SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2011; **4**:1104–1113
Published online 15 July 2010 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.235

RESEARCH ARTICLE

Fighting botnets with economic uncertainty

Zhen Li[1], Qi Liao[2]*, Andrew Blaich[2] and Aaron Striegel[2]

[1] Department of Economics and Management, Albion College, Albion, MI 49224, U.S.A.
[2] Department of Computer Science and Engineering, University of Notre Dame, Notre Dame, IN 46556, U.S.A.

ABSTRACT

Botnets have become an increasing security concern in today's Internet. Since current technological defenses against botnets have failed to produce results, it has become necessary to think about different strategies. Given that money is perhaps the single determining force driving the growth in botnet attacks, we propose an interesting economic approach to take away the root cause of botnet, i.e., the financial incentives. In this paper, we model botnet-related cyber crimes as a result of profit-maximizing decision-making optimization problem from the perspective of botmasters. By introducing the *uncertainty* level created by the *virtual bots*, we make determining the optimal botnet size infeasible for the botnet operators, and consequently the botnet profitability can fall dramatically. The theoretical model presented here has a large potential to fight off botnet-related attacks of varying revenue patterns. Copyright © 2010 John Wiley & Sons, Ltd.

KEYWORDS

botnet; economics; uncertainty; virtual bots; virtual machines; DDoS spam

***Correspondence**

Qi Liao, Department of Computer Science and Engineering, University of Notre Dame, Notre Dame, IN 46556, U.S.A.
E-mail: qliao@nd.edu

1. INTRODUCTION

Bots, sometimes referred to as *zombies*, are compromised computers that together constitute a bot network, known as a botnet, controlled by one or more botmasters. Critically, zombie computers are ranked as one of the largest threats facing the availability and operational security of network services [1,2]. It has been estimated that up to one quarter of all personal computers connected to the Internet participate in a botnet [3].

Over time, as the motives for cyber crime have shifted, the uses of the botnet have shifted as well. Cyber criminals whom once sought to create havoc and/or prove their technological prowess simply for bragging rights now slant toward making a profit [4–6]. Currently, botnets are commonly used for an array of malicious purposes which include: distributed denial-of-service attacks (DDoS), key-logging, ad click fraud, SMTP mail relays for spam, and identity/credit card theft to name a few. All of these malfeasants have the ability to generate large sums of potential revenue for the botmasters.

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 [2,7–11], but there has been limited success. Recent trends note that the botnet problem is not abating but rather increasing despite an increasing array of technical options [12]. Moreover, the botnets themselves continue to evolve and increase in sophistication with the most modern botnets employing hidden, robust, and complex Command and Control (C&C) infrastructures taking full advantage of years of systems research [11]. Thus, we posit that it is necessary for new directions in thinking how the botnet problem can be dealt with.

Since botnets have been widely used in varying activities, it is hard to design a single technique that can be applied to all the types of attacks. However, due to the shift in how cyber criminals function, economic theories may provide a solution to most, if not all, of the botnet issues. As more cyber criminals are becoming driven by money [4–6], removing the financial incentives that drive them is likely to help cure this growing botnet problem at the root cause. Inspired by this reasoning, this paper develops a theoretical framework that illustrates how virtual machines and uncertainty can be employed to combat botnets.

When making economic decisions, rational people compare costs and benefits, and will only act if the benefit exceeds the cost. Applying the principle to for-pay malicious activities, botmasters are by nature economic agents who participate in the underground Internet economy seeking economic returns [4]. Similar to other rational actors, such as consumers or firms, botmasters make economic

decisions with an attempt to reach the highest level of satisfaction, i.e., profit-driven botmasters make decisions regarding the optimal size of botnets, the number of C&C channels, etc. to reap the maximum level of profit.

One contribution of this paper is the systematic modeling of the botnet formation and operation as a result of *profit-maximizing decision-making* optimization problem from the perspective of the botmasters. Bot-based malicious activities are grouped into two major categories based upon their revenue patterns: attacks whose payoff is generally a lump sum payable when a specific threshold has been met (e.g., DDoS) and attacks whose payoffs are linearly increasing with the use of bots (e.g., sending spam). Two versions of a unified economic model are developed that are applicable to both types of attacks with equally well model predictions.

Another key contribution of the paper is to propose an economic solution to the botnet problem by taking advantage of the so called *virtual bots*[†] (honeypots running on virtual machines that are intended to be probed, accessed, and compromised) to reduce the profitability of botnets. More importantly, we introduce the idea of bringing economic *uncertainties* and *interference* into the botnet market. The uncertainty presented here is how many bots within a botnet are honeypots and how many are actual participants. As shown in this paper, uncertainties have a tremendous impact on the decision-making of botmasters regarding managing botnets largely *via* increased risks and reduced profitability of running botnets. The economic model discussed in this paper can help Internet security researchers improve their understanding of the interactions among botmasters and defenders, and open up a new window to see how economic mechanisms may work when facing the threatening of botnets.

The remainder of the paper is organized as follows. Section 2 discusses the technical background on botnets and related work. Section 3 develops the assumptions, the variables, and the profit level of botmasters in the benchmark model where virtual bots are not around. The botmasters' profit maximization problem is formalized for attacks either with lump sum or linear revenue patterns. Section 4 extends the benchmark model to accommodate the existence of honeypots. We first assume that the probability for a live bot to be virtual is fixed and then relax the assumption to analyze a more informative case in which the probability of virtual bots among live bots is private information. This section also describes how honeypots can be used to undermine botnet attacks from the root cause, i.e., economic incentives. In Section 5, we walk through a case study with numerical examples coupled with graphical illustrations on the impact by honeypots for different revenue patterns. Limitations and some deployment consideration are also discussed in this section. Finally, Section 6 concludes the work and suggests future work.

