MILITARY UNIVERSITY OF TECHNOLOGY

Faculty of Cybernetics

CLUSTERING-BASED METHOD FOR BOTNET DETECTION

Abstract

Hubert Ostap, M.Sc.

Supervisor: Ryszard Antkiewicz, Ph.D.

September 20, 2019

The ongoing arms race between botnet developers and developers of their detection methods has turned a simple centralized botnet into a very difficult to detect hybrid form of this kind of threat. Furthermore, a constant process of development and a very fast evolution makes botnets very hard adversaries to fight with. Because of a large number of botnet implementations there are also a lot of methods of their detection. On the other hand, a large growth of botnet implementations doesn't mean that all botnet detection methods are improving.

The most effective methods are based on the analysis of the network traffic, without the need to analyze the content of packets. Those methods do not require physical access to the potentially infected devices and are employed to identify suspicious communication in the network traffic. This is the main reason why they are most frequently implemented nowadays. They owe their popularity to the simplicity of use. In most cases they do not require any additional hardware; additionally, no modification in the structure of the network is needed. After suspicious communication, as well as the devices that generate that traffic, have been identified, analysis commences where host-based methods are used to discover for example other C2 servers. They could also be adopted in any part of a botnet life cycle but their main advantage is the possibility to detect even unknown botnets in creation or maintenance phases, which have not been used for any attack so far. There is a subgroup of especially effective methods which are based on detecting synchronous action. An representative of such methods is BotGAD. High efficiency of such methods is based on the assumption that botnets must work synchronously in order to achieve their goals. To conduct a successful SPAM campaign or a DDoS attack, it requires the Botmaster to use as many bots as possible. During the research, it was observed that synchronous activity occurs not only during the attack phase but also during the creation and management phases of the Botnet. This fact allows us to detect the threat before the first attack, which is a big improvement compared to the already known methods.

It was also observed during the research of different botnet detection methods (especially BotGAD) that there are situations in which legal users generate synchronous traffic, for example to of Facebook or Twitter servers during very important events such as football world championships or significant political events. All posts and comments written during such events are generated with high intensity, therefore this kind of network traffic is recognized as a synchronous action. Despite this, even in such situations cosine similarity factor never exceeds level of 0.5. The figure Figure 1 presents graphical illustrations of such a situation. Every source IP which connects to the destination IP being analyzed is plotted on the vertical axis and moments when the connection took place are on the horizontal axis. Red dots represent the connection time that belongs to the most active Source IP address. Between every pair of red dots there is a green vertical line, it's a border between clusters; those lines are created based on red dots which are the centers of clusters. Blue dots denote a connection to the selected Destination IP from IP addresses that belong to the analyzed network. If network traffic was gathered over few days, the chart representation will separate the days from each other with a vertical white line.

