploit inherent weaknesses in the DNS protocol, such as its use of the connectionless user datagram protocol (UDP). Doing so inundates a particular, targeted server with unexpected responses it must then process.

Often launched by someone with a grudge against the target company, such as a hacktivist, an unscrupulous competitor or a hostile government, these attacks can be a smokescreen tactic, distracting organisations from the data theft or deeper infiltration that is taking place elsewhere on their network.

"An organisation could suffer significant unwanted publicity and damage to its brand if its DNS server was unwittingly used as part of a reflection/amplification on another organisation's network"

Of course, if an organisation's external DNS falls victim to a volumetric attack such as this, its server could slow down and possibly crash, effectively disconnecting the organisation from the Internet. This would result in service disruption and direct loss of revenue, not to mention significantly costly work to bring the servers back online. Conversely, an organisation could suffer significant unwanted publicity and damage to its brand if its DNS server was unwittingly used as part of a reflection/amplification on another organisation's network.

DNS hijacking, which compromises the integrity of an organisation's DNS, redirects users trying to access a particular site to a practically identical imitation controlled by the hijackers. From there, hackers are able to acquire sensitive information such as user names and passwords. As with reflection/amplification, if an organisation's DNS was to be hijacked it could lead to a direct loss of revenue and a negative impact on its brand.

Threats to internal infrastructure

An organisation's internal DNS servers are also potential victims of infrastructure attacks that can lead to a drop in productivity, business downtime, and an increase in operational expenses.

The larger the organisation, the greater the number of endpoints within it that may become compromised and forced to take part in these attacks. For example, internal DNS DDoS attacks are currently on the rise. As with their external counterparts, these volumetric floods can overwhelm internal DNS servers, leading to slow performance and, potentially, eventual failure.

A large healthcare organisation recently suffered a flood attack of a million queries per second on its internal DNS servers, and an internal DNS outage in a large computer-storage company resulted in its employees being sent home for four hours.

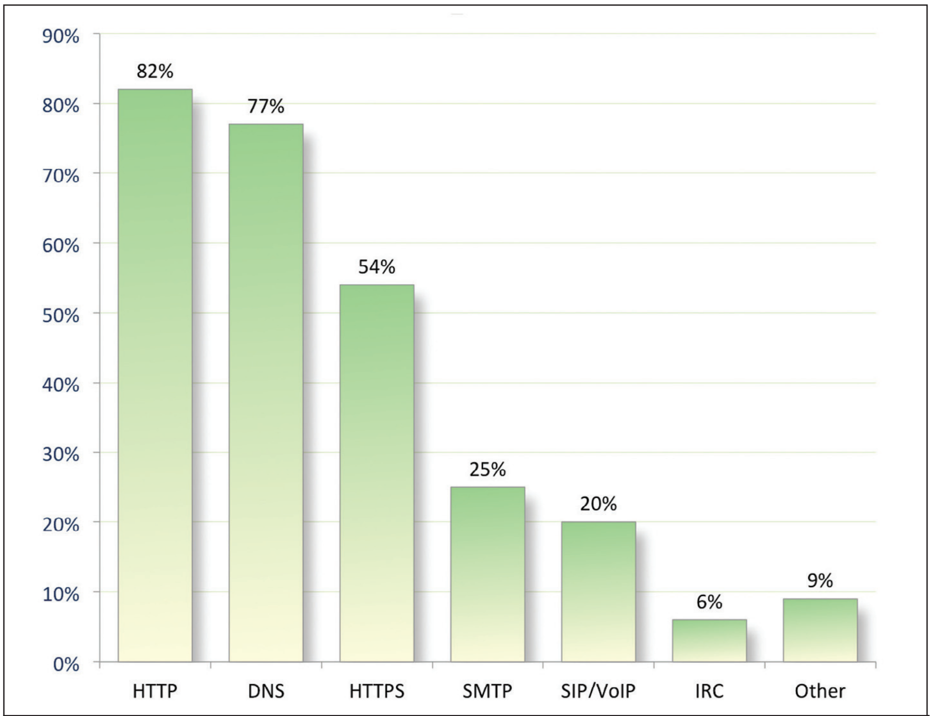
Other, more stealthy and sophisticated attacks stay under the radar, exhausting resources on recursive servers – the part of DNS that provides the required information to web clients. With attackers using advanced techniques ranging from simple NXDOMAIN attacks to highly sophisticated DDoS attacks involving botnets, chain reactions and misbehaving domains, the recursive servers can suffer effects such as resource exhaustion, cache saturation and outbound bandwidth congestion. At the same time the external authoritative server of the target domain will suffer DDoS.

Malware and APTs

The proliferation of mobile devices and mobile users in today's Bring Your Own Device (BYOD) culture means that there is a growing number of threats inside an organisation's firewall, as well as outside. Increasingly sophisticated APTs are using DNS to communicate with C&C servers, which makes the APTs harder to detect with traditional tools. Indeed, every single business network analysed for a recent security report was revealed to have traffic going to websites that hosted malware.[2]

Fast flux, for example, is a technique that involves malicious domains rapidly changing their identity and IP addresses to avoid being detected by traditional security solutions, while a domain-generation algorithm (DGA), sees malware randomly generating a large number of domain names with which it then attempts to communicate to receive updates or commands.

However, finding infected devices can be challenging – attack techniques can be hard to detect and take down, and the threat response time is often far too long. If malware such as this is allowed to spread within an organisation's network, it could lead to the theft of sensitive data or money. The GameOver Zeus botnet, for example, was famously responsible for the theft of hundreds of millions of dollars last year.



