Securing DNS to Thwart Advanced Targeted Attacks and Reduce Data Breaches

A SANS Whitepaper

Written by John Pescatore

November 2014

Sponsored by

Infoblox
Internet traffic is severely affected when critical DNS services are not reliable or are compromised by cyber attacks, just as highway traffic is disrupted or stopped when bridges are damaged. Even worse than disruption, insecure DNS services can be used by attackers to impersonate a business and route customer traffic to malicious sites that steal usernames, passwords, account information or valuable intellectual property.

DNS services can be secured with the right configuration and deployment of appropriate solutions, but in many IT organizations the responsibility is spread across multiple groups and often falls through the cracks. CEOs and CIOs should ensure first that DNS governance is well defined and then make sure those DNS services are delivered efficiently, reliably and securely.

This paper looks at the basics of DNS services, how they can be compromised, how to secure them more effectively and how an organization can actually use them as an asset to improve its security posture.
The DNS essentially provides the Internet’s “address book.” At the simplest level, DNS services manage and map human-understandable terms (e.g., www.sans.org) to computer network IP addresses (e.g., 66.35.59.202), just as the telephone system maps telephone numbers to the telephone network connection of a landline phone or mobile unit. Without such services, inter-device connectivity would not be possible.

As seen in Figure 1, DNS is implemented as a distributed, hierarchical database consisting of:

- **Internet root servers.** There are 13 named authorities that make up the Root Zone at the top of the hierarchy. These authorities manage the top-level domains, such as .com in the Figure 1 example.¹

- **Second-level domains.** Typically organizations are assigned a second-level domain, such as Google.com.

- **Subdomains.** Organizations can then create subdomains, such as www.Amazon.com or example.Amazon.com.

- **Hosts.** Endpoints (typically PCs or servers, but essentially anything that needs to communicate over the Internet) comprise the lowest level and are the location of IP addresses.

¹ [www.iana.org/domains/root/servers](http://www.iana.org/domains/root/servers)

For two hosts to communicate, each must traverse this hierarchy to obtain each other’s IP address. To do so, each host must have resolver software that queries a name server to find the appropriate IP address. Modern operating systems used by PCs and servers usually contain the resolver software, but some specialty devices or appliances contain independent resolver applications.

To translate (or resolve) a domain name into an IP address, the host resolver issues a series of queries to a DNS server it has been configured to use. This DNS server can be an authoritative name server or a DNS cache server that responds directly with the IP address, or the server may act recursively and query other name servers to obtain the IP address information.

DNS name servers are implemented at many levels within the enterprise or by using outside services. For internal DNS services, many Windows-centric enterprises use Microsoft Windows Server DNS, while organizations with more heterogeneous, mixed operating system environments often use BIND software to implement name servers.

Firewalls and routers also can be configured to act as DNS servers. For performance and reliability reasons, many large organizations elect to use dedicated DNS appliances as dedicated DNS servers. Also, managed DNS services are available to simplify DNS implementation.

Outside of the enterprise, ISPs provide DNS services along with bandwidth. External DNS-as-a-service offerings are also available that provide higher levels of performance and reliability than typical ISP services.

This discussion has focused on a basic understanding of DNS. Other, more complete DNS tutorials are available.3

The security, integrity and reliability of Internet commerce and communication depend on underlying DNS services. Successful attacks against DNS services fall into three major categories:

- **Denial of service (DoS).** If DNS services are taken down, business disruption occurs when users and systems can no longer communicate over many network paths. DNS servers that are not locked down can also be used to launch DNS amplification attacks against other target servers that result in high bandwidth DoS attacks.

- **Hijacking.** If the integrity of external DNS services has been compromised, customers attempting to reach an enterprise's website may actually unknowingly connect to attacker websites, where they may be tricked into downloading malware and/or exposing their username and password or other sensitive information.

- **Man in the middle (MitM).** If DNS services are compromised, attackers can cause all traffic to flow through their site and monitor all traffic between an enterprise's customers (or employees) and the Internet, without either side being aware of it. This can lead to exposure of passwords, credit card numbers, personal health information, intellectual property, etc.

The above list details the severe impacts of attacks against DNS services. It is also important to note that most modern forms of attack (often called advanced targeted threats or advanced persistent threats [APTs]) have to use DNS services to succeed. A typical attack might look like this:

1. The attackers target a user, often with a very targeted phishing email, and trick the user into going to a compromised website where a custom, targeted malicious executable is downloaded onto the user’s PC and escapes detection for long periods of time.

