Wikipedia
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Create a book
Download as PDF
Printable version

In other projects

Wikimedia Commons

Languages

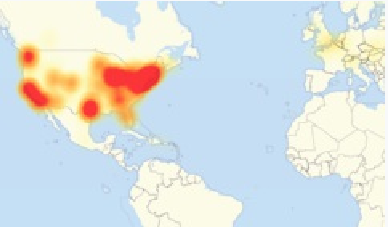
العربية
Català
Deutsch
Español
فارسی
Français
한국어
Bahasa Indonesia
עברית
Magyar
Русский
Svenska
Українська
中文
Edit links

2016 Dyn cyberattack

From Wikipedia, the free encyclopedia

The **2016 Dyn cyberattack** took place on October 21, 2016, and involved multiple distributed denial-of-service attacks (DDoS attacks) targeting systems operated by Domain Name System (DNS) provider Dyn, which caused major Internet platforms and services to be unavailable to large swathes of users in Europe and North America.[2][3] The groups Anonymous and New World Hackers claimed responsibility for the attack, but scant evidence was provided.[4]

Dyn cyberattack



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

Date	October 21, 2016
Time	12:10 – 14:20 UTC 16:50 – 18:11 UTC 21:00 – 23:11 UTC [*citation needed*][*needs update*]
Location	Europe and North America, especially the Eastern United States
Type	Distributed denial-of-service
Participants	Unknown
Suspect(s)	New World Hackers, Anonymous (self-claimed)

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 a large number of DNS lookup requests from tens of millions of IP addresses.[5] The activities are believed to have been executed through a botnet consisting of a large number of Internet-connected devices—such as printers, IP cameras, residential gateways and baby monitors—that had been infected with the Mirai malware.

Contents

Timeline and impact [edit]

According to Dyn, a distributed denial-of-service (DDoS) attack began at 7:00 a.m. (EDT) and was resolved by 9:20 a.m. A second attack was reported at 11:52 a.m. and Internet users began reporting difficulties accessing websites.[6][7] A third attack began in the afternoon, after 4:00 p.m.[5][8] At 6:11 p.m., Dyn reported that they had resolved the issue.[9][10]

Dyn Chief Strategy Officer and spokesperson Kyle York led the communication response with customers, partners and the market.

Affected services [edit]

Services affected by the attack included:

- Airbnb[11]
- Amazon.com[8]
- Ancestry.com[12][13]
- *The A.V. Club*[14]
- BBC[13]
- *The Boston Globe*[11]
- Box[15]
- *Business Insider*[13]
- CNN[13]
- Comcast[16]
- CrunchBase[13]
- DirecTV[13]
- *The Elder Scrolls Online*[13][17]
- Electronic Arts[16]
- Etsy[11][18]

- FiveThirtyEight[13]
- Fox News[19]
- *The Guardian*[19]
- GitHub[11][16]
- Grubhub[20]
- HBO[13]
- Heroku[21]
- HostGator[13]
- iHeartRadio[12][22]
- Imgur[23]
- Indiegogo[12]
- Mashable[24]
- National Hockey League[13]
- Netflix[13][19]
- *The New York Times*[11][16]
- Overstock.com[13]
- PayPal[18]
- Pinterest[16][18]
- Pixlr[13]
- PlayStation Network[16]
- Qualtrics[12]
- Quora[13]
- Reddit[12][16][18]
- Roblox[25]
- Ruby Lane[13]
- *RuneScape*[12]
- SaneBox[21]
- Seamless[23]
- *Second Life*[26]
- Shopify[11]
- Slack[23]
- SoundCloud[11][18]
- Squarespace[13]
- Spotify[12][16][18]
- Starbucks[12][22]
- Storify[15]
- Swedish Civil Contingencies Agency[27]
- Swedish Government[27]
- Tumblr[12][16]
- Twilio[12][13]
- Twitter[11][12][16][18]
- Verizon Communications[16]
- Visa[28]
- Vox Media[29]
- Walgreens[13]
- *The Wall Street Journal*[19]
- Wikia[12]
- *Wired*[15]
- Wix.com[30]
- WWE Network[31]
- Xbox Live[32]
- Yammer[23]
- Yelp[13]
- Zillow[13]

Investigation [edit]

The US Department of Homeland Security started an investigation into the attacks, a source.[2][33][34] No group of hackers claimed responsibility during or in the immediate aftermath of the attack.[35] Dyn's chief strategist said in an interview that the assaults on the company's servers were very complex and unlike everyday DDoS attacks.[7] 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.[7]

Play media

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 a large number of 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.[36] Dyn stated that they were receiving malicious requests from tens of millions of IP addresses.[5][37] 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 will make the investigation of the perpetrator more difficult.[38] Since then, Mirai has been adapted in other malware projects.[39]

On 25 October 2016, US President Obama stated that the investigators still had no idea who carried out the cyberattack.[40]

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.[41]

Perpetrators [edit]

In correspondence with the website Politico, hacktivist groups SpainSquad, Anonymous, and **New World Hackers** claimed responsibility for the attack in retaliation for Ecuador's rescinding Internet access to WikiLeaks founder Julian Assange, at their embassy in London, where he has been granted asylum.[4] This claim has yet to be confirmed.[4] 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."[42] New World Hackers has claimed responsibility in the past for similar attacks targeting sites like BBC and ESPN.com.[43]

On October 26, FlashPoint stated that the attack was most likely done by script kiddies.[44]

A November 17, 2016 *Forbes* article reported that the attack was likely carried out by "an angry gamer".[45]

See also [edit]

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

Computer security portal

Internet portal

References [edit]

1. ^ "Level3 outage? Current problems and outages". *downdetector.com*. Retrieved 23 October 2016.
2. ^ *a b* Etherington, Darrell; Conger, Kate. "Many sites including Twitter, Shopify and Spotify suffering outage". *TechCrunch*. Retrieved 2016-10-21.
3. ^ "The Possible Vendetta Behind the East Coast Web Slowdown". *Bloomberg.com*. Retrieved 2016-10-21.
4. ^ *a b c* Romm, Tony; Geller, Eric. "WikiLeaks supporters claim credit for massive U.S. cyberattack, but researchers skeptical". *POLITICO*. Retrieved 22 October 2016.
5. ^ *a b c* Newman, Lily Hay. "What We Know About Friday's Massive East Coast Internet Outage". *WIRED*. Retrieved 2016-10-21.
6. ^ "Sites across the internet suffer outage after cyberattack". *mashable.com*. Mashable. Retrieved October 21, 2016.
7. ^ *a b c* Perlroth, Nicole; Mccann, Erin (2016-10-21). "No, It's Not Just You. The Internet Is (Still) Having Problems". *The New York Times*. ISSN 0362-4331. Retrieved 2016-10-21.
8. ^ *a b* Lovelace Jr., Berkeley (21 October 2016). "After cyberassault KOs Amazon, Twitter, Spotify, third attack reported". *CNBC*. Retrieved 21 October 2016.
9. ^ "Dyn, Inc. Status - Update Regarding DDoS Event Against Dyn Managed DNS on October 21, 2016". *dynstatus.com*. Retrieved 21 October 2016.
10. ^ "Red Stag Fulfillment - Can Hackers Shut Down Your Ecommerce Business?". *redstagfulfillment.com*. Retrieved 21 October 2016.
11. ^ *a b c d e f g h* Heine, Christopher. "A Major Cyber Attack Is Hurting Twitter, Spotify, Pinterest, Etsy and Other Sites". *AdWeek*. Retrieved 21 October 2016.

AdWeek. Retrieved 21 October 2016.

