Int. J. Inf. Secur. (2014) 13:1–14
DOI 10.1007/s10207-013-0206-9

REGULAR CONTRIBUTION

Portfolio optimization of computer and mobile botnets

Qi Liao · Zhen Li

Published online: 18 August 2013

Abstract Botnet, a network of compromised computers controlled by botmasters, can perform various forms of malicious attacks and has emerged as one of the top security problems yet to be solved. Traditionally, botmasters have been focusing on herding computers. As mobile computing devices such as smart phones and tablets are becoming increasingly popular, there are more targets exposed to hacking risks. While technical approaches have so far received limited results, we study the botnet problem from an alternative angle, i.e., economic perspectives of botnet industry. In this paper, we play devil's advocate and think from the perspective of botmasters, i.e., how botmasters can evolve to maximize their profits in response to changing technologies. We adopt the concept of portfolio management, in which botmasters run their business through maintaining an optimal portfolio of PC and mobile devices to diversify risk and maximize profits of entire botnet industry. On the other hand, users may also maximize their utility function by keeping an optimal portfolio of network activities and data on their computers and mobile devices. The strategic playing by botmasters and users is modeled in a game theoretical framework. Various equilibrium solutions are discussed in terms of their welfare implications to botmasters and users. Understanding the optimal portfolio choice by botmasters provides insight for defenders, especially with evolving and diversified computing environments.

Q. Liao (✉)
Department of Computer Science, Central Michigan University, Mount Pleasant, MI 48859, USA
e-mail: liao1q@cmich.edu

Z. Li
Department of Economics and Management, Albion College, Albion, MI 49224, USA
e-mail: zli@albion.edu

Keywords Botnet · Mobile · Portfolio management · Security · Economics · Game theory · Optimization

1 Introduction

Botnet, a network consisted of compromised computers known as "bots" or "zombies," has become an increasing security concern [1–4]. Computers could be hacked and controlled by botmasters through malicious software (malware), ranging from carelessly running binaries from email attachments, to installing application software from untrusted sources, or to simply viewing a flash on a website. A wide spectrum of malicious activities can be carried out by botnets, e.g., sending out spam and automated ad clicks, stealing passwords and financial account information, and/or launching large-scale distributed denial-of-service attacks (DDoS) [5]. In the past decade, botnets have evolved into sophisticated distributed systems comprising millions of computers with decentralized control [6]. Zombie computers nowadays are ranked the single largest threat facing network services availability and operational security [2].

While computers remain the dominant platform for botnets, the increasing popularity of wireless and mobile computing devices makes them more attractive targets for botmasters. Cellular phones, especially smart phones, are not just devices to make phone calls, but share many functions as computers with their own operating systems (e.g., Apple's iOS, Google's Android, Symbian, BlackBerry, Windows 8/mobile series and Linux) and wireless Internet connections (e.g., 3G, 4G/LTE, WiMAX, Wi-Fi and Bluetooth). The highly capable mobile devices, most notably iPads and Android-based tablets, are rivaling PCs as the dominant Internet platform. Even eReaders such as Amazon Kindle and Barnes and Noble Nook may potentially run additional appli-

cations. The increasing user activities on mobile devices raises inevitable security concerns about the vulnerabilities of mobile devices [7–19].

The research on botnets has been largely focusing on technical analysis such as honeypots/honeynets [2,20,21], malware and vulnerability analysis [6,9–12],attack simulations [13–15], or command & control channels (C&C) [17–19,22]. Nevertheless, technical defenses miss the root cause of the botnet challenge, i.e., financial incentives. As more and more botnet-based attacks are driven by money [5,23–30], economic principles provide promising alternatives to deal with the botnet issue. Nevertheless, facing the threat of emerging mobile botnets, little is known about the effects mobile botnets may have on the overall health of the botnet economy. For example, how do money-seeking attackers choose which targets PC or mobile devices? How may PC and mobile users be affected by the changing behaviors of botmasters? Many other interesting questions can also be asked regarding the possible coexistence of PC and mobile botnets.

In this paper, we study how money-driven botmasters would choose to herd between PC and mobile botnets. We play devil's advocate and think from the perspective of botmasters, i.e., how botmasters can evolve to the emerging technologies in order to maximize their profits as an industry. In particular, we propose an interesting concept of *portfolio management* for botnet business, in which botmasters run their business through maintaining an optimal portfolio of the traditional computer botnets[1] and the emerging mobile botnets to reap the highest possible payoffs. Modeled in a game theoretical framework, users on the other hand also maximize their utility function by keeping an optimal portfolio of network activities and data on computers and mobile devices. Three cases of equilibria [31] are derived and discussed; in each case, botmasters' optimal portfolio includes PC botnets only, mobile botnets only, and a mix of PC and mobile botnets, respectively. In particular, the equilibrium in which only PC botnets are present is proved optimal from the perspective of users. To achieve such equilibrium, security of mobile devices should be assigned higher priority relative to PCs by defenders when facing the trade-off between user convenience and security. Through modeling the strategic playing by botmasters and users with game theoretical analysis and optimal portfolio analysis, our work helps security defenders prioritize their tasks to fight botnets more effectively.

The rest of the paper is organized as follows. Section 2 presents the base model (PC botnets only) and an extended model (PC and mobile botnets), and defines the optimization problem for both profit-maximizing botmasters and utility-maximizing users. We derive and discuss the significance of three equilibria in Sect. 3 and prove one of the equilibrium is optimal for users while botmasters are likely better off in other cases. Section 4 further illustrates the implications of the model via numerical simulation study, which visually examines how the decision variables and strategies affect the economic welfare of botmasters and users in terms of whether they are better off or worse off. In Sect. 5, we provide background information of botnets and discuss related work. We also survey and compare current research on the economic, optimizing and game theoretical approaches on botnet security. We conclude our paper in Sect. 6 with suggestion for future research.

[1] Throughout the paper, the terms "computer botnets" and "PC botnets" are used interchangeably.

2 Botnet portfolio

In this section, we formulate the *optimization problem* for both botmasters and users, i.e., how botmasters construct their botnet portfolio to reap the highest possible profit, and how users maximize their utility function by controlling activities on computers and mobile devices. A base model where only PC botnets exist is first developed. The base model is then extended to study the optimal decision-making by botmasters at the presence of both PC and mobile botnets.

2.1 Base model

As a starting point, we first lay out the base model in the absence of mobile botnets, i.e., only PC botnets are available. The optimal decision-making by botmasters can be modeled as the *optimization problem* for a typical botmaster to maximize his expected profit in Eq. (1):

$$\max_{\beta_p} E[\pi] = \beta_p \left\{ P_p(A) \cdot (R_p - C_p^o) - C_p^a \right\} \quad (1)$$

where $E[\pi]$ is the expected profit of the botmaster. A few key variables in the model are defined in Table 1.

2.1.1 Botnet revenue

Without loss of generality, the revenue model of botmasters (R) includes botmasters' revenue from stealing data (R^d) and attacking others (R^e), i.e., $R = R^d + R^e$. Confidential information stored on users' computers and mobile devices can be valuable to cybercriminals [25,26]. Compromising a computer or mobile device allows botmasters to steal data from the machine, including financial data such as bank accounts and credit card numbers, and other data such as social security numbers (SSN), email addresses, passwords, bank accounts and financial information, and other sensitive information. The *revenue from data* is denoted by R^d. Throughout the paper, subscripts p and m denote PCs and mobile devices, respectively, e.g., R_p^d means the per-bot data revenue from

Table 1 Summary of key variables in the botnet profit optimization model

R^{d}	Botmasters' revenue from harvesting data on bots (bank accounts, passwords, etc)
R^{e}	Botmasters' revenue from machine deployment (DDoS, Spam, etc)
C^{a}	The acquisition cost of compromising machines
C^{o}	The operation cost of maintaining botnets
A	User activity level (e.g., the number of applications installed, the frequency of financial transactions, the amount of data exchanged and stored on computers and mobile devices)
P	The probability of compromising a computer or a mobile device into the botnet
β	The botnet portfolio composition parameter measured by the likelihood for the botmaster to hack a particular machine
α	The percentage of user activity conducted by a computer or a mobile device
p, m	Subscripts denoting PC botnets or mobile botnets

compromising a PC and $R^{\mathrm{d}}_{\mathrm{m}}$ means the per-bot data revenue from compromising a mobile device. Data will continue to be the primary motivation behind cybercrimes—whether targeting traditional fixed computing or emerging mobile applications [32].

