Crime Pays If You Are Just an Average Hacker

Woohyun Shim
University of Trento
Povo, Trento - Italy
Email: woohyun@disi.unitn.it

Luca Allodi
University of Trento
Povo, Trento - Italy
Email: luca.allodi@unitn.it

Fabio Massacci
University of Trento
Povo, Trento - Italy
Email: fabio.massacci@unitn.it

***Abstract*—This study investigates the effects of incentive and deterrence strategies that might turn a security researcher into a malware writer, or vice versa. By using a simple game theoretic model, we illustrate how hackers maximize their expected utility. Furthermore, our simulation models show how hackers' malicious activities are affected by changes in strategies employed by defenders. Our results indicate that, despite the manipulation of strategies, average-skilled hackers have incentives to participate in malicious activities, whereas highly skilled hackers who have high probability of getting maximum payoffs from legal activities are more likely to participate in legitimate ones. Lastly, according on our findings, reactive strategies are more effective than proactive strategies in discouraging hackers' malicious activities.**

I. Introduction

There is widespread agreement that the high dependence on the Internet technology is causing a higher security risk to customers, businesses and the society as a whole. A wide variey of business models such as spam campaigns, botnets, identity theft and stealing credit card account information has been flourishing. The prevalence of this phenomenon led government agencies, international organizations and security vendors to make a concerted effort to develop several security policies against security threats. As a result, various policy tools and strategies have been proposed by researchers [1], [2] and have been enacted by governments (e.g., U.S. security breach notification laws and data protection laws) and supranational organizations (e.g. Seoul-Melbourne Anti-Spam Agreement and OECD Security Guidelines). While a range of policy tools and strategies continue to be developed to deal with this issue, most of them tend to be adopted without ascertaining the effectiveness. Moreover, few countermeasures are currently addressing the ever increasing issue of cybercrime markets [3], [4]. This study therefore investigate the effectiveness of possible policies and strategies focusing mainly on exploit markets in which tools, exploits and means to automatize cyber attacks are traded. Specifically, we use a scenario which features two players: a hacker, who needs to choose between legal activities (i.e., selling exploits to legitimate security vendors) and illegal activities (i.e. writing and selling an exploit kit in a black market), and a defender (i.e., a software vendor and a policy-maker) who needs to develop policies to mitigate hackers' illegal activities. In the analysis, we use a simple game theoretic model. We believe an exploit market is an appropriate target for the application of game theory, since it can assist in increasing our understanding of the effects of implemented security strategies on the decision making process of a hacker. The primary objectives of this study therefore are to:

1) Form a foundation for an analysis of a hacker's behaviour using game theory; we aim at explaining why illegal hacking behaviour is preferred to lawfully conforming behaviour.
2) Study how hacking technologies affect and are affected by changes in a game.
3) Investigate possibly effective strategies and policies to be enforced by government agencies and security vendors to deter hackers' malicious activities.

Our results show that, interestingly, hackers with an average skill are prone to participate in malicious cyber-activities; on the other hand, highly skilled hackers are more likely to engage in legitimate activities and disregard criminal ones. We also identify that, of an array of potentially effective strategic alternatives, directly reducing the returns from malicious activities is the only effective strategy for hackers both with a low-medium skill and with a high skill. Furthermore, our results confirm that policy makers should put more effort into reactive strategies than proactive strategies to mitigate hackers' malicious activities as indicated by Anderson et al. [5].

However, we should note that this study is only a first step toward a more complete modeling of cyber-perpetrators' actions and incentives for a variety of decision-making situations. The results presented in this paper are not to be intended as definitive, but rather as a starting point for more complete and articulated models for cybercrime. Nevertheless, we think our work provides interesting insights into the cyber-security environment, including interesting observations on which defensive actions are effective against strategic cyber-attackers. We also expect more empirical work to arise, hopefully, from our present discussion.

The remainder of the article is organized as follows: the next section reviews the previous literature. Section III develops a game-theoretic model and Section IV presents the results of our simulations. Lastly, discussion and limitations of this article are presented in Section V.

