別紙様式８

研　究　主　論　文　抄　録

論文題目　Development and Evaluation of a Comprehensible DNS Query Traffic based Statistical Bot Detection System and a Portable Security Appliance
（DNS クエリトラフィック統計型ボット検知システムおよび携帯型セキュリティ装置の開発および評価研究）

熊本大学大学院自然科学研究科　情報電気電子工学　専攻　　先端情報通信工学　講座
（　主任指導　　杉谷賢一　　教授　）

論文提出者　　ルデニャ　ロマニャ　デニス　アルトゥロ
(by　　LUDEÑA ROMAÑA, Dennis Arturo　　)

主論文要旨

The thesis describes the development and/or evaluation for the detection technologies of the bots like the computer virus infected- and remote controled-PC terminals and/or servers. Currently, it is very clear and we cannot find any other instance that suggest a new detection technology of the IP addresses of the bots by obseving the entory value changes of the source IP addresses and the query keywords in the DNS query packet traffic logs which are simultaneously generated by carrying out the cyber attack. Also, I suggested and evaluated three models: a random attack model, a targted attack model, and a host search attack model by observing the chage patterns of the both entropy values.

The thesis consists of 10 chapters.

In the chapter 1, I described threats of bots and their countermesure technologies, and the related works.

In the chapter 2, I described backgrounds, threats of the bots and the bots clustered network.

In the chapter 3, I described an intrusion detection system (IDS) and necessity of singnature independent IDS.

In the chapter 4, I discussed in general on a data regression analysis method or a data statistical analysis method.

In the chapter 5, I carried out statisical analysis with concentrating the source IP address and the query keyword in the DNS query packet log.

In the chapter 6, I carried out regression analysis on the query keywords in the DNS

query packet traffic log in which the traffic exceeded the threholds. As a result, I showed not only an important insight to detect the source IP addresses of the spam bots sending a lot of unsolicited e-mails but also showed a possibility for detecting the source IP addresses of the spam bots in the organization/campus networks by observing the change patterns in the source IP addresses- and the query keywords-based entropy values.

In the chapter 7, I suggested three models: a random attack (RA) model, a targeted attack (TA) model, and a host search (HS) attack model in the source IP address- and the query keyword-based entropy values of the DNS query packet traffic logs. In order to evaluate the attack models, I also carried out entropy analysis on the source IP addresses and the query keywords in the DNS query packet traffic logs through January 1st to December 31st, 2008. Consequently, I found that in the DNS traffic from the campus network, the TA bots were only observed, however, from the Internet, the RA, TA and HS attack bots were observed.

In the chapter 8, I found and reported that the both source IP address- and query keyword-based entropy values change symmetrically in the DNS query packet traffic based on the RA model like an outbound random spam bot attack, while in the DNS query packet traffic based on an outbound SSH dictionary attack, the both enropy values change unsymmetrically. Furthermore, I showed that the difference could be interpreted in terms of the difference between the numbers of the SSH servers and the E-mail servers on the Internet.

In the chapter 9, I developed a DNS query packet traffic observation based bot detection system appliance employing the both changes in the source IP address- and query keyword-based entropy values and has carried out a trial run in the examination environment LAN configured by the broadband router. Therefore, I described that the system could be useful and efficient for field survey of the ICT security when having to take into consideration the privacy.

In the chapter 10, I finally concluded and summarized the obtained results in the thesis.