Column: Micro Economics

The Aftermath of the Dyn DDOS Attack

Shane Greenstein
Harvard Business School

Nobody knows who organized the attack. It might have come from an angry gamer, or from a rogue spy, or, perhaps, an angry rogue spy playing games. The program hijacked many cameras and home devices, and redirected them to engineer a series of distributed denial of server (DDOS) attacks on a few hours apart, all on October 21, 2016. By executing this novel and rather clever hijack of many devices for a DDOS attack, the attack exposed an important vulnerability in today's internet.

The attack contains one other element. It aimed at Dyn, who acts as a name resolver. Dyn enables Internet traffic by translating the site's domain name (URL) into the IP address where the server behind that domain is to be found. During the later phases of the attack, Dyn servers were unable to process users' requests, and as a result, users lost access to web domains contracting with Dyn, such as Netflix, CNBC, and Twitter. Other well-known firms also were disabled, such as Airbnb, Etsy, Play Station Network, and Wikia.

By executing this novel and rather clever hijack of many devices for a DDOS attack, the attack exposed an important vulnerability in today's internet.

This article focuses on the aftermath of this event, which did not get headlines, but illustrates an important features of the situation. Specifically, how did users react? User behavior tells us something about the challenges facing suppliers, and in this case, it tells us about a basic challenge in network security today. It will take a bit of work to appreciate the lesson, and, let me tip my hand, the news is not good.

The article provides a summary of a longer study done by a group of my colleagues and myself.[1]

What happened?

Start with the basics. A website owner can set up its own name resolver, or hire somebody to do it for them. Many years ago most firms did it themselves. Like a lot of things on the internet, over time a set of professional firms emerged, while many technically sophisticated firms still perform this function for themselves.

What do name resolvers do? Start with the basics. It is a mouthful, but we need to understand it to understand what happened to Dyn.

When an application (such as a web browser) wants to access a page or resource located at a known domain name, it can access DNS records and a corresponding IP address. In principle, the application submits a request to a DNS "resolver" asking for the IP address corresponding to a given domain name. The resolver queries a root nameserver, which replies with the corresponding to the TLD nameserver specified by the domain name (e.g., ".com"). The resolver then queries that TLD nameserver with the second component

Digital Object Identifier 10.1109/MM.2019.2919886
Date of current version 23 July 2019.

Published by the IEEE Computer Society

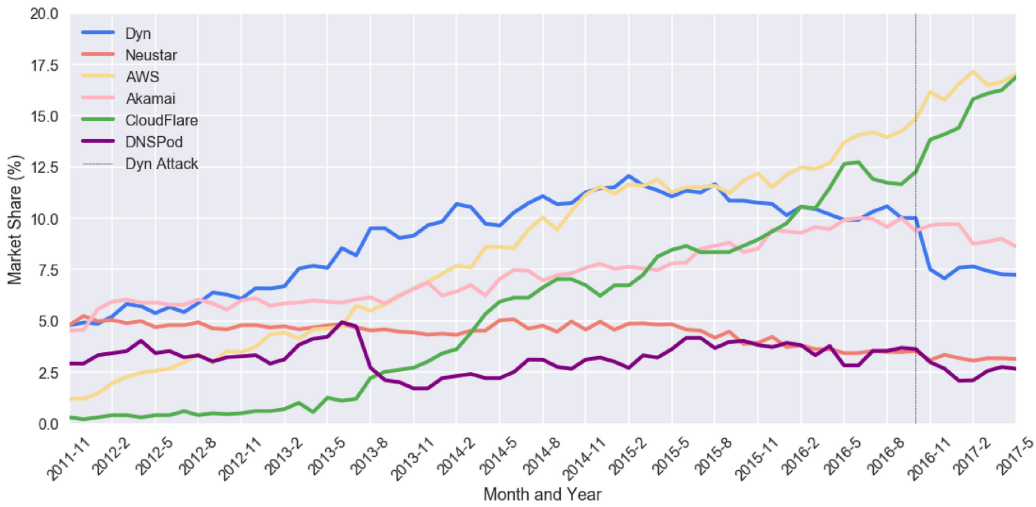

Figure 1. Market share for largest name servers.

of the domain name (e.g., "google"). The TLD nameserver retrieves that domain's authoritative nameservers (e.g., "ns1.google.com") and returns them to the resolver. Finally, the resolver queries one of the authoritative nameservers and receives a usable IP address for the domain. The IP address is passed back to the original application, which can use it to connect to the desired host. This entire process generally takes just milliseconds.

