International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.47-54
http://dx.doi.org/10.14257/ijsia.2015.9.11.05

Malicious Processor Detection based on the Security Agent

Seong-Muk Choi[1], Yeol-Joo Ryou[2], Hoo-Ki Lee[3], Hee-Hoon Cho[4] and Jong-Bae Kim[5*]

[1, 3]Dept. of IT Policy and Mgmt.,
Graduate School of Soongsil Univ.,
Seoul, 156-743, Korea
[2]Baileytech Co., Ltd., #804, IT Premier Tower, Gasan-dong,
Seoul, 153-707, Korea
[4, 5]Graduate School of Software, Soongsil University,*
Seoul, 156-743, Korea
[1]csm0107@gmail.com, [2] you10joo@gmail.com, [3]hk0038@korea.kr,
[4]heehoonc@naver.com, [5] kjb123@ssu.ac.kr*

Abstract

Recently, as Internet is widely used due to the increased spread of the internet network, the software with malicious intent is distributed via the internet and its infection path gets various too. In particular, attacks by Bot mainly work at C&C (command-and-control) server but it can be secured just by blocking IP because C&C server runs in form of IP. However, this attacker too gets gradually intelligent as they try to connect periphrastically in order to avoid server blocking. Once these malicious codes infiltrate user's system, it is not easy to detect it through general detection method while it is running. In this paper, we propose malicious process detection system based on security agent in order to prevent damage caused by malicious code infection from spreading.

Keywords*: Security, Malware, Botnet, System Model.*

1. Introduction

The software of malicious intent is called malicious software or malicious code or bot. Bot is short for robot, and refers to malicious programs that control the systems infected with a bot and performs various types of attacks. The malicious code forms network of Botnet and performs variety of attacks such as collecting information, sending mail, fishing, distributing malicious code, DDos (Distributed Denial of Service) attacks under order of Bot master. Botnet makes bad influence to network infra such as router and DNS (Domain Name System) server as well as the internet user [1].Infection path of Internet users' terminals by malicious code is like Fig. 1. First, a bot master hacks or update a server or web site of programs people use. Then, when the user performs the update while connected to that website or run a program, malicious code is installed on the user's system. Afterwards Bot agent that has been installed on user's system is connected to the C&C server of the bot master, the bot master gains control over the system. Therefore, the master robot may perform various malignant behaviors like attack of vulnerability through executing order to system which it gained control over. Malware detection technology is developed and information on the detected malware is distributed [2] but it can protect a system not infected with malware but hardly protect a system infected with malware from malicious order from bot master. To this end, a way of blocking connection to C&C server was used by utilizing the fact that C&C server usually runs in a form of IP

* Jong-Bae Kim is the corresponding author.

ISSN: 1738-9976 IJSIA

[3]. However, currently C&C servers are operated in form of the domain in order to avoid server blocking, TTL value of DNS is designated shorter, changing continuously IP of name server in order to avoid blocking of URL and IP by security equipment. Therefore, in order to prevent spread of damage by contagion of malicious code, a technique is required that can prevent malicious act which could occur later by blocking connection to C&C servers.

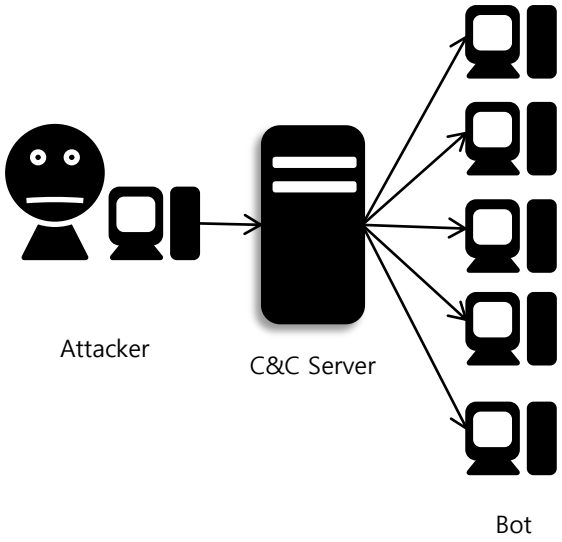

Figure 1. Architecture of Botnet

2. Related Works

As existing research on the bot detection, there is a study on method to treat malicious bots using DHCP like Figure 2. [4]. In this study, we propose a method that DHCP server provides the computers without malicious bot therapeutic vaccine with IP addresses in limited quantity