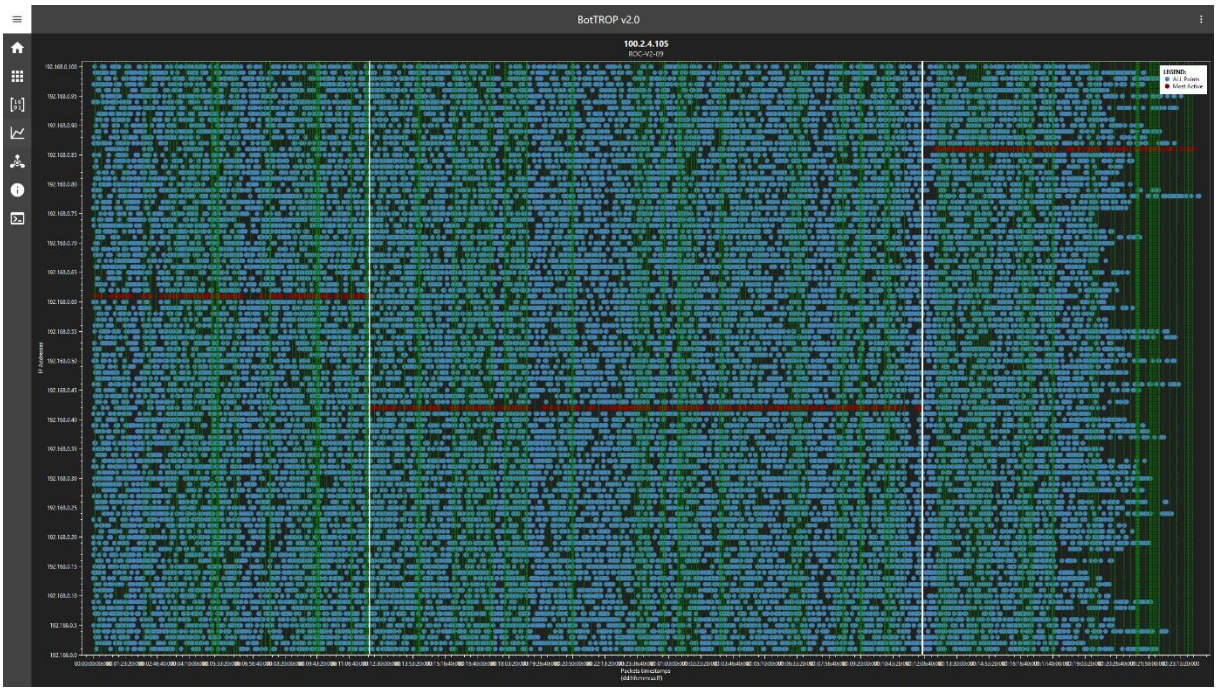

Figure 1 The Legal network traffic with 0.5 cosine similarity factor.

During the research even more intense legal network traffic never exceed 0.5. For comparison, a typical synchronous behavior of a botent has been graphically shown in the figure Figure 2.

Figure 2 The Synchronous network traffic generated by a botnet.

One can see here a much smaller amount of generated network traffic, but its specific arrangement causes that the cosine similarity factor is very high (0.8).This comparison proves BotTROP's effectiveness even during very intense network flow generated by legal users and botnets.

There a lot of different botnet detection methods but most of them are not efficient against unknown threats, moreover most of them are able to detect a botnet based on a specified protocol. The algorithm described in this dissertation is an attempt to change this situation and make networks more secure. BotTROP, just like BotGAD, identifies not only well-known botnets (which was proved in experiments with Powershell Empire, Neris and others) but also unknown threats (for example TwitterBot based on social networks, which was implemented for the need of this dissertation). It also improves detection of synchronous activity among different protocol.

The scientific task carried out in this dissertation was to build a method of detecting botnets using synchronous activity feature, such that the following requirements be met:

- an appropriate method of clustering network traffic will be used to detect synchronous communication;
- it will be possible to analyze network traffic for any communication protocol;
- it will be possible to detect not only already known botnets but also previously unidentified ones;
- the efficiency of botnets detection will be higher than for previously known methods based on the identification of synchronous communication.

The BotTROP method was created as a modification of the BotGAD algorithm. Major improvements and changes are listed below:

- resignation from grouping traffic in *Time Window*; instead, the clustering method is used to determine groups of moments when communication with a specific destination IP address is repeated (or a group of such addresses). This procedure allows us to remove the basic disadvantage of BotGAD, i.e. the need for determining the size of the *Time Window*. The correct *Time Window* length has a significant impact on the effectiveness of this method;
- making it possible to analyze many different communication protocols;
- speed up the whole process of analysis, which is very important especially in big networks;
- assuming the synchronism of botnets, it was possible to detect them during the creation and maintenance phases before the first attack is carried out. Thanks to the proposed method it is possible not only to identify a malicious C2 but also all the infected devices that belong to the identified botnet inside the monitored corporate network.

