Security Solutions

White Paper

neustar

Five Ways Neustar Strengthens DNS Security

Table of Contents

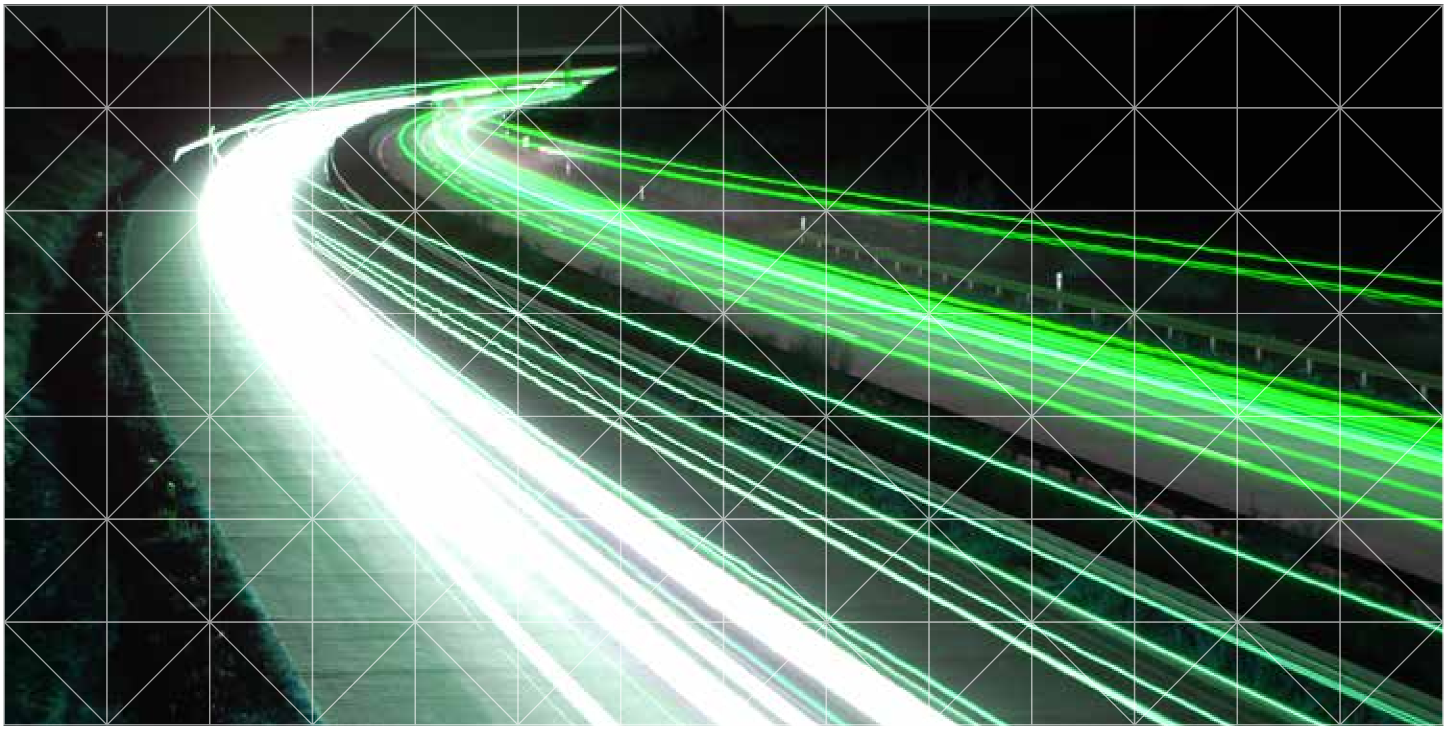
About DNS

The domain name system (DNS) grew to prominence during the early, innocent days of the Internet. During that time, Reagan-era users tended to work for government or educational organizations where trust was assumed and security was an afterthought. Since the online community was small and the Internet was sparsely used, the importance of DNS was not widely understood, and as a consequence, left undefended.

Fast-forward to today and you can see the resulting problems: criminals who redirect DNS queries to their own servers to steal credit card data and other sensitive information. There's also the exploding problem of distributed denial of service (DDoS) attacks, often aimed at DNS to cripple online business.

For businesses, the stakes are simple: no functioning DNS, no website or Internet presence.

Neustar, which has operated one of the world's largest, most trusted DNS networks for over 19 years, enhances DNS security in the following five ways.



1 DDoS Protection

Volumetric DDoS attacks have exploded in size to present day attacks exceeding 1 Tbps. Some of the largest attacks on record were aimed at DNS.