Nevertheless, stealing data is not the only use of bots. The bots can also be used to attack others and continue to generate revenue for botmasters [33]. For example, bots can be rented to launch a large-scale *distributed denial-of-service* (DDoS) attack. Traditional DoS attacks are magnitude based. A few attacker machines make a large number of SYN packets (flooding) in order to exhaust bandwidth resources. Such attacks are usually easy to detect and be filtered. In botnet-based attacks, all connection requests are legitimate that complete TCP handshakes and download objects, and are very hard to mitigate. Such attacks target server resources (much like flash crowd), i.e., network services get too overwhelmed in dealing with attackers' traffic to serve legitimate users. DDoS attacks can be launched by unfair business competitors, political dissidents, or for various blackmail/extortion purposes.

Besides DDoS, another important use of botnets is to send unsolicited commercial emails (*spam*) and *phishing* messages. More than 90 % of all emails circulating on the Internet are spam, and 80 % of spam is sent via zombie networks [25]. Botnets can provide an implementation of fast flux technology that allows cybercriminals to change website IP addresses without affecting the domain name, which extends the lifetime of phishing sites. Even a tiny percentage of responses from unsuspicious users to the vast number of spam/phishing messages will generate significant revenue for botmasters.

Last but not least, botnets can also be used to do *fraudulent ad clicks*. Online advertising agencies often use the pay-per-click (PPC) scheme to pay for unique clicks on advertisements. Such clicks are fraudulent when clicks on an ad have no genuine interest or intention of providing the advertiser any value. Profit-driven advertisement sub-syndicators for tier-one search engines may hire botmasters to automate ad clicks to increase their commission revenues. Botnets can also be used to inflate a web resource by creating links to the site being promoted to improve the website's position in search results, so that it gets more visitors via search engines. Botmasters get paid by owners of the website being promoted. All the above botnet *revenue from deployment* is denoted by R^{e}.

2.1.2 Botnet costs

We assume botmasters have limited resources. If botmasters had unlimited resources, there would be no upper bound of the botnet size botmasters could operate. Like any other business, in order to generate revenue, there must be costs (although very small) associated with botnets. The cost function of botmasters includes the *acquisition cost* (C^{a}) and the *operation cost* (C^{o}). The *acquisition cost* is botmasters' opportunity cost of time and money spent on writing codes or purchasing malicious software (malware) to compromise machines. The *operation cost* of maintaining botnets includes using either centralized (IRC) or decentralized (P2P) command and control (C&C) channels to control and update bots.

2.1.3 Profit-driven botmasters

We assume botmasters are profit-driven since financial motivations lie behind most cybercrimes and security-related Internet threats [5,23–30]. Botmasters allocate limited resources (C&C channels, energy, money, etc.) to manage PC botnets and mobile botnets to reap the maximum possible profit. In the base case where mobile devices are absent, profit-driven botmasters will herd PC botnets if and only if the expected profit is non-negative. That is, the optimal choice of the hacking probability for botmasters is

$$\beta_{\mathrm{p}} = \begin{cases} 1, & \text{if } P_{\mathrm{p}}(A)\cdot(R_{\mathrm{p}} - C^{\mathrm{o}}_{\mathrm{p}}) \geq C^{\mathrm{a}}_{\mathrm{p}}, \\ 0, & \text{if } P_{\mathrm{p}}(A)\cdot(R_{\mathrm{p}} - C^{\mathrm{o}}_{\mathrm{p}}) < C^{\mathrm{a}}_{\mathrm{p}}. \end{cases}$$

It has been widely recognized that the costs of herding and operating botnets tend to be much smaller compared to the potential gains of operating botnets and are likely to be ignored by botmasters. Moreover, the cost associated with herding botnets is implicitly taken into account by varying the compromise probability P. For instance, better protected machines are less likely to be compromised successfully (equivalent to a decrease in the compromise probability), and thus making it more *costly* for botmasters to herd botnets of

any given size. Due to the general belief that the costs of botnets tend to be trivial, in the rest of the analysis, we drop the cost component from botmasters' profit function, thus maximizing the *expected profit* and maximizing the *expected revenue* are equivalent to botmasters. In particular, as $C^{\mathrm{o}} \to 0$ and $C^{\mathrm{a}} \to 0, \beta_{\mathrm{p}} \to 1$. It is therefore reasonable to conclude that all botmasters herd PC botnets in the base case, i.e., $\beta_{\mathrm{p}} = 1$.

As above, in the absence of mobile devices, the decision-making by botmasters is essentially independent of how extensively and intensively users conduct network activities on computers. Since the costs of herding and maintaining botnets are small, the revenue-generating capabilities of PCs dominate, hence botmasters would all herd PC botnets.

2.1.4 Users

Without loss of generality, we assume users' goal is to maximize their *utility* (an economic term that measures happiness or satisfaction) from their usage of computing devices. The utility function of users is the difference between the welfare of using computer applications and the potential loss from compromised machines.

In the base model where users use only computers for network activities, users choose the overall level of activities to maximize their expected utility of using computers, i.e., $\max_A E[U(A)] = W \cdot f(A) - \beta_{\mathrm{p}} \cdot P_{\mathrm{p}}(A) \cdot R_{\mathrm{p}}^{\mathrm{d}}$, where $E[U(A)]$ is the expected utility. $W \cdot f(A)$ is the welfare received from network activities and W is a positive constant. The function $f(A)$ is increasing and concave ($f' > 0$, $f'' < 0$), reflecting a positive but diminishing marginal utility for users. Users' potential loss from hacked machines depends on the probability botmasters determine to attack a particular machine, the likelihood the machine is successfully compromised and the direct loss suffered by the user (e.g., data) from the compromised machine. Since machine deployment (e.g., ad clicks) usually does not cause direct monetary loss to users, botmasters' revenue from machine deployment is not included in users' utility function. Therefore, the game between botmasters and users is not zero-sum meaning the botmasters' revenue and the users' loss are not equal. Since botmasters herd computers for certain in the base case ($\beta_{\mathrm{p}} = 1$), the objective utility function of users becomes

$$\max_A E[U(A)] = W \cdot f(A) - P_{\mathrm{p}}(A) \cdot R_{\mathrm{p}}^{\mathrm{d}}(A). \tag{2}$$

2.1.5 Activity and vulnerability

The likelihood for a machine to be compromised is positively related to the user activity level. Intuitively, if a machine has zero application service running, not connected to the Internet, with no sensitive data stored, such a machine is of least interest to hackers. On the other hand, the chance of installing malware to a machine increases if the machine is more often connected to the Internet, or is used more frequently to download games from untrusted sources. User activity refers to factors such as the number of applications installed, the number of financial transactions conducted and the amount of data stored or exchanged. It is reasonable to assume the data revenue of botmasters is positively related to the network activities carried out by users on their machines. As in the user utility function (2), the user utility is increasing in the level of user network activities. Botmasters' expected revenue from stealing user information is also increasing in the level of user network activities. Users face the trade-off between convenience/usability and security.

Given the security level of machines, we define the probability function $P(A) \in [0, 1]$ as the likelihood for botmasters to successfully compromise a machine that is increasing and concave in user activity (i.e., $P' > 0$, $P'' < 0$), showing the diminishing marginal increase in the likelihood of compromise as network applications increase. $P(\infty) = 1$ corresponds to zero security level while $P(0) = 0$ corresponds to a hypothetical perfectly secure system.

2.2 Extended model

Things become complicated when mobile botnets enter the market in addition to PC botnets. What are the effects of the coexistence of PC and mobile botnets on botmasters' decision-making? Are botmasters and users better off or worse off as a result? What is the overall impact on the botnet economy?

To study these issues, we introduce a *portfolio management* scheme that catches the trade-off between financial gains and uncertainties faced by botmasters. Under the scheme, botmasters choose the distribution of their limited resources across computers and mobile devices to construct a portfolio composed of PC and mobile botnets in order to maximize the expected profits. To make the scenario even more interesting, we put the botnet portfolio management in the setting of a game theoretical framework to capture the interdependence of the choices made by botmasters and by users. Money-driven botmasters choose the best responses depending on the network activity diversification strategies chosen by users.

2.2.1 The optimization problem for botmasters

Equation (3) defines the maximization problem for botmasters to choose the optimal botnet portfolio composition including PC and mobile botnets.

$$\begin{aligned} \max_{\beta_{\mathrm{p}}, \beta_{\mathrm{m}}} E[R] = {} & \beta_{\mathrm{p}} \cdot P_{\mathrm{p}}(\alpha_{\mathrm{p}} A) \cdot R_{\mathrm{p}} \\ & + \beta_{\mathrm{m}} \cdot P_{\mathrm{m}}(\alpha_{\mathrm{m}} A) \cdot R_{\mathrm{m}} \\ \text{s.t.} \quad & \beta_{\mathrm{p}} + \beta_{\mathrm{m}} = 1, \end{aligned} \tag{3}$$

where $E[R]$ is the expected revenue generated by the botnet portfolio of botmasters.

Also in this optimization problem, the maximization of the *expected revenue* is equivalent to the maximization of the *expected profit* when both cost components of botmasters' profit function approach to zero.

In contrast to the base model, the decision variables of botmasters are the probabilities to attack computers (β_p) and mobile devices (β_m). Since computers and mobile devices run different operating systems on different architecture, codes written for computers are normally not readily applicable to mobile devices, and vice versa. It is therefore reasonable to assume that botmasters view PC botnets and mobile botnets as imperfect substitutes, and have to determine the best resource allocation between PC and mobile botnets.

Also different from the base model, in the coexistence model, botmasters' optimal decision-making depends on users' distribution of network activities between computers and mobile devices. Generally, the attractiveness of a machine to botmasters (in terms of vulnerability to attacks and financial rewards once compromised) increases as more network activities are completed by the machine. The percentages of users' network activities completed by computers and mobile devices are defined as α_p and α_m, respectively, where $\alpha_p + \alpha_m = 1$. Accordingly, $P_p(\alpha_p A)$ and $P_m(\alpha_m A)$ represent the probability for botmasters to successfully compromise a computer or a mobile device, respectively. P_p and P_m differ for various reasons. First, PC and mobile devices have dramatically different architectures and operating systems, intensified by multiple vendors. Second, the online behavior of users tends to be different when using computers or mobile devices. For example, home PCs follow diurnal patterns and are usually shut down at night. Smart phones may be on 24/7 thus increasing the exposure to attacks. Third, the human–computer interaction (HCI) design for mobile devices is usually restricted, making users much more likely to choose easy passwords or save passwords on devices.

The strategy variables β and α define the interplay by botmasters and users, which affects botmasters' revenue. The distribution of user activities between computers and mobile devices is essential because it directly affects users' risks of using various machines. For example, users may send emails and do e-commerce or e-banking exclusively on computers or mobile devices. They may also divide up those online activities in any matter between computers and mobile devices. How much information is leaked depends on the different uses of the machines and the applications used for those purposes. Assume users' potential loss from data stealing is evenly distributed across applications, $R_p^d = \alpha_p R^d$ and $R_m^d = \alpha_m R^d$ would be botmasters' gains from compromising computers and mobile devices, respectively. Once β_p and β_m are chosen, the *expected weights* of PC and mobile botnets in botmasters' botnet portfolio are determined accordingly, i.e., $\{\beta_p \cdot P_p(\alpha_p A) \cdot R_p\}/E[R]$ for PC and $\{\beta_m \cdot P_m(\alpha_m A) \cdot R_m\}/E[R]$ for mobile botnet, respectively.

2.2.2 The optimization problem for users

At the presence of both PC and mobile devices, users' expected utility is derived from using both types of machines:

$$\max_{A,\alpha_p,\alpha_m} E[U] = E[U_p(\alpha_p, A)] + E[U_m(\alpha_m, A)] \quad \text{s.t.} \quad \alpha_p + \alpha_m = 1 \tag{4}$$

Assuming separable additivity, users' total expected utility $E[U]$ is the sum of two separate expected utilities, $E[U_p]$ and $E[U_m]$, where $E[U_p(\alpha_p, A)] = W_p \cdot f(\alpha_p A) - \beta_p \cdot P_p(\alpha_p A) \cdot \alpha_p \cdot R^d$ is users' expected utility of using computers, and $E[U_m(\alpha_m, A)] = W_m \cdot f(\alpha_m A) - \beta_m \cdot P_m(\alpha_m A) \cdot \alpha_m \cdot R^d$ is users' expected utility of using mobile devices.

3 Equilibrium analysis

This section solves the optimization problems modeled in the previous section and considers the steady state equilibria of the game between botmasters and users. The discussion centers around the key decision variable β^* which is the botmasters' optimal portfolio composition factor of herding PC and mobile botnets. Three possible combinations of the botmasters' portfolio exist: Case-I (PC botnets only), Case-II (mobile botnets only) and Case-III (mixture of PC and mobile botnets), as discussed in the following sections.

3.1 The Case-I equilibrium

The scenario in the Case-I equilibrium is that botmasters do not herd mobile botnets and stay with PC botnets. The optimal choice for botmasters is

$$\beta_p^* = \begin{cases} 1, & \text{if } P_p(\alpha_p A) \cdot R_p \geq P_m(\alpha_m A) \cdot R_m, \\ 0, & \text{else.} \end{cases} \tag{5}$$

The Case-I equilibrium is the equilibrium solution of the game if $P_p(\alpha_p A) \cdot R_p \geq P_m(\alpha_m A) \cdot R_m$ for all botmasters, making herding PC botnets always more profitable than herding mobile botnets for any botmaster.

In the Case-I equilibrium, money-driven botmasters are not as interested in herding mobile botnets as with PC botnets. Hence, when users use both computers and mobile devices for online activities, the expected payoff of botmasters is

$$E[R] = P_p(\alpha_p A)(\alpha_p R^d + R_p^e) \tag{6}$$

which is smaller than $P_p(A)(R_p^d + R_p^e)$, botmasters' payoff in the bench model where users use only PCs for online

activities. Therefore, in the Case-I equilibrium, botmasters' expected payoff decreases when compared with the base model in which only PC botnets exist. Users are instead better off compared with the base model as mobile devices allow users to diversify network activities and hence risks.

3.1.1 Proof of optimality

The significance of equilibrium in game theory is that any party who unilaterally deviates from the equilibrium strategy is only worse off. Nevertheless, the equilibrium solution is not necessarily optimal. In this section, we prove that the Case-I equilibrium is the *optimal* equilibrium solution for *users* of all the three possible solutions since users are harmed less when botmasters choose to herd only PC botnets.

As botmasters stay with PC botnets, i.e., $\beta_p = 1$ and $\beta_m = 0$, the users' optimal level of network activities (denoted as A^*) solves the following optimization problem for any given α_p and α_m:

$$\max_A E[U] = W_p \cdot f(\alpha_p A) + W_m \cdot f(\alpha_m A) - P_p(\alpha_p A) \cdot \alpha_p R^d. \quad (7)$$

While in the base model, the users' optimal level of network activities (denoted as $\tilde{A}$) satisfies the following first-order condition by solving Eq. (2):

$$W \cdot f'(\tilde{A}) = P_p'(\tilde{A}) \cdot R_p^d, \quad (8)$$

where the left-hand side and the right-hand side are the marginal benefit and the marginal cost of user network activities, respectively. For example, if $f(A) = \sqrt{A}$ and $P_p(A) = 1 - \frac{1}{\sqrt{1+A}}$,[2] from Eq. (8), the users' optimal choice of network activities satisfies

$$\frac{(1+\tilde{A})^3}{\tilde{A}} = \frac{(R_p^d)^2}{W^2}. \quad (9)$$

Next, let us move to the scenario when botmasters herd both PC and mobile botnets. Let $P_p(\alpha_p A) \cdot R_p = P_m(\alpha_m A) \cdot R_m$. Since $\alpha_p + \alpha_m = 1$, $R_p = \alpha_p R^d + R_p^e$ and $R_m = \alpha_m R^d + R_m^e$, the optimal distribution of user network activities between computers (α_p^*) and mobile devices ($\alpha_m^* = 1 - \alpha_p^*$) can be found by solving the following equation given A:

$$P_p(\alpha_p^* A) \cdot (\alpha_p^* R^d + R_p^e) = P_m((1-\alpha_p^*)A) \cdot ((1-\alpha_p^*)R^d + R_m^e). \quad (10)$$

[2] The commonly used square root utility function satisfies both increasing and concave properties of utility. The specified probability function is increasing in user activity level and generates probability values ranging between 0 and 1. The theoretical proof of optimality does not depend on the specified functional forms.

To sum, the optimal user strategy (defined by $\{A^*, \alpha_p^*, \alpha_m^*\}$ that solve the users' utility maximization problem) can be derived from Eqs. (7) and (10) simultaneously.

At $f(A) = \sqrt{A}$ and $P(A) = 1 - \frac{1}{\sqrt{1+A}}$, A^* can be found by solving the below first-order condition of Eq. (7).

$$W_p \alpha_p^* (\alpha_p^* A^*)^{-1/2} + W_m \alpha_m^* (\alpha_m^* A^*)^{-1/2} = \alpha_p^* R^d (1 + \alpha_p^* A^*)^{-3/2}. \quad (11)$$

Note at $\alpha_p^* = 1$, the first-order condition is the same as in the base model.

Suppose users have the same preference over computers and mobile devices so that $W_p = W_m = W$. By taking the ratio of (8) and (11), we can derive the relative size of the optimal network applications as

$$\frac{A^*}{\tilde{A}} = \frac{(1+\alpha_p^* A^*)^3}{(\alpha_p^*)^2 (1+\tilde{A})^3}. \quad (12)$$

By comparing (7) with (2), we show that users are better off in the Case-I equilibrium than in the base model as follows.

Let $W_p = W_m = W$, the expected utility of users in the Case-I equilibrium is

$$E[U] = W\left\{f(\alpha_p^* A) + f(\alpha_m^* A)\right\} - \alpha_p^* R^d \cdot P_p(\alpha_p^* A). \quad (13)$$

Since the utility function $f(\cdot)$ is concave, $f(\alpha_p^* A) + f(\alpha_m^* A) > f(A)$ where $\alpha_p^* + \alpha_m^* = 1$. In addition, $\alpha_p^* R^d < R^d$ and $P_p(\alpha_p^* A) < P(A)$. That is, by diversifying network activities across computers and mobile devices, users are better off by having both increased activity level and reduced direct loss from information leakage, thus receiving larger expected utility compared to the base model.

3.2 The Case-II equilibrium

In the Case-II equilibrium, botmasters spend all their resources on mobile botnets. The optimal choice for botmasters is

$$\beta_m^* = \begin{cases} 1, & \text{if } P_m(\alpha_m A) \cdot R_m \geq P_p(\alpha_p A) \cdot R_p, \\ 0, & \text{else.} \end{cases} \quad (14)$$

The Case-II equilibrium is the solution of the game when $P_m(\alpha_m A) \cdot R_m \geq P_p(\alpha_p A) \cdot R_p$ is true for all botmasters, making the expected payoff of mobile botnets dominate that of PC botnets.

In the Case-II equilibrium, botmasters' expected payoff is $E[R] = P_m(\alpha_m A) R_m$. Compared to botmasters' expected payoff in the base model ($P_p(A)(R_p^d + R_p^e)$), whether botmasters are better off or worse off depends.

In the Case-II equilibrium, users' expected utility is

$$E[U] = W_p f(\alpha_p^* A) + W_m f(\alpha_m^* A) - P_m(\alpha_m^* A)\alpha_m^* R^d. \quad (15)$$

At $\beta_m = 1$ and $W_p = W_m = W$, users' optimal strategy satisfies both

$$W\{f'(\alpha_p^* A)\alpha_p + f'(\alpha_m^* A)\alpha_m\} = P_m(\alpha_m^* A)(\alpha_m^*)^2 R^d, \quad (16)$$

and Eq. (10).

As in the Case-I equilibrium, $f(\alpha_p^* A) + f(\alpha_m^* A) > f(A)$. However, in the Case-II equilibrium it is uncertain whether $P_m(\alpha_m^* A)\alpha_m^* R^d$ is greater than $P_p(A)R^d$. Although the Case-II equilibrium is ambiguous for both botmasters and users in terms of expected benefits, money-driven botmasters tend to be better off compared with the base case since they would only switch to mobile botnets if doing so is more profitable. Considering the reality that PC botnets are already widespread, they would still function though may be at a gradually descending rate as botmasters switch from PC to mobile botnets.

3.3 The Case-III equilibrium

The scenario in the Case-III equilibrium is that some botmasters focus on PC botnets while others on mobile botnets. Although each individual botmaster's choice is dichotomous (devoting all the limited resources to target one particular type of botnet only, either PC or mobile botnets), the overall botnet portfolio for all botmasters as a botnet industry is mixed and diversified.

Per Eq. (3), botmasters' optimal portfolio composition depends on the probability of compromise and the expected payoffs from herding PC and mobile botnets, i.e., $\beta_p = \beta_p(P_p, P_m, R_p, R_m)$ and $\beta_m = \beta_m(P_p, P_m, R_p, R_m)$, which further depends on user activities and their distribution across PC and mobile devices.

The Case-III equilibrium is realized in two circumstances. First, PC botnets and mobile botnets are equally profitable to botmasters. Second, PC botnets are more profitable to some botmasters while mobile botnets are more profitable to others. For illustration purpose, we use the first scenario to analyze the welfare effects of such equilibrium.

In the Case-III equilibrium, users' expected payoff is

$$E[U] = W_p \cdot f(\alpha_p^* A) + W_m \cdot f(\alpha_m^* A) - \alpha_p^* R^d \cdot P_p(\alpha_p^* A) - \alpha_m^* R^d \cdot P_m(\alpha_m^* A). \quad (17)$$

The optimal network activities (A^*) and their distribution over computers (α_p^*) and mobile devices (α_m^*) still solve Eqs. (10) and (11). At optimum botmasters are indifferent between PC or mobile botnets.

3.3.1 Discussion of equilibria

Table 2 provides a simplified ranking summary of the three scenarios of the equilibrium. Higher ranking means higher welfare for the corresponding party. For example, in the Case-I equilibrium, users are better off and botmaster are worse off compared to the base case, which is a win–lose situation. The Case-II equilibrium is largely a win–win situation in which both users and botmasters tend to be better off than the worst case but users are worse off and botmasters are better off compared to the Case-I equilibrium. The Case-III equilibrium is a lose–win situation which is the most favorable for botmasters (and least favorable for users) when botmasters' optimal botnet portfolio consists of both PC and mobile botnets.

Table 2 A simplified ranking summary of equilibria

	Botmasters	Users
Case-I	3rd	1st
Case-II	2nd	2nd
Case-III	1st	3rd

The Case-III equilibrium shows that when botmasters hack both PC and mobile devices, users are worse off as there is no safe haven for users to diversify risks. By contrast, botmasters benefit the most from this equilibrium and have the incentives to reach such equilibrium, perhaps through increasing their skills of hacking mobile devices, or exploring more revenue sources from mobile devices. From the defenders' point of view, they certainly want to avoid this equilibrium. Given that PC botnets are already widespread, the Case-III equilibrium would be imminent if defenders do not act much and quick. This equilibrium is more likely to occur when users conduct more activities on mobile devices, when mobiles are easier to hack and control, or when the economies of scale from operating botnets could be achieved with the large number of mobile devices.

As proved in Sect. 3.1.1, the Case-I equilibrium is optimal for users because it is a win–lose situation in which users are better off while botmasters are worse off. The significance of the Case-I equilibrium suggests that the key is to prevent botmasters from herding mobile botnets, which would only be the case when mobile botnets are not as profitable as PC botnets. From the economic perspective, reducing the expected profit of mobile botnets would require either reducing the revenue generated by botnets or increasing the cost of managing botnets.

In order to make this equilibrium possible, security defenders may think in the following two directions. First, to reduce botmasters' revenue from mobile botnets, users should follow the Case-I equilibrium for the optimal distribution of network activities/data on PCs and mobile devices. We should design some clever synchronization program that allows the application/data on the mobile devices not to exceed a threshold. By diversifying network activities across PC and mobile devices, users could have less financial loss by not putting all their eggs in one basket.

Second, to increase the cost of managing mobile botnets (equivalent to decreasing the compromise success rate P_{m} in the model), it is crucial to develop an industry standard to request mobile OS/application developers, vendors and cellular service providers to give higher priority to the security of mobile devices, thus making mobile devices relatively more robust to attacks. Although all system designs face the trade-off between usability and security, we argue the security concern for mobile devices should have higher priority relative to PCs.

In some sense, diversified architecture, multiple vendors, strict application examination and release policy may be good in terms of overall security of mobile devices. Besides Apple Store, many companies have launched their own application stores since 2008 including Android Market (now Google Play Store), Amazon Android Appstore, BlackBerry App World, Nokia Ovi Store, Palm App Catalog and Microsoft Windows Marketplace for Mobile. Markets, crowdsourcing and automatic detection infrastructure should work together to prevent potential vulnerabilities in applications from opening up the door for malware.

4 Numerical simulation study and discussion

In this section, we further study a few key issues discussed in previous sections via graphical illustration. In particular, we demonstrate how botmasters make decisions regarding whether to herd PC or mobile botnets, how botmasters' expected payoffs are affected at the presence of both PC and mobile devices, and how user welfare is affected by the coexistence of PC and mobile devices. Throughout the numerical simulation study, the utility function $f(A)$ and the probability function $P(A)$ still take the format as specified in Sect. 3 while the parameter values are assigned for illustration purposes only. The numerical examples simplify the complex relationship among important decision variables and provide insights and guidelines for botmasters, users and security defenders.

