theguardian

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'

Nicky Woolf in San Francisco

Wednesday 26 October 2016 21.42 BST

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.

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.”

More news

Topics

Hacking Data and computer security Internet Cybercrime