The Cyber-Attacks and Digital Economy in Malaysia during 1997-2016

Srirath Gohwong*

Abstract

This article focuses on the study of the cyber-attacks and digital economy in Malaysia during 1997-2016, by using data from Malaysia Computer Emergency Response Team (MyCERT), in order to (1) to find out the types and patterns of all cyber-attacks in Malaysia during 1997-2016, (2) to compare the cyber-attacks in Malaysia during 1997-2016 according to tourist seasons of Malaysia, and (3) to investigate the relationship between GDP of Malaysia and the cyber-attacks in Malaysia during 1997-2016. Frequency, percentage, mean, standard deviation, One Way ANOVA with LSD, and Pearson's Product-Moment Correlation are the statistics employed for data analysis. The level of significance was set at.05. The results are as follows: (1) there are 103,423 attacks, or 477 attacks per months during 1997 to 2016 in Malaysia. In each year, there are 6 months (August, September, July, June, October, and November) for high volume attacks due to many top events in Malaysia, (2) the big four in Malaysia during 1997-2016 are Fraud, Abusive content, Intrusions, and Malicious code with three patterns of attacks, (3) tourist seasons of Malaysia affected the cyber-attacks at the.05 level of significance, both overall and categorical level (Abusive content and Fraud). The amount of cyber-attacks in high season is always less than shoulder season and low season, and (4) there are high positive relationships between GDP of Malaysia and the cyber-attacks in the overall level, and categorical level (Availability, Intrusion Attempts, and Intrusions) at the.01 level of significance.

Keywords: Cyber-Attacks, Digital Economy, Malaysia, 1997-2016

Introduction

Now Malaysia is on the right track to become a developed country in the year of 2020 according to her long plan, Vision 2020. Digital economy with Multimedia Super Corridor (MSC) project in 1996 with Putrajaya and Cyberjaya is one of the key factor affecting the success of Malaysia's vision because it has changed Malaysia from product-based economy to knowledge-based economy or digital economy since 1996. (Ahmad Sarji Abdul Hamid, 1995; Ariff and Chuan, 2000; Abdulai (a), 2001; Abdulai (b), 2004; Ooi Kee Beng, 2006; Tapscott, 2015) However, the emerging of new economy or digital economy comes with the growth of cyber-attacks which lessens CIA triangle of information security, Confidentiality-Integrity-Availability. These attacks will diminish trusts of people on new economy. (Whitman and Mattord, 2003; Whitman and Mattord, 2008; Whitman and Mattord, 2012; Durand and Vergne, 2013; Boyle and Panko, 2015; Tapscott, 2015) For Malaysia, according to data since 1997 of Malaysia Computer Emergency Response Team (MyCERT, 2016), there are 103,423 attacks, or 477 attacks per months.

According to the above-mentioned concern, this article has three focuses on Malaysia, which is one of the close neighborhoods in AEC (Kotler, Kartajaya, and Huan, 2007), in order to get the basic information for trade and investment of Thailand in Malaysia as follows: (1) to find out the types and patterns of all cyber-attacks in Malaysia during 1997-2016, (2) to compare

* Faculty of Social Sciences, Kasetsart University, Thailand; Email: srirathg3@yahoo.com

the cyber-attacks in Malaysia during 1997-2016 according to tourist seasons of Malaysia, and (3) to investigate the relationship between GDP of Malaysia and the cyber-attacks in Malaysia during 1997-2016.

Type of Information Attacks

Cyber-attacks are any acts by threat agents for compromising the security of victims' devices for the interest of attackers. (Whitman and Mattord, 2003; Whitman and Mattord, 2008; Whitman and Mattord, 2012) There are various classification of information attacks (Whitman and Mattord, 2003; Whitman and Mattord, 2008; Whitman and Mattord, 2012; Oz, 2009; Brown, C.V. et al., 2014; Marakas and O'Brien, 2014; Valacich and Schneider, 2014; Boyle and Panko, 2015; Laudon and Laudon, 2016; European Computer Security Incident Response Team Network, 2003)

In this paper, eCSIRT's taxonomy will be employed for data analysis because it is the standardized framework which covers all above-mentioned classifications. In addition, it is very convenient for comparing with cyber-attacks in Thailand, which employs this classification for national cyber-security. (Gohwong, 2016)

European Computer Security Incident Response Team Network (eCSIRT) employs the WP4 Clearinghouse Policy-Release 1.2, the common framework for information security-classified by Jimmy Arvidsson in 2003, as follows: Abusive Content (Spam, Harassment, Child/Sexual/Violence), Malicious Code (Virus, Worm, Trojan, Spyware, Dialer), Information Gathering (Scanning, Sniffing, Social Engineering), Intrusion Attempts (Exploiting of known Vulnerabilities, Login attempts, new attack signature), Intrusions (Privileged Account Compromise, Unprivileged Account Compromise, Application Compromise), Availability (DoS, DDoS, Sabotage), Information Security (Unauthorized access to information, Unauthorized modification of information), Fraud (Unauthorized use of resources, Copyright, Masquerade), Other (All incidents which don't fit in one of the previous categories). (European Computer Security Incident Response Team Network, 2003)

Malaysia-Tourist Seasons and Events

For Malaysia, tourist seasons are classified into 3 seasons-high, shoulder, and low. The high season is during December to February. The shoulder season, between peak and off-peak seasons, is during July to November. The low season is during March to June. In addition, key events of Thailand are as follows: January (Thai Pongal, Thaipusam), February (Chinese New Year), March (Birthday of the Goddess of Mercy/ Guan Yin/ Kuan Yin), April (Petronas Malaysian Grand Prix), May (Wesak / Vesak Day), June (George Town Festival, Gawai Dayak, Festa de San Pedro, Dragon Boat Festival), July (Rainforest World Music Festival), August (Hungry Ghosts Festival, Malaysia's National Day), September (Mooncake Festival, Hari Raya Puasa), October (Deepavali, Hari Raya Haji), November (Thimithi), and December (Christmas). (Richmond et al., 2013)

Methodology

The cyber-attacks data during 1997-2016 are from Malaysia Computer Emergency Response Team (MyCERT, 2016). The scope of the study is 217 months during 1997 to 2016 because of no data in 7 months of 1997 (January, February, March, April, May, June and July) and 4 months of 2016 (September, October, November, December). The statistics employed in this study are frequency, percentage, mean, standard deviation, One Way

ANOVA with LSD and Pearson's Product-Moment Correlation. The level of significance is set at.05.

Findings

Types and patterns of all cyber-attacks in Malaysia during 1997-2016

All cyber-attacks in Malaysia during 1997-2016 are shown in Table 1 and Figure1.

Table 1 Types and patterns of all cyber-attacks in Malaysia during 1997-2016

eCSIRT Taxonomy	Malaysian Classification	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Abusive content	1	1897	2136	2316	2809	2369	3306	3248	3574	3524	3902	3943	3384	36408
Availability	2	52	31	72	50	50	32	47	79	49	66	41	20	589
Fraud	3	2357	2596	2594	2666	2768	2680	2445	2337	2217	2266	2101	2281	29308
Information gathering	4	34	26	43	75	40	102	47	76	45	34	39	31	592
Information security	5	0	0	0	0	0	0	0	0	0	0	0	0	0
Intrusion Attempts	6	298	276	340	473	393	352	355	518	1117	350	405	339	5216
Intrusions	7	1658	1946	2214	1814	1920	1895	1943	2237	1748	1775	1895	1762	22807
Malicious code	8	658	533	703	521	572	794	1093	1075	997	661	472	424	8503
Other	9	0	0	0	0	0	0	0	0	0	0	0	0	0
TOTAL		6954	7544	8282	8408	8112	9161	9178	9896	9697	9054	8896	8241	103423

Note: 1 = Content Related, Cyber Harassment, Spam; 2 = Denial of Service, Destruction, Mailbomb; 3 = Fraud and Forgery; 4 = Vulnerabilities Report, Vulnerability Probing, Drones Report, 5= N/A; 6 = Intrusion Attempt, Hack Threat; 7 = System Intrusion, Intrusion; 8 = Malicious code, Virus; 9 = N/A