Targets of application-layer attacks. Source: Arbor Networks.

Data exfiltration

Whether carried out intentionally by malicious insiders or unwittingly via malware-infected devices, DNS is increasingly being used as a pathway for data exfiltration too, with IP traffic being tunnelled through DNS port 53, which is rarely ever inspected, even by next-generation firewalls. Such attacks can result in sensitive information such as credit card details or company financials being stolen either by a DNS tunnel being established from within an organisation's network, or by encrypting and embedding chunks of the information in DNS queries and decrypting and reassembling them at the other end.

It's worth noting that commercially available software can be used to facilitate this kind of attack, with one recent example being a freeware tunnelling application released under the ISC licence for forwarding IPv4 traffic through DNS servers.

Comprehensive external DNS protection

Many security solutions claim to offer protection for DNS but, under scrutiny, can be limited in what they actually protect. Indeed, the majority will tend to be external solutions bolted on to a traditional security solution rather than being built from the ground up specifically to secure DNS against attacks.

The most effective way to address threats to DNS is to have intelligent detection capabilities built into the DNS servers themselves. A purpose-built external DNS server designed to provide defence against a wide range of DNS-based threats such as volumetric, exploits and reconnaissance attacks should use techniques such as those outlined below to continuously monitor for, detect and mitigate against DNS attacks while at the same time responding to legitimate queries.

"Any connection with C&C servers will be broken, disrupting the ability to steal data through standard network protocols and, at the same time, leading to fewer infections and inhibiting the propagation of malware inside the network"

Threat feeds can be used to ensure that the solution's defences are kept up to date on new and evolving threats as they emerge, without the need for patching, while hardware-accelerated DNS DDoS mitigation can be employed to ensure system integrity and availability is maintained even under extreme attack.

By discriminating between different query types and the normal rates associated with them, smart rate thresholds can significantly slow down DNS DDoS and flood attacks without denying services to legitimate users. Source-based throttling, for example, will detect abnormal queries by source and cause brute-force methods to fail, while destination-based throttling will detect abnormal increases in traffic grouped by target domains.

Automatically blacklisting non-responsive and misbehaving servers and zones will avoid too many outstanding queries to misbehaving and dead domains, while dynamically blocking clients that generate too many NXDOMAIN, NXRRset, or ServFail responses will prevent misbehaving clients from bringing down the DNS server.

Analysing packets for patterns of exploits that target certain vulnerabilities means that some attacks can be stopped before they have the chance to cause any damage, and filtering traffic with next-generation programmable processors makes it possible for malicious traffic to be dropped before it reaches the DNS server application. Even in advance of this, it's possible to identify reconnaissance activity and report it, allowing network teams to prepare a response before any attack is launched.

Furthermore, while action is taken against ongoing and planned attacks, periodic integrity checks should be carried out in order to eliminate any compromise to a system's records by DNS hijacking, and detailed reports compiled on attack points and sources, providing the intelligence needed to take action.

Securing internal DNS

The unique position that DNS holds within the network makes it the optimal enforcement point for protection against and response to attacks.

An effective internal DNS security solution will prevent APTs and malware from exploiting DNS, preventing data exfiltration and protecting mission-critical DNS infrastructure from attacks, all without the need for an organisation to make changes to its network architecture. Defending against a wide range of DNS-based attacks to maximise service availability, an internal DNS security solution will use techniques such as those outlined below to continuously monitor for, detect and drop DNS attacks such as DNS DDoS, exploits, cache poisoning, and DNS tunnelling.

By employing DNS response policy zones (RPZs) and threat intelligence on known malicious destinations, an internal solution will be able to intercept DNS queries associated with malware and APTs, and disrupt communication with external C&C servers and botnets. This blacklist of malicious destinations can be kept up to date through the use of a continuous threat intelligence feed, and should ideally be integrated with industry-standard ecosystems for information sharing and centralised threat mitigation.

The solution should also prevent the loss of sensitive information by detecting and preventing data exfiltration via DNS tunnelling. Focusing on large UDP/TCP queries and responses, along with the number of too-large requests in a given timeframe, will enable the solution to detect any DNS tunnelling attempts and drop any queries that go beyond a given threshold. Any connection with C&C servers will also be broken, disrupting the ability to steal data through standard network protocols and, at the same time, leading to fewer infections and inhibiting the propagation of malware inside the network.

DNS is a critical piece of network architecture that is far too valuable to be left vulnerable. For this very reason, along with the fact that it has not been adequately protected in the past, it has become a highly attractive target for attacks.

By ensuring the right security solution is in place to defend its DNS from external and internal threats, and by looking at the unique position of DNS as a strength rather than a vulnerability, an organisation can convert its DNS servers from Achilles' heels to network security assets, helping to improve its overall security posture.

About the author

Chris Marrison is a consulting solutions architect at Infoblox where he works with some of its largest customers. Prior to joining Infoblox, he was responsible for building the core Internet services for Virgin.Net, Which Online, and NTLWorld, before moving to a business-oriented ISP which specialised in providing value-added services to multi-tenant buildings funded by Canary Wharf Group, British Land and others. Infoblox (www.infoblox.com) delivers network control solutions, the fundamental technology that connects end users, devices and networks. These solutions enable more than 8,100 enterprises and service providers to transform, secure and scale complex networks.

References

1. 'Worldwide Infrastructure Security Report'. Arbor Networks. Accessed Sep 2015. www.arbornetworks.com/resources/infrastructure-security-report.
2. '2014 Annual Security Report'. Cisco. Accessed Sep 2015. www.cisco.com/web/offers/lp/2014-annual-security-report/index.html.