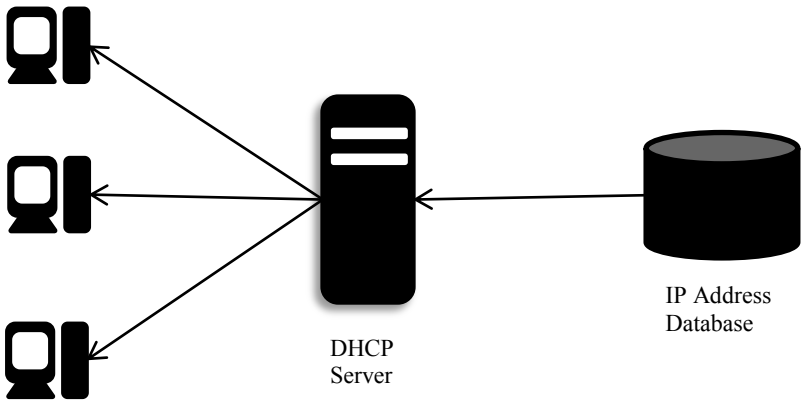

Figure 2. DHCP Service

The study on the game bot detection method using a behavior pattern model [5] suggests game bot detection method where manipulation or avoidance by game bot user is difficult by comparing human behavior with bots in a respective server. The study suggests how to detect game bot by defining the model of behavior pattern

difference and using naive Bayesian classifier. As a study about malicious process control, there is a security framework [6] for improving performance of the malicious process control system. The proposed security framework can decrease cost of constructing control server by using virtual machine and can increase the probability of internet worm attack detection of type of partly attack by using extra unused IP addresses dynamically for detecting internet worm attack. There is also a study [7] on the malignant process control system to protect the server from internet worm attacks. The proposed system consists of the control server which drives service programs same as the protected server and detects multicasting attack from internet worm. Proposed system can respond effectively to the new internet worm since it does not use detection rule and when integrated with existing security systems, the security can be further enhanced.

3. Detection of Malicious Process

Detection process for malicious process is conducted like in Figure. 3. Through detecting and transferring of executable file by process monitoring, which conducts malicious behavior and analyzing terminal device that performs update of related information and detected process executable file, information is transferred by security control server which determines blocking like Figure. 4.

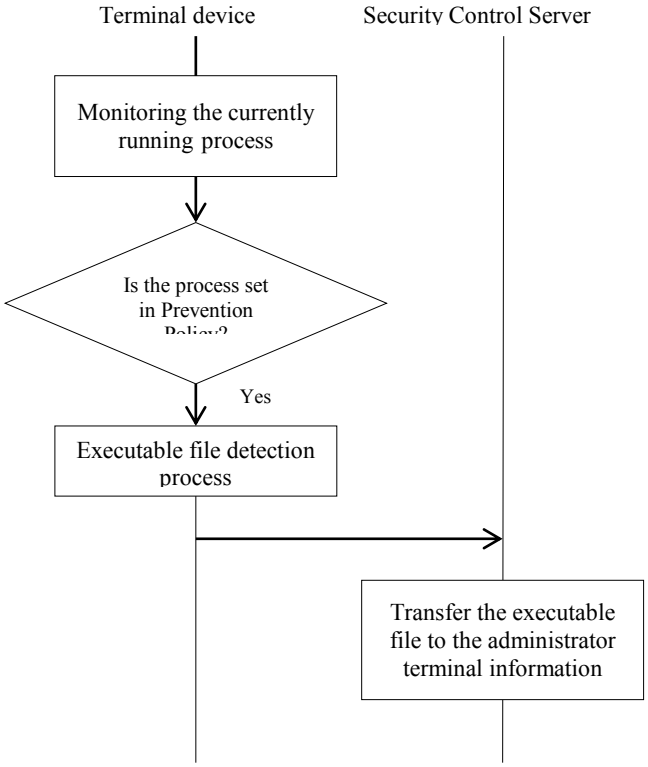

Figure 3. Detection Process of Malicious Program

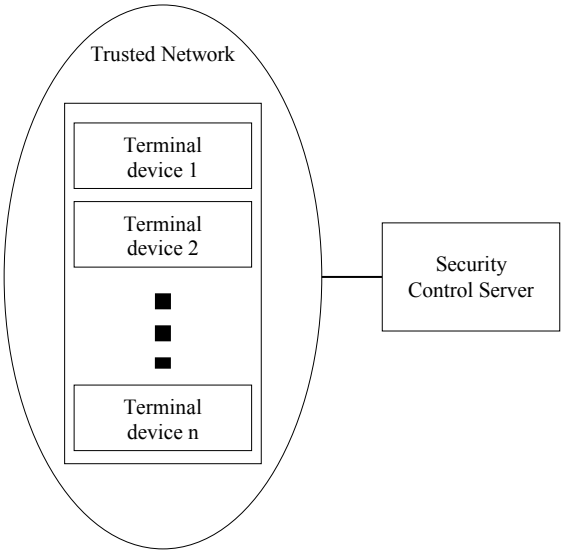

Figure 4. Architecture of Terminal Device and Security Control Server

3.1. System Terminal Device

Detection process for malicious process is performed via the terminal device. The terminal apparatus is composed of 5 components of communication, input, output, and storage and security agent like Figure 5.

