TOP TEN DNS ATTACKS

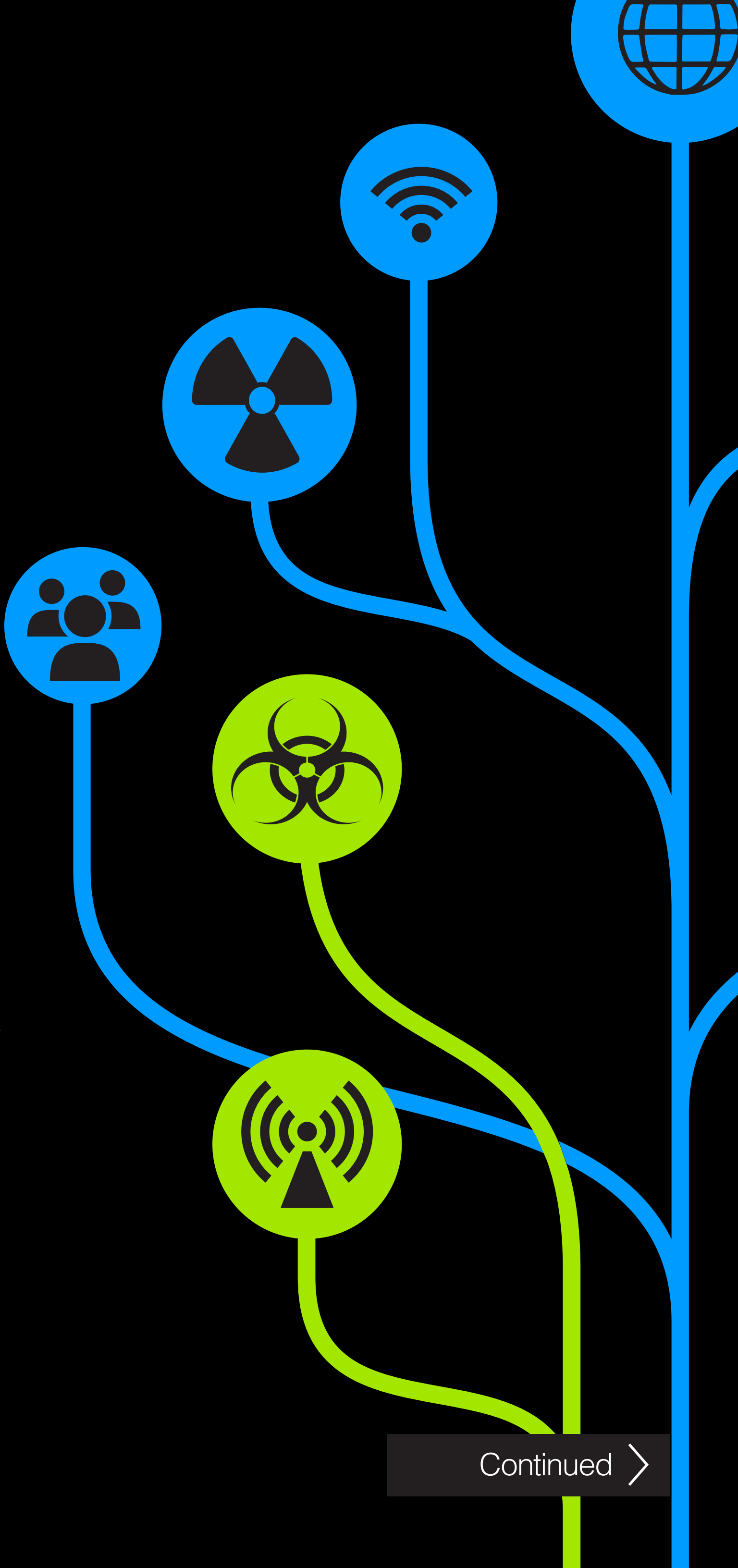
PROTECTING YOUR ORGANIZATION AGAINST TODAY'S FAST-GROWING THREATS

Infoblox®
CONTROL YOUR NETWORK

Introduction

Your data and infrastructure are at the heart of your business. Your employees, business partners, and customers are getting more connected, and rely on the network to support their most important business processes.