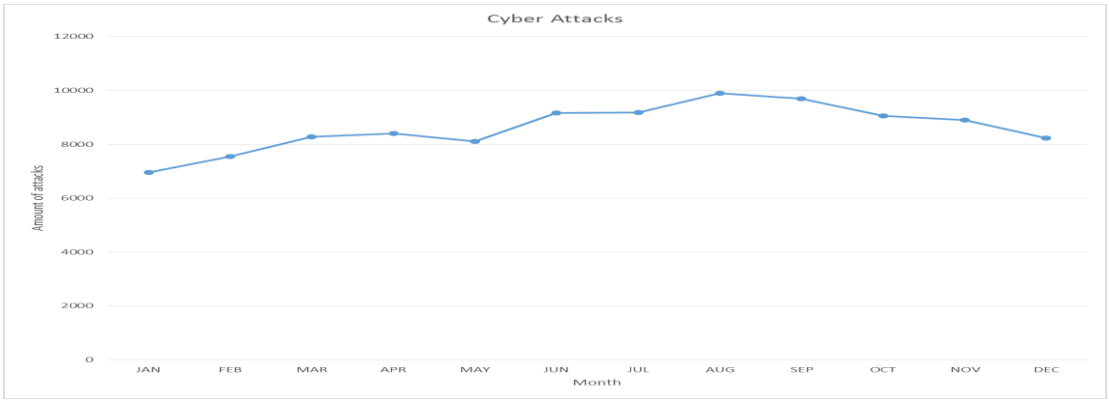

Figure 1 Amount of all cyber-attacks per month in Malaysia during 1997-2016

The findings found as follows:

1) There are 103,423 attacks, or 477 attacks per months during 1997 to 2016 in Malaysia.

2) In aspect of Month, there are 6 months, or half a year, for high volume attacks. They are orderly presented as follows: August, September, July, June, October, and November. In these months, there are many top events in each months as follows: June (George Town Festival, Gawai Dayak, Festa de San Pedro, and Dragon Boat Festival), July (Rainforest World Music Festival), August (Hungry Ghosts Festival, Malaysia's National Day), September (Mooncake Festival, Hari Raya Puasa), October (Deepavali, Hari Raya Haji), and November (Thimithi). It stands for that approximately 66.7% of these dangerous months have more than two top events per month whereas another six low-volume-attacks months has approximately 16.7% for two top events per month.

3) In aspect of techniques of the attacks, there are big four in Malaysia during 1997-2016, see Table2, which occupy the major role of the attacks for 11 months of year as follows: Fraud, Abusive content, Intrusions, and Malicious code. In Malaysia, there are three clear patterns of the big four attacks as follows: Pattern I (big role for 7 months: April, June, July, August, October, November, and December)-Abusive content is highest, orderly

followed by Fraud, Intrusions, and Malicious code; Pattern II (big role for 4 months: January, February, March, and May)-Fraud is highest, orderly followed by Abusive content, Intrusions, and Malicious code; and Pattern III (big role for 1 months, September)-Abusive content is highest, orderly followed by Fraud, Intrusions, and Intrusion Attempts.

Table2 Overall of cyber-attacks in Malaysia during 1997-2016

eCSIRT Taxonomy	Malaysian Classification	TOTAL	Mean
Abusive content	Content Related, Cyber Harassment, Spam	36408	167.78
Fraud	Fraud and Forgery	29308	135.06
Intrusions	System Intrusion, Intrusion	22807	105.10
Malicious code	Malicious code, Virus	8503	39.18
Intrusion Attempts	Intrusion Attempt, Hack Threat	5216	24.04
Information gathering	Vulnerabilities Report, Vulnerability Probing, Drones Report	592	2.73
Availability	Denial of Service, Destruction, Mailbomb	589	2.71
Information security	N/A	0	0.00
Other	N/A	0	0.00
TOTAL		103423	476.60

Intrusion Attempts, such as hacking, is highest only on September with 1,117 attacks. In average, Intrusion Attempts will occur only 474 attacks per months.

Comparison of the cyber-attacks in Malaysia during 1997-2016 according to tourist seasons of Malaysia

The comparison between tourist seasons of Malaysia and the cyber-attacks in Malaysia during 1997-2016 is shown in Table 3.

Table 3 Comparison of the cyber-attacks in Malaysia during 1997-2016 according to tourist seasons of Malaysia

eCSIRT taxonomy		SS	df	MS	F	P
Abusivecontent	Between Groups	3217920.533	2	1608960.267	6.455	.018*
	Within Groups	2243311.467	9	249256.830		
	Total	5461232.000	11			
Availability	Between Groups	935.050	2	467.525	1.817	.217
	Within Groups	2315.867	9	257.319		
	Total	3250.917	11			
Fraud	Between Groups	366187.200	2	183093.600	12.135	.003*
	Within Groups	135789.467	9	15087.719		
	Total	501976.667	11			
Informationgathering	Between Groups	2071.200	2	1035.600	2.532	.134
	Within Groups	3681.467	9	409.052		
	Total	5752.667	11			
IntrusionAttempts	Between Groups	124481.000	2	62240.500	1.289	.322
	Within Groups	434443.667	9	48271.519		
	Total	558924.667	11			
Intrusions	Between Groups	53864.300	2	26932.150	.846	.461
	Within Groups	286444.617	9	31827.180		
	Total	340308.917	11			
Maliciouscode	Between Groups	215910.050	2	107955.025	2.536	.134
	Within Groups	383092.867	9	42565.874		
	Total	599002.917	11			
TOTAL	Between Groups	5936006.700	2	2968003.350	12.060	.003*
	Within Groups	2214876.217	9	246097.357		
	Total	8150882.917	11			

* Significant at the.05 level

The finding found that, in overall, tourist seasons of Malaysia affected the cyber-attacks during 1997-2016 at the.05 level of significance. In addition, the post hoc test revealed that shoulder season (Mean = 9344.20) is higher than both low Season (Mean = 8490.75) and high Season (Mean = 7579.67).

In categorical level, Abusive content and Fraud affected the cyber-attacks during 1997-2016 at the.05 level of significance. In addition, the post hoc test of Abusive content revealed that shoulder season (Mean = 3638.20) is higher than both low season (Mean = 2700.00) and high season (Mean = 2472.33). For post hoc test of Fraud, it was found that low season (Mean = 2677.00) is higher than both high season (Mean = 2411.33) and shoulder season (Mean = 2273.20).

The relationship between GDP of Malaysia and the cyber-attacks in Malaysia during 1997-2016

The association between GDP of Malaysia and the cyber-attacks in Malaysia during 1997-2016 is shown in Table 4.

There are high positive relationship between GDP of Malaysia and the cyber-attacks in Malaysia during 1997-2016 in the overall level, and categorical level (Availability, Intrusion Attempts, and Intrusions) at the.01 level of significance.

Table 4 The association between GDP of Malaysia and the cyber-attacks in Malaysia during 1997-2016

Cyber-attacks in Malaysia during 1997-2016	**GDP (current US$)**	
	r	**P**
Abusive content	.180	.462
Availability	.923	.000*
Fraud	.349	.143
Information gathering	.434	.063
Intrusion Attempts	.822	.000*
Intrusions	.745	.000*
Malicious code	.180	.462
Total	**.706**	**.001***

* Significant at the.01 level

Discussion

1) There are 103,423 attacks, or 477 attacks per months during 1997 to 2016 in Malaysia. In each year, there are 6 months (August, September, July, June, October, and November) for high volume attacks due to many top events in Malaysia. The reason may be that these dangerous months are in the shoulder season (July to November) and low season (June) which internet traffic is not strictly monitored by government as the months in high season. In addition, this finding revealed that the more access to Internet under digital economy since 1996, the less information security. (Whitman and Mattord, 2012)

2) In aspect of techniques of the attacks, the big four in Malaysia during 1997-2016 are Fraud, Abusive content, Intrusions, and Malicious code with three patterns of attacks. Though Intrusion Attempts is not in the big four but it has high amount of attacks. These attacks focus on privacy and quality of life (Abusive content), property rights and intellectual property (Fraud), online anonymity (Fraud), network security (Availability, Intrusion, Intrusion Attempts, Malicious Code/Malware). (Himma and Tavani, 2008; Quinn, 2012; Quinn, 2015; Laudon and Laudon, 2016)

3) For comparison of the cyber-attacks in Malaysia during 1997-2016 according to tourist seasons of Malaysia, tourist seasons of Malaysia affected the cyber-attacks at the.05 level of significance, both overall and categorical level (Abusive content and Fraud). The amount of cyber-attacks in high season is always less than shoulder season and low season. This finding supports the previous findings in (1) that the shoulder season and low season

which internet traffic is not strictly monitored by government as the months in high season, and in (2) these attacks focus on privacy and quality of life (Abusive content), property rights and intellectual property (Fraud), online anonymity (Fraud).

4) For the investigation of association between GDP of Malaysia and the cyber-attacks in Malaysia during 1997-2016, there are high positive relationships between GDP of Malaysia and the cyber-attacks in the overall level, and categorical level (Availability, Intrusion Attempts, and Intrusions) at the.01 level of significance. This finding supports the previous findings in (1) that the more access to Internet under digital economy, the less information security, and in (2) these attacks focus on network security for piracy (Availability, Intrusion, and Intrusion Attempts).

Conclusion

This article focuses on the study of the cyber-attacks and digital economy in Malaysia during 1997-2016, by using data from Malaysia Computer Emergency Response Team (MyCERT), in order to (1) to find out the types and patterns of all cyber-attacks in Malaysia during 1997-2016, (2) to compare the cyber-attacks in Malaysia during 1997-2016 according to tourist seasons of Malaysia, and (3) to investigate the relationship between GDP of Malaysia and the cyber-attacks in Malaysia during 1997-2016. The findings give an important lesson for Thailand, which just fully join the digital economy in 2014, that the more access to Internet under digital economy (Malaysia since 1996), the less information security. In addition, it is not easy to find the balance between access and information security, especially in digital economy. (Whitman and Mattord, 2012; Tapscott, 2015; Gohwong, 2016)

References

Abdulai, D. 2001. **Malaysia and the k-economy: Challenges, Solutions and the Road Ahead**. Selangor Darul Ehsan: Pelanduk Publications (M) Sdn Bhd.

Abdulai, D. 2004. **Can Malaysia transit into the K-Economy: Dynamic Challenges, Tough Choices and the Next Phase**. Selangor Darul Ehsan: Pelanduk Publications (M) Sdn Bhd.

Ariff, I. & Chuan, G. (eds.). 2000. **Multimedia Super Corridor**. Kuala Lumpur: Leeds Publications.

Beng, O. 2006. **Era of Transition: Malaysia after Mahathir**. Singapore: Institute of Southeast Asian Studies.

Boyle, R. & Panko, R. 2015. **Corporate Computer Security**. Essex: Pearson Education Limited.

Brown, C. et al. 2014. **Management Information Technology**. Essex: Pearson Education Limited.

Durand, R. & Vergne, J. 2013. **The Pirate Organization: Lessons from the Fringes of Capitalism**. Boston: Harvard Business Review Press.

European Computer Security Incident Response Team Network (eCSIRT). 2003. **WP4 Clearinghouse Policy-Release 1.2 (2003)**. Retrieved from www.ecsirt.net/cec/service /documents/wp4-clearinghouse-policy-v12.html.

Gohwong, S. 2016. "The Cyber-attacks and digital economy in Thailand during 2012-2016." in K. Jermsittiparsert, T. Sriyakul & B. Sheehan. **Proceedings of the 1st International Conference.** Bangkok: Political Science Association of Kasetsart University, pp. 1-10.

Hamid, A. 1995. **Malaysia's Vision 2020: Understanding the Concept, Implications and Challenges**. Selangor Darul Ehsan: Pelanduk Publications (M) Sdn Bhd.

Himma, K. & Tavani, H. (eds.). 2008. **The Handbook of Information and Computer Ethics**. New Jersey: John Wiley and Sons.

Kotler, P., Kartajaya, H. & Huan, H. 2007. **Think ASEAN! Rethinking Marketing toward ASEAN Community 2015**. Singapore: McGraw-Hill.

Laudon, K. & Laudon, J. 2016. **Management Information Systems: Managing the Digital Firm**. Essex: Pearson Education.

Malaysia Computer Emergency Response Team (MyCERT). 2016. **MyCERT Incident Statistics**. Retrieved from https://www.mycert.org.my/statistics/2016.php.

Marakas, G. & O'Brien, J. 2014. **Introduction to Information Systems**. Singapore: McGraw-Hill Education.

Oz, E. 2009. **Management Information Systems**. Boston: Course Technology.

Quinn, M. 2012. **Ethics for the Information Age**. New Jersey: Pearson Education.

_____. 2015. **Ethics for the Information Age**. New Jersey: Pearson Education.

Richmond, S. et al. 2013. **Discover Malaysia & Singapore: Experience the best of Malaysia & Singapore**. China: Lonely Planet Publications Pty Ltd.

Tapscott, D. 2015. **The Digital Economy: Rethinking Promise and Peril in the Age of Networked Intelligence.** New York: McGraw-Hill.

Valacich, J. & Schneider, C. 2014. **Information Systems Today: Managing in the Digital World**. Essex: Pearson Education.

Whitman, M. & Mattord, H. 2003. **Principles of Information Security**. Massachusetts: Thomson Course Technology,

Whitman, M. & Mattord, H. 2008. **Management of Information Security**. Massachusetts: Thomson Course Technology.

Whitman, M. & Mattord, H. 2012. **Principles of Information Security**. CHINA: Course Technology.