NETWORKWORLD

How the Dyn DDoS attack unfolded

A massive botnet patched together and deployed around the world swamped regional DNS data centers

By Tim Greene
Executive Editor, Network World

OCT 21, 2016 4:52 PM PT

Today's attacks that overwhelmed the internet-address lookup service provided by Dyn were well coordinated and carefully plotted to take down data centers all over the globe, preventing customers from reaching more than 1,200 domains Dyn was in charge of.

The attacks were still going on at 7 p.m. Eastern time, according to ThousandEye, a network monitoring service.

Dyn’s service takes human-language internet addresses such as www.networkworld.com and delivers the IP addresses associated with them so routers can direct the traffic to the right locations.

By flooding Dyn, the attack prevented traffic from reaching Dyn’s customers, who include Amazon, Etsy, GitHub, Shopify, Twitter and the New York Times.

The DDoS attack force included 50,000 to 100,000 internet of things (IoT) devices such as cameras and DVRs enslaved in the Mirai botnet, as well as an unknown number of other devices that are parts of other botnets, says Dale Drew, CSO of Level 3. He theorizes the mastermind behind the attack hired multiple botnets to compile the number wanted for the attacks.

It seems careful planning went into the attacks in order to insure that Dyn’s services were crippled worldwide, says Nick Kephart, Network Outage Analyst at ThousandEyes.

He says the first wave of the attack came against three Dyn data centers – Chicago, Washington, D.C., and New York - affecting mainly the East Coast of the U.S. because DNS lookups are routed to the nearest data center.

The second wave, which he says was ongoing at 7 p.m. Eastern time, hit 20 Dyn data centers around the world. This phase of the attack required extensive planning. Since DNS request go to the closest DNS server, that means the attacker had to plan a successful attack for each of the 20 data centers. That means having for enough bots in each region to be able to take down the local Dyn services, he says.

Drew says the attack consisted mainly of TCP SYN floods aimed directly at against port 53 of Dyn's DNS servers, but also a prepend attack, which is also called a subdomain attack. That's when attackers send DNS requests to a server for a domain for which they know the target is authoritative. But they tack onto the front of the domain name random prepends or subnet designations. The server won't have these in its cache so will have to look them up, sapping computational resources and effectively preventing the server from handling legitimate traffic, he says.

If the attack were against just one domain, it would indicate the attacker wanted to harm the owner of that domain, he says. In this case, the attack was across the range of domains Dyn was authoritative for, indicating that interrupting Dyn's services was the goal.

He says that Mirai, the malware behind gigantic IoT botnets, was involved. About 10% to 20% of all the 500,000 or so known Mirai bots were involved, but so were other devices.

Drew says Level 3 engineers are trying to figure out how many different devices in all were involved in the attacks.

ThousandEyes observed peering relationships between Dyn and internet providers breaking during the day, either because the connections failed or one or both parties decided it was in their best interests to do so.

Kephart says the botnet traffic headed to Dyn could have caused enough congestion at the edges of the internet backbone providers' networks that they cut them so legitimate traffic not even headed for Dyn could get through. For example, ThousandEyes noted that Level 3 broke its connection to Dyn.

Short of cutting them off, major internet backbone providers certainly had to reroute some traffic to avoid congestion the Dyn attacks created.

The attack was one of the largest against a DNS provider in terms of global scope, the duration of the attack and the numbers of domains – more than 1,200, conservatively – that were hit, Kephart says.

He says that given the large IoT botnet attacks over the past month, he expects more similarly effective attacks.

ThousandEyes observed Dyn customers either going to backup DNS providers, as Amazon did, or signing up with an alternative today after the attacks, as PayPal did.

Enterprises might look at lowering their time-to-life settings on their DNS servers so when attacks like this occur they can redirect traffic faster to another DNS service that is still available.

“It is really ominous,” Kephart says. “What’s scary is that it shows how some critical infrastructure is so important to so many services,” and that that infrastructure is vulnerable.

Join the Network World communities on Facebook and LinkedIn to comment on topics that are top of mind.

Tim Greene covers security and keeps an eye on Microsoft for Network World.

Follow

Must read: 10 new UI features coming to Windows 10

YOU MIGHT LIKE