But Domain Name System (DNS)-based attacks are on the rise, putting your data, revenue, and reputation at risk. If a DNS service goes down, your organization's Internet connectivity fails, and devices that are attached to the network stop working. Even a single serious attack could expose data or bring your business operations to a halt.

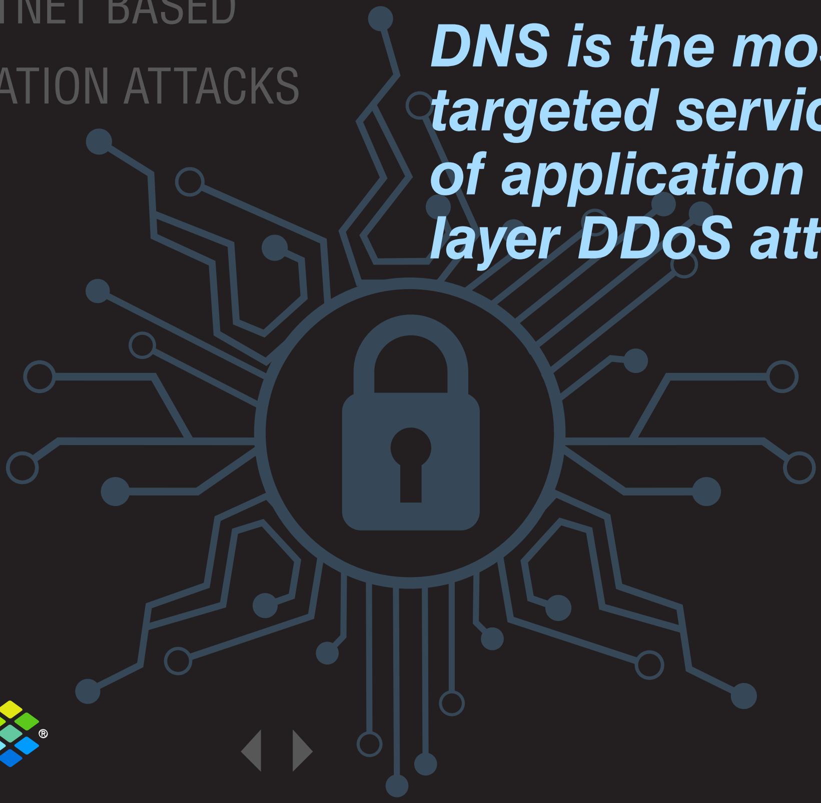


Continued

Traditional Security is Not Enough

Traditional firewall protection is ineffective against today's evolving DNS threats. Firewalls leave port 53 open, reserving it for DNS queries. They don't do much in terms of inspecting the queries coming in. So they can't provide protection against DNS-based distributed denial-of-service (DDoS) attacks like amplification, reflection, or other techniques. Stopping DNS attacks requires deep inspection and extremely high compute performance for accurate detection, which is not provided by the traditional solutions.

DNS is the most targeted service of application layer DDoS attacks.



A Constantly Evolving Threat

DNS-based DDoS attacks are not only difficult to discover. They are a moving target, constantly evolving and capable of impacting both external and internal DNS servers. Attackers employ a wide range of techniques, from basic methods like amplification/reflection, floods, and simple NXDOMAIN, to highly sophisticated attacks involving botnets, chain reactions, and misbehaving domains. They may come from the outside in, or from the inside out.

Hackers understand that DNS security is often overlooked, so DNS-based attacks are on the rise. According to the most recent Worldwide Infrastructure Security Report from Arbor Networks, DNS is the number one protocol used in reflection/ amplification attacks and is tied with http for the top targeted service of application-layer DDoS attacks. The sooner you add DNS-specific security as a layer in your defense-in-depth security strategy, the less risk to your organization. The first step is understanding how DNS-based attacks can impact your network and your business. Let's take a closer look at the top ten DNS-based threats, and how they work.

