Towards A Better Measure of Cybersecurity Awareness: An Exploratory Study of Online Scams in Pan-Asia (Extended Abstract)

Yunhui Zhuang[1], Yun-Sik Choi[2], Alvin Chung Man Leung[1]

Gene Moo Lee[3], Shu He[4], and Andrew B. Whinston[5]

[1]*Dept. of Information Systems, City University of Hong Kong, Hong Kong*

[2]*Dept. of Computer Science, UT Austin, TX, USA*

[3]*Dept. of Information Systems & Operations Management, UT Arlington, TX, USA*

[4]*Dept. of Operations & Information Management, University of Connecticut, CT, USA*

[5]*Dept. of Information, Risk, & Operations Management, UT Austin, TX, USA*

Email: yhzhuang2-c@my.cityu.edu.hk, yunsik@cs.utexas.edu,

shu.he@business.uconn.edu, gene.lee@uta.edu, acmleung@cityu.edu.hk,

abw@uts.cc.utexas.edu

Abstract

The ever increasing number of cyberattacks over the past decade motivates us to explore a more effective way to enhance the security awareness of the general public. Security ranking of firms against online scams may heighten such awareness towards security issues. Given the limited research in Pan-Asia, we are motivated to conduct an exploratory study to analyze the online scam status in the region. The main objective of this study is to develop an automated system that can take in security feeds from various resources, rank companies based on online scam volume, and provide free public access to our ranking data. To achieve this goal, we develop an information security index that reflects an organization's preparedness against online scams and a country's information security condition in Pan-Asia. A public website is also developed and security ranking of firms can be searched. To the best of our knowledge, this paper is among the first to propose an online scam ranking system for organizations in Pan-Asia. Our system also showcases how well organizations in Pan-Asia perform against online scams.

Keywords: Cybersecurity, Spam, Phishing, Online Scam, Information Security Index, Pan-Asia

Contributions

Technical vulnerabilities, insufficient economic motivations, and lack of effective legislation are the root causes of the burgeoning cybercrimes from both technical and economic perspectives (Anderson 2001; Gordon et al. 2003; Anderson and Moore 2006; D'Arcy et al. 2009). Organizations may not have a full understanding of their security problems. As such, we conduct an exploratory study in Pan-Asia to analyze the security status in the region. We aim to establish an automated system that can (1) receive and update online scam data, (2) rank organizations based on existing data, and (3) provide free access to the online scam ranking.

Methodology

We propose a novel design to monitor Pan-Asian organizations' security performances using externally observable data such as outgoing spam and phishing attacks and publish them on a public website. Previous related works show that security ranking is a good way to heighten public attention (Gal-Or and Ghose 2005, Moore and Claytone 2011, Quarterman et al. 2013, Tang et al. 2013, and He et al. 2015). As the ranking is related to organizations' reputation, they may be more proactive to address security issues. The publicized information allows consumers and investors to make informed decisions when they evaluate performance of a company.

Cybersecurity Evaluation Methodology

We use the volume of outbound spams and phishing to construct a comprehensive information security indicator. The volume of malicious emails originated from a company may be an indicator of the company's security status. More outbound spam or phishing emails may imply weaker corporate security infrastructure.

Data Collection

As an initial stage of our study, we focus on a few of countries in Pan-Asia as shown in Table 1. We collect spam and phishing intelligence feeds from reliable organizations as shown in Table 2. Using several ASN (Autonomous System Number) lookup services on Google, we manually identified 1915 valid Pan-Asian organizations in 6 countries and territories. We receive daily spam feeds from *Spamhaus' Composite Blocking List (CBL)* and *Spamikaze's Passive Spam Block List (PSBL)*, while phishing data feeds from the *Anti-Phishing Working Group (APWG)* and *OpenPhish*.

