A Game-Theoretical Approach for Finding Optimal Strategies in a Botnet Defense Model

Alain Bensoussan, Murat Kantarcioglu, Celine Hoe

University of Texas at Dallas

Abstract. Botnets are networks of computers infected with malicious programs that allow cybercriminals/botnet herders to control the infected machines remotely without the user's knowledge. In many cases, botnet herders are motivated by economic incentives and try to significantly profit from illegal botnet activity while causing significant economic damage to society. To analyze the economic aspects of botnet activity and suggest feasible defensive strategies, we provide a comprehensive game theoretical framework that models the interaction between the botnet herder and the defender group (network/computer users). In our framework, a botnet herder's goal is to intensify his intrusion in a network of computers for pursuing economic profits whereas the defender group's goal is to defend botnet herder's intrusion. The percentage of infected computers in the network evolves according to a modified SIS (susceptible-infectious-susceptible) epidemic model. For a given level of network defense, we define the strategy of the botnet herder as the solution of a control problem and obtain the optimal strategy as a feedback on the rate of infection. In addition, using a differential game model, we obtain two possible closed-loop Nash equilibrium solutions. They depend on the effectiveness of available defense strategies and control/strategy switching thresholds, specified as rates of infection. The two equilibria are either (1) the defender group defends at maximum level while the botnet herder exerts an intermediate constant intensity attack effort or (2) the defender group applies an intermediate constant intensity defense effort while the botnet herder attacks at full power.

1 Introduction

According to recent reports from Russian-based Kaspersky Labs [26] and Symantec [25], botnets (zombie networks)currently pose the biggest threat to the cybersecurity. In fact, Botnets have become a significant source of income for cybercriminals. According to [22], sources of income for the botnet business include distributed denial of service attacks, theft of confidential information, spam, phishing, search engine optimization) spam, click fraud, and distribution of adware and malicious programs.

To analyze the economic aspects of botnet activity and suggest feasible defensive strategies, we provide a comprehensive game theoretical framework that models the interaction between the botnet herder and the defender group (network/computer users). In our framework, a botnet herder's goal is to maximize his profits (equivalently minimize his cost) by intensifying his intrusion in

a network of computers whereas the defender group's goal is to maximize his profits/benefits (equivalently minimize his cost/loss) by defending the infection of computers. In view of the contagion of malicious programs used to expand botnets among computers, we model the evolution of percentage of infected computers in the network with an SIS epidemic model, in which a computer state may be either susceptible or infectious. The reason we work on an SIS model is due to the fact that a computer may be subject to multiple vulnerabilities and thus a computer is still vulnerable even recovering from one susceptibility.

Under a fixed level of defense applied by the defender group, we define botnet herder's optimal attack strategy as the solution to a cost minimization control problem. In addition, we solve the simultaneous move differential game between the botnet herder and the defender group. Each player optimizes his objective while considering their opponent's action. For the differential game, under equilibrium, we predict that either one of the players but not both will always play "full effort" strategy. The outcome hinges on the effectiveness of available defense strategies and control/strategy switching thresholds. Switching thresholds are determined by rates of infection, at which the player alters his action optimally. The existence of playing "full effort" strategy by one party under equilibrium is because the intermediate effort level strategy is not an admissible strategy. When the most effective defense strategy available cannot efficiently reduce the spread of malicious program, it drives the botnet activity towards the equilibrium where the defender group defends at maximum level and the botnet herder exerts an intermediate attack effort. One point to mention here is that the defender group can reduce the equilibrium infection size by posing sever penalties to botnet herder's attack effort. The other equilibrium is that the defender group exerts an intermediate defense effort and the botnet herder attacks at full power. This equilibrium occurs when the least effective defense strategy cannot efficiently deter the propagation of of malicious program but the most effective one can reduce the infection successfully. These results indicate that in some cases trying to defend against botnet activity may not be economically feasible instead the goal should be to limit the damage to an acceptable level. Also when significant resources are allocated to defend against particular botnet activity, botnet herders will choose to reduce their attack effort even if the defensive strategies are not very effective. To our knowledge, none of previous works suggested these two different equilibrium strategies.

2 Related Work

Our framework exploits the epidemic model[1] to characterize the fact that bots (infected machines) may spread malware to other hosts connected to the network . Studies related to epidemic models and computer worms in networks center on two themes. One theme focuses on the study of the epidemic thresholds on the network, for example [8]. The other theme combines the epidemic model

[1] This has been applied extensively to medical epidemics and has been applied to model the propagation of worms in the computer network.

with defense measures to study worm propagation in the presence of a defense measure, or to study the optimal patch deployment process across networks subject to contagion risk, for example, [16], [12] and among others.

Recognizing the defense measure taken by one individual in the network may have impacts on any other's security and defense strategy, researchers recently have combined the epidemic model with game theoretical modeling to capture interdependent security decisions. In [5], the authors combine an epidemic model for malware propagation in a network with a game model to study users' decisions whether to deploy security. [13] studies a network of interconnected agents' decisions about whether to invest some amount to self-protect and deploy security solutions which decrease the probability of contagion. The agents are subject to epidemic risks such as those caused by propagating viruses and worms. [14] studies a problem similar to [13] using local mean field analysis. Our paper instead focuses on the strategic interactions between the botnet herder and the defender group in which the infection of computers is subject to direct attack as well as propagation among hosts.

We develop a differential game model between the botnet herder and the defender group for simultaneous moves. Both players are strategic in their behavior, that is, they take actions that optimize their objective while also considering the actions of their opponent. The use of game theory in modeling interactions between an attacker and a defender has been adopted widely in the computer security domain recently. For example[18],[19] and [20] apply it to a network intrusion detection system, and [10] exploits it in modeling the network security. Most of the work focus on the matrix game setting. Our work focuses on continuous time state evolution and control application, solving differential games for optimal policies.

As botnet threats have become an increasing concern, the volume of research papers dealing with this issue increases. [22] discusses the economics of botnet in detail. [17] studies the use of honeypots to deter the development of a botnet. [13] studies the botnet security problem focusing on the interconnected host's security solution to the contagious risk of malware propagation. [23] models botnet related cybercrimes as a result of profit-maximizing decision making from the economic prospectives of both botnet masters and renters/attackers. They discuss how the uncertainty presented by honeypots can deter the botnet business.

This paper studies botnet problems in a game setting from two different angles. For a given level of network defense, like [23], we consider botnet related cybercrimes as a result of profit-maximizing (equivalently cost minimization) decision making. However, instead of studying how the uncertainty presented by honeypots can deter botnet business, we concentrate on finding the botnet herder's optimal attack strategy, a solution to a cost minimization control problem, given a fixed level of defense. In addition, unlike [23], we consider the contagious risk of malicious program spread among hosts. Similar to [13], we consider the interdependent security problem among the defender group by considering the contagious risk of malware propagation through contact. Nevertheless, we

employ the epidemic evolutionary process directly rather than exogenously assigning the transition probability of states as in [13]. For simultaneous moves, both botnet herder and the defender group take actions that optimize their objective in response to the actions of their opponent, different from [13], which considers game aspects in terms of interdependent security game within the defender group.

The other article similar to ours is [15] in which they mainly focus on one shot game between botnet herders and defenders and analyze botnet herder's attack coordinations as well as defender's interdependent security defense decision. They arrive at multiple Nash equilibria under different conditions. We focus on a continuous state evolution model, in which the state evolves according to the botnet herder's and the defender group's actions, so do the corresponding payoffs of both players. For a given level of network defense, we obtain botnet herder's optimal attack strategy as a feedback on the rate of infection; this prediction is somewhat similar to the appended short discussion of extensive-form games in [15], in which the equilibrium occurs at a certain level of attacks and defense. Surprisingly, for simultaneous moves, we arrive at different equilibrium results in which either one of the players will always play "full effort" strategies. Our prediction hinges on the effectiveness of available defense strategies and control/strategy switching thresholds, specified as rates of infection. The two possible closed-loop Nash equilibrium solution is either (1) the defender group defends at the maximum level while the botnent herder exerts an intermediate constant intensity of attack effort or (2) the defender group applies an intermediate constant defense effort while the the botnent herder attacks at full power.

3 Epidemic Model

In the area of virus and worm modeling, many studies have employed epidemiological models to understand the general characteristic of worm propagation. Depending on the model specifications, the state of a computer at a given time can be infectious, susceptible (vulnerable to a worm) or immune (excluded from further dynamics). In this study, we base our dynamics of number of infected computers in a network on the typical deterministic SIS model with some modifications to allow incorporating the attacker's and defender's strategies into the system dynamics. The formal definition of the classical SIS model is given in Sec. 3.1, and the modified one is given in Sec. 4.

3.1 Deterministic SIS Model

Because a computer may be subject to multiple vulnerabilities, a computer is still vulnerable even recovering from one susceptibility. Therefore, it is reasonable to work on an SIS model. In the classical SIS model, such as [9] and [4], a recovered host immediately becomes susceptible again. That is, in the SIS model, each host stays in one of two states: susceptible or infectious. For a fixed population system with N hosts, let $S(t)$ denote the number of susceptible hosts at time t

and $I(t)$ denote the number of infectious nodes at time t; then the dynamic of the system is described by the following set of differential equations:

$$\begin{cases} \frac{dy(t)}{dt} = -\beta x(t)y(t) + \gamma x(t),\ y(0) = 1 - x_0 \\ \frac{dx(t)}{dt} = \beta x(t)y(t) - \gamma x(t),\ x(0) = x_0,\ 0 \le x_0 \le 1 \end{cases},$$

where $y(t) = S(t)/N$, the percentage of susceptible nodes at time t, $x(t) = I(t)/N$, the percentage of infectious nodes at time t, $\beta \ge 0$ is the average number of transmissions possible from a given infected host in each period, and $\gamma \ge 0$ is the recovery rate. Since $dx/dt + dy/dt = 0$ and since $x(0) + y(0) = 1$, this implies that $x(t) + y(t) = 1$ for all $t \ge 0$. Now let $y(t) = 1 - x(t)$, we need only use the percentage of infected computers to completely describe the network dynamics.