II. Literature Review

While many studies have recognized and have addressed the harmful effects of cyber-perpetrators' wrongdoings, few have studied policies and strategies that can mitigate cyber-perpetrators' malicious activities. Accordingly, a growing number of strategies and policies related to cyber-crime have been employed in recent years, without enough consideration of the effects of these on cyber-attackers. Furthermore, most of the studies that suggested measures for preventing security incidents have been concerned about potential victims' prevention activities rather than investigating solutions to mitigate cyber-perpetrators' criminal activities. In this section, we first discuss cyber black market economics that initially motivated this study, then explore studies related to the redress of malicious cyber-activities.

A. Cyber Black Market Economics

A first analysis of black market economics was addressed in [6] by Franklin et al. They analyzed the amount of credit card numbers, banking information, and Social Serial Numbers (SSNs) circulating in Internet Relay Chat (IRC)[1] markets for a period of 7 months. According to their estimations the market is worth, overall, about 100 Million USD. Moreover, they show that about 5 percent of the logged data concerns trading of compromised hosts.

However, Herley et al. are skeptical about the reliability of these results [7]. They show that IRC markets feature all the characteristics of a typical "market for lemons" [8]: the vendor has no drawbacks in scamming the buyer because of the absence of a unique-ID and of a reputation system. Moreover, the buyer cannot in any way assess the quality of the good (i.e. the validity of the credit card and the amount of credit available) beforehand. On a folkloristic note, indeed, IRC markets are well known, in the underground community, to be markets for "newbie" and wanna-be scammers [7]. There are underground markets other than IRC ones; Savage et al. [4] analysed the private messages exchanged in six underground forums. Most interestingly, their analysis shows that these markets feature the characteristics typical of a regular market: sellers do re-use the same ID, the transactions are moderated, and reputation systems are in place and seem to work properly.

Dealing with criminals and illegal underground activities can be not only difficult and prone to error, but interpretation of experimental results can also be tricky and sometimes misleading [7], [9]. Moreover, Anderson et al. in [5] showed that, when it comes to new crimes perpetrated through and thanks to the Internet, the investment to defend against them surpasses the gains for the attacker of one order of magnitude: traditional technical countermeasures and strict business-internal policies proved to be extremely expensive and unfruitful. This suggests that more efficient and practical policies and "reactive" practices should be considered when dealing with cybercrime (e.g. increasing the cost of attacks by putting the bad guys in jail).

In regards with these new forms of cybercrime, we are mainly interested in Exploit Kits: these are tools traded in the black markets [10] that, once deployed, attack the victim systems that try to connect to them. They are widely used by cybercriminals to, for example, build botnets. These attack techniques are very well explored in a foundational study from Provos et al. [11].

The economic returns for an attacker have been studied in literature as well. Kanich et al. analyze the return on investment for three spam campaigns [3] launched by the Storm botnet, and show that the conversion rate (i.e. number of times the victim "clicks" on the spammed link and goes through the trade process to buy the product) are extremely low. This low success rate is taken into consideration by Herley in [12]; he observes that attackers pay the cost of "false positives" as well (e.g. users that are accounted as victims but are not). As a result, the cost for an attacker steadily increases as the density of "vulnerable" users decreases. Therefore, to economise the attack process, the attacker needs to choose carefully the population of victims she is going to attack. For example, less unsuccessful attacks (false positives) mean less visibility, which means that attackers can minimize the chance of having the police knocking on their door.

B. Redress of Malicious Cyber Activities

There has been abundant research on individual criminal behavior. While the literature focused mostly on analyzing a general model of criminal behavior, Cornish & Clarke [13] started to study a crime-specific model. They argue that people's choice to participate in criminal activities might be very different according to what specific goal and act are taken into account. More recently, many studies have started to apply the previous models and findings to malicious behaviors in cyber-space. Of these studies, the most referred policies for mitigating illegal activities in cyber-space were the legal system. According to Lipton [14], despite several deficiencies, criminal laws could be the most effective way to deal with many malicious activities in cyber-space. He also points out that criminal laws that deal particularly with malicious cyber-activities should clearly state what constitutes cyber-crimes and avoid relying on an approach from a pre-Internet era.

Recent literature suggests several additional mechanisms that could prevent cyber-perpetrators' wrongdoings. Lipton [14] and Broadhurst [15] suggest to use education and training to foster morality which could lead users to behave in a socially acceptable manner by creating an internal sense of guilt and increasing moral satisfaction. Several researchers including Hennig-Thurau & Walsh [16], Kwok & Gao [17], Liu et al. [18] and Wang et al. [19] argue that monetary and economic rewards are one of the most important mechanisms that promote users' well behavior. They therefore conclude that the existence of the reward system which allows users to converts their activities into monetary rewards might increase their positive cyber-conduct. In designing a theoretical model, strategies and policies against various malicious cyber activities identified in the literature review are used as variables.

III. Game Theoretic Model for a Hacker's Behavior

Alongside with the literature review proposed in Section II, we base our model on our direct observation of the black

[1] IRC used to be a very popular channel for quasi-anonymous instantaneous interactions between users.

markets. With the purpose of getting a more detailed and precise idea of how *blackhat* trades and tools work, we monitored the activities of many black markets for more than 6 months. In this work, in particular, we are interested in one of the kinds of tools traded in these markets: Exploit Kits.These tools are usually licensed over a one-year period; prices may vary in between 1,500 USD and 2,500 USD per year. In our model, cyber-attackers act as utility maximizers evaluating various factors including penalties and rewards in perpetrating cyber-crimes. In particular we consider a utility function that allows cyber-offenders to allocate their time to illegal cyber-activities while considering potential benefits and costs resulting from their wrongdoings.

A. The Basic Model

We consider two types of players in the study: a hacker who can sell an exploit kit which includes various vulnerabilities, or can sell the vulnerabilities to legitimate vendors (e.g., Google's bug bounty program, tipping point initiative or exposing them in a black-hat conference to be hired as a penetration tester) and a defender (e.g., a policy-maker or a security vendor). We regard a hacker as a single decision making entity no matter who is an individual hacker or a hacking group and, throughout, we use he for a hacker. He faces uncertain situations and needs to make a choice from a set of available actions. Each of these actions has a different probability of yielding an outcome. We assume that a hacker will choose the action that is likely to produce the highest utility from monetary and nonmonetary rewards. Actual outcomes are then assumed to be the result of the interplay between the decisions made by a hacker and a defender.

Since exploit-kit markets consist of players with competing and conflicting interests, this study assumes that the players make an effort to maximize individual payoffs (i.e., a noncooperative form). In order to investigate the game, we adopt and extend the framework of traditional game theoretic models [20] used in the studies of Mesquita & Cohen [21] and Krebs et al. [22]. Specifically, the game we propose here posits that a hacker's decision is a function of the expected payoffs from the exploit kits and the opportunity cost from committing these malicious activities. In contrast, defenders are assumed to formulate strategies based on what they know about hackers and exploit kit markets to deter hackers from producing, spreading and selling their exploit kits.

Table I reports a sum-up of the variables and their respective meaning. First, we consider a hacker. He has total time, T, and is assumed to participate in only two activities, defined as malicious activities such as producing and selling exploit kits in black markets, and normal activities including the development of legitimate software, that are socially acceptable. Therefore, we denote a fraction of a hacker's total time devoted to normal activities as L and a fraction of his total time spent on malicious activities as I (i.e., $L = T - I$).[2]

We now consider a hacker's expected utility. We assume that, from legitimate activities, a hacker can achieve maximum benefit, B, with probability p. In contrast, with probability $1-p$, the hacker can achieve only minimum benefits, S which is smaller than B (i.e., $B > S$). It should be noted that B and S can be increased not only by incrementing monetary rewards from legitimate activities as suggested by Hennig-Thurau & Walsh [16], Kwok & Gao [17] and Liu et al. [18], but also by fostering morality or the intrinsic motivation to act legitimately as proposed by Liption [14] and Broadhurst [15]. The levels of p and $1-p$ are often considered to be influenced by the hacker's personal characteristics including education level and previous job experience. The hacker's expected utility from legitimate activities, therefore, can be expressed as

$$EU_N = L(pB + (1-p)S) \tag{1}$$

where $L = T$.

We now take into account the case where a hacker chooses to participate in malicious activities (i.e., writing an exploit kit and selling it in black markets). We denote q as the probability of an exploit kit developed by the hacker being detected and disabled by defenders. The returns to the malicious activities are determined by the benefits gained from the exploit kit, Z, the timing of the detection and disablement of the exploit kit, t, which is normalized to be $[0, 1]$ (i.e., $0 \leq t \leq 1$), and the costs to the hacker, C. Similarly with the benefits from legitimate activities, Z is an important factor that determines a hacker's behavior as explained by Wang et al. [19]. The costs to the hacker, C, is caused by the detection and disablement of the exploit kit, including the loss of reputation and the penalty from criminal laws considered by Lipton [14]. Three things should be noted: first, benefits and costs are not restricted to monetary payoffs and losses. These can also take the form of psychological rewards (e.g., self-esteem or self-confidence) and disappointment (e.g., a sense of sinfulness or guilt). Second, unlike the previous criminology research, since it is extremely difficult, if not impossible, to arrest a malicious hacker who develop an exploit kit [23], we assume that the hacker can still have the returns from his legitimate activities even after an exploit kit developed by him is detected and disabled by defenders. Lastly, unlike the previous literature, we include the time of the detection and disablement, t, in the model since the time has a high impact on a hacker's final payoffs. As a result, we define the returns from an exploit kit being detected as $(T-L)(Zt-C)+L(pB+(1-p)S)$. On the other hand, the probability of a hacker's exploit kit not being detected by defenders can be expressed as $(1-q)$. In this case, the returns are equal to $(T-L)Z + L(pB + (1-p)S)$. Putting it all together, a hacker's expected utility of committing malicious activities in line with the ideas of the time allocation can be denoted as

$$\begin{aligned} EU_M = q&[(T-L)(Zt-C) + L(pB + (1-p)S)] \\ &+(1-q)[(T-L)Z + L(pB + (1-p)S)]. \end{aligned} \tag{2}$$

As a result, if a hacker puts all of his time on malicious activities, the expected utility becomes $T(q(Zt-C) + (1-q)Z)$.

[2] We also assume that there is no cost for the movement between the activities.

Activity type	Variable	Meaning
General	T	hacker's total time
	t	time for detection and neutralization of criminal activity
	p	probability of obtaining maximum benefit from legal activities
	1-p	probability of obtaining only minimum benefit from legal activities
	q	probability of detection of the criminal activity
	q-1	probability of non-detection of the criminal activity
Legal	L	fraction of time the hacker devotes to legal activities
	B	maximum benefit gained from a legal activity
	S	minimum benefit gained from a legal activity
Criminal	I	fraction of time the hacker devotes to criminal activities
	Z	maximum benefit gained from a criminal activity
	C	cost for the hacker in perpetrating criminal activities

TABLE I
MAP OF VARIABLES AND THEIR MEANING IN THE MODEL

From these expected utility functions, we can use a game theoretic model to investigate a hacker's decision process.

In the game, a defender moves first, so as to decide whether to enforce security policies and strategies against the activities related to exploit kits. A hacker then should decide whether he will involve in normal activities or malicious activities. If the hacker chooses to participate in malicious activities, the defenders again have to decide whether or not to impose additional security policies and strategies to the hacker's behavior. To solve this game theoretic model, it is important to identify the equilibria of the game. These show us under which conditions a hacker is expected to choose his involvement between socially acceptable activities and malicious activities. Briefly speaking, a hacker determines whether malicious activities or socially acceptable activities will yield a greater expected utility. If he believes $EU_N \geq EU_M$, then socially acceptable activities will be selected. Otherwise, a hacker will start allocate his time to malicious activities.

B. A Hacker's Response to Parameter Shifts

In this subsection, we examine the hacker's supply shift of malicious activities in response to changes in strategies. Following Mesquita & Cohen [21] and Krebs et al. [22], we manipulate six possible remedies for malicious activities in the model: p, q, S, B, C and Z. In addition to these variables, we also propose manipulating the timing of the detection and disablement (t). This is because defenders (e.g., security vendors) can affect the value of an exploit kit by providing their customers with patches which can disable the exploit kit, or can shorten the timing of the detection of the exploit kit by monitoring exploit markets.

Our simulation adopts an approach used in the study of Krebs et al. [22]. In each simulation analysis, we normalize all the values of the variables to 1.00. We then fix all of the variables except for the value for the key variable being manipulated: other things being equal, the key variable whose effect is being simulated will increase from 0.05 to 1.00 by 0.05 steps. As pointed out by Krebs et al., while fixed values used in the previous studies might be appropriate for the purpose of each of them, some of the variables should be adjusted for the purpose of this study [22]. We therefore estimate the values of q, C, Z, B, t and L based on several months of explorations in the exploit markets while we follow the study of Krebs et al. [22] for the values of p and S at .5 and .3 respectively. As for q, it may be very low as explained in Verizon's 2012 report on data breaches investigations [24]. Moreover, cooperation between law forces is often difficult[3], and the rate at which an attacker can change the address of his exploit kit is way higher than its detection rate by lawful security researchers. As a result, we fix the value of q at 0.1. C may also be low since arrest of a hacker is quite hard and the actual arrest rate is very low [25], [26], [23]. While cyber-criminals face very severe penalties when caught[4], it is certainly hard to prosecute and apprehend them since they usually stay outside the reach of law enforcement [1]. Given this situation, we fix the value of C at 0.2.

As for Z and B, we consider two cases: In one case, we fix the values of Z at 1.0 and B at 0.8 ($B > Z$). In the other case, we choose the values of Z at 0.8 and B at 1.0 ($Z > B$). This is to compare different types of hackers: a hacker valuing self-esteem and altruism vs. a hacker valuing sense of superiority and dominance. While indeed regular criminals often act out of need (e.g. they don't have a satisfying social status or they don't have a job), cyber-criminals are seemingly often well-educated and financially stable members of the society [23]. Hackers are indeed well-known to often act for fun or for reputation [27]. Being hackers' motivation not strictly related to their condition in the society, but rather an "emotional state", we feel that we should distinguish between the two cases in which the hacker is *a)* lawful-but-curious and *b)* criminally-minded.

In addition to these values, we also estimate the values for t and L which were not introduced in the previous studies. As previously mentioned, the detection rate of exploits is traditionally very low. Exploit kits continuously change domain, therefore tracking them down and disabling them is a very hard if not impossible task [28]. In our observation of exploit markets, we found a number of Exploit Kits that

[3] http://nakedsecurity.sophos.com/2012/01/19/koobface-gang-servers-russia-police/, accessed July 05 2012

[4] http://www.darkreading.com/database-security/167901020/security/attabreaches/224200531/index.html, accessed July 05 2012

feature 5+ years old vulnerabilities at the time of release. We therefore conclude that the average time for the neutralisation of an Exploit Kit is very high: we set t to .9.

As for L, we fix the value of it at 0.9, meaning that the fraction of time they devote to the criminal activity is low (0.1). This is because most of the hackers have regular jobs [23] and exploit kits do not require much time or effort to be managed, once their development is complete and the final product marketed.

IV. Results

We now discuss the results of the simulation tests. In the simulation we let the variables p, q, S, Z change from 0.05 to 1 with 0.05 steps. When a variable doesn't change, it is fixed to the value identified above. We ran simulations for both $Z > B$ and $B > Z$. Unsurprisingly, we found that most of the strategies and policies for reducing malicious activities of a hacker do not work as intended by defenders when the hacker values the benefits from exploit kit development and marketing more than the benefits from legitimate activities ($Z > B$).[5] However, it confirms that lowering the value of Z is the only effective strategy for hindering hackers participating in malicious activities. These results correspond to those from Mesquita's foundational study from 1995 [21].

The results for the second case ($B > Z$) are reported in Table II. The first column indicates the changes of the key variable in increments of 0.05 ranging from 0.05 to 1.00. The columns of each simulation model show the results of the comparison between the expected utilities from normal activities and malicious activities (i.e., $EU_N - EU_M$). That is, these columns display whether the changes in the variable are likely to be effective for reducing malicious activities: **succeed** indicates that the key variable might be effective whereas a blank cell means that the changes in the key variable will not be effective. Note that the models with the changes in the values of C, B and t are eliminated from the table because all the changes in the variables are not effective for mitigating malicious activities.

Table II indicates that, in addition to the strategies for decreasing the value of Z, several other strategies that are not effective in the previous tests become effective for reducing malicious activities if a hacker values the benefits from lawful activities more than the benefits from malicious activities. In detail, Model 1 suggests that increasing the value of p will make normal activities more attractive than malicious activities. Model 1 also indicated that only highly skilled hackers (i.e., hackers with a high probability of getting the maximum benefits from legal activities) are likely to devote their resources to legitimate activities. Model 2 confirms that the increase in the value of q can be an effective strategy for reducing malicious activities while such a scenario is unlikely as explained above. Model 3 also suggests that the reduction of the gap between the minimum and maximum benefits from legitimate activities increases hackers' participation in legitimate activities. Lastly, Model 4 indicates that reducing the value of Z makes malicious cyber activities less attractive.

In sum, the simulation models suggest the followings: First, the only key variable which can be effective for hackers with either $Z > B$ or $B > Z$ is to reduce the value of Z. However, developing policies and strategies to reduce the value of Z might be difficult. While several researchers have suggested building legitimate "markets for vulnerabilities" for reducing the the value of Z [29], these market are not as well-activated and well-developed as originally intended [30]. Second, while shortening the timing of the detection and disablement of a security threat might be an effective tool for reducing malicious activities, it might do nothing to make hackers reduce their malicious activities. Third, it is identified that developing policies and strategies for hackers with $Z > B$ is more problematic than developing those for hackers with $B > Z$. That is, hackers who value the benefits from legitimate activities more than the benefits from malicious activities are likely to give up malicious activities by changing the values of p, q, S and Z; on the other hand, hackers who regard the benefits from malicious activities higher than the benefits from normal activities are still likely to participate in malicious activities even after the manipulation of the key variables except for Z. This result corresponds to the hackers' profiles reported in other articles and in the news [23][6,7]: since they are relatively young, these traffic hackers are more likely to participate in malicious activities motivated by thrill-seeking, feelings of addiction, peer recognition, boredom with the educational system and lack of money [27], [31].

V. Discussion and Future Research

Currently, most of the research on malware threats has been studied from a technical lens, and hence other domains such as economic and political perspectives have been largely ignored. Furthermore, the focus on the research is mostly on the targets of attacks rather than on strategies and policies that can mitigate criminal activities associated with malware. With this article we want to fill this gap in the literature by conducting a study on strategies and policies for reducing malicious cyber-activities from an economic perspective. The results of this study are therefore not to be intended as definitive: while many of our conclusions are, we believe, sound and promising for future research, more complete models are needed to design realistic and effective mitigation strategies.

However, some key insights identified in this work could be interesting pointers for future work. Specifically, our results show that only *very good programmers and professionals* who have high probability of getting maximum payoffs from legitimate activities *are not prone to engage in criminal activities*. Indeed, only when one's likelihood of getting maximum benefits from lawful activities rises we can expect the actor not to play maliciously. This implies that it is not only true that

[5] The table of the results is not presented here, but is available for the interested reader upon request.

[6] http://www.informationweek.com/security/management/amazoncom-ddos-attacker-busted-in-cyprus/240004073

[7] http://nakedsecurity.sophos.com/koobface/

Changes in key variable	**Model 1:**	**Model 2:**	**Model 3:**	**Model 4:**
	p changes	q changes	S changes	Z changes
0.05				**Succeed**
0.1				**Succeed**
0.15				**Succeed**
0.2				**Succeed**
0.25				**Succeed**
0.3				**Succeed**
0.35				**Succeed**
0.4				**Succeed**
0.45				**Succeed**
0.5				**Succeed**
0.55		**Succeed**	**Succeed**	**Succeed**
0.6		**Succeed**	**Succeed**	**Succeed**
0.65		**Succeed**	**Succeed**	**Succeed**
0.7	**Succeed**	**Succeed**	**Succeed**	
0.75	**Succeed**	**Succeed**	**Succeed**	
0.8	**Succeed**	**Succeed**	**Succeed**	
0.85	**Succeed**	**Succeed**	**Succeed**	
0.9	**Succeed**	**Succeed**	**Succeed**	
0.95	**Succeed**	**Succeed**	**Succeed**	
1	**Succeed**	**Succeed**	**Succeed**	