Pan-Asian Countries	Number of Organizations with ASN
Mainland China	709
Hong Kong	388
Macau	4
Taiwan	182
Singapore	354
Malaysia	191
Unspecified	87
Total	*1915*

Table 1. Organizations in Pan-Asia

Attack	Source	Type
Spam	CBL	Email
	PSBL	Email
Phishing	APWG	Web
	OpenPhish	Web

Table 2. Data Sources

System Implementation

As shown in Figure 1, we use outbound spam and phishing volume as a proxy of the latent security condition. We use Google Cloud, Microsoft Azure, Slack as our cloud-based technical support to the whole experiment. Particularly, we develop a security ranking website (see Appendix) to provide organizational security reports to the public on a cloud platform using Google Cloud (outside Mainland China) and Microsoft Azure (for Mainland China). In order to ensure the completeness and correctness of receiving daily spam and phishing feeds, we also implement a backup system for maintenance purpose, so that raw data can be stored into multiple physical disk spaces to allow for fault tolerance.
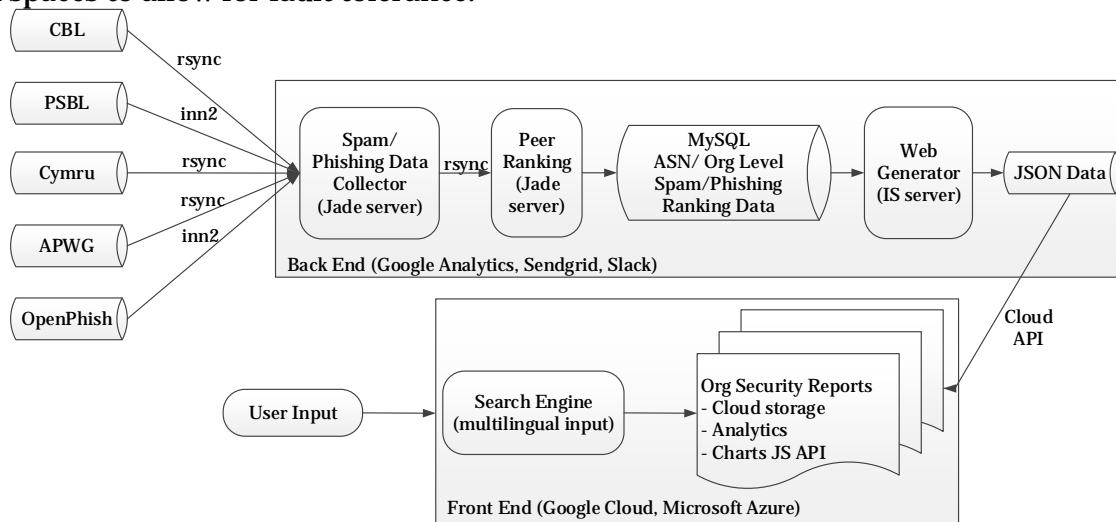
Figure 1. System Design and Implementation

Peer Ranking Effects

Peer ranking publishes an organization's security ranking against others. It essentially helps an organization to better evaluate its security performance. They can benchmark their current security status against their peers. Such feature may promote peer comparison and encourage organizations to adopt better security measures over time.

Borda Count

Our ranking system is developed based on an information security index which is derived from a composite Borda count, as in Adelsman and Whinston (1977), from four constituent rankings with CBL volume, PSBL volume, APWG volume, and OpenPhish volume. Organizations with higher Borda counts are ranked higher which indicate weaker security levels. To provide both macroscopic and microscopic views of the rankings, the ranking system calculates daily and monthly rankings.

Empirical Analysis

At this early stage, we construct a composite ranking system on a country level based on Borda count, which combines two different data sources into one rank score for spam and phishing in Figure 2 and Figure 3, respectively. We also implemented a

website that supports multi-language input to search for country-level and organizational-level rankings as shown in Figure 4 in the appendix.
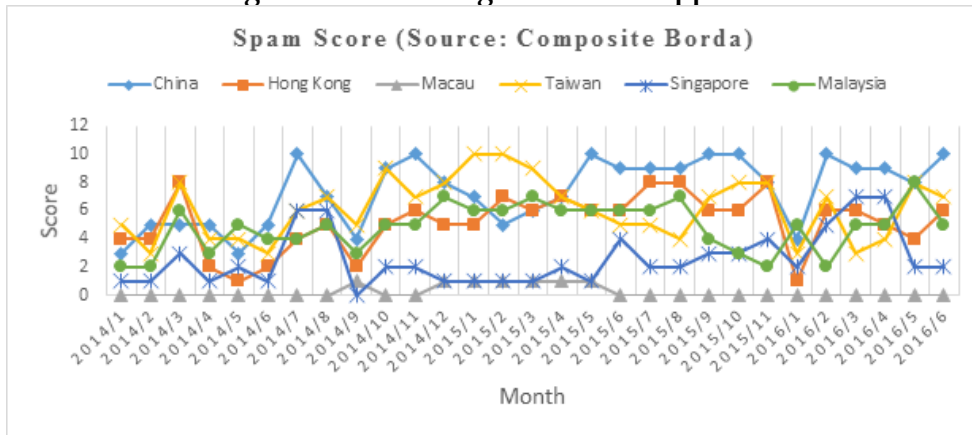
Figure 2. Composite Spam Score
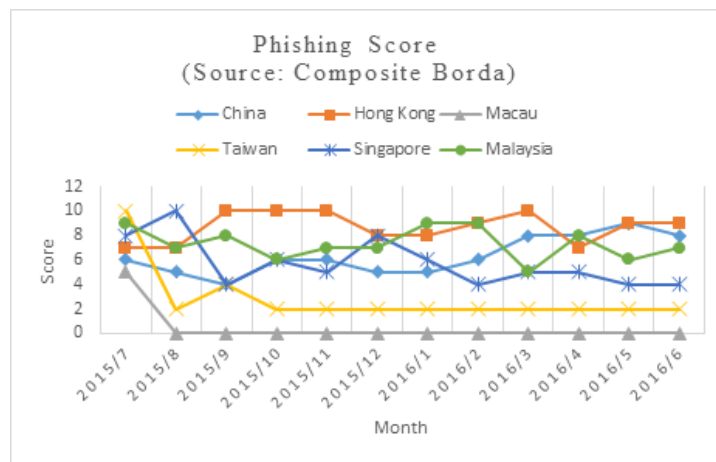
Figure 3. Composite Phishing Score

Discussion and On-going Research

The approaches and early-stage results of the present paper suggest some future directions. For example, our empirical work is just a starting point for online scams evaluation. A large-scale randomized field experiment will be conducted on 1915 Pan-Asian organizations with rigorous randomization to see the treatment effects of information sharing and publication on spam and phishing reduction.

Also, through various treatment channels, such as email, website, and social media, we can estimate the publicity treatment effect with the difference between different groups. The findings will be useful to public policy makers to develop new strategies to motivate firms to strengthen their information security infrastructure over time. Moreover, it may also give a better idea to law makers to evaluate the adequacy of existing cybercrime legislation when compared with neighboring countries in the Pan-Asian region.

In the long run, a nationwide cybersecurity evaluation agency sponsored by governments will be proposed in relation to the theme of this paper (i) that monitors and evaluates the security performance of all organizations on the Internet using

various data including spam, phishing, and DDoS attacks and (ii) that publishes organizations' cybersecurity evaluation reports to the public; along with regulations and policy on proactive organizational security information disclosure to alleviate the cybersecurity problem.

Acknowledgement

References

Adelsman, R. M. and Whinston, A. B. 1977. "Sophisticated voting with information for two voting functions." Journal of Economic Theory 15, no. 1: 145-159.

Anderson, R. 2001. "Why Information Security Is Hard - an Economic Perspective," Proceedings of 17th Annual Computer Security Applications Conference, 2001. ACSAC 2001. , pp. 358-365.

Anderson, R., and Moore, T. 2006. "The Economics of Information Security," Science (314:5799), pp. 610-613.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," Information Systems Research (20:1), pp. 79-98.

Gal-Or, E., and Ghose, A. 2005. "The economic incentives for sharing security information." Information Systems Research 16, no. 2: pp. 186-208.

Gordon, L.A., Loeb, M.P., and Lucyshyn, W. 2003. "Information Security Expenditures and Real Options: A Wait-and-See Approach," Computer Security Journal (19:2).

He, S., Lee, G.M., Han S., Whinston, A., 2016. How Would Information Disclosure Influence Organizations' Outbound Spam Volume? Evidence from a Field Experiment, Journal of Cybersecurity 2(1), 99-118.