2. Once the malicious software is loaded and executed, it uses DNS services to communicate with the attackers’ command and control (C2) server to download sophisticated attack code.

3. With malware downloaded, the attack code typically scans the internal name space (using DNS services once again) to locate databases or other targets of interest.

4. After the internal target is compromised, financial data or other targeted information is sent to the attackers’ site—requiring yet another use of DNS services.
Examples of DNS-dependent attacks that made headlines recently include:

- **CryptoLocker**—a Windows-based “ransomware” disguised as a PDF or voice mail audio file. Once a machine is infected, it downloads an algorithm that encrypts all the data on the local hard drive and asks for a ransom to retrieve the data.

- **GameOver Zeus (GOZ)**—a peer-to-peer botnet of infected machines that targeted mainly the financial services industry. It was responsible for theft of hundreds of millions of dollars.

A few recent DNS attacks drive home the severity of the problem and point to underlying vulnerabilities in DNS security.

**New York Times/Twitter SEA Attack**

In August 2013, the UK sites of both *The New York Times* and Twitter went down, and a hacktivist group, called the Syrian Electronic Army (SEA), took credit. The attackers compromised a Melbourne, Australia, register of DNS addresses and were able to modify DNS addresses of *The New York Times*, Twitter and other targets. This allowed the attackers to both cause business disruption and use MitM techniques to compromise customer data.

**Gaming Attack**

In June 2014, attackers used DNS amplification attacks to launch a distributed denial of service (DDoS) attack against a video gaming company. The attack peaked at over 100GBs and resulted in several hours of downtime for the target company.

---


**Phishware MitM Attacks**

In March 2014, PhishLabs observed a wave of MitM attacks targeting users of online banking and social media. The attacks used phishing techniques to deliver malware that changed DNS settings and installed a rogue certificate authority (CA). This caused corporate PCs to rely on the attackers’ DNS server for name resolution, and the rogue CA caused the PC to trust the information returned, without displaying anything unusual to the user or system administrators.

The attackers were then essentially sitting in the middle of all transactions between users and their bank accounts or other online financial services. They were able to modify transactions and copy all username/password information.

These are just a few of the recent occurrences. Other examples include:

- Google Malaysia DNS attack
- Honeypot DNS amplification attack data
- DNS amplification attack
- DNS OARC list of attacks

In addition to reporting that the number of large-scale DDoS attacks is increasing, one vendor says hackers use open DNS servers for launching and amplifying attacks.

Another increasing trend is “smoke screening,” where attacks on DNS are used as a diversion to keep the security and networking teams distracted, while breaching company network defenses at the back end to steal data.

---

8 [www.nothink.org/honeypot_dns.php#attacks](http://www.nothink.org/honeypot_dns.php#attacks)
10 [www.dns-oarc.net/files/web-brochure.pdf](http://www.dns-oarc.net/files/web-brochure.pdf)
11 [http://threatpost.com/large-scale-ddos-attacks-continue-to-spike](http://threatpost.com/large-scale-ddos-attacks-continue-to-spike)
Since compromise of DNS services can lead to severe business disruption and/or data exposure, most compliance regimes require securing DNS services, in the same way as other critical assets are secured. DNS is specifically mentioned in several compliance frameworks:

- The PCI DSS regulations require DNS servers to be in-scope for a PCI security assessment and for DNS logs to be archived.\(^\text{12}\)

- The National Institute of Standards and Technology (NIST) 800-53 rev 4\(^\text{13}\) has numerous requirements with regard to establishing and maintaining secure DNS services, and also points to NIST 800-81-2\(^\text{14}\) “Secure Domain Name System (DNS) Deployment Guide.”

- The Federal Financial Institutions Examination Council (FFIEC) posted compliance guidelines in January 2014 on DDoS attacks.\(^\text{15}\)

- The DDoS Quick Guide\(^\text{16}\) from the U.S. Department of Homeland Security and the Computer Security Incident Handling Guide\(^\text{17}\) from the U.S. Department of Commerce also cite DNS security.

- The Australian government publishes IT Security Threat and Risk Assessment (TRA) for public key infrastructure providers, including TRAs on DDoS and DNS vulnerabilities.\(^\text{18}\)

### Securing DNS Services

Monitoring DNS service use gives security professionals an opportunity to detect the various stages of advanced persistent threats. By combining threat information with DNS services, these attacks can also be disrupted by blocking DNS resolution of known malicious sites.

The availability of reliable Internet communications is critical to modern businesses, and keeping DNS services safe from attack is critical to avoid business disruption. While that seems obvious, all too often securing DNS services is overlooked. There are several reasons for this, but lack of organizational awareness on DNS attacks is typically the cause.


The most common underlying problem is the lack of clear DNS governance in the organization. Who in the enterprise has clear ownership, responsibility and authority for DNS services? While the security group almost invariably has responsibility for pointing out vulnerabilities, the members of the group do not see themselves as owning DNS services and hence being responsible for security of those DNS servers.

In many organizations, authority for DNS services often falls into IT operations (especially where Active Directory plays a key role in internal DNS) or network operations, particularly where ISP services are used.

The first step toward making sure the enterprise's DNS services are secure and reliable is defining and documenting the governance structure and processes. If ownership and responsibility for maintenance, updates and troubleshooting are clearly defined, routine and emergency issues can be addressed during the course of business, instead of creating a scramble each time or totally missing incidents and maintenance.

Some key areas to define include:

1. Identification and inventory of existing DNS services and resources, both internal and external, with responsibility/ownership assigned for each
2. Configuration and change management processes and responsibilities to ensure that secure DNS services are maintained
3. Vulnerability assessment and mitigation processes and responsibilities to ensure that DNS threats are proactively identified and mitigated
4. Budgetary needs and allocations to maintain reliability and security levels of DNS services

The role of the security group in each of these areas should be clearly delineated. It is not necessary for the security group to own all of the areas, but it is common to have the security group responsible for vulnerability assessment and important that security be part of all change reviews.

During the process of ensuring ownership and responsibility, enterprises also should define required availability and performance levels for DNS services and review the existing DNS delivery architecture to determine whether it meets those requirements currently and across any near-term network expansion plans.
For example, this review can help drive decisions about transitioning from software-based DNS services to a more reliable/higher performance appliance-based approach or third-party managed services.

The next step in ensuring DNS reliability is defining an appropriate level of security controls around enterprise DNS services. Security controls should be required by policy for internal DNS services and included as part of evaluation criteria and contractual requirements for any external DNS services or managed services that will be used.

**Implementing the Critical Security Controls**

A good starting point for this effort is the “Critical Security Controls” framework, coordinated by the Council on CyberSecurity, which represents a broad security community consensus of the security controls most effective for avoiding or stopping real-world threats. Figure 2 shows a summary of the various sections, with the controls highlighted in red representing those that include DNS security considerations.

![Figure 2. The Critical Security Controls (Source SANS 2014)](image)

---

19 [www.counciloncybersecurity.org/critical-controls](http://www.counciloncybersecurity.org/critical-controls)
While all of the controls are appropriate to an effective, efficient security program, the following sections discuss those that have the most direct applicability to DNS services and how they can be applied. Where possible, enterprises should address all of the referenced controls to keep DNS services secure and reliable. Where resources are limited, the Critical Security Controls (CSCs) should be implemented in the order presented.

Critical Controls 2, 3, 10—Software Inventory and Secure Configurations

Vital to keeping an enterprise’s DNS services secured is identifying the DNS-related software in use (resolvers, servers, etc.) and ensuring it is up to current patch levels and configured to best security practices. For example, in the first five months of 2014 alone, BIND software had five security advisories that required patching or configuration checking.20

DNS services may be delivered from PCs, servers and network equipment or may involve external parties, such as ISPs. Keeping enterprise DNS services secure requires that all servers, routers and firewalls running DNS services are configured correctly and not compromised. This can be a complex undertaking and often drives enterprises to move to dedicated, hardened DNS appliances—which reduce complexity, are more secure, and are simpler to configure and manage. Alternatively, some enterprises move to managed DNS services, thereby outsourcing the configuration-management effort.

In general, security increases when complexity goes down. Appliances generally reduce complexity more than software approaches do. However, the decision to base DNS services on software, appliances, managed services or some combination is unique to each organization and will be driven by business, organizational and budgetary constraints.

Critical Security Control 5—Malware Defense

DNS servers should be protected from the installation of any malicious executables that are part of advanced targeted attacks. Deploying traditional AV software on DNS servers can help protect them. More effectively, whitelisting software can be run on DNS servers to make sure unapproved software cannot be installed. Another option is to use DNS server appliances that have locked-down software configurations.

20 www.isc.org/downloads/software-support-policy/security-advisory
As mentioned earlier, modern attacks often use DNS services at several stages as they attempt to insert targeted malware for initiating data breaches. Critical Security Control 5 points out in sub-control 11: “Enable domain name system (DNS) query logging to detect Hostname lookup for known malicious C2 (command and control) domains.” This log data can be used as an early indication of a malware problem.

More advanced threats bypass traditional security mechanisms, so detecting these threats early before they can exfiltrate data is essential. DNS can be used as a detection asset for many of these cases. Utilizing RPZ feeds in the DNS server to keep a constantly updated blacklist of known malicious domains and using the DNS server itself to block malicious DNS queries to these bad domains can be a highly effective way of both detecting and disrupting advanced threats (see Figure 3).

**Figure 3. How Response Policy Zones Work**

**Critical Security Control 13—Boundary Defense**

To limit the attack aperture, internal DNS servers should be located behind next-generation firewalls and intrusion prevention systems that provide DNS-aware filtering capabilities. Another option is to put DNS servers in network segments protected by firewalls that focus on DNS protocols. This is a necessary precaution, but it does not provide complete security, since advanced targeted attacks often compromise user PCs or laptops and then launch the next stage of an attack from inside the firewall.
DNS and Regulatory Compliance (CONTINUED)

DNS services also need protection from DDoS attacks (see Figure 4). Since DDoS attacks essentially have unlimited bandwidth, it is impossible to simply oversize or over-provision a DNS server. Nor is simple DDoS protection that relies on rate limiting effective against modern DDoS attacks, since these kinds of attacks now also mix in resource starvation attacks that use low bit rate, specially crafted packets to force a server to run complex processes, causing the server to bog down or crash.

Maintaining DNS integrity is essential to prevent DNS hijacking, which can compromise boundary defenses.

DNS appliances should be installed behind boundary defenses that limit the attack aperture, but also must include updatable capabilities for protecting themselves against evolving attacks that get through such perimeter defenses. Maintaining DNS integrity is essential to prevent DNS hijacking, which can compromise boundary defenses—as was seen in the Syrian Electronic Army attack.
Critical Security Control 19—Secure Network Engineering

Securely architecting DNS services is one of the most important elements of Critical Security Control 19-3: “Deploy domain name systems (DNS) in a hierarchical, structured fashion, with all internal network client machines configured to send requests to intranet DNS servers, not to DNS servers located on the Internet. These internal DNS servers should be configured to forward requests they cannot resolve to DNS servers located on a protected DMZ. These DMZ servers, in turn, should be the only DNS servers allowed to send requests to the Internet”21 (see Figure 5).

![Figure 5. Critical Security Control 19: Secure Network Engineering](image)

According to CSC 19, there should be a minimum of two network segments or zones: the external-facing DMZ and the internal trusted network. Many organizations deploy additional zones, such as develop and test, data center or PCI segments. To meet the demands of “bring your own device” (BYOD), enterprises often establish a guest zone (for nonemployee access to network services) and a limited access zone (for employees using personally owned devices).

---


22 “CSC 19 System Entity Relationship Diagram,” www.sans.org/critical-security-controls/control/19
Those network segments should be separated by the Boundary Controls discussed in section CSC 13. All connections to DNS services should be limited between zones to only those absolutely necessary and explicitly allowed. By monitoring the DNS requests made within and between zones, enterprises can also gain early visibility into potential malware events or compromises.

Another part of secure network engineering for DNS is ensuring availability of services. To accomplish this, load balancing, switchover and high-availability configurations should be deployed.

**Critical Security Control 20—Penetration Testing**

As discussed previously, attackers often target DNS services for disruption and compromise. They often exploit multiple vulnerabilities (in both software and people) to launch complex, multistage campaigns. Penetration testing processes and tools essentially act as “attackers in a box” and use those same techniques to see whether sensitive information can be breached or business services disrupted.

A typical external penetration test will expose potential paths attacks could use to affect an enterprise's DNS services, as well as ways attackers might exploit an enterprise's DNS resources to launch attacks within its firewall or against other companies.

