Taking Down Twitter as easy as D.N.S.

Lori MacVittie, 2009-06-08

If they can take down Twitter via DNS, they can take your site, too.

Everyone is talking about the DoS (Denial of Service) attack on Twitter but most of them are missing what really happened. We're so used to defending against *HTTP*-based DoS attacks that we've missed that it's much easier to DoS a site based on the most critical piece of infrastructure on the Internet: DNS.

If you really wanted to take out a site like Twitter or Facebook using an HTTP-based DoS it would take a whole lot of serious traffic because those sites are designed and architected to handle millions of users making millions of requests *every second*. But if you wanted to take out a big site like that with a lot less effort (or bots) all you'd need to do is … right. Take out their nameservers (DNS).

As has been pointed out by this Threat Chaos post (and many others via Twitter – when they could actually get through) there appears to have been a sudden *decrease* in Twitter traffic around 9am EDT, not an *increase* as would be expected with a traditional HTTP-based DoS attack. If you then take a look at another post from Threat Chaos on the subject, you'll see that there was, in fact, a DNS attack perpetrated that affected Twitter:

> *DYNECT.NET Is a global load balancing service that must have taken the brunt of the attack against Twitter this morning. Their managed DNS service DYNDNS reports:*
>
> *DynDNS WebHop DDoS*
> *Thu, 06 Aug 2009 1632 UTC*
>
> *Beginning at approximately 1630 UTC, DynDNS servers experienced a very high traffic spike in our Newark Data Center. The high traffic resulted in an interruption in service for our website, NIC update, and WebHop. The WebHop service is currently down as we continue to investigate the source of the traffic.*
>
> *Update: 1755 UTC – DynDNS.com WebHop service is now functional. All of our other services (including our DNS services on DynDNS.com and Dynect Platform) have been fully functional during this entire time.*

The evidence appears to be pointing toward a DNS DoS as the culprit. That's still an attack *against* Twitter, but it's a very different set of concerns – and ultimately solutions – that need to be discussed if that turns out to be true.

UPDATE (8-7-2009): Dynect writes that the DNS issue referenced by ThreatChaos was unrelated to the attack; Twitter's DNS resolution services remained available throughout the attack. As Russ Garrett points out in a comment this is looking more like a typical old DoS attack.

DNS CRITICAL COMPONENT

Even if it turns out that the DNS DoS wasn't wholly responsible for Twitter's outage (and it's looking more and more that way), it still should force us all to take a moment and consider the ramifications of an attack on *our* DNS infrastructure.

DNS is one of the more (if not the most) critical components in an IP-based architecture. Without it we can't even *find* Twitter let alone interact with the site. That Twitter was attacked this morning is obvious and already heavily written about, but the importance of the attack on its nameservers has not been widely mentioned despite how much more of an impact an attack on DNS is to the availability of a web site and *all* its services it is than a simple HTTP-based DoS.

Without DNS nothing works: e-mail, web, voice, nothing. Everything relies upon those two servers that sit, lonely, translating host names to IP addresses for the world. DNS is under considerable strain all the time, and whether it's an attack or a sudden "event of interest", the additional strain of more queries can easily take a site down faster than even the ensuing traffic. Consider MSNBC during the 2008 U.S. Presidential election. Their site normally sees a lot of traffic, but spikes on election night drove over ***20 million unique visitors*** to view the ongoing results. That's 20 million people who were likely saturating DNS servers with requests, ostensibly with huge percentages of them at the same time – every hour when another poll closed. When we talk about how well their "infrastructure" performed it is often abstracted; we just say "their site" and leave most people believing that they must have some awesome infrastructure and applications running to support that high volume of traffic.

But that does an incredible disservice to the underlying infrastructure that while not as visible or sexy ends up being infinitely more important when you get down to brass tacks.

We have an infinite array of tools and tricks and processes around securing web applications, web servers, and web sites in general. We have multi-layer security in our application delivery controllers / load balancers, web application firewalls, firewalls, IPS, IDS, and access control. But we have very little comparatively speaking in the way of DNS-specific protections. We can't really limit access to them because, well, they ***must*** be available publicly and anonymously because that's the way the Internet works.

We may never know ***exactly*** what took out Twitter today. But we don't need to know to be able to take away a valuable lesson, albeit at the expense of Twitter and its users: DNS needs to be treated with a bit more respect. Its importance to availability and reliability should not be underestimated, nor should it simply be deployed in a corner and ignored.

- DNS for Twitter was attacked as well
- Rip and Replace Won't Solve Twitter's (Or Your) Security Problems
- Twittergate Reveals E-Mail is Bigger Security Risk than Twitter
- Cloud Balancing, Cloud Bursting, and Intercloud
- Intercloud: The Evolution of Global Application Delivery

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com