



Outsmart DNS DDoS Attacks With Corero

Introduction

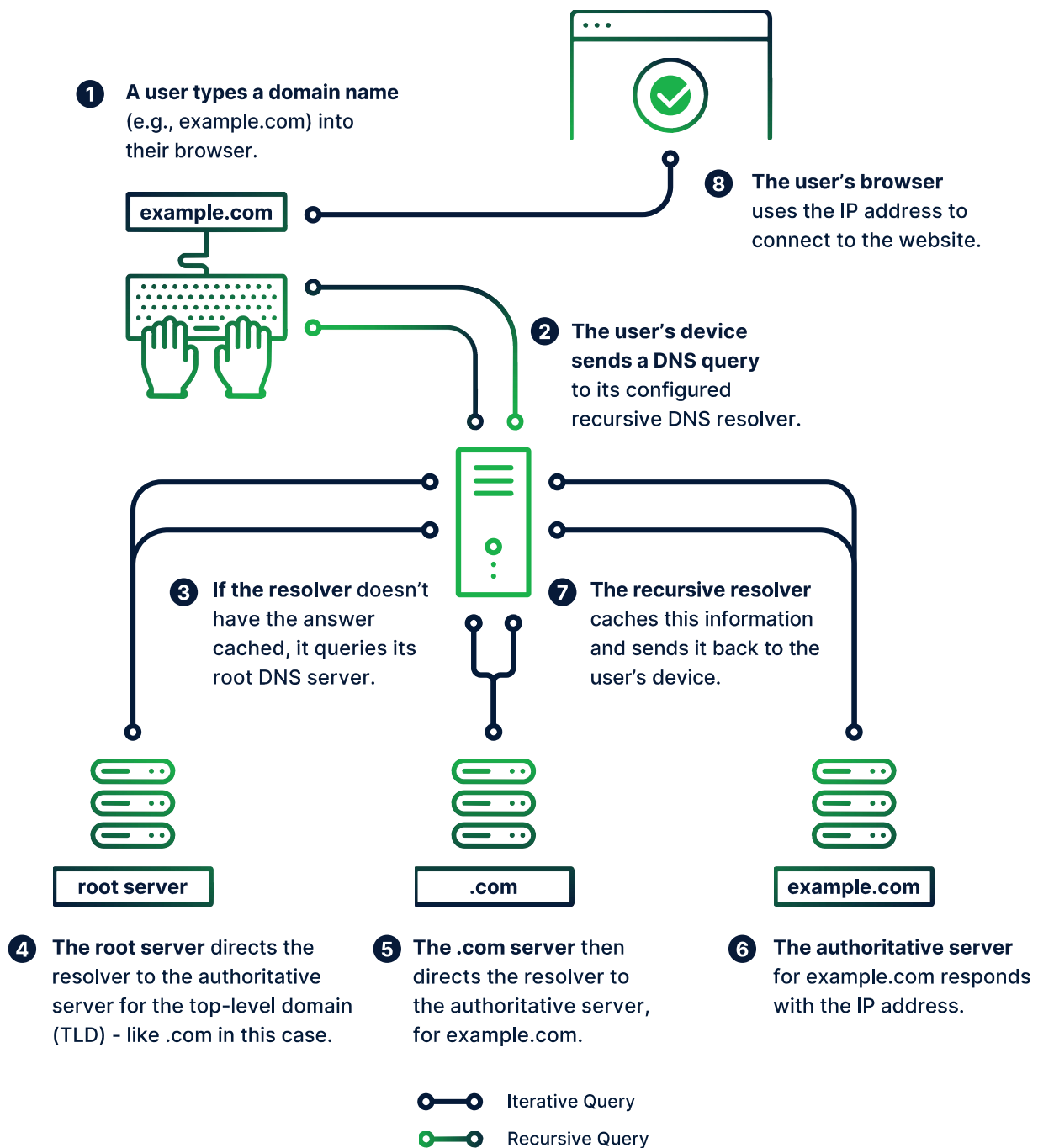
DNS attacks come in multiple forms. One of the most common is often called a ‘water torture.’ This type of attack slowly drains server resources, much like the constant dripping of water in its namesake. Its gradual nature can make it difficult to detect, or be mistaken for another resource-related issue, allowing it to persist for extended periods before being correctly identified and mitigated.