[†] Throughout the paper, virtual bots, virtual machines, and honeypots are sometimes used interchangeably.

2. BACKGROUND AND RELATED WORK

Botnets are a very real and quickly evolving problem. Many bots found today are a hybrid of previous threats combined with a communication system [10]. Botnets can be used for an array of malicious and illegal activities targeting people and organizations. An example of botnet-based attacks is illustrated in Figure 1. In this example, the botnet master controls an army of zombie computers (bots) *via* a combination of both centralized and decentralized C&C channels such as Internet relay chat (IRC) servers and peer-to-peer (P2P) distributed systems. Although various malicious usages of botnets are possible, two predominant attacking models are shown, namely using the botnets to launch DDoS attacks against a victim organization's web server and sending unsolicited commercial emails (spam) to an ISP's mail server. Also illustrated in Figure 1 is an example of business model of botnet operations. At the center of the botnet underground market, a botmaster utilizes bots for attacks with various revenue streams. For instance, DDoS attacks and blackmails/extortion launched by business competitors or political dissidents; online banking frauds from stolen financial data, promoting sales and marketing *via* sending spam, and/or pay-per-click revenue model for profit-driven advertisement sub-syndicators and search engines.

Defending against botnets is a highly challenging task. Traditionally, defenders have focused on technical solutions, including packet filtering [13,14], trace back [15–17], and host-based anomaly filtering [18–20]. While tools such as these are important, botnets have bypassed technical defenses, resulting in a never ending arms race between attackers and defenders, which is an undesirable position for a content provider.

We note that as researchers become more aware of the economic nature of Internet security problems, recent research has been seeking help from economic theories. To stem the flow of stolen credit cards and identity thefts, the work in Reference [4] proposes two technical approaches to reducing the number of successful market transactions, aiming at undercutting the cyber criminals verification or reputation system. The approach in Reference [18] uses game theory to model attackers and defenders. Although the approach is by nature a technical DDoS defense, it is interesting to notice that a game-theoretical framework is used to analyze the performance of the proposed defense system and to guide the design and performance tuning of the system.

Ford and Gordon [6] propose targeting malicious-code generated revenue streams from online advertising fraud. To combat malicious software, a business model attack generator multihost adware revenue killer (MARK) was proposed. Our model builds on the economic approach of Ford and Gordon. We introduce a threat model targeting a wide range of botnet-based attacks, not just online advertising fraud. The unique contribution of our study is to illustrate in detail how *virtual bots* can be

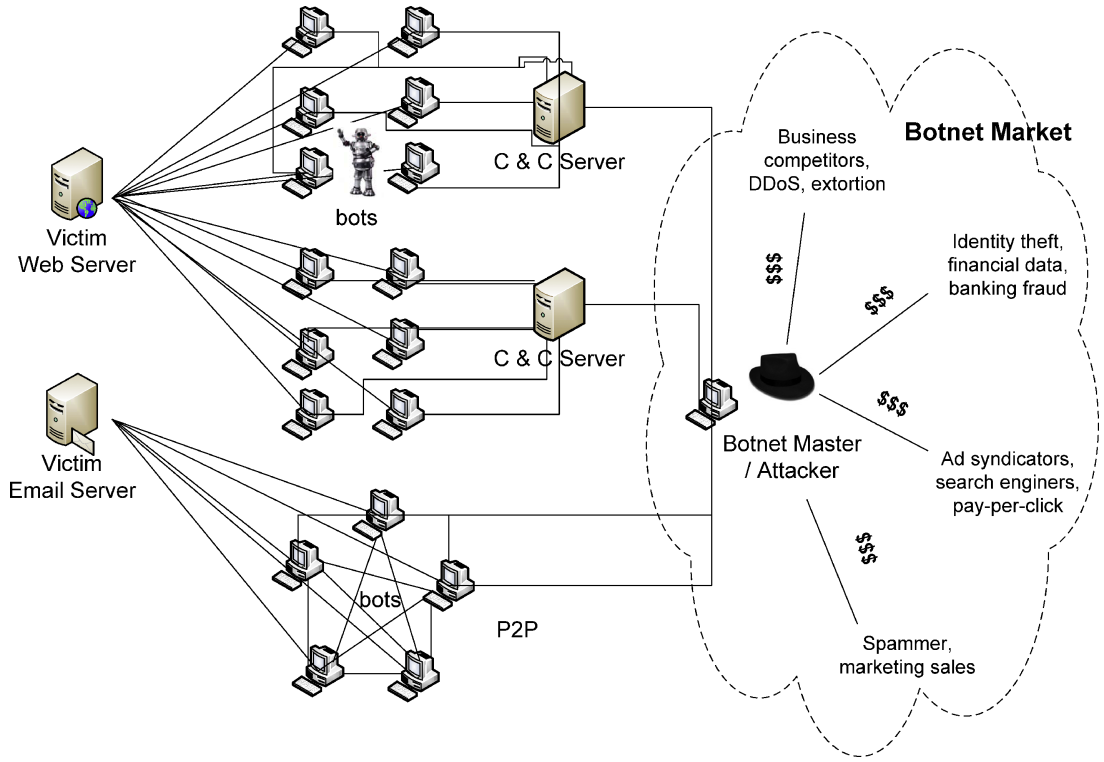

Figure 1. A scenario of botnet-related attacks launched by robot computers (bots) controlled by a botmaster. The control mechanisms can be either centralized (IRC servers) or decentralized (P2P) systems. At the center of a botnet market, botmasters operate botnets for various profit-driven activities with different revenue models.

deployed to change economic motivation of botnet operations.

