TOP TEN DNS ATTACKS ON SERVICE PROVIDER NETWORKS

PROTECT YOUR SUBSCRIBERS AND NETWORK INFRASTRUCTURE FROM GROWING THREATS
Introduction

Protecting subscribers and the network is fundamental to service provider success. Your subscribers expect network communications to be fast, always available, and highly secure. They won’t hesitate to switch providers if they experience disappointing performance or learn of a security breach. But today’s threat landscape is changing, creating escalating security challenges. Attacks against Domain Name System (DNS) infrastructure, critical to network function, are on the rise. They are threatening service availability, network performance, subscriber data, and your reputation.

Every subscriber and device communication depends on the network’s DNS infrastructure. When a DNS service attack hits, it can slow performance or spawn network outages. Your subscribers will experience poor or failed Internet connectivity, and some devices that are attached to the network may stop working altogether. Your high-value enterprise clients may find that customers can’t access their websites effectively—or at all.

All service providers—whether mobile, broadband, cable, or cloud—understand that security breaches can degrade the network, increase costs, and cause subscriber dissatisfaction and churn. Compromised DNS resources have a direct economic impact on you and your subscribers.
More Sophisticated Threats

DNS is the most targeted service of application layer DDoS attacks. Nearly all operators have experienced these threats, and attacks are increasing in frequency, volume, and complexity. Over the last year, common volumetric flood attacks have continued to rise, but service providers have also reported a wider range of new, more sophisticated techniques from hackers, including NXDOMAIN and Random Subdomain attacks. Highly complex, well-planned attacks are also on the rise, including combinations of botnets, chain reactions, and misbehaving domains.

Legacy DNS is Ineffective

Traditional DNS open-source software and Internet-facing firewall appliances were not designed for DNS security, and are ineffective against today’s evolving DNS threats. Stopping DNS attacks requires deep inspection with extremely high compute performance to maintain network performance during an attack. Most of today’s existing security solutions don’t have these capabilities.

Your legacy DNS equipment likely provides limited visibility into your DNS operations. You may only become aware that DDoS attacks are occurring after subscribers complain about slow connections or outages. You may not know if subscriber device clients have become infected with malware and can become unintentional participants in the attack. A hacker may target an enterprise, using your network to launch the attack. Even if you discover the attack, your legacy DNS equipment may offer few remediation options. Your only choice is to scale up your network to withstand the increased volume.

Given these new challenges, protecting DNS performance and integrity is more important than ever to your business success. You need to evaluate your network vulnerabilities, understand risks, and deploy DNS-specific security as a key element of your network security strategy. Understanding the nature of DNS attacks is the first step. In this eBook, we’ll take a closer look at the top ten DNS-based threats, and how they impact service provider networks.
NXDOMAIN Attack

A basic or classic NXDOMAIN attack is a DNS flood attack that can overwhelm server resources and impact performance. It works by sending a flood of queries to a DNS server to resolve a non-existent domain name. The recursive server tries to locate the fake domain, but cannot find it. Meanwhile, the server’s cache fills up with NXDOMAIN results, slowing DNS server response time for legitimate requests.
Random Subdomain Attack (Slow Drip)

Random subdomain, or “slow drip” attacks can tax recursive server resources in service provider networks and slow performance. Random subdomain attacks start with infected client devices or bots that create queries by adding randomly generated subdomain strings prefixed to the victim’s domain. For example, a client might query a non-existent subdomain like “xyz4433.ABCcorp.com”.

Random subdomain or slow drip attacks are difficult to detect, because each client may send only a small number of queries to a service provider’s DNS recursive server. But when many infected clients send requests, the impact on the recursive server performance is significant. In addition, the authoritative name servers of the target domain (ABCcorp.com) may get flooded with irrelevant requests, becoming unable to send responses. As the DNS recursive server in the service provider network waits for responses, its outstanding query limit becomes exhausted, and it too will be unable to respond.
Phantom Domain Attack

This type of attack forces the service provider’s DNS resolvers to resolve multiple “phantom” domains that have been set up by the attacker. These domains are slow to respond, or may not respond at all. The server continues to consume resources while waiting for responses, eventually leading to degraded performance or failure.
Floods

Volumetric flood attacks are the most common type of attack experienced by service providers. These attacks tie up available channels in your DNS servers with a large number of requests originating from many spoofed clients. The result is slower performance or denial of service to legitimate users.

