REPORT REPRINT

# DNS reboot: from commodity to strategic asset

JENNIFER PIGG CLARK

23 AUG 2016

DNS is a critical component of the network. It is pervasive, touching all devices attached to the internet; nevertheless, the DNS infrastructure is treated as little more than the internet equivalent of a phone book. Enterprises and CSPs should leverage the potential DNS offers for improved security, service creation and customer experience.

THIS REPORT, LICENSED EXCLUSIVELY TO AKAMAI, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. THIS REPORT IS SOLELY INTENDED FOR USE BY THE RECIPIENT AND MAY NOT BE REPRODUCED OR REPOSTED, IN WHOLE OR IN PART, BY THE RECIPIENT, WITHOUT EXPRESS PERMISSION FROM 451 RESEARCH.

451 Research®

©2016 451 Research, LLC | WWW.451RESEARCH.COM

Domain Name System (DNS) is a critical component of the network. It is pervasive, touching all devices attached to the internet; nevertheless, the DNS infrastructure is treated as little more than the internet equivalent of a phone book. The DNS cache-poisoning attack publicized by security researcher Dan Kaminsky in July 2008 succeeded in raising awareness about security vulnerabilities of DNS. However, enterprises and CSPs have not sufficiently looked at the flip side of DNS to appreciate the potential it offers.

## THE 451 TAKE

Enterprises and communication service providers (CSPs) should recognize that recursive DNS presents a significant opportunity. Desktop security/antivirus software cannot protect enterprises and consumers from the threats – such as bots, phishing, distributed denial-of-service (DDoS) attacks and unwanted content – today's internet brings. We believe DNS presents CSPs with the opportunity not only to help secure the network from attack, but to do so proactively while improving the customer experience. Migration to next-generation DNS can be done incrementally, without the CSP having to 'rip and replace' its existing DNS. An enhanced recursive DNS infrastructure can move CSPs toward the goal of the intelligent network and flexible, customized and differentiated services.

Recursive DNS enables the following enhancements with a focus on security.

- Material improvement in security
- Improved network performance
- Better resource utilization
- Service creation
- Enhanced customer experience

Simply put, recursive DNS asks: 'Where is this domain located?' and authoritative DNS answers: 'It's at this IP address.' Your recursive DNS sees all domains you attempt to access, and because of this, it is in the ideal position to get you to the sites you want to access and, accordance with your network policy, to protect you from sites that might be dangerous from a security perspective, annoying in terms of spam, or offensive due to inappropriate content.

## DNS SCALE: THE DEEPENING NAME POOL

At the beginning of 2009, there were 280 top-level domains (TLDs), 90% of which were country code domains (ccTLDs). As of August 16, according to Internet Corporation for Assigned Names and Numbers, there were 1,484 TLDs, almost 85% of which were generic domains – i.e., TLDs other than ccTLDs. Data from Verisign, which operates the authoritative domain name registries of the two largest TLDs – .com and .net – shows that there were about 326.4 million domain names as of the first quarter of 2016 across all TLDs, an increase of 3.8% over the fourth quarter of 2015. Registrations grew by 32.4 million, or 11%, year-over-year. The pace will continue as more people and things connect to the internet.

Next-generation DNS infrastructure and managed services must be able to deliver better internet performance than our legacy DNS infrastructure. It must be able to scale to meet evolving internet demands such as IoT, cloud services, IPv6 addressing and mobile device/mobile web. It must have the flexibility – enabled though strong policy implementation – to build differentiated value-added service capabilities, and it must enhance security in terms of its ability to protect itself, and also to protect end users from internet ne'er-do-wells.

The move toward cloud services amplifies the potential for DNS to help carriers differentiate their services through end-user access to flexible user-defined services that are rapidly provisioned, and through carrier access to the wealth of data accumulated in DNS recursive servers. This DNS data exfiltration can be used to enhance the customer experience but remains virtually untapped.

## DNS ROLE REVERSAL: FROM SECURITY VICTIM TO GUARDIAN

DDoS attacks continue to growing rapidly in scale and severity. Akamai reported in its Q4 2015 State of the Internet/Security report released in June that DDoS attacks were up 148.85% over Q4 2014, and DNS continues to be a popular attack vector. However, DNS can also be effective in identifying threats. By trending DNS activity, carriers can quickly detect patterns and use this information to predict and mitigate threats. DNS transactions can be monitored on a set of recursive servers in real time, with no negative impact on service response time. There are DNS services on the market today that can identify and characterize unusual activity and then calculate the likely scope and source of the threat via risk-assessment software tools. CSPs can leverage these tools to dramatically mitigate the impact of security attacks automatically, without operator intervention. CSPs should be leveraging DNS services to identify attacks as they occur and to shut down hackers before a DoS attack can achieve momentum or a spoofing attack can cause damage. Through the use of cloud-based and virtualized service, CSPs should be able to deploy these tools quickly without regard to geography and to mitigate attacks wherever and whenever they occur.

### Removing the botnet choke hold

Advanced DNS services are also able to help carriers protect against security threats that do not directly target the DNS system. A prime example of this is botnet detection and mitigation. According to the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), an organization composed of service providers and vendors involved in the fight against spam, bots can be programmed to:

- Steal identifying information and credentials
- Produce spam (bots are responsible for more than 90% of spam)
- Launch denial-of-service attacks
- Log keystrokes
- Send fraudulent DNS queries to support cache-poisoning attacks
- Support proxy services
- Enable surreptitious hosting services
- Initiate click fraud

Botnets rely on DNS for their normal operation. By tracking DNS queries performed by suspected bot hosts and then comparing those queries against domains known to support botnet command and control functions, the service provider can identify hosts that are infected with bot software. Identifying and then eliminating the bots from the network, the service provider frees up DNS server capacity, lowering capital costs while improving DNS query performance.