More modern penetration testing adds “inside-out” penetration testing, in which an internal PC is compromised (perhaps through compromised DNS services) and the testing demonstrates potential impacts. All penetration testing plans should include DNS services as targets and as services to be used in the simulated attack.
What’s Next for DNS Security?

Three major trends will have an impact on IT overall and how DNS services are provided and secured: virtualization and cloud, BYOD and the Internet of Things (IoT).

**Virtualization and Cloud**

The majority of new server workloads are being established on virtual server images, either in enterprise data centers or in public software-as-a-service or infrastructure-as-a-service (IaaS). Over time, enterprises tend to first virtualize their local data centers and then evolve to a hybrid architecture for IaaS services to meet temporary or spiking capacity needs.

One of the major benefits of such services is faster provisioning time and lower operational cost. However, the ability to quickly spin up new resources is highly dependent on the speed and reliability of DNS services.

To maintain the security and reliability of DNS services across this complex hybrid architecture, DNS management and reporting tools need to support the APIs used by VMware and other virtualization infrastructures. The security controls discussed in the previous section, such as configuration management and boundary security, also need to be provided.

The use of external SaaS or IaaS services means that requirements for DNS availability and security should be included in evaluation criteria and requirements for procurements of those services.

**Bring Your Own Device**

More smartphones and tablets than PCs are now being sold, and most IT organizations are required to support personally owned devices for business use. There are two DNS-related security issues:

1. Network access control technology can be used to detect when a device connects to the enterprise network and to determine whether it is a managed device or a personally owned device. By controlling DHCP and DNS services on a guest or limited-access network, enterprises can manage the risk of allowing personally owned devices.

2. Android and iOS devices include DNS resolver software. Attackers can target those devices to launch the same attacks they launch against PCs. Configuration and vulnerability assessment controls must ensure that mobile device DNS settings are not corrupted.
The Internet of Things

A recent SANS Survey on the IoT showed that security professionals are already dealing with the first of several waves of Internet-connected “things” and have begun to plan for the challenges of the next wave of more diverse, more complex devices. The sheer quantity of things that will be connected leads to scalability and manageability problems. Almost 90 percent of respondents recognized that changes to security controls will be required, with 50 percent believing major (if not complete) enhancements and replacements for many controls will be required.23

Internet-connected computing related to smart building and industrial control systems and medical applications were the most commonly cited concerns after consumer products. While these types of applications do not receive much IoT hype in the press, the use of embedded computing in those devices (as opposed to the layered operating systems and applications in PCs and servers that IT is accustomed to managing and securing) will cause major breakage in existing IT management and IT security visibility, vulnerability assessment, configuration management and intrusion prevention processes and controls, including DNS services.

To deal with the scale and scope of the IoT, DNS architectures need to support scalable, distributed approaches for service delivery and for updating and reporting.

Without proper consideration in an enterprise’s security plans, DNS provides an easy point of entry for disruption and unauthorized information access. Since DNS security has not been appropriately addressed in many organizations, advanced attacks have recently increased. However, several ways exist to help mitigate the problems caused by DNS vulnerabilities and instead use DNS as an asset in the security chain. Awareness is the first step toward implementing a more secure enterprise, followed by application of Critical Security Controls and awareness of trends toward more connectivity and devices.

Enterprises deploy power conditioning and uninterruptible power supplies to make sure data centers stay reliable and available, but in the Internet age DNS services are just as mission critical as electricity. IT and security organizations should establish clear governance of DNS services, emphasize security and reliability in the procurement and deployment of all DNS elements and services, and should also take advantage of the ability of well-run DNS services to improve detection and disrupt advanced targeted attacks.
John Pescatore joined SANS as director of emerging security trends in January 2013. He has 36 years’ experience in computer, network and information security. Before joining the SANS Institute, John was Gartner’s lead security analyst for 13 years, working with global 5000 corporations and major technology and service providers. Before joining Gartner, he was senior consultant for Entrust Technologies and Trusted Information Systems, where he started, grew and managed security consulting groups focusing on firewalls, network security, encryption and public key infrastructures. Prior to that, John spent 11 years with GTE developing secure computing and telecommunications systems. John began his career at the National Security Agency, where he designed secure voice systems, and the United States Secret Service, where he developed secure communications and surveillance systems. He holds a bachelor’s degree in electrical engineering from the University of Connecticut and is an NSA-certified cryptologic engineer. He is also an extra-class amateur radio operator, callsign K3TN.

SANS would like to thank this paper’s sponsor: