12-2012

Do hackers seek variety? An empirical analysis of website defacements

Kok Wei OOI

Seung-Hyun KIM

QIU-HONG WANG
Singapore Management University, qiuhongwang@smu.edu.sg

Kai Lung HUI

DO HACKERS SEEK VARIETY? AN EMPIRICAL ANALYSIS OF WEBSITE DEFACEMENTS

Research-in-Progress

Kok Wei Ooi
Department of Information Systems
National University of Singapore
ooikokwei@gmail.com

Seung Hyun Kim
Department of Information Systems
National University of Singapore
disksh@nus.edu.sg

Qiu-Hong Wang
School of Management
Huazhong University of Science & Technology
qhwang@mail.hust.edu.cn

Kai Lung Hui
School of Business and Management
Hong Kong University of Science and Technology
klhui@ust.hk

Abstract

The importance of securing the cyberspace is higher than ever along with the evolution of cyber attacks launched by hackers with malicious intention. However, there has been little research to understand the hackers who are the most important agents determining the landscape of information security. This paper investigates the behaviors of hackers using a longitudinal dataset of defacement attacks. Based on theories of economics of criminal behaviors and variety seeking, we find that hackers seek variety in choosing their victims in terms of region, hacking method, and the type of operating systems; as their prior experience is focused in terms of hacking methods, target regions or operating systems, they tend to launch more attacks using new hacking methods, or against targets in new regions or using new operating systems. Furthermore, hackers are more likely to seek variety as the time interval between the previous and the current attack becomes longer.

Keyword: Economics of information security, hacker, website defacement, variety seeking

Introduction

The importance of securing the cyberspace is higher than ever along with the evolution of cyber attacks. Businesses incur huge financial losses due to security incidents every year. An FBI/McAfee study estimates that the cost of cybercrimes to the US economy is over 400 billion dollars, which is equivalent to 3.4 % of its GDP (cf. Cardoso 2007). Many companies have faced multiple very sophisticated attacks including "advanced persistent threat (APT)" that is launched by a highly capable group to target a specific victim effectively over a long period of time (CSI 2011).

As the Internet plays a more prominent role in our economy, persistent threats would become the main security issue in many organisations. Computer hackers would be the key actor in the majority of security incidents including APT. However, due to the anonymity of computer hackers, there has been little research on their behaviour and preferences (Karnow 1994; Van Beveren 2001) understanding of which will serve as an important ground for effective policy and decision making by governments and organizations. Mahmood et al. (2010) emphasize, "*we are at arm's length from black hat motivations and future dark plans*." A lack of black hat studies has also left the rich theories in criminology and psychology largely unexploited and untested in understanding hackers' behaviors. Furthermore, given the persistency of attacks launched by the same attacker over time, an empirical study of the behavior of hackers in a longitudinal setting is imperative.

Defacement is one type of security attack whereby a hacker replaces the appearance of a website or a webpage by breaking into the hosting server. Previously, most defacement incidents were concentrated on websites of individuals or smaller companies. However, as more and more "important" websites are being defaced in recent years, defacement poses a significant threat to organizations. For example, Twitter and Baidu were hijacked by "Iranian Cyber Army" in December 2009 and January 2010, respectively. The FBI job website was defaced in October 2009. Microsoft's website had been defaced multiple times. Zone-h recently reported that 1.5 million websites were defaced in 2010.

Using data on defacement attacks spanning several years, this paper studies the variety seeking behaviors of hackers. In particular, we study why hackers may repeatedly select similar or dissimilar targets in terms of the targets' regions or operating systems, and the hacking methods that they use over time. We find that hackers are more likely to seek variety in choosing their victims in terms of region, hacking method, and the type of operating systems; as their prior experience is focused in terms of hacking methods, target regions or operating systems, they tend to launch more attacks using new hacking methods, or against targets in new regions or using new operating systems. Furthermore, hackers are more likely to seek variety as the time interval between the previous and the current attack becomes longer.