4 The State Equation

Our model bases on the classical SIS model with some modifications given:

$$\begin{aligned} \frac{dx(t)}{dt} =& cv_H\big(x(t)\big)\big(1 - x(t)\big) + \beta x(t)\big(1 - x(t)\big) \\ & - \big(\gamma_{\min} + v_D\big(x(t)\big)(\gamma_{\max} - \gamma_{\min})\big)x(t),\ x(0) = x_0,\ 0 \le x_0 \le 1 \end{aligned}$$

The time argument will be suppressed in future where no confusion arises. Thus, we rewrite the state equation as:

$$\frac{dx}{dt} = cv_H(x)(1 - x) + \beta x(1 - x) - \big(\gamma_{\min} + v_D(x)(\gamma_{\max} - \gamma_{\min})\big)x,\ 0 \le x_0 \le 1 \tag{1}$$

In (1),

1. $cv_H(x)(1 - x)$ expresses the increment of percentage of infected computers due to botnet herder's ongoing direct attack effort (not from contagion), where c is the average attack successful rate, $v_H(x) \in [0, 1]$ is the attack effort intensity, the botnet herder's control, indicating how aggressively the botnet herder tries to intensify his intrusion.
2. $v_D(x) \in [0, 1]$ depicts the defender group's defense effort, the defender group's control. In our specification, we assume that there is a set of available defense strategies which can range the effectiveness of defense from minimum level to maximum level, and we relate the effectiveness to the coefficient γ, assigning the corresponding minimum and maximum level of protection by $\gamma_{\min}$, and $\gamma_{\max}$ respectively. From the term $\gamma_{\min} + v_D(x)(\gamma_{\max} - \gamma_{\min})\big)$, it is clear that, through the decision of the defense effort (the control), $v_D(x)$, the defender group is able to attain the effectiveness of defense provided by available defense strategies within the range of minimal effectiveness and maximal effectiveness. For example, if $v_D(x) = 1$, the defender group exercises full defense effort to achieve the maximal effectiveness of defense provided by the available defense strategies, thus achieving defense level $\gamma_{\max}$.

5 Attack and Defense Game between Botnet Herder and Defender Group

We begin with a simplified game first, in which the botnet herder solves his optimal intrusion in response to a given level of defense strategies, and continue with a simultaneous move game between the botnet herder and the defender group, in which both parties solve their own optimal strategy in response to their opponent's action.

5.1 Main Assumption

We first briefly justify the rationality of main assumptions used in the model.

1. Botnet herder's operational cost function $f_H(x)$ satisfies the conditions $f_H(x)' < 0$ and $f_H(x)'' > 0$, where x is the percentage of infected computers in the network. This assumption implies that botnet herder's operational cost decreases at a decreasing rate as the number of infected computer increases. In fact, the botnet herder's operational cost can be defined as the sum of fixed development cost[2] and the loss from mismatching market demand[3]. We present an explicit example of the possible cost function. Given a fixed network size N, assuming that the development cost of the malicious program is $\overline{C} > 0$ and per unit loss from mismatching matching marketing demand is $b > 0$ with market demand $D > 0$, we can simply specify the botnet herder's operational cost function as:$f_H(x) = \overline{C} + b \times e^{D-Nx}$, which clearly satisfies the condition $f_H(x)' < 0$ and $f_H(x)'' > 0$. The first term captures the fact of free duplicates after development, and the second term captures the loss from mismatching market demand.
2. Defender group's operational cost function (equivalently, loss value function) $f_D(x)$ satisfies $f_D(x)' > 0$ and $f_D(x)'' > 0$. It is expected that the defending cost increases at an increasing rate as the number of infected machine increases because the complexity of workloads and defending software programs escalates and more professionals are needed.
3. The recovery rate provided by the defense strategy is faster than the contact transmission rate, i.e., $\gamma > \beta$ (or $\gamma_{\max} > \beta$). This is a reasonable assumption since otherwise it may imply the case that all computers in the network are compromised.
4. $x_H^* < x_D^*$: The steady-state infection percentage achieved when the botnet herder exerts an intermediate attack effort and the defender group defends at the maximum level is less than steady-state infection percentage reached by the situation where the defender group exerts an intermediate defense effort and the botnet herder attacks at the maximum level. This assumption is intuitively understandable, since, cetris paribus, full attack coupled with an intermediate level of defense shall cause a higher infection rate than the maximal defense coupled with an intermediate level of attack.

[2] Once the malicious program is developed, it is free to duplicate.

[3] By [22], the more bots that the botnet herder owns, the more they can charge for their bots

5.2 Game under a Fixed Level of Defense

We start with a simple game first. In this game, we assume that the botnet herder is able to observe the defender's defense strategy fixed at a certain level. It is reasonable to assume that defenders' actions are observable to the botnet herder since defenders are "known" subjects to the botnet herder, but not vice versa. The assumption of the defense strategy fixed at a certain level may be viewed as an application of Nash equilibrium achieved in five different interdependent security games by [7] given a fixed probability of attack assumption. Under this game, the problem of interest will be the botnet herder's optimal strategy. Therefore, we do not need to consider the defender group's strategy and action (the control); thus, for ease of presentation, we rewrite the state equation (1) as:

$$\frac{dx}{dt} = cv(x)(1-x) + \beta x(1-x) - \gamma x,\ x(0) = x_0,\ 0 \le x_0 \le 1. \tag{2}$$

Let $f(x)$ be botnet herder's cost function with $f'(x) < 0$, and $f''(x) > 0$. Next, let $k > 0$, a constant, be the per unit time cost associated with botnet herder's attack effort; thus his total cost of attack effort per unit time is $v(x) \times k$. Note that we may interpret this effort cost as the extra penalty cost from increasing probability of getting caught due to the increasing severity of attack. This is in fact an observed phenomenon in the real world botnet operation as suggested by [24] and [15]. The botnet herder's objective, subject to the dynamics of (2), is to minimize the discounted total cost (operation cost plus effort cost) with a constant discount rate r over an infinite time horizon:

$$\begin{cases} \inf_{v(\cdot)} \left\{ J_x\big(v(\cdot)\big) = \int_0^\infty e^{-rt}\big(f(x) + kv(x)\big)dt \right\} \\ 0 \le v(x) \le 1 \end{cases}. \tag{3}$$

For this fixed level of defense game, botnet herder's optimization problem can in fact be viewed as a control problem, where the control, the intensity of attack effort $v(x)$, is the strategy that botnet herder can take. To solve the minimization problem, we form the current value Hamiltonian associated with (3) given:

$$H(x, v(x), p) = f(x) + kv(x) + p\big(cv(1-x) + \beta x(1-x) - \gamma x\big). \tag{4}$$

The first two terms in (4), $f(x) + kv(x)$, represent botnet herder's instantaneous cost, while the third term represents the future cost of percentage change of infected computers. We can interpret $p(t)$ as the botnet herder's marginal cost at time t. The optimal control, $\hat{v}(x)$, is obtained by minimizing the Hamiltonian H. Because the Hamiltonian is linear in $v(x)$, the optimal control, $\hat{v}(x)$ takes the following bang-bang and (a possible) singular form:

$$\hat{v}(x) = \begin{cases} 1 & \text{if } H_v < 0 \\ u\ (0 < u < 1, \text{ to be determined}) & \text{if } H_v = 0 \\ 0 & \text{if } H_v > 0, \end{cases} \tag{5}$$

where $H_v = \frac{\partial H}{\partial v(x)} = k + pc(1-x)$. When H_v is negative, the botnet herder exerts full attack effort ($v(x) = 1$), and when H_v is positive, the botnet herder exerts zero attack effort ($v(x) = 0$). When $H_v = 0$ and stays at this value, an intermediate level of effort $0 < u < 1$ is exerted. This phase is referred to as singular. The singular region has the additional property that the values of the control and the state variables are constant in this region; that is, it exhibits a steady-state property.

The adjoint equation is:

$$\dot{p} = -\frac{\partial H}{\partial x} + rp == -f'(x) + p\big(cv + \beta(2x-1) + \gamma + r\big). \tag{6}$$

Differentiating H_v with respect to t, we have:

$$\dot{H}_v = \dot{p}c(1-x) - pc\dot{x}. \tag{7}$$

Substituting (2) and (6) into (7), and set (7) equal to zero, we obtain:

$$f'(x) = \frac{k}{c(1-x)}\big(\beta(1-x) - \frac{\gamma}{1-x} - r\big). \tag{8}$$

We can solve (8) for the steady state percentage of infected computers, x^*, a constant; the optimal control $\hat{v}(x)$ in this singular region is a fixed rate and found by solving $\dot{x} = 0$ at x^*:

$$\hat{v}(x) = u = -\frac{\beta x^*(1-x^*) - \gamma x^*}{c(1-x^*)}. \tag{9}$$

Equation (9) indicates that, like the steady-state percentage of infected computer, the intensity of attack effort in the singular region, u, is also constant.

In the following Theorem 1, we describe the botnet herder's optimal attack strategy (control policy) given a fixed level of defense from the defender group.

Theorem 1. *The optimal feedback of the botnet herder is given:*

$$\hat{v}(x) = \begin{cases} 1 \ \textit{if}\, x < x^* \\ u \ \textit{if}\, x = x^* \\ 0 \ \textit{if}\, x > x^*, \end{cases} \tag{10}$$

where $u = -\frac{\beta x^*(1-x^*) - \gamma x^*}{c(1-x^*)}$, *and* $x^* < \frac{\sqrt{(c+\gamma-\beta)^2+4c\beta}-(c+\gamma-\beta)}{2\beta}$.

Proof. See Appendix A. □

Theorem 1 states that if the starting percentage of infected computer $x_0 > x^*$, then it is optimal for the botnet herder to "reduce" his percentage of invasion in the network to x^* by exerting zero attack effort, i.e., $\hat{v}(x) = 0$. The reason is that once the percentage of infection passes the steady-state level, x^*, the opportunity cost of getting caught/traced outweighs the size benefits of the

operation cost. If $x_0 < x^*$, then the botnet herder aggressively leverages his infection in the network by applying full attack effort, $\hat{v}(x) = 1$, to increase the percentage of infected computer up to x^*. If $x = x^*$, then the constant intensity of attack effort, $\hat{v}(x) = u$, would be implemented by the botnet herder and stays at the same level afterwards. The prediction of converging to an optimal steady state level corresponds to the recent observation of dormant Confiker botnet.[24]

5.3 Nash Game between Botnet Herder and Defender Group

We now consider a simultaneous move game. The botnet herder now optimizes his operation taking into account defender group's simultaneous dynamic interaction and so does the defender group.

A. Botnet Herder The botnet herder's problem is similar to Sec. 5.2 except that now he must consider defender group's action in solving his optimization problem. Due to introducing another player, we now denote botnet herder's cost function by $f_H(\cdot)$, control by $v_H(x)$ and the cost of effort per unit time by k_H.

B. Defender Group As described in Sec. 4, there exists a set of available defense strategies which can range the effectiveness of defense from minimal level to maximal level, and we relate the effectiveness to the coefficient γ, assigning the corresponding minimal and maximal level of protection by $\gamma_{\min}$, and $\gamma_{\max}$ respectively. The defender group chooses their optimal strategy by exerting their defense effort $v_D(x) \in [0, 1]$, which can in turn allow the defender group to attain the effectiveness of defense within the range of minimal effectiveness and maximal effectiveness.

Without doubt, the defender group needs to pay costs to defend against infection. We relate the defender group's operational cost with percentage of infected computers denoted by $f_D(x)$ with $f'_D(x) > 0$, and $f''_D(x) > 0$. In addition, like the botnet herder's problem, we associate the defender group with a constant effort cost, $k_D > 0$, per unit time, and thus his total defense effort cost per unit time is $v_D(x) \times k_D$. It is reasonable to assume that defender group's defense effort cost increases as additional defense efforts exerted to achieve a higher level of defense. The defender group's problem is to minimize discounted total cost (operation cost plus effort cost) over an infinite time horizon taking into account the botnet herder's action.

C. State Equation Recall From Sec. 4, the dynamics of percentage of infected computers in a network taking into account both parties' strategies is given:

$$\frac{dx}{dt} = cv_H(x)(1-x) + \beta x(1-x) - \big(\gamma_{\min} + v_D(x)(\gamma_{\max} - \gamma_{\max})\big)x,\ 0 \le x_0 \le 1 \tag{11}$$

D. Differential Game The botnet herder's optimization problem is given:

$$\begin{cases} \phi_H(x) = \inf_{v_H(\cdot)} \left\{ J_x^H\big(v_H(\cdot), v_D(\cdot)\big) = \int_0^\infty e^{-rt}\big(f_H(x) + k_H v_H\big)dt \right\} \\ 0 \le v_H \le 1 \end{cases},$$

and the defender group's optimization problem is given:

$$\begin{cases} \phi_D(x) = \inf_{v_D(\cdot)} \left\{ J_x^D\big(v_H(\cdot), v_D(\cdot)\big) = \int_0^\infty e^{-rt}\big(f_D(x) + k_D v_D\big)dt \right\} \\ 0 \le v_D(x) \le 1 \end{cases};$$

both are subject to the dynamics of (11). For ease of presentation, we will use v_H and v_D in replace of $v_H(x)$ and $v_D(x)$ where no confusion arises. The current value Hamiltonian associated with the botnet herder's and defender group's optimization problems are given in (12) and (13) respectively:

$$\begin{aligned} H^H(x, v_H, v_D, p_1) =& f_H(x) + v_H k_H + p_1\big(c v_H(1-x) \\ &+ \beta x(1-x) - \big(\gamma_{\min} + v_D(\gamma_{\max} - \gamma_{\min})\big)x\big). \end{aligned} \tag{12}$$

$$\begin{aligned} H^D(x, v_H, v_D, p_2) =& f_D(x) + v_D k_D + p_2\big(c v_H(1-x) \\ &+ \beta x(1-x) - \big(\gamma_{\min} + v_D(\gamma_{\max} - \gamma_{\min})\big)x\big). \end{aligned} \tag{13}$$

The interpretations of (12) and (13) are similar to (4). The optimal controls of the botnet herder and the defender group, $\hat{v}_H$ and $\hat{v}_D$, are obtained by minimizing the corresponding Hamiltonian, H^H and H^D. Because the Hamiltonian is linear in the corresponding controls, v_H and v_D, the optimal controls, $\hat{v}_H$ and $\hat{v}_D$, take the bang-bang-(possible)singular forms, which are given in (14) and (15) respectively:

$$\begin{aligned} &\hat{v}_H = \mathbb{1}_{H^H_{v_H}<0} + u_H \mathbb{1}_{H^H_{v_H}=0}, \text{ where } 0 < u_H < 1 \text{ is to be determined,} \\ &\text{and } H^H_{v_H} = \frac{\partial H^H}{\partial v_H} = k_H + p_1 c(1-x). \end{aligned} \tag{14}$$

$$\begin{aligned} &\hat{v}_D = \mathbb{1}_{H^D_{v_D}<0} + u_D \mathbb{1}_{H^D_{v_D}=0}, \text{ where } 0 < u_D < 1 \text{ is to be determined,} \\ &\text{and } H^D_{v_D} = \frac{\partial H^H}{\partial v_D} = k_D - p_2(\gamma_{\max} - \gamma_{\min}). \end{aligned} \tag{15}$$

Equation (14) tells us that when $H^H_{v_H}$ is negative, the botnet herder exerts full attack effort ($v_H = 1$), when $H^H_{v_H}$ is positive, the botnet herder exerts zero attack effort ($v_H = 0$) and when $H^H_{v_H} = 0$ and stays at this value, an intermediate level of effort $0 < u_H < 1$ is exerted. The interpretation for (15) is the same.

E. Equilibrium Solution We look for a Nash equilibrium solution such that

$$J_x^H\big(\hat{v}_H(\cdot), \hat{v}_D(\cdot)\big) \le J_x^H\big(v_H(\cdot), \hat{v}_D(\cdot)\big),\ v_H \in [0,1]. \tag{16}$$

$$J_x^D\big(\hat{v}_H(\cdot), \hat{v}_D(\cdot)\big) \le J_x^D\big(\hat{v}_H(\cdot), v_D(\cdot)\big),\ v_D \in [0,1]. \tag{17}$$

Employing (14) and (15), we can write the Hamiltonians ,(12) and (13), with the bang-bang-singular optimal controls as:

$$\hat{H}^{H}(x,\hat{v}_{H},\hat{v}_{D},p_1,p_2) = f_{H}(x) - \big(k_{H} + p_1 c v_{H}(1-x)\big)^{-} + p_1\big(\beta x(1-x) - \gamma_{\min}x\big) - p_1(\gamma_{\max}-\gamma_{\min})x\big(\mathbb{1}_{H^{D}_{v_D}<0} + u_{D}\mathbb{1}_{H^{D}_{v_D}=0}\big). \quad (18)$$

$$\hat{H}^{D}(x,\hat{v}_{H},\hat{v}_{D},p_1,p_2) = f_{D}(x) - \big(k_{D} - p_2(\gamma_{\max}-\gamma_{\min})x\big)^{-} + p_2(\beta x(1-x) - \gamma_{\min}x) + p_2 c(1-x)\big(\mathbb{1}_{H^{H}_{v_H}<0} + u_{H}\mathbb{1}_{H^{H}_{v_H}=0}\big). \quad (19)$$

From Dynamic Programming, the Nash equilibrium solution must satisfy the following system of Bellman equations:

$$\begin{cases} r\phi_{H}(x) = \hat{H}^{H}(x,\hat{v}_{H},\hat{v}_{D},\phi'_{H}(x),\phi'_{D}(x)) \\ r\phi_{D}(x) = \hat{H}^{D}(x,\hat{v}_{H},\hat{v}_{D},\phi'_{H}(x),\phi'_{D}(x)) \end{cases} . \quad (20)$$

Before proceeding further, we define the following notations for facilitating presentation:

- Define θ_{H} as the switching threshold for the botnet herder such that $\hat{v}(\theta_{H}) = 1,\ \text{if}\ x < \theta_{H},\ \text{and}\ \hat{v}(\theta_{H}) = 0,\ \text{if}\ x > \theta_{H}$.
- Define θ_{D} as the switching threshold for the defender group such that $\hat{v}(\theta_{D}) = 0,\ \text{if}\ x < \theta_{D},\ \text{and}\ \hat{v}(\theta_{D}) = 1,\ \text{if}\ x > \theta_{D}$.
- Define $\gamma = \gamma_{\max} - \gamma_{\min}$.

We are now ready to state solutions related to (20).

