Neustar® Insights

It's Time for a Serious Talk

3 Questions to Ask Your DNS Host about Lowering DDoS Risks

By Link King, Senior Technologist, Neustar

neustar®
Real Intelligence. Better Decisions.™

It's no secret that DDoS attacks are worsening by the day. From the largest financial institutions to smaller Internet companies, everyone's a target—including DNS providers like us. Neustar provides UltraDNS and recently dealt with an attack on our network that was massive by industry standards, impacting our customers and even our upstream providers.

In the weeks since, we've had wide-ranging conversations with clients wanting to know how they can optimize protection as DDoS attacks increase in frequency and size. Most of these conversations boil down to three key questions and form the conversation you should be having, too—whether you use Neustar, another provider or your in-house team to manage your external DNS.

1. How do you handle DDoS attacks against your DNS infrastructure?

That is, what technologies does your provider use to identify and mitigate attacks? Ask specifically about types of DDoS mitigation hardware. Does your provider use diverse equipment to block different types of attacks?

Whoever your DNS provider is, make sure they layer their defenses. It's a best practice to mitigate attacks locally, with always-on equipment deployed on premise, plus a failover to the cloud when attacks become too large. This hybrid approach lets DDoS responders mitigate as soon as attacks appear and use cloud-based bandwidth to scale up defenses. Attack sizes have grown significantly, with the largest recorded attacks growing 1000% since 2008, from 40 Gbps to 400+ Gbps in 2014. Extra cloud capacity is no longer a "maybe we should" but a must-have.

In layering our protection, Neustar equips all our DNS nodes with DDoS mitigation equipment. They constantly monitor for traffic that's malformed or coming from suspicious locations in higher than normal volumes. In many cases, mitigation happens locally. But if an attack is supersized, our policy is "Shoot first and ask questions later" as we migrate malicious traffic to the Neustar DDoS mitigation network—a completely separate infrastructure. We isolate DDoS-related traffic on a purpose-built mitigation network, removing that traffic from the DNS network without resolution delays. At that point, any potential damage is limited to the target nameserver IP's. Additionally, with impact isolated to just the target, we are free to be more aggressive with our countermeasures. This is a key component for managed DNS providers, coupled with.....

2. How would you shield my domains from attacks on other customers?

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 nameserver announcements. This increases the chances you'll feel someone else's pain. Most attacks your provider deals with won't be aimed at you but at a domain sharing your nameserver announcement.

It's crucial to know how your provider isolates traffic. Neustar, for instance, organizes our DNS network into segments, each with a nameserver announcement shared by only a small group of customers (dedicated name servers are available too). With many fewer customers sharing host names and IP addresses, you face drastically lower odds of feeling a ripple effect. This DDoS protection-centric approach enables us to move individual name server announcements from the DNS network to the DDoS mitigation network, again, without interrupting resolution. We can provide effective, immediate mitigation to those under attack AND prevent any collateral impact for customers still on the DNS network.

Making sure you're on a segmented nameserver announcement—and they come with different architectures—is the single most effective way to protect your DNS traffic. Yes, segmentation means work for you. You'll need to work with your provider to move all those domains. It's worth it, though. The proof? During the attack that hit Neustar's network, most of our segmented customers felt little or no impact. Those experiencing latency or brief loss of service were part of a larger group that hadn't yet moved their domains onto more specialized name server announcements.

3. How would you handle an attack against one of my domains?

To a degree, the answer to this might echo the technology discussion above, focusing on hardware, network architecture, cloud-based tools and more. But it's not all about machines. People and process matter, too.

In a DDoS emergency, there's no substitute for having the right skill sets. Ask your DNS provider or any you might consider about the people on their DDoS mitigation team. Whether they're in-house or hired hands, you need to know what kind of experience they have. And don't be afraid to get in the weeds. How exactly do they handle specific signatures: malformed DNS, TCP SYN attacks, TCP queries or legitimate UDP/53 queries? What kind of training do they undergo and how often do they run drills?

Better yet, see if they offer simulations of attack responses. To line up a WebEx simulation from the Neustar Security Operations Center, contact us. Or inquire about visiting our SOC and meeting our DDoS responders. Besides getting the details you need about their backgrounds and methodologies, you'll establish something that pays off later: good communication.

Don't wait to have the talk.

Maybe you've seen these numbers or others equally bad. DDoS happens an average of 3,000 times a day. According to Neustar's 2014 DDoS Attacks and Impact Report, 71% more companies were targets last year than in 2012. More than 40% estimated revenue losses at over $1M a day.

Start the conversation with your DNS host today.DDoS isn't going away, but you can contain it. As always, asking the right questions is your best first step.

About Neustar

Neustar, Inc. (NYSE: NSR) Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services and data analytics, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time. More information is available at **www.neustar.biz.**

21575 Ridgetop Circle, Sterling, VA 20166
+1 571.434.5400 / www.neustar.biz

3 Questions to Ask Your DNS Host about Lowering DDoS Risks -v061214

neustar®
Real **Intelligence.** Better **Decisions.**™