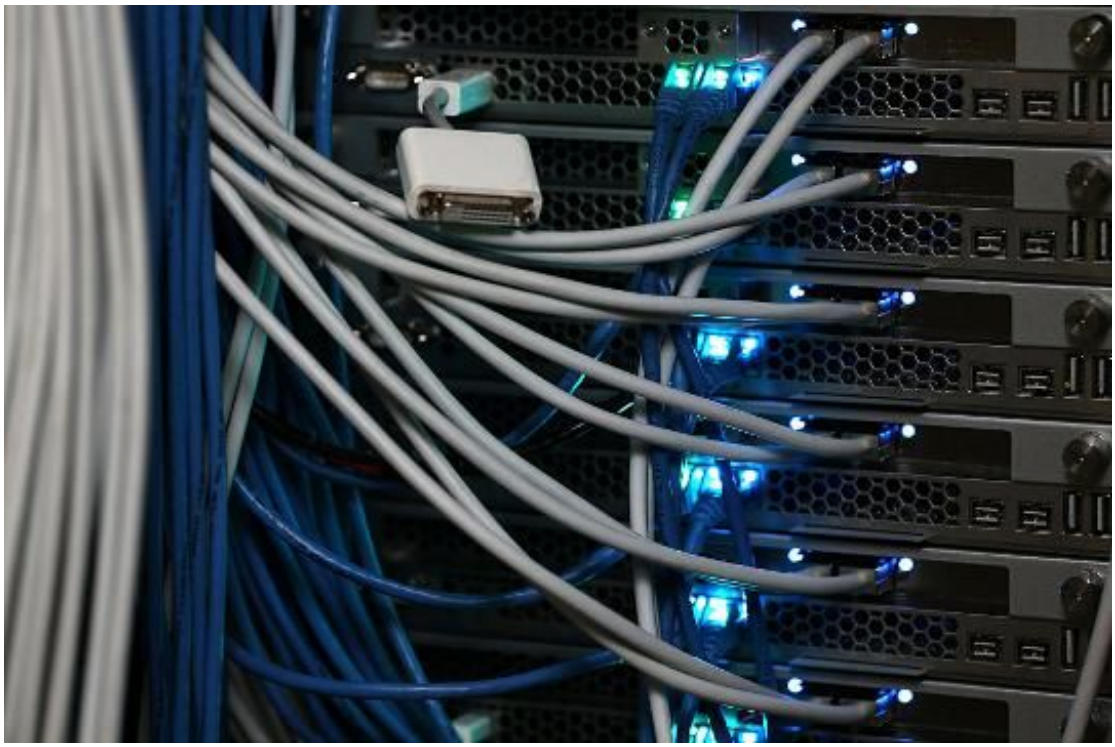
# Waves of cyber attacks hit Netflix, Spotify, Twitter

usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/

10/21/2016



If you live on the East Coast and had trouble accessing Twitter, Spotify Netflix, Amazon or Reddit Friday morning, you were not alone. USA TODAY

SAN FRANCISCO — At least two successive waves of online attacks blocked multiple major websites Friday, at times making it impossible for many users on the East Coast to access Twitter, Spotify, Netflix, Amazon, Tumblr and Reddit.

The first attacks appear to have begun around 7:10 am Friday, then resolved towards 9:30 am, but then a fresh wave began.

The cause was a large-scale distributed denial of service attack (DDoS) against Internet performance company Dyn that blocked user access to many popular sites standstill.

Dyn reported the sites going down at around 11:10 a.m. UTC, or roughly 7:10 a.m. ET, posting on its website that it "began monitoring and mitigating a DDoS attack against our Dyn Managed DNS infrastructure."

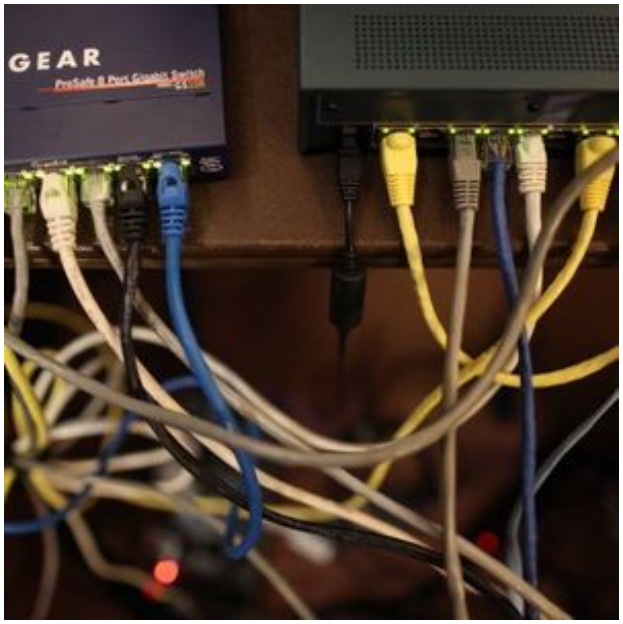
In an update posted at 8:45 a.m. ET, the company confirmed the attack, noting that "this attack is mainly impacting US East and is impacting Managed DNS customers in this region. Our Engineers are continuing to work on mitigating this issue."

White House Press Secretary Josh Earnest said the Department of Homeland Security was “monitoring the situation" but that “at this point I don’t have any information about who may be responsible for this malicious activity.”