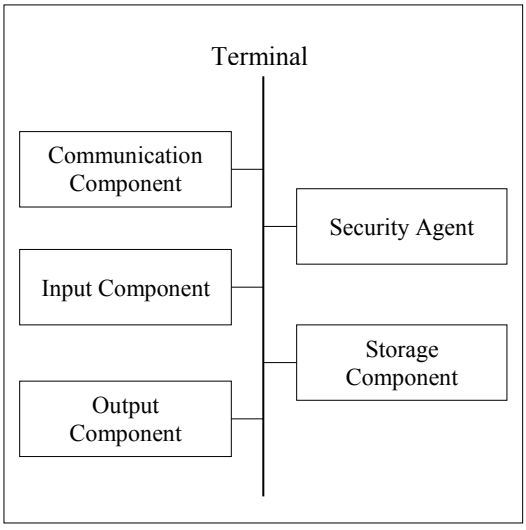

Figure 5. Components inside a Terminal

Communication Component performs a communication with the security management server through a communication network. Wire/Wireless communication module like mobile communication, satellite communication, wireless communication module and Internet and short-range wireless communication module like WiFi(Wireless Fidelity) also performs a communication function as components of it. Input module of input / output component (I/O Component) is a means for inputting a user's request for operation control of

the terminal device. When the user makes an operation to control, it serves to convert the request received in operation to an electrical signal and displays the screen information according to the application driven. In general, it is composed of a small flat panel display devices such as LCD (Liquid Crystal Display) and OLED (Organic Light Emitting Diodes). Storage Component keeps a program necessary to control operation of terminal device, data and block policy produced when the program is executed. Policy contains not only malicious codes but also information of a malicious domain as well as domain and the IP address of a malicious server, hacked servers, malware download server and C&C server and abnormal process list.

Security Agent determines whether the process currently executed belongs to Block policy. By monitoring the traffic from the terminal device and comparing it with a predefined threshold value, it detects traffic generated abnormally excessive. After detection, it examines the IP address of its destination associated with the abnormal traffic and decides whether the IP matches the IP on the list of offenders. If the IP is included in the list of IP blocks, the security agent decides if it is the process set in block policy and restricts access of the IP. It also picks up DNS query traffic and compares inner query name with domain list for blocking. Through this process it determines whether the block should be blocked.

3.2. Security Management Server

Security Management Server consists of block policy database, block policy creation components and monitoring components like Figure 6.

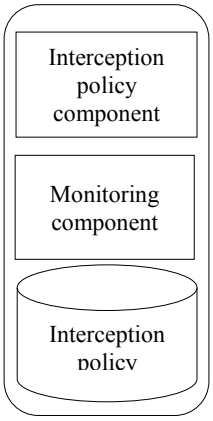

Figure 6. Inside of Security Control Server

Protection policy generating component obtains file based on URL information received from the terminal device and performs inspection of the file for the infection. Malware inspection by blocking policy component is performed by detecting malicious code or malicious domains obtained from a file. And after this, the test result is transmitted to the terminal device and at this time, malware infection test results includes the identification information of the file identified as malware, the distribution URL of a file and information of malicious domain.

Monitoring component receives executable file information from the terminal device and transmits received executable file information to terminal of controller by monitoring consistently multiple terminal devices connected through a network.

Here, the executable file includes information such as processor of the malicious behavior, program, installed folder, a header, a hash value, a source IP, and a destination IP.

In addition, by performing malware scan by running the executable file in the virtual environment by considering it to be a new process of no history of malicious code examination in case process which completed examination of malicious code doesn't exist in block policy data base, corresponding process can be updated in block policy data base.

The blocking policy database contains the block policy. Block policy means information about malicious domain which tries to connect to malicious code and it contains information like domain and IP address of C&C server.

3.3. Terminal Device of Controller

Terminal device of controller is implemented in the screen like Figure 7, below.