4.1 User expected utility

First, we show how users can increase their expected utility (Fig. 1) while enjoying more network activities (Fig. 2) on computers and mobile devices in the Case-I equilibrium. Throughout the case study, we specify $W_{\mathrm{p}} = W_{\mathrm{m}} = 20$ and $R^{\mathrm{d}} = 55$. In the base model where users use computers only, users' expected payoff is $E[\tilde{U}] = 24.8$ (at $A = 10$ and $\alpha_{\mathrm{p}} = 100\,\%$) by Eq. (2). When users use both computers and mobile devices, their expected utility $E[U^*]$ in the Case-I equilibrium is $E[U^*] = 20(\sqrt{10\alpha_{\mathrm{p}}}+\sqrt{10(1-\alpha_{\mathrm{p}})})-55\alpha_{\mathrm{p}}(1-\frac{1}{\sqrt{1+10\alpha_{\mathrm{p}}}})$ by Eq. (13).

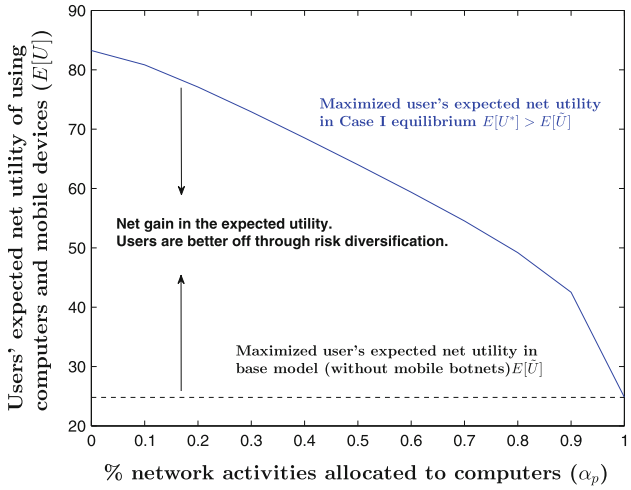


Fig. 1 In the optimal Case-I equilibrium where botmasters stay with PC botnets, user expected utility exceeds that of the base model through risk diversification by distributing network activities between computers and mobile devices

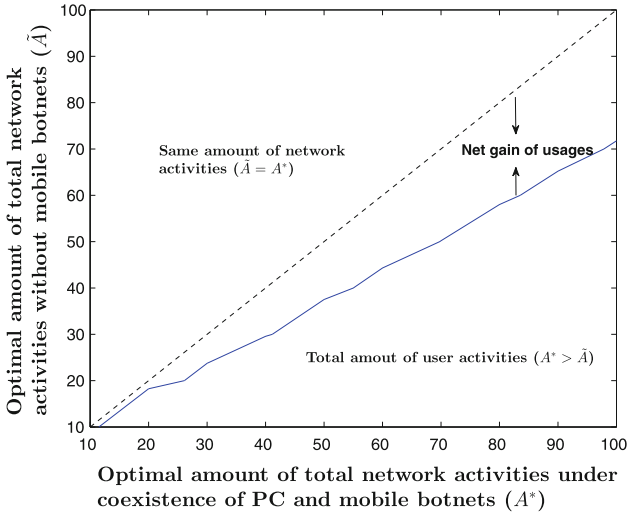


Fig. 2 In the Case-I equilibrium, users are further better off in terms of the increase in total network activities compared to the base model

Figure 1 illustrates how user's expected utility ($E[U^*]$) in the Case-I equilibrium changes with the distribution of network activities to computers (α_{p}). As shown, $E[U^*]$ is decreasing in α_{p}. A smaller α_{p} means more intensive use of mobile devices for network activities. If a smaller α_{p} is sufficient to make PC botnets more financially attractive to botmasters (possibly when the security of mobile devices is supreme for instance), having mobile devices in use will provide buffer room for users, benefiting users with risk diversification opportunities. The straight line in Fig. 1 is the user utility in the base model. It can be seen that users are better off as they gain in their expected utility through diversifying network activities on computers and mobile devices.

Equation (12) is the relative size of network activities in the Case-I equilibrium (A^*) and the base model ($\tilde{A}$). Figure 2

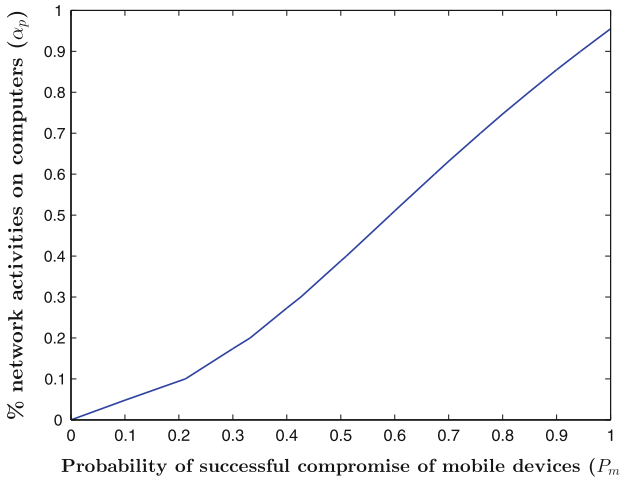


Fig. 3 The distribution of user activities to computers based on the security of mobile devices to achieve the Case-I equilibrium

plots A^* and $\tilde{A}$ at $\alpha_p = 0.5$. As shown, users gain in network activities ($A^* > \tilde{A}$) when using both computers and mobile devices.

4.2 User activity portfolio

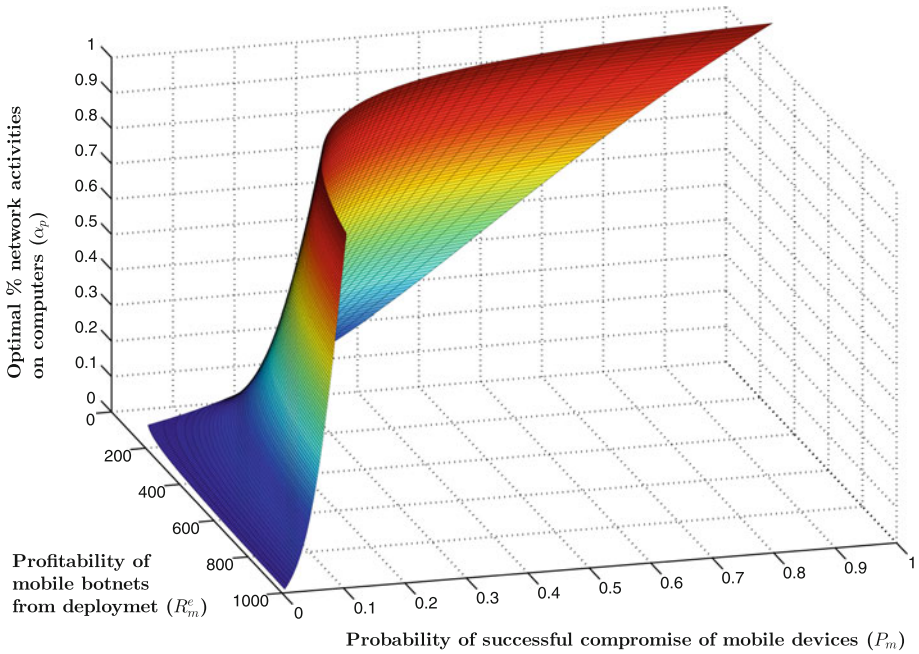
Next we show in Figs. 3 and 4, how the distribution of network activities to computers (α_p), the profitability of mobile botnets from machine deployment (R_m^e) and the probability of successful compromise of mobile botnets(P_m) are interdependent to achieve the Case-I equilibrium. In particular, Eq. (10) has to be satisfied to effectively prevent botmasters from herding mobile botnets. Let $R_p^e = R_m^e = 100$. Along with previously specified parameter values and functional forms, we get $(1-\frac{1}{\sqrt{1+10\alpha_p}})(55\alpha_p+100) = P_m(55(1-\alpha_p)+100)$. As shown in Fig. 3, α_p and P_m are positively related: Users should allocate more network activities to computers when mobile devices are less secure to keep botmasters from switching to mobile botnets. From the perspective of users, a smaller P_m (more secure mobile devices) is preferred in which case mobile devices could allow more risk diversification opportunities for users.

Besides the security of mobile devices, user utility depends also on the relative profitability of PC and mobile botnets. Figure 4 adds the profitability of mobile botnets from machine deployment (R_m^e) to Fig. 3 as the third dimension. Let R_m^e be unspecified while all the other parameters stay at previously defined values. Equation (10) becomes $(1 - \frac{1}{\sqrt{1+10\alpha_p}})(55\alpha_p + 100) = P_m(55(1 - \alpha_p) + R_m^e)$. As shown in Fig. 4, as the profitability of mobile botnets from machine deployment increases, the percentage of network activities allocated to computers should also increase proportionally to reach the Case-I equilibrium.

