Summary: DNS-based DDoS attacks are constantly evolving, and attackers employ a wide range of techniques from basic methods like amplification/reflection and floods to NXDOMAIN attacks that vary from classic to highly sophisticated attacks involving client and CPE botnets, chain reactions, and misbehaving servers. An NXDOMAIN attack can overwhelm server resources and impact performance. It can affect internal recursive servers as well as external authoritative servers.

NXDOMAIN Attack on Recursive Servers

In the classic NXDOMAIN attack, the attacker sends a flood of queries to a Domain Name System (DNS) server to resolve a non-existent domain name. The DNS server tries to resolve the domain but cannot find it. In the process, its cache gets filled up with NXDOMAIN results, slowing response for legitimate requests. Many DNS server administrators fail to realize that what they think are performance problems are actually NXDOMAIN attacks on their DNS server. NXRRSET is another form of NXDOMAIN attack in which, for instance, the A record exists, but the AAAA or MX record does not, and those are being queried against.

In the random subdomain attack (which can also be a phantom domain attack, described a little later), the attacks are generated from a series of clients that prepend randomly generated subdomain strings to DNS requests to resolve non-existent domain names within the target domain—for example: http://6ctloyPiVsHsd.targetsite.com or http://kT51epKLGkN.targetsite.com.

The DNS recursive servers try to resolve the fake domains through recursion out to the Internet, but cannot. This recursion consumes central processing unit (CPU) cycles and other resources. Meanwhile, the server's cache is being filled up with NXDOMAIN results, slowing DNS server response time for legitimate requests (cache pollution). When the cache gets filled up with NXDOMAIN/NXRRSET responses, valid cache entries get pushed out, leading to further service degradation.

The eventual target of the attack can be the authoritative server of the targetsite.com, but it can impact all recursive servers between the client and the authoritative server.

What distinguishes a phantom domain attack is that the zone/authoritative targetsite.com server is specifically set up for the attack, and may in fact impact the recursive server by deliberately being slow to respond, returning TRUNC responses to elicit a Transmission Control Protocol (TCP) connection—all in the endeavor to consume available resources of the recursive server.

NXDOMAIN Attack on Authoritative Servers

NXDOMAIN attacks can affect authoritative servers as well. When the attacker sends requests for non-existing domains, such as http://6ctloyPiVsHsd.targetsite.com, to the authoritative server of targetsite, targetsite's authoritative server doesn't have the IP address for which it is authoritative in its memory. This impacts older DNS servers not running the most recent releases of BIND, and can reduce performance for DNS servers that have inadequate memory resources or that have to query the disk.

The slow-drip random subdomain attack is performed as described in the previous section, but by very large numbers of clients (in a botnet), each of which sends a slow stream of DNS queries. This results in a significant volume of traffic arriving on incoming network links of the target domain.

If the authoritative server is well protected by something like Infoblox External DNS Security, then the most likely form of outage is the flooding of the incoming network links. This is the kind of situation in which the use of anycast (as used by the root servers) can blunt many attacks.
Mitigating NXDOMAIN Attacks

Infoblox’s DNS security portfolio consists of:

- Infoblox External DNS Security, which can shield networks from many attacks, including NXDOMAIN, that target the external Internet facing server
- Internal DNS Security, which can protect internal recursive servers from NXDOMAIN attacks, advanced persistent threats (APTs), malware, and data exfiltration

Running on purpose-built DNS appliances, these solutions effectively protect both your external and internal DNS and Dynamic Host Configuration Protocol (DHCP) infrastructure. In addition, Infoblox security products leverage continual, automatic updates to protect against new and evolving attacks and emerging malicious domains and networks.

Security from the Ground Up

Protection starts with the hardware—Infoblox purpose-built appliances are hardened for security during the manufacturing process and certified for Common Criteria Level EAL-2. One-click enablement and automatic key refresh eliminate the usual complexity of implementing DNS Security (DNSSEC).

Automatic Blackholing, Adjustable Recursive Timeouts, and Cache Pollution Prevention

Infoblox External DNS Security and Internal DNS Security have specific capabilities built in to mitigate all known types of NXDOMAIN attacks:

- Automatic blackholing of bad and misbehaving domains/servers, and the application of rate limiting on traffic going to miscreant or overwhelmed servers, result in SRVFAIL being returned to the clients, telling them that their DNS request failed.
- Client-based mitigation techniques include looking at the behavior of a client, and—if a client generates a high rate of NXDOMAIN, NXRRset, or SRVFAIL responses—blocking requests from that client’s IP address for a configurable period of time.
Even during an attack, the solution doesn't allow NXDOMAIN responses to push out valid cache entries, and it ensures that the needed cache refresh takes place to allow for continuous service.

• For authoritative servers, Infoblox servers now have the list of authoritative IP addresses in memory, which improves performance when NXDOMAIN attacks hit them.

• If a distributed denial of service (DDoS) attack is constantly being experienced, the timeout for recursive name lookup can be lowered to quickly free up the resources in the DNS resolver and prevent the concurrent number of outstanding DNS queries from maxing out.

Guarding against Outside-in Attacks

Infoblox External DNS Security provides defense against the widest range of DNS-based attacks such as volumetric attacks, NXDOMAIN, exploits, and DNS hijacking for external authoritative servers. This provides secure, highly available, and trustworthy DNS services even when your network is under attack. Through comprehensive reports, the solution gives you a centralized view of attacks that are happening on your network.

Guarding against Inside-out Attacks

Infoblox Internal DNS Security is an easy-to-deploy, appliance-based solution that protects mission-critical DNS and DHCP infrastructure from attacks such as NXDOMAIN, stops APT and malware communications, and prevents data exfiltration—without the need for endpoint agents or changes to your network architecture.

Don’t Let NXDOMAIN Attacks Bring Your Servers Down

Any attack on your DNS server means downtime and disruption to your business, not to mention brand damage, customer defection, and lost revenue. Intelligently mitigate NXDOMAIN and other DNS DDoS attacks with DNS solutions that are purpose built with security in mind.

Contact us today to find out more about how you can defend against NXDOMAIN and other such DNS attacks on your critical infrastructure.

About Infoblox

Infoblox delivers critical network services that protect Domain Name System (DNS) infrastructure, automate cloud deployments, and increase the reliability of enterprise and service provider networks around the world. As the industry leader in DNS, DHCP, and IP address management, the category known as DDI, Infoblox (www.infoblox.com) reduces the risk and complexity of networking.