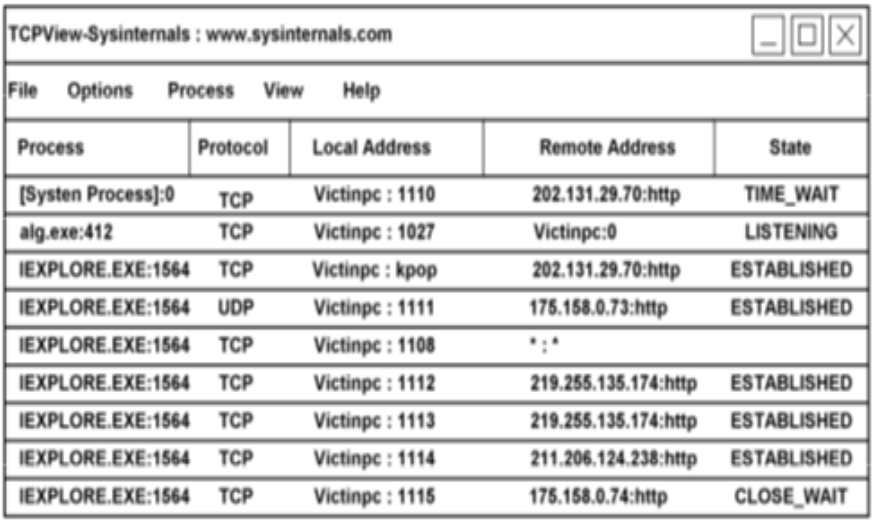

Figure 7. Screen of Controller's Terminal Device

The screen displays processes, protocols, local address, remote address and connection status. Here the process means process running currently and protocol does protocol being used currently and local address does IP address or host name of local terminal device.

Remote address shows IP address or host name and port number of the remote terminal. Connection Status indicator shows connection termination idle status, connection termination status, receiving status for connection request, transmitting status for connection request, connection to socket termination status, connection termination transmitting idle status to remote place, connection transmitting idle status to remote place with open port, final confirmation idle status after connection termination, idle status to secure receiving from remote place after connection termination and connection list index(green: normal connection, red: disconnected or terminated, yellow: connection changed).

4. Conclusions

This study suggests a system model that detects malicious code in process of inner system and blocks it as well as prevents infection of malicious code by installing security agent. Suggested system model consists of a terminal device and security control device. Information about process is transferred to security control server through a terminal

device. Information transferred to security control server should go through malicious code detection process by inner policy. Through it, a process that penetrates into system and conduct malicious conduct is blocked. The above system model can maintain security by trying to detect penetrating malicious codes different from existing method that prevents invasion of malicious codes.

References

[1] Y-C Choung, Y-G Bae. "Study on Security Measures of e-Gov with Dynamic ICT Ecosystem" JKIICE, vol. 18, no. 6, **(2014)** Jun., pp.1249-1254.
[2] K-y Cho, D-i Jang, M-S Kim, H-C Jeong, B-N Noh. "Botnet Detection Technique using Traffic Profiling Method" JAITC, volume 9, **(2011)**, pp.83 – 93.
[3] Gu, G, J. Zhang,., & W. Lee,. "Botnet Detection Technique using Traffic Profiling Method" NDSS, **2008**
[4] H-Y Kim . "A Malicious Bot Curing Technique Using DHCP" JKSCI .2012, vol. 17, no. 6, pp. 111 – 115.
[5] S-h Park, H-W Jung, T. Yoon, J-H Lee."Behavior Pattern Modeling based Game Bot detection" ETRI ,vol. 35, no 6, pp.1058 – 1067.
[6] I-S Kim, J-m Choi "Security Framework for Improving the Performance of the Malicious Process Control System" JKSII **(2013)** pp.61-71
[7] I-S Kim "A Malicious Process Control System for Protecting Servers from Internet Worm Attacks" KICS, **2010**, pp.431-439.

Authors

Seong-Muk Choi, he received bachelor's degree in Computer Information Engineering in Cheongju University, Cheongju (2001). He received his master's degree in e-Business (Master of Business Administration) in Konkuk University, Seoul (2007). He is studying his doctor's degree of IT Policy & Management in Soongsil University, Seoul. His current research interests include Open Source Software and Security.

Yeol-Joo Ryou, he received his bachelor's degree in Physics in Chosun University (1993). His current research interests include 3D Golf Trajectory and Open Source Software Security.

Hoo-Ki Lee, he received master's degree in Information Security Engineering in Dongguk University (2008). He is studying his doctor's degree in IT Policy & Management in Soongsil University, Seoul. His research interests focus on Cyber Security information sharing and analysis.

Hee-Hoon Cho, he received his bachelor's degree in Computer Science in Korea Polytechnic University (2015). He is studying his master's degree in Software Engineering at the Graduate School ofSoftware, Soongsil University, Seoul. His current research interests include Open Source Software and Security.

Jong-Bae Kim, he received his bachelor's degree in Business Administration in University of Seoul, Seoul (1995) and master's degree (2002), doctor’s degree in Computer Science in Soongsil University, Seoul (2006). Now he is a professor at the Graduate School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.