A typical flood attack is the TCP SYN flood. This DDoS attack takes advantage of the three-way handshake that's used to start a Transmission Control Protocol (TCP) connection.

An attacker sends its target spoofed synchronization (SYN) packets that include the source IP address of actual service provider subscriber devices. The targeted server then sends SYN-ACK packets to the designated subscribers, but never receives acknowledgment because the actual subscriber's client doesn't recognize the transmission. Your DNS servers keep these channels open waiting for a response that doesn't come, tying up resources and making them unavailable to legitimate users. Eventually, the server may stop responding to new connection requests coming from legitimate users.
DNS Tunneling

DNS tunneling attacks can provide attackers with an always-available back channel to exfiltrate stolen data or to bypass service provider billing systems for free access to services such as premium Wi-Fi.

They are based on using DNS as a covert communication channel to bypass a perimeter security device such as a firewall or the authentication and charging process for a premium Wi-Fi hotspot.

Attackers tunnel protocols like SSH or HTTP within DNS, then secretly pass stolen data or tunnel IP traffic. Once access is gained through the DNS tunnel, the attacker is granted “free” access to the Internet. This tunnel also can allow the attacker to transfer files through the service provider network, download new code to existing malware, or have complete remote access to the system.
DNS Cache Poisoning

DNS cache poisoning corrupts a DNS server's cache with bogus data such as a rogue address, opening the door to data theft of logins, passwords, and user credit card numbers, as well as other threats.

1. Attacker queries a recursive name server (of a service provider or enterprise) for a subdomain that doesn't exist (e.g. q0001.ABCcorp.com)
2. The recursive name server does not have the IP address and queries an ABCcorp.com name server
3. Before the ABCcorp.com name server can send NXDOMAIN response, the attacker sends lots of spoofed responses that look like they are coming from a legitimate ABCcorp.com server.
4. The recursive name server accepts a spoofed response and caches the record
5. A user queries the recursive name server for the IP address of www.ABCcorp.com
6. The recursive name server replies to the user with a cached rogue IP address
7. The user connects to a site controlled by attacker, which may look exactly like the real ABCcorp website
Distributed Reflection DoS Attack (DrDoS)

A distributed reflection DoS attack (DrDoS) uses open recursive servers (open resolvers) on the Internet to unwittingly participate in attacks against a target. These types of attacks use reflection and amplification techniques to spoof their identity and increase the magnitude and effectiveness of an attack.

Attackers send their spoofed queries to open resolvers (or misconfigured service provider home gateways acting as open resolvers). They sometimes query thousands of servers at a time. Each query is designed to elicit a large response, and send an overwhelming amount of data to the victim’s IP address. DrDos can target service providers IP addresses as well as enterprise. In either case, DrDos attacks create unnecessary traffic load on the service provider network. Additionally, DrDoS attacks can tie up home gateways, slowing down the Internet response and degrading the user experience.
Botnet-Based Attacks from Smart Devices

Botnets remain an important part of the threat landscape, and attackers continue to develop innovative ways to use them. Botnets can be used to launch DDoS and other types of attacks on service provider infrastructure, partners, or subscribers.

The attacks start with compromised smart devices such as smartphones, tablets, machine-to-machine devices (e.g., smart meters or video monitoring devices) or even small cells and Wi-Fi access points.

Attackers infect these devices with malware, causing them to form a botnet to send DDoS traffic to the targeted victim. This type of attack can exert an unnecessary load on a service provider DNS infrastructure, which will have a direct impact on DNS response rate.

Botnet-based attacks can also create issues with the compromised smart devices. Performance may slow significantly on the device, and bad actors can ex-filtrate login credentials and other data via an SSL proxy. An attacker may use the device to order unauthorized premium services. Or they may use the infected device to launch attacks against other service provider environments, such as internal networks, retail sites, or managed service networks to further expand the security threat.
DNS Hijacking

DNS hijacking overrides a domain's registration information in the service provider DNS cache or other caching layer. The modified information is set to point to rogue DNS servers.

When users try to access a legitimate website, such as a bank, credit card company, or their service provider customer portal, they are redirected to a bogus site that looks much like the real thing—but is controlled by the attacker. DNS hijacking can put sensitive personal data at risk, including user names, passwords, and credit card information.
Domain Lock-Up Attack

A domain lock-up attack employs resolvers and domains that are set up by attackers to establish TCP-based connections with DNS resolvers. The targeted DNS resolvers can be owned by a service provider or its enterprise customers. When a DNS resolver requests a response, these domains send “junk” or random packets to keep them engaged. The attacker’s domains are deliberately slow to respond, which keeps the resolvers engaged longer.

When a DNS resolver establishes connections with the misbehaving domains, its resources are depleted, and if totally exhausted, the DNS resolver locks up.
Detect and Mitigate DNS Attacks

DNS attacks are increasingly attractive for hackers. The growing sophistication of these attacks makes it easier for them to remain undetected by large service provider organizations. For example, firewalls only lightly inspect DNS traffic, so DDoS attacks may evade detection. Without a DNS specific protection plan including monitoring, central visibility, and continuous threat updates, service providers may remain unaware of DDoS attacks until subscribers complain—especially when they involve large numbers of geographically dispersed DNS servers.

To safeguard your network and subscribers, you need clear inter-departmental communication and assignment of responsibility for DNS security. Start by defining the methods, procedures, and tools you have in place to detect and mitigate DNS attacks.

Secure DNS Essentials

A proactive, dynamic approach is essential against a constantly changing threat landscape. As attacks become more nimble and sophisticated, and DNS infrastructure grows with traffic, automation and scalability are key.

Carrier-Grade, High Performance Solution

Service providers, including mobile, broadband, cable or cloud require a hardened, DNS solution to protect against today’s threats. It should include:

Advanced DNS DDoS detection and mitigation: Intelligent detection of inappropriate volumes of traffic and live, global threat feed to provide dynamic updates of new threats to all DNS infrastructure elements simultaneously.

Very high performance and scalability: Ability to minimize latency and sustain performance (QPS) during an attack.

Central management, control, and visibility: The large number of DNS elements deployed by service providers requires a well-integrated, maintainable solution that can monitor and manage with high level visibility.

Ultra-High Availability: DNS is a mission-critical function that must rapidly recover from any network, software, or hardware failures.
Infoblox Advanced DNS Protection (ADP)

Infoblox provides secure DNS through carrier grade DNS solutions.

The Infoblox 4030 DNS Caching Appliance is purpose-built to deliver new levels of scalability, security, management, and DoS/DDoS protection for service providers. Paired with patented Infoblox Grid™ technology, Infoblox solutions eliminate single points of failure and enable you to automate and manage appliance upgrades and patches from a single point.

Infoblox ADP has built-in, intelligent attack protection that keeps track of source IP addresses of DNS requests, as well as the DNS records requested. The solution can intelligently drop excessive DNS DDoS requests from the same IP address, saving resources to respond to legitimate requests.

Infoblox solutions use dedicated network packet inspection hardware together with automated threat intelligence rules to stop protocol-based attacks like DNS amplification, reflection, and cache poisoning. Infoblox actively monitors the latest DNS-based vulnerabilities and ensures that the solution provides protection against attacks out of the box. Automatic rule set updates provide protection against new and evolving attacks without the need for downtime or patching.

DNS Firewall

DNS Firewall protects against advanced persistent threats (APTs) and malware by:

- **Enforcing response policies** on traffic from infected endpoints to suspicious domains
- **Leveraging an automated, customizable threat update service** that provides up-to-date threat data on known malicious domains
- **Providing insightful reporting** on malicious DNS queries including threat severity and impact, and pinpointing infected devices

Together, these components of a secure DNS solution deliver the intelligence, performance, and proactive protection service providers need to safeguard their networks and subscribers.

To learn more about how Infoblox solutions can help you get out in front of DNS-based attacks, visit [www.infoblox.com](http://www.infoblox.com).
For more information visit www.infoblox.com