The interesting idea that uncertainties introduced by the virtual bots can be applied to defend against one specific botnet-related attacks (DDoS) was first proposed in Reference [21]. This paper extends the previous work in an important direction: the model has been extended to be applicable to a much wider array of botnet-based attacks that have either lump sum payments or linearly increasing payoffs in the use of bots. We emphasize that economic uncertainties generated by virtual bots can discourage a broader range of botnet-based malicious activities by fighting botnets at the root cause, i.e., financial incentives.

Lastly, we acknowledge that an earlier measurement study [22] reports a similar practice that has been effectively adopted by music industries to inject and spread 'fake' files into P2P file sharing system. The goal of these so called pollution companies is to trick unsuspecting users into frequently downloading polluted copies of copyrighted content, and as a result users may then become frustrated and abandon P2P file sharing. While it is related to the idea of virtual bots proposed in this work, we focus on a novel function of honeypots to combat botnets by removing the economic incentives of botnets, which is supported by the formal optimization modeling analysis.

3. THE BENCHMARK MODEL: WHEN VIRTUAL BOTS ARE NOT AROUND

Today, a large fraction of Internet-based crimes are profit driven and can be modeled roughly as rational behavior. The exponential growth of botnets with millions of infected computers bought and traded in an underground market has evolved into billion-dollar 'shadow industry' [23]. Being such a lucrative business, Internet malicious activities have become popular and remain difficult to eliminate. Any effective approach aimed at eliminating such activities must remove the financial incentives from them. Botnet economics is by nature similar to other economics whereby rational individuals driven by profits make economic decisions to maximize their well-being. Applying the cost–benefit analysis from economics to Internet crimes, a botmaster will only keep botnets if the benefit of doing so exceeds costs.

In this section, we consider a benchmark model, in which virtual bots are not present to interfere with botnets. Bot-related attacks are grouped into two categories based upon their revenue streams: Type-1 attacks (e.g., DDoS) with lump sum payments only payable for successful attacks and Type-2 attacks (e.g., spam or ad clicks) whose payoffs are

linearly increasing in the use of bots. In the benchmark model, we will develop two versions of an economic model of profit maximization for a representative botmaster, which are applicable to Type-1 and Type-2 attacks, respectively, in a honeypot-free Internet economy.

In general, profit is the difference between revenue and costs, which may be either monetary or psychological. Since it is hard to measure or quantify psychological benefits and costs, we focus on the monetary aspect of the analysis. Also in this paper, for simplicity, botmasters and attackers (hereinafter 'botmasters') are modeled as a single party rather than two separate parties. All model analysis and conclusions work equally well regardlessly since the rental payment by attackers is just the revenue by botmasters. Market price of renting bots affects only income distribution among malicious practitioners rather than the overall botnets' profitability, which depends on fundamental factors such as the cost structure of herding bots and income generated from exploiting (instead of renting) bots.

3.1. Type-1 attacks with lump sum payments

In Type-1 attacks, attackers only get paid when the goal of initiating such attacks is met. For example, DDoS attackers are only compensated if the victim site is successfully disabled. A minimum number of machines is generally required to achieve a Type-1 task, called the effective number of bots. We assume that technical capability determines the effective number of bots, which botmasters take as given.

Botmasters use C&C channels,[‡] to communicate with zombie computers in botnets. A typical C&C channel can accommodate a maximum of q machines. The size of q is determined by technological processes and limited by the capacity of the channel, i.e., q is exogenous.

The profit maximization problem for a representative botmaster who launches Type-1 attacks is therefore:

$$\begin{aligned} \max_{N,k} \text{(profit)} &= M_1 - c * k \\ s.t. \quad & N * U \geq n^e \\ & k \geq \frac{N}{q} \end{aligned} \tag{1}$$

The notation of symbols is explained below:

- M_1 is the lump sum payment for Type-1 attacks, contingent upon launching a successful attack;
- N is the footprint of botnet, i.e., the overall size of infected population in the lifetime of a botnet;
- c is the unit cost of maintaining a C&C channel (plus the average cost of coordinating across multiple channels);
- n^e is the effective number of bots;
- $U = (t/24) * (d/7)$ is the time proportional usage of regular bots, which operate on average t h per day and d days per week to follow the diurnal patterns and physical constraints of the owners.[§] For example, if $t = 8$ and $d = 5$, $U \approx 0.24$, or 24% chance that a bot is online. $N * U$ is thus the number of live bots that can be used to launch an attack.

Noticeably, the botmaster has two control variables: the size of botnet (N), and the number of C&C channels to maintain (k). There are two constraints that regulate the choice of these control variables. The first constraint requires the number of live bots must be no less than the effective number of bots necessary to win the attack. Constraint two specifies that the number of C&C channels must be sufficient to support the botnet.

Since the lump sum payment for Type-1 attacks is fixed, maximizing profit is equivalent to minimizing costs. The botmaster minimizes the number of channels to reduce both the attack cost and the attack signature (for stealthy purpose), equivalently minimizing the size of the botnet. In the steady state, the botnet's footprint is $N = n^e/U$, and the optimal number of C&C channels to maintain is $k = n^e/(U * q)$.

From above when the botmaster of Type-1 attacks does not have to worry about the existence of virtual bots, efficient market results are achieved by realizing the effective number of C&C channels and the botnet size. Let Π_1 be the profit of Type-1 attacks in the benchmark model. It has the following formula:

$$\Pi_1 = M_1 - c * \frac{n^e}{U * q} \tag{2}$$

Type-1 attacks are profitable as long as $M_1 > (c * n^e/(U * q))$. Therefore, the botmaster's benchmark profit is deterministic.

3.2. Type-2 attacks with linearly increasing payoffs

For those cyber crimes whose payoffs are linearly increasing in the use of botnets, the optimal solution to the profit maximization problem is different from that of Type-1 attacks. Despite different revenue patterns, the cost function of the botmaster remains unchanged. The profit maximization

[‡] While the dominant C&C channel in today's botnet is IRC [9] the parameter for botnet maintenance costs applies to all underlying technique adopted to control bots, whether through centralized C&C or other decentralized systems such as P2P.