Moore, T. and Clayton, R. 2011. "The Impact of Public Information on Phishing Attack and Defense." Communications & Strategies 81.

Quarterman, J.S., Linden, L., Tang, Q., Lee, G.M., and Whinston, A. 2013. "Spam and Botnet Reputation Randomized Control Trials and Policy," Proceedings of the 41st Research Conference on Communication, Information and Internet Policy, pp. 1-13.

Tang, Q., Linden, L., Quarterman, J.S., and Whinston, A. 2013. "Improving Internet Security through Social Information and Social Comparison: A Field Quasi-Experiment," in: Proceedings of Workshop on Economics of Information Security.

Appendix
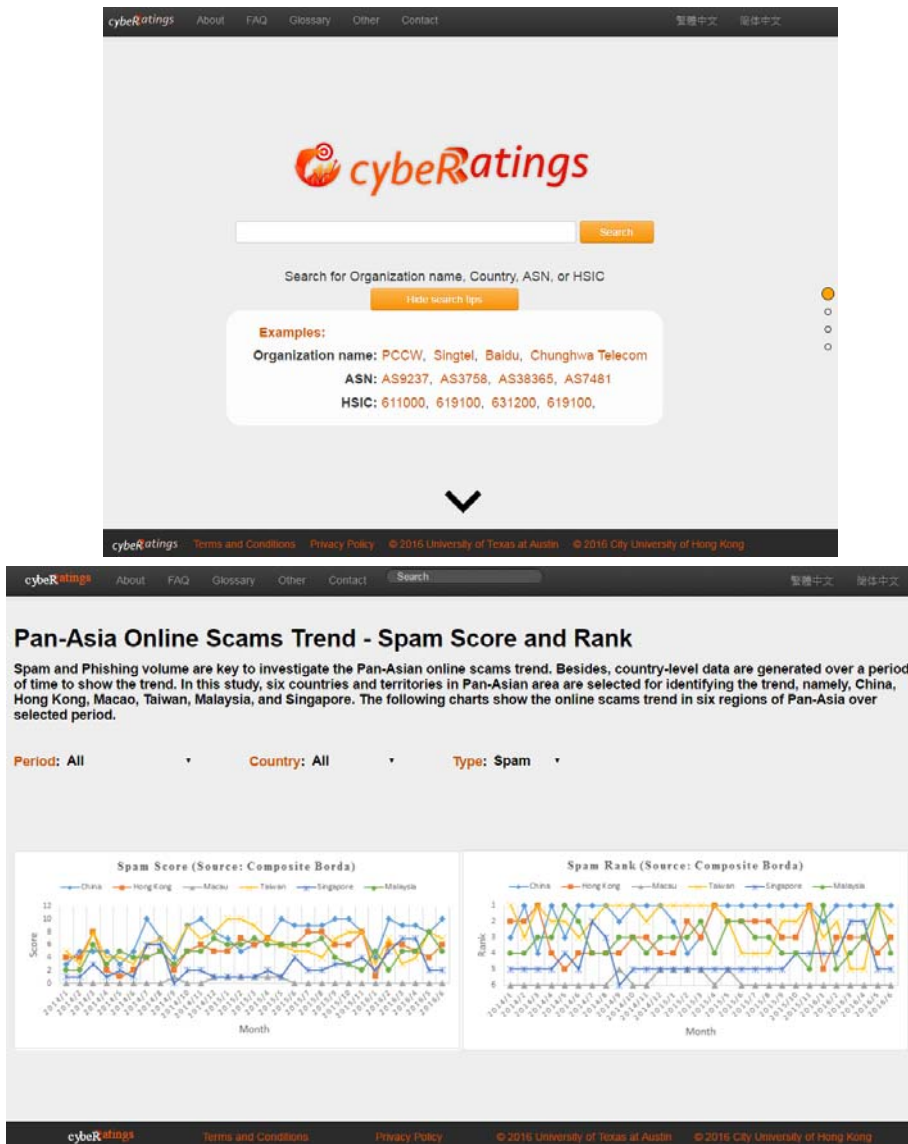
Figure 4. Screenshots of Online Scam Ranking Website