The Cyber-attacks in Vietnam during 2010-2016

Srirath Gohwong
Kasetsart University, Thailand
E-mail: srirathg3@yahoo.com

Abstract

This article focuses on the study of the cyber-attacks in Vietnam during 2010-2016, by using Asia Pacific Computer Emergency Response Team (APCERT)'s data, in order to (1) to find out the types and patterns of all cyber-attacks in Vietnam during 2010-2016, and (2) compare the cyber-attacks between Vietnam and Thailand during 2012-2016. Frequency, percentage, Z-score were employed for data analysis. The results are as follows: (1) There were 191,714 cyber-attacks in Vietnam during 2010-2016, (2) During 2010-2016, Deface was the highest cyber-attacks in Vietnam, followed by Malware, and Other, (3) Since 2015, there was an upward trend of cyber-attacks of Deface (Intrusion), Malware / Malicious Code, and Phishing (Fraud) whereas Other had a downward trend, (4) The comparison of Z-score in cyber-attacks between Vietnam and Thailand found that Thailand had higher cyber-attacks than Vietnam in Fraud and Malicious Code whereas Vietnam was at the top of Intrusion and Other.

Keywords: Cyber-attacks, Vietnam, 2010-2016

Introduction

Vietnam is a leading country in ASEAN with strong economy-GDP growth by 6.2 percent in 2016, higher than the average GDP annual growth of ASEAN by 4.5 percent-though she is under communist regime with censorship and online information monitoring. (World Bank, 2017) In addition, the digital economy of Vietnam is run by 1.7% of local businesses only-has very little effect on Vietnam's GDP with less than 5% though she has conducted the reform of market economy and public agencies since 2012 according to her long plan-VIETNAM's Socio-Economic Development Strategy for the period of 2011-2020. (Economica Vietnam, 2012; The Voice of Vietnam Online, 2017) However, with limited readiness of digital economy in Vietnam, there were 191,714 cyber-attacks in Vietnam during 2010-2016 or approximately 27,388 attacks per year according to Asia Pacific Computer Emergency Response Team (APCERT)'s data. (APCERT, 2016) The amount of cyber-attacks in Vietnam is very interesting for Thailand, one of the top 10 of FDI providers in 2016 with US$ 700 million (Vietnam Briefing, 2017) because Thailand, with lower GDP growth than Vietnam by only 3.2 percent, had more severe cyber-attacks than Vietnam in 2016. With data of both countries during 2012-2016 from APCERT and the study of "The Cyber-attacks and digital economy in Thailand during 2012-2016" (APCERT, 2016; Gohwong, 2016), Z-score of Thailand was 4.40 whereas Vietnam was 3.72.

According to the above-mentioned concern, this article has two vital objectives in order to get the basic information for trade and investment of Thailand in Vietnam as follows: (1) to find out the types and patterns of all cyber-attacks in Vietnam during 2010-2016, and (2) compare the cyber-attacks between Vietnam and Thailand during 2012-2016 due to the availability of Thai data.

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 & Mattord, 2012) There are various classification of information attacks. (Whitman & Mattord, 2012; Brown et al., 2014; Marakas & O'Brien, 2014; Valacich & Schneider, 2014; Boyle & Panko, 2015; Laudon & 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)

Methodology

The cyber-attacks data were from VNCERT (APCERT, 2016). The scope of study was during 2010-2016 due to the availability of data. The statistics employed in this study were frequency, percentage, and Z-score.

Findings

The overall of cyber-attacks in Vietnam during 2010-2016

All cyber-attacks in Vietnam during 2010-2016 were shown in Table 1 and Figure 1.

Table 1 Overall of all cyber-attacks in Vietnam during 2010-2016

VN's Incidents Classification	Phishing	Deface	Malware	Other	Total
2016	10057	77654	46664	0	134375
	(7.48)	(57.79)	(34.73)	(0)	(100)
2015	5104	6188	3885	3979	19156
	(26.64)	(32.30)	(20.28)	(20.77)	(100.00)
2014	1458	8291	10037	8400	28186
	(5.17)	(29.42)	(35.61)	(29.80)	(100.00)
2013	2469	1603	2142	165	6379
	(38.71)	(25.13)	(33.58)	(2.59)	(100.00)
2012	970	770	852	0	2592
	(37.42)	(29.71)	(32.87)	(0.00)	(100.00)
2011	385	340	13	17	755
	(50.99)	(45.03)	(1.72)	(2.25)	100.00
2010	233	19	8	11	271
	(85.98)	(7.01)	(2.95)	(4.06)	(100.00)
Total	20676	94865	63601	12572	191714
	(10.78)	(49.48)	(33.17)	(6.56)	(100.00)

Source: APCERT (2016)

According to Table 1, the cyber-attacks in Vietnam during 2010-2016 were 191,714 cyber-attacks or approximately 27,388 attacks per year. However, there were only Phishing (a kind of Fraud), Deface / Web Defacement (a kind of Intrusion), Malware / Malicious code, and Other. Deface (94,865 attacks / 49.48%) was the highest cyber-attacks in Vietnam, followed by Malware (63,601 attacks / 33.17%), and Other / all incidents out of eCSIRT's taxonomy (12,572 attacks / 6.56%).

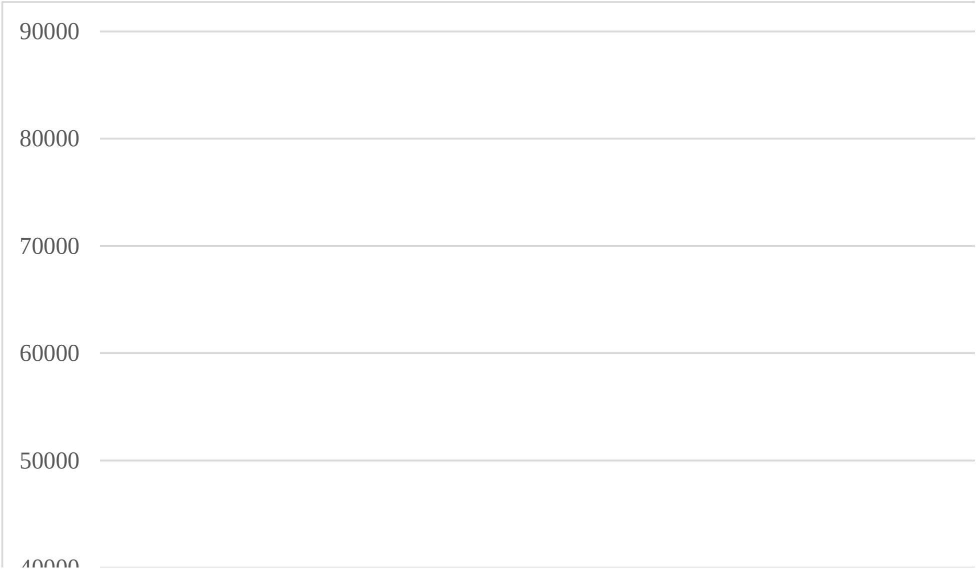

Figure 1 Trend of overall cyber-attacks in Vietnam during 2010-2016
Source: APCERT (2016)

In addition, according to Figure 1, in overall since 2015, there was an upward trend of cyber-attacks of Deface (Intrusion), Malware / Malicious Code, and Phishing (Fraud) whereas Other had a downward trend.

The comparison of cyber-attacks between Vietnam and Thailand during 2012-2016
In order to display the differences of cyber-attacks between Vietnam and Thailand during 2012-2016, Z-score was applied in this study for standardizing data from two sources, which had different amount, data collection methods and mean. (Rowntree, 1991; Rumsey, 2011)

Table 2 Z-score of cyber-attacks between Vietnam and Thailand during 2012-2016

Z-score of TH and VN during 2012-2016	Fraud	Intrusion	Malicious code	Other
TH	0.63	0.15	0.67	-1.46
VN	-0.72	1.22	0.41	-0.91

Source: APCERT (2016)

According to Table 2, Thailand had higher cyber-attacks than Vietnam in Fraud and Malicious Code with approximately.6 S.D. whereas Vietnam was at the top of Intrusion (with 1.22 S.D.) and Other (with -.91 S.D.).

Discussion

There are interesting issues from the findings.

First, the type of cyber-attacks in Vietnam during 2010-2016 were mainly found in four techniques of attacks-Phishing (a kind of Fraud), Deface / Web Defacement (a kind of Intrusion), Malware / Malicious code, and Other. The reason of only four cyber-attacks was that the digital economy of Vietnam was in the initial stage. Though there were 49,063,762

Internet subscribers or 51.5% of Vietnamese in 2016, there were very few local businesses - 1.7% only for running businesses in the digital economy whereas the fixed broadband penetration in Vietnam was quite low. The fixed broadband subscriber in Vietnam was a small base that the penetration has slowly become larger from 6% in 2013 to 8% in 2015 and 9% in 2016. In addition, though mobile broadband penetration in Vietnam has been significantly increased from 14% in 2011 to 31% in 2014 and 43% in 2016, its speed, slower than fixed broadband, did not support the growth of cyber-attacks. (BSA / Software Alliance, 2016; Internet World Stats, 2016; BuddeComm, 2017; Voice of Vietnam Online, 2017)

In addition, all of four cyber-attacks in Vietnam during 2010-2016 mainly focused on individual-oriented cyber-attacks approximately 60.3% with Intrusions (Deface here with 94,865 attacks), and Fraud (Phishing here with 20,676 attacks) due to the limited growth of digital economy of Vietnam, as mentioned in the earlier. The cyber criminals in Vietnam employed Deface and Phishing in order to lessen the faith of visitors or users towards online transaction of organizations.