4.3 Botmasters' strategy and profitability

Figure 5 plots the expected payoff functions of PC and mobile botnets for botmasters based on user activities and their distribution between computers and mobile devices. The control variable for botmasters is β where botmasters herd PC and/or mobile botnets depending on their *relative* profitability. As shown in Fig. 5, if the surface of the expected payoff of PC botnets is on top of that of mobile botnets, the optimal strategy for botmasters is to choose $\beta_p = 1$ and $\beta_m = 0$, and $\beta_p = 0$

Fig. 4 The profitability of mobile botnets from machine deployment, the probability of successful compromise of mobile devices and the distribution of user activities between PC and mobile devices are interdependent to achieve the Case-I equilibrium



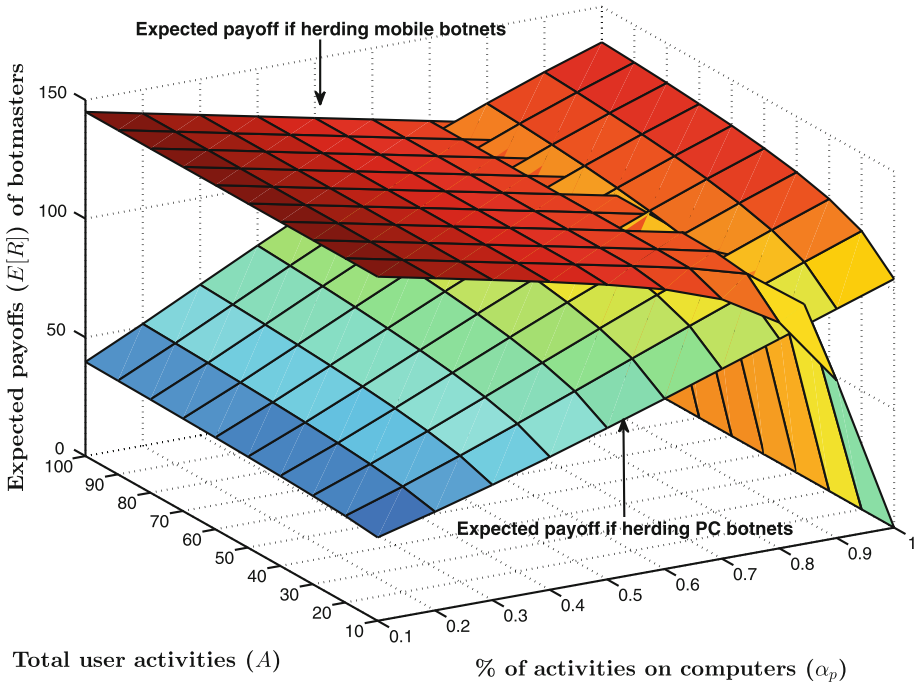


Fig. 5 Botmasters' decision-making based on the *relative* profitability of PC and mobile botnets (i.e., always choose the higher surface)

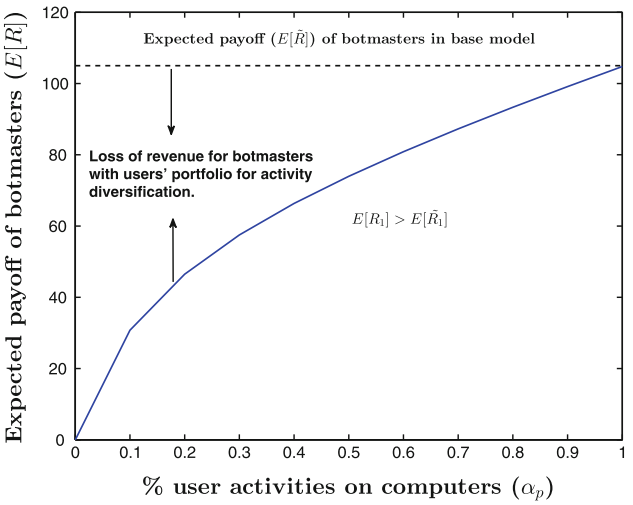


Fig. 6 In the Case-I equilibrium, users' risk diversification and portfolio management of network activities across computers and mobile devices reduce the profitability of botmasters significantly compared to the base model

and $\beta_m = 1$ vice versa. Botmasters are indifferent between herding PC or mobile botnets at the intersection of the two surfaces since the expected payoffs are equal. Although an individual botmaster's choice is dichotomous, the overall botnet business as an industry is mixed and diversified (a botnet portfolio).

Figure 6 shows that botmasters are worse off in the Case-I equilibrium compared to the base model. In particular, two curves are drawn representing botmasters' expected payoffs in the base model ($E[\tilde{R}] = 105$) and in the Case-I equilibrium ($E[R_1^*] = (1 - \frac{1}{\sqrt{1+10\alpha_p}})(55\alpha_p + 100)$). As can be seen, users' risk diversification across computers and mobile devices can effectively reduce the expected payoffs of botmasters.

As above, the Case-I equilibrium is optimal in which users are better off and botmasters are worse off compared to the base model. The optimum would only be achieved if botmasters could be successfully kept from herding mobile botnets, which would be the case if mobile botnets are not as profitable as PC botnets for money-seeking botmasters.

In contrast to the Case-I equilibrium, when botmasters target both PC and mobile devices, they can be better off compared to the base model. In other words, the expected payoffs for botmasters in the Cases-II and Case-III equilibria may be higher than the base model, as shown in Fig. 7a where botmasters herd mobile botnets, and in Fig. 7b where botmasters herd both PC and mobile botnets. However, botmasters are not always better off since there exist combinations of A and α that can make botmasters' expected payoffs fall below the base model.

5 Related work

We categorize the botnet-related research into two general groups, the technical approach and the economic approach. We first discuss the technical approach in terms of malware analysis and detection, DDoS attacks, command and control (C&C) channels, etc., focusing on mobile botnet defense. We then discuss the economic approach to analyzing botnet problems along with game theoretical modeling.

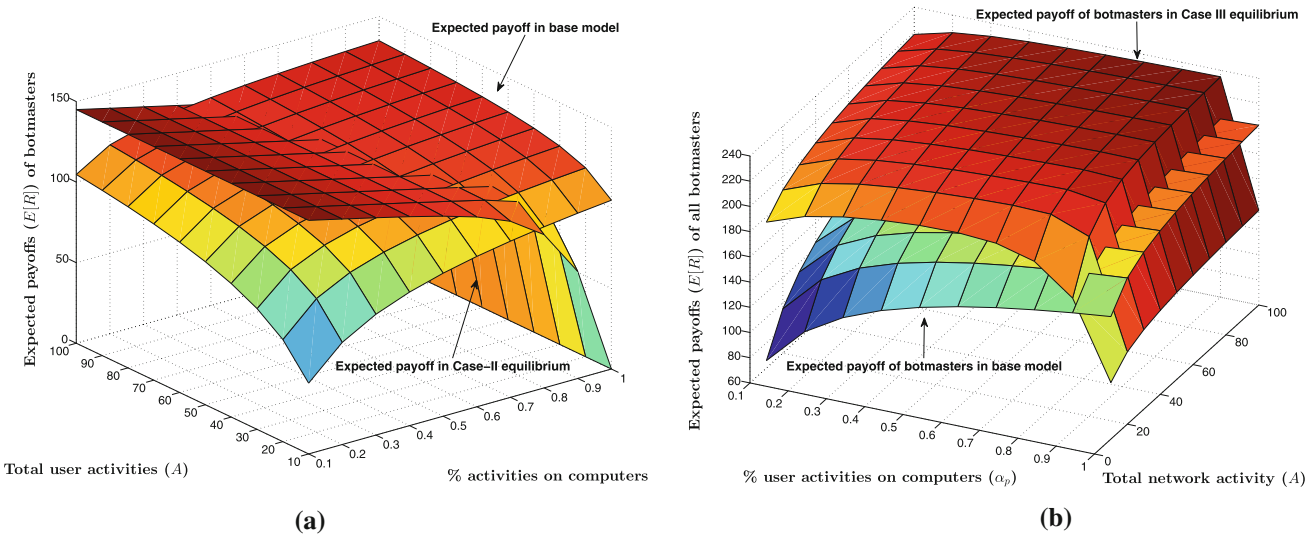


Fig. 7 With the coexistence of PC and mobile botnets, botmasters are most likely better off compared to the base model. **a** Expected payoff of botmasters in the Case-II equilibrium. **b** Expected payoff of botmasters in the Case-III equilibrium

5.1 Computer and mobile botnets

In response to the increasing use of botnets for attacks, sophisticated techniques have been suggested in order to measure, understand and develop possible defenses against botnets [2,6,22,34–36]. Recent trends note that the botnet problem is not abating but rather increasing despite an increasing array of technical options [37].