Theorem 2. *Assume $x^{*}_{H} < x^{*}_{D}$ where x^{*}_{H}, and x^{*}_{D} are solutions to $F_{H}(x) = f'_{H}(x)c(1-x) + k_{H}\big(r - \beta(1-x) + \frac{\gamma_{\max}}{1-x}\big) = 0$ and $F_{D}(x) = f'_{D}(x)\gamma x - k_{D}\big(r + \beta x + \frac{c}{x}\big) = 0$ respectively. There exist two Nash equilibrium solutions:*

1. *For $\theta_{H} = x^{*}_{H}$ and $\theta_{D} \le x^{*}_{H}$.*
   Assume (i) $\beta < \gamma_{\max}$ and (ii) $c(1-x^{*}_{H}) + \beta x^{*}_{H}(1-x^{*}_{H}) - \gamma_{\max}x^{*}_{H} > 0$.
   There exists a equilibrium solution at x^{*}_{H} such that the botnet herder applies optimal feedback policy with $\hat{v}_{H}(x^{*}_{H}) = u_{H} = -\frac{1}{c(1-x^{*}_{H})}\big(\beta x^{*}_{H}(1-x^{*}_{H}) - \gamma_{\max}x^{*}_{H}\big)$ and the defender group applies the optimal policy $\hat{v}_{D}(x^{*}_{H}) = 1$. The optimal feedback for the botnet herder and the defender group can be summarized as:
   Botnet Herder:

$$\hat{v}_{H}(x) = \begin{cases} 1 & if\, x < x^{*}_{H} \\ u_{H} & if\, x = x^{*}_{H} \\ 0 & if\, x > x^{*}_{H} \end{cases} . \quad (21)$$

   Defender Group:

$$\hat{v}_{D}(x) = \begin{cases} 1\ if\, x > \theta_{D} \\ 0\ if\, x < \theta_{D} \end{cases} , and\ \hat{v}_{D}(x^{*}_{H}) = 1. \quad (22)$$

2. *For $\theta_D = x_D^*$ and $x_D^* < \theta_H$.*
Assume (i) $c(1-x_D^*)+\beta x_D^*(1-x_D^*)-\gamma_{\max}x_D^* < 0$. and (ii) $c(1-x_D^*)+\beta x_D^*(1-x_D^*)-\gamma_{\min}x_D^* > 0$. There exists a equilibrium solution at x_D^* such that the botnet herder applies optimal feedback policy with $\hat{v}_H(x_D^*) = 1$ and the defender group applies the optimal policy $\hat{v}_D(x_D^*) = u_D = \frac{c(1-x_D^*)+\beta x_D^*(1-x_D^*)-\gamma_{\max}x_D^*}{\gamma x_D^*}$. The optimal feedback for the botnet herder and the defender group can be summarized as:
Botnet Herder:

$$\hat{v}_H(x) = \begin{cases} 1 \text{ if } x < \theta_H \\ 0 \text{ if } x > \theta_H \end{cases}, \text{and } \hat{v}_H(x_D^*) = 1. \tag{23}$$

Defender Group:

$$\hat{v}_D(x) = \begin{cases} 1 & \text{if } x > x_D^* \\ u_D & \text{if } x = x_D^* \\ 0 & \text{if } x < x_D^* \end{cases}. \tag{24}$$

In addition, if

1. $c(1-x_H^*) + \beta x_H^*(1-x_H^*) - \gamma_{\max}x_H^* > 0$,
2. $c(1-x_D^*) + \beta x_D^*(1-x_D^*) - \gamma_{\max}x_D^* < 0$,
3. $c(1-x_D^*) + \beta x_D^*(1-x_2^*) - \gamma_{\min}x_D^* > 0$,

and $\tilde{x}_H > x_D^*$, $\tilde{x}_D < x_H^*$, we can either take $\theta_H = \theta_D = x_H^*$ or $\theta_H = \theta_D = x_D^*$.

Proof. See Appendix B. □

The above theorem states that there are two possible Nash equilibria.One equilibrium occurs at the infection rate equal to x_H^*, a steady-state solution to the botnet herder's minimization problem given the full defense effort exerted from the defender group. This equilibrium occurs when the available defense strategy with maximal effectiveness cannot efficiently reduce the spread of malicious program; thus an intermediate defense effort is not an admissible strategy (control) for the defender group. This is an equilibrium such that the state remains at $x_H^* > \theta_D$. The botnet herder will exert full attack effort if $x < x_H^*$, exert zero attack effort if $x > x_H^*$, and apply the intermediate constant control $\hat{v}_H(x^*) = -\frac{1}{c(1-x_1^*)}\left(\beta x_H^*(1-x_H^*) - \gamma_{\max}x_H^*\right)$ when $x = x_H^*$ and the state and the attack effort will remain at this level. The defender group applies zero defense effort (i.e., $v_D = 0$) if $x < \theta_D$ and maximum defense effort (i.e., $v_D = 1$) if $x > \theta_D$. At $x = \theta_D$, the defender group is indifferent in taking either control since the state cannot remain on θ_D. When the state reaches x_H^*, the equilibrium occurs and will stay at this level in which the botnet herder applies the intermediate constant control u_H and the defender group maximizes his defense effort.

The other equilibrium occurs at the infection rate $x_D^* < \theta_H$, a solution to the defender group's steady-state minimization problem given the full attack effort from the botnet herder. This equilibrium occurs in the environment where the

available defense strategy with minimal effectiveness cannot efficiently deter the propagation of of malicious program, but the one with maximal effectiveness can reduce the infection successfully. In this environment, an intermediate level of attack effort is not admissible to the botnet herder. This is an equilibrium such that the state remains at $x_D^* < \theta_H$. The interpretation of the optimal feedback policy for the botnet herder and the defender group is similar to the above paragraph.

The equilibrium solution in which the botnet herder exerts a constant attack effort, $u_H \in (0,1)$ and the defender maximizes his defense level is consistent with the observation for Confiker botnet. The Confiker botnet herder decides to stay dormant since the size of the botnets (i.e., infected computers) is too big to keep the probability of getting caught low. Apparently there is not a powerful defense strategy which can successfully deter the infection from this known Confiker botnet. In the equilibrium, the best that defender group can do is to apply maximal defense level available. On the contrary, though the defense strategy cannot effectively deter the infection, the owner of Confiker botnet will not exert full attack to gain higher infection rate since the penalty from being too big is severe. The other equilibrium solution in which the defender group exerts a constant defense level, $u_D \in (0,1)$ and the botnet herder applies full attack effort is a situation where this equilibrium infection size yields most benefits to both parties.

6 Conclusion

In this paper, we study botnet business as a game between the botnet herder and the defender group in which the dynamics of infected computers evolve according to a modified SIS epidemic model taking into account both parties' actions. For a given level of defense of the network, we obtain the botnet herder's optimal strategy as a feedback on the rate of infection. For simultaneous moves, both players are strategic in their behavior. We solve the differential game and obtain two possible closed-loop Nash equilibrium solutions. These predictions provide insights to the network society as to how the botnet business equilibrium might look like given available defense strategies. In addition, the optimal feedback policies might offer some guidelines for the network society as to how to respond to the botnet attack strategically optimal. Realizing that the evolution of infected computers may not be fully controlled by the group of botent herder and the defender group through their available strategies alone, we are working on extending the SIS dynamics into the one subject to stochastic disturbances [1].

A Proof Theorem 1

Lemma 1. *Set:*

$$F(x) = f'(x)c(1-x) + k\big(r - \beta(1-x) + \frac{\gamma}{1-x}\big) \tag{25}$$

Assume: $f'(0)c + k(r+\gamma-\beta) < 0$. *There exists a unique* x^* *such that* $F(x^*) = 0$.

Proof. From (25), we have $F(1) = \infty$ and $F(0) < 0$. In addition, we have $F'(x) = c\big(f''(x)(1-x) - f'(x)\big) + k\beta + \frac{k\gamma}{(1-x)^2} > 0$ since $f''(x) > 0$ and $f' < 0$. The result thus follows. □

Lemma 2. *Assume (1) $\beta < \gamma$, and (2) $(\beta x^* + c)(1-x^*) - \gamma x^* > 0$ where x^* is the unique solution to (25). We have $x^* < \frac{\sqrt{(c+\gamma-\beta)^2+4c\beta}-(c+\gamma-\beta)}{2\beta}$, which is a solution to a long-run steady state, $\dot{x} = 0$ with $v(x) = 1$.*

Proof. There is only one 0 for $G(x) = (\beta x + c)(1-x) - \gamma x,\ x \in (0,1)$, which is at $x = \frac{\sqrt{(c+\gamma-\beta)^2+4c\beta}-(c+\gamma-\beta)}{2\beta}$. The result follows directly. □

After establishing useful lemmas, we turn to the proof of Theorem 1.

Proof. We proceed first by relying Dynamic Programming arguments and then complete with verification of effectiveness of optimal control trajectories.

We first rely on Dynamic Programming (DP) arguments. It is well known that if the value function is smooth, the corresponding feedback leads to an optimal solution. The botnet herder's value function is defined as:

$$\phi(x) = \inf_{v(\cdot)} \big\{ J_x\big(v(\cdot)\big) = \int_0^\infty e^{-rt}\big(f(x) + kv\big)dt \big\}. \tag{26}$$

By DP, we can write the Bellman equation:

$$\begin{aligned} r\phi(x) &= \inf_{v(\cdot)} \big[f(x) + vk + \phi'(x)\dot{x} \big] \\ &= \inf_{v(\cdot)} \big[f(x) + vk + \phi'(x)\big(cv(1-x) + \beta x(1-x) - \gamma x\big) \big] \\ &= \inf_{v(\cdot)} H(x, v, \phi'(x)) \\ &= \inf_{v(\cdot)} H(x, v, p), \text{ where } p = \phi'(x). \end{aligned} \tag{27}$$

From (5), we know that the optimal control, $\hat{v}$ takes the form:

$$\hat{v} = \mathbb{1}_{k+pc(1-x)<0} + u\mathbb{1}_{k+pc(1-x)=0}, \tag{28}$$

and we can rewrite the Hamiltonian as:

$$H(x, v, p) = f(x) + p\big(\beta x(1-x) - \gamma x\big) - \big(k + pc(1-x)\big)^-;$$

hence:

$$\begin{aligned} r\phi(x) &= f(x) + p\big(\beta x(1-x) - \gamma x\big) - \big(k + pc(1-x)\big)^- \\ &= f(x) + \phi'(x)\big(\beta x(1-x) - \gamma x\big) - \big(k + \phi'(x)c(1-x)\big)^-. \end{aligned} \tag{29}$$

