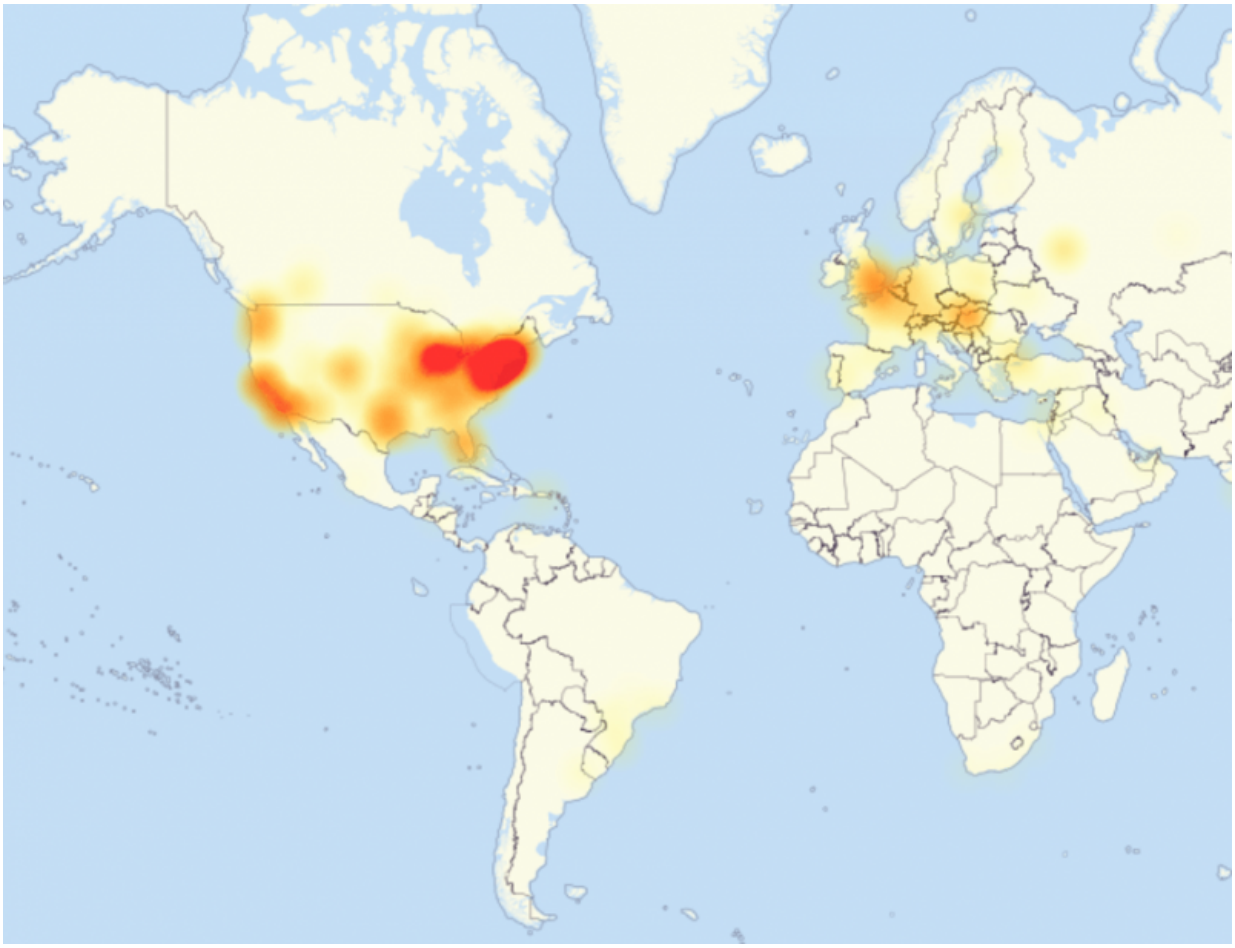
# Is someone really trying to find out if they can destroy the internet?

October 24 2016, by David Glance



Level 3 Outage Map. Credit: Downdetector.com

A prolonged Internet outage prevented access to major sites like Twitter,

Netflix, Spotify and The New York Times on Friday. The attack has commentators concerned that this is was a practice run for future, promising more frequent and widespread disruption of the internet. The distributed denial of service attack (DDoS) targeted the dynamic domain name service provider Dyn and came in three waves during the day.

Dyn provides internet address translation through DNS servers to take a name like www.nytimes.com and translate it into an address like 170.149.159.130. Denial of service attacks use a variety of techniques to keep the DNS servers busy. The attacks work by flooding DNS servers with millions of requests that seem legitimate but are for fake addresses, causing the DNS server to get overloaded. Real DNS requests from real users can't get through and so it appears that the site they are trying to get to, like www.netflix.com is down.

DNS attacks operate in a number of different ways but those that affected the Dyn servers were using a range of techniques that included sending requests for sites that had random characters attached to the start of a valid domain e.g. abcd123.nytimes.com. Because these addresses are essentially valid, the DNS server tries to look up the address but gets tied up because of the sheer volume of requests. The attacks are difficult to guard against because the requests are essentially valid.

The sheer volume of requests were being sent in part by the Mirai botnet of Internet of Things devices, mostly internet-connected cameras and digital video recorders. This botnet has been in a previous attack this month on the website of a security reporter Brian Krebs.

These types of attacks have been occurring more frequently and because they involve pieces of internet infrastructure, have a more widespread impact. Last month, security analyst Bruce Schneier wrote that he believed that state actors were increasingly probing for weaknesses in the basic infrastructure of the internet in order to be able to mount large-

scale devastating attacks. Because of the increase in number and intensity of DDoS type attacks in recent years, security analysts have theorised that some of the attacks are masking the probing of vulnerabilities.

A particular fear is that a DDoS attack could prevent people from voting online during the US election on November 8th. Overseas military and citizens are allowed to vote online in several US states and everyone in Alaska can vote online. Russia has already been implicated in the hack of Democratic National Committee emails and organising their release through WikiLeaks. There is concern that the Russians will try and discredit the election process in whatever way they can and disrupting it through a DDoS attack on the day would be one way of achieving this.

The risk of this actually effecting the vote on the day has been dismissed however as the window for voting online in some of these situations is weeks before the election rather than on the day. When Alabama trialled online electronic voting during the primaries, their site was in fact attacked, but although it slowed down the site, it didn't prevent anyone from voting.

There is also the possibility that this attack was actually just hackers going after a particular site that happened to be using the Dyn service. The source code for the Mirai botnet was released on October 1st and since that time, other hackers have been using the code to expand the number of bots involved and create their own botnets. DDoS attacks may actually just be hackers testing out the power of their creations.

The internet remains incredibly vulnerable to attacks on its infrastructure and right now, there are few ways of avoiding them. Because Internet of Things devices like cameras, digital video recorders, and a whole range of other equipment are being used as vehicles to launch DDoS attacks, making sure that the devices are secure would be a priority. However,

manufacturers are creating these devices in a way that doesn't allow for automated, un-monitored updates which is what is really required for security patches to be applied when they are discovered. Governments could potentially legislate that they should take all efforts to ensure their devices are secure before allowing the public to connect them to the internet, but this would need all countries of the world to do this.

It does bring into question the ability of governments to put even more of its interface with the public online since as soon as it does, it becomes a potential target for malicious actors. Governments in particular need to become more adept at dealing with this possibility, especially after the Australian Bureau of Statistics demonstrated that it was unable to run an online census collection successfully in the face of relatively minor DDoS attacks.

*This article was originally published on* The Conversation. *Read the* original article.

Source: The Conversation