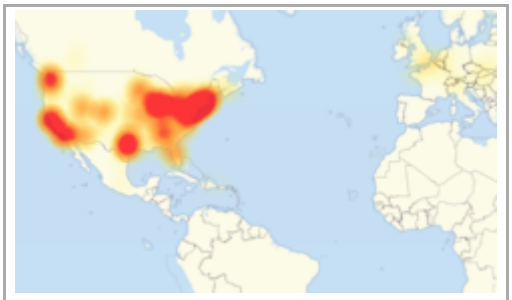
DDoS attacks on Dyn

On October 21, 2016, three consecutive distributed denial-of-service attacks were launched against the Domain Name System (DNS) provider Dyn. The attack caused major Internet platforms and services to be unavailable to large swathes of users in Europe and North America.[3][4] The groups Anonymous and New World Hackers claimed responsibility for the attack, but scant evidence was provided.[5]

As a DNS provider, Dyn provides to end-users the service of mapping an Internet domain name—when, for instance, entered into a web browser—to its corresponding IP address. The distributed denial-of-service (DDoS) attack was accomplished through numerous DNS lookup requests from tens of millions of IP addresses.[6] The activities are believed to have been executed through a botnet consisting of many Internet-connected devices—such as printers, IP cameras, residential gateways and baby monitors—that had been infected with the Mirai malware.

DDoS attacks on Dyn



Map of areas most affected by attack, 16:45 UTC, 21 October 2016.[1]

Date	October 21, 2016
Time	11:10 – 13:20 UTC 15:50 – 17:00 UTC 20:00 – 22:10 UTC[2]
Location	Europe and North America, especially the Eastern United States
Type	Distributed denial-of-service
Participants	Unknown
Suspects	New World Hackers, Anonymous (self-claimed)

Contents

Affected services

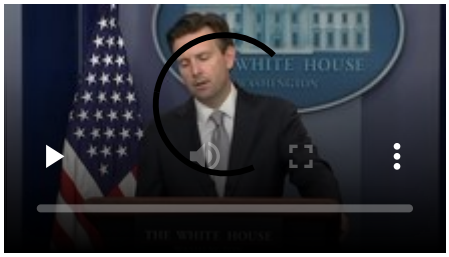
Services affected by the attack included:

- Airbnb[7]
- Amazon.com[8]
- Ancestry.com[9][10]
- *The A.V. Club*[11]
- BBC[10]
- *The Boston Globe*[7]
- Box[12]
- *Business Insider*[10]
- CNN[10]
- Comcast[13]
- CrunchBase[10]
- DirecTV[10]
- *The Elder Scrolls Online*[10][14]
- Electronic Arts[13]
- Etsy[7][15]
- Evergreen ILS
- FiveThirtyEight[10]
- Fox News[16]
- *The Guardian*[16]
- GitHub[7][13]

- Grubhub[17]
- HBO[10]
- Heroku[18]
- HostGator[10]
- iHeartRadio[9][19]
- Imgur[20]
- Indiegogo[9]
- Mashable[21]
- National Hockey League[10]
- Netflix[10][16]
- *The New York Times*[7][13]
- Overstock.com[10]
- PayPal[15]
- Pinterest[13][15]
- Pixlr[10]
- PlayStation Network[13]
- Qualtrics[9]
- Quora[10]
- Reddit[9][13][15]
- Roblox[22]
- Ruby Lane[10]
- *RuneScape*[9]
- SaneBox[18]
- Seamless[20]
- *Second Life*[23]
- Shopify[7]
- Slack[20]
- SoundCloud[7][15]
- Squarespace[10]
- Spotify[9][13][15]
- Starbucks[9][19]
- Storify[12]
- Swedish Civil Contingencies Agency[24]
- Swedish Government[24]
- Tumblr[9][13]
- Twilio[9][10]
- Twitter[7][9][13][15]
- Verizon Communications[13]
- Visa[25]
- Vox Media[26]
- Walgreens[10]
- *The Wall Street Journal*[16]
- Wikia[9]
- *Wired*[12]
- Wix.com[27]
- WWE Network[28]
- Xbox Live[29]
- Yammer[20]
- Yelp[10]
- Zillow[10]

Investigation

The US Department of Homeland Security started an investigation into the attacks, according to a White House source.[30][31][32] No group of hackers claimed responsibility during or in the immediate aftermath of the attack.[33] Dyn's chief strategist said in an interview that the assaults on the company's servers were very complex and unlike everyday DDoS attacks.[34] Barbara Simons, a member of the advisory board of the United States Election Assistance Commission, said such attacks could affect electronic voting for overseas military or civilians.[34]



White House spokesperson Josh Earnest responds on October 21, 2016, the day of the attack

Dyn disclosed that, according to business risk intelligence firm FlashPoint and Akamai Technologies, the attack was a botnet coordinated through numerous Internet of Things-enabled (IoT) devices, including cameras, residential gateways, and baby monitors, that had been infected with Mirai malware. The attribution of the attack to the Mirai botnet had been previously reported by BackConnect Inc., another security firm.[35] Dyn stated that they were receiving malicious requests from tens of millions of IP addresses.[6][36] Mirai is designed to brute-force the security on an IoT device, allowing it to be controlled remotely.