It was unclear Friday if the attacks are focused on Dyn specifically or companies that it provides services to, said Carl Herberger, vice president of security at security company Radware.

The attack is “consistent with record-setting sized cyberattacks seen in the last few weeks,” he said.

He noted that easy-to-use computer code that allows even amateurs to create to create robot networks, so-called 'bot nets', to attack websites was released by hackers earlier this month




Amazon, whose web service AWS hosts many of the web's popular destinations including Netflix, also reported East Coast issues around the same time. In an update posted at 9:36 a.m. ET it said that it had "been resolved and the service is operating normally."

Amazon noted that it was suffering from a "hostname" issue and it was not immediately clear if it was related to the DDoS attack Dyn received.

Denial of service attacks are when someone, or a group of people, floods a particular site or service with large amounts of fake traffic in an attempt to overwhelm the system and take it offline. It was not immediately clear who initiated Friday's attack or why.

A post on Hacker News first identified the attack and named the sites that were affected. Several sites, including Spotify and GitHub, took to Twitter this morning to post status updates once the social network was back online.

Twitter users similarly took to the service to keep lists of which sites were down and comment on the situation. The term DDoS quickly vaulted to among the top of the site's list of "Trending Topics" in the United States.

"DDoS attack this morning takes out Reddit, Twitter & Spotify," wrote user @Anubis8. "Work productivity increases by 300%."

"Anyone else having a whole lot of trouble with sites loading properly this morning?," tweeted Emmy Caitlin. "Paypal is down, Twitter was down, Netflix half loading."

**How the attack works**

Dyn provides DNS service, effectively an Internet address book for companies and that’s what’s being attacked said Steve Grobman, chief technology officer for Intel Security.

DNS stands for Domain Name Servers. These are computers that contain databases of URLs and the Internet Protocol addresses they represent.

"If you go to a site, say www.yahoo.com, your browser needs to know what the underlying Internet address that’s associated with that URL is. DNS is the service that does that conversion,” said Grobman.

For example, the IP address for yahoo.com is 209.191.88.254.

The attack is on the Dyn server that contains that address book. Dyn provides that service to multiple Internet companies, so when someone types in twitter.com or tumblr.com or Spotify.com, via a complex series of jumps the address book is able to tell their browser which numerical IP address to look at.

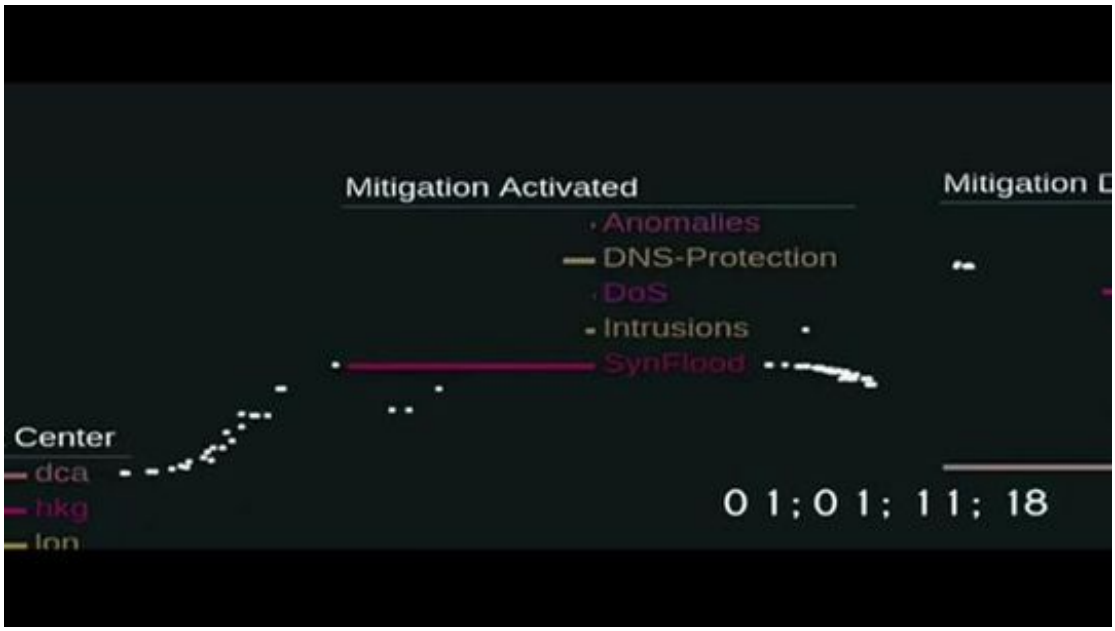
The DDoS attack floods that server with illegitimate requests, so many that very few real requests can get through. The user gets a message that the server is not available. Service is intermittent because a few requests are

sometimes still able to go through.

In addition, many sites keep cached address books their computers can refer to. However those caches always have a time limit on them and when that “time to live” expires, they must go back to the DNS server to confirm the IP address is valid. If the DNS server is unavailable, a site that was working could suddenly stop being available, said Grobman.

*Follow Eli Blumenthal on Twitter @eliblumenthal*

*Elizabeth Weise covers technology and cybersecurity for USA TODAY. Follow her at @eweise.*




This Distributed Denial of Service attack directed at a large financial institution is one of the largest ever recorded.