16th Workshop on Generalized Nets and Data Mining
10 February 2018, Sofia, Bulgaria, 29–35, ISSN 1313-6860

Generalized Net Model of Botnet Network

Ivan Batakov

Faculty of Computer Science and Engineering, Software Engineering
Burgas Free University
62 San Stefano Street, Burgas - 8001, Bulgaria
email: mmdollar@gmail.com

Abstract: Malicious botnets have become a common threat and pervade large parts of the Internet today. Existing surveys and taxonomies focus on botnet topologies, Command and Control (C&C) protocols, and botnet objectives. Methods for botnet establishment and operation have evolved significantly over the past decade resulting in the need for detection methods that are capable of detecting new, previously unknown types of botnets. In this paper we are going to show you a simple model of a botnet network.
Keywords: Botnet, Security, Network topology.
AMS Classification: 68Q85, 94A60.

1 Introduction

Over the last two decades, the Internet and more generally cyberspace have had tremendous influence on all spheres of society. Our daily lives, our fundamental rights, our social interactions and our economies depend on the impeccable work of information and communication technologies. The availability of open and free cyberspace has boosted the political and social inclusion of the world; it has removed the barriers between countries, communities and citizens, providing opportunities for interaction and the exchange of information and ideas worldwide; it provided a forum for free expression of opinions and the exercise of fundamental rights and supported people in their aspirations for democratic and fairer societies - this became particularly impressive during the Arab Spring.

Other ways of winning using the Internet, though not so direct, are botnet networks [5]. Botnet is a network that involves a number of computers that are "zombie" to perform activities that are being transferred from elsewhere. Some malicious code-makers aim to turn a system into a zombie - installing malicious code that opens backdoors and effectively gives the hacker control over the computer and he (the author/hacker) can use it for different things [4]. The idea is to have many such computers - hundreds, thousands, millions. These armies of workers are sold / leased to other people who are willing to pay large amounts of money to own such a resource that can use it for various attacks, spamming, and what not. As the Cryptocurrencies grew, more and more botnets started to enter the market in order to mine currencies (one big botnet could earn several million euros per month) [6]. All this is done in secret without the user

understanding that his computer is being used for such things as the surface system continues to obey the user so that he/she does not doubt that there is wrong with their system. Therefore, sometimes (more often and more often) similar infections come accompanied by a rootkit to mask all these unwanted actions the computer performs.

2 Generalized Net Model

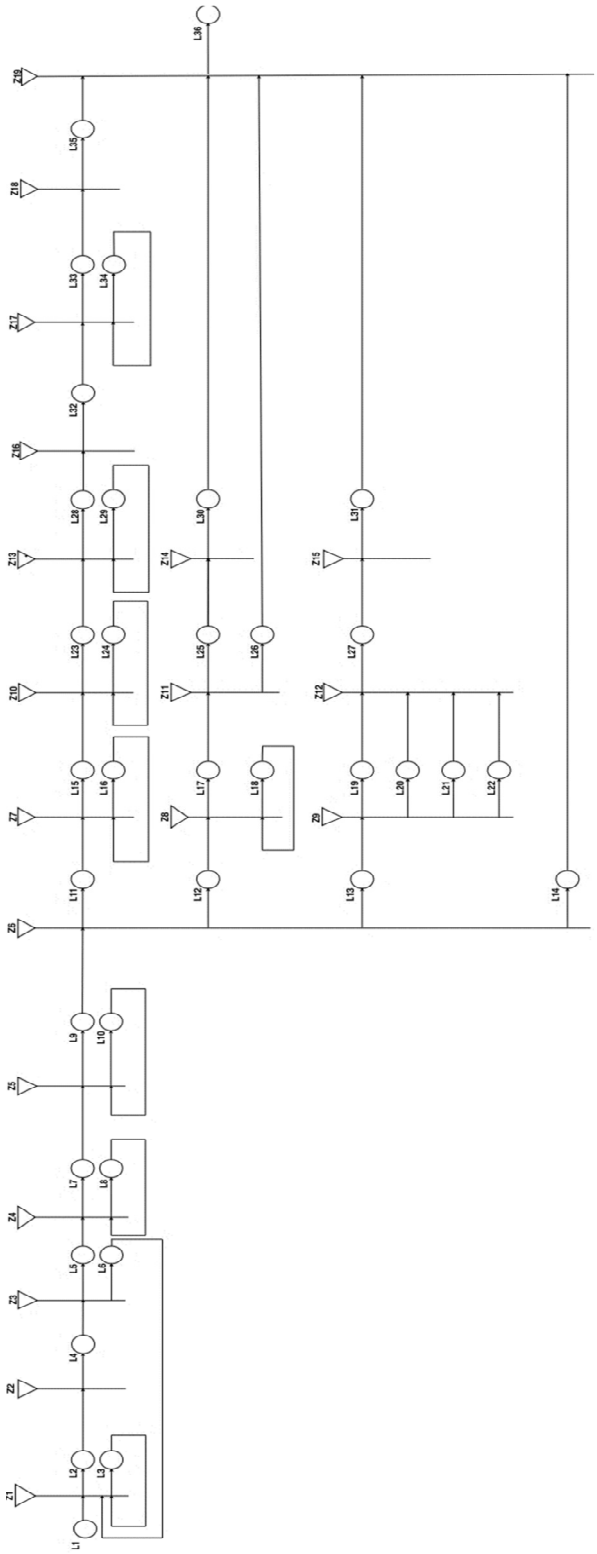

Figure 1. Generalized net model

The starting characteristics of the token L_1 is “Server connection“.
M – the capacities of the places is 1 for all.

$$Z_1 = \langle \{L_1\}, \{L_2, L_3\}\ R_1, \vee(L_1, L_3, L_6) \rangle$$

Z_1 – Connecting to the server

$$R_1 = \begin{array}{c|cc} & L_2 & L_3 \\ \hline L_1 & W_{1,2} & W_{1,3} \\ L_3 & W_{3,2} & W_{3,3} \\ L_6 & false & true \end{array}$$

Token receives a characteristic „Established connection“.
$W_{1,2} = W_{3,2}$ - Connection established;
$W_{3,2} = W_{3,3}$ - Connection is not established;

$$Z_2 = \langle \{L_2\}, \{L_4\}, R_2, \vee(L_4) \rangle$$

Z_2 – Saving IP Address…in the database

$$R_2 = \begin{array}{c|c} & L_4 \\ \hline L_2 & true \end{array}$$

$$Z_3 = \langle \{L_4\}, \{L_5, L_6\}, R_3, \vee(L_4) \rangle$$

Z_3 – Getting access to command web page

$$R_3 = \begin{array}{c|cc} & L_5 & L_6 \\ \hline L_4 & true & false \end{array}$$

Token receives a characteristic „Access to webpage“.

$$Z_4 = \langle \{L_5\}, \{L_7, L_8\}\ R_4, \vee(L_5, L_8) \rangle$$

Z_4 – Login check

$$R_4 = \begin{array}{c|cc} & L_7 & L_8 \\ \hline L_5 & W_{5,7} & W_{5,8} \\ L_8 & W_{8,7} & W_{8,8} \end{array}$$

Token receives a characteristic „Correct username“.
$W_{5,7} = W_{8,7}$ - Username is correct;
$W_{5,8} = W_{8,8}$ - Username is not correct;

$$Z_5 = \langle \{L_7\}, \{L_9, L_{10}\}, R_5, \vee(L_7, L_{10}) \rangle$$

Z_5 – Check to see if the command exists

$$R_5 = \begin{array}{c|cc} & L_9 & L_{10} \\ \hline L_7 & W_{7,9} & W_{7,10} \\ L_{10} & W_{10,9} & W_{10,10} \end{array}$$

Token receives a characteristic “Command“.
$W_{7,9} = W_{10,9}$ - The command exists;
$W_{7,10} = W_{10,10}$ - The command does not exist;

$$Z_6 = \langle \{L_9\}, \{L_{11}, L_{12}, L_{13}, L_{14}\}, R_6, \vee(L_9) \rangle$$
Z_6 – Check the type of the command

$$R_6 = \begin{array}{c|cccc} & L_{11} & L_{12} & L_{13} & L_{14} \\ \hline L_9 & W_{9,11} & W_{9,12} & W_{9,13} & W_{9,14} \end{array}$$