This paper contributes to the literature on information security in the following ways. First, to the best of our knowledge, this is the first paper that examines a choice made by hackers in a longitudinal setting. Second, we show that hackers choose their victims in the spirit of variety seeking. Although it may be more efficient for hackers to focus on certain types of victims due to economies of learning, we find that hackers do seek variety in terms of the profiles of victims, perhaps because they become satiated with the targets that they previously attacked. The variety seeking behavior hints that psychic benefit of committing cybercrime may change even in the short run, which has been implicitly suggested in the criminology literature (Clark and Davis 1995).

Theoretical Backgrounds

The rational choice theory in criminology serves as an overarching framework to understand the cost and benefit components of a hacker' rational decision. The literature on consumer's variety seeking behaviors in marketing, psychology and economics will help on refining specific cost and benefit components that affect the hacker's behaviors to seek variety in the context of information security.

Criminology Theory

The literature in criminology suggests that criminals make rational decisions before committing an illegal activity (Becker 1968; Clark and Davis 1995; Kshetri 2006; Png et al. 2006). A criminal would analyze the cost and benefit of committing the crime or selecting a target. The attractiveness of a target is one of the

factors that constitutes the benefit in the cost-benefit analysis. An attractive target would possess a high perceived value to the hacker in terms of tangible, iconic or reprisal value (Clarke 1999; Tonry and Farirington 1995). Based on the criminology literature (Becker 1968; Clark and Davis 1995), Kshetri (2010) suggests a conceptual framework in which a hacker commits a cybercrime if

$$M_b + P_b > O_{cp} + O_{cm}P_aP_c \quad (1)$$

where M_b = monetary benefit of committing the crime; P_b = psychic benefit of committing the crime; O_{cp} = psychic costs of committing a cybercrime, such as the fear or apprehension of punishment; O_{cm} = monetary opportunity costs of conviction; P_a = the probability of arrest; P_c = the probability of conviction.

Although simple, the framework provides a useful insight to understanding a hackers' incentive to commit hacking attacks over time. More and more hackers today are motivated by financial incentives (Kaspersky 2005). For example, an IT graduate in Romania may earn around $ 400 per month whereas he may be able to make several thousand dollars per months by engaging in the cybercrime economy (Claburn 2008). Psychic benefits can be explained by intrinsic motivation of hackers (Kshetri 2006). Such benefits include fun and testing their skills. Psychic costs include apprehension of punishment, guilt, and mental energy. In fact, penetrating into computer systems may require a large amount of domain knowledge, effort, and time. However, the widespread hacking tools available on the internet have made hacking possible even for amateurs without sophisticated knowledge about hacking. The last term in equation (1) captures any foregone monetary income by being arrested and serving a criminal sentence.

In addition to hackers' incentives, few studies (Sim 2005; Van Beveren 2001; Young et al. 2007) in the information security literature have examined hackers' behavioral motivations. However, it is notable that these studies rely primarily on survey data instead of observing actual hacking behaviors.

Variety Seeking Behaviors

Variety seeking has been studied extensively in marketing, psychology, and microeconomics (Givon 1984; Kahn 1995; McAlister and Pessemier 1982; Sajeesh and Raju 2010; Seetharaman and Che 2009; Wang and Goh 2012). Variety seeking is an individual's tendency of try out a wide variety of products. In marketing and psychology, the variety seeking behavior can be motivated by three factors which are satiation/stimulation, external situation, and future preference uncertainty (Givon 1984; Kahn 1995; McAlister and Pessemier 1982; Sajeesh and Raju 2010).

Prior research has documented that satiation and stimulation, as intrapersonal motives, may cause the direct variety seeking behavior (Kahn 1995; McAlister and Pessemier 1982). For instance, individuals would seek variety to avoid boredom. The drivers of variety seeking are not limited to the needs and availability of resources. In addition, McGuire (1976) has also suggested the need of novelty as a psychological motivation for variety seeking. There is a relationship between variety seeking behavior and the level of stimulation received from novelty, complexity, incongruity and changes. Furthermore, whenever stimulation drops below the satisfactory level, cognitive action will cause individuals to engage in exploratory and variety seeking behavior.