Here’s a breakdown: Picture your domain name system (DNS) servers being bombarded with endless requests for non-existent domains (NXDOMAIN). This is the essence of DNS water torture—a type of distributed denial-of-service (DDoS) attack aimed at depleting your DNS infrastructure’s resources. By sending a high volume of fake requests, attackers exhaust your DNS servers’ resources, causing service slow-downs, disruptions, or downtime for legitimate users.

Comparing Normal and Water Torture Traffic

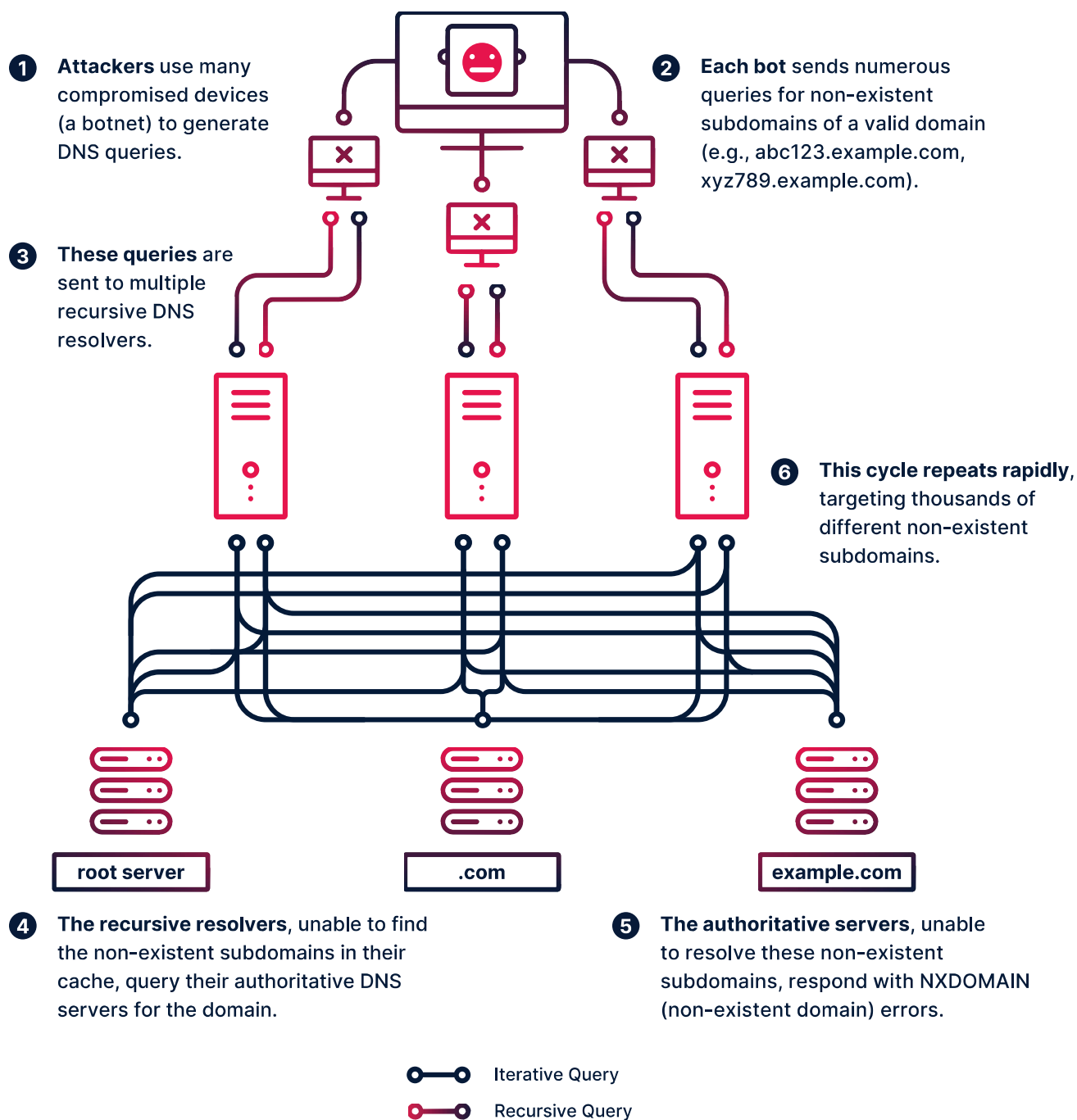
Normal DNS Traffic

Let's go over how DNS traffic typically flows. This process is usually quick and efficient, with DNS servers smoothly handling legitimate requests.