[§] While on average honeypots may run longer hours than real machines, it does not mean all real machines have identical patterns. In addition, it is easy to set honeypots some on/off pattern randomly to trick botmasters.

problem for a typical botmaster is now:

$$\max_{N,k} (\text{profit}) = m_2 * N * U - c * k$$
$$s.t. \quad k \geq \frac{N}{q} \tag{3}$$

where m_2 is the per-bot payoff for Type-2 attacks with linear income. For example, m_2 may be interpreted as the value of total spam sent by an average bot in a period of time, or the per-bot revenue received from fraudulent ad clicks.

Type-2 attacks are not constrained by a threshold to get payoffs. The number of constraints is reduced to one. Profit increases as revenue increases and/or cost decreases. For any given income level, cost minimization leads to the following conclusion: The optimal number of C&C channels to maintain is $k = N/q$, just enough to support the botnet. Nevertheless, there is no closed-form solution for the optimal botnet size.

The profit level of Type-2 attacks for the botmaster, denoted as Π_2, has the following expression:

$$\Pi_2 = \left(m_2 * U - \frac{c}{q}\right) * N \tag{4}$$

where c/q is the per-bot cost of maintaining a C&C channel. As long as $m_2 * U > c/q$, there would be no upper-bound limiting the botnet size, or the optimal botnet size for Type-2 attacks would be $N \to \infty$ in the benchmark model. Type-2 attacks allow strong financial incentives for running botnets. The model predictions are in line with the real world observations of a simultaneous trend in both reduced weight of Type-1 attacks such as DDoS and more widespread and quickly expanding botnets [1].

4. OPTIMIZATION MODEL WITH VIRTUAL BOTS

To solve the botnet problems from the root cause, we have to reduce their profitability and make the business less attractive. Economic theory suggests that uncertainty is costly [24,25]. When market situations become less clear for some reason, market participants would be reluctant to do business and ask for higher compensation for the increased risks resulting from ambiguity. The idea provides a new line of thinking about interfering with the operation of botnets—to make it less efficient, less deterministic, and hence, less profitable. This work proposes creating virtual bots for fighting the botnets regardless of payment patterns of botnets.

Although the concept of honeypots and virtual machines is not new in information security fields, honeypot/honeynet technology [26] has mainly been used to analyze malware behavior or to trace the botmaster [9,27,28]. To the best of our knowledge, the economic function of virtual machines has not been studied so far. We thus propose a new role that virtual machines may play—undermining botnets from the root cause by removing financial incentives.

In this section, we extend our benchmark model to allow the existence of virtual bots in a botnet. We still distinguish between two types of attacks according to the way botmasters get paid. We first model Type-1 attacks with lump sum payments in the presence of virtual bots and then modify the model to apply to Type-2 attacks with linearly increasing payoffs in the presence of virtual bots.

The introduction of virtual bots creates uncertainty for the botnet as a whole. Inactive bots would reduce the attractiveness of herding botnets. Systematically, how shall we quantify the level of uncertainty and effectiveness of virtual bots? To that end, a new variable is introduced: throughout the analysis, p_v stands for the percentage of virtual bots among *live* bots. Notice that live bots refer to the total usable bots that are on the network at any given time, not the total population of the botnet. That is

$$p_v = \frac{V}{V + (N - V) * U} \tag{5}$$

where V is the number of virtual bots. Initially, p_v is assumed to be fixed and known to botmasters. The assumption is then relaxed by making p_v hidden information and unknown to botmasters.

4.1. Fixed probability of virtual bots

In the benchmark model for Type-1 attacks, the optimal botnet size is sufficient to have n^e live bots required to achieve a task. In the presence of virtual bots, if keeping the same footprint, insufficient live bots would make the attack unsuccessful due to inactive virtual bots. Because of virtual bots, the live population has to be larger than the effective number of machines. How large must the botnet size be?

We introduce virtual bots to the profit maximization problem for a typical botmaster of Type-1 attacks:

$$\max_{N^v,k^v} (\text{profit}) = M_1 - c * k^v$$
$$s.t. \quad (1 - p_v)\{V + (N^v - V) * U\} \geq n^e$$
$$k^v \geq \frac{N^v}{q} \tag{6}$$

where the superscript v refers to the presence of virtual bots. In particular, N^v is the optimal botnet size, and k^v is the optimal number of C&C channels in the presence of *known* chance of virtual bots among live bots. The optimization modeling (6) differs from (1) in the first constraint, which now requires sufficient 'true' live bots to achieve a task.

Given the lump sum payment, profit is maximized at the lowest cost level. Solving the problem results in two conclusions. First, the new equilibrium size of botnet changes to

$$N^v = \frac{\frac{n^e}{(1-p_v)} - (1 - U) * V}{U} \tag{7}$$

Second, to accommodate the N^v footprint, the botmaster has to maintain $k^v = (n^e/(1-p_v) - (1-U)*V)/(U*q)$ C&C channels. Equation (7) can be simplified by taking into account how p_v and V are related in the steady state. Since p_v is the number of virtual bots as a share of all live bots and the number of live bots is $n^e/(1-p_v)$ in the steady state, $p_v = V/\{n^e/(1-p_v)\}$, or

$$V = \frac{n^e * p_v}{1-p_v} \tag{8}$$

Plugging Equation (8) into Equation (7), the equilibrium and optimal botnet size that a botmaster needs to maintain under known probability of virtual bots among live bots becomes

$$N^v = \frac{n^e}{U} + \frac{n^e * p_v}{1-p_v} \tag{9}$$

In the presence of virtual bots, not only is the steady state size of botnet larger, but the profit of Type-1 attacks, denoted as Π_1^v, also declines to

$$\Pi_1^v = M_1 - c * \frac{\frac{n^e}{(1-p_v)} - (1-U)*V}{U*q} \tag{10}$$

For Type-2 attacks with linear payoffs, the botmaster's profit maximization problem is defined as follows in the presence of virtual bots:

$$\max_{N^v,k^v} (\text{profit}) = m_2 * (1-p_v) * \{V + (N^v - V) * U\} - c * k^v$$
$$s.t. \quad k^v \geq \frac{N^v}{q} \tag{11}$$

Compared with Equation (3), the revenue received is reduced by p_v for any live population while the constraint remains unchanged. Let Π_2^v be the profit level of Type-2 attacks:

$$\Pi_2^v = m_2 * (1-p_v) * \{V + (N^v - V) * U\} - c * \frac{N^v}{q} \tag{12}$$

Since Type-2 attacks are not subject to a threshold, the botmaster is still motivated to keep as many compromised machines as possible as long as the marginal increase in profit is non-negative when recruiting one more bot, i.e., $N^v \to \infty$. Nevertheless, the per-bot profit is lowered by inactive virtual bots.

As above, for botnet-based attacks with either Type-1 or Type-2 income stream, the interference by virtual bots tends to reduce their profitability, lowering financial incentives for conducting such malicious activities.

4.2. Uncertain matters

In reality, the number of virtual bots is hidden information *unknown* to botmasters. In this section we relax the assumption of a fixed and known p_v and introduce *uncertainty* to the botnet market. We denote the probability for Type-1 attacks to be successful as s, which depends on p_v and the size of the botnet:

$$s = f(p_v, N^u) \tag{13}$$

where N^u is the size of botnet in the *uncertain* environment. s is decreasing in p_v and increasing in N^u, and has a discrete format: $s = 1$ if $(1-p_v)\{V + (N^v - V) * U\} \geq n^e$; or $s = 0$ if $(1-p_v)\{V + (N^v - V) * U\} < n^e$ by Equation (13).

The *expected* payment for Type-1 attacks is $M_1 * s$, and the botmaster's profit maximization problem when launching such attacks is therefore

$$\max_{N^u,k^u} (\text{profit}) = M_1 * s - c * k^u$$
$$s.t. \quad k^u \geq \frac{N^u}{q} \tag{14}$$

where the two control variables are both denoted with a superscript u, meaning the decision-making is in an uncertain scenario. To make Type-1 attacks successful (i.e., $s = 1$), the botmaster has to use at least $n^e/(1-p_v)$ machines. As $p_v \to 1, n^e/(1-p_v) \to \infty$. The size of botnet and C&C channels are both increasing in p_v as well.

It is important to note that the *unknown* p_v makes it impossible to solve the maximization problem. The botmaster faces a tradeoff between a successful Type-1 attack and costs. Therefore, the botmaster's profit level depends on p_v, V, and N^u as

$$\Pi_1^u = M_1 * f(p_v, N^u) - c * \frac{\frac{n^e}{(1-p_v)} - (1-U)*V}{U*q} \tag{15}$$

Since $f(p_v, N^u) \leq 1$, and p_v is increasing in V, the profitability of Type-1 attacks falls and is also uncertain.

The economic model has suggested that the introduction of virtual bots tends to reduce the profitability of bot-related attacks regardless of revenue patterns. A natural question is how effective virtual bots can be and how many of them are required in order to wipe out the profitability of botnets? In the following, we discuss how virtual bots themselves are sufficient to significantly undermine botnets.

Let $\hat{p}_v$ be the critical (minimum) percentage of virtual bots among live bots necessary to make botnet operation break even (zero profitability). However, it is important to note that making botnet business break even is a *sufficient* condition to reduce financial attractiveness of herding bots but not a *necessary* condition. Running botnets will be less attractive as long as its profitability is not as much as before. Reduced profits also help prevent newcomers from entering the business. Virtual bots themselves can thus remove financial incentives for underground botnet economy and they have a large potential to reduce unfavorable Internet practices.

For Type-1 attacks, the break-even $\hat{p}_v$ that solves $\Pi_1^v = 0$ based on Equation (10) satisfies the relationship $M_1 = c *$

(N^v/q). Or in other words by Equation (9), $\hat{p}_v$ satisfies

$$\hat{p}_v = \frac{1}{1 + \frac{n^e}{\frac{M_1 * q}{c} - \frac{n^e}{U}}} \tag{16}$$

Considering how p_v is related to the number of virtual bots V, as in Equation (8), the critical number of virtual bots among live bots to make Type-1 attacks break even is

$$\hat{V} = \frac{M_1 * q}{c} - \frac{n^e}{U} \tag{17}$$

From Equations (5) and (12), the break-even chance of virtual bots among live bots for Type-2 attacks, $\hat{p}_v$, satisfies

$$m_2 * (1 - \hat{p}_v) * \frac{V}{\hat{p}_v} = \frac{c}{q} * N^v \tag{18}$$

Or equivalently, given the botnet size, the break-even number of virtual bots for Type-2 attacks satisfies

$$\hat{V} = \left(1 - \frac{c}{q * m_2 * U}\right) * N^v \tag{19}$$

Since the optimal botnet size approaches infinity, there does not exist a closed-form solution for the critical percentage of virtual bots. The profitability of Type-2 attacks not only depends on the comparison between per-bot payoff m_2 and per-bot C&C channel cost c/q, but also depends on the number of virtual bots at presence (V) and the actual size of the botnet chosen by the botmaster (N^v).

The analysis illustrates how the existence of right amount of virtual bots may alter economic motivation of botmasters. $\hat{V}$ virtual bots, as in Equations (17) and (19), shall be sufficient to cause non-profitability of botnets of both Type-1 and Type-2 attacks, especially when the botmaster is risk averse.

Botmasters could have guessed the break-even chance of virtual bots among live bots $\hat{p}_v$, adjusted their behaviors accordingly, and converted a loss into a profit. In reaction to this, defenders may have to increase the number of virtual machines, which may further force botmasters to expand botnets. Consequently, having p_v just fixed at the level of $\hat{p}_v$ is not the optimal strategy. Such a strategy may only result in an unfavorable situation similar to an arms race.

As stated earlier, our proposed strategy becomes much more effective by making likelihood of virtual bots p_v *uncertain*. Without defenders' commitment to creating just the 'right' number of virtual bots to reach the critical $\hat{p}_v$, it is difficult if not impossible for botmasters to guess the actual number of virtual bots. Therefore, there is no way to make an optimal decision. The uncertainty not only discourages botmasters from entering the market, but also helps reduce the operation costs for the defenders. The defenders may lower the number of virtual bots without the botmasters being aware of this. The uncertainty (or randomness of creating virtual machines in some sense) facilitates the implementation of the proposed method. Uncertainty makes optimal decision-making regarding size of botnets unachievable.

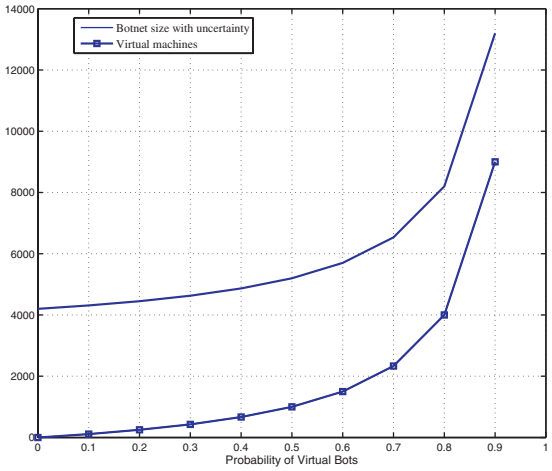

Figure 2. For Type-1 attacks, optimal botnet size and live population under uncertainty are both increasing in the chance of virtual bots.

5. CASE STUDY AND DISCUSSION

In this section, we demonstrate important relationships among virtual bots, optimal botnet size, and profitability of Type-1 and Type-2 attacks through numerical examples and graphical demonstration of the model. Then limitation and a few deployment considerations are discussed.

5.1. Examples and illustration

For Type-1 attacks, let $(1 - p_v)\{V + (N^u - V) * U\} \geq n^e$ be satisfied, hence $f(p_v, N^u) = 1$. The break-even chance of virtual bots thus depends on parameters (M_1, c, n^e, q, U) as in Equation (16). For illustration purposes, suppose $M_1 = 1,000$, $c = 10$, $n^e = 1,000$, $q = 50$, $t = 8$, and $d = 5$. Note c and n^e affect $\hat{p}_v$ negatively, while M_1, q, t, and d affect $\hat{p}_v$ positively. Negative impacts on $\hat{p}_v$ is favorable from the perspective of fighting botnets. The corresponding break-even chance of virtual bots among live bots applicable to Type-1 attacks is $\hat{p}_v = 0.44$. To reach the break-even $\hat{p}_v$, the required number of virtual bots is $\hat{V} = 800$ from Equation (17). The corresponding optimal size of the botnet is $N = 5{,}000$ from Equation (9). Figure 2 shows how the number of virtual bots and the botnet size are related to p_v, applicable to Type-1 attacks. The profitability Π_1^u of Type-1 attacks is related to p_v by the following relationship:

$$\Pi_1^u = 1,000 - 10 * \frac{\frac{1,000}{1-p^v} - \left(1 - \frac{8}{24} * \frac{5}{7}\right) * \frac{1,000 * p_v}{1-p_v}}{\frac{8}{24} * \frac{5}{7} * 50}$$

which is illustrated graphically in Figure 3.

Next, we extend the numerical example to Type-2 attacks with linearly increasing payoffs. Let per-bot payoff $m_2 = 1$;

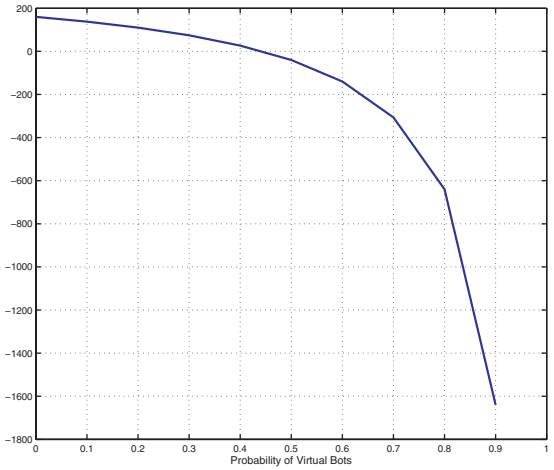

Figure 3. Profitability of Type-1 attacks decreases with increasing chance of virtual bots.

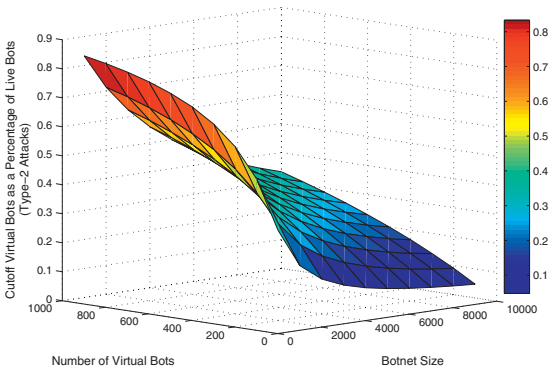

Figure 4. The cutoff percentage of virtual bots among live population of botnets at any given time to make Type-2 attacks unprofitable.

the number of virtual bots necessary to reduce profit to zero at any given botnet size satisfies:

$$\hat{V} = 0.16N^u$$

as specified by Equation (19). For example, if the botmaster maintains a botnet size of 5000, then 800 virtual bots shall be sufficient to reduce the profitability of Type-2 attacks to break even.

More generally, from Equation (18), the break-even $\hat{p_v}$ for Type-2 attacks depends on the comparison between V and N^u as $(1 - \hat{p_v})V/\hat{p_v} = (10/50) * N^u$ by relaxing the diurnal patterns of real bots, i.e., the actual time usage U of real bots is unknown. Figure 4 shows how the cutoff p_v is related to V and N^u for Type-2 attacks with the following numerical relationship:

$$\hat{p_v} = \frac{1}{1 + 0.2\frac{N^u}{V}}$$

For example, given a botnet size $N^u = 5000$ and virtual bots $V = 500$ accounting for approximately one-third of all live

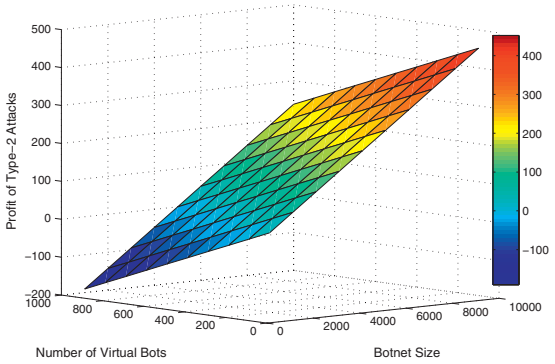

Figure 5. Decreasing relationship between virtual bots and profitability of Type-2 attacks.

bots at $U = 0.22$ according to Equation (5), then botnets would have zero profitability.

With the earlier specified parameters (including the diurnal patterns of real bots), the botmaster's profit for Type-2 attacks depends on the relative size of virtual bots and botnet according to Equations (5) and (12):

$$\Pi_2^u = \frac{1}{21}N^u - \frac{5}{21}V$$

For example, given the botnet size at 5000, 800 virtual bots are required to lower profit to zero. Figure 5 plots the relationship.

In summary, the numerical and graphical illustration in this case study shows how the existence of virtual bots may reduce economic attractiveness for deploying botnets, regardless of payment types. Making p_v uncertain will make the situation challenging and unpredictable for botmasters.

5.2. Discussion

As the optimization problem targets on profit-driven botnet activities, the rationality assumption and economic incentives do not always hold in certain attack models such as state-sponsored attacks. In addition, the effectiveness of the virtual bots largely depends upon the capability of camouflaging virtual bots since attackers may potentially detect honeypots in their botnet by checking whether the compromised machines in the botnet can successfully send out unmodified malicious traffic to attackers' sensors or whether the bot controller in their botnet can successfully relay potential attack commands [28]. While it is beyond the scope of the paper to suggest counter-detecting techniques/strategies or what tools are necessary to disguise honeypots from being detected, we note there have been solid research studies [26,29,30] that developed sophisticated systems to quarantine, disinfect, and join the botnet environment for tracking botnet channels while satisfying the safe legal practice. Also with the increasing practice of server consolidation, virtual machine technologies are adopted in almost every organization for saving hardware

and energy costs of data centers, thus making virtual machine detection less meaningful.

Using virtual bots to combat botnets is feasible in that the magnitude of virtual bots does not have to be big as shown in Section 5.1. Previous studies [8,10,29,30] have found that although the botnet size ranges from roughly a few hundreds to hundreds of thousands, the effective sizes of a botnet connected to a C&C channel rarely exceed a few thousand bots at any given point in their lifetime. If the probability for a live machine to be virtual is at a decent level, botnets will be significantly affected. The botnet controller community features a constant and continuous struggle over who has the largest amount of high-quality infected machines. Since botnet masters have to keep recruiting new machines even when fully aware of the existence of honeypots, the virtual bots' entry to botnets can never be shut down.

While the economic framework provides a solid botnet defense foundation, one question remains namely who has the incentives to deploy virtual bots. First, the government-funded agencies such as cyber security division of Department of Defense (DoD) or Department of Homeland Security (DHS) might be a major player in deployment of virtual bots. Second, a probably better deployment practice might be a distributed scheme, where each organization contributes a few inexpensive computers that offer virtual slices to serve as honeypots, much like a cooperative computing pool. A distributed deployment will not only avoid imposing costs on just one agency but further increase the effectiveness of virtual bots in a geographically diversified environment. While the cost for organizations to contribute a few virtual slices is relatively low, the reward is immediately tangible. For example, if botmasters are aware that an organization has virtual bots deployed and blacklist that organization's domain from their botnets, this essentially makes all computers within that organization immune to botnet-related compromise. Another advantage is that according to the weakest-link threat model [31], attackers will only try to compromise the weakest computers in a network. Using a few honeypots (weakest-link) as a protecting layer on top of real valuable machines in an organization's network might be a smart approach. Additionally, the byproducts data collected by virtual bots have monetary value for security software industries for researching and product development purpose.

6. CONCLUSION

Profit-driven botnet attacks impose serious threats to the modern Internet. Given that money is perhaps the single determining force driving the growth in botnet attacks, we propose an interesting economic approach to take away the root cause of botnet, i.e., the financial incentives. By introducing the uncertainty level created by the virtual bots, we make determining the optimal botnet size infeasible for the botnet operators, and consequently the botnet profitability can fall dramatically.

The proposed scheme is advantageous *versus* existing schemes in that it strikes at the root motivation for the botnets themselves, i.e., the profit motivation. The theoretic framework applies to a large variety of botnet-based attacks with either lump sum type of payments (DDoS) or with linear payoffs (spam and ad clicks, etc). We believe this paper demonstrates how the application of economic principles can offer significant benefit in combating botnets. Besides mathematical evaluation, future works need to be carried out to provide a more accurate assessment in the effectiveness of the model through actual implementations and a geographically diversified deployment. The paper is one of a series of related works. Besides technical considerations, economic, legal, social, and ethical factors all may play certain roles in defending botnets. A wealth of research can be carried out along this line of thinking.

REFERENCES

1. Worldwide Infrastructure Security Report vol. iii. 2007. *ARBOR NETWORK*, Available at: http://www.arbornetworks.com/report
2. McCarty B. Botnets: big and bigger. *IEEE Security & Privacy* 2003; **1**(4): 87–90.
3. Weber T. Criminals may overwhelm the web. *BBC NEWS*, 25 January 2007. Available at: http://news.bbc.co.uk/2/hi/business/6298641.stm
4. 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*, Alexandria, Virginia, 2007; 375–388.
5. Golubev V. Criminals in computer related crimes. *Computer Crime Research Center*. Available at: http://www.crime-research.org/library/Golubev_nov1.html
6. Ford R, Gordon S. Cent, five cent, ten cent, dollar: hitting botnets where it really hurts. In *New Security Paradigms Workshop*, 2006; 3–10.
7. Karasaridis A, Rexroad B, Hoeflin D. Wide-scale botnet detection and charaterization. In *USENIX Workshop on Hot Topics in Understanding Botnets (HotBots'07)*, 2007.
8. 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)*, February 2006.
9. Grizzard JB, Sharma V, Nunnery C, Kang BB, Dagon D. Peer-to-peer botnets: Overview and case study. In *First Workshop on Hot Topics in Understanding Botnets (HotBots07)*, Cambridge, MA, 10 April 2007; 1.
10. 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)*, 2005; 39–44.

11. Wang P, Sparks S, Zou CC. An advanced hybrid peer-to-peer botnet. In *First Workshop on Hot Topics in Understanding Botnets (HotBots07)*, Cambridge, MA, 10 April 2007; 2.
12. Turner D, Fossi M, Johnson E, *et al*. Symantec global internet security threat report—trends for July–December 07. *Symantec Enterprise Security*, vol. XIII, April 2008.
13. Mahajan R, Bellovin S, Floyd S, Ioannidis J, Paxon V, Shenker S. Controlling high bandwidth aggregates in the network. *ACM SIGCOMM Computer Communication Review* 2002; **32**(3): 62–73.
14. Yau DKY, Lui JCS, Liang F, Yam Y. Defending against distributed denial-of-service attacks with max–min fair server-centric router throttles. *IEEE/ACM Transactions on Networking* 2005; **13**(1): 29–42.
15. Park K, Lee H. On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack. In *Proceedings of INFOCOM*, 2001; 338–347.
16. Snoeren A, Partridge C, Sanchez L, *et al*. Hash-based IP traceback. In *Proceedings of SIGCOMM*, 2001; 3–14.
17. Savage S, Wetherall D, Karlin AP, Anderson T. Practical network support for (IP) traceback. In *Proceedings of SIGCOMM*, 2000; 295–306.
18. Xu J, Lee W. Sustaining availability of web services under distributed denial of service attacks. *Transactions on Computers* 2003; **52**(2): 195–208.
19. Jin C, Wang H, Shin K. Hop-count filtering: an effective defense against spoofed DoS traffic. In *Proceedings of the 10th ACM Conference on Computer and Communications Security*, 2003; 30–41.
20. Jin S, Yeung D. A covariance analysis model for DDoS attack detection. In *Proceedings of the IEEE International Conference on Communications (ICC)*, vol. 4, June 2004; 1882–1886.
21. 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, 25–28 June 2008.
22. Liang J, Kumar R, Xi Y, Ross KW. Pollution in p2p file sharing systems. In *Proceedings of IEEE INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, vol. 2, 13–17 March 2005; 1174–1185.
23. Computer scientist fights threat of 'botnets'. *Science Daily*, 10 November 2007. Available at: http://www.sciencedaily.com/releases/2007/11/071108141303.htm
24. Knight FH. *Risk, Uncertainty, and Profit*. Hart, Schaffner & Marx; Houghton Mifflin Company: Boston, MA, 1921.
25. Alchian AA. Uncertainty, evolution, and economic theory. *The Journal of Political Economy (JSTOR)* 1950; **58**(3): 211–221. 1950.
26. Bächer P, Holz T, Kötter M, Wicherski G. Know your enenmy: tracking botnets. *The Honeynet Project & Research Alliance*, March 2005.
27. Know your enemy: tracking botnets. *The Honeynet Project*, 2008. Available at: http://www.honeynet.org/papers/bots/
28. Zou C, Cunningham R. Honeypot-aware advanced botnet construction and maintenance. In *International Conference on Dependable Systems and Networks*, Philadelphia, PA, 25–28 June 2006; 199–208.
29. Rajab MA, Zarfoss J, Monrose F, Terzin A. A multifaceted approach to understanding the botnet phenomenon. In *6th ACM SIGCOMM Conference on Internet Measurment, SESSION: Security and Privacy*, 2006; 41–52.
30. Rajab MA, Zarfoss J, Monrose F, Terzis A. My botnet is bigger than yours (maybe, better than yours): why size estimates remain challenging. In *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets*, Cambridge, MA, 2007; 5.
31. Grossklags J, Christin N, Chuang J. Security investment (failures) in five economic environments: a comparison of homogeneous and heterogeneous user agents. In *Proceedings of Workshop on the Economics of Information Security (WEIS '08)*, Hanover, New Hampshire, 25–28 June 2008.