Cybersecurity investigator Brian Krebs noted that the source code for Mirai had been released onto the Internet in an open-source manner some weeks prior, which made the investigation of the perpetrator more difficult.[37]

On 25 October 2016, US President Obama stated that the investigators still had no idea who carried out the cyberattack.[38]

On 13 December 2017, the Justice Department announced that three men (Paras Jha, 21, Josiah White, 20, and Dalton Norman, 21) had entered guilty pleas in cybercrime cases relating to the Mirai and clickfraud botnets.[39]

Perpetrators

In correspondence with the website *Politico*, hacktivist groups SpainSquad, Anonymous, and **New World Hackers** claimed responsibility for the attack in retaliation against Ecuador's rescinding Internet access to WikiLeaks founder Julian Assange, at their embassy in London, where he had been granted asylum.[5] This claim has yet to be confirmed.[5] WikiLeaks alluded to the attack on Twitter, tweeting "Mr. Assange is still alive and WikiLeaks is still publishing. We ask supporters to stop taking down the US internet. You proved your point."[40] New World Hackers has claimed responsibility in the past for similar attacks targeting sites like BBC and ESPN.com.[41]

On October 26, FlashPoint stated that the attack was most likely done by script kiddies.[42]

A November 17, 2016, *Forbes* article reported that the attack was likely carried out by "an angry gamer".[43]

A September 20, 2018, WeLiveSecurity article stated the its three creators meant it as a way of gaining an advantage in fierce competition surrounding the computer game Minecraft – by preventing players from using competitors' servers and driving them to their own servers in order to ultimately make money off them.[44]

On December 9, 2020, one of the perpetrators pleaded guilty to taking part in the attack. The perpetrator's name was withheld due to his or her age. [45]

See also

- WannaCry ransomware attack
- Mirai (malware)
- Vulnerability (computing)

References

1. "Level3 outage? Current problems and outages" (http://downdetector.com/status/level3/map/). *downdetector.com*. Retrieved 23 October 2016.
2. Dyn (26 October 2016). "Official Dyn Analysis Summary" (https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/). *dyn.com*. Retrieved 5 February 2019.
3. Etherington, Darrell; Conger, Kate (21 October 2016). "Many sites including Twitter, Shopify and Spotify suffering outage" (https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/). *TechCrunch*. Retrieved 2016-10-21.

4. "The Possible Vendetta Behind the East Coast Web Slowdown" (https://www.bloomberg.com/news/articles/2016-10-21/internet-service-disrupted-in-large-parts-of-eastern-u-s). *Bloomberg.com*. Retrieved 2016-10-21.
5. Romm, Tony; Geller, Eric (21 October 2016). "WikiLeaks supporters claim credit for massive U.S. cyberattack, but researchers skeptical" (http://www.politico.com/story/2016/10/websites-down-possible-cyber-attack-230145). *Politico*. Retrieved 22 October 2016.
6. Newman, Lily Hay. "What We Know About Friday's Massive East Coast Internet Outage" (https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/). *WIRED*. Retrieved 2016-10-21.
7. Heine, Christopher. "A Major Cyber Attack Is Hurting Twitter, Spotify, Pinterest, Etsy and Other Sites" (http://www.adweek.com/news/technology/major-cyber-attack-hurting-twitter-spotify-etsy-shopify-and-other-sites-174214). *AdWeek*. Retrieved 21 October 2016.
8. Lovelace Jr., Berkeley (21 October 2016). "After cyberassault KOs Amazon, Twitter, Spotify, third attack reported" (https://www.cnbc.com/2016/10/21/major-websites-across-east-coast-knocked-out-in-apparent-ddos-attack.html). *CNBC*. Retrieved 21 October 2016.
9. Turton, William. "This Is Probably Why Half the Internet Shut Down Today [Update: It's Happening Again]" (https://gizmodo.com/this-is-probably-why-half-the-internet-shut-down-today-1788062835). *Gizmodo*. Retrieved 2016-10-21.
10. Chiel, Ethan. "Here Are the Sites You Can't Access Because Someone Took the Internet Down" (http://fusion.net/story/360952/which-sites-affected-ddos-attack/). *Fusion*. Retrieved 21 October 2016.
11. Chavez, Danette (21 October 2016). "Here's why half the internet went down today" (https://www.avclub.com/article/heres-why-half-internet-went-down-today-244611). *The A.V. Club*. Retrieved 21 October 2016.
12. Murdock, Jason (21 October 2016). "Twitter, Spotify, Reddit among top websites knocked offline by major DDoS attack" (http://www.ibtimes.co.uk/twitter-spotify-reddit-among-top-websites-knocked-offline-by-major-ddos-attack-1587646). *International Business Times UK*. Retrieved 21 October 2016.
13. Meyer, Robinson; LaFrance, Adrienne. "What's Going On With the Internet Today?" (https://www.theatlantic.com/technology/archive/2016/10/when-the-entire-internet-seems-to-break-at-once/504956/). *The Atlantic*. Retrieved 2016-10-21.
14. @TESOnline (21 October 2016). "We are still investigating intermittent login issues some players are experiencing across all megaservers" (https://twitter.com/TESOnline/status/789545206228156416) (Tweet) – via Twitter.
15. "Massive web attacks briefly knock out top sites" (https://www.bbc.com/news/technology-37728015). *BBC News*. 21 October 2016.
16. Thielman, Sam; Johnston, Chris (21 October 2016). "Major cyber attack disrupts internet service across Europe and US" (https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service). *The Guardian*. Retrieved 21 October 2016.
17. Hinckley, Story (21 October 2016). "Did the East Coast just suffer a massive cyberattack?" (http://www.csmonitor.com/Technology/2016/1021/Did-the-East-Coast-just-suffer-a-massive-cyberattack). *Christian Science Monitor*. Retrieved 21 October 2016.
18. Hughes, Matthew (21 October 2016). "A massive DDOS attack against Dyn DNS is causing havoc online [Updated]" (https://thenextweb.com/security/2016/10/21/massive-ddos-attack-dyn-dns-causing-havoc-online/). *The Next Web*. Retrieved 21 October 2016.
19. "Having internet problems today? Here's what's going on" (http://www.wjhg.com/content/news/Having-internet-problems-today-Heres-whats-going-on-397907861.html). *WJHG-TV*. Retrieved 21 October 2016.

20. Chacos, Brad. "Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline" (http://www.pcworld.com/article/3133847/internet/ddos-attack-on-dyn-knocks-spotify-twitter-github-etsy-and-more-offline.html). *PCWorld*. Retrieved 22 October 2016.
21. Menn, Joseph (22 October 2016). "Cyber attacks disrupt PayPal, Twitter, other sites" (https://www.reuters.com/article/us-usa-cyber-idUSKCN12L1ME). *Reuters*. Retrieved 23 October 2016.
22. "DDoS Attack on DNS; Major sites including GitHub PSN, Twitter Suffering Outage" (https://www.hackread.com/ddos-attack-dns-sites-suffer-outage/). *HackRead*. 21 October 2016. Retrieved 23 October 2016.
23. "[RESOLVED] Unscheduled Maintenance" (https://web.archive.org/web/20161024025120/https://community.secondlife.com/t5/Status-Grid/RESOLVED-Unscheduled-Maintenance/ba-p/3075187). Archived from the original (https://community.secondlife.com/t5/Status-Grid/RESOLVED-Unscheduled-Maintenance/ba-p/3075187) on 24 October 2016. Retrieved 23 October 2016.
24. Joel Westerholm. "Så sänktes Twitter och Regeringen.se i attacken (https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=6547041)", Sveriges Radio, 24 October 2016. Retrieved 30 October 2016.
25. "U.S. internet disrupted as firm hit by cyberattacks" (http://www.cbsnews.com/news/internet-disrupted-dyn-hit-by-ddos-cyberattack/). *CBS News*. Retrieved 21 October 2016.
26. Lecher, Colin (21 October 2016). "Denial-of-service attacks are shutting down major websites across the internet" (https://www.theverge.com/2016/10/21/13357344/ddos-attack-websites-shut-down). *The Verge*. Retrieved 21 October 2016.
27. Gallagher, Sean (21 October 2016). "DoS attack on major DNS provider brings Internet to morning crawl [Updated]" (https://arstechnica.com/security/2016/10/dos-attack-on-major-dns-provider-brings-internet-to-morning-crawl/). *Ars Technica*. Retrieved 21 October 2016.
28. Wolkenbrod, Rob (21 October 2016). "Why is the WWE Network Down on Friday, October 21?" (http://dailyddt.com/2016/10/21/wwe-network-down-ddos-attack/). *Daily DDT*. Retrieved 22 October 2016.
29. Sarkar, Samit (21 October 2016). "Massive DDoS attack affecting PSN, some Xbox Live apps (update)" (http://www.polygon.com/2016/10/21/13361014/psn-xbox-live-down-ddos-attack-dyn). *Polygon*. Retrieved 23 October 2016.
30. Etherington, Darrell; Conger, Kate (21 October 2016). "Many sites including Twitter, Shopify and Spotify suffering outage" (https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/). *TechCrunch*. Retrieved 2016-10-21.
31. "Government probes major cyberattack causing internet outages" (http://www.politico.com/story/2016/10/websites-down-possible-cyber-attack-230145). *Politico*. Retrieved 2016-10-21.
32. Finkle, Jim; Volz, Dustin. "Homeland Security Is 'Investigating All Potential Causes' of Internet Disruptions" (http://time.com/4540921/internet-dyn-outage-homeland-security/). *Time*. Retrieved 2016-10-21.
33. "Popular sites like Amazon, Twitter and Netflix suffer outages" (https://money.cnn.com/2016/10/21/technology/ddos-attack-popular-sites/index.html). *money.cnn.com*. CNN Money. 21 October 2016. Retrieved October 21, 2016.
34. Perlroth, Nicole; Mccann, Erin (2016-10-21). "No, It's Not Just You. The Internet Is (Still) Having Problems" (https://www.nytimes.com/2016/10/22/business/internet-problems.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Retrieved 2016-10-21.
35. "Blame the Internet of Things for Destroying the Internet Today" (http://motherboard.vice.com/read/blame-the-internet-of-things-for-destroying-the-internet-today). *Motherboard*. Retrieved 2016-10-27.