Now, set $z(x) = k + \phi'(x)c(1-x)$, we have $z'(x) = c\big(\phi''(x)c(1-x) - \phi'(x)\big)$. Set $F(x) = f'(x)c(1-x) + k\big(r - \beta(1-x) + \frac{\gamma}{1-x}\big)$. Employing (29), we obtain:

$$z'(x) - z(x)\frac{r - \beta(1-x) + \frac{\gamma}{1-x}}{(\beta x + c\mathbb{1}_{z(x)<0})(1-x) - \gamma x} + \frac{F(x)}{(\beta x + c\mathbb{1}_{z(x)<0})(1-x) - \gamma x} = 0. \tag{30}$$

If $k+\phi'(x)c(1-x)<0$ (i.e., $z(x)<0$), by (30), we have:

$$\frac{d}{dx}\left[z(x)e^{-\int_0^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}\right]+\frac{F(x)}{(\beta x+c)(1-x)-\gamma x}e^{-\int_0^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}=0. \tag{31}$$

If $k+\phi'(x)c(1-x)>0$ (i.e., $z(x)>0$), by (30), we have:

$$\frac{d}{dx}\left[z(x)e^{\int_x^1 \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}\right]+\frac{F(x)}{\beta x(1-x)-\gamma x}e^{\int_x^1 \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}=0. \tag{32}$$

We look for an optimal strategy such that:

$$\hat{v}(x)=\begin{cases}1 \text{ if } x<x^*\\ u \text{ if } x=x^*\\ 0 \text{ if } x>x^*,\end{cases} \tag{33}$$

For $x^*<x<1$, by (32), we set:

$$z(x)e^{\int_x^1 \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}+\int_{x^*}^x \frac{F(\zeta)}{\beta\zeta(1-\zeta)-\gamma x}e^{\int_\zeta^1 \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}d\zeta=0, \tag{34}$$

hence

$$z(x)=-\int_{x^*}^x \frac{F(\zeta)}{\beta\zeta(1-\zeta)-\gamma x}e^{\int_\zeta^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}d\zeta. \tag{35}$$

The condition $z(x)>0$ is clearly satisfied. To complete the proof for this region, we also need to establish $z(x)$ satisfies the boundary condition for $z(1)=k$ when $x\to 1$. Note that (35) can also be written as:

$$z(x)=k-ke^{\int_{x^*}^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}-\int_{x^*}^x \frac{f'(x)c(1-\zeta)}{\beta\zeta(1-\zeta)-\gamma\zeta}e^{\int_\zeta^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}d\zeta, \tag{36}$$

which shows that $z(x)\to 1$ as $x\to 1$ since $e^{\int_\zeta^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}\le\frac{1-x}{1-\zeta}$ and $|\int_{x^*}^x \frac{f'(\zeta)c(1-\zeta)}{\beta\zeta(1-\zeta)-\gamma\zeta}e^{\int_\zeta^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}d\zeta|\le C(1-x)(x-x^*)$. The boundary at $x=1$ is satisfied.

Next, for $0<x<x^*$, by (31), we set:

$$-z(x)e^{-\int_0^x \frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}+\int_x^{x^*} \frac{F(\zeta)}{(\beta\zeta+c)(1-\zeta)-\gamma\zeta}e^{-\int_0^z eta\frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}d\zeta=0, \tag{37}$$

hence

$$z(x)=\int_x^{x^*} \frac{F(\zeta)}{(\beta\zeta+c)(1-\zeta)-\gamma\zeta}e^{-\int_x^z eta\frac{r-\beta(1-\xi)+\frac{\gamma}{1-\xi}}{(\beta\xi)(1-\xi)-\gamma\xi}d\xi}d\zeta, \tag{38}$$

and we obtain $z(x) > 0$ since inside the integral $F(\zeta) < 0$, and, by assumption 2, $(\beta\zeta + c)(1-\zeta) - \gamma\zeta > 0$.
Finally, at $x = x^*$, we have $z(x^*) = 0$. Using $\phi'(x^*) = \frac{-k}{c(1-x^*)}$ with (27), we obtain x^* satisfies:

$$r\phi(x^*) = f(x^*) - \frac{k}{c(1-x^*)}(\beta x^*(1-x^*) - \gamma x^*), \tag{39}$$

and $f'(x^*)c(1-x^*) + k(r - \beta(1-x^*) + \frac{\gamma}{1-x^*}) = F(x^*) = 0$. By Lemma 1, x^* is uniquely defined. Also by Lemma 2, we have $x^* < \frac{\sqrt{(c+\gamma-\beta)^2+4c\beta}-(c+\gamma-\beta)}{2\beta}$. For $x = x^*$, (38) corresponds to a fixed rate $x(t) = x^*$. By setting $\dot{x}|_{x=x^*} = 0$, we obtained the optimal control as:

$$\hat{v} = u = \frac{\beta x^*(1-x^*) - \gamma x^*}{c(1-x^*)}.$$

Therefore, we have obtained the optimal feedback of the botnet herder:

$$\hat{v}(x) = \begin{cases} 1 \text{ if } x < x^* \\ u \text{ if } x = x^* \\ 0 \text{ if } x > x^* \end{cases}. \tag{40}$$

To complete the proof, we proceed with verification of the effectiveness of the optimal trajectories and we obtain the desired results. Detailed verification procedures are available upon request. □

B Proof of Theorem 2

We first state the following useful lemma, which provide the uniqueness property of potential signular-control solutions.

Lemma 3. *Define:*

$$F_{H}(x) = f'_{H}(x)c(1-x) + k_{H}\big(r - \beta(1-x) + \frac{\gamma_{\max}}{1-x}\big). \tag{41}$$

$$\widetilde{F}_{H}(x) = f'_{H}(x)c(1-x) + k_{H}\big(r - \beta(1-x) + \frac{\gamma_{\min}}{1-x}\big). \tag{42}$$

$$F_{D}(x) = f'_{D}(x)\gamma x - k_{D}\big(r + \beta x + \frac{c}{x}\big). \tag{43}$$

$$\widetilde{F}_{D}(x) = f'_{D}(x)\gamma x - k_{D}\big(r + \beta x\big). \tag{44}$$

Assume:
(1) $f'_{D}(0)\gamma > k_{D}\beta$.
(2) $f'_{H}(0)c + k_{H}(r + \gamma_{\max} - \beta) < 0$, *and* $f'_{D}(1) - k_{D}(r + \beta + c) > 0$.
Then there exist unique x^*_{H}, x^*_{D}, $\tilde{x}_{H}$, $\tilde{x}_{D}$ *such that*

$$\begin{cases} F_{H}(x^*_{H}) = 0, & F_{D}(x^*_{D}) = 0, \\ \widetilde{F}_{H}(\tilde{x}_{H}) = 0, & \widetilde{F}_{D}(\tilde{x}_{D}) = 0. \end{cases} \tag{45}$$

Hence also $\tilde{x}_{H} > x^*_{H}$ *and* $\tilde{x}_{H} < x^*_{H}$.

Proof. By assumption (1) and botnet herder's and defender's operational cost function assumptions, which are $f'_{H}(x) < 0,\ f''_{H}(x) > 0,\ f'_{D}(x) > 0$, and $f''_{D}(x) > 0$, we have $F'_{H}(x) > 0,\ F'_{D}(x) > 0,\ \widetilde{F}'_{H}(\tilde{x}) > 0,\ \widetilde{F}'_{D}(\tilde{x}) > 0$; thus all functions are monotone increasing. By assumption (2), we have $F'_{H}(0) < 0,\ \widetilde{F}'_{H}(0) < 0,\ F'_{H}(1) = \infty,\ \tilde{F}'_{H}(1) = \infty,\ F'_{D}(0) = -\infty, \widetilde{F}'_{D}(0) = 0,\ F'_{D}(1) > 0$, and $\tilde{F}'_{D}(1) > 0$. Therefore, there exist unique $x^*_{H},\ x^*_{D},\ \tilde{x}_{H},\ \tilde{x}_{D}$ in $(0,1)$ such that (45) holds. As a consequence of $F_{H}(x) > \widetilde{F}_{H}(x)$ and $F_{D}(x) < \widetilde{F}_{D}(x)$, we have $\tilde{x}_{H} > x^*_{H}$ and $\tilde{x}_{D} < x^*_{D}$. □

We now turn to prove Theorem 2.

Proof. Recall $z_{H}(x) = k_{H} + \phi'_{H}(x)c(1-x)$, and $z_{D}(x) = k_{D} - \phi'_{D}(x)(\gamma_{\max} - \gamma_{\min})x$. By (20), (18), and (19), we arrive:

$$\begin{cases} r\phi_{H}(x) = f_{H}(x) - z_{H}(x)^{-} + \phi'_{H}(x)\big(\beta x(1-x) - \gamma_{\max}x\big) \text{ if } z_{D}(x) < 0 \\ r\phi_{H}(x) = f_{H}(x) - z_{H}(x)^{-} + \phi'_{H}(x)\big(\beta x(1-x) - \gamma_{\min}x\big) \text{ if } z_{D}(x) > 0 \end{cases}, \tag{46}$$

and

$$\begin{cases} r\phi_{D}(x) = f_{D}(x) - z_{D}(x)^{-} + \phi'_{D}(x)\big(c(1-x) + \beta x(1-x) - \gamma_{\min}x\big) & \text{if } z_{H}(x) < 0 \\ r\phi_{D}(x) = f_{D}(x) - z_{D}(x)^{-} + \phi'_{D}(x)\big(\beta x(1-x) - \gamma_{\min}x\big) & \text{if } z_{H}(x) > 0 \end{cases}. \tag{47}$$

Differentiating (46) and (47) with x respectively, we arrive:

$$\begin{cases} z'_{H}(x)\big(c(1-x)\mathbb{1}_{z_{H}(x)<0} + \beta x(1-x) - \gamma_{\max}x\big) - z_{H}(x)\big(r - \beta(1-x) + \frac{\gamma_{\max}}{1-x}\big) \\ \qquad + f'_{H}(x)c(1-x) + k_{H}\big(r - \beta(1-x) + \frac{\gamma_{2}}{1-x}\big) = 0, \qquad \text{if } z_{D}(x) < 0 \\ z'_{H}(x)\big(c(1-x)\mathbb{1}_{z_{H}(x)<0} + \beta x(1-x) - \gamma_{\min}x\big) - z_{H}(x)\big(r - \beta(1-x) + \frac{\gamma_{\min}}{1-x}\big) \\ \qquad + f'_{H}(x)c(1-x) + k_{H}\big(r - \beta(1-x) + \frac{\gamma_{1}}{1-x}\big) = 0, \qquad \text{if } z_{D}(x) > 0 \end{cases}, \tag{48}$$

and

$$\begin{cases} -z'_{D}(x)\big(c(1-x) + \beta x(1-x) - (\gamma_{\min} + (\gamma_{\max} - \gamma_{\min})\mathbb{1}_{z_{D}(x)<0})x\big) + z_{D}(x)\big(r + \beta x + \frac{c}{x}\big) \\ \qquad + f'_{D}(x)(\gamma_{\max} - \gamma_{\min})x - k_{D}\big(r + \beta x + \frac{c}{x}\big) = 0, \qquad \text{if } z_{H}(x) < 0 \\ z'_{D}(x)\big(\beta x(1-x) - (\gamma_{\min} + (\gamma_{\max} - \gamma_{\min})\mathbb{1}_{z_{D}(x)<0})x\big) - z_{D}(x)\big(r + \beta\big) \\ \qquad + f'_{D}(x)(\gamma_{\max} - \gamma_{\min})x - k_{D}\big(r + \beta x\big) = 0, \qquad \text{if } z_{H}(x) > 0 \end{cases}. \tag{49}$$

Noting $z_{H}(1) = k_{H},\ z_{D}(0) = k_{D}$ and combining with (48), (49), we thus look for solutions such that $z_{D}(x) > 0,\ z_{H(x)<0}$ in $(0, \theta_{D})$, $z_{D}(x) < 0,\ z_{H(x)<0}$ in (θ_{D}, θ_{H}), and $z_{D}(x) < 0,\ z_{H(x)>0}$ in $(\theta_{H}, 1)$, where θ_{H} and θ_{D} are the switching threshold for the botnet herder and the defender group respectively and $\theta_{H} > \theta_{D}$. That is, θ_{H} is the switching threshold for the botnet herder such that $\hat{v}(\theta_{H}) = 1$, if $x < \theta_{H}$, and $\hat{v}(\theta_{H}) = 0$, if $x > \theta_{H}$ (i.e., $z_{H}(\theta) \gtrless 0$ if $x \gtrless \theta_{H}$). Similarly, θ_{D} is the switching threshold for the defender group such that $\hat{v}(\theta_{D}) = 0$, if $x < \theta_{D}$, and $\hat{v}(\theta_{D}) = 1$, if $x > \theta_{D}$ (i.e., $z_{D}(\theta) \gtrless 0$ if $x \lessgtr \theta_{D}$).
Situation A: $\theta_{H} = x^*_{H}$ and $\theta_{D} \leq x^*_{H}$

1. For $x < \theta_{_D}$, we have $z_{_H}(x) < 0$ and $z_{_D}(x) > 0$. By (48) and (42), we have:

$$z'_{_H}(x)\big(c(1-x)+\beta x(1-x)-\gamma_{\min}x\big)-z_{_H}(x)\big(r-\beta(1-x)+\frac{\gamma_{\min}}{1-x}\big)+\widetilde{F}_{_H}(x)=0;$$

thus

$$\frac{d}{dx}\big[z_{_H}(x)\exp\big(-\int_0^x\frac{r-\beta(1-\xi)+\frac{\gamma_{\min}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi}d\xi\big)\big]+$$
$$\frac{\widetilde{F}_{_H}(x)}{c(1-x)+\beta x(1-x)-\gamma_{\min}x}\exp\big(-\int_0^x\frac{r-\beta(1-\xi)+\frac{\gamma_{\min}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi}d\xi\big)=0.$$

Also,

$$-z'_{_D}(x)\big(c(1-x)+\beta x(1-x)-\gamma_{\min}x\big)+z_{_D}(x)\big(r+\beta x+\frac{c}{x}\big)+F_{_D}(x)=0;$$

thus

$$\frac{-d}{dx}\big[z_{_D}(x)\exp\big(\int_x^1\frac{r+\beta\xi+\frac{c}{\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi}d\xi\big)\big]+$$
$$\frac{F_{_D}(x)}{c(1-x)+\beta x(1-x)-\gamma_{\min}x}\exp\big(\int_x^1\frac{r+\beta\xi+\frac{c}{\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi}d\xi\big)=0.$$

2. For $\theta_{_D} < x < x^*_{_H}$, we have $z_{_H}(x) < 0$ and $z_{_D}(x) < 0$. We have:

$$z'_{_H}(x)\big(c(1-x)+\beta x(1-x)-\gamma_{\max}x\big)-z_{_H}(x)\big(r-\beta(1-x)+\frac{\gamma_{\max}}{1-x}\big)+F_{_H}(x)=0;$$

thus

$$\frac{d}{dx}\big[z_{_H}(x)\exp\big(-\int_0^x\frac{r-\beta(1-\xi)+\frac{\gamma_{\max}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\max}\xi}d\xi\big)\big]+$$
$$\frac{F_{_H}(x)}{c(1-x)+\beta x(1-x)-\gamma_{\max}x}\exp\big(-\int_0^x\frac{r-\beta(1-\xi)+\frac{\gamma_{\min}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\max}\xi}d\xi\big)=0.$$

Also,

$$-z'_{_D}(x)\big(c(1-x)+\beta x(1-x)-\gamma_{\max}x\big)+z_{_D}(x)\big(r+\beta x+\frac{c}{x}\big)+F_{_D}(x)=0;$$

thus

$$\frac{-d}{dx}\big[z_{_D}(x)\exp\big(\int_x^1\frac{r+\beta\xi+\frac{c}{\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\max}\xi}d\xi\big)\big]+$$
$$\frac{F_{_D}(x)}{c(1-x)+\beta x(1-x)-\gamma_{\max}x}\exp\big(\int_x^1\frac{r+\beta\xi+\frac{c}{\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\max}\xi}d\xi\big)=0.$$

3. For $x > x_H^*$, we have $z_H(x) > 0$ and $z_D(x) < 0$. We have:

$$z_H'(x)\big(+ \beta x(1-x) - \gamma_{\max} x\big) - z_H(x)\big(r - \beta(1-x) + \frac{\gamma_{\max}}{1-x}\big) + F_H(x) = 0;$$

thus

$$\frac{d}{dx}\big[z_H(x)\exp\big(-\int_{x_H^*}^{x} \frac{r-\beta(1-\xi)+\frac{\gamma_{\max}}{1-\xi}}{\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big)\big] + \frac{F_H(x)}{\beta x(1-x)-\gamma_{\max}x}\exp\big(-\int_{x_H^*}^{x} \frac{r-\beta(1-\xi)+\frac{\gamma_{\min}}{1-\xi}}{\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big) = 0.$$

Also,

$$-z_D'(x)\big(\beta x(1-x) - \gamma_{\max} x\big) + z_D(x)\big(r + \beta x\big) + \widetilde{F}_D(x) = 0;$$

thus

$$\frac{-d}{dx}\big[z_D(x)\exp\big(\int_{x}^{1} \frac{r+\beta\xi}{\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big)\big] + \frac{\widetilde{F}_D(x)}{\beta x(1-x)-\gamma_{\max}x}\exp\big(\int_{x}^{1} \frac{r+\beta\xi}{\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big) = 0.$$

We take $z_H(x_H^*)$ and, by using the above results, define z_H as follows:

1. For $x > x_H^*$, we set:

$$z_H(x) = -\int_{x_H^*}^{x} \frac{F_H(\zeta)}{\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(\int_{\zeta}^{x} \frac{r-\beta(1-\xi)+\frac{\gamma_{\max}}{1-\xi}}{\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big)\big] d\zeta, \tag{50}$$

and, by assumption $\beta < \gamma_{\max}$, we deduce the condition $z_H(x_H^*) > 0$ is clearly satisfied.

2. For $\theta_D < x < x_H^*$, we set:

$$z_H(x) = -\int_{x}^{x_H^*} \frac{F_H(\zeta)}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(-\int_{x}^{\zeta} \frac{r-\beta(1-\xi)+\frac{\gamma_{\max}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big)\big] d\zeta, \tag{51}$$

and, by assumption $c(1-x_H^*) + \beta(1-x_H^*) - \gamma_{\max}x_H^* > 0$, we deduce the condition $z_H(x) < 0$ is clearly satisfied.

3. For $x < \theta_D$, we have:

$$z_H(x) = z_H(\theta_D)\exp\big(-\int_{x}^{\theta_D} \frac{r-\beta(1-\zeta)+\frac{\gamma_{\min}}{1-\zeta}}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\min}\zeta} d\zeta\big] + \int_{x}^{\theta_D} \frac{\widetilde{F}_H(\zeta)}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\min}\zeta}\big[\exp\big(-\int_{x}^{\zeta} \frac{r-\beta(1-\xi)+\frac{\gamma_{\min}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi} d\xi\big)\big] d\zeta, \tag{52}$$

and $\zeta < \theta_D < x_H^*$ implies $c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\min}\zeta > c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi > 0$; therefore, the condition $z_H(x_H^*) < 0$ is clearly satisfied.

To this point, θ_D remains arbitrary with $\theta_D < x_H^*$. We now turn to $z_D(x)$.