TABLE II
Simulation Results when $B > Z$. Z is fixed at 0.8 and B is fixed at 1.0.

one does not have to be a very good programmer in order to be a malicious hacker, but also true that a *very good programmer is not likely to be a malicious hacker*. Therefore,

1) Good policies that can increase the likelihood of achieving maximum returns from lawful activities would prevent the very good professionals from going rogue.
2) Policies could also be tuned to assure that only low-scale professionals are willing to "join the dark side". Accordingly, this would *decrease the quality of the attack tools* traded in black markets, and possibly their effectiveness in infecting machines and, for example, building botnets.

Another possible strategy is to increase the minimum benefits for a hacker ("S" in our model). This would encourage even "average skilled" hackers in joining legal activities rather than criminal ones.

Moreover, despite resulting from a completely different approach, our conclusions are in accordance with those of a recent study from Anderson et al. [5]: "response policies" is where policy makers should put more effort into: Increasing detection rates is an effective strategy to deter cyber-criminals from going rogue. We are, however, very far from achieving that goal: our model predicts a detection rate higher than 50% to be effective; in the current state of cyber-security, this is far from being accomplished. A more plausible strategy is to cleverly increase the minimum benefit for legitimate activities (S) in cooperation with higher detection rates (q): this may turn out to be an effective strategy in real-world scenarios.

In spite of the interesting findings, this study has some limitations that might offer additional avenues for future study and are important to underline here. First, our model doesn't cope with indirect effects of variables. For example, it is reasonable to think that a higher detection rate (b) would also increase the costs for the attacker C. These considerations are left for future work. one should recognise that, even with a well-crafted strategy for coping with malicious activities, its implementation might be problematic and therefore unrealistic. For example, an exploit provider may not be inside the jurisdiction where cyber-crime is committed [1]. Because the Internet can be accessed by anyone throughout the world, it might be very difficult, if not impossible, to apply strategies that are made for a specific country to other countries or to prosecute a foreign cyber-perpetrator. As a result, while this study can help in pointing policy-makers and security vendors toward theoretically supported strategies, it is clear that further investigation and additional empirical studies in the field are required. Moreover, the results of our model may change because of complementary or substitution effects between the key variables, or the expansion of the model. All of these issues are very interesting and critical points to be address in future work: we believe that the model presented in this paper can be a good candidate as a starting point for upcoming research in the field.

References

[1] M. Van Eeten and J. Bauer, "Economics of malware: Security decisions, incentives and externalities," OECD, Tech. Rep., 2008.

[2] M. Van Eeten, J. Bauer, H. Asghari, S. Tabatabaie, and D. Rand, "The role of internet service providers in botnet mitigation: An empirical analysis based on spam data," OECD STI Working Paper, Tech. Rep., 2010.

[3] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage, "Spamalytics: an empirical analysis of spam marketing conversion," in *Proc. of CCS'08*, ser. CCS '08. ACM, 2008, pp. 3–14.

[4] M. Motoyama, D. McCoy, S. Savage, and G. M. Voelker, "An analysis of underground forums," in *Proc. of IMC'11*, 2011.

[5] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in *Proc. of WEIS'12*, 2012.

[6] J. Franklin, V. Paxson, A. Perrig, and S. Savage, "An inquiry into the nature and causes of the wealth of internet miscreants," in *Proc. of CCS'07*, 2007, pp. 375–388.

[7] C. Herley and D. Florencio, "Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy," *Springer Econ. of Inf. Sec. and Priv.*, 2010.

[8] G. A. Akerlof, "The market for "lemons": Quality uncertainty and the market mechanism," *The Quarterly Jour. of Econ.*, vol. 84, pp. pp. 488–500, 1970.

[9] C. Kanich, N. Chachra, D. McCoy, C. Grier, D. Y. Wang, M. Motoyama, K. Levchenko, S. Savage, and G. M. Voelker, "No plan survives contact: experience with cybercrime measurement," in *Proc. of CSET'11*, 2011.

[10] Symantec, *Analysis of Malicious Web Activity by Attack Toolkits*, online ed., Symantec, Available on the web at http://www.symantec.com/threatreport/topic.jsp?id=threat_activity_trends&aid=analysis_of_malicious_web_activity, 2011, accessed on June 1012.

[11] N. Provos, P. Mavrommatis, M. A. Rajab, and F. Monrose, "All your iframes point to us," in *Proc. of USENIX'08*, 2008, pp. 1–15.

[12] C. Herley, "Why do nigerian scammers say they are from nigeria?" in *Proc. of WEIS'12*, 2012.

[13] D. B. Cornish and R. V. Clarke, "Understanding crime displacement: An application of rational choice theory," *Criminology*, vol. 25, no. 4, pp. 933–948, 1987.

[14] J. Lipton, "What blogging might teach about cybernorms," *Akron Intell. Prop. J.*, vol. 4, p. 239, 2010.

[15] R. Broadhurst, "Developments in the global law enforcement of cyber-crime," *Policing: An International Journal of Police Strategies & Management*, vol. 29, pp. 408–433, 2006.

[16] T. Hennig-Thurau and G. Walsh, "Electronic word-of-mouth: Motives for and consequences of reading customer articulations on the internet," *International Journal of Electronic Commerce*, vol. 8, pp. 51–74, 2003.

[17] J. S. Kwok and S. Gao, "Knowledge sharing community in p2p network: a study of motivational perspective," *Journal of Knowledge Management*, vol. 8, pp. 94–102, 2004.

[18] S. Liu, H. Liao, and Y. Zeng, "Why people blog: an expectancy theory analysis," *Issues in Information Systems*, vol. 8, no. 2, pp. 232–237, 2007.

[19] X. Wang, H. Teo, and K. Wei, "What mobilizes information contribution to electronic word-of-mouth system? explanations from a dual-process goal pursuit model," in *Workshop Association for Informational Systems, Oklahoma*, 2009.

[20] A. Dixit, S. Skeath, and D. Reiley, *Games of strategy*. WW Norton New York, 1999.

[21] B. B. D. Mesquita and L. E. Cohen, "Self-interest, equity, and crime controls: A game-tehoretic analysis of criminal decision making," *Criminology*, vol. 33, no. 4, pp. 483–518, 1995.

[22] C. P. Krebs, M. Costelloe, and D. Jenks, "Drug control policy and smuggling innovation: a game-theoretic analysis," *Journal of Drug Issues*, vol. 33, no. 1, pp. 133–160, 2003.

[23] G. IB, "State and trends of the russian digital crime market," Group IB, Tech. Rep., 2011.

[24] W. Baker, M. Howard, A. Hutton, and C. D. Hylender, "2012 data breach investigation report," Verizon, Tech. Rep., 2012.

[25] J. Baltazar, "More traffic, more money: Koobface draws more blood," TrendLabs, Tech. Rep., 2011.

[26] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *Proc. of NSPW'09*, ser. NSPW '09. ACM, 2009, pp. 133–144.

[27] O. Turgeman-Goldschmidt, "Hackers' accounts: Hacking as a social entertainment," *Social Science Computer Review*, vol. 23, no. 1, p. 8, 2005.

[28] C. Grier, L. Ballard, J. Caballero, N. Chachra, C. J. Dietrich, K. Levchenko, P. Mavrommatis, D. McCoy, A. Nappa, A. Pitsillidis, N. Provos, M. Z. Rafique, M. A. Rajab, C. Rossow, K. Thomas, V. Paxson, S. Savage, and G. M. Voelker, "Manufacturing compromise: the emergence of exploit-as-a-service," in *Proc. of CCS'12*. ACM, 2012, pp. 821–832.

[29] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, p. 610, 2006.

[30] C. Miller, "The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales," in *Proc. of WEIS'07*, 2007.

[31] P. Taylor, *Hackers: crime in the digital sublime*. Psychology Press, 1999.