Token receives a characteristic „Type of command“.
$W_{9,11}$ - The command is from type Keylogger (software which logs all keypresses);
$W_{9,12}$ - The command is from type Ping Flood (type of cyber attack);
$W_{9,13}$ - The command is from type getInfo;
$W_{9,14}$ - The command is from type exit;

$$Z_7 = \langle \{L_{11}\}, \{L_{15}, L_{16}\}, R_7, \vee(L_{11}, L_{16}) \rangle$$
Z_7 – Check to see if the keylogger is installed

$$R_7 = \begin{array}{c|cc} & L_{15} & L_{16} \\ \hline L_{11} & W_{11,15} & W_{11,16} \\ L_{16} & W_{16,15} & W_{16,16} \end{array}$$

Token receives a characteristic „Downloaded Keylogger“.
$W_{11,15} = W_{11,16}$ - Keylogger is downloaded;
$W_{16,15} = W_{16,16}$ - Keylogger is not downloaded;

$$Z_8 = \langle \{L_{12}\}, \{L_{17}, L_{18}\}, R_8, \vee(L_{12}, L_{18}) \rangle$$
Z_8 – Check to see if the bot has a stable internet connection

$$R_8 = \begin{array}{c|cc} & L_{17} & L_{18} \\ \hline L_{12} & W_{12,17} & W_{12,18} \\ L_{18} & W_{18,17} & W_{18,18} \end{array}$$

Token receives a characteristic „Internet connection“.
$W_{12,17} = W_{12,18}$ - The internet connection is stable;
$W_{18,17} = W_{18,18}$ - The internet connection is not stable;

$$Z_9 = \langle \{L_{13}\}, \{L_{19}, L_{20}, L_{21}, L_{22}\}, R_9, \vee(L_{13}) \rangle$$

Z_9 - Check for available information about the infected computer

$$R_9 = \begin{array}{c|cccc} & L_{19} & L_{20} & L_{21} & L_{22} \\ \hline L_{13} & W_{13,19} & W_{13,20} & W_{13,21} & W_{13,22} \end{array}$$

Token receives a characteristic „Used software“.

$$Z_{10} = \langle \{L_{15}\}, \{L_{23}, L_{24}\}, R_{10}, \vee(L_{15}, L_{24}) \rangle$$

Z_{10} – Check to see if the Keylogger is started

$$R_{10} = \begin{array}{c|cc} & L_{23} & L_{24} \\ \hline L_{15} & W_{15,23} & W_{15,24} \\ L_{24} & W_{24,23} & W_{24,24} \end{array}$$

Token receives a characteristic „Keylogger status“.
$W_{15,23} = W_{15,24}$ - Keylogger is started;
$W_{24,23} = W_{24,24}$ - Keylogger is not started;

$$Z_{11} = \langle \{L_{17}\}, \{L_{19}, L_{20}\}, R_{11}, \vee(L_{17}) \rangle$$

Z_{11} – Check to see if the target has internet

$$R_{11} = \begin{array}{c|cc} & L_{25} & L_{26} \\ \hline L_{17} & W_{17,25} & W_{17,26} \end{array}$$

Token receives a characteristic „Target status“.

$$Z_{12} = \langle \{L_{19}, L_{20}, L_{21}, L_{22}\}, \{L_{27}\} R_{12}, \vee(L_{19}, L_{20}, L_{21}, L_{22}) \rangle$$

Z_{12} - Processing the collected information

$$R_{12} = \begin{array}{c|c} & L_{27} \\ \hline L_{19} & true \\ L_{20} & true \\ L_{21} & true \\ L_{22} & true \end{array}$$

Token receives a characteristic „Processed information“.

$$Z_{13} = \langle \{L_{23}\}, \{L_{28}, L_{29}\}, R_{13}, \vee(L_{23}, L_{29}) \rangle$$