Other than an internal desire for variety, a change in external situations may also lead to an individual's variety seeking behavior as a response to the change. The situation that dictates variety seeking behaviors may include changes in the set of feasible alternatives, changes in tastes, or changes in the constraints facing the individual (McAlister and Pessemier 1982).

Hypotheses Development

Based on the theories on rational choice and variety seeking, we expect that a hacker's prior experience may discount its net benefit derived from ongoing attacks. Further, hackers' variety seeking intention may differ from that of consumers in the following aspects. First, consumers' purchase benefits both themselves and vendors, but hackers' attack induces loss to victims. Second, consumers seek variety for fun or stimulation from the psychological perspective, or due to diminishing marginal benefit from the economic perspective. However, criminals seek variety because of diminishing returns from the same victim, to reduce the risk of being arrested, or to avoid more stringent penalty to recurring crimes. Another possible reason is from the strategic response of victims. Note all of these will affect the cost and

benefit components in Equation (1). Although hacking experience may drive down a hacker's cost to attack the same victim, the marginal cost to attack the same victim may rise as the victim becomes more alert and enhances its protection measures. Unlike the research on consumer behavior where surveys and experiments can be carried out to measure consumers' perceived benefit and cost from repeat purchases, hacker communities are mostly underground. However, observations on hackers' prior choices of victims and time intervals between attacks may help us predict or infer the hacker's variety seeking intention.

Concentration of Prior Experience

Ransbotham and Mitra (2009) argue that a cyber attack may not be a single event; cyber attacks are often interdependent on each other and can be part of the whole information security compromise process. We conceptualize that a hackers' decision to seek variety in terms of the type of victims is affected by his prior experience. As discussed above, the literature on variety seeking suggests that individuals may get bored of the same product after repeatedly consuming it (Kahn 1995; McAlister and Pessemier 1982). In the framework given in (1) above, psychic benefit (P_b) from fun, excitement, and enjoyment decreases as a hacker's experience is concentrated in certain types of victims. Therefore, we expect that hackers are likely to seek variety when there is a higher concentration of prior experience.

Furthermore, there exists an additional reason to prescribe more variety seeking activities when hackers' prior experience is concentrated. Hackers look for an opportunity to test and learn new skills through exercises. As the learning literature suggests, the marginal benefit of learning by doing diminishes as an individual accumulates more and more experience (Argote and Epple 1990). Therefore, a victim of the same kind becomes less attractive when a hacker's prior experience is concentrated, which may trigger variety seeking.

Each country or region would have their unique characteristic such as IT infrastructure, regulation for information security, and awareness of information security (Kshetri 2010). These characteristics determine the difficulties of penetrating into systems and the way attacks are made. A hacker who repeatedly attacks the same region would get very familiar with the characteristics and become proficient with it. Thus, the challenge for attacking the website would be reduced. That is, the perceived benefit (i.e. enjoyment, excitement, and gain in knowledge) from attacking the same region will decrease, and thus a hacker will be more likely to seek variety by attacking a new region. We hypothesize:

- Hypothesis 1a: A hacker is more likely to seek variety in terms of victim's region as their prior experience is more concentrated in particular regions.

Every operating system has its own characteristics including system facilities, vulnerabilities, design flaws, and architecture. Every operating system will require hackers to use different exploit and tools to initiate an attack (Arora et al. 2010; Arora et al. 2008; Ozment 2005). Targeting the same system constantly may cause a hacker to become satiated, and thus the hacker may need to seek variety to achieve the state of arousal. Attacking the same type of systems would offer fewer opportunities to test new skills, and thus variety seeking would be stimulated. We hypothesize:

- Hypothesis 1b: A hacker is more likely to seek variety in terms of victim's operating system as their prior experience is more concentrated in particular operating systems.

Hackers can employ different hacking methods such as SQL injection, server intrusion, and brute force attacks, when they compromise systems. All these different methods of attack require different techniques and skill sets. Similar to the case of operating systems, each attack method would use different exploit, tools and tasks. Repeatedly applying the same method would cause a hacker to feel bored eventually, and thus the hacker would want to seek variety to gain enjoyment from the novelty of new attack methods. Boredom would reduce the perceived benefits; in contrast, variety seeking would increase the learning benefit from novelty. We hypothesize:

- Hypothesis 1c: A hacker is more likely to seek variety in terms of the methods of hacking as their prior experience is more concentrated in particular methods of hacking.

Inter-attack Time Interval

The prior literature has shown that variety seeking behaviors may be resulted from an individual's response to changes in external situations. In the context of cyber attacks, the fast-moving information technology may make changes in the characteristics of alternative victims, changes in the set of feasible hacking techniques, or changes in the constraints facing a hacker. These external forces may drive down a hacker's perceived net benefit from repeatedly attacking victims possessing similar characteristics, and hence increase the likelihood of varied behavior. For instance, after a certain period of time since a hacker has made an attack, the vulnerabilities may be patched up in the system updates, and other vulnerabilities will be discovered and addressed. The patches will stop the attacker from using the exploit found on that particular operating system. The patches may also stop hackers from using the same attack methods because the vulnerabilities have been removed. Ozment and Schechter (2006) have suggested that frequent patching of the system has diminished the number of vulnerabilities found in the system in the long run (Ozment and Schechter 2006). Likewise, after a period of time, policy makers or managers will introduce new policy and regulation which would affect the IT infrastructure, security regulation, and security awareness.

It is notable that a hacker can accumulate knowledge about attacking systems in specific regions, compromising specific types of operating systems, and applying a certain types of hacking methods. While attacking a victim possessing the same characteristics as previous victims may be less costly due to learning, the changes in external environments mentioned above may make hackers more difficult to launch an attack by applying the same techniques as before. Taken together, as the time elapsed between the prior attack and the current attack, prior knowledge gained by cumulative experience becomes obsolete. Thus, a hacker is less constrained by his prior experience and free to seek variety at the similar cost to attacking previously acquainted regions and systems with familiar hacking methods.

Furthermore, learning occurs when the same tasks are repeatedly performed (Argote and Epple 1990), but individuals may forget the knowledge that they learned previously. Forgetting is facilitated especially when the task is not being carried out for a long time (Darr et al. 1995). The amount of knowledge forgotten in the task would depend on the time elapsed (Bailey 1989; Teyarachakul et al. 2011). Again, the productivity gain by prior experience is less binding, which leads to more variety seeking behaviors. Based on the discussions, we hypothesize:

- Hypothesis 2a: A hacker is more likely to seek variety in terms of region as the time elapsed since his previous attack becomes longer.
- Hypothesis 2b: A hacker is more likely to seek variety in terms of operating systems as the time elapsed since his previous attack becomes longer.
- Hypothesis 2c: A hacker is more likely to seek variety in terms of the method of hacking as the time elapsed since his previous attack becomes longer.

Research Methodology

Data Collection

We collected our data from Zone-h.org. Zone-h is a privately owned website that archives defaced websites based on defacers' self-report. Typically, once a hacker defaces a website, it notifies Zone-h about the details of the defacement incident through the Zone-h webpage. The reported information includes the URL of the defaced website, the reason for defacements (e.g., for fun, for political reasons, to be a best defacer, etc.), the hacking method (e.g., SQL injection, known vulnerability, etc.), the type of victim's operating systems (e.g., Linux, Solaris, Win XP, MacOS, etc.), and the notifier identity. The reasons for defacements, mode of hacking, and the operating systems types are chosen by a notifying hacker unit from drop-down lists that were pre-defined by Zone-h.org. The Zone-h's web server automatically captures the defaced webpage at the time of report. The captured webpage is manually verified by Zone-h's staff to rule out fake reports.

The original data collected from Zone-h contains 3,545,153 observations of 30,627 hacking units collected in the period from 29 February 2000 to 9 April 2010. To capture the data of the latest hacker behavior, we included only the hackers who joined in the most recent five years. Considering that a single server may host more than one website, defacement attacks that are made to the same IP address by the same hacker within 24 hours are considered mass defacementon a web server and counted as a single attack. In order to study the dynamics of choices over a certain period of time, we sampled the first 30 defacements since the hacking unit has made three defacements. That is, a sequence of 30 attacks from the 4th attack was included. This procedure is to make sure that the concentration of prior defacements can be properly coded. We finally had 1,946 unique hacker units in our dataset.

Variables Measurement

We construct three dependent variables related to variety seeking behaviors: variety seeking in terms region, operating systems, and hacking methods. The variety seeking variables are generated based on prior experience of the attacker. 0 is assigned if the attacker has any prior experience with a certain attribute (region, operating system, and hacking method) of the current defacement attack; 1 indicates that the attacker had no prior experience with the attribute of the current defacement attack. For example, if a hacker had defaced 10 websites hosted in North America and Europe and has just defaced a website in Europe again, his variety seeking in terms of region will be coded as zero; his variety seeking variables will be coded as one if he defaces a website hosted in Asia. In the dataset, there are six possible regions for a defaced website including North America, South America, Europe, Asia, Africa, and Australia. The regions were identified by matching the victim's IP addresses with the IP geolocation data obtained from MaxMind. Similarly, there are 39 and 29 different types of operating systems and hacking methods that can be chosen by a hacker from a drop-down list in Zone-h.

We use the Herfindahl-Hirschman Index (HHI) to measure the concentration in prior experience (Herfindahl 1950; Hirschman 1945). HHI is commonly used to measure the concentration in an industry, but is also often applied in other contexts. For example, the HHI of prior experience in terms of region is $ConcentrationRegion = \sum_{j=1}^{N} S_j^2$ where N is the number of categories (i.e., regions) and s_j is the share of region category j in prior attacks. Two other concentration variables (*ConcentrationOS* and *ConcentrationMode*) are coded in the same way.

The inter-attack time since last attack (*InterAttackTime*) is calculated by counting the number of days between the last and the current attack. We take logarithms to reflect a diminishing effect.

We include other control variables such as age, a set of dummies for calendar years (*y2005-y2009*), concentration in prior defacements in terms of reasons (*ConcentrationReason*), a set of dummies indicating different motivations for defacements (*Reason1-Reason6*) and log of the number of prior defacements made by the same hacker unit (*LogPriorExp*erience). Age is calculated by the number of years elapsed since the first defacement attack made by the hacker until the current defacement attack. Reason 1 through Reason 6 indicate "As a challenge," "Heh...just for fun!," "I just want to be the best defacer," "Patriotism," "Political reasons," and "Revenge against that website." The reason is unknown for some defacements and not recorded in the dataset. The variable for concentration of reasons in prior attacks is calculated using HHI. In addition to controlling for different motivations that hackers carry, we also control for a general stock of experience that a hacker unit possesses by *LogPriorExp*erience. In the learning literature, log of the number of cumulative experience is frequently used to account for the effect of prior experience (Argote and Epple 1990). This variable also controls for a possible reduction in the choice set as they gain more experience and fewer choices are left for variety seeking.

Model Development

Since the dependent variables have discrete binary values, the classical linear regression would not be suitable in analyzing this model. Instead, a panel logit model would be appropriate (Greene 2007). The probability density of variety seeking in terms of category k in the t-th defacement by hacker unit i is

$$\Pr(VS_{it}^{k} = 1 \mid X_{it}^{k}) = \frac{e^{\alpha_i^k + \beta^k X_{it}^k}}{1 + e^{\alpha_i^k + \beta X_{it}^k}} \quad (2)$$

where k = *{Region,OS,Mode}* represents a type of variety seeking ; α_i^k captures unobserved hacker-specific fixed effects; and $\beta^k X_{it}^k$ is the linear function of the hacker unit and temporal characteristics. For example, for VS_{it}^{Region}, variety seeking in terms of region is

$$\beta^{Region} X_{it}^{R} = \beta_1^{Region} \cdot InterAttackTime_{it}^{Region} + \beta_2^{Region} \cdot ConcentrationRegion_{it} + \beta_3^{Region} \cdot Controls_{it}^{Region} \quad (3)$$

For variety seeking in terms of operating systems and hacking methods, $ConcentrationRegion_{it}$ is simply replaced with $ConcentrationOS_{it}$ and $ConcentrationMode_{it}$, respectively. We use the fixed effects logit model for estimation.

Table 1. Descriptive Statistic of Variables for the First 30 observations per Hacker Unit

Variable	N	Mean	Std. Dev.	Min	Max
VS^{Region}	64,421	0.050	0.219	0.000	1.000
VS^{OS}	64,421	0.056	0.231	0.000	1.000
VS^{Mode}	64,421	0.114	0.317	0.000	1.000
ConcentrationRegion	64,421	0.586	0.196	0.200	1.000
ConcentrationOS	64,421	0.680	0.204	0.160	1.000
ConcentrationMode	64,421	0.550	0.305	0.066	1.000
InterAttackTime	64,421	0.640	1.007	0.000	7.287
LogPriorExperience	64,421	2.695	0.636	1.099	3.466
ConcentrationReason	64,421	0.643	0.278	0.143	1.000
Reason1	64,421	0.135	0.342	0.000	1.000
Reason2	64,421	0.317	0.465	0.000	1.000
Reason3	64,421	0.162	0.369	0.000	1.000
Reason4	64,421	0.186	0.389	0.000	1.000
Reason5	64,421	0.075	0.264	0.000	1.000
Reason6	64,421	0.089	0.285	0.000	1.000
Age	64,421	0.078	0.348	0.000	4.000
y2005	64,421	0.104	0.306	0.000	1.000
y2006	64,421	0.304	0.460	0.000	1.000
y2007	64,421	0.162	0.369	0.000	1.000
y2008	64,421	0.196	0.397	0.000	1.000
y2009	64,421	0.198	0.399	0.000	1.000

Estimation Results

The descriptive statistics for all the variables are shown in Table 1. The preliminary results are presented in table 2. The coefficients for dummy variables on reasons and years have been omitted for brevity. The results show that the hypotheses are well supported. The three equations for variety seeking in terms of region, operating systems, and hacking methods have the pseudo R^2 of around 0.15, 0.10 and 0.10.

All the concentration variables testing Hypothesis 1a to 1c have significant and positive effects on each type of variety seeking. For region variety seeking, the concentration of region in prior attacks (*ConcentrationRegion*) has a coefficient of 6.81; For operating systems variety seeking, the concentration of operating systems in prior attacks (*ConcentrationOS*) has a coefficient of 5.64; For variety seeking in hacking methods, the concentration of hacking methods (*ConcentrationMode*) has a coefficient of 2.21.

For all three models, we find a positive and significant effect of the inter-attack time since last attack (*InterAttackTime*). Overall, our empirical results are consistent with the hypotheses.

It is also notable that some dummy variables for reasons were significant in our results. Interestingly, hackers are least variety seeking when they deface as a challenge (Reason 1); they are least variety seeking in terms of hacking method when they deface due to patriotism (Reason 4); they are least variety seeking in terms of operating systems when they deface for fun (Reason 2).

As a robustness check, the model was re-estimated using a sequence of 50 observations (instead of 30). We have confirmed that the estimation of 50 observations shows similar results compared to the estimation with a sequence of 30 observations.

Table 2. Estimation Results

Variables	Hypothesis	Region Variety Seeking	System Variety Seeking	Hacking Method Variety Seeking
ConcentrationRegion	H1a	6.808*** (0 .197)		
ConcentrationOS	H1b		5.639*** (0.168)	
ConcentrationMode	H1c			2.210*** (0.134)
InterAttackTime	H2a-H2c	0.171*** (0 .019)	0.186 *** (0.016)	0.340 *** (0.013)
LogPriorExperience		-0.163*** (0.036)	-0.222*** (0.030)	-0.792*** (0.024)
ConcentrationReason		-0.131 (0.167)	-0.370* (0.148)	-1.191*** (0.134)
Age		0.053 (0.153)	0.024 (0.132)	-0.030 (0.093)
Number of Observations		53,717	58,280	52,162
Number of Hacker Units		1,792	1,946	1,740
Log likelihood		-8327.2191	-11130.008	-14941.828
Pseudo R^2		0.148	0.099	0.100

*Significant at 1 % ***, 5 % **, and 10% *. The numbers in parentheses are standard errors.*

Discussion and Implication

While it may appear more efficient to hack systems with prior experience, our study suggests that hackers do seek variety in terms of the profiles of their victims. It may appear more cost-effective to invest resources to protect their systems against more prevalent attacks and hackers. However, our study implies that decision makers in organizations and policy makers have to secure their systems against a more diverse set of hackers from different regions and backgrounds. Our findings highlight to managers and policy maker the importance of re-evaluating and revising the information security policy on a regular basis against hackers whose attack patterns are different from previously known ones. Furthermore, the variety seeking behavior hints that psychic benefit of committing cybercrime may change even in the short run, which has been implicitly suggested in the criminology literature (Clark and Davis 1995).

Our results on Hypothesis 2 indicate that hackers tend to engage in variety seeking after stopping for a long period of time. The main interest of policy makers is to deter hackers from making further attacks possibly by enforcing stricter regulations. Our finding suggests that if a hacker is not completely deterred and comes back after a certain period of time, it may become more difficult to identify and apprehend the hacker as the pattern of attacks may be different from previous ones. For example, hackers often leave their "signature" behind, which can be used in matching with previously known hackers.

One important limitation of our study is that the data are self-reported by hackers, and the accuracy of our results may be sensitive to any omitted reports. However, we believe that the data are reasonably accurate in that hackers conducting defacements report to Zone-h.org primarily to show off their skills and success. Our future model will address such a bias using the Heckman correction. In addition, our binary dependent variable to measure variety seeking may be limited in capturing every aspect of variety seeking behavior.

This study develops and conducts a preliminary test of a theoretical model that explains the variety seeking behaviors by hackers. To the best of our knowledge, this is the first attempt to examine a choice made by hackers in a longitudinal setting. We expect that this research would shed some light in understanding the behavior of hackers and their decision making. In the future, we plan to extend this research by identifying other factors that determine hackers' variety seeking while conducting more robustness checks. We will also extend our work to study the motivations of variety seeking. For example, variety seeking in regions may be more related to boredom than variety seeking in hacking methods which may be more influenced by learning benefits.

Acknowledgements

We thank for financial support from the Ministry of Education Academic Research Fund, NUS (R-253-000-089-112), and grant from the NSFC (71001042).

References

Argote, L., and Epple, D. 1990. "Learning Curves in Manufacturing," *Science* (247:4945), Feb, pp 920-924.

Arora, A., Krishnan, R., Telang, R., and Yang, Y.B. 2010. "An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure," *Information Systems Research* (21:1), Mar, pp 115-132.

Arora, A., Telang, R., and Xu, H. 2008. "Optimal Policy for Software Vulnerability Disclosure," *Management Science* (54:4), Apr, pp 642-656.

Bailey, C.D. 1989. "Forgetting and the Learning Curve: A Laboratory Study," *Management Science* (35:3), Mar, pp 340-352.

Becker, G.S. 1968. "Crime and Punishment: Economic Approach," *Journal of Political Economy* (76:2), pp 169-217.

Cardoso, L.S. 2007. "Cyber Crime and Critical Information Infrastructure Impact." International Telecommunication Union.

Claburn, T. 2008. "The Cybercrime Economy," in: *InformationWeek*.

Clark, J.R., and Davis, W.L. 1995. "A Human Capital Perspective on Criminal Careers," *Journal of Applied Business Research* (11:3), pp 58-64.

Clarke, R. 1999. "Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods," in: *Police Research Series Paper 112*. London: Home Office Policing and Reducing Crime Unit.

CSI. 2011. "Csi Computer Crime and Security Survey 2010/2011."

Darr, E.D., Argote, L., and Epple, D. 1995. "The Acquisition, Transfer, and Depreciation of Knowledge in Service Organizations: Productivity in Franchises," *Management Science* (41:11), Nov, pp 1750-1762.