### Don't go there – DNS redirects

DNS can also be used to redirect users away from known phishing and malware domains/sites and to defeat typo-squatters. The key to this lies in a strong policy engine combined with frequently updated (measured in seconds, not minutes or hours) and comprehensive data of blacklisted sites from security intelligence agencies that feeds into the policy database.

Typo-squatters wreak brand havoc, siphon away revenue, and severely impact user experience and security through a variety of schemes, all of which capitalize on URL typos to misdirect users to:

- A competitor's website
- The correct site via an 'affiliate site' – collecting affiliate commissions for the site referral when there was no site referral
- A 'gripe site' – a site that expresses the opposite opinion to that of the intended site
- Internet pornography
- A mimicked site as a phishing scheme to gather personal information, including passwords, from users who believe they are on the intended site.
- To install malware or adware onto the user's device

By eliminating the majority of spam (and improving DNS query response time), the service provider improves the user's experience. The decrease or elimination of phishing, online scams, bogus antivirus applications, ransomware and malware provides direct benefit to the end user. This, in turn, translates directly to bottom-line benefits to the carrier with:

- Improved brand loyalty
- Increased subscriber retention
- Decrease in call center contacts

## ENABLING USER SECURITY AND CONTROL

Users need access to the content they want. They do not want to worry about unintentionally accessing inappropriate content or worry about inappropriate content – including a wealth of web-based threats – accessing them. 451 Research consumer survey data indicates that users do not expect the federal government to regulate web content and access. Consumers do, however, look for help from CSPs in protecting themselves and their children from security breaches and inappropriate or illegal content. DNS, combined with a robust and flexible policy control and enforcement system, is key to identifying and then redirecting the user away from inappropriate, unwanted or downright dangerous websites.

Carriers can use their DNS and network policy infrastructure to provide not just coarse-grained URL filtering for an enterprise or home, but to tailor services to the individual user – improving the customer experience and, again, increasing brand loyalty and subscriber retention by:

- Enabling the user to define the level of content control
- Allowing users to block access to sites they personally consider offensive
- Preventing accidental navigation to websites that host illegal content
- Providing multiple levels of parental control specific to the child or device
- Providing parental monitoring services
- Decreasing transaction times (e.g., medical device sensor data posts)

### Curfews in the age of the internet

A January 2016 study from the Pew Research Center, 'Parents, Teens and Digital Monitoring,' shows that parents are concerned both about their teens giving out personal information online (whether intentionally or by mistake) and about teens accessing inappropriate content. As a result, most parents implement their own computer usage policies. For example:

- 61% of parents have checked which websites their teens have visited
- 48% of parents know their teens' e-mail passwords
- 48% of parents have looked through their teens' phone call records or messages

However, these measures are not enough; parents want and need help, and they should be able to turn to their service providers for this help.

- 39% of parents report using parental controls for blocking, filtering or monitoring their teens' online activities.
- 16% use parental controls to restrict their teens' use of cellphones.
- 16% use monitoring tools on their teens' cellphones to track location.

While the Pew study looked at teens aged 13-17, the survey results show that parents saw a need for stricter controls for younger teens. However, the sharpest uptick in mobile and smartphone acquisition by minors is younger still – between the ages of nine and 12. OFCOM, the communications regulator in the UK, published survey results last year showing that at age nine, slightly under 20% of children in the UK have a mobile phone. By age 13, that percentage jumps to 80%, and roughly 70% of the kids have smartphones with the nearly limitless opportunity for misuse that comes with these bewitching devices.

The capability to differentiate by domain can enable the service provider to offer the end user personalized control. An example of this is parental control services, which block access to inappropriate or illegal sites such as pornography, gambling, self-hurt and child exploitation images. However, this is a very sensitive issue because it is perilously close to infringing on net-neutrality regulations. We advise that two safeguards should be in place when service providers offer parental control as a service:

- The sites list must be from multiple trusted sources. Recent attempts to block access to socially marginal sites by some EMEA and Asia-Pacific government agencies have led to wildly inappropriate sites being included on the lists, such as opposing political parties, free press and, on the more bizarre side, a travel agency.
- The default setting must be opt-out. The decision to block access to the domains must be offered on a per-user basis with the ability for each user to opt in. This helps the service provider avoid potential public relations or regulatory issues that, for example, both Google and Facebook have experienced with default opt-in settings for features that impacted user privacy.

## CONCLUSION: DNS IN 2016

We believe DNS presents CSPs with the opportunity not only to help secure the network from attack, but to do so proactively while improving the customer experience. DNS enables navigation of the web and makes email systems possible. Every network trend 451 Research tracks brings us closer to the ability to connect from any device to any other networked device, anywhere, at any time. We are always pushing the boundaries of our networks, and the architecture of DNS is a critical enabler of this expansion. Enterprises can realize the advantages of DNS in a number of ways, including outsourcing DNS infrastructure to a cloud services provider that offers enhanced DNS service, or even by supplementing existing DNS with 'premium DNS' for disaster avoidance or perhaps for use by customers who subscribe to value-added services. The bottom line is that migration to next-generation DNS can be done incrementally, without the CSP having to 'rip and replace' its existing DNS. An enhanced recursive DNS infrastructure can move CSPs toward an intelligent network and flexible, customized and differentiated services.