In practice, many users request the same thing repeatedly, so it is possible to cache the answers to many of the intermediate steps, and that can speed up the resolution even more. More to the point, caching across many servers acts as a quasi-buffer against a DDOS attack, especially if the attack can be rebuffed in a short time.

The emergence of numerous lessons and automated standard practices has gone hand-in-hand with the emergence of professional firms. Such firms know how to provide services at scale. In turn, and as with many other professional markets, some of them became good at their service, and that performance attracted many customers.

Thus emerged an ironic outcome. While the internet contains many points of resiliency, the increasing concentration of services in a small number of providers has created concentrated points of failure. To say it another way, Dyn performed approximately 10% of nameserver services in the United States (prior to the attack), so bringing it down could bring down 10% of the internet's servers. Since name resolution also supports a range of other communications, such as email, it could also cripple communications at many firms. That is a big deal.

As should be obvious, the potential economic losses could be enormous. Many businesses, especially internet businesses, lose a lot of revenue from being down for a day.

That motivates a basic question: after this attack, what did users do? It did not take much professional experience to understand the vulnerability or the lessons. Businesses were vulnerable to a single point of failure. A website could construct a form of insurance by performing a simple act: maintaining multiple name servers with multihoming.

We set out to find out two things. First, how many firms maintain multihoming? Second, how did the use of resolvers change after the Dyn attack? Figure 1, which is taken from Figure 7 of our study,[1] tells a big part of the answer we found. This figure shows the market shares for the largest providers of nameservers between late 2011 and the middle of 2017.

What did firms do?

Figure 1 shows that, long before the Dyn attack, name servers had embarked on a general trend toward more concentration. The growth of three firms—Dyn, AWS, and Cloudflare—drove this trend. Dyn's growth had already begun to level off by 2014, while AWS and Cloudflare have continued to grow unabated throughout the time period.

The figure actually does not tell the entire story. We did a little investigation, and found that both AWS and Cloudfare attract a high

fraction of the contracts from newly founded firms. Older firms tend to use others.

We also found that, as expected, over time an increasing fraction of users contracted with providers instead of doing it themselves. Close to 60% do it themselves in 2011, while close to 30% do it in 2017. In other words, the market shares rise during a time when the number of customers practically doubled.

The figure also illustrates the big surprise. The attack on Dyn had consequences for its commercial success. Many of its users seem to have blamed Dyn for the downtime, and shifted to another provider. Within a couple months Dyn lost a quarter of its customers. Ouch.

The least expensive insurance against another attack is multihoming with more than one resolver. Let us be clear about it: It is not expensive. It is just a minor hassle to maintain multiple suppliers.

But wait, that is not the only surprise. It is also important to notice *what did not happen:* We did not find much multihoming after the Dyn attack. Around 11% of existing domains multihomed prior to the Dyn attack, and about 18% did so after the attack. New domains multihomed at a rate of less than 5% prior to the attack, and after the attack about 8% did. In short, there was an uptick in multihoming, but the vast majority of sites continued to use a single provider.

Why does that matter? The least expensive insurance against another attack is multihoming with more than one resolver. Let us be clear about it: It is not expensive. It is just a minor hassle to maintain multiple suppliers. (And, moreover, many aspects of web administration are no worse a hassle. That is the job, after all.)

Not illustrated in the figure are minutia of market shares. In case you were wondering, most of the multihoming among existing websites came from customers of Dyn and somewhat from Neustar (another large provider). No other provider saw a big change.

You might reasonably reply that Cloudflare's security model makes it difficult to multihome, but does protect against this type of attack. Which is true. But what accounts for so little with all the others? Most users act as if they do not care.

CONCLUSION

Let us summarize. There was a DDOS attack on Dyn. It demonstrated a new vulnerability, and we are still vulnerable to another similar attack. In fact, we may be *more vulnerable* now that bad actors have watched the prior demonstration.

How did the user community act? The two big headlines are: 1) a fraction of customers acted as if they blamed Dyn, and took precautions; and 2) all but a small fraction of non-Dyn customers did not act as if they learned any lesson.

I do not know about you, but I do not feel any safer. Sigh.

REFERENCE

1. S. Bates, J. Bowers, S. Greenstein, J. Weinstock, and J. Zittrain, "In support of internet entropy: Mitigating an increasingly dangerous lack of redundancy in DNS resolution by major websites and services," NBER working paper 24317, 2018. [Online]. Available at SSRN: https://ssrn.com/abstract=3241740

Shane Greenstein is a professor at the Harvard Business School. Contact him at sgreenstein@hbs.edu.