Dyn Statement on 10/21/2016 DDoS Attack

OCTOBER 22, 2016 **KYLE YORK (HTTP://HUB.DYN.COM/AUTHORS/KYLE-YORK)**

It's likely that at this point you've seen some of the many news accounts of the Distributed Denial of Service (DDoS) attack Dyn sustained against our Managed DNS infrastructure this past Friday, October 21. We'd like to take this opportunity to share additional details and context regarding the attack. At the time of this writing, we are carefully monitoring for any additional attacks. Please note that our investigation regarding root cause continues and will be the topic of future updates. It is worth noting that we are unlikely to share all details of the attack and our mitigation efforts to preserve future defenses.

I also don't want to get too far into this post without:

1. Acknowledging the tremendous efforts of Dyn's operations and support teams in doing battle with what's likely to be seen as an historic attack.
2. Acknowledging the tremendous support of Dyn's customers, many of whom reached out to support our mitigation efforts even as they were impacted. Service to our customers is always our number one priority, and we appreciate their understanding as that commitment means Dyn is often the first responder of the internet.
3. Thanking our partners in the technology community, from the operations teams of the world's top internet companies, to law enforcement and the standards community, to our competition and vendors, we're humbled and grateful for the outpouring of support.

Attack Timeline

Starting at approximately 7:00 am ET, Dyn began experiencing a DDoS attack. While it's not uncommon for Dyn's Network Operations Center (NOC) team to mitigate DDoS attacks, it quickly became clear that this attack was different (more on that later). Approximately two hours later, the NOC team was able to mitigate the attack and restore service to customers. Unfortunately, during that time, internet users directed to Dyn servers on the East Coast of the US were unable to reach some of our customers' sites, including some of the marquee brands of the internet. We should note that Dyn did not experience a system-wide outage at any time – for example, users accessing these sites on the West Coast would have been successful.

After restoring service, Dyn experienced a second wave of attacks just before noon ET. This second wave was more global in nature (i.e. not limited to our East Coast POPs), but was mitigated in just over an hour; service was restored at approximately 1:00 pm ET. Again, at no time was there a network-wide outage, though some customers would have seen extended latency delays during that time.

News reports of a third attack wave were verified by Dyn based on our information. While there was a third attack attempted, we were able to successfully mitigate it without customer impact.

Dyn's operations and security teams initiated our mitigation and customer communications process through our incident management system. We practice and prepare for scenarios like this on a regular basis, and we run constantly evolving playbooks and work with mitigation partners to address scenarios like these.

What We Know

At this point we know this was a sophisticated, highly distributed attack involving 10s of millions of IP addresses. We are conducting a thorough root cause and forensic analysis, and will report what we know in a responsible fashion. The nature and source of the attack is under investigation, but it was a sophisticated attack across multiple attack vectors and internet locations. We can confirm, with the help of analysis from Flashpoint and Akamai, that one source of the traffic for the attacks were devices infected by the Mirai botnet. We observed 10s of millions of discrete IP addresses associated with the Mirai botnet that were part of the attack.

Thank You Internet Community

On behalf of Dyn, I'd like to extend our sincere thanks and appreciation to the entire internet infrastructure community for their ongoing show of support. We're proud of the way the Dyn team and the internet community of which we're a part came together to meet yesterday's challenge. Dyn is collaborating with the law enforcement community, other service providers, and members of the internet community who have helped and offered to help. The number and type of attacks, the duration, the scale, and the complexity of these attacks are all on the rise. As a company, we have for years worked closely with the internet community to assist when others encountered attacks like these and will continue to do so.

It is said that eternal vigilance is the price of liberty. As a company and individuals, we're committed to a free and open internet, which has been the source of so much innovation. We must continue to work together to make the internet a more resilient place to work, play and communicate. That's our commercial vision as a company and our collective mission as an internet infrastructure community. Thank you.

Kyle York
Chief Strategy Officer

About the Author

Kyle York is Dyn's Chief Strategy Officer and has been a long-time executive, having joined in 2008. Over the years, he has held go-to-market leadership roles in worldwide sales, marketing, and services. In his role as CSO, Kyle focuses on overall corporate strategy, including: positioning and evangelism, new market entry, strategic alliances and partnerships, M&A, and business development. Outside of Dyn, Kyle is an angel investor, entrepreneur, and advisor in several startups. Follow Kyle on Twitter: @kyork20 (http://twitter.com/kyork20) and @Dyn (http://twitter.com/dyn).

Follow on Twitter (https://twitter.com/@kyork20) *More Content by Kyle York (http://hub.dyn.com/authors/kyle-york)*

NO PREVIOUS ARTICLES

NEXT ARTICLE

(http://hub.dyn.com/dyn-blog/recent-iot-based-attacks-what-is-the-impact-on-managed-dns-operators)

Recent IoT-based Attacks: What Is...

Everyone from the C suite to K Stre...

MOST RECENT ARTICLES

(http://hub.dyn.com/dyn-blog/recent-iot-based-attacks-what-is-the-impact-on-managed-dns-operators)

3 days ago (2016-10-20T08:55:00)

Recent IoT-based Attacks: What is the Impact On Managed DNS Operators?

Everyone from the C suite to K Street has seen the news of the most recent

Read Now

(http://hub.dyn.com/dyn-blog/balancing-new-markets-infrastructure-costs-and-performance-how-can-you-win-like-netflix)

4 days ago (2016-10-19T09:01:00)

Balancing New Markets, Infrastructure Costs, And Performance: How Can You Win Like Netflix?

The internet is such an attractive tool because it connectivity opens up the

Read Now

(http://hub.dyn.com/dyn-blog/ensure-your-infrastructure-s-performance-can-handle-black-friday-traffic-peaks)

10 days ago (2016-10-13T09:00:00)

Ensure Your Infrastructure's Performance Can Handle Black Friday Traffic

Finding the right technologies ahead of

Read Now

(http://hub.dyn.c
you-notice-the-c
internet-on-1-oc

11 days ago (2016-

**Did You Nc
Change in
On 1 Octol**

On Octobe

that the Ur
to "hand o

Read Nov

Return to Dyn Content Hub Home (http://hub.dyn.com/)