Dyn DNS Cyberattack

By Bryce Kolton

12/7/2016 | INFO 312

Introduction

On October 21st 2016, a terabit sized attack took down internet connectivity for users across the globe. Over three waves, millions of users were interrupted during main business hours. The attack targeted Dyn (pronounced “dine”), a company that in part provides Domain Name Service registration for websites. Companies affected included Amazon, BBC, CNN, Comcast, Fox, GitHub, Netflix, PayPal, Reddit, Starbucks, Twitter, Verizon, Visa, Wikia and hundreds more.

Credit card terminals were inoperative, news sites unavailable, and users unable to reach some of the internet’s most popular websites. The internet ground to a halt for several hours, with major Fortune 500 companies among those affected. The focus of this risk management report will be the cyberattack at large; The background, causes, previous mitigations, response, still present risks, and recommendations after one of the largest cyberattacks ever recorded.

Understanding the Domain Name Service

As an illustrative example, let’s say you want to visit a new grocery store your friend just told you about, “Sya’s Grocery.” You know the name, but you need to find the physical address. By using a service like Google Maps, you can transcribe the human-readable name into the destination. The Domain Name Service works much the same way, but for URLs. When you type in “google.com,” your computer is clueless to the ‘real address’ it’s supposed to go to. That’s where DNS steps in: your device asks its closes DNS server “Who is ‘google.com’?” If the server doesn’t know, it’ll pass the request along until it finds a server that does. Once a request is found, the DNS responds “You can find ‘google.com’ at 216.58.193.110,” at which point your machine caches the result for a short amount of time and connects to Google’s servers.

The DNS is provided to regular web users for free; Dyn and other companies make their money off website owners who pay DNS companies to list their sites. Any DNS servers that are paid to keep the IP record are known as Primary DNS Servers, and never clear the entry from their data.

The DNS is required for the internet to function. If an end user’s DNS servers go down, the end user will need to reconfigure their device to another server or enter IP addresses directly. If all Primary Servers for a company go down, then the company’s websites are unreachable except by direct IP entry.

The Attacks

The first attack began at 7:10am Eastern. Dyn began receiving higher-than-average lookup requests on DNS servers in Asia, South America, Eastern Europe, and the Western US. All signs pointed to a Distributed Denial of Service attack. DDoS attacks are fairly common, and automated protection methods activated immediately. Shortly after as Dyn began to manually filter traffic, all attackers suddenly switched their targeted servers to the Eastern US servers, quickly overloading them, and bringing down thousands of websites for Eastern US internet users.[1]

Understanding DDoS Attacks

A Distributed Denial of Service is a type of cyberattack that relies on the use and control of many devices to repeatedly send bogus requests to a service, and consume all available bandwidth. DDoS attacks are frequently made by thousands or even millions of infected. DDoS attacks can be accurately visualized as hundreds of people trying to fit through one door, blocking out legitimate visitors.

Dyn quickly implemented high-strength traffic rate limiters, which limited the number of packets received to keep servers from crashing. Excess packets targeted at US East servers were then rerouted to other DNS servers across the globe. Finally, Dyn ran packet requests through internal system monitors, which scrubbed out bogus traffic, returning service to US East customers by 9:20am Eastern.

Two further attacks followed, one at 11:50am and another at 4:00pm. The second attack was stronger and more geographically diverse, but ultimately employed the same general technique. Dyn improved on their original strategy, and mitigated the attack in under an hour and a half. The third and final attack interrupted service minorly as Dyn became better at defending with its new methods.

An important aspect of DNS queries is expiration time. DNS records cached on non-Primary DNS Servers will auto-delete after a set amount of time. Thousands of records are deleted and re-requested at any given moment across the internet. As the attacks continued, other DNS servers made legitimate requests to DYN servers for IP address lookups. These legitimate requests were denied, at which point the requesting server continued to send lookup requests over and over. These legitimate requests amplified the attack, and Dyn estimates that legitimate DNS lookup requests reached nearly 20x regular traffic levels alone[2].

[1] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[2] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

Response and Analysis

News agencies were quick to jump on the story, in part because most themselves were affected. Speculators rose up, attributing blame to Russia[3], sparking fears over the imminent election[4], and generally causing panic. As the hours wore on, only to turn to days and then weeks, no party showed responsibility for the attack. Both hacktivist groups *Anonymous* and *New World Hackers* came forward and announced responsibility, but neither provided evidence. The vectors of attack were far more powerful and sophisticated compared to previous efforts by the groups[5], leading experts to cast doubt on the hacktivists' claims. The Department of Homeland Security announced a formal investigation in the days following the attack, but so far they have gleaned no new information[6]

Attacking the Domain Name System with advanced firepower is rare. Hacktivist groups typically divide their causes, and attack organizations or websites in highly targeted take-downs[7]. Attacking the DNS is like shooting the internet with a shotgun: imprecise, wide, and effective. Without a clear link between a specific organization and a supposed infraction, narrowing suspects becomes particularly difficult. Researchers suspected the program responsible for the attack to be Mirai, a popular botnet malware, which would usually aid efforts. However, Mirai's source code had been posted online prior to the attack, which further widens the suspect pool[8].

Internet of Things Devices

IoT devices are 'smart' devices that connect to the internet. They range in form and function from refrigerators to cars, baby monitors to routers, video cameras to doors. Many devices operate under a client-server model, whereby the device only talks to one or two other devices on the internet, usually being the manufacturers' servers for data reporting and updating. Most of these devices run Linux.

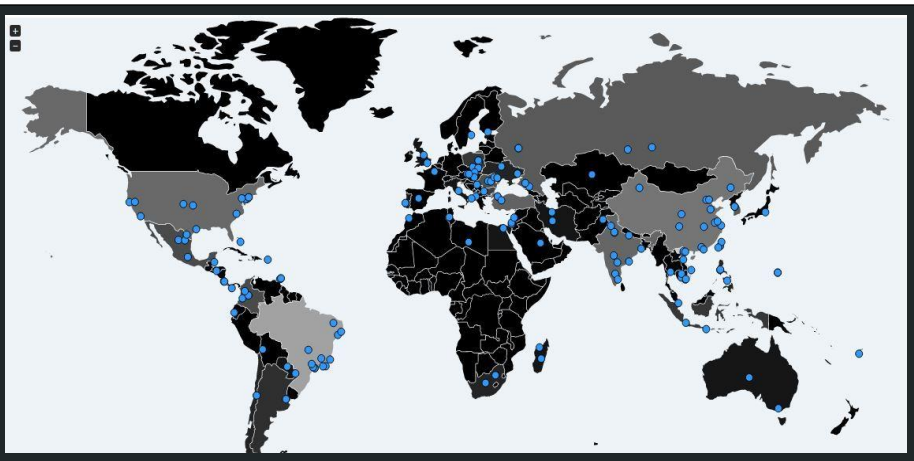
Although protected with a username and password, IoT device manufacturers will often post the default administrator login credentials online for users to login to their devices. These default credentials, if left unchanged, allow anyone to login upon the device's discovery.

Researchers and experts have grasped for understanding of the attack after tentatively ruling out Russia. Experts blame low-level 'script kiddies' to deep web criminals showing off capabilities before selling the botnet to buyer[9]. Ultimately, there still lacks a motive or suspect.

---

[3] http://heavy.com/news/2016/10/ddos-attack-cyber-russia-false-flag-us-putin-trump-obama-cia-north-korea-poodlecorp-netflix-twitter/
[4] http://mashable.com/2016/10/29/election-day-cyberattack/#feuR7nekUmqH
[5] http://www.politico.com/story/2016/10/websites-down-possible-cyber-attack-230145
[6] https://www.rt.com/usa/363705-third-ddos-attack-dyn-internet/
[7] http://www.wsj.com/articles/anonymouss-hackers-targeting-islamic-state-online-1447881328
[8] https://github.com/jgamblin/Mirai-Source-Code
[9] https://techcrunch.com/2016/10/26/dyn-dns-ddos-likely-the-work-of-script-kiddies-says-flashpoint/

Dyn's mitigation tactics, although not thoroughly novel, did advance previous DDoS defense methods. Throughout the attack, Dyn spread news and remained communicative [10]. Moving above and beyond the call, the company also produced and published advanced how-tos that detail steps to take if a company wants to set up DNS registrations with other registries[11] [12]; Telling customers to list with other DNS companies as well as theirs could lower overall revenue slightly, but speaks volumes to corporate responsibility and community involvement.



Mirai infected devices and their IP locations. Many are difficult to track.

Throughout the ordeal Dyn worked with other internet providers and their customers to resolve issues as quickly as possible. Dyn has reported an enormous outpouring of support and understanding from their major customers.[13]

Botnets and 'The Future'

Botnets are groups of compromised devices that check a centralized server for commands. Infection can happen through a variety of vectors, be it security lapses, poor firewalls, bad programming, or known login credentials.

Mirai (Japanese for "the future") is a malware program that slaves infected devices into a botnet. Mirai is the likely culprit for some of the largest DDoS attacks ever recorded. When it encounters a login screen, Mirai attempts common administrator credentials for IoT devices. If it breaches security, it then uninstalls other malware, and loads itself into memory. Now in direct administrative control, Mirai spams random IP addresses with login requests to further the botnet while periodically checking a listed command server for instructions. Mirai is curious in that when the device is restarted, the malware is removed; however, if the device remains unpatched, reinfection is assured.

The source code for Mirai was publicly posted to GitHub, an online code sharing website, weeks before the Dyn cyberattack. Anyone could easily download Mirai and begin a botnet with little experience

[10] http://hub.dyn.com/traffic-management/dyn-statement-on-10-21-2016-ddos-attack
[11] http://hub.dyn.com/traffic-management/how-multi-vendor-dns-can-protect-your-internet-presence
[12] http://hub.dyn.com/traffic-management/advanced-secondary-dns-for-the-technically-inclined
[13] http://hub.dyn.com/traffic-management/dyn-statement-on-10-21-2016-ddos-attack
Image http://defendmagazine.org/2016/11/01/hacking-back-the-mirai-botnet-technical-and-legal-issues/

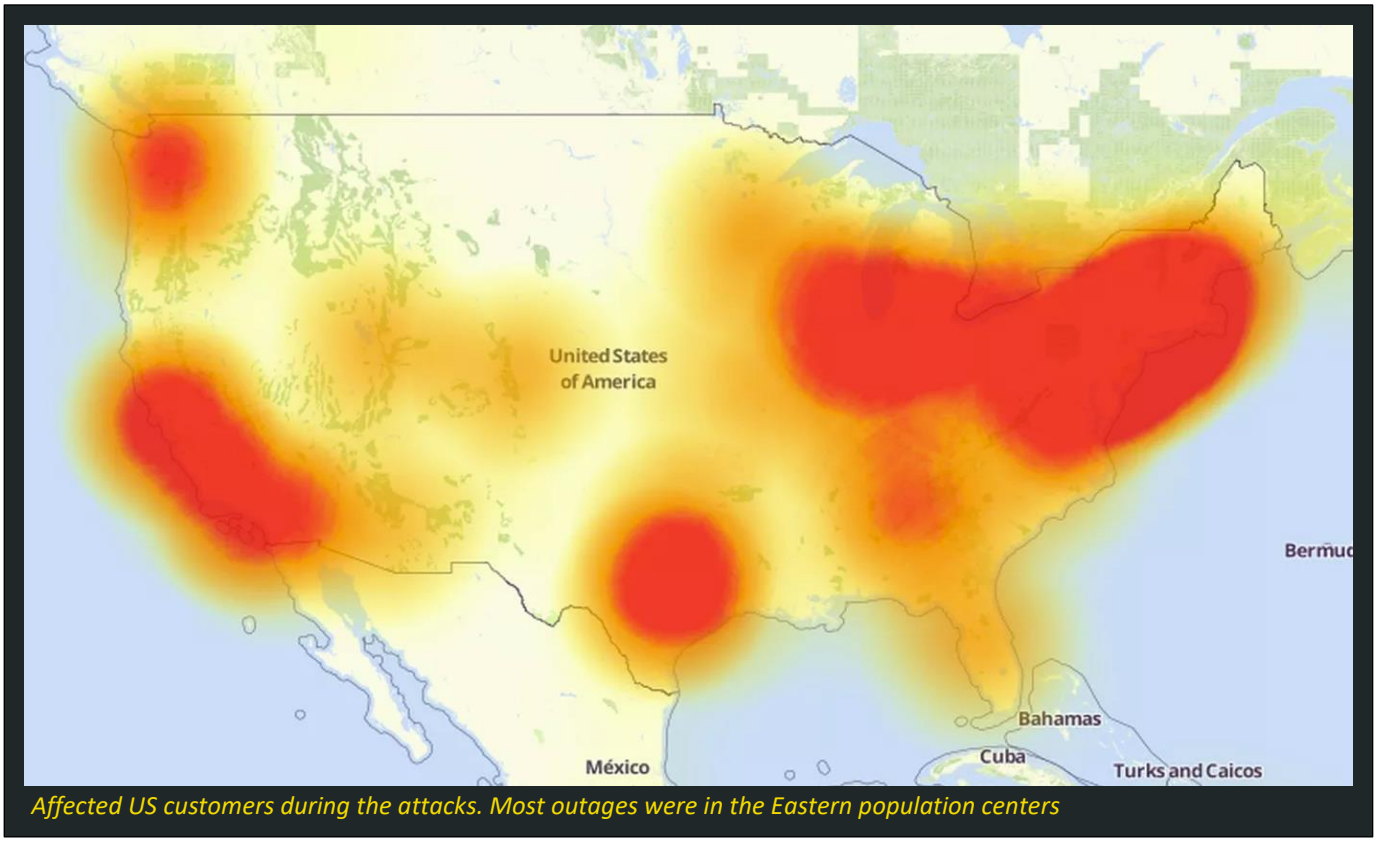
Risks

The Dyn DNS Cyberattack shows issues in present use of the DNS at large, spanning risk categories, likelihoods and threat levels. Below is a subset of the most important risks that surfaced during and after the attack.

Name	Type	Target	Severity	Description
Prolonged Service Interruption	External	Providers	Existential	Customers may leave if providers are unable to restore services in short time or if DDoS attacks commonly interrupt service.
IoT Insecure	Process	Anyone	Very High	IoT devices are a wild west; low accountability, poor security, and bad practices allow easy access for criminals.
DDoS Attack	External	Anyone	Low – High	DDoS attacks can affect anyone at any time; depending on the service interrupted, the cost can be staggering.
Short Time To Live	Process	Providers	High	DNS servers frequently check Primary Servers for records, sometimes caching data for only 5 minutes before expiry, generating unnecessary data loads
DDoS Against DNS Amplifiable	Systems	Providers	High	Constant queries and table updates cause DNS servers to routinely request data. If the data is not found, servers continue requesting until their needs are met, adding to network traffic.
Few DNS Entries	Process	Users	Medium	End user systems typically have only one or two DNS servers listed; If those servers go down, the end users are unable to communicate outward

Of all the risks, a prolonged service interruption is the most catastrophic for anyone targeted. DDoS attacks are not limited to the DNS—any device or set of devices with an IP address is targetable. Most large companies have resources to deal with such an attack, but individuals and small businesses are frequently unprepared. For companies that operate on the internet, continuous upkeep is paramount to making money. Service interruptions are existential threats that must be mitigated

The Internet of Things has seen explosive growth in recent years[14]. Unfortunately, while internet companies have been pushing for whole-scale encryption of all internet traffic[15], IoT manufacturers either were not included or simply don't care. By securing all devices with a default administrative password, access to non-configured devices is trivial. A cracked device is extremely dangerous, as most IoT devices are primarily concerned with data gathering and processing; a criminal could watch electric reads on a power meter to tell if someone is home, for example.



Affected US customers during the attacks. Most outages were in the Eastern population centers

[14] http://www.forbes.com/sites/louiscolumbus/2015/12/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2015/#79d0c9af48a0

[15] https://www.wired.com/2016/09/cloudflare-launches-three-pronged-attack-encrypt-web/

Image http://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained

Recommendations

Dyn

Dyn as a company performed admirably. In the face of one of the largest and most sophisticated cyberattacks ever recorded, the company operated quickly, communicated all actions, accepted help when needed, and developed brand new DDoS mitigation methods all while keeping total affected time below four hours. Post attack, Dyn provided resources for their customers to avoid outages in the future, directly working against their best business interests for the good of the internet community at large. The company continues to publish reports on the attack two months later. All things considered, the emergency plans Dyn has are top notch, and are a glowing example for the technology industry. I have no recommendations for specific improvements with Dyn's procedures.

Time To Live and the Domain Name Service

The DNS represents a highly-centralized point of failure. The internet is designed to be decentralized in part to protect against just these attacks. Instead, an over-reliance on readily-available domain-lookup services has superseded good caching policy. Specifying a TTL on resources is important: it allows domains to be bought, sold, and transferred. But extremely short TTLs do more harm than good. Amazon.com servers have the same IP addresses for years at a time and don't benefit at all from short TTLs. I recommend several mitigation efforts:

1. Lengthen TTL on all DNS servers and end devices

   Domain registries just don't need to be updated that much. This effort can be targeted as well: certain domains that haven't changed in days or months can get longer TTLs while domains that are still for sale can be given short ones. If a service requires constantly changing DNS records, then the service can operate its own routing server that handles the requests. Generally provided DNS servers could see their default TTLs double with minimal internet impact.

2. Have devices wait until a response before deleting dead records

   When a TTL expires, the record is immediately deleted, and if a new request comes in, then the server must send out a request. Instead of deleting the record immediately, I propose a device could mark the record as 'deprecated.' If the domain is requested, the device will query the DNS for a new record. If the service responds, the record is updated. If not, the deprecated route is used instead, and the device requests the record again on the next request. This allows internet traffic to continue flowing while a Primary Server is down.

Server Diversity

3. Increase number of listed DNS servers on end devices

   Most end devices only have one or two DNS servers saved. When the DNS servers crash, the internet is still operable, but the device won't be able to reach any services not cached. This applies for finding other DNS servers as well, and the only workaround is manual entry of a DNS server, far too complicated for the average internet user. Devices should allow for more than two DNS servers, and should also preferentially choose servers that are both geographically diverse and represented by different companies. For example, my home Windows machine has both Primary and Secondary servers located in Seattle and owned by Comcast. A more robust option would be to have a Primary located nearby and owned by Comcast, a secondary also nearby and owned by Amazon, and a tertiary located across the world in Europe and owned by O2. If both local servers crash, I would still have (albeit slow) internet access until rectification of the problem.

4. Use multiple companies for DNS

   All companies should have at minimum two companies providing Primary Server record keeping. As with the diversity on end devices, companies should also have their Primary Servers spread over a wide geographic area to combat the chance of geographical outages.

An Internet of Things fridge. These types of devices are frequently unprotected and easy targets for botnets

Image http://fm.cnbc.com/applications/cnbc.com/resources/img/editorial/2014/02/21/101434928-461697665.530x298.jpg?v=1392990407

Internet of Things Devices

5. Lock down the IoT

   Entire papers have been written on the challenges of IoT devices, and I won't try to duplicate them. In short, companies should not be giving all devices a common login combo, should force username and password requests at first startup, and should keep their devices up-to-date on the most recent security software.

   A secondary option is to hide IoT devices behind another more secure internet connected device, much like how Fitbits connect to a phone in order to connect to internet services. A home base that uses Bluetooth instead of IP Ethernet and that plugs directly into a router provides a singular point to protect instead of many IoT devices.

Server Spam

6. Stop querying a DNS server for a time after no response

   This is a simple fix: If a DNS server is down, and fails to respond to multiple requests, then devices should be default remove the server from their pool for some time. If every DNS server didn't spam Dyn with requests, and instead paused for 5 to 15 minutes after multiple successive failed requests, Dyn would have seen dramatically reduced traffic. Adding this safeguard also lowers the risk of DNS message amplification, lowering the overall power of DDoS on the DNS.

Conclusion

The Dyn Domain Name Service Cyberattack was an unprecedented and sophisticated attack. Dyn acted with exceptional grace, speed and transparency to mitigate damage and restore connectivity. Information gained from the attack was freely shared so as to protect the world against similar attacks in the future.

A number of small changes to the baseboard of internet connectivity could help assure future DNS attacks have less impact, and basic security updates to Internet of Things devices could disable an entire class of malware programs. Unfortunately, other companies have been slow to react, and many of the risks identified by the Distributed Denial of Service ordeal remain unaddressed. Future attacks similar to this one are likely against other companies until security and risk management improve.

With so little information regarding the motive and identity of the perpetrators, and little action to address the lessons provided, it is possible another large-scale attack could happen again at any time, and target far more important and vulnerable systems.