Are Your DNS Servers as Secure and Available as the Rest of Your Network?
Are Your DNS Servers as Secure and Available as the Rest of Your Network?

If nothing about your business depends on the Internet, and none of your sensitive data is connected to it, then maybe you don’t have to worry about security issues related to your Domain Name System (DNS) servers.

If, on the other hand, your internal communications, relationships with suppliers, marketing efforts, customer service, and even sales take place via email, web sites, and HTTP file transfer, then functioning DNS servers are essential to users finding applications and each other—and you should be very concerned because DNS is probably a hole in your security.

In 2012, 7.8 million new malware threats emerged. Mobile threats grew by 1,000 percent.\(^1\) Eight hundred and sixty-five successful breaches compromised 174 million records. Sixty-nine percent of them utilized malware. Eighty-three percent took weeks or months to discover.\(^2\) And according to an October 2012 study by the Ponemon Institute, the annual cost of malware breaches across 13 industries, ranging from defense to retail, averaged $8.4 million.

![Average annualized cost by industry sector](chart.png)

*Industry was not represented in the FY2010 benchmark sample.

Source: Ponemon Institute, October 2012

Malware is a serious financial threat for every major business sector.

Like the legal IT activities they bring under attack, hacking, infiltration, sabotage, and data theft just keep getting better. We’re not talking about mischievous teenagers anymore. We’re talking about government cyberwar teams, censors in totalitarian regimes, unscrupulous competitors, hacktivists, and international criminals.

\(^1\) McAfee Threats Report: Third Quarter 2012

\(^2\) Verizon Security Study 2012
Is DNS a Hole in your Security?

In the midst of this heightened danger, DNS servers are an often-overlooked weak point that traditional signature-based security and even contemporary security intelligence and event management (SIEM) approaches ignore. In a recently published report, Prolexic points out that attacks on DNS servers have tripled over the last year, and that DNS is the second-most-popular attack vector behind Hypertext Transfer Protocol (HTTP).

![DNS is #2 attack vector protocol](chart)

Because DNS works unobtrusively behind the scenes—and yet is pervasive and continuous—it makes an excellent vehicle for communicating with Internet-based systems and exfiltrating information.

Domains with Trojan-horse spyware and backdoor codes can be easily found via DNS queries—undetected by almost all security approaches. Once they are inside the firewall, they can communicate with the malefactors who created them using the same DNS path they entered on. Spyware can collect financial data, account numbers, passwords, credit-card numbers, and other keys that give access to sensitive data and send it to criminals.

And because DNS queries are asymmetrical, a response is usually many times larger than the query, which means that your DNS system itself can be made to amplify an attack. Hackers can send one packet of data and cause a flurry that is amplified by thousands—effectively stopping your business in its tracks.
Even Today’s Elaborate Security Measures Don’t Address DNS.

Today’s incident detection and prevention solutions can block APTs and malware. Firewalls and web filters can block bad content, bad sites, and bad links such as phishing links.

But these otherwise effective defenses can be circumvented by seemingly acceptable content, dynamic IPs and URLs, communications, and data sent via DNS. Even if subsequent IP sessions or URL connections are blocked, damage may already have been done.

Malware can be written to avoid most existing security approaches in a variety of ways. It can be made to repack to avoid signature-based detection or to change domains dynamically to circumvent web filters, and botnet controllers can randomly and frequently change IP addresses to circumvent firewalls.

The only way to plug the DNS hole in your network security is to directly address the vulnerabilities unique to DNS.

The Basics of Protecting DNS

Securing your enterprise against DNS-exploiting attacks requires a multi-level approach that extends from your infrastructure to your applications and encompasses standards, practices, information, and purpose-built defenses.
Hardening Appliances, Operating Systems, and Applications

Today’s cybercriminals know commodity servers inside out and have refined techniques for compromising them. Purpose-built appliances are inherently more reliable, manageable, scalable, and secure than general-purpose servers. And the software that runs on them usually offers features—such as real-time environmental and fault monitoring—that bundled utilities don’t have.

But hardening the appliances is just the first step. In the face of today’s increasingly effective attacks, operating systems and applications must have security built in. And one of the most important aids in accomplishing this is an international standard called the Common Criteria for Information Technology Security Evaluation.

The standard is so effective that the U. S. government has used it as the basis for its security certification scheme, and solutions from Common Criteria Evaluation Level 2-certified vendors provide additional levels of protection.

Applying the Principles of High Availability

Your network architecture should be managed from a central appliance that pushes global configuration data and other information out to other appliances, and it should be coupled with an integrated, zero-administration, real-time database so that the infrastructure can continue to deliver services without data loss or corruption if a device or a wide-area network (WAN) fails or becomes infected and needs to be quarantined.

Connections and communications across the network should follow established principles of high availability.

- The central appliance and all its subordinate appliances should be instantly upgradable in case a new operational fix or security flaw has been identified or a new patch has been made available.
- Servers should be linked in high-availability pairs, with constant back-and-forth health checking and automatic failover. There should be no single point of failure, and if a link fails temporarily, communications should go into a queue that is maintained until the link is restored.
- Industry-standard Secure Socket Layer (SSL) encryption should be used in VPN tunnels to reduce the vulnerability of the entire infrastructure.
- The central controlling appliance should be coupled with a mirrored backup appliance at another site that can take over instantly.

