Infoblox®
CONTROL YOUR NETWORK

WHITEPAPER

Top Five DNS Security Attack Risks and How to Avoid Them

How to Effectively Scale, Secure, Manage, and Protect Your DNS

Table of Contents

> "If your data center is not available, all the compliance or data integrity in the world is not going to help your customers, business, or your brand. DDOS is the number one threat to the availability of data center resources..."
>
> Rob Ayoub, Frost and Sullivan, Global Program Director, Network Security

Executive Overview

Cyber attacks on Domain Name System (DNS) servers represent one of the most significant threats to Internet security today. Because DNS is used by nearly all networked applications – including email, Web browsing, ecommerce, Internet telephony, and more – these types of attacks threaten the very basis of modern communications and commerce. Whether conducted for financial motives, political gain, or the notoriety of the hacker, the damage from a DNS attack can be devastating for the target organizations.

This paper will highlight how traditional DNS infrastructure deployments can actually increase the risks of DNS attacks. The paper also covers best practices and options for a hardened DNS layer that can minimize the risk of experiencing a DNS attack by identifying the symptoms and implementing a response faster.

DNS Attacks Are on the Rise

Today's headlines are filled with reports of successful DNS attacks.

- AT&T suffers DNS outage caused by DDOS attack
- Broadcaster Al-Jazeera knocked offline with DNS attack
- 65,000 Internet users in the United States lose connectivity because of DNS changer malware
- Bank of America customers cannot access website or account information because of a DOS/DDOS attack

That's just four headlines reported by the press, but there are likely thousands of other DNS attacks that never reach the press because of their size or because the organization wants to keep the information private. The motives for hacking into an organization's internal servers can be for financial gain, but with many DNS attacks, the intended objectives can be political gain or notoriety.

Domain Name System (DNS) servers are essential network infrastructure that map domain names (e.g., yahoo.com) to IP addresses (e.g., 66.94.234.13), directing Internet inquiries to the appropriate location. Domain name resolution conducted by these servers is required to perform any Internet-related request from Web browsing, email and ecommerce to cloud computing.

External Name Server Basics

External name servers provide two important services to a corporate network: Resolving Internet domain names, usually on behalf of internal resolvers and name servers; and answering queries about the company's domain names for name servers on the Internet. The former role is critical to accessing web sites, sending electronic mail, and just about any other use of the Internet by the company and its employees. The latter role is necessary for the company to conduct business on the Internet, for access to the company's web site, for inbound electronic mail delivery, and more.

In well-designed DNS architectures, these roles are split between two sets of external name servers. For this paper, servers that assist in the resolution of Internet domain names will be referred to as "forwarders," and name servers that answer queries about the company's domain names as "authoritative name servers."

DNS Security Flaws and Management Challenges

There are several architectural challenges and security flaws inherent in the original design of the DNS protocol for external name servers.

Complex Management

Although most administrators recognize the importance of external name servers, the occasional misconfiguration or operational mistake is inevitable, largely because of the complexity of managing most name servers. For example, nearly every administrator of a BIND name server—the preferred make of external name server—has made a mistake and introduced a syntax error into a named.conf file or zone data file (a similar risk of human-error is also high when using non-BIND solutions, like Microsoft). However, a syntax error in a zone data file, gone unnoticed, will render the name server unable to load that zone, and will result in a name server returning either old data or no data. Worse, a syntax error in the name server's configuration file will prevent the name server from starting.

Attack Vulnerabilities

Many administrators don't take the simple precaution of configuring their forwarders to process recursive queries only from internal IP addresses. This may be because they don't know how or because they don't understand the implications of leaving an external name server "open" to recursive queries.

For example, an inherent vulnerability occurs when a name server allows recursive queries from arbitrary IP addresses. This approach is vulnerable to cache-poisoning attacks, in which a hacker can induce the name server to cache fabricated data. In the most famous attack of this kind, Eugene Kashpureff poisoned the caches of hundreds of Internet name servers, leading them to direct users accessing www.intemic.net to the IP address of a web server run by an organization called the AlterNIC.

It's difficult to overstate the damage an attack like this could cause today: a hacker could redirect traffic intended for a bank's web site to a web server with a replica of the site's content, and steal account numbers and passwords; or siphon off traffic meant for a web-based merchant to an identical web site and capture credit card numbers.

