財團法人台灣網路資訊中心因公出國人員報告書

101 年 7 月 23 日

報告人 姓　名	顧靜恆	服務單位及職稱	網址組經理
出國期間	101 年 7 月 14-19 日	出國地點	希臘科斯
出國事由	參加 2012 16th WSEAS International Conference on Computers 研討會		
報告書內容應包含： 一、出國目的 二、考察、訪問過程 三、考察、訪問心得 四、建議意見 五、其他相關事項或資料 （內容超出一頁時，可由下頁寫起）			
授權聲明欄	本出國報告書同意貴中心有權重製發行供相關研發目的之公開利用。 授權人：　　（簽章）		

附一、請以「A4」大小紙張，橫式編排。出國人員有數人者，依會議類別或考察項目，彙整提出報告。
註二、請於授權聲明欄簽章，授權本中心重製發行公開利用。

一、出國目的

WSEAS(World Scientific and Engineering Academy and Society)成立於 1996 年，為世界科學與工程學會與協會，是一個國際性組織，目的是促進新的數學方法和計算技術的發展，特別是在一般和工程科學的應用上。此外，WSEAS 出版物具有廣泛的認同與主要的科學指標。

此次 2012 16th WSEAS International Conference on Computers 研討會於 2012 年 7 月 15 日至 17 日假希臘科斯舉辦，參加此次研討會主要為投稿的兩篇論文進行發表，題目分別為 A Study of the Service-based IPv6 Readiness Model for Government Agencies 及 Building an Anti-Botnet Platform to Mitigate Botnet，並與各國專家學者進行經驗學習交流。

二、考察、訪問過程

此次研討會安排了許多場次的專題演講，並將通過審查接受的論文安排在下午場次中發表，7 月 15 日至 7 月 17 日研討會議程中，安排的專題演講如下：

Keynote Lecture 1:

Energy, Environment and Importance of Power Electronics
by Prof. Bimal K. Bose, The University of Tennessee, USA.

Keynote Lecture 2:

Current Video Coding Standards: H.264/AVC, Dirac, AVS China and VC-1
by Prof. K. R. Rao, University of Texas at Arlington, USA
and Dr. Do Nyeon Kim, Barun Technologies, Corp., SOUTH KOREA.

Keynote Lecture 3:

Program Analysis beyond Closed-form Expressions for Maximum Parallelization
by Dean Kleanthis Psarris, City University of New York-Brooklyn College, USA.

Keynote Lecture 4:

Folding and Unfolding Related Issues, Especially Decompositions, in Data Processing
by Prof. Metin Demiralp, Istanbul Technical University, TURKEY.

Keynote Lecture 5:

Human Control Strategies for Multi-Robot Teams
by Prof. Katia Sycara, Carnegie Mellon University, PA, USA.

Plenary Lecture 1:

Innovations in Nanotechnology and Neurotechnology for Human Enhancement
by Prof. Jeanann Boyce, Computer Science at Montgomery College, USA.

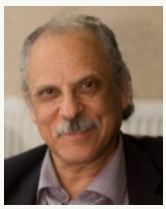
Plenary Lecture 2:

Fast Information Retrieval for Textual and Geometrical Applications
by Prof. Vaclav Skala, University of West Bohemia & VSB-Technical University of Ostrava, CZECH REPUBLIC.

Plenary Lecture 3:

Knowledge creation capacity in designing new products for industry as extension of constructing university theoretical knowledge
by by Prof. Les Mark Sztandera, Philadelphia University, USA.

Plenary Lecture 4:



Machine Learning in Biomedical Informatics
by Prof. Abdel-Badeeh M. Salem, Ain Shams University, EGYPT.

Plenary Lecture 5:

Digital Music Libraries: From Deregulation to Reconstruction
by Assis. Prof. Dionysios Politis, Aristotle University of Thessaloniki, GREECE.

Plenary Lecture 6:

Multimedia Application – Effective Support of Education
by Prof. Eva Milková, University of Hradec Králové, CZECH REPUBLIC.

Plenary Lecture 7:

Towards Petaflop Computing – An example application on Jet Noise Simulation
by Prof. Anastasios Lyrintzis, Embry-Riddle Aeronautical University, USA.

Plenary Lecture 8:

Design and implementation of river's sectors clustering models
by Prof. Dana Simian, University "Lucian Blaga" of Sibiu, ROMANIA.

Plenary Lecture 9:

On the Inversion of Adjacent Tridiagonal and Pentadiagonal Matrices
by Prof. N. A. Baykara, Marmara University, TURKEY.

Plenary Lecture 10:

Simulation of Multiphase Porous Media Flows on High-Performance Hybrid Computing Systems
by Prof. Boris Chetverushkin, Russian Academy of Sciences, RUSSIA.

Plenary Lecture 11:

Image Processing in Biometrics and Forensic Science
by Prof. Ryszard S. Choraś, University of Technology and Life Sciences, POLAND.

7 月 15 日論文發表議程如下：

Sunday July 15th 2012

Conference Room: Aegle B
Time: 13:00-15:30
COMPUTERS Session: Computational Techniques and Algorithms
Chair: Anastasios S. Lyrintzis, Cheng-Hung Huang

The Use of Petaflop Computing for Jet Noise Predictions	Chandra S. Martha, Yingchong Situ, Nitin Dhamankar, Anastasios S. Lyrintzis, Gregory A. Blaisdell, Zhiyuan Li	68104-226
Estimation of the Acid and Salt Diffusivities for Polymer Solution Using Inverse Algorithm in A Wet Spinning Process	Cheng-Hung Huang, Ming-Yuan Lee, Hsi-Mei Chen	68104-004
Fluctuation Free Differentiation via Circular Contour Integration	Ercan Gurvit, N. A. Baykara, Metin Demiralp	68104-133
Modeling of MMI Control System with Three Operators	George I. Popov, Maria P. Hristova, Rumen Trifonov	68104-235
Theory of Modeling and Simulation in Practice of Computer Modeling and Design	Josef Sedivy, Stepan Hubalovsky, Jan Chromy, Karel Dvorak	68104-223
Mining Frequent Strong Common Families in Weighted Leaf-Labeled Trees	Kyung Mi Lee, Keon Myung Lee	68104-211
A Computational Study of a Prebiotic Synthesis of L-Arginine	N. Aylward	68104-124
A Computational Study of a Prebiotic Synthesis of L-Lysine	N. Aylward	68104-127
An Efficient Hash-based Association Rule Mining Approach for Document Clustering	Noha Negm, Passent Elkafrawy, Abd-Elbadeeh Salem	68104-166

Sunday July 15th 2012

Conference Room: Melambus
Time: 16:00-18:30
COMPUTERS Session: Software Engineering
Chair: Agostino Poggi, Agni Dika

ASiDE - A Software Framework for Complex and Distributed Systems	Agostino Poggi	68104-139
Conversion of Numbers to Text and to Speech in Albanian	Avni Rexhepi, Agni Dika, Adnan Maxhuni	68104-217
Software Reliability Compliance Model for Requirements Faults	Chandasekaran Subramaniam, Kanchana Natarajan	68104-130
Development of Algorithmic Thinking and Imagination: Base of Programming Skills	Eva Milková	68104-136
Optimized Source Code Generation from State Charts	Michal Bližňák, Tomáš Dulík, Roman Jašek, Pavel Varacha	68104-007
Signature Verification Based on Fractal Coding Scheme	Nadia M. G. Al-Saidi	68104-055
User Friendly Querying of Weakly Structured Data	Pavel Kácha	68104-112
Achievements of Interoperability between Governmental Information Systems	Tasho Tashev	68104-187

7 月 16 日論文發表議程如下：

Monday July 16th 2012

Conference Room: Melambus
Time: 16:00-18:00
COMPUTERS Session: Information Science and Applications I
Chair: Dionysios Politis, Hamid Abachi

Music Libraries: The Legitimate and Ethical Battlefield of Music Distribution	Dionysios Politis	68104-082
An Integrated Music Chromaticism Model	Dionysios Politis, Dimitrios Margounakis	68104-046
Analysis of NetworkMetrics of Master-Slave Multi-Super-Hypercube X-Tree Architecture	Hamid Abachi	68104-049
Ethical Paradigms in Biomechanical Innovations in Nanotechnology and Neurotechnology: Analyzing the Impact of Computer Technology on Tissue Engineering and Human Enhancement	J. S. Boyce	68104-202
Human Control Strategies for Multi-Robot Teams	Katia Sycara, Michael Lewis	68104-022
Compatibility Issues for the Constructive Impositions in High Dimensional Model Representation Based Data Decomposition	Metin Demiralp	68104-151

Monday July 16th 2012

Conference Room: Melambus
Time: 18:00-20:00
COMPUTERS Session: Information Science and Applications II
Chair: Petra Poulova, Erkan Ulker

A Two Factor Biometric Framework for User Authentication	Monica Carfagni, Matteo Nunziati, Matteo Palai	68104-058
The System of User Roles and Modelling of Access Privileges	Monika Simkova, Petra Poulova	68104-169
CESNET CSU System	Pavel Vachek	68104-148
Database System within the Computer Science Education	Petra Poulová, Ivana Šimonová, Monika Šimková	68104-121
Knot Estimation of the B-Spline Curve with Strength Pareto Evolutionary Algorithm 2 (SPEA2)	Saban Gülcü, Erkan Ülker	68104-118
Duality and Robust Computation	Vaclav Skala	68104-037

Conference Room: Aegle A
Time: 18:00-20:00
COMPUTERS Session: Image, Sound and Signal Processing I
Chair: Ales Prochazka, Anastasia Rita Widiarti

Biomedical Image Enhancement, Segmentation and Classification UsingWavelet Transform	A. Prochazka, J. Mares, M. Yadollahi, O. Vysata	68104-031
Widiarti-Winarko Algorithm for Grouping Syllables Result from the Javanese Literature Document Image Recognition	Anastasia Rita Widiarti, Edi Winarko	68104-097
Bit Error Probability Analysis of Cooperative Relay Selection OFDM Systems Based on SNR Estimation	B. Rama Devi, K. Kishan Rao, M.Asha Rani	68104-196
A Hybrid Case-Based and Content-Based Retrieval Engine for Mobile Cancer Management System - MCMS	Bassant Mohamed ElBagoury, Mohamed Roushdy, Abdel-Badeeh M.Salem	68104-085
Feature Matching in Off-Line Signature Verification	Bence Kovari, Hassan Charaf	68104-232
Computer-Aided Image Processing Method for Yarn Hairiness Evaluation	Rocco Furferi, Matteo Nunziati, Lapo Governi, Yary Volpe	68104-061

7 月 17 日論文發表議程如下：

Tuesday July 17th 2012

Conference Room: Aegle B
Time: 12:30-14:30
COMPUTERS Session: Image, Sound and Signal Processing II
Chair: Eréndira Rendón, Martin Nemec

Method to Classify Colposcopic Images	Eréndira Rendón, Adriana Díaz, Itzel Abundez, Eduardo Gasca	68104-178
3D Modeling Using Stereo Projection	Tomas Popek, Martin Nemec, Michal Krumnikl, Radoslav Fasuga	68104-028
A Unified Approach for Textual and Geometrical Information Retrieval	Vaclav Skala	68104-016
Holography, Stereoscopy and Blender 3D	Vaclav Skala	68104-040
Object Segmentation and Tracking in Image Sequences Based on the 3D Relative Potential Field	Xiaodong Zhuang, N. E. Mastorakis	68104-175

Conference Room: Akeso
Time: 12:30-14:30
COMPUTERS Session: Internet Applications I
Chair: Abdel-Badeeh Salem, Maria Mach-Król

Web-Based Ontology of Knowledge Engineering	Abdel-Badeeh M. Salem, Hisham S, Katoua	68104-091
Intelligent Methodologies for Medical Knowledge Management	Abdel-Badeeh M. Salem, Maria Mach-Król	68104-052
Reflection on the Development of eLearning in the Czech Republic	Blanka Frydrychová Klímová, Petra Poulová	68104-199
Web Sources in Academic Setting Comparative Study	Černá Miloslava, Poulová Petra	68104-109
Towards an Adaptation for the Web of Our Authoring Tool	Imane Ryane, Moncef Bentaleb, Mohammed Khalidi Idrissi, Samir Bennani	68104-070
Client/Server Implementation of an ATL Model Checker Using Web Services	Laura Florentina Stoica, Florin Stoica, Dana Simian	68104-142
Malicious Behavior in Voice over IP Infrastructure	Miroslav Voznak, Jakub Safarik, Lukas Macura, Filip Rezac	68104-043
Modular SIP Server on Embedded Platform	Miroslav Voznak, Lukas Macura, Jiri Slachta	68104-094

Tuesday July 17th 2012

Coffee Break: 14:30-15:00

Conference Room: Aegle A
Time: 15:00-17:30
COMPUTERS Session: Internet Applications II
Chair: Rumen Trifonov, Ching-Heng Ku

Ontology-Based Learning Environment in Distance Education Systems	Amin Daneshmand Malayeri, Nikos E. Mastorakis	68104-106
Framework for Personalized e-Learning Model	Maija Sedleniece, Sarma Cakula	68104-220
Mapping Tool for Networks Using OSPF and LLTD Protocols	Pavel Kriz, Filip Maly	68104-115
Web Content Management of the e-Government Sites	Roumen Trifonov, Georgi Popov, Valeri Mladenov	68104-190
A Study of the Service-based IPv6 Readiness Model for Government Agencies	Shian-Shyong Tseng, Ai-Chin Lu, Ching-Heng Ku, Chi-Ming Chu, Geng-Da Tsai	68104-172
Building an Anti-Botnet Platform to Mitigate Botnet	Shian-Shyong Tseng, Ai-Chin Lu, Nai-Wen Hsu, Geng-Da Tsai, Ching-Heng Ku	68104-181
Monitoring Environmental Changes and Medical Risks Using Distributed Mobile Applications	Sveatoslav Vizitiu, Lazar Sidor, Lupou Marius Gavril, Buta Ioan Bogdan	68104-184
Components of the Virtual Internet Classroom Model for Distance Learning of Information Content	Željko Marčićević, Radovan Tomić, Dragica Tomić	68104-064

Conference Room: Aegle B
Time: 15:00-17:00
COMPUTERS Special Session: Internet Computing and Security
Chair: Antoanela Naaji

Security Solution for False Antivirus Detection	Catalin Pop, Marius Popescu, Antoanela Naaji	68104-076
Preprocessing Using Structuring Element for Handwriting and Hand Printed Document Analysis	Dan L. Lacrăma, Florentina Anica Pintea, Florin Alexa	68104-100
About Recommender-Like Systems Using Co-Clustering Criteria	Klaus Bruno Schebesch	68104-103
Rest Web Services in Java Using WS-Wrapper	Ploscar Adina	68104-079
Using Forensic Techniques for Internet Activity Reconstruction	Zsolt Nagy	68104-088
AJAX-Based Data Collection Method for Recommender Systems	Zsolt Nagy	68104-214

三、考察、訪問心得

本次會議中投稿了兩篇論文，並且被審核通過，安排在 7 月 17 日下午 Internet Applications 的場次中發表。 這兩篇論文，一篇是由曾憲雄董事長、呂愛琴副執行長、顧靜恆經理、朱志明組長、蔡更達工程師，共同撰寫的 A Study of the Service-based IPv6 Readiness Model for Government Agencies 論文；另一篇是由曾憲雄董事長、呂愛琴副執行長、許乃文組長、蔡更達工程師及顧靜恆經理，共同撰寫的 Building an Anti-Botnet Platform to Mitigate Botnet 論文。 每一篇論文報告時間為 20 分鐘，並且接受大家的提問。

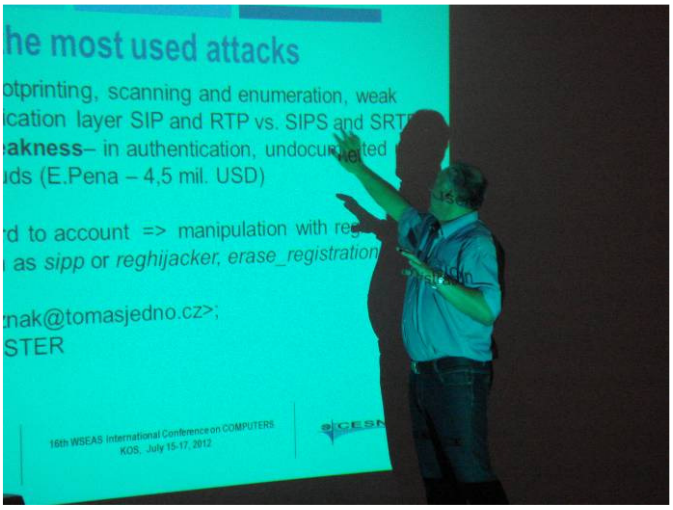
此次會議由顧靜恆經理代表出席發表這兩篇論文，並進行簡報(見圖一和圖二)。 論文全文請詳見附件一和附件二。

圖一、
顧靜恆經理發表 A Study of the Service-based IPv6 Readiness Model for Government Agencies 論文

圖二、
顧靜恆經理發表 Building an Anti-Botnet Platform to Mitigate Botnet 論文

此次研討會中，Internet 相關的論文投稿踴躍，在 Internet Applications 方面就佔了兩個場次，共有 16 篇論文發表，許多發表文章在介紹 WEB 的相關應用成果以及 Web 為基礎的內容管理等(見圖三)。另外在網路安全方面，也有多篇論文發表，如 Antivirus detection 等。(見圖四)

圖三、
Abdel-Badeeh M. Salem 發表 Web-Based Ontology of Knowledge Engineering 論文



圖二、
Miroslav Voznak 發表 Malicious Behavior in Voice over IP Infrastructure 論文

四、建議事項

(一) 網際網路的應用越來越廣泛，各國教授及研究人員的論文成果值得多加觀摩交流與學習。

(二) 此次研討會有許多歐洲國家的教授參與，借由此研討會可以與歐洲的研究成果取得互相交流的機會，也可以思考互相合作互補的創新研究主題和方式，對於台灣與歐洲國家建立更多相互合作的機會能有更多實質的幫助。

(三) 此次研討會除了電腦領域之外，同時也有其他領域的研討會同時舉行，例如通信、電路、能源、環境、系統整合、水資源、地質和地震、醫學生理學等等，對於跨領域的資訊科技的應用，以及利用網路來進行資訊傳輸與管理等方面，可以有機會進行相互的交流，以激發更多可能的創新應用。

附件一：

A Study of the Service-based IPv6 Readiness Model for Government Agencies

SHIAN-SHYONG TSENG[1, 2], AI-CHIN LU[2],
CHING-HENG KU[2], CHI-MING CHU[2], GENG-DA TSAI[2]
[1] Dept. of Applied Informatics and Multimedia, Asia University
[2] Taiwan Network Information Center
TAIWAN
{sstseng, aclu, chku, cmchu, dar}@twnic.net.tw

Abstract: - While confronting the global IPv4 address exhaustion, it is important and crucial for the entire Internet environment to smoothly upgrade to the next generation Internet Protocol, IPv6. In the strategy of IPv6 upgrade, the government network service running in the top-down manner is much easier than the commercial ISP to conduct IPv6 transition. How to handle the penetration rate of the IPv6 upgrade by the IPv6 readiness for government agencies become an interesting topic. In this study, service-based IPv6 readiness measurement criteria from the perspectives of service, software, and core network are proposed and a practical trial is proposed for the large-scale systematic survey of the IPv6 readiness for government agencies. In the data collection, we define a data format of the stocktaking survey and a collection process of this trial that is to reconfirm the effectiveness of the data format of the stocktaking survey which can successfully obtain the required data of the IPv6 readiness. Besides, the data of the IPv6 readiness measurement criteria can be easily acquired by our proposed authoring system. Finally, the mechanism has been successfully examined to obtain the IPv6 readiness for government agencies in Taiwan.

Key-Words: - serviced-based IPv6 Readiness, data collection, data analysis

1 Introduction

1.1 Background and Motivation

Network measurement [1] is a measurement activity of network characteristics. It measures the network features, including network topology, network routing, network traffic, the network anomalies, network performance bottlenecks, etc. Generally, the collected measurement information can be used to improve the network operation and management.

In order to measure different network characteristics, the so-called Network Measurement Infrastructure was proposed [2]. It used multiple measuring points in different locations on the network to obtain the measurement results from each measurement point to infer the status of network environment.

Some distributed measurement architectures have been proposed [3], where the common features of these architectures rely on a few (e.g., dozens) of distributed measurement nodes, to measure large-scale network. Besides, the different type of the distributed measurement architecture [4] based on point to point type to construct a large-scale measurement system was also proposed. In the large-scale network measurement, data acquisition can be divided into direct access to the actual data and indirect estimation of the data in order to increase measurement accuracy.

Facing the depletion of IPv4 address, how to find a feasible approach which can smoothly and steadily upgrade from the IPv4 network to IPv6 network environment is a globally concerned issue.

To solve the above issue, our idea is to firstly upgrade the government agencies from IPv4 to IPv6 due to the following reasons. First is the government network service running in the top-down manner is much easier than the commercial ISP to conduct IPv6 transition. Second is that the knowledge and experience learned from the government IPv6 transition can be used to help the industry to grasp the business opportunities of developing innovative application and services. The third is that the budget can be easily estimated based upon the existing or future equipment investment.

In this study, service-based IPv6 readiness measurement criteria are proposed and a practical trial for the large-scale systematic survey for government agencies is done according to the IPv6 readiness criteria. This mechanism is also successfully examined to obtain the IPv6 readiness for government agencies in Taiwan.

1.2 Related work

The global organization, the Internet Corporation for Assigned Names and Numbers (IANA), allocated the last five IPv4 blocks to Regional Internet Registries (RIRs) on February 3, 2011[5]. The regional organization, Asia-Pacific Network Information Center (APNIC) managing the IP address in the Asia-Pacific region announced that the IPv4 address is exhausted and will stop the normal allocation of IPv4 addresses for Asia-Pacific countries on 15 April, 2011[6].

The Network Working Group of the Global Internet Engineering Task Force, IETF, pass through the RFC 5211 in July 2008 to announce an Internet Transition Plan [7], which proposed the stage and schedule planning for the smooth transition of IPv4 networks to IPv6 network as a global reference basis for network deployment.

Until the end of April 2012, there are 184 countries/economies around the world have been allocated of the IPv6 address [8]. It means that many countries have paid attention to the development of IPv6 networks. Besides, many developed countries also give the priority to the IPv6 network upgrade in the government to promote the development of the IPv6 industry and the private enterprise.

There are some IPv6 development surveys in the world. The Internet Association Japan [9] and the European Commission [10] had started the IPv6 penetration survey to understand IPv6 development. In addition, the international IPv6 Status Survey [11] provides five measurement indicators. S. S. Tseng [12] proposed an IPv6 readiness model with seven criteria as the promotion indicators of IPv6 readiness. However, some indicators, such as ratio of the connection of the DNS and Web from the users, the IPv6 traffic of tunnel broker, the number of IPv6-enabled products, are not suitable as the IPv6 readiness criteria for the government agencies according to the properties of public network service.

Our contribution in this paper is to propose measurement criteria of the IPv6 readiness for the government agency, and the proposed criteria have been successfully examined in the systematic large-scale survey in Taiwan.

2 Architecture of the service-based IPv6 readiness

In this paper, we proposed a service-based IPv6 readiness architecture, including five measurement criteria from the perspectives of service, software, and core network, as shown in Fig. 1.

Services	• **Ratio of public network Services on the IPv6 Web, E-mail, DNS, FTP**
Software	• **Ratio of the supporting IPv6 in the Operation System** • **Ratio of the supporting IPv6 in Service Software**
Core Network	• **Ratio of the supporting IPv6 in the network equipment for the access** • **Ratio of the supporting IPv6 in the network equipment for the management**

Figure 1. Measurement Model of IPv6 Readiness with five measurement criteria

In this serviced-based IPv6 readiness architecture, the perspective of the service is of the major concern, in which the ratio of the public network service is the measurement criterion. According to the trial of the stocktaking survey, it includes four major public network services such as the IPv6 Web, Email, DNS, FTP.

In the dimension of the software, two measurement criteria, the ratio of the supporting IPv6 in the operation system and the ratio of service software of the public network service are proposed.

In the dimension of the core network, two measurement criteria, the ratio of the supporting IPv6 in the network equipment for the access and the ratio of the supporting IPv6 in the network equipment for the management of the public network service are also proposed.

3 Data Collection Process of the IPv6 Upgrade

In order to obtain the service-based IPv6 readiness for government agencies, we propose a trial of the large-scale systematic survey to collect the related data, as shown in the following:

As shown in Fig.2, the process consists of several steps, such as the pre-process of stocktaking of the public network service, the interview of government agencies, the data acquisition of government agencies, the data review of stocktaking, question acquisition and modification of the survey data format, and the confirmation of the data format for the stocktaking survey.

This goal of this trial is to reconfirm the effectiveness of data format of the stocktaking

survey which can successfully obtain the required data of the IPv6 readiness.

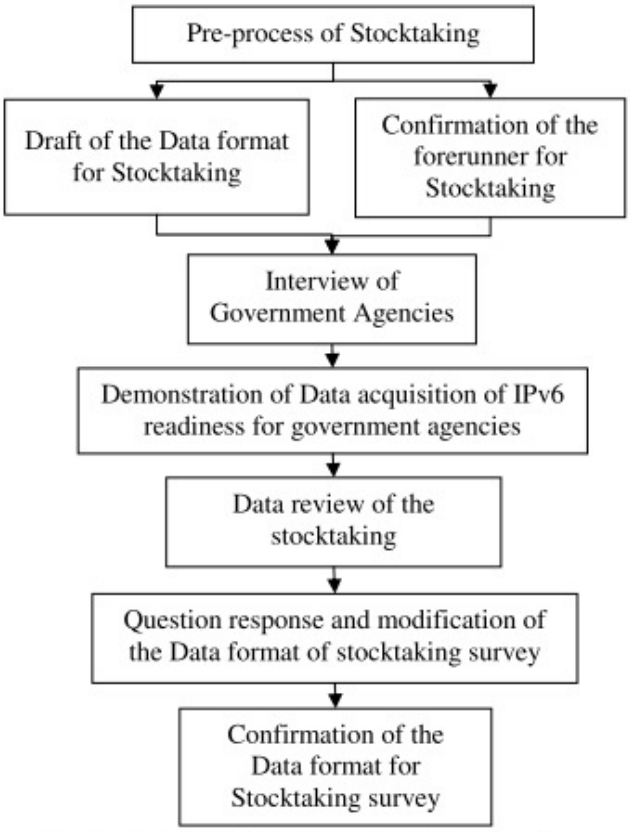


Figure 2. The workflow of the trial for the data collection to confirm the criteria data format for the stocktaking survey

The data format of the stocking survey consists of the following items:

1. The serial number of the Service
2. The categories of the service: Web, Email, DNS, FTP, others
3. The name of the service
4. The description of the service
5. The URL of the service
6. The recommended year for IPv6 upgrade of the service
7. The serial number of the software/hardware
8. The categories of the software/hardware: WWW host, WWW service software, Email host, Email service software, DNS host, DNS service software, FTP host, FTP service software, VPN host, VPN service software, Proxy host, Proxy service software, Cache host, Cache service software, Router, Layer 2 switch, Layer 3 switch, Layer 4 switch, Load Balancer, Firewall
9. The name of the software/hardware
10. The version of the operation/service software
11. The software/hardware supports IPv6: YES or NO
12. The software/hardware enable IPv6: YES or NO
13. The recommended year for IPv6 upgrade of the software/hardware
14. The upgrade method for the software/hardware

4 Statistical Analysis of the IPv6 Upgrade

Based upon the data format an authoring system [13] is then developed. From March to April 2011, there are 5,270 public network services collected from 798 Taiwan government agencies using this system.

4.1 Services

4.1.1 Ratio of public network Services on the IPv6 Web, E-mail, DNS, FTP

In the total 5,270 public network services, the distribution and the percentages of the different kind of services are shown in Table 1 and Figure 3, respectively.

The percentage and the ratio of the IPv6 enabled public network services are shown in the Table 2 and Figure 4, respectively. In our study, the IPv6 enabled service means that its software, operation system and service software, and its network environment all have been enabled in IPv6.

Table 1. The distribution of the public network services

Service Type	Numbers	Percentages
Web services	3,556	67%
Email services	609	12%
DNS services	524	10%
FTP services	40	1%
Other services	544	10%

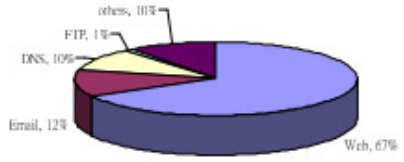


Figure 3. The ratio of major public network services

Table 2. The percentages of the IPv6-enabled public network services

Service Type	Numbers of IPv6-enabled	Percentages of IPv6-enabled
Web Services	41	1%
Email services	10	1.6%
DNS services	17	3.2%
FTP services	0	0%
Other services	14	2.1%

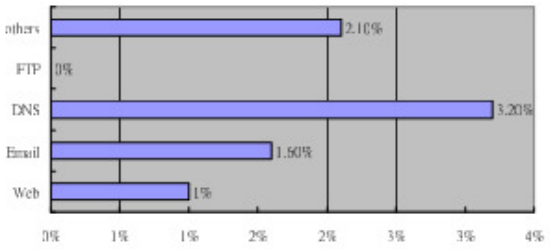


Figure 4. The ratio of IPv6 readiness for IPv6-enabled public network services

It can be easily seen that because the DNS service is the basis of all other services, the percentage in the DNS service is higher than those in other services.

According to the survey of the IPv6 Taiwan directory [14], there already have 7,769 IPv6 web sites established in Taiwan. Among them, the increment is 316 websites, around 4%, compared to those in 2011 as shown in Figure 5.

One further question is that we want to know the reason why the service that cannot enable IPv6. We have found that it is because most of the network environments are not available for IPv6; hence, how to increase the percentage of the IPv6 readiness in the network environment becomes our future work.

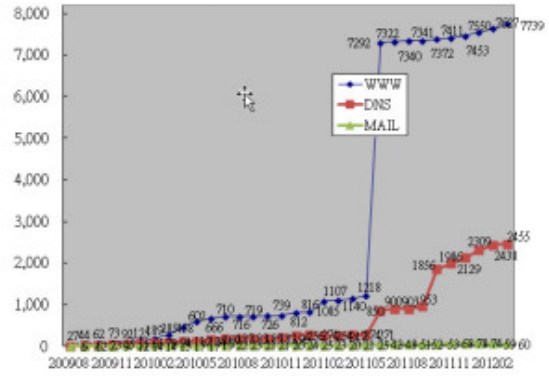


Figure 5. The number of the IPv6-enabled servers, Web, DNS, and Email, in Taiwan

4.2 Software

4.2.1 Ratio of the supporting IPv6 in the Operation System

Table 3 and Table 4 show the percentages of the IPv6-supported operation system in the public network services and the percentages of the IPv6-enabled operation system in the public network services, respectively.

Table 3. The percentages of the IPv6-supported operation system in the public network services

Host of Services	Numbers	Numbers(Percentages) of IPv6-supported
Web host	4157	3223(78%)
Email host	733	472(64%)
DNS host	632	430(68%)
FTP host	72	56(78%)
VPN host	18	4(22%)

Table 4. The percentages of the IPv6-enabled operation system in the public network services

Host of Services	Numbers	Numbers(Percentages) of IPv6-enabled in the operation system
Web host	4157	113(2.7%)
Email host	733	26(3.5%)
DNS host	632	33(5.2%)
FTP host	72	0(0%)
VPN host	18	0(0%)

4.2.2 Ratio of the supporting IPv6 in Service Software

Table 5 and Table 6 show the percentages of the IPv6-supported service software in the public network services and the percentages of the IPv6-enabled service software in the public network services, respectively.

Table 5. The percentages of the IPv6-supported service software in the public network services

Service Type	Numbers of software	Numbers(Percentages) of IPv6-supported
Web	4,022	2,814(70%)
Email	686	295(43%)
DNS	538	373(69%)
FTP	61	41(67%)
VPN	3	0(0%)

Table 6. The percentages of the IPv6-enabled service software in the public network services

Service Type	Numbers of software	Numbers(Percentages) of IPv6-enabled
Web	4,022	118(2.9%)
Email	686	29(4.2%)
DNS	538	14(2.6%)
FTP	61	0(0%)
VPN	3	0(0%)

Table 7 shows the percentages of the service software brand in the public network services which will be used to help promote the IPv6 upgrade. According to Table 5 and Table 7, we can find that

the percentage of the Email which supports IPv6 is lower than those of other services; it is because most of the email software systems are not available for IPv6.

Table 7. The percentages of the service software for major public network services

Services	Software Name	Numbers	Percentages
WEB	Windows IIS	1854	46%
	Apache	849	21%
	Tomcat	305	8%
DNS	BIND	169	50%
	Windows	171	50%
Email	Exchange	128	20%
	Sendmail	63	10%
	Mail2000	56	9%

4.3 Core Network

4.3.1 Ratio of the supporting IPv6 in the network equipment for the access

Table 8 and Table 9 show the percentages of the IPv6-supported network equipment for the public network services and the percentages of the IPv6-enabled network equipment for the public network services, respectively.

Table 8. The percentages of the IPv6-supported network equipment for the public network services

Network Equipments	Numbers	Numbers(Percentages) of IPv6-supported
Router	1,137	463(41%)
Layer 2 switch	785	359(46%)
Layer 3 switch	952	581(61%)
Layer 4 switch	175	43(25%)

Table 9. The percentages of the IPv6-enabled network equipment for the public network services

Network Equipments	Numbers	Numbers(Percentages) of IPv6-enabled
Router	1,137	67(5.9%)
Layer 2 switch	785	31(3.9%)
Layer 3 switch	952	40(4.2%)
Layer 4 switch	175	2(1.1%)

From the Table 9, we can see the percentage of the IPv6-enabled network equipment is still low.

4.3.2 Ratio of the supporting IPv6 in the network equipment for the management

Table 10 and Table 11 show the percentages of the IPv6-supported network management equipment for the public network services and the percentages of the IPv6-enabled network management equipment in the public network services, respectively.

Table 10. The percentages of the IPv6-supported network management equipment for the public network services

Network Management Equipments	Numbers	Numbers (Percentages) of IPv6-supported
Load Balancer	465	217(47%)
Firewall	1,739	1,083(62%)

Table 11. The percentages of the IPv6-enabled network management equipment for the public network services

Network Management Equipments	Numbers	Numbers (Percentages) of IPv6-enabled
Load Balancer	465	6(1.3%)
Firewall	1,739	87(5%)

We know that the network management equipment, such as the load balance and the firewall, is very critical for the network service; hence, the higher supporting from these equipment vendors becomes very important.

Besides, it is well known that the traffic of IPv6 also can reflect the growth of the network environment in IPv6. As shown in Figure. 6, the growth of the traffic of IPv6 is low in this year.

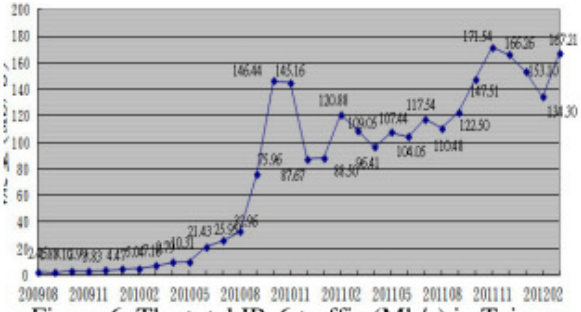


Figure 6. The total IPv6 traffic (Mb/s) in Taiwan

5 Conclusion

In this study, service-based IPv6 readiness measurement criteria from the perspectives of service, software, and core network are proposed and a practical trial is proposed for the large-scale systematic survey of the IPv6 readiness for government agencies in Taiwan.

In the data collection, we have designed a data format of the stocktaking survey and a collection

process of this trial. The data of the IPv6 readiness measurement criteria is acquired by our proposed authoring system. This mechanism is also successfully examined to obtain the IPv6 readiness for government agencies in Taiwan. In order to successfully introduce the process of the stocktaking survey, we also hold three seminars, which have 609 attendees from the government, in February 2012.

According to the collected data, we find that the highest percentage of the public network service is the Web service, but the percentage of IPv6-enabled is still low, because most of the network environments are not available for IPv6. From the data of the software dimension, the ratio of the operation system is higher than that of the service software. From the data of the core network dimension, the ratio of the IPv6-supported network is still less than 50%.

With the arrival of the IPv4 address depletion, we will continuously carry out the measurements of the IPv6 readiness and care about the overall development trend about the public network services.

Acknowledgement

This paper is partially sponsored by the Taiwan IPv6 Upgrade Promotion Program and the Interoperability and accreditation of next generation Internet project (No. MOTC-DPT-101-01) by the Ministry of Transportation and Communication of the Republic of China.

References:

[1] Caceres, R.; Duffield, N.; Feldmann, A.; Friedmann, J.D.; Greenberg, A.; Greer, R.; Johnson, T.; Kalmanek, C.R.; Krishnamurthy, B.; Lavelle,D.;Mishra, P.P.; Rexford, J.; Ramakrishnan, K.K.; True, F.D.; vanderMemle, J.E., "Measurement and Analysis of IP Network Usage and Behavior", Communications Magazine, IEEE, Volume:38, Issue:5, Pages:144-151, May 2000

[2] Wijata, Y.I.; Niehaus, D.; Frost, V.S., "A scalable agent-based network measurement infrastructure", Communications Magazine, IEEE, Volume:38, Issue:9, Pages:174-183, Sept. 2000

[3] Internet Measurement Infrastructure, Available at: http://www.caida.org/analysis/performance/measinfra

[4] Ching-Feng Li, "P2P-Based Programmable Network Measurement Infrastructure", Thesis, Nationa Tsing Hua University, 2004.

[5] IANA, "Global Policy for the Allocation of the Remaining IPv4 Address Space", 3 February 2011, http://www.icann.org/en/news/in-focus/global-addressing/remaining-ipv4

[6] APNIC, "Key Turning Point in Asia Pacific IPv4 Exhaustion", http://www.apnic.net/__data/assets/pdf_file/0018/33246/Key-Turning-Point-in-Asia-Pacific-IPv4-Exhaustion_English.pdf

[7] IETF RFC 5211: An Internet Transition Plan，http://64.170.98.42/html/rfc5211

[8] Global IPv6 address statistics，http://trace.twnic.net.tw/ipstats/statsipv6.php

[9] Measurement of IPv6 readiness, Internet Association Japan，http://v6metric.jp/en/index.html

[10] European Commission, "IPv6 Deployment Monitoring", 14 December, 2010, http://ipv6-ghent.fi-week.eu/files/2010/12/1335-Rob-Smets-v2.pdf

[11] IPv6 status survey, http://www.mrp.net/IPv6_Survey.html

[12] S. S. Tseng, A. C. Lu, C. H. Ku, and G. D.Tsai, "A Study on Measurement Model of IPv6 Readiness", Proceedings of 2010 Cross-Strait Conference on Information Science and Technology, CSCIST 2010, Yanshan University, Qinhuangdao, P.R.China, pp. 647-651, July 9-11, 2010.

[13] stocktaking management system, http://www.gsnv6.tw

[14] IPv6 Taiwan Directory, http://v6directory.twnic.net.tw

附件二：

Building an Anti-Botnet Platform to Mitigate Botnet

SHIAN-SHYONG TSENG[1,2], AI-CHIN LU[2],
NAI-WEN HSU[2], GENG-DA TSAI[2], CHING-HENG KU[2]
[1]Dept. of Applied Informatics and Multimedia, Asia University
[2]Taiwan Network Information Center
TAIWAN
{sstseng, aclu, snw, dar, chku}@twnic.net.tw

Abstract- In recent years, with the rapid growth of the Internet applications and services, botnet becomes one of the most severe threats on the Internet. Because the botnets can be automatically evolved as different localized versions in a short period of time, how to find an effective and efficient approach to detect and notify the Botnet attack becomes an important and interesting issue. To cope with the issue, we proposed a collective intelligence approach which aims to enable the systematic and dynamic creation of malware information and knowledge. Accordingly, we developed an anti-botnet platform together with a social networking structure, and an anti-botnet service web site, where the collaborative anti-botnet platform is used to collect the Botnet attack information through the Honeypot Deployment of different organizations and the proposed social networking structure can help build the consensus to select the attributes of the Botnet. The collected data can be then sent to the Anti-Virus Software Vendor to develop the antidote which can be free downloaded by the infected Internet users. Besides, an anti-botnet web site is also developed for Botnet information query, and malware prevention teaching. According to the experimental results, we show that the platform can be used to reduce the Botnet and malware attacks, and the collected information and knowledge can be used to enhance the national information and communication security.

Key-Words: - Anti-Botnet Platform, Honeypot, Botnet, collective intelligence, social networking, consensus building

1 Introduction

1.1 Background and Motivation

The development of network technology brings the convenience of the communication between people, but the issues of the information security caused by a variety of system vulnerability or weaknesses are increasing dramatically.

In all kinds of new Internet-based intrusion attack, one of the greatest damages is so-called the Botnet attacks, commonly known as "zombie network" or the "robot network". Bot attacks which often happened with the e-mail, instant messaging or the computer system vulnerabilities to hack computers are hidden in the program of the computer[1], and the infected computers with the bot invasion are connected as the botnet. The behavior of Botnet viruses is different from the original Trojans, where the original Trojans only attack a specific target, but the Botnet just like worm can slowly spread in the network space and trigger the computer attack by itself when it finds the vulnerabilities of the computer [2].

Because the botnets can be automatically evolved as different variants in a short period of time, how to find an effective and efficient approach to detect and notify the Botnet attack is our concern. In this paper, we proposed an anti-botnet platform [3] which can collaboratively collect the Botnet attack information through the Virtual Honeypot deployment of different organizations including TWCERT/CC, governmental and commercial ISPs [4]. The collected data can be then sent to the Anti-Virus Software Vendor [5] to develop the antidote which can be free downloaded by the infected Internet users, where the related ISPs help to notify the Botnet attack for the users.

1.2 Related work

According to the Symantec Global Internet Security Threat Report[6], overall in 2011, botnets produced approximately 81.2% of all spam in circulation. With the power of botnets, robot networks of computers infected with malware and under the control of cybercriminals, spammers can pump out billions of spam emails every day, clogging-up company networks and slowing down communications. There were, on average, 42 billion spam messages a day in global circulation in 2011, compared with 61.6 billion in 2010. Hence, Botnet takedowns can reduce Spam volumes. For example,

the overall number of spam fell consider-ably in the year from 88.5% of all email in 2010 to 75.1% in 2011. This was largely thanks to law enforcement action which shut down Rustock, a massive, worldwide botnet that was responsible for sending out large amounts of spam. On March 2012, Microsoft and US law enforcements took down the Rustock botnet. Besides, FBI awarded court order to shut down the Coreflood botnet by sending a "delete" command (included in the threats design) to compromised computers on April 2012.

As to the Botnet attack detection and prevention, the Japanese Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy,Trade and Industry (METI) launched the Cyber Clean Center plan that is implemented by the Telecom-the ISAC Japan, and JPCERT / CC and IPA, where 76 ISPs and anti-virus software industry are involved[7]. Besides, Hailong Wang[8] proposed the Role-based collaborative information collection model for Botnet detection.

In order to mitigate the Botnet efficiently and effectively, our basic idea is to standardize both the communication protocol of the collected Botnet attack information and the process of the data transmission through social networking. Accordingly, our proposed anti-Botnet platform consists of the following steps: the detection and collection of the Bot, the classification of the bot, the development of the antidote of the bot, the notification of the infected users, and the provision of the downloadable antidote.

To evaluate the effectiveness and the efficiency of the anti-Botnet platform, the proposed procedure in the anti-Botnet platform has been successfully examined in Taiwan. The results show that the domestic infection proportion, which is the ratio of the infective domestic IP addresses and infective global IP addresses, is gradually reduced. It means that the platform can effectively reduce the number of Bots.

2 Social Networking Structure

2.1 Bot Collection based on the Cooperation among the Social Networking Groups

A social networking is a social structure made up of a set of actions (such as individuals or organizations). In the proposed social networking structure, as shown in Figure 1, five groups including TANet CERT, TWNCERT, NCC-CERT, TWIA, and TWCERT/CC form Taiwan Security Alliance, where TWCERT/CC plays the role of coordinator and each group may consist of several members deploying Honeypots. Through the cooperation among all the members, the mission of the Bot collection in our anti-Botnet platform can be easily achieved.

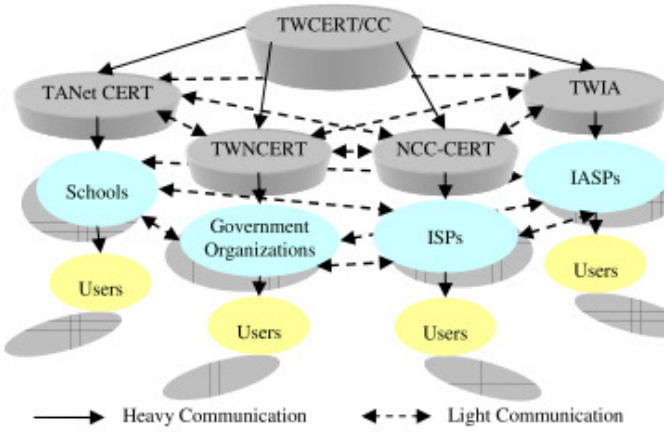


Figure 1. The Groups of Social Networking Structure

2.2 Consensus Building of the attributes of the Botnet

To collect Botnet attack information efficiently, our idea is to standardize the communication protocol of the collected Botnet attack information collaboratively. During the consensus building process of the selection of the attributes of the data schema for the malware information, the privacy issue is most concerned for different groups in our social networking structure.

Besides, the attributes of the instance of the attack event are also selected by the groups. These attributes will be used to build the antidote database for user downloading.

In this study, the consensus is reached through the heavy communication and the monthly discussion by the proposed social networking structure. We finally select nine useful attributes of the Botnet from the 31 attributes in the Honeypot database as shown in the following.

Field	Data Type	Description
malware_id	integer(4)	malware sample serial number
hash_sha512	Character (128)	Hash sha512
hash_md5	Character(32)	Hash MD5
first_collection_time	timestamp with time zone	acquired time of the malware sample

malware_content	String	content of the malware sample
malware_download_site	string(512)	download site of the malware
attack events sequence	<($inet_1$,$inet_1$,timestamp$_1$), ($inet_2$,$inet_2$,…), (…)>	each attack event in the sequence includes honeypot IP, source IP address of the attack event, and time of the attack event

3 Architecture of Anti-Botnet Platform

As we know, the Virtual Honeypot is a security resource whose value lies in being probed, attacked or compromised. In this section, we are concerned with how to collect more Bot data from a variety of program data sources and how to efficiently provide the antidote.

As we know, Nepenthes, a low-interaction Honeypot, can simulate the known vulnerabilities. Therefore, when the malicious code attacks these weaknesses, the information of the malware can be automatically stored. In the process of the collection of Bot, the collaboration of the members of our social networking structure that deploy honeypots in different locations can help simultaneously collect the malware and the attack information from different organizations.

Based upon the consensus of the attributes of the Bots, we developed an anti-botnet platform to collect the Botnet attack information through the Nepenthes Honeypot Deployment of different organizations.

The Anti-Botnet platform consists of four major steps as shown in Figure 2.

Step 1: Filter the Bot instances having antidote using the Bot signature (MD5) matching method.

Step 2: Develop the antidote for the new Bot found in Step 1.

Step 3: ISPs make the user notification for the infected users.

Step 4: Provide the antidote and maintain the antidote DB.

3.1 Filtering the Bot instances having Antidote

To classify the collected malware instances into the ones having antidote and the ones not having antidote, the signature, such as the MD5 data, of the new Bot instance is compared with those of the bots having antidotes. If matched, we send the IP addresses, timestamp, antidote download URL to ISPs. The ISP will then notify the user to download the antidote. Otherwise, the sample, timestamp, and MD5 code will be sent to the anti-virus vendor for developing the antidote.

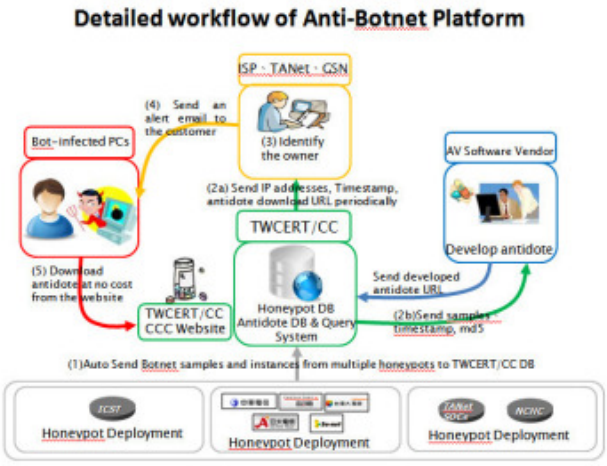


Figure 2. The workflow of the process in the Anti-Botnet Platform

3.2 Deployment of the Antidote

In the process of developing the antidote, the Anti-virus company joining our project used the sand box method to develop the antidote for the new Bot. The produced antidote is sent back to the TWCERT / CC and stored into antidote DB site for the users to download.

In the last two years, the statistics results show that the average antidote developing time is about 2 days and the detoxification rate is more than 95%.

3.3 User Notification

After receiving the notification of the information of the antidote, the ISP will notify the corresponding user to download the antidote.

In the process of the user notification, we design the automatic notification system to immediately notify ISPs, and the ISP can then efficiently notify the user within 8 hours.

4 Anti-Botnet Service Web site

With the supports of the social networking groups, an anti-botnet web site is further developed for Botnet information query, the antidote download,

and malware prevention teaching.[3] After the users downloaded the antidote and removed the Bot from the infected computer, we also provide the related knowledge of the antidote to them. Besides, the real-time information update and the on-line help are also provided in this web site.

In order to increase the users' Botnet knowledge, four kinds of learning contents are provided on the web site, such as

(1) Software Security, including the installation of anti-virus software and software upgrade,
(2) Device Security, including how to enable firewall and setup the configuration, protect against any malicious programs trying to attack via USB drive,
(3) Network Security, including using private IP address to increase the level of the security, and
(4) User Behavior Security, including must-not-visit and the untrusted URL, to avoid opening the unknown email, and change password frequently.

5 Performance Analysis of Anti-BOTNET platform

We had implemented the anti-BOTNET platform prototype to collect Bot information and produce the corresponding antidote since July 2011. At the end of 2011, this platform started to notify the relevant users to download the antidote for the removal of the malware.

In order to evaluate the performance of the anti-Botnet platform, the following analyses have been done.

5.1 Analysing the service ports of collected instances

To know how many of the infected sites are servers, we have scanned over 35,000,000 domestic IPv4 addresses to see whether a service port, such as DNS, Web and mail service of the site is on. Compared the results with the IPs of Bot instances, we can determine the infective site is a server or a client. We therefore found that 98% of the infected sites without opening the service ports are regular personal computers. This is consistent with our intuition; the security protection level of user's computer is usually lower than that of the server.

5.2 Analysis of the Infection rate of Botnet

In order to know the effectiveness of the anti-Botnet platform, we calculate the proportion of infective domestic IP addresses R_t in infective global IP addresses as follows.

$$R_t = \frac{N_t}{N_f + N_t}, \text{ where}$$

N_t : *number of Infective IP addresses in Taiwan*

N_f : *number of Infective foreign IP addresses*

Until April 2012, there are more than 15,900,000 instances are collected from 59,591 foreign sources (IP addresses) and 16,285 of them are domestic IP addresses, about 27%, as shown in Figure 3. It can be seen that the proportion of the infective domestic IP addresses is gradually reduced. It shows that our platform can effectively reduce the number of Bots.

5.3 Statistics of the antidote developing time

We analyze the time elapsed in the development of the antidote to show the efficiency of the antidote development. Besides, the download rate of the antidote is also proposed.

As to the collected 19,235 malware samples including 629 unsolved sample, the antidote production rate is 96.7%. Besides, 66.3% of the antidotes can be developed within one day.

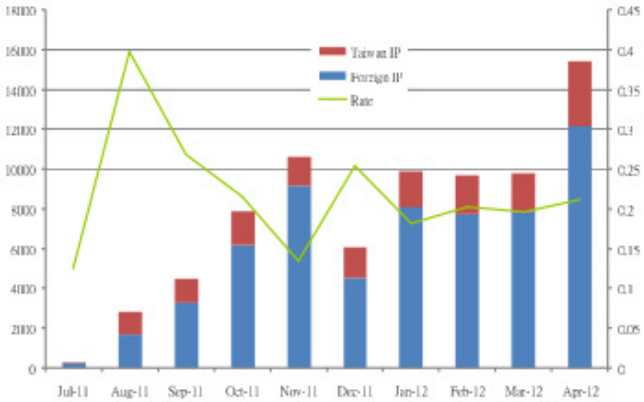


Figure 3: Source IP of instances and the proportion of the infective domestic IP addresses and infective global IP addresses.

5.4 Analysis of BOTNET malware categories

To find the development trends and the Bot behavior within the infective range for the mitigation of Bot[9][10], twelve categories of the malware including 18606 malware samples are classified as shown in Figure 4[11]. According to the statistics, we found that 86% of malwares have

been downloaded by the http protocol and 86% of them are with the execution file.

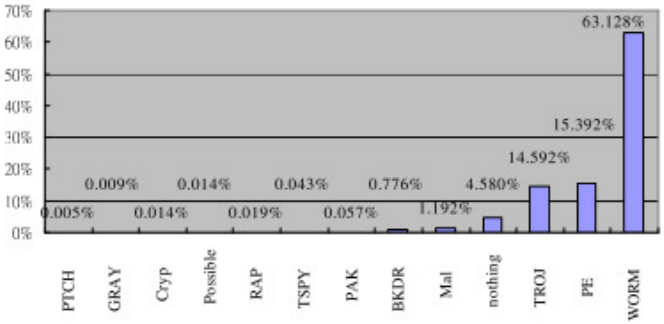


Figure 4: The proportion of the type of the collected malware

6 Conclusion

In this paper, we successfully proposed a collective intelligence approach which aims to enable a systematic and dynamic creation of malware information and knowledge.

Accordingly, we developed an anti-botnet platform together with a social networking structure, and an anti-botnet service web site, where the collaborative anti-botnet platform is used to collect the Botnet attack information through the Honeypot Deployment of different organizations.

The proposed social networking structure can successfully help build the consensus to select the attributes of the data schema of the Botnet and collaboratively collect the Bots. Besides, an anti-botnet web site is also developed for Botnet information query, and malware prevention teaching.

According to the experimental results, we show that the platform can be used to reduce the Botnet and malware attacks.

To evaluate the effectiveness and the efficiency of the anti-Botnet platform, the proposed procedure in the anti-Botnet platform has been successfully examined in Taiwan. The results show that the domestic infection proportion, which is the ratio of the infective domestic IP addresses and infective global IP addresses, is gradually reduced. It means that the platform can effectively reduce the number of Bots.

In the near future, we will continuously improve this anti-botnet platform service to mitigate the variant Bots in Taiwan.

.

Acknowledge

This paper is partially sponsored by the Taiwan Network Information Center (TWNIC) and TWCERT/CC.

References:

[1] Workshop on Understanding Botnets of Taiwan 2011 (BoT 2011), http://ntu.botnet.tw/BoT2011/

[2] Hacks In Taiwan Conference, http://hitcon.org/hit2011/

[3] Cyber Clean Center Taiwan, https://ccc.cert.org.tw/

[4] Taiwan Internet Association, http://www.twia.org.tw/

[5] Trend Micro, http://www.trendmicro.com/

[6] Symantec, "2011 Trends of Internet Security Threat Report", Volme 17, April 2012.

[7] Cyber Clean Center Japan, https://www.ccc.go.jp/

[8] Hailong Wang; Zhenghu Gong, Role-based Collaborative Information Collection Model for Botnet Detection, Collaborative Technologies and Systems (CTS), 2010 International Symposium Page: 473-480

[9] Ming-Zong Huang; Chia-Mei Chen, Hybrid Botnet Detection, http://ndltd.ncl.edu.tw/cgi-bin/gs32/gsweb.cgi?o=dnclcdr&s=id=%22098NSYS5396050%22.&searchmode=basic

[10] Tung-Ming Koo, Hung-Chang Chang, Quan-Wei Guo, 2011, Construction P2P firewall HTTP-Botnet defense mechanism, 2011 IEEE International Conference on Computer Science and Automation Engineering, 2011/06/10-12, IEEE, Shanghai, China.

[11] Virus Total, "Free Online Virus, Malware and URL Scanner", http://www.virustotal.com/