Other desirable features include a hardened operating system with no root access, two-factor authentication for login, detailed audit logging, EAL-2 Common Criteria Certification, and granular access control.

Continually Updating Critical Information

A key way to guard against DNS security threats is to know where they come from, so that you can block DNS queries to known bad domains, and can prevent internal servers from communicating with them in the event that the servers do become infected. The solution here is a robust domain reputation service drawing on credible sources throughout the world and keeping pace with the constant changes hackers make to circumvent security efforts.
Visibility into day-to-day network data is also important. Historical reporting, especially on DNS activity, enhances security by making it possible to track intermittent and suspicious activity over time. By being aware of factors such as how many queries are going to questionable outside addresses or whether any of your DNS servers are sending an unusual number of queries, you can detect infected clients quickly, limiting the damage and eliminating the infection.

**Protecting Against DNS Cache Poisoning**

In a cache poisoning attack, the hacker inserts a false address record for an Internet domain into the DNS query. If the DNS server accepts the record, subsequent requests for the address of the domain are answered with the address of a server controlled by the attacker. For as long as the false entry is cached, incoming web requests and emails will go to the attacker’s address.

Systemic vulnerabilities to cache poisoning have prompted the Internet community to begin widespread implementation of the Domain Name System Security Extensions (DNSSEC). The recent Kaminsky attack demonstrated the frightening ease with which DNS cache poisoning attacks can be mounted.

DNSSEC is the only solution that plugs the DNS cache poisoning security hole conclusively. Many top-level zones, including .arpa, .gov, and .org as well as the root zone, have already been signed using DNSSEC. This new technological strategy allows appropriately configured name servers to validate answers cryptographically from these zones—effectively eliminating the possibility of cache poisoning. Going forward, many additional zones will be signed, including .net and .com. So every organization needs to assess its DNSSEC implementation drivers and readiness and develop a DNSSEC policy and implementation plan.

**Taking DNS Away from Malware and APTs**

The most important step in fortifying your DNS servers is taking measures to disrupt malware communications by blocking or redirecting outgoing queries addressed to bad domains. This is accomplished via a combination of:

- A domain reputation service such as the one mentioned above
- A network architecture that makes it possible to distribute domain data to DNS recursive servers in near real time
- DNS firewall application that disallows queries to malware sites or redirects them to a landing page or “walled garden” site defined by your network administrator
- Logging capabilities for collecting information that helps your IT team investigate the sources of malware and cleanse infected devices
Infoblox DNS Firewall

Infoblox is the first and only DNS/DHCP/IPAM vendor to achieve Common Criteria’s highly rigorous EAL-2 certification, which ensures that Infoblox government and enterprise customers have hardened infrastructure that will withstand the most serious security challenges amid the emerging threat landscape.

Our specific solution to the challenge of securing DNS servers is the Infoblox DNS Firewall, which includes:

- The Infoblox DNS Firewall application
- You choice of purpose-built, security-hardened physical appliances or virtual platforms for VMware and Microsoft HyperV
- The Infoblox DNS Firewall Malware Data Feed Service for comprehensive, accurate, and current malware data to detect and resolve malware weeks to months faster than in-house efforts
- The ability to define policies—such as block, redirect, pass through, and log—for a precise response to each threat
- Automated and simplified deployment and management of DNSSEC
- Integration with FireEye APT, which supplies zero-day APT domain information for DNS blocking
- Detailed reports on traffic rates, drill down into RPZ traffic by IP and MAC address and device type, and APT domains (via FireEye).

The Infoblox DNS Firewall provides comprehensive protection against DNS-exploiting malware.

On August 27, 2013, a group calling itself the Syrian Electronic Army (SEA) hacked into the system of domain name registration company in Australia and preplaced the registered name servers of one of the world’s largest newspapers, a global social-media site, and several other organizations with SEA’s own name servers. In addition to the obvious defacement-style attack, this potentially meant the SEA could access emails sent to the organizations and login information on their websites.
Many security threats today are launched by organizations with deep resources, such as cyberwar teams, unscrupulous competitors, government censors, hacktivists, and international criminals.

Within two and one half hours, Infoblox had confirmed the attack, Infoblox Malware Data Feed was updated with the IP addresses of the malicious name servers, and all Infoblox DNS Firewall customers had those addresses in their DNS Firewall servers. Just half an hour later, access attempts to the hijacked name servers were being blocked by Infoblox DNS Firewall—so that no web, email, Telnet, or FTP communications were being redirected to SEA.

DNS Firewall also logs all attempted connections with malicious destinations, complete with device IP and MAC addresses and device fingerprints for future remediation. Upon confirmation that the affected organizations had the correct name servers, the blocked entries were removed and access to the correct (non-hijacked) sites was restored via an automatic update.

Let Us Help You Close the DNS Security Hole.

DNS vulnerability is a serious risk to your business, and now is the time to do something about it. Organizations around the world are being protected from threats such as the SEA attack by Infoblox DNS Firewall. Contact us today, and learn more about how you can strengthen your defenses and deprive potential attackers of a weak point to attack.

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 6,700 enterprises and service providers in 25 countries control their networks.