DNS Water Torture

Now, let's look at a DNS water torture attack. In this scenario, attackers overwhelm DNS servers with a flood of queries for non-existent subdomains, draining resources and blocking legitimate traffic. These fake requests often look legitimate, making it difficult to distinguish good traffic from bad.



Why is DNS DDoS Protection Important?

Many DNS attacks go undetected or are mistaken for other website performance issues. As DNS attack strategies evolve, many solution providers either lack effective DNS DDoS protection, or their systems fail to identify these subtle yet damaging attacks. Without proper protection, your website or services could become slow or even entirely inaccessible, which can severely impact your business.

Impact on Your Infrastructure



Resource Exhaustion:

Continuous NXDOMAIN requests can overwhelm your DNS servers, leading to excessive CPU and memory usage.



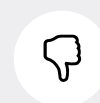
Service Disruption:

Legitimate users may experience delays or be unable to access services, leading to a poor user experience.



Increased Costs:

You may need additional resources and efforts to mitigate these attacks, driving up operational costs.



Reputation Damage:

Frequent service interruptions can tarnish your brand's reputation, eroding customer trust and loyalty.

How Corero Stops DNS Attacks

Introducing Corero SmartWall ONE™

SmartWall ONE is your ultimate defense against DNS DDoS attacks. Its advanced technology ensures your DNS infrastructure remains resilient and fully operational, even during severe assaults.

Key Features and Benefits



Real Time Protection

SmartWall ONE identifies DNS water torture patterns in real-time, delivering immediate responses to block the attacks.

Advanced algorithms distinguish between legitimate traffic and malicious requests, ensuring genuine users remain unaffected.



Proactive Threat Intelligence

The solution leverages global threat intelligence to stay ahead of evolving attack vectors. Continuous updates ensure protection against the latest DNS attack tactics.



Behavior Analysis

Monitors client behavior and blocks requests from IP addresses generating a high rate of NXDOMAIN, NXRRset, or SRVFAIL responses for a configurable period.



Optimized Resource Management

Lowers timeout for recursive name lookups to free up resources. Increases TTL on existing records to reduce the need for frequent updates.



Rate Limiting

Limits the rate of traffic to overwhelmed servers, preventing resource exhaustion.



Why Corero?



See Everything, Miss Nothing

We use advanced data analytics to give you a crystal-clear picture of what's happening, making it super easy to spot and understand DDoS attack patterns. You get all the details you need, minus the headache.



Quick on the Draw Against DDoS

We're always on guard, blocking those massive, headline-making, attacks and the sneaky, smaller ones that other systems might miss.



Sorting the Good from the Bad, Accurately and Automatically

We'll halt malicious DDoS traffic in its tracks, stopping it cold before it has a chance to disrupt your operations. And the cherry on top? We do all this seamlessly, ensuring your services run without a hiccup.



Cut Costs, Not Corners

Our automated defenses mean you spend less time and money dealing with DDoS headaches. SmartWall ONE keeps things running so smoothly, you'll wonder why you ever put up with anything less.



Set It and Forget It Protection

We'll handle DDoS attacks automatically, keeping everything connected and moving without you having to lift a finger.



On-Prem or Hybrid Protection

Enhance your cloud-only solution with our highly accurate, real-time, on-premises protection. Our hybrid protection is so seamless, you won't even know it's there.



Flexible to Fit Your Needs

No matter the deployment, SmartWall ONE molds to fit your setup. Physical, virtual, in the thick of it, or on the sidelines—we've got you covered, ensuring attacks are stopped before they can do any damage.



Amplify Your Profits and Your Services

If you're a service provider, SmartWall ONE is your golden ticket to offering top-tier, real-time DDoS protection as a service. Enhance your revenue streams while securing your customers' operations against disruptions, all without affecting their legitimate traffic.

Protect Your DNS Infrastructure with Corero SmartWall ONE

Don't let DNS attacks compromise your operations. Trust our SmartWall ONE to deliver unparalleled protection, ensuring your DNS infrastructure remains resilient and reliable.

Speak with a Specialist

Visit corero.com to discover how we can safeguard your business.