Second, the trend of cyber-attacks in Vietnam since 2015 was an upward trend of cyber-attacks of Deface, Malware, and Phishing. The reason was that there was a quantum leap growth of online shopping by Vietnamese from 67% in 2015 to 94% in 2016 with Vietnam’s low readiness of cyber laws. The cyber laws of Vietnam did not cover all necessary issues about cyber-attacks such as privacy, interoperability and government procurement. New data breach notification requirements, for example, were just applied for privacy in 2014. (BSA / Software Alliance, 2016; DI Marketing, 2016)

Last, the overall comparison of cyber-attacks between Thailand and Vietnam during 2012-2016 by using Z-score, shown in Table 2, was that Thailand with GDP growth by 3.2 percent has more severe cyber-attacks than Vietnam with GDP growth by 6.2 percent in 2016. In the categorical level, Thailand had higher cyber-attacks than Vietnam in Fraud and Malicious Code-two of the big four of cyber-attacks in Thailand according to the study of Srirath Gohwong in 2016 (Gohwong, 2016), whereas Vietnam was at the top of Intrusions and Other. The findings revealed that cyber-criminals in Vietnam mainly destroyed reputation and trust of organizations (by Deface / Intrusion) whereas cyber-criminals in Thailand principally steal people’s identity (by Phishing-a type of Fraud) and lessen availability of data, computer, and network (by Malware) because Vietnam had some laws about privacy on E-Transactions 2005, Information Technology 2006, Protection of Consumers’ Rights 2010 whereas Thailand had no privacy law. Thailand’s Personal Data Protection Bill was in the stage of public policy formulation. That was why Fraud and Malware played a big role in Thailand because they both directly attacked the availability of privacy, data, computer, and network. For Intrusion, this cyber-attack against network security was outstanding in Vietnam because the cybercrime laws of Vietnam did not cover all activities in the Budapest Convention on Cybercrime-the first international treaty on crimes on Internet and other computer networks-whereas Thailand’s cybercrime laws closely covered the convention. (BSA / Software Alliance, 2016)

Conclusion

This article focuses on the study of the cyber-attacks in Vietnam during 2010-2016 in order to (1) to find out the types and patterns of all cyber-attacks in Vietnam during 2010-2016, and (2) compare the cyber-attacks between Vietnam and Thailand during 2012-2016 due to the availability of Thai data. The findings found that the cyber-attacks in Vietnam during 2010-2016 were 191,714 cyber-attacks. Cyber-attacks in Vietnam during 2010-2016 chiefly focused on individual-oriented cyber-attacks with Intrusions (Deface), and Fraud (Phishing) due to the limited growth of digital economy of Vietnam. An upward trend of cyber-attacks of Deface, Malware, and Phishing obviously occurred in Vietnam since 2015. In addition, cyber-criminals in Vietnam mainly destroyed reputation and trust of organizations while cyber-criminals in Thailand principally steal people's identity and lessen availability of data, computer, and network.

References

APCERT. 2016. **APCERT Annual Report 2016**. Retrieved from www.apcert.org/documents/pdf/APCERT_Annual_Report_2016.pdf.

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

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

BSA (Software Alliance). 2016. **2016 BSA Global Cloud Computing Scorecard: Confronting New Challenges**. Retrieved from cloudscorecard.bsa.org/2016/.

BuddeComm. 2017. **Vietnam-Fixed Broadband, Digital Economy and Digital Media-Statistics and Analyses.** Retrieved from www.budde.com.au/Research/Vietnam-Fixed-Broadband-Digital-Economy-and-Digital-Media-Statistics-and-Analyses?r=51.

DI Marketing. 2016 **Study about Online Shopping Behavior in Vietnam.** Retrieved from www.slideshare.net/mobile/dimvn/ecommerce-usage-in-vietnam-2016.

Economica Vietnam. 2012. **Vietnam Socio-Economic Development Strategy 2011-2020.** Retrieved from www.economica.vn/Portals/0/Documents/1d3f7ee0400e42152bdcaa439bf62686.pdf**.**

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

Internet World Stats. 2016. **Vietnam Internet Usage Stats and Marketing Report**. Retrieved from www.internetworldstats.com/asia/vn.htm.

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

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

Rowntree, D. 2000. **Statistics without tears**. London: Penguin Books.

Rumsey, D. 2011. **Statistics for dummies**. Indianapolis: John Wiley and Sons.

Gohwong, S. 2016. "The Cyber-attacks and digital economy in Thailand during 2012-2016." in **Proceedings of the 1st International Conference.** Bangkok: Political Science Association of Kasetsart University

The Voice of Vietnam Online. 2017. **Growing a digital economy in Vietnam**. Retrieved from english.vov.vn/economy/growing-a-digital-economy-in-vietnam-355757.vov.

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

Vietnam Briefing, 2017. **Vietnam in 2017: Spotting Opportunities for FDI.** Retrieved from www.vietnam-briefing.com/news/vietnam-2017-spotting-opportunities-fdi.html/

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

World Bank, 2017. **GDP growth (annual %)**. Retrieved from data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG