Technology CyberSecurity

Largest ever DDoS attack: Hacker makes Mirai IoT botnet source code public

The botnet code that took journalist Brian Krebs and French web host OVH offline is now freely available.

By Mary-Ann Russon

October 3, 2016 14:53 BST

The botnet behind the world's largest ever distributed denial of service (DDoS) attack that took out security journalist Brian Krebs' website could soon rear its head again as the source code has been made freely available for any hacker to take advantage of.

A hacker known only as 'Anna-senpai' has released the source code for the Mirai malware and a tutorial for setting it up on HackForums.net, which is one of the most popular hacking communities on the internet and is freely accessible on the open web.

Mirai hijacks connected Internet of Things (IoT) devices by continuously scanning the internet until it discovers systems and devices that are using the default usernames and passwords that are set by the factory before the product is first shipped to customers.

The malware turns the connected things into zombie bots that the hacker can control using a command and control (C&C) server and use to flood targets with web traffic to knock them offline.

Anna-senpai says that he or she has decided to make the malware's source code available because since the attack on Krebs' website and French web hosting provider OVH, which was found to be caused by hijacked security cameras, among other things, internet service providers (ISP) around the world have wised up to the dangers of unsecure IoT devices.

The hacker doesn't plan on using the code anymore as the number of zombie bots that can be hijacked is dropping to below 300,000 per attack, but he or she reckons that the code could still be substantially useful to anyone else that wants to try something similar.

The world's largest ever DDoS attack

On 20 September, KrebsOnSecurity.com was hit by a large and sustained, recordbreaking 665 Gbps DDoS attack designed to take the website offline. Krebs believes that the attack was likely issued by members of an Israeli online attack-for-hire service called vDOS, who were angry for Krebs for naming the two 18-year-old co-owners, who were arrested by Israeli police on the same day that the story came out.

This belief is further backed up by Anna-senpai's post, as the "readme" text file included with the source code is signed "FREEAPPLE4JACK", which is the online username used by one of the two arrested vDOS co-owners.

The DDoS attack raged on for three days and eventually Krebs' DDoS attack prevention service Akamai admitted defeat, fearing that it could no longer shield the website without impacting paying customers. Krebs' site was taken offline for two days, until Google decided to step in with its free DDoS attack mitigation service Project Shield, which is offered to verified journalists and nonprofit organisations for free.

Krebs explains that although IoT devices are easy to hack using Mirai and another IoT malware called Bashlite, it is easy for the infected things to be fixed. The devices just need to be rebooted, which deletes the malicious code from the memory. However, if you don't change the default password on the IoT thing in question, you're just opening yourself to being hacked yet again, and this can happen within just a few minutes of the device being rebooted and uninfected.

Bashlite's source code was leaked online in early 2015, and according to security firm Flashpoint and US telco Level 3 Communications, the malware has already managed to take over around one million IoT connected devices, so DDoS attacks could soon be on the rise if Mirai gains popularity too.