Traditionally, botnets are comprised of fixed computers and servers. During the past decade, we observe the fast-growing popularity and highest penetration rate of smart phones, tablets and other mobile computing devices among users. The rapid expansion of highly capable but largely insecure mobile devices raises concerns that mobile devices could be the next target of hackers and become what we refer to as *mobile botnets*.

Traynor et al. [11,13] demonstrated the disruptive ability of a mobile botnet composed of as few as 11,750 compromised mobile phones to degrade service to area-code sized regions by 93 %. They also analyzed mobile operating system (OS) vulnerability and jamming attacks and effects on network service. It is possible to create a mobile phone botnet on the most popular smart phone (iPhone) [14]. Vulnerabilities in most mobile phones can be exploited for carrying out large-scale DoS attacks using SMS messages [15].

Security of mobile devices has been the subject of a number of recent studies. A survey [7] studied mobile security and various attack vectors from different layers: hardware, system and users, and targeting at different types of mobile devices, OS, wireless links and malware. Study in [16] compared mobile security versus fixed computer security. Mobile devices face a wide range of new security challenges and malicious threats due to different computing environments such as resource constraints, attack types, architecture, platforms and HCI usability. Contemporary mobile platform (Android and iOS) threats and security model are studied in [8].

Malicious software (malware) specifically designed for mobile devices has been developed or analyzed. For example, Felt et al. [10] surveyed existing mobile malware of iOS, Android and Symbian and discussed current and future incentives for writing mobile malware. The incentives include selling user credential, premium-rate calls and SMS, SMS spam, search engine optimization, ransom, ad click fraud, invasive advertising, in-application billing fraud, government surveillance, email spam, DDoS and proximity-based credit card transaction using near field communication (NFC). Schlegel et al. [12] developed Soundcomber, a low-profile (minimum traffic volume) sensory malware that extracts audio sensor data of the phone thus can potentially steal credit card numbers and PINs. To detect mobile malware, current practice relies on mobile application markets, which requires manual intervention. Nadji et al. [9] proposed an Airmid system for automated detection and response to malware infections on mobile devices based on their network behavior.

Command and control (C&C) channel is another important component of botnets, used by botmasters to control and maintain bots, and to send instructions to bots. Research [17] revealed that Bluetooth is feasible for C&C channels for mobile phone-based botnets due to repetitive nature of human daily routines. Simulation shows C&C messages can be propagated to two-thirds of infected nodes within 24 h. In addition, SMS messages as C&C channel, P2P structure as topology [18], or steganography combined with web URLs [19] can also be used to make mobile botnets feasible.

5.2 Economics of botnets

Defending against botnets is highly challenging. While the above studies are important, botnets have bypassed technical defenses, resulting in a never ending arms race between attackers and defenders, which is usually an undesirable position for defenders. Thus, it is necessary to *rethink* the botnet problem.

We argue that the botnet problem is essentially an economic problem. Botnets have the potential to provide botmasters with a large variety of income sources [5,23–28]. Currently, botnets are commonly used in distributed denial-of-service attacks (DDoS), key-logging, ad click fraud, SMTP mail relays for spam, identity/financial accounts theft, etc., all of which have the ability to generate large amount of revenue for botmasters. As more cybercriminals become driven by money, removing the financial incentives driving them is likely to help solve the growing botnet problem from the root cause.

As researchers become more aware of the economic nature of Internet security problems, recent research has been seeking help from economic studies. To stem the flow of stolen credit cards and identity thefts, two technical approaches were proposed in [38] to reduce the number of successful market transactions, aiming at undercutting the cybercriminals' verification or reputation system. In a similar vein, Ford and Gordon proposed targeting malicious-code generated revenue streams from online advertising fraud [23].

Botnet malicious activities have become more organized and money-driven, and a digital underground economy for hacking-related goods and services has evolved. Vömel et al. [28] studied the infrastructure and modes of operation of this underground economy by examining the traffic captured on IRC channels via data collection from honeypots. There could exist a two-tier underground economy of IRC market [26], the upper tier where gangs and alliances can extract value from their resources, avoid taxes and gain higher profit, and the lower tier consisting of those who must buy resources or who cannot monetize the data they steal. The features of the underground economy, including the flow of goods, services, and resources, social costs and profits, roles and incentives of private and public protection, are also studied in [30].

The economics of botnet spam is surveyed in [29], which estimated an extremely high "externality ratio" of the spam market: the society loses $100 for every $1 of profit to a spammer. The social cost is approximately $20 billion per year in the USA alone, compared to the annual revenue of $200 million earned by botmasters from spamming US consumers. The economic incentives behind DDoS attacks against femtocell network services are modeled in [39]. Garg et al. [40] compared organized digital crime (ODC) such as botnets to a classical economic model of smuggling. They claimed there are situations where ODC leads to an increase in social welfare.

Finally, game theory [41] provides a formal mathematical framework to study the interactions between interdependent rational players. The results of the game are characterized as one or more Nash equilibria [31]. Although game theory is applied primarily to economics, it has been used in many other disciplines, including recent research on security of communication networks. In particular, game theory can have applications in six categories of security and privacy problems [42]: security of the physical and MAC layers, security of self-organizing networks, intrusion detection systems, anonymity and privacy, economics of network security and cryptography.

The interactions between botmasters and defenders can be analyzed as an SIS epidemic model [43,44] with external entrances based on optimal control theory. In particular, two equilibria were derived in [43], i.e., (a) defender: max level, botmaster: intermediate level; and (b) defender: intermediate level, botmaster: max level. Results in [44] showed it is optimal for botmasters to reduce infection rate when the percentage of infected host is over some threshold as the opportunity cost of getting caught or traced surpasses the size benefits of the operation cost. In addition, cooperative and competitive games have been modeled between two types of botnets with different outcomes of infection rates and survival ability [45].

Despite the above research on the underground economy and game theory applications, little has been done to understand the strategies in face of the imminent threat of emerging mobile botnets in addition to existing computer botnets. We think from botmasters' point of view regarding how botmasters should run their business in face of the opportunity of mobile botnets. We propose a novel idea of botnet portfolio management of herding both PC and mobile botnets versus user activity portfolio of using computers and mobile devices. We model the strategic playing by botmasters and users in a game theoretical framework. The equilibria derived provide useful insights for security defenders to understand, analyze and ultimately remove financial incentives of botnet problems.

6 Conclusion and future work

Botnets are important problems of today's Internet. Traditionally, the botnet industry includes only computer botnets. With the rising popularity of mobile devices such as smart phones and tablets, mobile botnets are emerging. In this paper, we study the security implications of the possible coexistence of PC and mobile botnets from an economic point of view based on the observation that the majority of botnet-based cybercrimes are driven by money, and therefore, by understanding the economics of the botnet business,

we may fight the botnet problem from the root cause, i.e., the financial incentives.

We adopt an interesting *portfolio* concept in managing botnet as an industry and model the decision-making by botmasters and users as *optimization* problems, in which profit-driven botmasters seek to maximize their expected profits from herding a portfolio of PC and mobile botnets while users seek to maximize their expected utility from using a portfolio of computers and mobile devices. The strategic playing by botmasters and users naturally fit in a game theoretical framework, from which three equilibria are derived and discussed. From defenders' point of view, the Case-I equilibrium is optimal for users because users are better off while botmasters are worse off, a win–lose situation. While security is important for both computers and mobile devices, security should have higher priority for mobile devices in order to achieve the optimal equilibrium.

Understanding the equilibria of botmasters, on the other hand, may as well provide valuable insight for security practitioners to prioritize their time and effort to fight against botnets more effectively. With the fast evolving computing environments and network technologies, more "things," such as smart phones, sensors, healthcare devices, or even appliances, will become the first-class citizens of future Internet. Analyzing the relationship of these emerging botnets will be interesting future work.