1. We have $z_D(\theta_D) = 0$.
2. For $0 < x < \theta_D$, we have:

$$z_D(x) = -\int_x^{\theta_D} \frac{F_D(\zeta)}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\min}\zeta}\big[\exp\big(-\int_x^{\zeta}\frac{r+\beta\xi+\frac{c}{\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi}d\xi\big)\big]d\zeta,$$

   Since $c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\min}\zeta > 0$ for $\zeta < \theta_D < x_H^*$ and $F_D(\zeta) < 0$ because $x_H^* < x_D^*$, $z_D(x) > 0$ is satisfied.
3. For $\theta_D < x < x_H^*$, we have:

$$z_D(x) = \int_{\theta_D}^{x} \frac{F_D(\zeta)}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(\int_{\zeta}^{x}\frac{r+\beta\xi+\frac{c}{\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\max}\xi}d\xi\big)\big]d\zeta,$$

   and $c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\min}\zeta > 0$ as well as $F_D(\zeta) < 0$; therefore, $z_D(x) < 0$ is satisfied.
4. For $x > x_H^*$, we have:

$$z_D(x) = z_D(x_H^*)\exp\big(\int_{x_H^*}^{x}\frac{r+\beta\zeta}{\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}d\zeta\big)+ \tag{53}$$

$$\int_{x_H^*} x\frac{\widetilde{F}_D(\zeta)}{\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(\int_{\zeta}^{x}\frac{r+\beta\xi}{\beta\xi(1-\xi)-\gamma_{\max}\xi}d\xi\big)\big]d\zeta. \tag{54}$$

   We know that $\tilde{x}_D < x_D^*$ and $x_H^* < x_D^*$. However, we may have $\tilde{x}_D > x_H^*$ or $\tilde{x}_D < x_H^*$.
   (a) If $\tilde{x}_D < x_H^*$, then $\beta\zeta(1-\zeta)-\gamma_{\max}\zeta < 0$ for $\zeta < 1$ thanks to the assumption $\beta < \gamma_{\max}$ and $\widetilde{F}_D(\zeta) > 0$ because of $\zeta > x_H^* > \tilde{x}_D$. Hence, we arrive at the condition needing to be satisfied, $z_D(x) < 0$. Therefore, all conditions are satisfied without any condition on θ_D except $\theta_D < x_H^*$. We can take $\theta_D = x_H^*$
   (b) If $\tilde{x}_D > x_H^*$, we cannot assert a priori $z_D(x)$ given by (54) is less than zero. We proceed as follows:
   Consider the expression for $x < x_H^*$:

$$\Gamma(x) = \int_x^{x_H^*}\frac{F_D(\zeta)}{(\beta\zeta+c)(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(\int_{\zeta}^{x_H^*}\frac{r+\beta\xi+\frac{c}{\xi}}{(\beta\xi+c)(1-\xi)-\gamma_{\max}\xi}d\xi\big)\big]d\zeta$$
$$+\int_{x_H^*}^{\tilde{x}_D}\frac{\widetilde{F}_D(\zeta)}{\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(\int_{\zeta}^{\tilde{x}_H}\frac{r+\beta\xi}{\beta\xi(1-\xi)-\gamma_{\max}\xi}d\xi\big)\big]d\zeta.$$

   In the above equation, the second integral is a fixed positive number and the first integral, denoted as I(x), is negative. We have I(x) $\leq \infty$ as $x \to 0$, $\Gamma'(x) > 0$, and $\Gamma(x_H^*) > 0$. Therefore, there exists a unique $\theta_D < x_H^*$ such that $\Gamma(\theta_D) = 0$. From (54), we have, for $< x_H^* < x < \tilde{x}_D$,

$z_D(x) \leq z_D(\tilde{x}_D) = \Gamma(\theta_D) = 0$; hence $z_D(x) < 0$. For $x < \tilde{x}_D$, we have:

$$z_D(x) = z_D(\tilde{x}_D) \exp\big(\int_{\tilde{x}_H}^{x} \frac{r+\beta\zeta}{\beta\zeta(1-\zeta)-\gamma_{\max}\zeta} d\zeta\big) + \int_{\tilde{x}_D}^{x} \frac{\widetilde{F}_D(\zeta)}{\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(\int_{\zeta}^{x} \frac{r+\beta\xi}{\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big)\big] d\zeta,$$

which is less than zero.

Therefore, we have found a pair $\theta_D \leq x_H^*$ and $z_D(\theta_D) = 0,\ z_H(x_H^*) = 0$. The optimal policies for the botnet herder and the defender group are:

Botnet Herder:

$$\hat{v}_H(x) = \begin{cases} 1 & \text{if } x < x_H^* \\ u_H & \text{if } x = x_H^* \\ 0 & \text{if } x > x_H^* \end{cases}. \tag{55}$$

Defender Group:

$$\hat{v}_D(x) = \begin{cases} 1 \text{ if } x > \theta_D \\ 0 \text{ if } x < \theta_D \end{cases}. \tag{56}$$

and $\hat{v}_D(x_H^*) = 1$.

At x_H^*, an equilibrium, $\hat{v}_H(x_H^*) = u_H = -\frac{1}{c(1-x_H^*)}\big(\beta x_H^*(1-x_H^*) - \gamma_{\max} x_H^*\big)$ which is between 0 and 1 by assumption $c(1-x_H^*)+\beta(1-x_H^*)-\gamma_{\max}x_H^* > 0$, and $\hat{v}_D(x_H^*) = 1$.

At θ_D, we have $\hat{v}_H(\theta_D) = 1$. However, θ_D cannot be an equilibrium point since it would require a control $\hat{v}_H(\theta_D) = u_D = \frac{1}{\gamma\theta_D}\big(\beta\theta_D(1-\theta_D) - \gamma_{\min}\theta_D + c(1-\theta_D)\big) > 1$, which is not admissible. The control $\hat{v}_H(\theta_D)$ is indifferent since the state cannot remain at θ_D.

Situation B: $\theta_D = x_D^* < \theta_H$

We take $z_D(x_D^*)$ and define $z_D(x)$ as follows:

1. For $0 < x < x_D^*$, we set:

$$z_D(x) = -\int_{x}^{x_D^*} \frac{F_D(\zeta)}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\min}\zeta}\big[\exp\big(-\int_{x}^{\zeta} \frac{r+\beta\xi+\frac{c}{\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\in}\xi} d\xi\big)\big] d\zeta,$$

and for $\zeta < x_D^*$, $c(1-\zeta)+\beta(1-\zeta)-\gamma_{\min}\zeta > 0$, and $F_D(\zeta) < 0$; hence, $z_D(x) > 0$ is satisfied.

2. For $x_D^* < x < \theta_H$, we have:

$$z_D(x) = \int_{x_D^*}^{x} \frac{F_D(\zeta)}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(\int_{\zeta}^{x} \frac{r+\beta\xi+\frac{c}{\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big)\big] d\zeta,$$

and from $c(1-x_D^*)+\beta(1-x_D^*)-\gamma_{\max}x_D^* < 0$, we can state that for $\zeta > x_D^*$, $\theta_D \leq x_H^*$, $c(1-\zeta)+\beta(1-\zeta)-\gamma_{\max}\zeta < 0$ and $F_D(\zeta) < 0$; hence, $z_D(x) < 0$ is satisfied.

3. For $x > \theta_H$, we have:

$$z_D(x) = z_D(\theta_H) \exp\big(\int_{\theta_H}^{x} \frac{r+\beta\zeta}{\beta\zeta(1-\zeta)-\gamma_{\max}\zeta} d\zeta\big) + \int_{\theta_H}^{x} \frac{\widetilde{F}_D(\zeta)}{\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(\int_{\zeta}^{x} \frac{r+\beta\xi}{\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big)\big] d\zeta.$$

For $\zeta > \theta_H > x_D^*$, $\widetilde{F}_D(\zeta) > F_D(\zeta) > 0$; hence $z_D(x) < 0$ is satisfied.

So far no constraints are imposed for θ_H except for $\theta_H > x_D^*$. We turn now to $z_H(x)$.

1. For $\theta_H < x < 1$, we set:

$$z_H(x) = -\int_{\theta_H}^{x} \frac{F_H(\zeta)}{\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(\int_{\zeta}^{x} \frac{r-\beta(1-\xi)+\frac{\gamma_{\max}}{1-\xi}}{\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big)\big] d\zeta,$$

and since $\beta\xi(1-\zeta)-\gamma_{\max}\zeta < 0$, and $F_H(\zeta) > 0$, we deduce the condition $z_H(x) > 0$ is satisfied.

2. For $x_D^* < x < \theta_H$, we set:

$$z_H(x) = -\int_{x}^{\theta_H} \frac{F_H(\zeta)}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(-\int_{x}^{\zeta} \frac{r-\beta(1-\xi)+\frac{\gamma_{\max}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big)\big] d\zeta. \tag{57}$$

For $x_D^* < x < \theta_H$, we have $c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\max}\zeta$ thanks to the assumption $c(1-x_D^*)+\beta x_D^*(1-x_D^*)-\gamma_{\max}x_D^* < 0$ and $F_H(\zeta) > 0$ since $x_H^* < x_D^* < x < \zeta$; hence, $z_H(x) < 0$ is satisfied.

3. For $0 < x < x_D^*$, we have:

$$z_H(x) = z_H(x_D^*)\exp\big(-\int_{x}^{x_D^*} \frac{r-\beta(1-\zeta)+\frac{\gamma_{\min}}{1-\zeta}}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\min}\zeta} d\zeta\big) + \int_{x}^{x_D^*} \frac{\widetilde{F}_H(\zeta)}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\min}\zeta}\big[\exp\big(-\int_{x}^{\zeta} \frac{r-\beta(1-\xi)+\frac{\gamma_{\min}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi} d\xi\big)\big] d\zeta. \tag{58}$$

We know that $\tilde{x}_H < x_H^*$. However, we may have $\tilde{x}_H > x_D^*$ or $\tilde{x}_H < x_D^*$.

