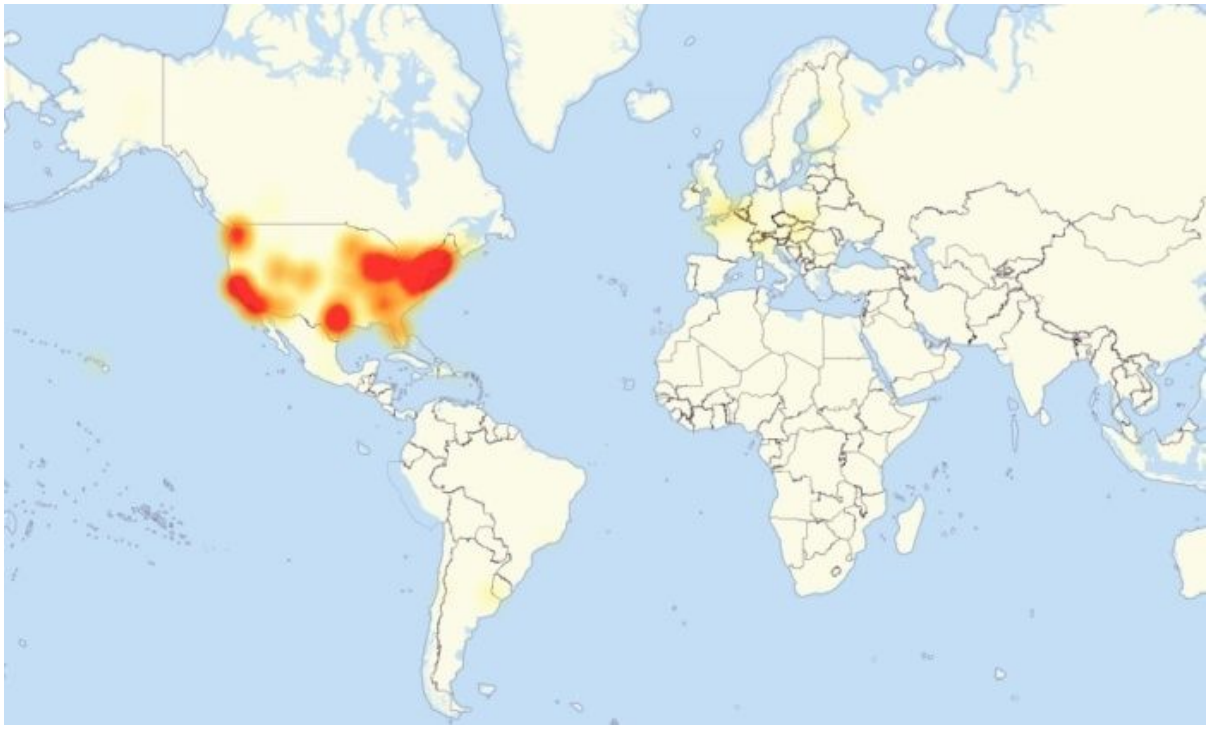
# An IoT botnet is partly behind Friday's massive DDOS attack

## DVRs and other devices compromised with the Mirai malware are being the attack.



A map of Friday's massive DDOS attack and the internet outages involved.

Malware that can build botnets out of IoT devices is at least partly responsible for a massive distributed denial-of-service attack that disrupted U.S. internet traffic on Friday, according to network security companies.

Since Friday morning, the assault has been disrupting access to popular websites by flooding a DNS service provider called Dyn with an overwhelming amount of internet traffic.

Some of that traffic has been observed coming from botnets created with the Mirai malware that is estimated to have infected over 500,000 devices, according to Level 3 Communications, a provider of internet backbone services.

About 10 percent of those Mirai infected devices are participating in Friday's DDOS attack, said Dale Drew, the company's chief security office in Periscope livestream. However, other botnets are also partaking in the attack, he added.

DDOS attacks and botnets are nothing new. However, the Mirai malware appears especially worrisome for its awesome power. An attack on the website of cybersecurity Brian Krebs last month managed to deliver 665Gbps of traffic to Kreb's site, making it one of the largest DDOS attacks ever recorded.

Unlike other botnets that rely on PCs, the Mirai malware targets internet-connected devices such as cameras and DVRs that have weak default passwords, making them easy to infect. Adding to the worry is that the developer behind Mirai has released the malware's source code to the hacker community.

Security firm Flashpoint said it has been able to confirm that some of the Mirai-infected machines involved in Friday's attack are DVRs.

The botnets participating in Friday's assault, however, are separate and distinct from those used to take down Kreb's website back In September, the security firm said.

Both Level 3 and Flashpoint have said copycat hackers have been trying to exploit the Mirai code since it was publicly released.

Friday's attack is still ongoing, according to Dyn. Its engineers are trying to mitigate "several attacks" aimed at its infrastructure. The company has also reportedly said that the DDOS attacks are coming from "tens of millions of IP addresses at the same time."

BRON: KAN, M., (2016), An IoT botnet is partly behind Friday's massive DDOS attack. Internet, via http://pcworld.com/article/3134056/hacking/an-iot-botnet-is-partly-behind-fridays-massive-ddos-attack.html op 22 oktober 2016.

---

# Ddos-aanval op dns-provider Dyn werd uitgevoerd met Mirai-botnet

Degene achter de ddos-aanval van vrijdag op dns-provider Dyn maakte gebruik van het Mirai-botnet, bestaande uit vele verschillende iot-apparaten. Eenzelfde netwerk werd kort geleden ook gebruikt om de website van securityjournalist Brian Krebs plat te leggen.

Zowel securitybedrijf Flashpoint als Dale Drew, securityhoofd van internetprovider Level 3, zeggen bij de aanval van vrijdag kenmerken gezien te hebben die erop duiden dat het om een Mirai-botnet gaat. Flashpoint zegt dat er in het botnet onder andere digitale videorecorders zitten waarvan bekend is dat ze vatbaar zijn voor verslaving aan het Mirai-netwerk. Dale Drew spreekt er tegenover Network World van dat er zo'n 50.000 tot 100.000 door Mirai geïnfecteerde iot-apparaten betrokken waren bij de aanval. Dat zou 20 procent zijn van het gehele Mirai-netwerk, dat volgens hem 500.000 apparaten behelst. Daarnaast werden ook nog andere botnets ingezet, maar daar is geen verdere informatie over bekend.

De aanval zou voornamelijk bestaan hebben uit *tcp syn floods*, verzoeken van clients om een *handshake* uit te voeren met een server. Daarnaast zou ook een grote hoeveelheid *subdomain attacks* plaats hebben gevonden, waarbij bots niet alleen naar een door Dyn beheerd domein navigeren, maar ook nog een obscuur, niet-bestaand subdomein opvragen. De dns-servers moeten dan nagaan of het subdomein wel bestaat of niet, wat extra rekenkracht vergt ten opzichte van een normaal verzoek tot verbinden.

De eerste aanval, die ongeveer twee uur lang aanhield, was gericht op Dyn-datacentra in Chicago, Washington D.C. en New York. Vandaar ook dat gebruikers aan de oostkust van de VS hier hinder van ondervonden; dns-lookups gaan bij Dyn altijd via de dichtstbijzijnde server. De tweede aanval was er een die ongetwijfeld nauwkeurig gepland is, aangezien deze 20 Dyn-datacentra wereldwijd tegelijk trof, om zo een veel grotere groep gebruikers te treffen. Van die laatste aanval hadden gebruikers hier in West-Europa dus ook last.

Volgens Nick Kephart, storingsanalist bij netwerkbedrijf ThousandEyes, hebben verschillende *internet backbone providers* zoals Level 3 er op een gegeven moment voor gekozen om hun verbinding met

Dyn tijdelijk af te breken om te voorkomen dat er ook buiten Dyn en de geassocieerde websites om congestie zou ontstaan. Hij vertelt dat ook aan Network World.

Het Mirai-botnet werd kort geleden nog ingezet om de website van securityonderzoeker Brian Krebs uit de lucht te halen. Kort daaropvolgend zette een persoon met de naam 'Anna-senpai' de broncode voor het botnet online voor iedereen om te gebruiken. De malware die erbij gebruikt wordt, richt zich op niet of zwak beveiligde iot-apparaten als ip-camera's en digitale videorecorders. Mirai is ook ingezet bij een ddos-aanval op de Franse internetprovider OVH. De ddos op de site van Krebs ging met 600Gbit/s en die op OVH met 1Tbit/s. Onduidelijk is hoeveel bandbreedte er kwam kijken bij de aanval op Dyn.

Op het moment lijkt het erop dat de aanvallen zijn opgehouden, zo schrijft ook Dyn zelf. Websites als die van Reddit, Soundcloud, Spotify, The New York Times, GitHub, Twitter en AirBnB zijn op het moment van schrijven vanuit Nederland ook gewoon bereikbaar.

BRON: HENDRIKMAN, M. (2016), Ddos-aanval op dns-provider Dyn werd uitgevoerd met Mirai-botnet. Internet, via https://tweakers.net/nieuws/117059/ddos-aanval-op-dns-provider-dyn-werd-uitgevoerd-met-mirai-botnet.html op 23 oktober 2016