12. ^ a b c d e f g h i j k l Turton, William. "This Is Probably Why Half the Internet Shut Down Today [Update: It's Happening Again]". *Gizmodo*. Retrieved 2016-10-21.
13. ^ a b c d e f g h i j k l m n o p q r s t u Chiel, Ethan. "Here Are the Sites You Can't Access Because Someone Took the Internet Down". *Fusion*. Retrieved 21 October 2016.
14. ^ Chavez, Danette (21 October 2016). "Here's why half the internet went down today". *The A.V. Club*. Retrieved 21 October 2016.
15. ^ a b c Murdock, Jason (21 October 2016). "Twitter, Spotify, Reddit among top websites knocked offline by major DDoS attack". *International Business Times UK*. Retrieved 21 October 2016.
16. ^ a b c d e f g h i j k Meyer, Robinson; LaFrance, Adrienne. "What's Going On With the Internet Today?". *The Atlantic*. Retrieved 2016-10-21.
17. ^ @TESOnline (21 October 2016). "We are still investigating intermittent login issues some players are experiencing across all megaservers" (Tweet) – via Twitter.
18. ^ a b c d e f g "Massive web attacks briefly knock out top sites". *BBC News*. 21 October 2016.
19. ^ a b c d Thielman, Sam; Johnston, Chris (21 October 2016). "Major cyber attack disrupts internet service across Europe and US". *The Guardian*. Retrieved 21 October 2016.
20. ^ Hinckley, Story (21 October 2016). "Did the East Coast just suffer a massive cyberattack?". *Christian Science Monitor*. Retrieved 21 October 2016.
21. ^ a b Hughes, Matthew (21 October 2016). "A massive DDOS attack against Dyn DNS is causing havoc online [Updated]". *The Next Web*. Retrieved 21 October 2016.
22. ^ a b "Having internet problems today? Here's what's going on". *WJHG-TV*. Retrieved 21 October 2016.
23. ^ a b c d Chacos, Brad. "Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline". *PCWorld*. Retrieved 22 October 2016.
24. ^ Menn, Joseph (22 October 2016). "Cyber attacks disrupt PayPal, Twitter, other sites". *Reuters*. Retrieved 23 October 2016.
25. ^ "DDoS Attack on DNS; Major sites including GitHub PSN, Twitter Suffering Outage". *HackRead*. 21 October 2016. Retrieved 23 October 2016.
26. ^ "[RESOLVED] Unscheduled Maintenance". Archived from the original on 24 October 2016. Retrieved 23 October 2016.
27. ^ a b Joel Westerholm. "Så sänktes Twitter och Regeringen.se i attacken", Sveriges Radio, 24 October 2016. Retrieved 30 October 2016.
28. ^ "U.S. internet disrupted as firm hit by cyberattacks". *CBS News*. Retrieved 21 October 2016.
29. ^ Lecher, Colin (21 October 2016). "Denial-of-service attacks are shutting down major websites across the internet". *The Verge*. Retrieved 21 October 2016.
30. ^ Gallagher, Sean. "DoS attack on major DNS provider brings Internet to morning crawl [Updated]". *Ars Technica*. Retrieved 21 October 2016.
31. ^ Wolkenbrod, Rob (21 October 2016). "Why is the WWE Network Down on Friday, October 21?". *Daily DDT*. Retrieved 22 October 2016.
32. ^ Sarkar, Samit (21 October 2016). "Massive DDoS attack affecting PSN, some Xbox Live apps (update)". *Polygon*. Retrieved 23 October 2016.
33. ^ "Government probes major cyberattack causing internet outages". *POLITICO*. Retrieved 2016-10-21.
34. ^ Finkle, Jim; Volz, Dustin. "Homeland Security Is 'Investigating All Potential Causes' of Internet Disruptions". *TIME.com*. Retrieved 2016-10-21.
35. ^ "Popular sites like Amazon, Twitter and Netflix suffer outages". *money.cnn.com*. CNN Money. Retrieved October 21, 2016.
36. ^ "Blame the Internet of Things for Destroying the Internet Today". *Motherboard*. Retrieved 2016-10-27.
37. ^ Perlroth, Nicole (2016-10-21). "Internet Attack Spreads, Disrupting Major Websites". *The New York Times*. ISSN 0362-4331. Retrieved 2016-10-22.
38. ^ Statt, Nick (October 21, 2016). "How an army of vulnerable gadgets took down the web today". *The Verge*. Retrieved October 21, 2016.
39. ^ "DDoS To DynDNS: The Internet Breaks". *Eyerys.com*. October 21, 2016. Retrieved October 21, 2017.
40. ^ CNN, 25 October 2016, Obama: We have no idea who carried out huge cyberattack
41. ^ Justice Department, 13 December, 2017, Justice Department Announces Charges And Guilty Pleas In Three Computer Crime Cases Involving Significant Cyber Attacks
42. ^ Han, Esther (22 October 2016). "WikiLeaks' strange admission around internet attacks against Netflix and Twitter". *The Sydney Morning Herald*. Retrieved 22 October 2016.
43. ^ The Associated Press (2016-10-21). "Cyberattacks on Key Internet Firm Disrupt Internet Services". *The New York Times*. ISSN 0362-4331. Retrieved 2016-10-22.
44. ^ Lomas, Natasha (26 October 2016). "Dyn DNS DDoS likely the work of script kiddies, says FlashPoint". *TechCrunch*. Retrieved 26 October 2016.
45. ^ https://www.forbes.com/sites/leemathews/2016/11/17/angry-gamer-blamed-for-most-devastating-ddos-of-2016/#78871c472dac

Wikimedia Commons has media related to *October 2016 Dyn cyberattack*.

v · t · e	Hacking in the 2010s	
← 2000s	Timeline	2020s →
Major incidents	2010	Operation Aurora · Australian cyberattacks · Operation Payback
	2011	HBGary Federal · DigiNotar · RSA SecurID compromise · Operation Tunisia · 2011 PlayStation Network outage · Operation AntiSec
	2012	Stratfor email leak · LinkedIn hack
	2013	South Korea cyberattack · Snapchat hack · 2013 Yahoo! data breach
	2014	Anthem medical data breach · Operation Tovar · iCloud leaks of celebrity photos · Sony Pictures hack · Russian hacker password theft · 2014 Yahoo! data breach
	2015	Office of Personnel Management data breach · Hacking Team · Ashley Madison data breach · VTech data breach · SWIFT banking hack
	2016	Bangladesh Bank robbery · Hollywood Presbyterian Medical Center ransomware incident · Commission on Elections data breach · Democratic National Committee cyber attacks · DCCC cyber attacks · **Dyn cyberattack** · Russian interference in U.S. election
	2017	WannaCry ransomware attack · Westminster cyberattack · Petya cyberattack (2017 cyberattacks on Ukraine) · Equifax data breach · Deloitte breach · Disqus breach
Groups		Anonymous (associated events) · Bureau 121 · Cozy Bear · CyberBerkut · Derp · Equation Group · Fancy Bear · GNAA · Goatse Security · Guccifer 2.0 · Hacking Team · Iranian Cyber Army · Lizard Squad · LulzRaft · LulzSec · New World Hackers · NullCrew · NSO Group · PayPal 14 · PLA Unit 61398 · PLATINUM · Pranknet · RedHack · Rocket Kitten · The Shadow Brokers · Syrian Electronic Army · TeaMp0isoN · Tailored Access Operations · UGNazi · Yemen Cyber Army
Individuals		George Hotz · Guccifer · Hector Monsegur · Jeremy Hammond · Junaid Hussain · Kristoffer von Hassel · Mustafa Al-Bassam · MLT · Ryan Ackroyd · Topiary · The Jester · weev
Major vulnerabilities publicly disclosed		Evercookie (2010) · iSeeYou (2013) · Heartbleed (2014) · Shellshock (2014) · POODLE (2014) · Rootpipe (2014) · Row hammer (2014) · JASBUG (2015) · Stagefright (2015) · DROWN (2016) · Badlock (2016) · Dirty COW (2016) · Cloudbleed (2017) · Broadcom Wi-Fi (2017) · EternalBlue (2017) · DoublePulsar (2017) · Silent Bob is Silent (2017) · KRACK (2017) · ROCA vulnerability (2017) · BlueBorne (2017) · Meltdown (2018) · Spectre (2018)
Malware		Bad Rabbit · Careto / The Mask · CryptoLocker · Dexter · Duqu · Duqu 2.0 · FinFisher · Flame · Gameover ZeuS · Mahdi · Metulji botnet · Mirai · NSA ANT catalog · Pegasus · Petya · R2D2 · Shamoon · Stars virus · Stuxnet · Vault 7 · WannaCry · X-Agent

Categories: 2016 in computer science | Denial-of-service attacks | October 2016 crimes in Europe | October 2016 crimes in the United States | Internet of things | WikiLeaks | Botnets | Malware | Domain name system | Hacking in the 2010s | Cloud infrastructure attacks & failures

This page was last edited on 5 January 2018, at 22:17.