Z_{13} – Check to see if there are any keys pressed

$$R_{13} = \begin{array}{c|cc} & L_{28} & L_{29} \\ \hline L_{23} & W_{23,28} & W_{23,29} \\ L_{29} & W_{29,28} & W_{29,29} \end{array}$$

Token receives a characteristic „Key pressed“.
$W_{23,28} = W_{23,29}$ - A key is pressed;
$W_{29,28} = W_{29,29}$ - No key is pressed;

$$Z_{14} = \langle \{L_{25}\}, \{L_{30}\}, R_{14}, \vee(L_{25}) \rangle$$
Z_{14} – Sending packet

$$R_{14} = \begin{array}{c|c} & L_{30} \\ \hline L_{25} & true \end{array}$$

Token receives a characteristic „Packet status“.

$$Z_{15} = \langle \{L_{27}\}, \{L_{31}\}, R_{15}, \vee(L_{27}) \rangle$$
Z_{15} – Prints information on the terminal

$$R_{15} = \begin{array}{c|c} & L_{31} \\ \hline L_{27} & true \end{array}$$

$$Z_{16} = \langle \{L_{28}\}, \{L32\}, R_{16}, \vee(L_{6}) \rangle$$
Z_{16} – Writing every key press in the log file

$$R_{16} = \begin{array}{c|c} & L_{32} \\ \hline L_{28} & true \end{array}$$

$$Z_{17} = \langle \{L_{32}\}, \{L_{33}, L_{34}\}, R_{17}, \vee(L_{32}, L_{34}) \rangle$$
Z_{17} – Send the log file to the server every 60 min.

$$R_{17} = \begin{array}{c|cc} & L_{33} & L_{34} \\ \hline L_{32} & W_{32,33} & W_{32,34} \\ L_{34} & W_{34,33} & W_{34,34} \end{array}$$

$W_{32,33} = W_{32,34}$ - 60 minutes have passed since the last send log file;
$W_{34,33} = W_{34,34}$ - 60 minutes have not passed since the last send log file;

$$Z_{18} = \langle \{L_{33}\}, \{L_{35}\}, R_{18}, \vee(L_{33}) \rangle$$
Z_{18} – Log file is being send to the ftp server

$$R_{18} = \begin{array}{|c|c|} \hline & L_{35} \\ \hline L_{33} & true \\ \hline \end{array}$$

$$Z_{19} = \langle \{L_{35}, L_{26}, L_{31}, L_{14}\}, \{L_{36}\}, R_{19}, \vee(L_{35}, L_{26}, L_{31}, L_{14}) \rangle$$

Z_{19} – Check for the status of the program/command

$$R_{19} = \begin{array}{|c|c|} \hline & L_{36} \\ \hline L_{35} & true \\ \hline L_{26} & true \\ \hline L_{31} & true \\ \hline L_{14} & true \\ \hline \end{array}$$

3 Conclusion

In this article, I tried to show how a summary network of a simple Botnet type works in order to understand more about them, how to protect against them and how attackers control them. Using the power of a few thousand bots, it's viable to stop almost any site or network instantly. Even in unskilled hands it should be obvious that botnets are a loaded and powerful weapon. Since botnets represent such a powerful threat, we need different mechanisms to counteract it. That is why more research is needed in this area, the attackers do not sleep. As these threats continue to adapt and change, security must be the case.

References

[1] Atanassov, K., *On Generalized Nets Theory*, Prof. M. Drinov Academic, Publ. House, Sofia, 2007.

[2] Orozova D., *Generalized Net Models of intelligent tutoring environments*, "Prof. Marin Drinov" Academic Publishing House, Sofia, 2011.

[3] Orozova, D., K. Atanassov, Generalized Net Model of the Process of Selection and Usage of an Intelligent e-Learning System, *Comptes rendus de l'Académie bulgare des Sciences*, book No 5, vol. 65, 2012, pp. 591-598,

[4] *New(ish) Mirai Spreader Poses New Risks* (article), `https://securelist.com/newish-mirai-spreader-poses-new-risks/77621/`

[5] IT-Security researcher, `https://abuse.ch/`

[6] *Smominru Monero mining botnet making millions for operators*, ProofPoint, 31 January 2018: `https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators`