MYCERT ITP Paper **NISER-MYC-ITP-7040-2**

Comparative Analysis on Incident Statistics for Year 2003: A Comparison between MyCERT and US CERT

MyCERT Unit

Issue 1.00
7 July 2004

National ICT Security and Emergency Response Centre
c/o MIMOS Berhad Technology Park Malaysia 57000 Kuala Lumpur
Tel: +60 (0)3 8996 1901 Fax: +60 (0)3 8996 0827
http://www.niser.org.my

MYCERT ITP Paper NISER-MYC-ITP-7040-2

Comparative Analysis on Incident Statistics for Year 2003:
A Comparison between MyCERT and US CERT

MyCERT Unit

Issue 1.00
7 July 2004

National ICT Security and Emergency Response Centre
c/o MIMOS Berhad Technology Park Malaysia 57000 Kuala Lumpur
Tel: +60 (0)3 8996 1901 Fax: +60 (0)3 8996 0827
http://www.niser.org.my

[This page is intentionally left blank]

DOCUMENT AUTHORISATION

DOCUMENT TITLE: Comparative Analysis on Incident Statistics for Year 2003: A Comparison Between US CERT and MyCERT

REFERENCE: **NISER-MYC-ITP-7040-2**

ISSUE: 1.00

DATE: 7 July 2004

PREPARED BY: ____________________________ ______________

Sharifah Roziah Mohd Kassim Date
Incident Analyst
MyCERT

APPROVED BY: ____________________________ ______________

Solahuddin Shamsuddin Date
Manager of MyCERT

DISTRIBUTION: UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

COPYRIGHT AND CONFIDENTIALITY STATEMENT

The copyright of this document, which may contain proprietary information, is the property of National ICT Security and Emergency Response Centre. The document shall not be disclosed, copied, transmitted or stored in an electronic retrieval system, or published in any form, either wholly or in part without prior written consent.

The document shall be held in safe custody and treated in confidence.

Registered office: Technology Park Malaysia, 57000 Kuala Lumpur

Printed in Malaysia

TRADEMARKS

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. National ICT Security and Emergency Response Centre cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

WARNING AND DISCLAIMER

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and National ICT Security and Emergency Response Centre shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

DOCUMENT CHANGE LOG

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
1.00	20040630	All	Initial issue of document

PAGE RELEASE RECORD

This document consists of the following pages:

PAGE	RELEASE
i - x	1.00
1 - 12	1.00
A – 1 - 3	1.00
B – 1 - 2	1.00

CONTENTS

DOCUMENT AUTHORISATION iii
DOCUMENT CHANGE LOG v
PAGE RELEASE RECORD vi
CONTENTS vii
ACRONYMS viii
REFERENCES ix
1 Summary 1
2 Introduction 1
2.1 Brief Introduction to MyCERT and the US CERT 1
2.2 Overview 2
2.3 Objective 2
2.4 Limitations to the Analysis 3
2.5 Assumptions 3
3 Statistics 4
3.1 MyCERT's Incident Statistics 2003 4
3.2 US CERT's Incident Statistics 2003 5
4 Statistics Analysis 6
4.1 Overview 6
4.2 Analysis on the Trend in Type of Incidents by MyCERT and US CERT 9
5 Recommendations 14
6 Conclusion 16

ACRONYMS

MyCERT	Malaysian Computer Emergency Response Team
US CERT	United States Computer Emergency Response Team

REFERENCES

1) MyCERT's Incidents Statistics 2003
http://www.mycert.org.my

2) US CERT's Incident Statistics 2003
http://www.us-cert.org

3) Clickz
http://www.clickz.com/stats

4) Malaysian Commissions of Multimedia and Communications
http://www.mcmc.gov.my

[This page is intentionally left blank]

1 SUMMARY

This comparative analysis will analyze the Incidents Statistics 2003 reported to the Malaysian Computer Emergency Response Team (MyCERT), representing a developing country's CERT and the US Computer Emergency Response Team (US CERT), representing a developed country's CERT. The incidents analyzed will be include the analysis that are limited to critical incidents only which are Intrusion, Denial of Service, Malicious Codes and Hack Attempts. The analysis will compare both CERTs' statistics in terms of number of incidents reported, the trend in security incident and the similarity between both CERTs statistics. It will also looks into factors contributing to the difference in the number of incidents reported to both CERTs and the factors contributing to the different trend in security incidents for both CERTs. At the end of the analysis, some recommendations targeted for users/system administrators in developing countries are included in defending and handling incidents associated with the trend in the security incident.

2 INTRODUCTION

2.1 Brief Introduction to MyCERT and the US CERT

Malaysian Computer Emergency Response Team (MyCERT) was formed in January 13, 1997 and started its full operation on March 01, 1997. Operating from the Mimos Berhad office at the Bukit Jalil, Technology Park Malaysia, MyCERT provides a point of reference for the Internet community in Malaysia to deal with computer security incidents and methods of prevention.

MyCERT also works closely with the CERT Coordinating Centre, FIRST, APCERT, AUSCERT, besides other CERTs around the world and the Malaysian Police, in dealing with security incident reports.

MyCERT's main mission is to address the computer security concerns of local Internet users and its vision is to reduce the probability of successful attacks and lower the risk of consequential damage.

US-CERT is a partnership between the Department of Homeland Security and the public and private sectors. Established to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. US-CERT was established in September 2003 as a public-private partnership charged with improving computer security preparedness and response to cyber attacks in the United States

US-CERT also provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the United States government about cyber security.

2.2 Overview

The number of computer and internet security incidents around the globe is increasing rapidly day by day as a result of new threats and vulnerabilities being discovered, besides several other contributing factors to such increase. Systems/networks around the world that are connected to the network and with telecommunications infrastructures are posed to various threats, regardless of systems/networks belonging to a developing country, i.e. Malaysia, Thailand, Philippines or to a much developed countries, i.e. the US, Japan, Korea. Computers that were once used primarily for research analysis, data collection, simulation, data storage, graphics etc have been misused to operate intrusions, denial of services and economic frauds.

In response to the increasing number of security incidents affecting the globe, this paper will conduct a comparative analysis on the reported security incidents between the Malaysian Computer Emergency Response Team's (MyCERT) and the United States Computer Emergency Response Team's(US CERT). The study will be representing a developing country's CERT and a developed country's CERT. The Abuse/Incident Statistics for Year 2003 representing the above countries will be used as a basis for the comparative study.

2.3 Objective

The objective of this paper is to compare and analyze the factors contributing to the difference in the number of incidents reported to MyCERT and US CERT and the difference in the trends in security incidents in Malaysia, a developing country and in the US, a developed country. This will eventually help organizations and individuals in the particular country to identify/analyze the threats and find proper countermeasures against the threats, posing their systems and networks.

2.4 Limitations to the Analysis

The comparative analysis will cover only the following critical incidents:

- Intrusion – root compromise, web defacement
- Denial of Service
- Malicious code – worm/virus/Trojan
- Hack attempts/threats – reconnaissance activities, port scanning

2.5 Assumptions

This analysis assumes that the higher number of incidents reported to the US CERT is not due to the fact that there are more vulnerable/unpatched systems/networks running in the US compared to in Malaysia.

3 STATISTICS

3.1 MyCERT's Incident Statistics 2003

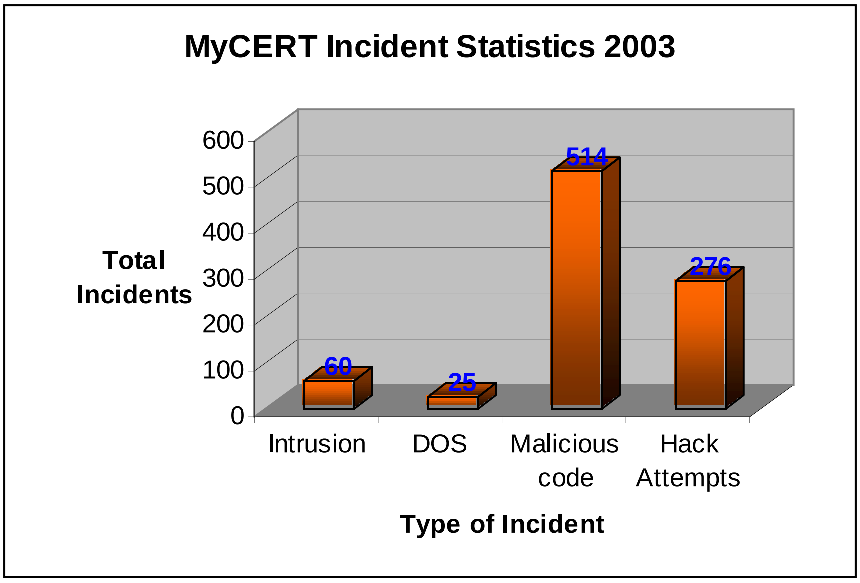


Chart 1: Type of Incident MyCERT

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
Intrusion	4	2	0	5	11	3	1	4	1	8	9	12
Denial of service	0	0	0	1	1	1	1	0	0	0	1	0
Malicious Code	16	6	3	24	51	13	40	207	89	40	14	11
Hack Attempts	20	4	42	40	41	44	38	13	18	0	7	9

Table 1: Type of Incident by Month

3.2 US CERT's Incident Statistics 2003

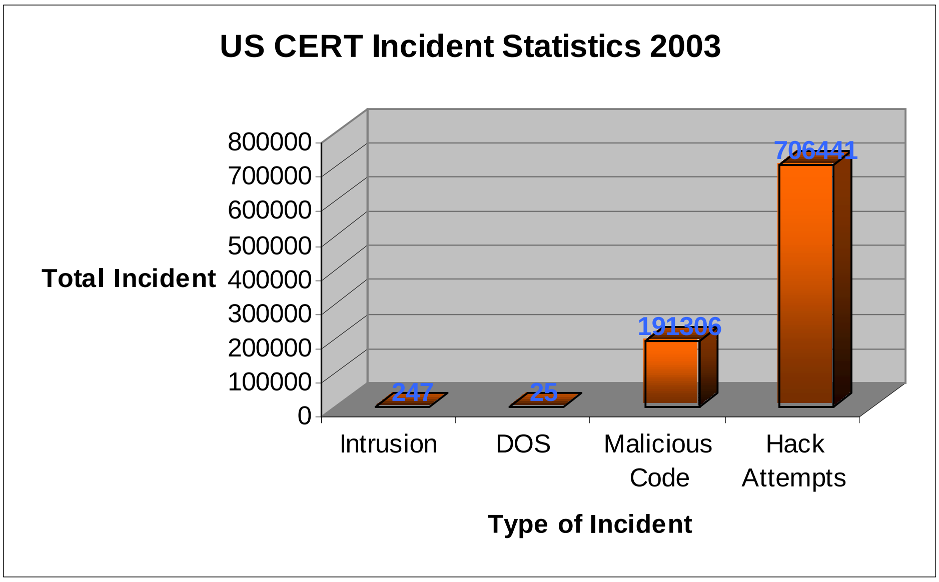


Chart 2: Type of Incident US CERT

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec
Intrusion	20	22	32	35	13	11	8	22	12	10	18	24
Denial of service	2	6	6	1	1	0	2	1	0	4	2	0
Malicious Code	24	161	16	7	12006	206	24	14993	687	38280	29170	95732
Hack Attempts	2892	8638	20349	10115	35112	7742	24943	17889	203853	91254	22824	260830

Table 2: Type of Incident by Month

4 STATISTICS ANALYSIS

4.1 Overview

The year 2003 saw a tremendous increase in the MyCERT's incidents statistics with a total of 855 incidents on intrusions, denial of service, malicious code and hack attempts were reported. As for US CERT, a total of 897 999 incidents were reported, which is hundred times higher than MyCERT's statistics. This analysis assumes that the higher number of incidents reported to the US CERT is not due to the fact that there more vulnerable/unpatched systems/networks running in the US compared to Malaysia. But the imbalance in the total number of incidents reported to MyCERT and US CERT could possibly be due to few factors as below:

a) The rate of computers and Internet usage is comparatively higher in a developed country such as in the US compared to a developing country such as in Malaysia. Higher usage of computers and Internet indicates the possibility of higher rate of security incidents to the systems and networks. This includes the higher rate in systems/networks operating e-businesses, e-banking and tele-workings in developed countries compared to developing countries.

According to Clickz at http://www.clickz.com/stats, the total number of Internet users in the US as of December 2003 is 152,109,000 million as compared to the US population, as of July 2003 which was estimated at 290,342,554 million, according to the CIA World Fact Book. This means that the percentage of Internet users in the US is 52.3% as of December 2003.

As in Malaysia, according to PIKOM Malaysia, the total of Internet users in Malaysia as of December 2003 is 8.6 million and according to the CIA World Fact Book, the population of Malaysia as at July 2003 was estimated at 23,092,940 million. This means that the percentage of Internet users in Malaysia is 37.2% as of December 2003. A pie chart depicting the differences is as below:

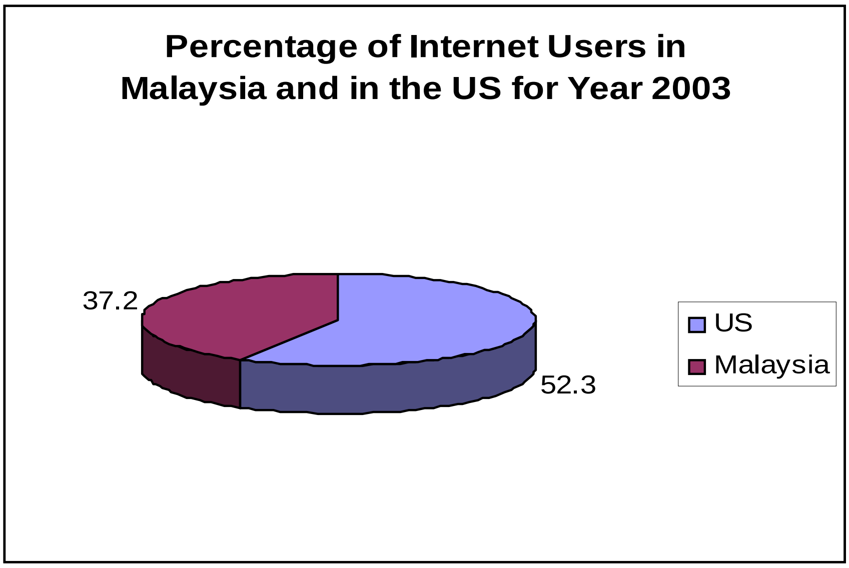


Chart 3: Percentage of Internet Users 2003

b) Users/organizations in developed countries, such as in the US are more inclined to report security incidents to their respective CERTs or their ISPs, as compared to users/organizations from developing countries such as Malaysia who are reluctant to do the same. As a result, the number of incidents reported in a developing country is much lower than a developed country. Some of the reasons why users/organizations from a developing country are reluctant to report security incidents are:

i) Users/organizations feel that such incidents are confidential enough for not to report to any other party, i.e. CERT, ISP.

ii) Users/organizations feel that it is not important to report any security incidents to another party, i.e. CERT, ISP.

iii) System/Network Administrators feel that they can solve/handle the problem/incident themselves without having to report and get assistance from their CERT or ISP.

c) Hacking activities, i.e. reconnaissance activities, port scannings are more actively/widely carried out with vast availability of more sophisticated hacking tools in developed countries compared to developing countries. Thus more systems and networks are probed/scanned as a result of these vigorous activities.

Higher number of incidents on intrusions (root compromise, web defacement) was reported to the US CERT compared to the MyCERT, with a total of 247 reports and 60 reports made respectively. The US CERT has recorded a triple number of incidents on intrusions as compared to MyCERT. The higher number of intrusion incidents reported to US CERT could possibly be due to a higher number of vulnerable systems/networks running e-businesses, e-banking and tele-workings in developed countries as compared to developing countries.

More reports were reported on denial-of-service incidents to the US CERT compared to MyCERT, with a total of 25 incidents and a total of 5 reports made respectively. Again the reason for this was due to the higher/wider usage of computers/internet in developed countries compared to developing countries. This high usage allows bigger opportunities for more vulnerable systems/networks to be attacked as compared to a developing country with lower usage of computers and networks.

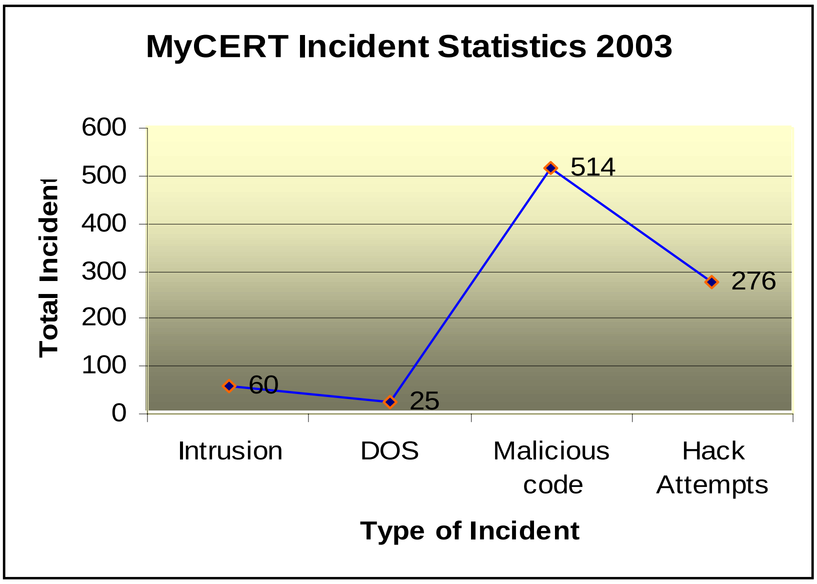
A higher number of reports on malicious code incidents, which includes worm, virus and Trojan, were reported to the US CERT compared to MyCERT, with a total of 191,306 incidents and a total of 514 incidents reported respectively. The higher rate of malicious codes incidents reported to the US CERT would be obviously due to the higher rate of computers/systems being used in developed countries compared to developing countries with lower rate computers/systems being used.

More reports on hack attempts which include reconnaissance activities and port scanning were reported to the US CERT with a total of 706,441 reports as compared to a total of 276 incidents reported to MyCERT. The higher rate may indicate that reconnaissance activities and other hack attempts/probes are more heavily carried out in developed countries as compared to developing countries. Systems/networks belonging to developed countries are becoming major targets for probing/reconnaissance activities as compared to those belonging to developing countries. Some possible reasons to this could be due to the fact that systems/networks belonging to developed countries contain more valuable information/data that may impose high interest on many people. Or it could also because the systems/networks are equipped with high end technologies that may lure the hackers to probe them.

In this statistics analysis, we conclude that more security incidents are reported to the US CERT as compared to MyCERT for year 2003, with a total of 897 999 incidents and a total of 855 incidents reported respectively.

4.2 Analysis on the Trend in Type of Incidents Reported to MyCERT and US CERT

The US CERT and MyCERT show a different trend of incident types reported to them respectively. This is based on the number of reports reported on each category/type of incidents. Analyzing on MyCERT's statistics as in the below graph, Malicious Code incidents have become a trend of incident reported to MyCERT compared to other types of incidents. A total of 514 incidents were reported to MyCERT on Malicious Codes, which is about 60.11% of the four (4) categories of incidents reported to MyCERT for year 2003, as shown in the graph below. This trend subsequently may represent developing countries generally. Following malicious code is hack attempts as a second trend with a total of 276 reports reported to MyCERT, then a total of 60 reports reported on Intrusions as the third trend and the lowest trend is on denial-of-service with a total of 5 reports been made.



Graph 1: Type of Incident

For the past two years, malicious code has contributed to serious impacts in terms of financial loss, unavailability of information/data and service disruption to countries around the globe, including developing countries like Malaysia. With the wide availability of tools/scripts on the Internet which can be obtained for free, more and more worms and their variants are released, with an average of 10 new worms per month. For example, in the case of Blaster worm which first appeared in August 2003 and after one (1) week of Blaster worm's propagation, the Nachi worm was released, and after two weeks of Nachi worm's activities, a variant of Sobig worm, the Sobig.F was released in the wild. The above trio worms had contributed to about 70% of worm incidents reported to MyCERT for year 2003. This indicated in the Incidents Statistics 2003, in which July and September had contributed the highest number of worms reported with a total 291 incidents.

Reasons for this trend were due a higher number of incidents reported on malicious codes compared to any other incidents. This could possibly be due to a few factors as below:

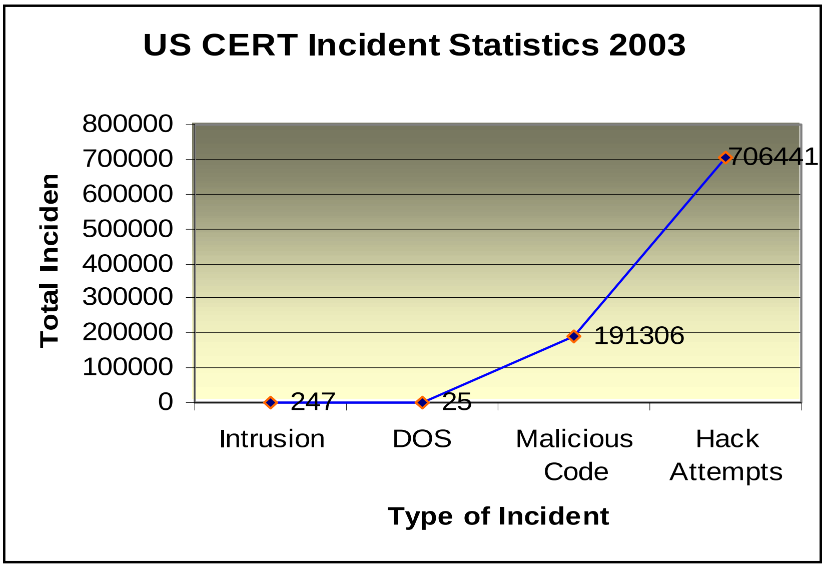
i) More users are using systems/hosts running on Windows platforms, well known platform for worm transmissions compared to other operating systems, i.e. Linux, Solaris.

ii) Lack of awareness, importance and knowledge in system/network security amongst users/systems administrators. This includes lack of knowledge on proper steps/mechanisms on recovery and eradication from incidents related to malicious codes.

iii) No proper defense mechanisms against worms/viruses propagations. Hosts/systems do not have proper Anti-virus softwares installed on their systems. Besides having not installing Anti-virus softwares, users also fail to install Personal Firewall on their systems. Personal Firewalls help in blocking certain ports related to worm activities besides blocking any attempts to install any malicious codes on the system. Many organizations still do not have Anti-virus filters on their email gateways to block any worm attachments coming into the network.

iv) Not updating anti-virus softwares with latest virus signatures and not fixing any known vulnerabilities in certain operating systems associated to worm activities.

v) Not reporting to proper channels for example to the CERTs, ISPs for assistance during an incident. As a result, users/system administrators are depriving themselves from having proper guidance/knowledge on recovery and eradication steps/mechanism. This eventually contributes to re-occurrence of incidents to the organization, as encountered by MyCERT in many incidents reported to them.



Graph 2: Type of Incident

As for the US CERT, the above graph shows that ‘Hack Attempts’ is the trend of incident reported to them as compared to other incidents. A total of 706,441 reports were reported which is about 78.6% of the total of the four (4) category of incidents reported, followed by ‘Malicious Code’ as the second trend with a total of 19,106 reports, then a total of 247 reports on ‘Intrusion’, the third trend and a total of 25 reports on ‘Denial-of-Service’, the lowest trend of incident in the US. Somehow, some similarities exist in both CERTs, in terms of the lowest trend of incidents, with ‘Intrusions’ and ‘Denial-of-Service’ being the lowest trend of incident in both CERTs.

Some possible reasons on ‘Hack Attempts’ being a trend in incident of in the US CERT, subsequently representing developed countries could be due to:

i) More and more reconnaissance activities and port scanning are actively conducted than other incidents in developed countries such as in the US compared to developing countries such as in Malaysia.

ii) Higher rate of systems/networks connected to the Internet in developed countries, i.e. the US is comparatively much higher as compared to systems/networks in developing countries. Thus, giving greater chance for the number of systems/networks being probed.

iii) Higher population and enthusiasm among intruders/script kiddies to probe more systems/networks had contributed to higher number of hack attempts incidents in developed countries as compared to developing countries.

Interesting finding indicates that the statistics shows that ‘Intrusions’ and ‘Denial-of-Service’ as the lowest trend of incidents for both CERTs. MyCERT and US CERT recorded lowest number of reports on ‘Denial-of-Service’ incidents for 2003. Some of the factors that may contribute to the lowest number of reports on ‘Denial-of-Service’ could be due to that more intruders/script kiddies are interested in indulging on worm activities and port scannings/probings. Another factor could be due to the more tremendous impacts malicious code and hack attempts incident could cause. For example, an Internet worm could lead to a serious denial-of-service as a result of vigorous/massive probing of the worms towards target machines and continuous/successful hack attempts could lead to a total compromise/destruction of a machine.

The trend analysis for year 2003 concludes that the trend of incident in Malaysia, representing developing country is Malicious Codes and the trend of incident in the US, representing a developed country is Hack Attempts, based on the number of incidents reported. However, both CERTs recorded Intrusions and Denial-of-Service as the lowest trend of incident for year 2003.

5 RECOMMENDATIONS

Some of the recommendations that can be followed/adhered by users/system administrators in defending against the malicious codes incident within MyCERT constituency and in developing countries as a whole are:

i) Having proper defense mechanism against malicious codes activities. The defense mechanism here includes anti-virus softwares for hosts/systems to block any incoming worms/viruses to the host/system. The Anti-virus softwares also can scan and remove any worm/viruses that may have infected the host/system. It is also recommended to install Personal Firewalls at hosts/systems in order to alert and block any Trojans being installed to the host/system. Personal Firewalls also can be configured to close any ports related to worm activities, thus minimizing worm's propagation.

ii) System Administrators are advised to install anti-virus filters at emails gateways to block any incoming worm attachments to the network. This helps in minimizing the worms' infection and propagation within a network. System administrators must constantly monitor the worm's activities and make efforts to close any ports related to worms' activities at their routers/firewalls.

iii) Users/system administrators must make sure that the defense mechanisms running on their hosts/systems are regularly updated/upgraded. For example, anti-virus softwares must be regularly updated with latest signature files in order for the anti-virus software to be able to detect and block any new worms/viruses.

iv) Users/system administrators must make sure the machines they are running are free from any vulnerabilities associated to worm activites. Otherwise they need to patch and upgrade their machines prior to connecting to the network.

v) Users/system administrators are advised to report to their CERTs or ISPs on detecting any incidents related to malicious codes. The reporting of such an incident is very important in assisting users/system administrators in total elimination of the incident, by gaining proper step/mechanism on containment, recovery and eradication.

vi) ISPs are recommended to monitor any known malicious codes activities and make efforts in blocking any ports related to vigorous/massive propagation of an Internet worm at the ISP level to help in minimizing the infection and propagation.

vii) Users/system administrators are advised to arm themselves with proper knowledge and skills in defending and handling incidents related to malicious codes.

6 CONCLUSION

In conclusion, the incident statistics shows higher number of reports reported to the US CERT as compared to MyCERT. The reason could be due to higher rate of computers and Internet usage in the US as compared to Malaysia, besides lack of reporting of incidents in Malaysia as compared to the US. The analysis also concludes with the difference in trend of incidents in both countries with malicious codes being a trend of incident in Malaysia and hack attempts being a trend of incident in the US. Factors contributing to such differences has been analyzed and discussed in this paper. In addition, the analysis also found that both CERTs had recorded lowest number of incidents for intrusion and denial-of-service, simultaneously recorded as lowest trend of incidents in both CERTs. This could be due to the fact that more intruders/script kiddies are keen on activities related to malicious codes and hack attempts as compared to intrusions and denial-of-service. However, the trend may keep changing with the evolvement and advancement in technologies coming forth.