

Advertisement

Support The Guardian

NewsContribute

OpinionSubscribe

Sport

Culture

Search jobs

Sign in

Search

More

US edition

USWorldEnvironmentSoccerUSBusinessTechScience

Hacking

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week’s denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the ‘primary source of malicious attack’

- Major cyber attack disrupts internet service across Europe and US



Dyn estimated that the attack had involved ‘100,000 malicious endpoints’, and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

Nicky Woolf in San Francisco

@nickywoolf

Wed 26 Oct 2016
16.42 EDT



774 423

This article is over 2 years old

The cyber-attack that brought down much of America’s internet last week was caused by a new weapon called the Mirai botnet and was likely the largest of its kind in history, experts said.

The victim was the servers of Dyn, a company that controls much of the internet’s domain name system (DNS) infrastructure. It was hit on 21 October and remained under sustained assault for most of the day, bringing down sites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US.

most viewed in US

LiveBrexit vote: Jeremy Corbyn tables no-confidence



Can we secure the internet of things in time to prevent another cyber-attack?

[Read](#)

The cause of the outage was a distributed denial of service (DDoS) attack, in which a network of computers infected with special malware, known as a “botnet”, are coordinated into bombarding a server with traffic until it collapses under the strain.

What makes it interesting is that the attack was orchestrated using a weapon called the Mirai botnet. According to a [blogpost](#) by Dyn published on Wednesday, Mirai was the “primary source of malicious attack traffic”.

Unlike other botnets, which are typically made up of computers, the Mirai botnet is largely made up of so-called “[internet of things](#)” (IoT) devices such as digital cameras and DVR players.

Because it has so many internet-connected devices to choose from, attacks from Mirai are much larger than what most DDoS attacks could previously achieve. Dyn estimated that the attack had involved “100,000 malicious endpoints”, and the company, which is still investigating the attack, said there had been reports of an extraordinary attack strength of 1.2Tbps.

To put that into perspective, if those reports are true, that would make the 21 October attack roughly twice as powerful as any similar attack on record.

David Fidler, adjunct senior fellow for cybersecurity at the Council on Foreign Relations, said he couldn’t recall a DDoS attack even half as big as the one that hit Dyn.

Mirai was also used in an attack on the information security blog [Krebs on Security](#), run by the former Washington Post journalist Brian Krebs, in September. That one topped out at 665 Gbps.

“We have a serious problem with the cyber insecurity of IoT devices and no real strategy to combat it,” Fidler said. “The IoT insecurity problem was exploited on this significant scale by a non-state group, according to initial reports from government agencies and other experts about who or what was responsible.

“Imagine what a well-resourced state actor could do with insecure IOT devices,” he added.

According to Joe Weiss, the managing partner at the cybersecurity firm Applied Control Solutions and the author of Protecting Industrial Control Systems from Electronic Threats, it is hard to know what Mirai could become. “A lot of these cyber-attacks start out as one particular type of attack and then they morph into something new or different,” he said. “A lot of this is modular software.

“I can’t speak for anyone else,” Weiss continued. “[But] I don’t know that we really understand what the endgame is.”

As 2019 begins...



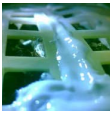
motion after May defeat – Politics live



Theresa May loses Brexit deal vote by majority of 230



Chris Christie accuses Jared Kushner of political 'hit job' in explosive new book



Giant leaf for mankind? China germinates first seed on moon



Gillette #MeToo ad on 'toxic masculinity' gets praise – and abuse

Advertisement

... we're asking readers to make a new year contribution in support of The Guardian's independent journalism. More people are reading our independent, investigative reporting than ever but advertising revenues across the media are falling fast. And unlike many news organisations, we haven't put up a paywall – we want to keep our reporting as open as we can. So you can see why we need to ask for your help.

The Guardian is editorially independent, meaning we set our own agenda. Our journalism is free from commercial bias and not influenced by billionaire owners, politicians or shareholders. No one edits our editor. No one steers our opinion. This is important as it enables us to give a voice to those less heard, challenge the powerful and hold them to account. It's what makes us different to so many others in the media, at a time when factual, honest reporting is critical.

Please make a new year contribution today to help us deliver the independent journalism the world needs for 2019 and beyond. **Supporting The Guardian has never been easier, thanks to improvements we recently made. Contribute today from as little as as \$1 – and it only takes a minute. Thank you.**

Support The Guardian



Topics

Hacking

Data and computer security

Internet Cybercrime news



Reuse this content

related stories



Marcus Hutchins: cybersecurity experts rally around arrested WannaCry 'hero'

11 Aug 2017



WannaCry ransomware has links to North Korea, cybersecurity experts say

15 May 2017



'Accidental hero' halts ransomware attack and warns: this is not over

13 May 2017



Massive cyber-attack grinds Liberia's internet to a halt

3 Nov 2016

Yahoo confirms 'state-sponsored' hackers stole personal data from 500m accounts

23 Sep 2016

520

Hackers for Hillary: event attendance 'through the roof' after Trump remarks

4 Aug 2016

473

Cyberwar is not coming to the US – it's already here

4 Aug 2016

Internet experts see 'major cyber attacks' increasing over next decade

29 Oct 2014

43

promoted links from around the web
Content

Recommended by Outbrain

About this



You could save \$668 on car insurance by switching to Progressive

PROGRESSIVE

US Cardiologist: It's Like a Pressure Wash for Your Insides

HEALTH HEADLINES



Excellent Car Accident Attorneys In Bellevue. See The List

...

Incredible new 2018 Luxury Sedans Will Blow You Away

YAHOO! SEARCH



How Can You Outsmart Amazon? Turns Out It's Pretty Simple

HONEY

The Link Between Turmeric and Rheumatoid Arthritis

HEALTHCENTRAL



If You're Over 40 And Own A Computer, This Game Is A Must-Have!

VIKINGS

Over 65? It is Time For A Dental Insurance Plan. Search For Insurance Coverage

MYDENTAL-INSURANCE.COM

comments (423)

Sign in or create your Guardian account to join the discussion.

Advertisement

Order by Oldest Threads Collapsed

1 2 3 4



dracflav 26 Oct 2016 15:54

22

It didnt take down the internet - it took down domain names.

Share

Report



Tintenfische dracflav 26 Oct 2016 16:11

76

Which made using the Internet a bit bloody tricky for people who weren't computer geeks. So for the vast majority of people "took down the internet" is appropriate.

Share

Report



mrwobbles dracflav 26 Oct 2016 16:16

17

Semantics, it stopped the proper functioning of the internet for several million users and brought down some significant servers. It was also a relatively small botnet, the January storm botnet had anywhere between 1-50 million devices under its control.

Share

Report

Show 3 more replies



Snaga 26 Oct 2016 15:59

13

The next step will be internet superfraudsters using Mirai to for crime on a global scale (probably a bigger risk than state cyber warfare). You won't be able to look at your fridge in the same way again. It's probably trying rob you.

Share

Report



HHeLiBeSnaga 26 Oct 2016 16:08

12

Or close the door with your head inside.

Share

Report



maxximateSnaga 26 Oct 2016 16:23

2

Unless they start blowing up fibre optic cables on the ocean floor.

Share



Report

Show 3 more replies

Most popular

How an egg beat Kylie Jenner at her own Instagram game
Amazon Echo Show (2nd gen) review: Alexa's bigger, brighter smart display
The internet, but not as we know it: life online in China, Russia, Cuba and India
Intruder alert! The best smart home security cameras
‘Inbox infinity’: is ignoring all your emails the secret to a happy 2019?
The great British Brexit robbery: how our democracy was hijacked
CES 2019: from beer tech to a banned sex toy – 10 standout gadgets
Why time management is ruining our lives
Microsoft Surface Pro 6 review: a fantastic tablet PC you shouldn't buy
Robotic dildo barred from top tech showcase, prompting sexism claims

Advertisement

Most commented The Guardian view on May's Brexit deal: it's over, but what's next? 	Most shared Theresa May loses Brexit deal vote by majority of 230 
---	---

US World Environment Soccer US Business **Tech** Science

Sign up to our daily email

Email
address

About us	All topics	Advertise with us
Contact us	All writers	Guardian Labs
Complaints & corrections	Digital newspaper archive	Search jobs
Secure Drop	Facebook	
Work for us	Twitter	

Support The Guardian

Contribute Subscribe

[Privacy policy](#)

[Cookie policy](#)

[Terms & conditions](#)

[Help](#)

[Back to top](#)