Givon, M. 1984. "Variety Seeking through Brand Switching," *Marketing Science* (3:1), pp 1-22.

Greene, W.H. 2007. *Econometric Analysis*, (6th Edition ed.). Prentice Hall.

Harlam, B.A., and Lodish, L.M. 1995. "Modeling Consumers' Choices of Multiple Items," *Journal of Marketing Research* (32:4), Nov, pp 404-418.

Herfindahl, O.C. 1950. "Concentration in the U.S. Steel Industry." Unpublished doctoral dissertation: Columbia University.

Hirschman, A.O. 1945. *National Power and the Structure of Foreign Trade*. Berkeley : University of California Press.

Kahn, B. 1995. "Consumervariety-Seeking among Goods and Services: An Integrativereview," *Journal of Retailing and Consumer Services* (2:3), pp 139–148.

Karnow, C. 1994. "Recombinant Culture: Crime in the Digital Network." Computer Professionals for Social Responsibility.

Kaspersky, E. 2005. "Challenges We Face in Today's Cyber World," in: *AVAR 2005 Conference*. China.

Kshetri, N. 2006. "The Simple Economics of Cybercrimes," *IEEE Security & Privacy* (4:1), Jan-Feb, pp 33-39.

Kshetri, N. 2010. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer.

Mahmood, M.A., Siponen, M., Straub, D., Rao, H.R., and Raghu, T.S. 2010. "Moving toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue," *MIS Quarterly* (34:3), Sep, pp 431-433.

McAlister, L., and Pessemier, E. 1982. "Variety Seeking Behavior: An Interdisciplinary Review," *Journal of Consumer Research* (9:3), pp 311-322.

McGuire, W.J. 1976. "Some Internal Psychological Factors Influencing Consumer Choice," *Journal of Consumer Research* (2:4), pp 302-319.

Ozment, A. 2005. "The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting," in: *Workshop on the Economics of Information Security (WEIS 2005)*. Boston, U.S.

Ozment, A., and Schechter, S. 2006. "Milk or Wine: Does Software Security Improve with Age?," *Proceedings of the 15th USENIX Security Symposium*, Vancouver, B.C., Canada.

Png, I., Tang, C.Q., and Wang, Q.-H. 2006. "Hackers, Users, Information Security," in: *Workshop on Economics of Information Security (WEIS2006)*. England: pp. 1-22.

Ransbotham, S., and Mitra, S. 2009. "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research* (20:1), Mar, pp 121-139.

Sajeesh, S., and Raju, J.S. 2010. "Positioning and Pricing in a Variety Seeking Market," *Management Science* (56:6), Jun, pp 949-961.

Seetharaman, P.B., and Che, H. 2009. "Price Competition in Markets with Consumer Variety Seeking," *Marketing Science* (28:3), May-Jun, pp 516-525.

Sim, K.L., and Koh, H. C. . 2005. "An Empirical Investigation of Hacking Behavior," *The Review of Business Information Systems* (9:4), pp 41-58.

Teyarachakul, S., Chand, S., and Ward, J. 2011. "Effect of Learning and Forgetting on Batch Sizes," *Production and Operations Management* (20:1), Jan-Feb, pp 116-128.

Tonry, M., and Farirington, D. 1995. "Strategic Approaches to Crime Prevention," *Crime and Justice: A Review of Research* (19, Building a Safer Society: Strategic Approaches to Crime Prevention), pp 1-20.

Van Beveren, J. 2001. "A Conceptual Model of Hacker Development and Motivations," *Journal of E-Business* (1:2), pp 1-9.

Wang, Q., and Goh, K.Y. 2012. "Investigating Consumers' Variety Seeking Behavior in the Light of Online Reviews: An Individual Level Panel Analysis," *Proceedings of the 45th Hawaii International Conference on System Sciences*, Maui, Hawaii, pp. 3188-3197.

Young, R., Zhang, L., and Prybutok, V.R. 2007. "Hacking into the Minds of Hackers," *Information Systems Management* (24:4), pp 281–287.