◀ ▶

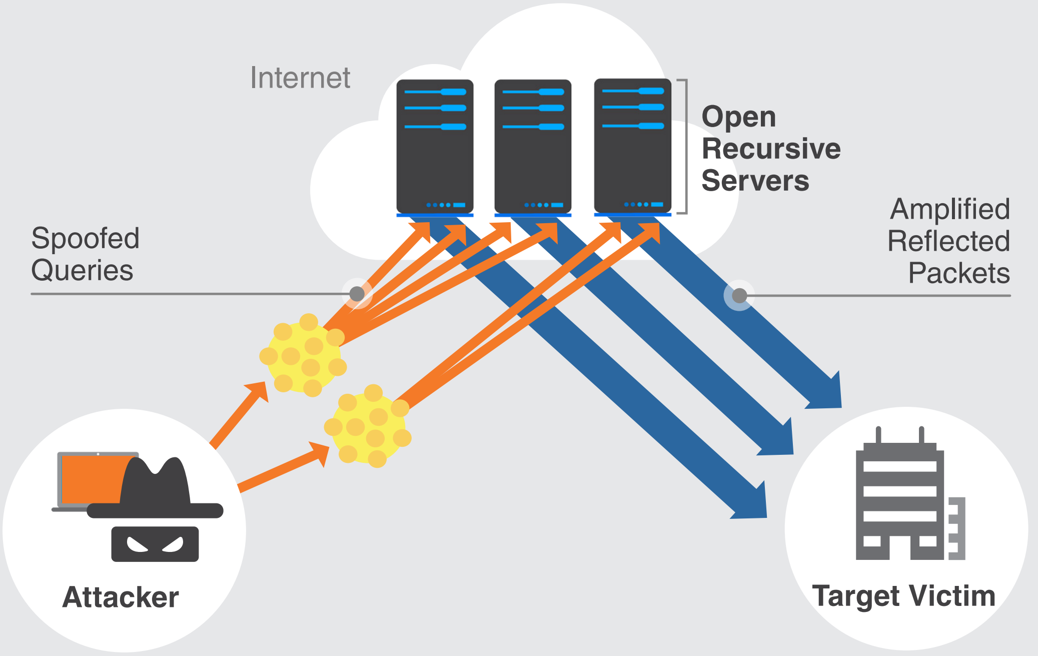
INTRODUCTION
01 DRDOS
02 FLOODS
03 DNS TUNNELING
04 BASIC NXDOMAIN
05 PHANTOM DOMAIN
06 RANDOM SUB-DOMAIN
07 DOMAIN LOCK-UP
08 CPE BOTNET BASED
MITIGRATION ATTACKS

Distributed Reflection DoS Attack (DrDoS)

A distributed reflection DoS attack, or DrDoS attack, uses third-party 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. Authoritative name servers can also be used for this attack.

Attackers send their spoofed queries to multiple open recursive servers—sometimes 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. When a victim is hit by the DDoS attack, it can cause slow performance or site outages that can shut down important business processes.

How The Attack Works

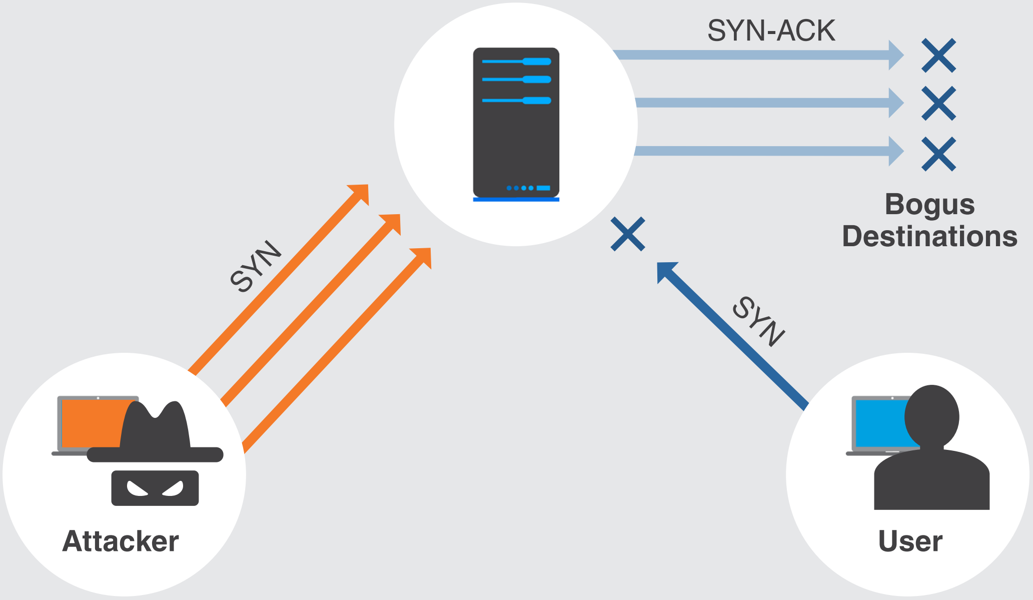


Floods

An example of a flood is a TCP SYN flood. A TCP SYN flood attack is a DoS attack that 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 bogus destinations. The targeted server then sends SYN-ACK packets to the bogus destinations, but never receives acknowledgement, so the connections are never completed.

These half-opened connections fill up the listen queue on the server. Finally, the server stops responding to new connection requests coming from legitimate users.

How The Attack Works

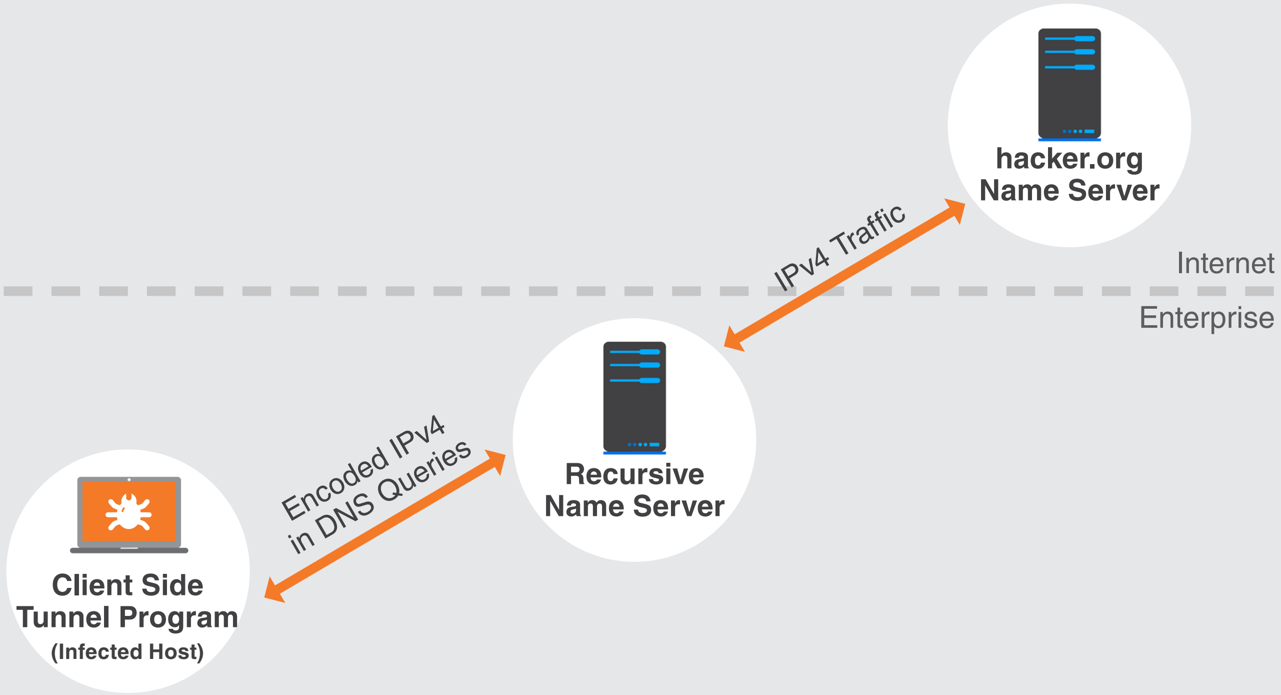


DNS Tunneling

DNS tunneling attacks can provide attackers with an always-available back channel to exfiltrate stolen data. It's based on using DNS as a covert communication channel to bypass a firewall. Attackers tunnel protocols like SSH or HTTP within DNS, then secretly pass stolen data or tunnel IP traffic.

A DNS tunnel can be used as a full remote control channel for a compromised internal host. This lets them transfer files out of the network, download new code to existing malware, or have complete remote access to the system. DNS tunnels can also be used to bypass captive portals, to avoid paying for Wi-Fi service.

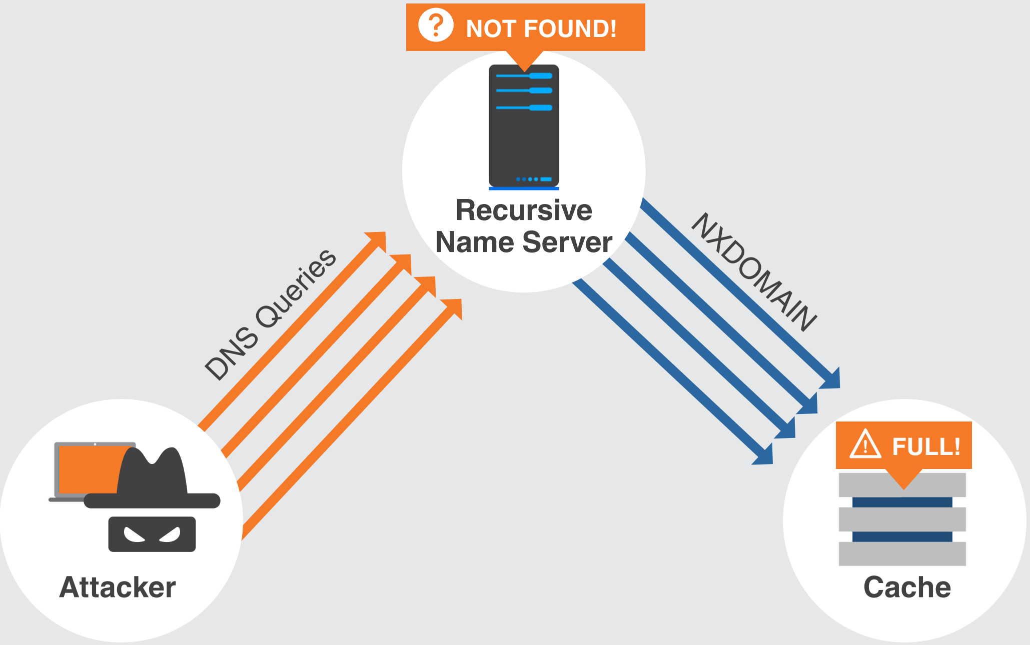
How The Attack Works



Basic NXDOMAIN Attack

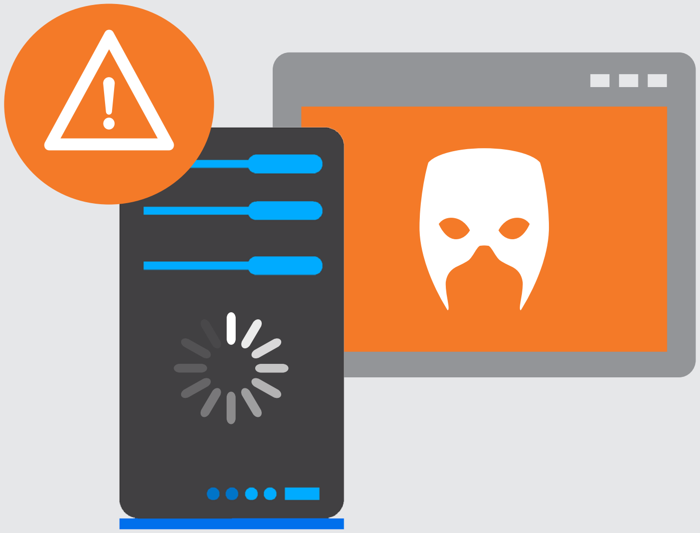
A basic NXDOMAIN attack is a DNS flood attack that can overwhelm server resources and impact performance. It works by sending a flood of queries to a DNS server to resolve non-existent domain names. The recursive server tries to locate the fake domains, but cannot find them. Meanwhile, the server's cache fills up with NXDOMAIN results, slowing DNS server response time for legitimate requests.

How The Attack Works



Phantom Domain Attack

This type of attack forces the DNS resolver 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.

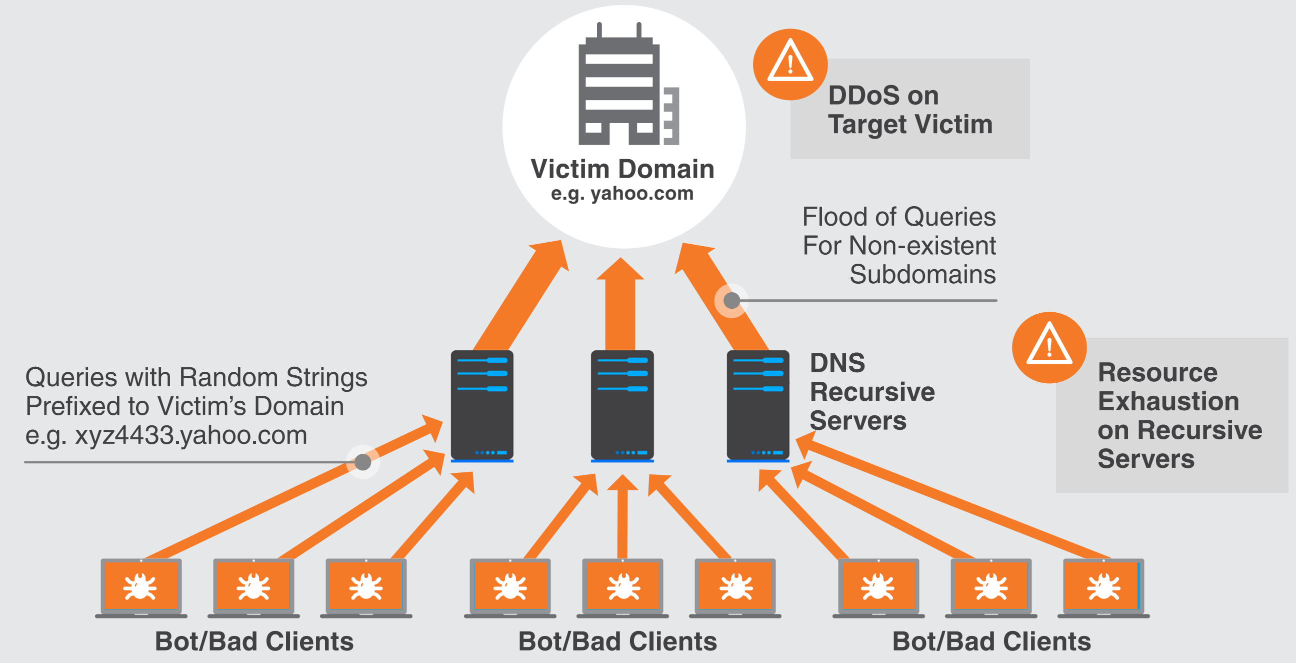


Random Subdomain Attack (Slow Drip)

Random subdomain, or “slow drip” attacks can tax recursive server resources and slow performance. They 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.yahoo.com.”

Random subdomain attacks are difficult to detect, because each client may send only a small number of queries to its DNS recursive server. But when many infected clients send requests, the impact on the recursive server is significant. In addition, the authoritative name servers of the target domain (yahoo.com) experience DDoS and responses may never come back from the target domain. As the DNS recursive server waits for responses, its outstanding query limit becomes exhausted. In addition, the authoritative name servers of the target domain (yahoo.com) experience DDoS.

How The Attack Works



Victim Domain
e.g. yahoo.com

DDoS on Target Victim

Flood of Queries For Non-existent Subdomains

DNS Recursive Servers

Resource Exhaustion on Recursive Servers

Queries with Random Strings Prefixed to Victim’s Domain e.g. xyz4433.yahoo.com

Bot/Bad Clients

Bot/Bad Clients

Bot/Bad Clients

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. 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 to requests, which keeps the resolvers engaged longer.

When a DNS resolver establishes connections with the misbehaving domains, its resources become exhausted, and it locks up.

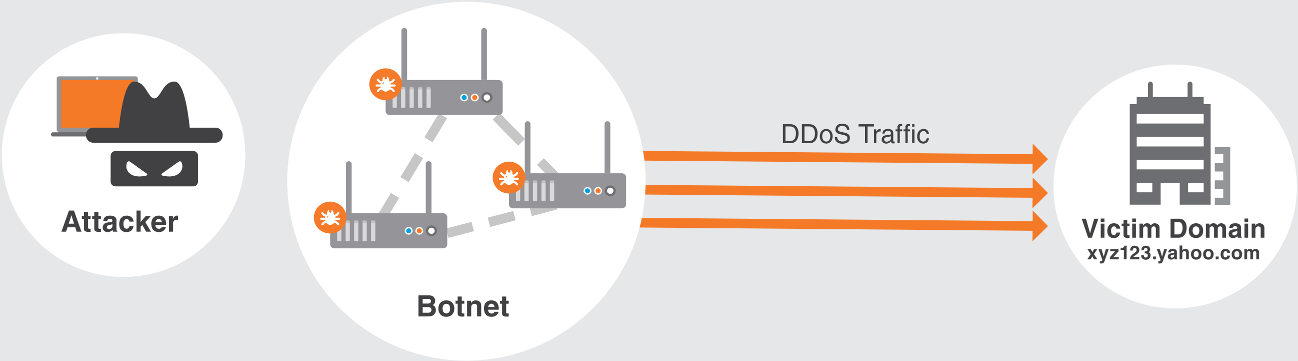
INTRODUCTION
01 DRDOS
02 FLOODS
03 DNS TUNNELING
04 BASIC NXDOMAIN
05 PHANTOM DOMAIN
06 RANDOM SUB-DOMAIN
07 DOMAIN LOCK-UP
08 CPE BOTNET BASED
MITIGRATION ATTACKS

Botnet-Based Attacks from CPE Devices

Botnets remain an important part of the threat landscape, and attackers continue to develop innovative ways to use them. Random subdomain attacks can use botnets to target all traffic to one site or domain. The attacks start with compromised customer premises equipment (CPE) device like switches and routers. These devices may be supplied by an ISP, or purchased by the customer.

Attackers infect these CPE devices with malware, causing them to form a botnet to send DDoS traffic to the targeted site. The victim's domain is hit with a DDoS attack that exhausts DNS resolver resources. Botnet-based attacks can also create issues with the compromised CPE equipment. Bad actors can exfiltrate login credentials and other data via an SSL proxy. Or they may use the infected CPE to launch attacks against the victim's PCs and environments, further expanding the security threat.

How The Attack Works



Mitigating DNS-Based Attacks

It's clear that DNS-based attacks are increasingly attractive for hackers. All too often, DNS security does not receive the attention it needs from IT organizations.

So how can you safeguard your business against DNS-based attacks? The first step is communication. Get your IT teams together and determine who in your organization is responsible for DNS security. Discuss the types of methods, procedures, and tools you have in place to detect and mitigate DNS attacks. Consider whether you would know if an attack was happening—and the best way to stop it.

Then get down to business with the components of a DNS-based security infrastructure built for today's extreme threat levels.

Harden Your Infrastructure

The solid foundation of a secure DNS infrastructure is a dedicated, purpose-built DNS appliance that minimizes attack surfaces with:

- No extra or unused ports open to access the servers
- No root login access with the OS
- Role-based access to maintain overall control

The appliance should feature two-factor authentication for login access, web access using HTTPS for encryption, and SSL encryption for appliance interaction through APIs.

Integrate and Consolidate Your Security Efforts

Most organizations gather threat intelligence from multiple sources and implement security technologies from a wide range of vendors—resulting in siloed security protocols and processes and operational inefficiencies. IT is left managing too many alerts with too little visibility and context. Here's how to overcome this difficulty.

Continued

The Infoblox Actionable Network Intelligence Platform™ delivers security from the core of your network. It eliminates the DNS blind spot, provides valuable network context, and bridges security silos. The platform brings together threat intelligence and enterprise context to help you manage risk and gain unprecedented visibility for combating threats. It enables you to:

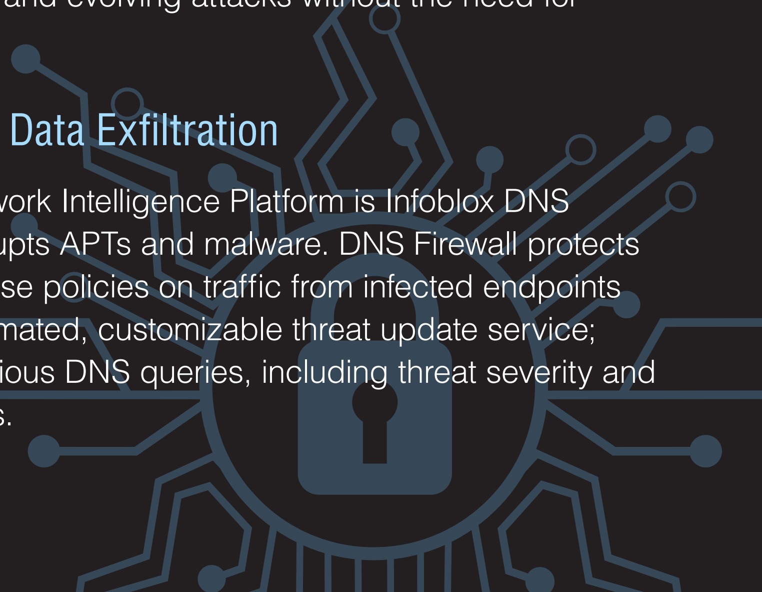
- Prioritize response based on enterprise context and risk
- Protect by instantly blocking malicious activity at the control point
- Predict threats that could compromise the network by leveraging the federated platform

Protect against External DNS-based Attacks

Infoblox Advanced DNS Protection uses the dedicated appliances of the Actionable Network Intelligence Platform to address external attacks that target your Internet-facing DNS. It provides built-in, intelligent attack protection that keeps track of source IPs of DNS requests, as well as the DNS records requested.

The solution can intelligently drop excessive DNS DDoS requests from the same IP, saving resources to respond to legitimate requests. To stop protocol-based attacks like DNS amplification, reflection, and cache poisoning, Advanced DNS Protection uses dedicated network packet inspection hardware together with automated threat intelligence rules.

Infoblox actively monitors the latest DNS based vulnerabilities and ensures that the solution provides protection against attacks out of the box. The rule set is automatically updated to provide protection against new and evolving attacks without the need for downtime or patching.



Protect against APTs, Malware, and Data Exfiltration

Another component of the Actionable Network Intelligence Platform is Infoblox DNS Firewall, which effectively detects and disrupts APTs and malware. DNS Firewall protects against APTs/malware by enforcing response policies on traffic from infected endpoints to suspicious domains; leveraging an automated, customizable threat update service; and delivering insightful reporting on malicious DNS queries, including threat severity and impact and the location of infected devices.

Learn More

Together, these components of the Actionable Network Intelligence Platform deliver the intelligence, performance, and proactive protection you need to safeguard your organization against today's threats. To learn more about how Infoblox solutions can help you get out in front of DNS-based attacks, visit www.infoblox.com.

For more information visit www.infoblox.com

Infoblox
CONTROL YOUR NETWORK