MBNA Publishing House Constanta 2021

Proceedings of the International Scientific Conference SEA-CONF

IoT Botnets Detection

To cite this article: S. BÎRLEANU, D. GLĂVAN, C. RĂCUCIU and M. PREDA, Proceedings of the International Scientific Conference SEA-CONF 2021, pg.57-60.

Available online at www.anmb.ro

ISSN: 2457-144X; ISSN-L: 2457-144X

doi: 10.21279/2457-144X-21-007

IoT Botnets Detection

S Bîrleanu, D Glăvan, C Racuciu, M Preda
sorin.birleanu@mta.ro

Abstract: Threats of this type are a serious problem, in 2017 there were records in terms of bandwidth (over 1Tbps) related to DDoS attacks carried out using IoT (Internet of Things) botnets. A botnet is a network that includes a series of devices connected to the Internet, called bots. The term "botnet" is composed of the words "robot" and "network". Each of these devices has been infected with malware that allows the attacker to remotely control them. Thus, botnets can be used to carry out distributed denial-of-service attacks (DDoS attacks), data theft, and sending spam messages, allowing the attacker to access the device and its connection. , which means that each device must be identified / isolated / repaired individually. One of the techniques for detecting bot attacks is the so-called "signature-based systems", in which the software will try to detect patterns in the request packet. This paper presents a method for detecting IoT Botnets as well as the main features of strong Botnet networks.

1. Introduction

IoT is the totality of devices that have the ability to detect aspects of the real world, such as light, humidity, movement, temperature, which are connected to the Internet. All this data is collected and, based on it, IoT acts. For example, if your LEDs are connected to an intelligent control system, they will turn on and off automatically, without your intervention, depending on the amount of natural light or the presence / absence of movement (people, animals, etc.) detected of sensors. Smart devices can communicate with each other via Wi-Fi technology or through applications specially designed for smartphones, tablets or laptops. Of course, you are at the heart of the entire IoT system. You are the one who controls the action of your devices, even remotely, taking into account your needs. Botnets are networks composed of remotely controlled computers or "bots". These computers have been infected with malware that allows them to be controlled remotely. Some botnets are made up of hundreds of thousands - or even millions - of computers. If your computer is part of a botnet, it is infected with a type of malware. The bots contact a remote server - or just get in touch with other robots nearby - and wait for instructions from the botnet controller. This allows an attacker to control a large number of computers for harmful purposes.

Computers in a botnet can also be infected with other types of malware, such as keyloggers that record your financial information and send it to a remote server. What makes a computer part of a botnet is that it is remotely controlled along with many other computers. The creators of the botnet can later decide what to do with the botnet, direct the robots to download additional types of malware and even act together.

The IoT infrastructure is a dynamic network with self-configuring capabilities based on standard interoperable communication protocols. Today, the development of the IoT concept has become a priority. The number of smart devices connected to the network has exceeded the number of the population. According to research, almost 50 billion smart devices are currently connected, but the main problem remains the low security of these devices. Security issues such as the inability to defend against brute force attacks for a large number of devices. Thus, IoT is becoming a modern tool used by cybercriminals to obtain sensitive data.

Cyber attackers use IoT devices to install ransomware, obtain personal information, and include it in a botnet. Botnets are used in spam, phishing, malware delivery, but especially in DDoS. IoT has become a priority when it comes to the security of devices connected to the Internet. In 2016, there were DDoS attacks on companies that have a major impact on society such as Amazon and Twitter and about 500,000 devices were compromised.

This paper presents a method for detecting IoT Botnets as well as the main features of strong Botnet networks. Also here, it describes from a technical point of view, a method by which infected IoT devices are found.

2. Botnets

The main goal of a cyber attacker while compromising IoT devices is to include them in a botnet. Botnet is a network of infected devices that are controlled by malware. Typically, attackers use special Trojan programs to bypass device IDS and IPS, thus gaining unauthorized control over the devices they integrate into a botnet and remotely control them. Mainly, this network consists of devices with a low level of security. The distribution of IoT devices has been fast-paced lately, so they have become a priority target of attackers aiming to compromise important personal data. The Mirai botnet is considered to be the largest botnet in history.

It consisted of the following stages:

- Scanning the IPv4 address space to obtain sensitive devices with open TCP ports;
- Using a TELNET network service;
- Performing a brute force attack;
- Once the device is part of the botnet, it scans the address space to find other vulnerable devices.

Once the device is part of the Botnet, the user of the device may not be aware of this and perform malicious actions by commanding the attacker. Over time, other types of Botnet have appeared, such as Amnesia and Leet Botnet. Currently, there is a significant increase in the number of DDoS attacks. Due to the large number of devices and the low security of these devices, botnets remain a priority of cyberspace. Figure 1 shows the steps that must be taken for a device to become an efficient part of a botnet.

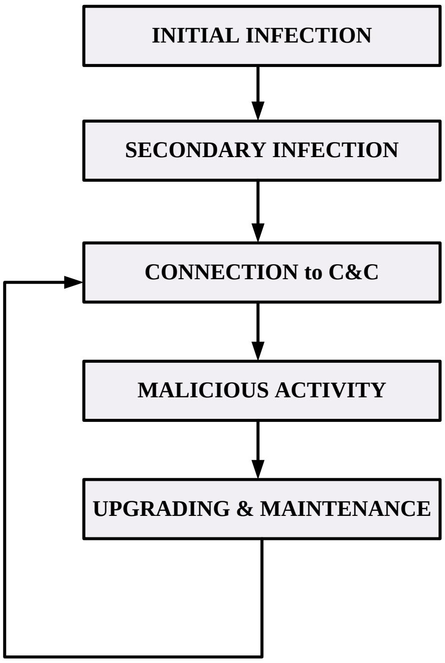

Figure 1 Life-cycle

In the first stage, a compromise of a vulnerable device is made, this being considered as a potential bot. In the second stage, the download and installation of malware takes place, which is necessary to achieve communication. The third step is to connect to the command and control server. The next step is malicious activity. The last stage is represented by monitoring and maintaining the connection. At any time, if the chain breaks, it avoids the large-scale loss of information. This paper presents a method of detecting botnets in the propagation stage, representing the first stage.

3. Methodology

In this paper, a logistic regression model is used to detect botnets. This model is a statistical model used to estimate the probability that an event will occur based on a set of variables (predictors). The logistic regression is based on the function f (y) expressed as follows:

$$f(y) = \frac{1}{1 + e^{-y}}$$

y is expressed as a linear function with n input variables.

$$y = \beta_0 + \beta_1 x_1 + \cdots + \beta_n x_n$$

Based on the variables, the probability of an event is expressed as follows:

$$P(x_1, x_2, \ldots, x_{n-1})=f(y)$$

This logistic regression model is used to estimate the probability that a device will be part of an IoT botnet. To create this model, the following parameters are used that have been selected as predictors:

- Port of destination-most attackers rely on brute force attacks to gain access to the device;
- Open source ports-malicious requests are sent by the host through the open port used to obtain instructions from the command and control server;
- Number of requests;
- The interval between requests;
- Number of requests on other ports.

This model can be used to detect botnet networks that are used for unauthorized access to IoT devices by carrying out brute force attacks on TELNET / SSH services.

4. Conclusion

For this model, it is estimated that the number of smart devices is about 50 billion, they have a very low level of security. Thus, IoT botnets are becoming a very popular tool for carrying out larger attacks such as DDoS used by cybercriminals. It is necessary to protect personal data, a technique for detecting IoT botnets. This paper presents a technique for detecting IoT botnets in the propagation phase, if an infected IoT device compromises other devices to increase the size of the botnet. This model applies to brute force attacks using TELNET or SSH protocols.

REFERENCES

[1] Friess P., Gusmeroli S.,Bassi A. 2011 *Internet of Things-Global Technological and Societal Trends*

[2] Gubbi J., Marusic S., Palaniswami 2013 *A vision, architectural elements, and future directions*

[3] Dobbins R. 2016 *Mirai IoT botnet description and ddos attack mitigation*

[4] Ylonen T. 2006 *The secure shell (SSH) protocol architecture*

[5] Perdisci R., Lee, W. 2008 *BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection*