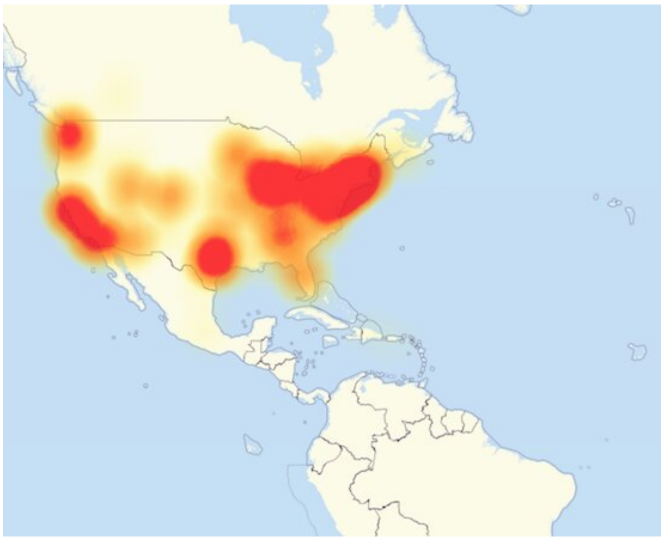
Four years since the Mirai-Dyn attack… is the Internet safer?

30 October 2020, by Daniel Tkacik



In October 2016, the Mirai-Dyn cyberattack crashed large portions of the Internet in North America for several hours. Credit: Wikimedia Commons

On October 21st 2016, millions of household IoT devices were infected with the malware Mirai and instructed to send data requests to Dyn, a widely used Domain Name Server (DNS) that acts like a switchboard for the Internet. This tidal wave of requests crashed over 175,000 domains—including Twitter, PayPal, and other web giants—for several hours, affecting tens of millions of users.

Four years later, is the Internet more resilient? A team of Carnegie Mellon University CyLab researchers are presenting a new study aimed at answering that very question at this week's Internet Measurement Conference.

"It seems that the lessons learned from the 2016 Dyn attack have only been acted upon by a handful of websites that were directly impacted," says Aqsa Kashaf, a Ph.D. student in Electrical and Computer Engineering (ECE) and lead author of the new study.

The Mirai-Dyn attack in 2016 was successful because of what Kashaf and her team refer to as critical dependencies. The domains affected by the Mirai-Dyn attack were critically dependent on Dyn, a third-party DNS. In other words, they relied solely on Dyn, so when Dyn went down, so did they.

To assess how websites have (or have not) changed since the 2016 attack, Kashaf and her co-authors analyzed 100,000 of the most popular websites as ranked by Alexa Internet, a web traffic analysis company. They looked at the dependencies of those websites in 2016 and then compared them with dependencies in 2020.

"Since the Dyn attack had such a huge impact, you would think websites would adapt as a result," says Kashaf.

Turns out, overall, critical dependency on DNS providers has in fact increased around five percent in 2020 compared to 2016. However, the researchers note, more popular websites have adapted to decrease their critical dependency.

"We interpret this to mean that the most popular websites care more about availability than the less popular ones," says Kashaf.

The researchers also focused on dependencies of two other services associated with delivering content to users online, both of which are performed in the blink of an eye when a user navigates to a website: content delivery networks, which host and deliver the content a user sees (e.g., video content for streaming), and certificate validation from a certificate authority, which confirms a secure connection.

The researchers found similar results: they observed little to insignificant changes in critical dependencies relative to 2016, but the most popular websites had decreased their dependencies.

This problem of critical dependencies isn't unique to websites, the researchers say. They ran two preliminary case studies of two other sectors—hospitals and smart home companies—and found that third-party dependencies leave these sectors vulnerable to Mirai-Dyn-like attacks as well.

"One obvious recommendation for websites is that they should build in more resilience and redundancy when using third party services," says Kashaf. "…and service providers need to support and encourage this redundancy. You can't have just a single point of failure."

Moving forward, the researchers envision building a tool that would allow web administrators to easily analyze and inspect their own website's dependency structure, empowering them to make informed decisions in choosing new service providers.

More information: Aqsa Kashaf et al. Analyzing Third Party Service Dependencies in Modern Web Services, *Proceedings of the ACM Internet Measurement Conference* (2020). DOI: 10.1145/3419394.3423664

Provided by Carnegie Mellon University
APA citation: Four years since the Mirai-Dyn attack… is the Internet safer? (2020, October 30) retrieved 17 January 2021 from https://techxplore.com/news/2020-10-years-mirai-dyn-internet-safer.html