(a) If $\tilde{x}_H < x_D^*$, then $\zeta < x_D^*$ implies $\widetilde{F}_H(\zeta) < 0$ and from the assumption $c(1-x_D^*)+\beta x_D^*(1-x_D^*)-\gamma_{\max}x_D^* < 0$ $\beta\zeta(1-\zeta)-\gamma_{\max}\zeta > 0$, $c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi > 0$; hence, we arrive at the condition needing to be satisfied, $z_H(x) < 0$. Therefore, all conditions are satisfied without any condition on θ_H except $\theta_H > x_D^*$. We can take $\theta_H = x_D^*$

(b) If $\tilde{x}_H > x_D^*$, the second term in (58) is positive for $\tilde{x}_H < x < x_D^*$. Therefore, we define θ_H so that

$$\int_{x_D^*}^{\theta_H} \frac{F_H(\zeta)}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(-\int_{x_D^*}^{\zeta} \frac{r-\beta(1-\xi)+\frac{\gamma_{\max}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\max}\xi} d\xi\big)\big] d\zeta + \int_{\tilde{x}_H}^{x_D^*} \frac{\widetilde{F}_H(\zeta)}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\min}\zeta}\big[\exp\big(-\int_{\tilde{x}_H}^{\zeta} \frac{r-\beta(1-\xi)+\frac{\gamma_{\min}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi} d\xi\big)\big] d\zeta = 0. \tag{59}$$

In (59), the second integral is a fixed positive number and the first integral is positive. Consider:

$$\Lambda(x) = \int_{x_D^*}^{x} \frac{F_H(\zeta)}{c(1-\zeta)+\beta\zeta(1-\zeta)-\gamma_{\max}\zeta}\big[\exp\big(-\int_{x_D^*}^{\zeta}\frac{r-\beta(1-\xi)+\frac{\gamma_{\max}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\max}\xi}d\xi\big)\big]d\zeta$$
$$+\int_{\tilde{x}_H}^{x_D^*}\frac{\widetilde{F}_H(\zeta)}{c(1-zeta+\beta\zeta(1-\zeta)-\gamma_{\min}\zeta}\big[\exp\big(-\int_{\tilde{x}_H}^{\zeta}\frac{r-\beta(1-\xi)+\frac{\gamma_{\min}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi}d\xi\big)\big]d\zeta.$$

Then we have $\Lambda'(x) > 0$, $\Lambda(x_D^*) > 0$, and $\Lambda(x) \leq \infty$ as $x \to 1$. Therefore, there exists a unique $\theta_H < x_H^*$ such that (59) holds. From (58), we have, for $\tilde{x}_H < x < x_D^*$, $z_H(x) \leq \Lambda(\theta_H) = 0$ and $z_H(\tilde{x}_H) = 0$; hence $z_H(x) < 0$. For $x < \tilde{x}_H$, we have:

$$z_H(x) = \int_{x}^{\tilde{x}_H}\frac{\widetilde{F}_H(\zeta)}{c(1-\zeta)+\beta(1-\zeta)-\gamma_{\min}\zeta}\big[\exp\big(-\int_{x}^{\zeta}\frac{r-\beta(1-\xi)+\frac{\gamma_{\min}}{1-\xi}}{c(1-\xi)+\beta\xi(1-\xi)-\gamma_{\min}\xi}d\xi\big)\big]d\zeta,$$

which is less than zero.

Therefore, we have found a pair $x_D^* < \theta_H$ and $z_H(\theta_H) = 0,\ z_D(x_D^*) = 0$. The optimal policies for the botnet herder and the defender group are:

Botnet Herder:

$$\hat{v}_H(x) = \begin{cases} 1 \text{ if } x < \theta_H \\ 0 \text{ if } x > \theta_H \end{cases}, \tag{60}$$

and $\hat{v}_H(x_D^*) = 1$.

Defender Group:

$$\hat{v}_D(x) = \begin{cases} 1 & \text{if } x > x_D^* \\ u_D \text{ if } x = x_D^* \\ 0 & \text{if } x < x_D^* \end{cases}. \tag{61}$$

At x_D^*, an equilibrium, $\hat{v}_D(x_D^*) = u_D = \frac{c(1-x_D^*)+\beta x_D^*(1-x_D^*)-\gamma_{\max}x_D^*}{\gamma x_D^*}$, which lies between 0 and 1, and $\hat{v}_D(x_D^*) = 1$. At θ_H, we have $\hat{v}_D(\theta_H) = 1$. The control $\hat{v}_H(\theta_H)$ is indifferent to the botnet herder since the state cannot remain at θ_H.

In addition, if $\theta_H = x_H^*$, we must take $\hat{v}_D(x_D^*) = u_D$ and $\hat{v}_H(x_D^*) = 1$.

Also if

(a) $c(1-x_H^*)+\beta x_H^*(1-x_H^*)-\gamma_{\max}x_H^* > 0$,

(b) $c(1-x_D^*)+\beta x_D^*(1-x_D^*)-\gamma_{\max}x_D^* < 0$,

(c) $c(1-x_D^*)+\beta x_D^*(1-x_2^*)-\gamma_{\min}x_D^* > 0$,

and $\tilde{x}_H > x_D^*$, $\tilde{x}_D < x_H^*$, we can either take $\theta_H = \theta_D = x_H^*$ or $\theta_H = \theta_D = x_D^*$. □

References

1. A. Bensoussan, M. Kantarcioglu, and C. Hoe, *Botnet Defense Under Uncertainty: A Stochastic Differential Game Approach*, Working Paper, University of Texas at Dallas, 2010.

2. B. Rowe, D. Reeves, and M. Gallaher, *The Role of Internet Service Providers in Cyber Security*, Institute for Homeland Security Solutions, June 2009. Available onlin: https://www.ihssnc.org/portals/0/PubDocuments/ISP-Provided_Security_Rowe.pdf
3. F. Burckhardt, *Modeling Infectious Decsases in Virtual Realities*, The 24th Chaos Communication Congress, December, 2007.
4. F. Cohen, *Computer Viruses Theory and Practice*, Computer and Security, vol. 6, pp22-35, February 1987.
5. G. Theodorakopoulos, J. S. Baras and J-Y. Le Boudec, *Dynamic Network Security Deployment under Partial Information*, Proceedings of the 46th Annual Allerton Conference On Communication, Control, and Computing, 2008, pp 261-267.
6. H. Frith, *Home Internet Users Biggest Threat to Business*, The Times Online, July 2005. Available online: http://technology.timesonline.co.uk/tol/news/tech_and_web/article540371.ece.
7. J. Grossklags, N. Christin, and J. Chuang, *Security investment (failures) in five economic environments: A comparison of homogeneous and heterogeneous user agents*, Proceedings of the 7th Workshop on the Economics of Information Security (WEIS 2008).
8. J. Liu, Y. Tang and Z. R. Yang, *The Spread of Disease with Birth and Death on Networks*, Journal of Statistical Mechanics: Theory and Experiment, 2004.
9. J.O. Kephart and S.R. White, *Directed-Graph Epidemiological Models of Computer Viruses*, Proceedings of IEEE Symposium on Security and Provacy, pp 343-361, 1991.
10. K- W. Lye and J. Wang, *Game Strategies in Network Securities*, International Journal of Information SecurityJuly, vol. 1, no. 1-2, pp 71-86, 2005.
11. L. J. S. Allen, *An Introduction to Stochastic Epidemic Models – Part I*, 2008 Summer School on Mathematical Modeling of Infectious Diseases, University of Alberta.
12. M. Bloem, T. Aplcan, and T. Basar, *Optimal and Robust Epidemic Response for Multiple Networks*, IFAC Control Engineering Practice, vol. 17, no. 5, pp 525-533, 2009.
13. M. Lelarge, *Economics of Malware: Epidemic Risks Model, Network Externalities and Incentives*, The 8th Workshop on the Economics of Information Security (WEIS 2009).
14. M. Lelarge and J. Bolot, *A Local Mean Field Analysis of Security Investments in Networks*, Proceedings of the Third International Workshop on Economics of Networked Systems, pp 25-30, 2008.
15. N. Fultz and J. Grossklags, *Blue versus Red: Towards a model of distributed security attacks*,Proceedings of the Thirteenth International Conference Financial Cryptography and Data Security (FC'09); Lecture Notes in Computer Science (LNCS), No. 5628, Springer Verlag, pp. 167-183, 2009.
16. O. Toutonji and S-M Yoo, *An Approach against a Computer Worm Attack*, International Journal of Communication Networks and Information Security, 1(2), pp 47-53, August 2009.
17. P. Baucher, T. Holz, M. Kotter and G. Wicherski, *Konw your Enemy: Tracking Botnets*, Available online: *http : //www.honeynet.org/papers/bots*.
18. T Alpcan and T Basar, *A Game Theoretic Appropach to Decision and Analysis in Network Intrusion Detection*, Proceeding of the 42nd IEEE Conference on Decision and Control, pp 2595-2600.

19. T Alpcan and T Basar, *A Game Theoretic Analysis of Intrusion Detection in Access control Systems*, Proceeding of the 43rd IEEE Conference on Decision and Control, pp 1568-1573.
20. T Alpcan and T Basar, *An Inrtusion Detection Game with Limited Observations*, The 12th Int. Symp. on Dynamic Games and Applications, 2006.
21. Y. Huang, X. Geng ,and A. Whinston, *Defeating DDoS Attacks by Fixing the Incentive Chain*, ACM Transactions on Internet Technology, 17(1), article 5, pp 1-5, 2007.
22. Y. Namestnikov, *The Economics of Botnets*, Available online: http://www.viruslist.com/en/downloads/pdf/ynam_botnets_0907_en.pdf.
23. Z. Li, Q. Liao and A. Striegel, *Botnet Economics: Uncertainty Matters*, The 7th Workshop on the Economics of Information Security (WEIS 2008).
24. *Conficker Botnet 'Dead In the Water', Researcher Says* , Available online: http://darkreading.com/vulnerability_management/security/attacks /showArticle.jhtml?articleID= 224201115
25. *Symantec Global Internet Security Threat Report*, Available online: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_x_04-2010.en-us.pdf
26. *Kaspersky Security Bulletin: Malware evolution 2008*, Availablr online: http://www.securelist.com/en/analysis?pubid=204792051