36. Perlroth, Nicole (2016-10-21). "Internet Attack Spreads, Disrupting Major Websites" (https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Retrieved 2016-10-22.
37. Statt, Nick (October 21, 2016). "How an army of vulnerable gadgets took down the web today" (https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained). *The Verge*. Retrieved October 21, 2016.
38. CNN, 25 October 2016, Obama: We have no idea who carried out huge cyberattack (https://money.cnn.com/2016/10/25/technology/cyberattack-obama-dyn-ddos/index.html)
39. Justice Department, 13 December 2017, Justice Department Announces Charges And Guilty Pleas In Three Computer Crime Cases Involving Significant Cyber Attacks (https://www.justice.gov/usao-nj/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases)
40. Han, Esther (22 October 2016). "WikiLeaks claims its supporters are behind the massive DDoS cyber attack" (http://www.smh.com.au/technology/technology-news/wikileaks-points-to-its-supporters-for-massive-ddos-cyber-attack-20161021-gs881u.html). *The Sydney Morning Herald*. Retrieved 22 October 2016.
41. Satter, Raphael; Fowler, Bree; Bajak (21 October 2016). "Cyberattacks on Key Internet Firm Disrupt Internet Services" (https://web.archive.org/web/20161025073904/https://www.nytimes.com/aponline/2016/10/21/world/europe/ap-disruptive-cyberattack.html). *The New York Times*. ISSN 0362-4331 (https://www.worldcat.org/issn/0362-4331). Archived from the original (https://www.nytimes.com/aponline/2016/10/21/world/europe/ap-disruptive-cyberattack.html) on 2016-10-25. Retrieved 22 October 2016.
42. Lomas, Natasha (26 October 2016). "Dyn DNS DDoS likely the work of script kiddies, says FlashPoint, so i guess that means anonymous did it, as most of anonymous are script kiddies anyway" (https://techcrunch.com/2016/10/26/dyn-dns-ddos-likely-the-work-of-script-kiddies-says-flashpoint/). *TechCrunch*. Retrieved 26 October 2016.
43. Mathews, Lee (17 November 2016). "Angry Gamer Blamed For Most Devastating DDoS Of 2016" (https://www.forbes.com/sites/leemathews/2016/11/17/angry-gamer-blamed-for-most-devastating-ddos-of-2016/#78871c472dac). *Forbes.com*. Retrieved 20 April 2018.
44. Foltýn, Tomáš (20 September 2018). "Mirai's architects avoid prison thanks to work for FBI" (https://www.welivesecurity.com/2018/09/20/mirais-architects-avoid-prison-thanks-work-fbi/). *welivesecurity.com*. Retrieved 5 October 2021.
45. "Individual Pleads Guilty to Participating in Internet-of-Things Cyberattack in 2016" (https://www.justice.gov/opa/pr/individual-pleads-guilty-participating-internet-things-cyberattack-2016). *justice.gov*. 9 December 2020. Retrieved 7 January 2021.