Difficult Upgrades

With BIND and Microsoft name servers, upgrading to a new version of the software is non-trivial. Upgrading involves, at the very least, downloading new source code, compiling, testing, and installing it. In many cases, incompatibilities with previous versions force administrators to modify configurations or zone data or, worse, actually read the documentation. Consequently, many administrators put off the crucial task of upgrading their name servers when new versions are released.

This can have disastrous effects. Months after a buffer overrun was discovered and patched in the code, the LiOn worm exploited the vulnerability to infect hundreds of name servers around the Internet. The worm also installed a "rootkit," which the worm's author (or anyone else familiar with the worm's operation) could use to gain root access to the infected host. The hacker could have modified or destroyed zone data, or in some circumstances could have used the name server as a stepping-stone into the unprepared company's network. Even today, it is highly likely there are still name servers on the Internet that were compromised during LiOn's spread, unknown to their administrators.

Ever-Growing Attack Options

One of the biggest challenges for IT organizations is the varied and ever-changing options for DNS attacks. Common attacks include:

Attack Type	Description
TCP SYN Flood Attacks	A DDoS DNS attack, typically leaves "hanging" connections by flooding DNS server with new TCP connection requests until the target machine fails.
UDP Flood Attack	A DDoS DNS attack, sends a large number of UDP packets to a random port on the targeted host to confuse or overwhelm the target machine until it fails.
Spoofed Source Address/ LAND Attacks	A DDoS DNS attack, sends a spoofed TCP or UDP packet with the target host's IP address to an open port as both source and destination. The reason this attack works is because it causes the machine to reply to itself continuously, therefore making it essentially unavailable to other applications.
Cache Poisoning Attacks	A core DNS attack, poisons DNS cache typically in order to send legitimate requests to malicious websites.
Man in the Middle Attacks	A core DNS attack, a compromised machine in the network can penetrate and take over the entire DNS structure and then route legitimate requests to malicious websites.

There are many other ways a DNS server may be compromised, and newer, more complex methods are being devised all the time in the underworld of botnets, but these five happen with the most frequency and have characteristics common to many others.

Aren't General-Purpose Computers Good Enough for DNS?

Most companies deploying external name servers have chosen computers running general-purpose operating systems as their platform. While this deployment may be inexpensive to deploy and may function, general-purpose servers have several major risks that actually increase the propagation of DNS attacks:

- General-purpose operating systems require significant knowledge and effort to secure. Securing a UNIX OS requires understanding which network and system services should be disabled and how to disable them, which patches are necessary, which kernel modules and device drivers are needed and which are extraneous, how to configure UNIX packet filters, and much more.
- In addition to patching the OS, the name server code itself frequently needs to be upgraded to address vulnerabilities or simply to add new features. This usually must be done separately from upgrading the operating system.

- General-purpose OSs support user logins. Hackers can use these to gain administrator-level access to the operating system. Even in the best case, with secure logins and benign users, those users may inadvertently destabilize the operating system by installing software that consumes system resources, by filling disks, etc.
- Most general-purpose operating systems offer all-or-nothing administration, empowering administrators to either change any aspect of the name server's configuration and zone data, or nothing. Giving a junior administrator only limited access to the name server is nearly impossible.
- Configuration of a name server's internal security mechanisms is difficult, and consequently often ignored by even seasoned administrators.

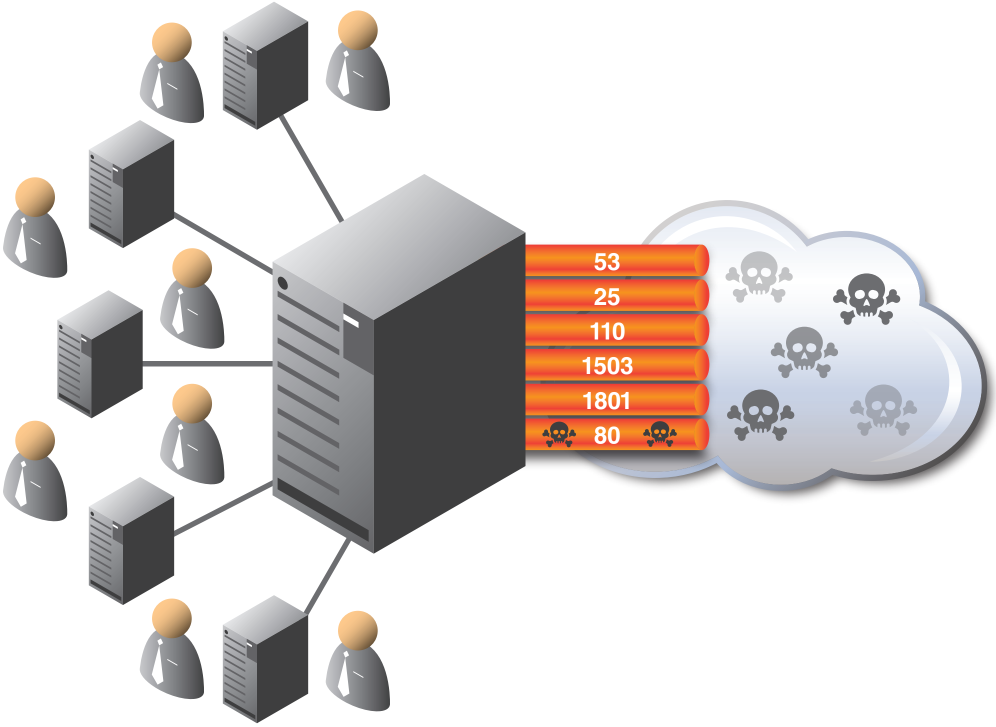

Figure 1. The conventional DDI approach is to use computers running general-purpose operating systems as their platform.

Shortcomings of the conventional approach include:

- Many open ports are subject to attack
- Users have OS-level account privileges on server
- Requires time-consuming manual updates
- Requires multiple applications for device management
- Inconsistent or outdated security procedures

Securing Your DNS Infrastructure and Applications

Instead of relying on general-purpose servers and hoping your internal IT team will never leave a hole in the system, organizations can leverage purpose-built appliances with intuitive interfaces and embedded expertise to improve DNS availability and reduce the risk of DNS attacks.

Most IT executives understand the value of purpose-built solutions but implement general purpose servers because they think they are less expensive. However, the focused approach reduces the risk of configuration errors, supplies the expertise you need to have available, and reduces the cost of implementation and maintenance due to the risk reduction and staff empowerment.

The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide origin authentication of DNS data, authenticated denial of existence, and data integrity.

The Infoblox Approach to DNS Security

Infoblox helps organizations implement robust, secure, and manageable DNS infrastructure. By leveraging hardened appliances that run on patented Grid™ technology, users eliminate the architectural challenges of general-purpose servers and reduce the risk of DNS attacks.

The Infoblox platform, Trinzic DDI, is an appliance-based network services software suite delivering state-of-the-art DNS, DHCP, and IP address management (DDI), with seamless and agentless integration to Microsoft servers. This Grid technology is an advanced, highly available, fault-tolerant, and massively scalable network solution that improves management and availability with centralized management and robust failover capabilities.

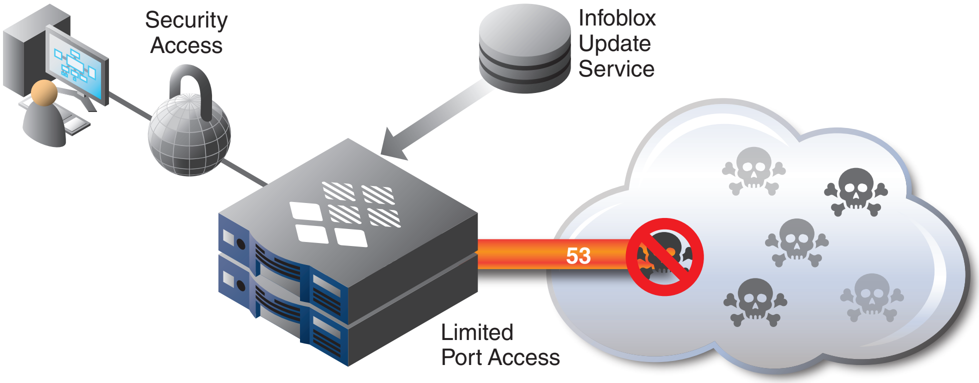

Figure 2. The Infoblox DNS Appliance approach uses dedicated hardware and a hardened, purpose-built operating system to ensure DNS security.

Benefits of Purpose-Built Appliances

Infoblox products deliver the automated network control needed to keep today's complex networks up and running. Infoblox customers can expect a significant increase in network availability and a large reduction in network capital and operational expenses, along with improved management. These improvements are why the world's largest banks, the largest retailers, the largest manufacturers and over 30% of the Fortune 500 run their networks on Infoblox.

Infoblox provides:

- **Security from the Ground Up.** Infoblox appliances are built from the ground up with security in mind. With an overall design objective to defeat attempts to hack into the appliance, the operating system is not off-the-shelf, the kernel has been hardened, and only required interfaces are enabled. No possibility of errant root access greatly eliminates unnecessary risk.
- **The Ability to Block Internal and Co-Lo Threats.** The Infoblox database is password-protected, and even configuration files are not stored in clear-text. Password standards are configurable by the administrator only. Even individuals with physical access cannot connect to the device or view the LCD screen without authorization.
- **Multi-Layer DDoS Protection.** Infoblox provides multi-layered protection against even massive, botnet-driven Distributed Denial of Service (DDoS) attack with features such as intelligent DDoS detection, traffic rate limiting, Anycast capabilities to distribute load, and more.
- **The Richest Set of Security Functionality in the Market.** Infoblox has built a comprehensive set of security extensions to BIND that as a whole provide the richest functionality in the market as well as the ability to leverage partner capabilities. These capabilities include blacklisting, NXDOMAIN Redirection, DNSSEC, HSM, hardware authentication, and more.
- **The Highest Levels of Security.** The Infoblox system runs in some of the most secure environments in the USA and the world. While we aren't allowed to even discuss many of these customers, our current certifications include JITC Certifications for IPv6, and Common Criteria EAL-2 Certification.
- **Protection against Man-in-the-Middle Attacks.** Security throughout the Infoblox Grid prevents Man-in-the-Middle attacks through the use of VPN, encrypted communications, HTTPS, separate management port, and other tools.
- **Transparency for Regional Disasters.** The Infoblox Grid architecture with redundant Grid Masters ensures that your DNS lifeblood will continue to flow, automatically and transparently, even if a regional disaster strikes.
- **Precise Control Over Who Gets What.** The ability to set granular permissions at the object level means that you can grant access exactly and only to what's needed by that device, application, or person.
- **Very High Availability.** The Infoblox Grid architecture provides very high availability by design. Infoblox's security is not impacted by operating system updates, database patches, and other server-related tasks. Once Infoblox issues a security fix, it can be immediately resolved by a live or scheduled code push.
- **Automatic Audits.** Infoblox provides full logging of all administrative changes and reporting capabilities, to ensure that you can audit security both externally and internally.

Attack Type	How Infoblox Counters
TCP SYN Flood Attacks	The Infoblox 4030 appliance tracks the number of SYN requests per second. If the number of SYN requests goes above a threshold the code examines the requests to see if clients are responding with ACK’s. If not, then the request is dropped.
UDP Flood Attack	If the Infoblox 4030 appliance detects that a high number of packets with a very small payload are being received from a client or pool of clients, it first prioritizes requests then uses a selective packet discard mechanism to throttle traffic.
Spoofed Source Address/ LAND Attacks	The Infoblox 4030 appliance validates all incoming packet source addresses. If it detects that the source address is its own address it drops the packet, thereby nullifying this attack.
Cache Poisoning Attacks	Security throughout the Infoblox Grid prevents cache poisoning attacks via use of VPN, encrypted communications, HTTPS, separate management port, and more.
Man in the Middle Attacks	Security throughout the Infoblox Grid prevents Man-in-the-Middle attacks via use of VPN, encrypted communications, HTTPS, separate management port, and more.

Conclusion

DNS attacks are on the rise from both the outside and the inside. In fact, a recent study found that DNS attacks grew by 600% in 2011 alone ! With this massive growth, it appears that the current infrastructure is under unremitting and escalating attacks, and IT organizations must find a better way to deal with this risk.

By employing rigorous design practices for hardware and software, selecting the most secure elements, proactively eliminating vulnerabilities, locking down systems, vigilantly monitoring security alerts, and responding quickly and proactively, Infoblox ensures that its customers’ core network services remain secure and robust in these turbulent times.

For more information on Infoblox solutions, please visit www.infoblox.com .

CORPORATE HEADQUARTERS:

+1.408.986.4000

+1.866.463.6256

(toll-free, U.S. and Canada)

info@infoblox.com

www.infoblox.com

EMEA HEADQUARTERS:

+32.3.259.04.30

info-emea@infoblox.com

APAC HEADQUARTERS:

+852.3793.3428

sales-apac@infoblox.com