An important part of this dissertation was the verification of the properties of the BotTROP method. During this process the following issues were encountered:

- very low availability of the network traffic generated by real botnets. The exception is malicious network traffic made available by researchers from the Czech Technical University, which was collected by Honeypot launched under the Malware Capture Facility Project [MCFP] project. In addition, the network traffic captured within the Military University of Technology in Poland was used for verification. Apart from legal traffic, there were 12 destination IP addresses associated with various botnets which were successfully identified by BotTROP. Also, 36 IP addresses were identified in this traffic, with which communication was carried out in a particularly synchronous manner, this fact may indicate that they are also associated with botnet networks;
- network traffic generated by unknown botnets is not available for obvious reasons. In order to verify BotTROP's ability to detect unidentified botnets, two simulators were

implemented: Legal Network Traffic Simulator (LNTS) and Botnet Network Traffic Simulator (BNTS).Furthermore tool called TwitterBOT was also implemented for this purpose.

The BotTROP algorithm, whose requirements are presented in Chapter II, has been fully implemented and tested on both simulated and real-time traffic. For the purposes of comparison with another method, the BotGAD algorithm has been implemented. Just as BotTROP, it tries to detect synchronous activity. Thanks to this, an empirical comparison was possible, which showed a significant advantage of the BotTROP method. It is worth adding that the BotGAD method was implemented by its developers only for the purposes of the DNS protocol. For comparative purposes it was extended by the author of this dissertation to all TCP and UDP traffic.

The verification of the BotTROP method involves two types of different experiments:

1. The experiment whose purpose is to detect real and simulated botnets based on network traffic composed of the following components:
   - real computer networks traffic of the Military University of Technology in Warsaw, Poland;
   - real traffic generated by real-life malware and registered in the Czech Technical University in Prague during The Malware Capture Facility Project (MCFP);
   - network traffic generated by Powershell Empire and TwitterBot;
2. The experiment whose purpose is to detect botnets in network traffic generated by a botnet simulator and a legal network traffic simulator.

The aim of the first experiment was to verify the ability of the BotTROP method to detect known and unknown botnets and to analyze any communication protocol – the results are presented in chapter 5.1. The second experiment sought to evaluate the quality of the BotTROP method and to compare it with the quality of the BotGAD method – the results are presented in chapter 5.2. All the results prove that BotTROP is a very efficient method for botnet detection of any kind, no matter the protocol or architecture. It is very important to underline that the role of the BotTROP method is to identify synchronous activity which in most cases takes place in malicious activity. Implementing a white list where synchronous activity is also spotted, for example during system upgrades can help to decrease the number of false negatives and false positives rate. Presented results also reveal that the BotGAD method is very dependent on *Time Window* parameter, which is one of its biggest disadvantages. This makes the method unusable against unknown botnets because it is necessary to set up a relevant parameter for communication sessions with its C2. The BotTROP method is independent of *Time Window* parameters and can be used efficiently even against unknow - malicious or legal - network traffic, which in turn makes it possible to identify an unknown botnet.

It is possible to use the BotTROP method in a production environment without any modification but there are a lot of improvements that are going to be made in the nearest future.

In order to use BotTROP in a working network, it is only necessary to provide its traffic for analysis. Currently, this is done by saving the traffic to a separate file. Currently work is underway on the possibility of on-line analysis without the need to collect the analyzed network traffic. Afterwards, all the collected network traffic is analyzed by the BotTROP algorithm, the administrator has the possibility to verify the cosine similarity for each destination address and a preview of which hypothesis was adopted by the SPRT method. The described tool is extended toward a possibility of continuous monitoring and calculation of the results obtained

in order to transform them into a graph showing the dependence of cosine similarity and time. This will allow the administrator to visually observe subsequent changes. In addition, it will enable the administrator to visually observe subsequent changes and allow them to quickly identify synchronous traffic that may appear or disappear depending on the day of the week. This functionality is useful because it has been observed that some botnets are not active during the weekend. Analyzing the network traffic at the Military University of Technology, it was observed that the average cosine similarity decreased during the weekend in one situation: it happened due to the shutdown of computers at the university in most rooms on those days.

The implemented project meets all the requirements listed above simultaneously proving a very high effectiveness not only for simulated traffic but also for real communication within botnets.