DNS QuickSecure Solution™

Infoblox
CONTROL YOUR NETWORK

Overview

Newly developed attacks on Domain Name System (DNS) servers represent one of the most significant threats to Internet security in the last decade. Because DNS is used by nearly all networked applications—including email, Web browsing, ecommerce, Internet telephony and more—the new attacks threaten the basis of modern communications and commerce. No DNS system is completely immune, and there are no comprehensive quick fixes. Network security experts and responsible vendors have rallied to address the flaws, and initial, short-term fixes have been released. However, the longer-term solutions to securing DNS are still being debated, and there have already been successful attacks on patched DNS systems. Experts agree that networked organizations need to prepare for an extended "arms race" of new DNS attacks followed by incremental fixes until a comprehensive solution is developed. The Infoblox DNS QuickSecure Solution provides organizations with a first line of defense, establishing in effect a "DNS Firewall" that works with existing DNS infrastructure and provides a hardened DNS layer that can be upgraded quickly and easily, with no downtime.

New Attacks on DNS Threaten the Security of All Internet Applications

On August 6th 2008 Dan Kaminsky, an independent security researcher, released details of a new way to exploit flaws in the security of the DNS protocol. DNS is the "Internet phone book", translating names (e.g. www.google.com) into Internet Protocol (IP) addresses (e.g. 64.233.167.99). This essential translation function is the foundation of all Internet applications, including Web browsing, email, ecommerce, hosted applications (e.g. SalesForce.com), and more. The new attack, which results in "cache poisoning", enables an attacker to pollute the data in DNS servers—including those managed by your company and your service provider—with bogus information that re-routes your traffic to the attacker's sites by changing data in DNS to point to their IP address instead of yours. Once traffic is re-routed attacks can take many forms, most of which are extremely difficult to detect:

- An attacker may impersonate your Web presence and collect private data from your customers, partners and employees.
- Your email may be sent to an intermediary server where it is opened and even modified before reaching you or your intended recipient.
- Your anti-spam system can be fooled into allowing malicious email and blocking legitimate email.
- Your Web traffic may be sent to a site that looks like your intended destination (say, your bank's Web site) but is operated by attackers, where they can collect your user name, accounts and passwords.
- An attacker can use the "Forgot Password" function on your Web site to retrieve your users' passwords.
- Your Web traffic or ecommerce transactions may be routed through an intermediary site where they are "sniffed" and modified before being passed on to the intended destination.

The full scope of the new attacks on DNS is still being understood, but the conclusion is clear: The exposure is very serious, and it affects every individual and organization on the Internet:

> "There are already credible reports of increased DNS cache-poisoning attacks 'in the wild,' which indicate that attackers are attempting to exploit this vulnerability. Emerging technical details have caused Gartner to revise its original view of the potential enterprise impact of this vulnerability and the urgency of the enterprise response to it." August 8, 2008
>
> Gartner

DNS QuickSecure Solution™

Infoblox
CONTROL YOUR NETWORK

DNS Systems Must be Patched Now — and in the Future

Internet security and DNS experts have been universal in their calls for organizations to update their DNS software to the latest versions with short-term fixes that reduce the risk of a successful attack. Many vendors—including Microsoft, Cisco, Infoblox and others—cooperated on implementing the fixes and had updated software available on July 8, 2008, the day that CERT issued an Advisory warning of the new exploit and the need to patch. The global response has been less than complete, with some reports claiming that as many as 70%, and others reporting that as few as 50% of organizations had patched their DNS systems. In any case, the first patch will not be the last as it only made the attacks more difficult, but not impossible to implement. And since DNS is often used to verify the authenticity of certificates and other forms of identity, solutions such as SSL and OpenID are also vulnerable. Successful attacks against patched DNS servers have already been reported, heralding a new DNS security arms race.

The Internet technical community is evaluating solutions that address the fundamental security flaws inherent in the original design of the DNS protocol, including widespread deployment of DNSSEC. The search for a longer term solution is ongoing and urgent, but the timeframe for an accepted solution is not known. In the meantime, it's clear that there will be a cycle of short-term fixes and patching, followed by new exploits, followed by new patches, until a long-term solution is identified and implemented. Organizations therefore should consider means to fortify their DNS systems and prepare for a migration to a new, more secure DNS infrastructure.

Secure Your DNS Infrastructure — and All of Your Applications — Quickly and Easily

The Infoblox DNS QuickSecure Solution™ enables organizations to protect their current DNS infrastructures without major upgrades, and provides a solution for dealing efficiently and easily with the coming DNS security arms race.

The Infoblox DNS QuickSecure Solution uses a protective layer of secure DNS servers between an organization's existing DNS servers and the Internet to function as a "DNS Firewall" that is easy to update as new exploits and subsequent patches are released. The Infoblox QuickSecure Solution is made possible by the following:

- DNS servers are vulnerable to cache-poisoning attacks if they process a particular type of DNS request, called a "recursive query," over the public Internet to anonymous, non-trusted DNS servers. These types of requests are made by DNS servers when they don't know the answer to a client request and need assistance from another DNS server. A layer of Infoblox appliances installed between existing DNS servers and the Internet shields the internal DNS servers and allows the appliances to handle recursive queries bound for the Internet, making the internal servers immune to cache poisoning.
- The Infoblox Reporting Toolkit provides real-time graphs that make it easy to monitor DNS activity and spot attacks. New features in the Infoblox NIOS software provide automatic alerts when attack thresholds are exceeded, and query rate limiting enables administrators to thwart attacks in progress.

Infoblox appliances have built-in high availability operation that enables pairs of appliances to operate with zero downtime, even during software upgrades. Infoblox appliances support Anycast, which enables DNS requests to be automatically re-routed away from servers that may be down or under attack. Infoblox Grid technology enables a collection of Infoblox appliances to be managed as a single system. Operations such as software upgrades, system-wide backup and restore, and others can be executed with a single operation, and with no system downtime.

Infoblox appliances are dedicated, hardened systems that are inherently more secure than standard server hardware and operating systems. Infoblox is a member of CERT and other security organizations, has advance notice of new exploits and issues security patches in hours when necessary. Using Infoblox appliances and Grid technology enables customers to maintain a robust, dynamic DNS perimeter without having to replace existing DNS infrastructure. The Infoblox NIOS™ operating system provided with all Infoblox appliances can be configured to support any DNS role—including authoritative servers, secondaries, caching servers, and any combination—so organizations can easily migrate to a best-practices DNS architecture

over time with no loss of investment. Infoblox appliances can support a wide range of services on a single appliance in addition to DNS—including DHCP, IPAM, RADIUS, FTP/TFTP/HTTP, NTP and others, providing resiliency, security, and centralized management for all core network services.

The Infoblox DNS QuickSecure Solution can be implemented easily in any existing environment. The figures below show an example using an existing infrastructure containing both Microsoft DNS and BIND, however it applies to any other DNS implementation:

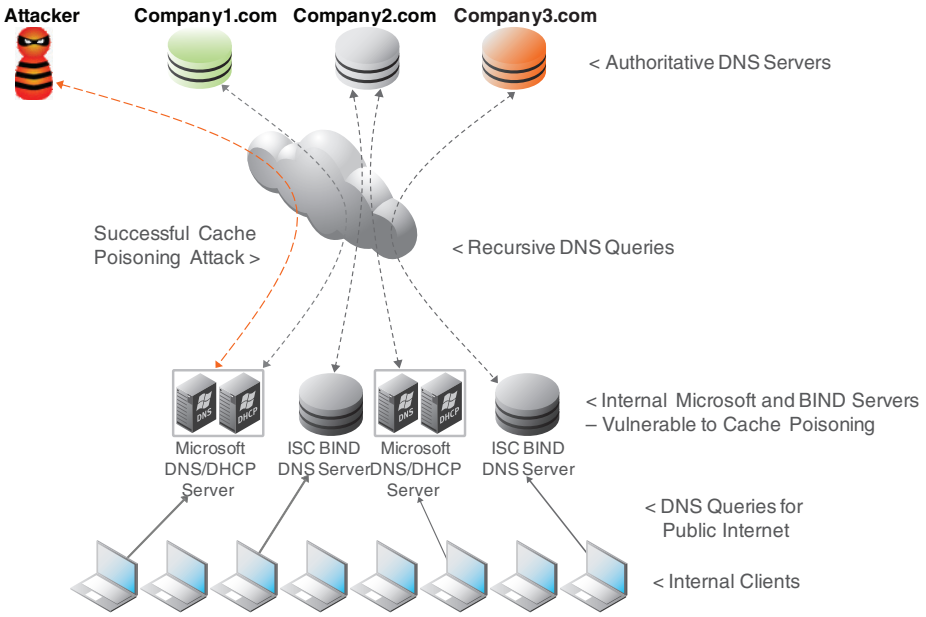


Figure 1: Vulnerable Design

A typical existing DNS implementation will require frequent, disruptive patching of internal DNS servers.

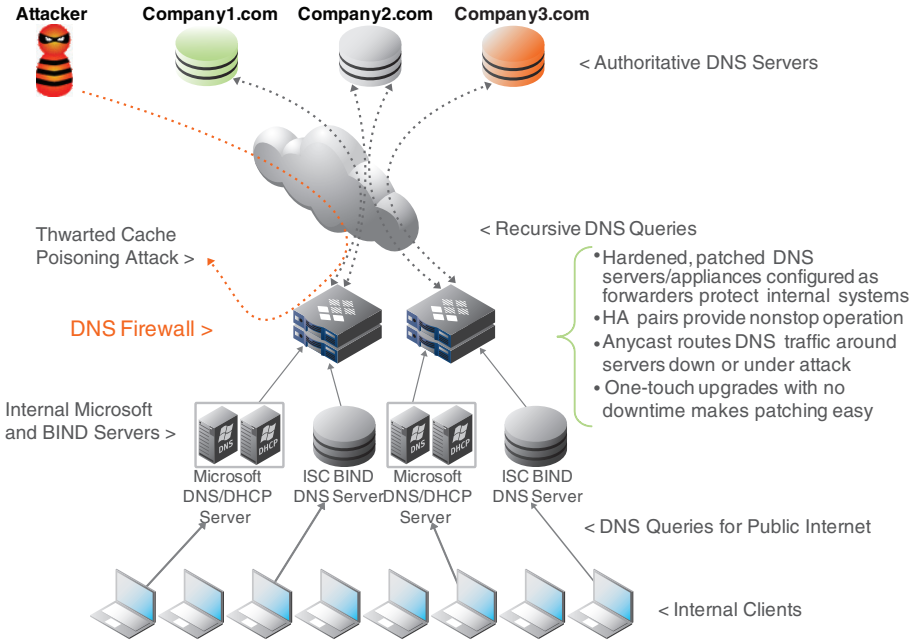


Figure 2: Next Generation Infoblox QuickSecure Design

A secure grid of Infoblox appliances configured as forwarders can be added to any existing infrastructure to provide a secure "DNS Firewall" that can be updated quickly, with zero downtime.

Attack Alerting and Mitigation Features Provide Real-time Detection and Prevention

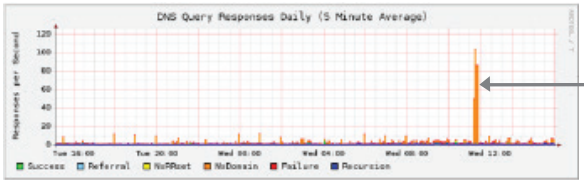
Once the Infoblox QuickSecure solution is deployed, it significantly narrows the exposure of a company and helps defend and prevent cache poisoning and other future attacks. However, this is equivalent to putting a lock on the front door of a building – it doesn't prevent somebody from trying to break in. Effective security involves "security in-depth" which means that you lock the door but then also provide an alarm in case somebody attempts to break in, as well as a guard to stop them if they do try to attack. Infoblox is adding features which provide effective monitoring, alerting and attack mitigation for cache poisoning attacks.

The recent cache poisoning attack has tell-tale signs which can be monitored and, if detected, used as a basis for sending alerts to administrators. Infoblox is adding monitoring and alerting for two different signatures of the attack, i.e. mis-matched DNS message IDs and mis-matched UDP ports in responses. For each system that is a recursive server, the administrator can set a threshold for each parameter. When the threshold is exceeded, an alert is sent via email and/or SNMP trap.

In addition, if customers are using a SNMP reporting package, these two parameters will be made available in the Infoblox custom DNS MIB which will allow integration with existing monitoring systems.

DNS Protocol Monitoring

— Real-time reporting

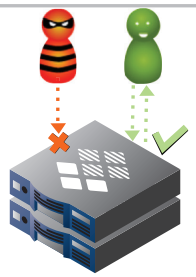


Attack Alerts

— Email/trap when attack profile thresholds exceeded

Attack Mitigation

— Limit DNS query rate by source address and other parameters



Infoblox also provides customers with the Infoblox Reporting Toolkit which can help administrators monitor their Infoblox systems. The toolkit provides graphs of DNS message types including another tell-tale sign of an attack in progress. Above is an example graph that illustrates the drastic increase indicating that a system is under attack.

Infoblox is also adding the ability to defend or stop an attack. New commands allow an administrator to rate-limit or stop all traffic going to an IP address or network. For example, if somebody is trying to poison the www.bank.com DNS information, the administrator can stop or limit all recursive queries (and spoofed responses) from the IP addresses of the bank.com DNS servers.

DNS QuickSecure Solution™

Infoblox
CONTROL YOUR NETWORK

The combination of monitoring, alerting and mitigation provide DNS administrators the tools they need to defend against today's attacks, and the Infoblox grid enables fast, downtime-free upgrades that ensure protection when new attacks force additional updates and changes to DNS.

To learn more about Infoblox solutions or products, please contact us at info@infoblox.com or call +1.408.986.4000.

About Infoblox

Infoblox (NYSE:BLOX) helps customers control their networks. Infoblox solutions help businesses automate complex network control functions to reduce costs and increase security and uptime. Our technology enables automatic discovery, real-time configuration and change management and compliance for network infrastructure, as well as critical network control functions such as DNS, DHCP and IP Address Management (IPAM) for applications and endpoint devices. Infoblox solutions help over 6,100 enterprises and service providers in 25 countries control their networks.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com