There Are Numerous Types of DDoS Attacks That Target DNS

DNS amplification is one of many attack methods. In this assault, attackers exploit the vast number of "open" DNS servers on the Internet which can be used to respond to any and all small look-up queries with a spoofed IP of the target. The target then receives much larger DNS responses that quickly overwhelms its capacity. The goal: block legitimate DNS queries by exhausting network capacity.

Another common type of attack is DNS floods, which are directed at the DNS servers hosting specific website(s). These try to drain server-side assets (for instance, memory or CPU), with a barrage of UDP requests, generated by running scripts on compromised botnet machines.

Neustar Offers Multiple Layers of DDoS Protection

To defend against all types of DNS-based attacks, UltraDNS comes with multiple layers of DDoS protection.

First, we equip all our DNS nodes with DDoS mitigation equipment. They constantly monitor for malformed traffic as well as traffic from suspicious locations in higher than normal volumes. In many cases, mitigation happens locally.

If an attack is supersized, we automatically re-route malicious traffic to the Neustar DDoS mitigation network (Neustar SiteProtect), a completely separate, purpose-built infrastructure. This limits any potential damage to the target nameserver IP's. With the impact isolated, the team in our 24/7 Security Operations Center is free to be more aggressive in their counter measures.

Speaking of Isolation...

2 Nameserver Segmentation

Throughout the industry, highly scalable DNS has become a cloud-based service with hundreds or thousands of customers—each with numerous domains—clustered on single networks and sharing a nameserver.

This increases the chances you'll feel someone else's pain. If you use a third-party DNS provider, most attacks on their network won't be aimed at you, but at a domain sharing your provider assigned nameserver.

It's Smart to Isolate the Impact of a DDoS Attack

Neustar organizes the UltraDNS network into segments, each with a nameserver announcement shared by only a small group of customers (dedicated name segments are available too). With fewer customers sharing host names and IP addresses, you face drastically lower odds of feeling a ripple effect.

Analogy time: Imagine being in a large hall with 10,000 people and one person jumps up screaming so loudly that nobody can hear the speaker. Now imagine that same scenario, but with just 20 other folks. The impact of the screamer is limited to just the 20 and when the screamer starts, Neustar's name server segmentation and DDoS mitigation strategy instantly moves the entire room to a sound proof area, removes the well behaved audience members, and works to muffle the screamer before bringing everyone else back in.

Be Protected Whether You or Someone Else Is Hit

This approach enables us to move individual nameserver announcements from the DNS network to the DDoS mitigation network without significantly delaying query resolutions. We can provide effective, immediate mitigation to those under attack AND prevent any collateral impact for customers still on the DNS network.

When using cloud provided DNS services, Being on a segmented nameserver announcement is an effective way to protect your DNS traffic.

3 Non-Open Source Resolver

DNS resolvers—the servers that respond to all those requests to resolve domain names—ensure that users are routed to the correct sites. The most common software application used to manage DNS is BIND, or Berkeley Internet Name Domain. Developed at the University of California at Berkeley in 1983, BIND still accounts for the vast majority of global name server implementations. Now fully in the public domain, the source code to BIND is readily available to be explored and exploited by malicious hackers.

Over the years, BIND has undergone a number of changes, with major revisions taking the code base from BIND version 4 to BIND version 8, and currently BIND version 9. But in terms of security, keeping up with the changes to protect a BIND-based DNS service is quite difficult. In fact, BIND is one of the all-time most common programs to be identified in the global notification system of vulnerabilities, known as CVE or Common Vulnerabilities and Exposures.

Slam the Door on Resolver Threats

Neustar UltraDNS solved that problem years ago. We developed a proprietary code and asked third-party security auditors to look for vulnerabilities. They found none that attackers could exploit remotely, either to steal restricted privileges or hamper directory resolution.

Besides supporting standard DNS specifications and RFCs (requests for comments), Neustar has enhanced our resolvers to extend the DNS capabilities while providing extra redundancy and security. Most legacy DNS server implementations never come close.

4 DNSSEC (DNS Security Extensions)

As they help Internet users find the sites they need, DNS servers query one another. To speed things up, servers cache results for a specified length of time. If there's a query for the same name before the resource record times out, a server will give the cached answer instead of querying another machine.

DNS Cache Poisoning Enables Pharming Attacks

While this improves efficiency, it also invites cache poisoning. This occurs when a DNS server, usually compromised by criminals, supplies a false answer to a DNS request. Users wind up on phony sites that ask for personal information or simply activate malware.

