Cybersecurity

Case Study - Botnet

1.2.6 Bots and Botnets

Article:

Mirai IoT Botnet Co-Authors Plead Guilty
DEC 13, 2017
Retrieved from: https://krebsonsecurity.com/2017/12/mirai-iot-botnet-co-authors-plead-guilty/
Source: Krebs on Security
Author: Brian Krebs

The U.S. Justice Department on Tuesday unsealed the guilty pleas of two men first identified in January 2017 by KrebsOnSecurity as the likely co-authors of Mirai, a malware strain that remotely enslaves so-called "Internet of Things" devices such as security cameras, routers, and digital video recorders for use in large scale attacks designed to knock Web sites and entire networks offline (including multiple major attacks against this site).

Entering guilty pleas for their roles in developing and using Mirai are 21-year-old Paras Jha from Fanwood, N.J. and Josiah White, 20, from Washington, Pennsylvania.

Jha and White were co-founders of Protraf Solutions LLC, a company that specialized in mitigating large-scale DDoS attacks. Like firemen getting paid to put out the fires they started, Jha and White would target organizations with DDoS attacks and then either extort them for money to call off the attacks, or try to sell those companies services they claimed could uniquely help fend off the attacks.

In addition, the Mirai co-creators pleaded guilty to charges of using their botnet to conduct click fraud - a form of online advertising fraud that will cost Internet advertisers more than $16 billion this year, according to estimates from ad verification company Adloox.

The plea agreements state that Jha, White and another person who also pleaded guilty to click fraud conspiracy charges — a 21-year-old from Metairie, Louisiana named Dalton Norman — leased access to their botnet for the purposes of earning fraudulent advertising revenue through click fraud activity and renting out their botnet to other cybercriminals.

As part of this scheme, victim devices were used to transmit high volumes of requests to view web addresses associated with affiliate advertising content. Because the victim activity resembled legitimate views of these websites, the activity generated fraudulent profits through the sites hosting the advertising content, at the expense of online advertising companies.

Jha and his co-conspirators admitted receiving as part of the click fraud scheme approximately two hundred bitcoin, valued on January 29, 2017 at over $180,000.

Prosecutors say Norman personally earned over 30 bitcoin, valued on January 29, 2017 at approximately $27,000. The documents show that Norman helped Jha and White discover new, previously unknown vulnerabilities in IoT devices that could be used to beef up their Mirai botnet, which at its height grew to more than 300,000 hacked devices.

Summary

In mid 2016, two young men helped write the Marai malware, which used IoT devices (with either the default password or no set password) to create a giant botnet. The malware attacked routers, baby cameras, printers, and any other devices that were using default passwords. The two men, Paras Jha and Josiah White, used this botnet to attack their school's network to delay exams and delay other students from signing up for classes. Paras and Josiah then decided to start a company, Protraf, to stop botnets – just like the ones they operated. They also rented out their botnet to another man, Dalton Norman, who used it to gain clicks (or visits) to pages that contained advertisements. This allowed him to earn hundreds of thousands of dollars from advertising companies who thought their ads were being looked at by a lot of people but it was just the botnet faking the numbers.

When the FBI started closing in on these men, they released the source code for Marai to help hide their tracks. This source code was used for multiple DDoS attacks, including the 2016 Dyn attack that brought down major websites like Amazon, Reddit, and PayPal. All three men were caught and convicted but received substantially reduced sentences in exchange for cooperating with investigators to catch cyber criminals. Variations of the Marai malware continue to exist to this day.

Questions

- Creating and maintaining botnets is currently illegal under the Computer Fraud and Abuse Act and other related cyber laws. Should there be a specific law created to make use of botnets expressly illegal?
- If you only use/rent a botnet (but are not the creator), are you breaking the same laws?
- Most botnets are used for spam and DoS attacks. When might it be legal/ethical to create/use a botnet? Are there any valid uses of a botnet? What if the US military wanted to attack a foreign threat actor? How would that be different?
- Is it legal to produce "fake views" on a website with a botnet to earn advertising money? What laws might be broken?
- Should cyber criminals be allowed to reduce their sentences if they work with investigators to catch other cyber criminals?
- The Mirai botnet preyed on devices using default passwords. In 2018, California created the California Consumer Protection Act which prohibits manufacturers from shipping products with a single default password for all devices. Is this protection enough to stop further such attacks?

Further Study

- Wikipedia's Page on the 2016 Attack: https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
- Department of Justice's 2015 memo on fighting malware (published before the Mirai case): https://www.justice.gov/archives/opa/blog/prosecuting-sale-botnets-and-malicious-software