References

1. ARBOR NETWORK . Worldwide Infrastructure Security Report, vol. III, (online). http://www.arbornetworks.com/report (2007)
2. McCarty, B.: Botnets: big and bigger. IEEE Secur. Priv. **1**(4), 87–90 (2003)
3. Dagon, D., Gu, G., Lee, C.P., Lee, W.: A Taxonomy of Botnet Structures. In: Twenty-Third Annual Computer Security Applications Conference (ACSAC). Miami Beach, Florida (2007)
4. Rajab, M.A., Zarfoss, J., Monrose, F., Terzin, A.: A Multifaceted Approach to Understanding the Botnet Phenomenon. In: 6th ACM SIGCOMM Conference on Internet Measurement, SESSION: Security and Privacy, Rio de Janeiro, Brazil, pp. 41–52 (2006)
5. Franklin, J., Paxson, V., Perrig, A., Savage, S.: An inquiry into the nature and causes of the wealth of internet miscreants. In: The 14th ACM Conference on Computer and Communications Security, SESSION: Internet Security, pp. 375–388. Alexandria, Virginia (2007)
6. Grizzard, J.B., Sharma, V. Nunnery, C., Kang, B.B., Dagon, D.: Peer-to-Peer Botnets: Overview and Case Study. In: First Workshop on Hot Topics in Understanding Botnets (HotBots07), pp. 1–1. Cambridge, MA (2007)
7. Becher, M., Freiling, F.C., Hoffmann, J., Holz, T., Uellenbeck, S., Wolf, C.: Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In: Proceedings of the 32nd IEEE Symposium on Security and Privacy (S&P 2011), pp. 96–111. Berkeley, CA (2011)
8. Delač, G., Silić, M., Krolo, J.: Emerging security threats for mobile platforms. In: Proceedings of the 34th International Convention MIPRO, pp. 1468–1473. Opatija, Croatia (2011)
9. Nadji, Y., Giffin, J., Traynor, P.: Automated remote repair for mobile malware. In: Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC'11), pp. 413–422. Orlando, FL (2011)
10. Felt, A.P., Finifter, M., Chin, E. Hanna, S. Wagner, D.: A survey of mobile malware in the wild. In: Proceedings of the 1st ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM'11), pp. 3–14. Chicago, IL (2011)
11. Traynor, P., Amrutkar, C., Rao, V., Jaeger, T., McDaniel, P., Porta, T.L.: From mobile phones to responsible devices. Secur. Commun. Netw. **4**(6), 719–726 (2011)
12. Schlegel, R., Zhang, K., Zhou, X., Intwala, M., Kapadia, A., Wang, X.: Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. In: Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS'11). San Diego, CA (2011)
13. Traynor, P., Lin, M., Ongtang, M., Rao, V., Jaeger, T., Mcdaniel, P., Porta, T.L.: On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. In: Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), pp. 223–234. Chicago, Illinois (2009)
14. Mulliner, C., Seifert, J.P.: Rise of the iBots: owning a telco network. In: Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software (Malware), pp. 71–80. Nancy, France (2010)
15. Mulliner, C., Golde, N., Seifert, J.P.: SMS of Death: from analyzing to attacking mobile phones on a large scale. In: Proceedings of the 20th USENIX Security Symposium, pp. 24–40. San Francisco, CA (2011)
16. Oberheide, J., Jahanian, F.: When mobile is harder than fixed (and vice versa): demystifying security challenges in mobile environments. In: Proceedings of the Eleventh Workshop on Mobile Computing Systems and Applications (HotMobile'10), pp. 43–48. Annapolis, MD (2010)
17. Singh, K., Sangal, S., Jain, N. Traynor, P. Lee, W.: Evaluating Bluetooth as a medium for botnet command and control. In: Proceedings of the 7th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA'10), pp. 61–80. Bonn, Germany (2010)
18. Zeng, Y., Shin, K.G., Hu, X.: Design of SMS commanded-and-controlled and P2P-structured mobile botnets. In: Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC'12), pp. 137–148. Tucson, AZ (2012)
19. Xiang, C., Binxing, F., Lihua, Y., Xiaoyi, L., Tianning, Z.: Andbot: towards advanced mobile botnets. In: Proceedings of the 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET'11), pp. 11–17. Boston, MA (2011)
20. Bächer, P., Holz, T., Kötter, M., Wicherski, G.: Know your Enemy: Tracking Botnets. In: The Honeynet Project and Research Alliance (2005)
21. Zou, C., Cunningham, R.: Honeypot-Aware Advanced Botnet Construction and Maintenance. In: International Conference on Dependable Systems and Networks, pp. 199–208. Philadelphia, PA (2006)
22. Wang, P., Sparks, S., Zou, C.C.: An Advanced Hybrid Peer-to-Peer Botnet. In: First Workshop on Hot Topics in Understanding Botnets (HotBots07), pp. 2–2. Cambridge, MA (2007)
23. Ford, R. Gordon, S.: Cent, Five Cent, Ten Cent, Dollar: Hitting Botnets Where it Really Hurts. In: New Security Paradigms Workshop, Dagstuhl, Germany, pp. 3–10 (2006)
24. Li, Z., Liao, Q., Striegel, A.: Botnet Economics: Uncertainty Matters. In: Proceedings of Workshop on the Economics of Information Security (WEIS '08). Hanover, New Hampshire (2008)
25. Namestnikov, Y.: The Economics of Botnets. White Paper, Kaspersky Lab Woburn, MA (2009)

26. Herley, C., Florencio, D.: Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy. In: The Eighth Workshop on the Economics of Information Security (WEIS '09). University College London, England (2009)
27. Li, Z., Liao, Q., Blaich, A., Striegel, A.: Fighting botnets with economic uncertainty. J. Secur. Commun. Netw. Wiley Intersci. **4**(10), 1104–1113 (2011)
28. Vömel, S., Holz, T., Freiling, F.C.: "I'd like to pay with your visa card" an illustration of illicit online trading activity in the underground economy. Technical Report TR-2010-004, Department for Mathematics and Computer Science, University of Mannheim (2010)
29. Rao, J.M., Reiley, D.H.: The Economics of Spam. J. Econ. Perspect. **26**(3), 87–110 (2012)
30. Cárdenas, A., Radosavac, S., Grossklags, J., Chuang, J., Hoofnagle, C.: An Economic Map of Cybercrime. In: The 37th Research Conference on Communication, Information and Internet Policy (TPRC). George Mason University Law School, Arlington, VA (2010)
31. Nash, J.: Equilibrium points in n-person games. Proc. Natl. Acad. Sci. **36**(1), 48–49 (1950)
32. Georgia Tech Information Security Center (GTISC). Emerging Cyber Threats Report for 2009. (2008)
33. Schiller, C., Binkley, J. Evron, G., Willems, C., Bradley, T. Harley, D., Cross, M.: Botnets: The Killer Web App, p. 480 Syngress, Waltham, MA, ISBN: 1597491357 (2007)
34. Karasaridis, A., Rexroad, B., Hoeflin, D.: Wide-scale Botnet Detection and Charaterization. In: USENIX Workshop on Hot Topics in Understanding Botnets (HotBots'07) Cambridge, MA (2007)
35. Dagon, D., Zou, C., Lee, W.: Modeling Botnet Propagation Using Time Zones. In: Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS'06) San Diego, CA (2006)
36. Cooke, E., Jahanian, F., McPherson, D.: The Zombie roundup: understanding, detecting, and disrupting botnets. In: Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI), pp. 39–44 Cambridge, MA (2005)
37. Turner, D., Fossi, M., Johnson, E., Mack, T., Blackbird, J., Entwisle, S., Low, M.K., McKinney, D., Wueest, C.: Symantec global internet security threat report–trends for july–december 07. Symantec Enterp. Secur. **13**, 5–8 (2008)
38. Franklin, J. Paxson, V., Perrig, A., Savage, S.: An inquiry into the nature and causes of the wealth of internet miscreants. In: Proceedings of the 14th ACM conference on Computer and Communications Security, SESSION: Internet Security, pp. 375–388. Alexandria, Virginia (2007)
39. Segura, V., Lahuerta, J.: Modeling the economic incentives of DDoS attacks: femtocell case study. In: The Eighth Workshop on the Economics of Information Security (WEIS), pp. 107–119. University College London, England (2009)
40. Garg, V., Husted, N., Camp, J.: The smuggling theory approach to organized digital crime. In: eCrime Researchers Summit (eCrime), pp. 1–7. San Diego, CA (2011)
41. von Neumann, J., Morgenstern, 0.: Theory of Games and Economic Behavior. Princeton University Press, Princeton (1944)
42. Manshaei, M.H., Zhu, Q., Alpcan, T., Başar, T., Hubaux, J.-P.: Game theory meets network security and privacy. ACM Computing Surveys (CSUR), vol. 45, No. 3. NewYork, Article No. 25 (2013)
43. Bensoussan, A., Kantarcioglu, M., Hoe, S.(C.): A game-theoretical approach for finding optimal strategies in a botnet defense model. In: Proceedings of the First international conference on Decision and game theory for security (GameSec), pp. 135–148. Berlin, Germany (2010)
44. Shang, Y.: Optimal Attack Strategies in a Dynamic Botnet Defense Model. Int. J. Appl. Math. Inf. Sci. **6**(1), 29–33 (2012)
45. Song, L., Jin, Z., Sun, G.: Modeling and analyzing of botnet interactions. Physica A: Stat. Mech. Appl. **390**(2), 347–358 (2011)