How can it happen? In many cases, DNS servers don't verify that the responses they receive from other servers relate to the original query. A server will cache bad information and pass it along to others that are DNS clients of the compromised machine.

To Protect You, DNSSEC Comes Standard with UltraDNS

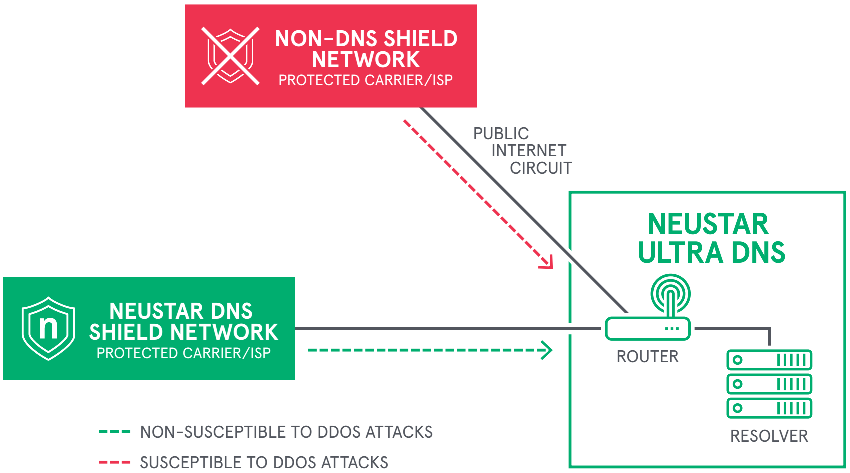
DNSSEC is a set of security extensions which authenticate DNS responses. The secret: a series of public/private key combinations to sign information resources. It works by providing a public key that allows the user's resolver to confirm that a DNS answer matches the cryptographic version. All transactions are signed—attackers can't simply spoof the packets.

In more basic terms, DNSSEC secures the DNS process by protecting against cache poisoning, pharming attacks and other serious threats.

5 DNS Shield™

As the old security adage goes, you're only as strong as your weakest link. But what if you could improve your strength posture by eliminating the weak links? By reducing the dependency on public internet connections, the DNS Shield network has essentially cut out the middle – and most dangerous – part of the DNS transaction where the vast majorities of DDoS attacks and DNS cache poisoning attempts take place.

HOW DNS SHIELD WORKS



The private network that the DNS Shield network employs offers three key benefits:

Lower Latency

In some cases, even if UltraDNS is working flawlessly, other Internet connectivity issues could cause degradation in DNS performance, thus leading to a poor user experience. By permitting DNS traffic to avoid general Internet networking, the DNS Shield Network provides an online experience that is both fast and efficient.

Enhanced Security

The recent IoT-enhanced DDoS attacks that made the Internet inaccessible will soon become a thing of the past. By creating a private network for DNS resolution within provider networks, the DNS Shield Network minimizes exterior threats like DDoS attacks and cache poisoning attempts.

Better Reliability

In the event of a DDoS attack or significant outage against UltraDNS, DNS queries will continue to resolve within the private networks where DNS Shield is deployed. This resiliency ensures a superior Internet experience for users looking for websites and other vital online assets.

Learn More About Neustar UltraDNS

Thousands of global companies rely on **Neustar UltraDNS**, including much of the Fortune 500 and the Alexa Top 100 online businesses. It delivers the performance they depend on—100% uptime, fast, accurate query responses and extreme scalability—plus the added security they need.

With 24/7 support from our Network and Security operations centers, Neustar fully manages your DNS so you can focus on the path ahead.

Learn more at:

www.security.neustar

About Neustar.

Every day, the world generates roughly 2.5 quadrillion bits of data. Neustar (NYSE: NSR) isolates certain elements and analyzes, simplifies and edits them to make precise and valuable decisions that drive results. As one of the few companies capable of knowing with certainty who is on the other end of every interaction, we're trusted by the world's great brands to make critical decisions some 20 billion times a day. We help marketers send timely and relevant messages to the right people. Because we can authoritatively tell a client exactly who is calling or connecting with them, we make critical real-time responses possible. And the same comprehensive information that enables our clients to direct and manage orders also stops attackers. We know when someone isn't who they claim to be, which helps stop fraud and denial of service before they're a problem. Because we're also an experienced manager of some of the world's most complex databases, we help clients control their online identity, registering and protecting their domain name, and routing traffic to the correct network address. By linking the most essential information with the people who depend on it, we provide more than 12,000 clients worldwide with decisions—not just data.

More information is available at

www.home.neustar