Should ISPs be liable for negative externalities of botnets?

Shinya Kinukawa*

June 24, 2012

Abstract

A botnet, a network of computers under the control of an on-line attacker, is an important threat to cybersecurity since it is a popular method to carry out a wide range of criminal services on the internet. Several researchers argue that Internet Service Providers (ISPs) should be liable for damages caused by their customers' computers consisting of botnets in order to make ISPs secure their networks. This paper evaluates ISP liability for violations of cybersecurity based on an economic model of a monopolistic ISP providing network access. The results of model analysis show that imposing liability on the ISP can decrease social welfare if the cost of cleaning up botnet malware from users' computers is not sufficiently low. In that case, the equilibrium access fee becomes so high that both the ISP's profits and consumer surplus decrease compared to the case that the ISP does nothing against botnets. On the other hand, if the cleanup cost is sufficiently low, the ISP can have an incentive to voluntarily clean up botnet malware from users' computers without liability.

Keywords: ISP, liability, botnets

*Komazawa University

1 Introduction

The internet has been growing as an infrastructure in the global economy. The rapid growth of cloud-computing services makes the internet further important for every type of users from individual consumers to large corporations. However, the internet is not as safe as other important infrastructures such as water supply. Cybersecurity is continuously threatened by malicious attacks such as distributed denial of service (DDoS) attacks and theft of proprietary data.[1]

A current major threats to cybersecurity is the proliferation of botnets, a popular method of attack impacting nearly all aspects of cybersecurity including sending spam, committing online-advertising fraud, launching DDoS attacks, hosting phishing attacks, and anonymizing attack traffic (Moore, 2010). A botnet is a network of computers infected by a type of malware to make those computers under the control of an attacker. Although individual computers constructing a botnet are controlled by criminals as an attack method, botnet malware tends not to obviously advertise their presence to the users of those computers (StopBadware Inc, 2011). Therefore, the individual users of botnet-infected computers often do not realize the infection.

Internet service providers (ISPs) are currently exempted from liability for violations of cybersecurity, and many of them take no action against their customers' infection to malware because of their weak incentive to intervene (Moore, 2010). However, ISPs have been generally considered as a key player to remove botnets from the internet, and several scholars and security experts have discussed whether or not ISPs should be responsible to cybersecurity.[2]

Lichtman and Posner (2006) argue that ISPs should be liable for damages caused by their customers' malware-infected computers. The reasons are that ISPs control the gateways through which malicious codes enter the network and that imposing liability on ISPs is consistent with conventional tort law principles. Moore (2010) recommends a less aggressive approach that gives ISPs

[1] See, for example, Touré (2011) for recent cases of cyber attacks against information infrastructure and private sectors.

[2] For a survey of literature on cybersecurity and ISP, see Rowe et.al. (2009). Security experts' opinions are fund in an article on CIO.com, "Seeing No Evil: Is It Time To regulate the ISP industry" (by Matt Villano, 2005/11/1). van Eeten et al. (2010) provides an empirical evidence that most malware are sent by machines connected to ISPs.

safe harbor if they clean up customers' infected machines upon notification. In either approach, assigning ISPs the responsibility for cybersecurity imposes a costly obligation on ISPs and thus can cause ISPs to overreact. Because ISPs have only a weak incentive to provide access to customers whose computers are vulnerable to malware, imposing liability on ISPs for the acts of their customers can lead ISPs to purge those risky customers from the network (Lichtman and Posner, 2006). Such a concern about ISPs' overreaction may justify government subsidy for a part of the cost to clean up infected computers, which is suggested by Clayton (2010) and Moore (2010).

This paper evaluates ISP liability for violations of cybersecurity using an economic model examining its effects on social welfare. In the model, a monopolistic ISP provides local network access, and a continuum of users are heterogeneous on their incentives to pay the access fee and to take precautions against malware. There are both positive and negative externalities in the network. All on-line users create positive externalities, but a part of on-line users who do not take precautions create negative externalities because their computers are vulnerable to botnet malware infection. Moreover, the ISP can secure its network by incurring cost to clean up botnet malware from their customers' computers or by simply purging users whose computers are vulnerable to botnet malware. Using this model, we examine the ISP's incentives to secure the network and evaluate the effects of the ISP's actions on social welfare.

The model analysis reveals that the low clean-up cost is crucial to achieve safe network maximizing social welfare. If the clean-up cost is sufficiently low, securing the network by cleaning up botnet malware can increases the profits of the monopolistic ISP. In that case, negative externalites are removed from the network without a large increase in the access fee and thus total number of on-line users, which create positive externalities, increase as a result. If the clean-up cost is not sufficiently low, liability can force the ISP to clean up botnet malware, but the higher access fee decreases total number of on-line users. Moreover, for high clean-up cost, the ISP may rather choose to purge a part of users who do not take precautions against malware in order to secure the network. In the latter cases, the social welfare decreases because positive externalities decrease due to the loss of a part of on-line users. The results

would rationalize government subsidiary or support to ISPs for cleaning up botnet malware from users' computers to secure the network.

The rest of the paper is organized as follows. Section 2 presents the model. Section 3 examines the ISP's incentive and social welfare where it has only two options: it cleans up botnet malware from users' computers or does nothing against botnet. Section 4 examines the third option for ISP, that is, disconnecting the access of users who does not take precautions, and compare the effects on social welfare between the three actions of the ISP. Section 5 concludes the paper.

2 Model

We consider a local Internet access market where a monopolistic Internet service provider (ISP) provides network access.[3] ISP first decides whether or not to secure the network by cleaning up botnets incurring cost $c > 0$ per an on-line user, and then determines the access fee p_i that maximizes its profit. The index $i = 0, 1$ denotes the network's security status changed by ISP: $i = 0$ denotes that ISP takes no action to secure the network and $i = 1$ denotes that ISP secures the network by cleaning up botnets.

In the above setting, we assume that the cost of cleaning up botnets from the network increases as the total number of on-line users increases, whether or not a user's computer is infected. The first step of cleaning up botnets malware from infected computers is the identification of such computers, which requires inventing an effective method.[4]. Therefore, the cleanup cost can depend on the number of all computers connected to the ISP's network.

Types of users are continuum indexed by x on the interval $[0, 1]$ with a unit density.[5] Let n_i be the number of users who pay the network access fee and thus be on-line. If ISP takes no action to secure the network, it maximizes $\pi_0 = n_0 p_0$. If ISP decides to clean up botnet malware, it maximizes $\pi_1 = n_1 p_1 - n_1 c$.

[3]The monopolistic ISP assumption is reasonable when only limited choices of Internet access are available to consumers or there are significant switching costs in changing ISP. See Economides (2008) and Choi and Kim (2010).

[4]See, for example, Cyber Clean Center (2010)

[5]Potential users of the network include content providers such as cloud-computing service providers as well as end-users.

Users decide whether or not to pay the access fee p_i to be on-line. At the same time, they also decide whether or not to take precautions against malware infection such as installing security software, which can imposes different costs for different user types. Let n_{si} be the number of on-line users who take precautions ("secure users") and n_{vi} be the number of on-line users who do not take precautions ("vulnerable users"). The total number of on-line users is given as $n_i = n_{si} + n_{vi}$. The utility of a secure user located at $x \in [0,1]$ under ISP's decision i is

$$u_{si}(x) = n_i - (1-\delta_i)n_{vi} + \alpha - \beta_s(1-x) - p_i, \tag{1}$$

and the utility of a vulnerable user located at $x \in [0,1]$ under ISP's decision i is

$$u_{vi}(x) = n_i - (1-\delta_i)n_{vi} - \beta_v x - p_i. \tag{2}$$

The utility of off-line users is zero.

In the above equations of the utility, n_i denotes the network externalities determined by the total number of on-line users, while $(1-\delta_i)n_{vi}$ denotes the negative externalities determined by the number of vulnerable on-line users, where $\delta_i \in [0,1]$. The negative externalities describe a situation where vulnerable users' computers construct botnets and are controlled by attackers. An increase in vulnerable users would spread botnets and thus increase the risk of attacks against all on-line users. ISP can decrease the negative externalities by making a costly effort to clean up botnet malware from users' computers ($i = 1$), and for simplicity we set $\delta_1 = 1$, that is, ISP can completely remove the negative externalities. On the other hand, when ISP take no action against botnets ($i = 0$), there exist negative externalities of botnets in the network, and we set $\delta_0 = 0$.

The parameters $\alpha, \beta_s, \beta_v > 0$ determine benefits and losses of users' decision whether or not to take precautions against cybersecurity. The parameter α is the benefits that are the same for all user types, and β_s is the difference in users' cost for taking precautions. Since botnets are not the only sources of damages to users, ISP's cleaning-up botnets and users' precautions are not substitute but rather complement each other.[6] For secure users, $\alpha - \beta_s(1-x)$ denotes the

[6]For example, USB flash memory storage devices are major vehicles for computer virus.

net benefits of taking precautions. User-types x located at close to 1 are those who receive large benefits from precautions, while user-types x close to 0 receive only small or negative benefits because of relatively large costs. For vulnerable users, $-\beta_v x$ denotes the expected losses due to vulnerability to cybersecurity, that is, the cost of not taking precautions. User-types close x to 1 suffer large damages when they do not take precautions, while user-types x close to 0 suffer little damage even without precautions. In the following, we set $\beta_s = \beta_v = \beta$.

3 Equilibrium prices and demands of the network access

Let $x = x_{vi}, x_{si}$ be such that $u_{vi}(x_{vi}) = 0$ and $u_{si}(x_{si}) = 0$, where $x_{vi} < x_{si}$. Then, $n_{vi} = x_{vi}$ and $n_{si} = 1 - x_{si}$. When ISP takes no action against botnets ($i = 0$), from the utility (1) and (2),

$$n_{s0} + \alpha - \beta n_{s0} - p_0 = 0 \quad \text{and} \quad n_{s0} - \beta n_{v0} - p_0 = 0.$$

Similarly, when ISP cleans up botnets from the network ($i = 1$),

$$n_1 + \alpha - \beta n_{s1} - p_1 = 0 \quad \text{and} \quad n_1 - \beta n_{v1} - p_1 = 0.$$

Secure and vulnerable users' demands of the network accesses in each $i = 0, 1$ are given as,

$$n_{s0} = \frac{\alpha - p_0}{\beta - 1}, \quad n_{v0} = \frac{\alpha - \beta p_0}{\beta(\beta - 1)}, \quad n_{s1} = \frac{\alpha(\beta - 1) - \beta p_1}{\beta(\beta - 2)}, \quad n_{v1} = \frac{\alpha - \beta p_1}{\beta(\beta - 2)}.$$

So that these demand functions are decreasing in the access fee p_i, the parameter β is restricted to $\beta > 2$, which implies that costs for users' precautions are sufficiently different.

ISP determines the access fee p_i maximizing π_i, where $\pi_0 = (n_{s0} + n_{v0})p_0$ and $\pi_1 = (n_{s1} + n_{v1})(p_1 - c)$. Both the profit functions π_0 and π_1 are concave in p_i since $\beta > 2$ is assumed. The first order condition is given as $\alpha(\beta+1) - 4\beta p_0 = 0$ for $i = 0$, and $\alpha - 4p_1 + 2c = 0$ for $i = 1$. The equilibrium access fee and the number of on-line users are

$$p_0 = \frac{\alpha(\beta + 1)}{4\beta}, \quad n_{s0} = \frac{\alpha(3\beta - 1)}{4\beta(\beta - 1)}, \quad n_{v0} = \frac{\alpha(3 - \beta)}{4\beta(\beta - 1)},$$

for $i = 0$, and

$$p_1 = \frac{\alpha + 2c}{4},\ n_{s1} = \frac{1}{\beta - 2}\left\{\frac{\alpha(3\beta - 4)}{4\beta} - \frac{c}{2}\right\},\ n_{v1} = \frac{1}{\beta - 2}\left\{\frac{\alpha(4 - \beta)}{4\beta} - \frac{c}{2}\right\}$$

for $i = 1$, respectively.

In the following, the parameters α, β, and c are restricted so that $n_{si}, n_{vi} > 0$ and $n_i \leq 1$. First, $n_{s0} > 0$ is satisfied since $\beta > 2$, but $n_{v0} > 0$ requires $\beta < 3$. If the difference in users' costs for precautions is too large, all on-line users will take precautions because of large cost of not taking them. Then, β is set to

$$2 < \beta < 3.$$

Second, $n_{s1}, n_{v1} > 0$ require $\alpha(3\beta - 4) - 2\beta c > 0$ and $\alpha(4 - \beta) - 2\beta c > 0$, which give the upper bound of c as

$$c < \min\left\{\frac{\alpha(3\beta - 4)}{2\beta}, \frac{\alpha(4 - \beta)}{2\beta}\right\} = \frac{\alpha(4 - \beta)}{2\beta} \equiv \overline{c},$$

since $3\beta - 4 > 4 - \beta$ for $\beta > 2$. Third, from $n_i = n_{si} + n_{vi} \leq 1$,

$$n_0 = \frac{\alpha(\beta + 1)}{2\beta(\beta - 1)} \leq 1 \quad \text{and} \quad n_1 = \frac{\alpha - 2c}{2(\beta - 2)} \leq 1,$$

which give the upper bound of α and the lower bound of c as

$$\alpha \leq \frac{2\beta(\beta - 1)}{\beta + 1} \equiv \overline{\alpha}, \quad c \geq \frac{\alpha}{2} - \beta + 2 \equiv \underline{c}.$$

Finally, since $\underline{c} > 0$, the lower bound of α is given as

$$\alpha > 2(\beta - 2) \equiv \underline{\alpha}.^{7}$$

4 ISP's incentive to clean up botnet malware

When ISP cleans up botnet malware from the network, users' demand for network access and thus ISP's profits can increase because of the elimination of negative externalities. At the same time, if the clean-up cost per user largely raises the access fee, the demand and ISP's profits can also decrease. In this section, we examine how the clean-up cost c affects ISP's profits and social welfare.

[7] $\underline{\alpha} < \overline{\alpha}$ is easily confirmed by directly calculating $\overline{\alpha} - \underline{\alpha}$. For $\underline{c} < \overline{c}$, $\overline{c} - \underline{c} = (\beta - 2)(\beta - \alpha)/\beta$. When α takes the largest value $\overline{\alpha}$, $\beta - \overline{\alpha} = \beta(3 - \beta)/(\beta + 1) > 0$ since $\beta < 3$, which implies that $\underline{c} < \overline{c}$ for $\alpha \leq \overline{\alpha}$.

We first show that there exits c such that the total numbers of on-line users under the secured ($i = 1$) and non-secured ($i = 0$) network are equal. The difference in the number of on-line users between the secured and non-secured network is given as

$$\begin{aligned} n_1 - n_0 &= \frac{\alpha - 2c}{2(\beta - 2)} - \frac{\alpha(\beta + 1)}{2\beta(\beta - 1)} \\ &= \frac{\alpha - \beta(\beta - 1)c}{\beta(\beta - 1)(\beta - 2)}. \end{aligned}$$

Therefore, $n_1 = n_0$ when

$$c = \frac{\alpha}{\beta(\beta - 1)} \equiv c^*.$$

Lemma 1 $\underline{c} \leq c^* < \overline{c}$

Proof. See Appendix.

Thus, if $c \in [\underline{c}, c^*)$, the total number of on-line users increases if ISP changes its decision from taking no action to cleaning up botnets.

ISP's incentive to clean up botnet malware can be examined by defining $D_1(c) \equiv \pi_1 - \pi_0$, the difference in the profits under the secured and non-secured network:

$$\begin{aligned} D_1(c) &= n_1(p_1 - c) - n_0 p_0 \\ &= \frac{1}{2(\beta - 2)} c^2 - \frac{\alpha}{2(\beta - 2)} c + \frac{\alpha^2}{8(\beta - 2)} - \frac{\alpha^2(\beta + 1)^2}{8\beta^2(\beta - 1)}, \end{aligned}$$

which takes the minimum value at $c = \alpha/2$. Since $\overline{c} = (\alpha/2)\{(4 - \beta)/\beta\} < \alpha/2$ for $\beta > 2$, $D_1(c)$ is decreasing in $c \in [\underline{c}, \overline{c})$. It can be shown that if α and c are sufficiently small, $D_1(c) > 0$ and thus $\pi_1 > \pi_0$.

Lemma 2 For $\alpha \in [\underline{\alpha}, \alpha^+)$, where $\alpha^+ \equiv \overline{\alpha}\sqrt{\frac{\beta-2}{\beta-1}}$, there exists $c^+ \in (\underline{c}, c^*)$ such that $D(c^+) = 0$ and $D_1(c) > 0$ for $c \in [\underline{c}, c^+)$.

Proof. See Appendix.

The parameter α determines users' benefits of their own precautions against all types of security risks. Lemma 2 implies that ISP can have an incentive to clean up botnet malware when users' own precautions can not adequately protect their computers. Furthermore, for ISP to have an incentive to clean up botnet malware, the cost should be smaller than the level that on-line users increase as a result of ISP's cleanup.

Social welfare is defined as the sum of ISP's profits (π_i) and consumer surplus (CS_i). The latter is given as

$$\begin{aligned} CS_i &= \int_0^{x_{vi}} u_{vi}(x)dx + \int_{x_{si}}^1 u_{si}(x)dx \\ &= \frac{1}{2}x_{vi}u_{vi}(0) + \frac{1}{2}(1-x_{si})u_{si}(1) \\ &= \frac{1}{2}n_{vi}u_{vi}(0) + \frac{1}{2}n_{si}u_{si}(1). \end{aligned}$$

It can be shown that if the number of on-line users under the secured network ($i = 1$) is larger than that under non-secured network ($i = 0$), so is the consumer surplus.

Lemma 3 $n_1 > n_0 \iff CS_1 > CS_0$.

Proof. See Appendix.

From the lemma 1, 2, and 3, ISP's profits and social welfare under the two security statuses of the network are summarized as follows.

Proposition 1 Assume $\alpha \in [\underline{\alpha}, \alpha^+)$. Then,

(i) If $c \in [\underline{c}, c^+)$, then $\pi_1 > \pi_0$ and $CS_1 > CS_0$.

(ii) If $c \in [c^+, c^*)$, then $\pi_1 \leq \pi_0$ and $CS_1 > CS_0$.

(iii) If $c \in [c^*, \overline{c})$, then $\pi_1 < \pi_0$ and $CS_1 \leq CS_0$.

If the cleanup cost c is sufficiently small that $c < c^+$, there is no need to impose liability on ISP to secure the network because ISP has an incentive to do so voluntarily. Social welfare, defined as $\pi_i + CS_i$, is also maximized in this case. If $c \geq c^+$, imposing liability on ISP can improve consumer surplus because ISP does not have an incentive to voluntarily clean up botnet malware. Nevertheless, the cost should be smaller than c^* since otherwise the high access fee excludes marginal on-line users and decreases consumer surplus.

5 ISP's incentive to disconnect vulnerable users

As mentioned in Introduction, if liability for violations of cybersecurity is imposed on ISP, it may overreact. Because detecting and cleaning up botnet

malware in users' computers are costly, ISP may rather choose to disconnect users whose computers are vulnerable to malware infection. In this section, we examine ISP's incentive to disconnect vulnerable users and its welfare impact.

5.1 Equilibrium and consumer surplus

Let $i = 2$ denote the case that ISP disconnects users who do not take precautions against malware. In this case, only secure users are on-line and have utility

$$u_2(x) = n_2 + \alpha - \beta(1 - x) - p_2.$$

All other users are off-line and have zero utility. Let x_2 be such that $u_2(x_2) = 0$. Since $1 - x_2 = n_2$, the demand function is given as

$$n_2 = \frac{\alpha - p_2}{\beta - 1}.$$

ISP determines p_2 maximizing the profit $\pi_2 = n_2 p_2$, which is concave since $\beta > 2$ is assumed. The first order condition gives

$$p_2 = \frac{\alpha}{2} \quad \text{and} \quad n_2 = \frac{\alpha}{2(\beta - 1)},$$

where $n_2 < 1$ by the assumption $\alpha \leq \overline{\alpha}$ since

$$n_2 \leq \frac{\overline{\alpha}}{2(\beta - 1)} = \frac{\beta}{(\beta + 1)} < 1.$$

By lemma 3, consumer surpluses under ISP's three actions ($i = 0, 1, 2$) can be compared using the number of on-line users n_i. Then, it is shown that consumer surplus becomes the smallest if ISP disconnects the vulnerable users from the network.

Lemma 4 $CS_2 < \min(CS_0, CS_1)$.

5.2 ISP's incentive to disconnect vulnerable users

First, the comparison of $\pi_2 = n_2 p_2$ with $\pi_0 = n_0 p_0$ is as follows.

$$\begin{aligned} \frac{\pi_0}{\pi_2} \lesseqgtr 1 \quad &\Longleftrightarrow \quad \frac{(\beta+1)^2}{2\beta^2} \lesseqgtr 1 \iff \beta + 1 \lesseqgtr \sqrt{2}\beta \\ &\Longleftrightarrow \quad \beta \gtreqless \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1 \approx 2.41. \end{aligned}$$

Since $\beta \in (2,3)$, ISP can have an incentive to disconnect vulnerable users even without liability.[8]

If $\beta > \sqrt{2}+1$, disconnecting vulnerable users is more profitable for ISP compared to letting them connected without taking costly effort to clean up botnet malware. In this case, the degree of precautions' cost difference among users is so large that secure users are willing to pay the higher access fee if the network is secured by disconnecting vulnerable users ($p_2 > p_0$ is easily confirmed). On the other hand, if $\beta \leq \sqrt{2}+1$, ISP will not disconnect vulnerable users unless liability is imposed. In this case, the degree of precautions' cost difference is not large enough for secure users to pay the higher access fee (p_2). Then, charging the lower access fee (p_0) to as many users as possible including vulnerable ones is more profitable for ISP.

To compare π_2 with π_1, define $D_2(c) \equiv \pi_1 - \pi_2$:

$$\begin{aligned} D_2(c) &= n_1(p_1 - c) - n_2 p_2 \\ &= \frac{1}{2(\beta-2)}c^2 - \frac{\alpha}{2(\beta-2)}c + \frac{\alpha^2}{8(\beta-2)} - \frac{\alpha^2}{4(\beta-1)}. \end{aligned}$$

ISP's incentives to disconnect vulnerable users and to clean up botnet malware are examined according to the two cases of the parameter β above.

5.2.1 Does ISP disconnect vulnerable users when liability is imposed?

First, we assume $\beta < \sqrt{(2)}+1$. Then, ISP does not disconnect vulnerable users unless liability is imposed since $\pi_2 < \pi_0$. Moreover, if $c < c^+$, ISP's optimal choice is to clean up botnet malware from users' computers since $\pi_0 < \pi_1$.

Suppose $c \geq c^+$. Then, if liability is imposed on ISP, it has to secure the network by choosing whether to clean up botnet malware or to disconnect vulnerable users. If ISP chooses to clean up botnet malware, it should be $D_2(c) > 0$. Both $D_1(c)$ and $D_2(c)$ are convex quadratic functions taking the minimum values at $c = \alpha/2$, and thus $D_2(c)$ is a vertical shift up of $D_1(c)$ since

[8] In fact, there exist cases that ISPs voluntarily disconnected their users whose computers are the source of cybersecurity violations. For example, in 2008, a US hosting service provider McColo Corp., which had hosted botnets for years, was unplugged by two ISPs that were providing Internet connectivity to it. See "Host of Internet Spam Groups Is Cut Off" by Brian Krebs, washingtonpost.com, November 12, 2008.

$\pi_2 < \pi_0$. Then, by setting c^{++} such that $D_2(c^{++}) = 0$, it follows that $c^+ < c^{++}$. It can be also shown that $D_2(c^*) < 0$ by calculating $D_2(c^*) = n_0(p_1 - c^*) - n_2 p_2$ ($n_1 = n_0$ when $c = c^*$) and thus $c^{++} < c^*$ (see figure 1).

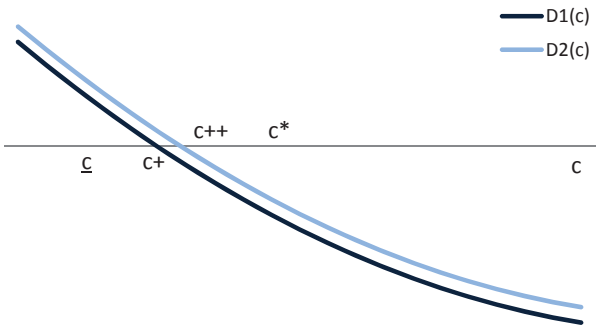

Figure 1: $D_1(c)$ and $D_2(c)$

Let $\alpha \in [\underline{\alpha}, \alpha^+)$ so that $D_1(\underline{c}) > 0$. Then, if $c \in [c^+, c^{++})$ and liability is imposed on ISP, it chooses to clean up botnet malware rather than to disconnect vulnerable users by the above arguments. In this case, the profit of cleaning up botnet malware is smaller than that of taking no action ($D_1(c) \leq 0$ for $c \geq c^+$), but consumer surplus increases by imposing liability since $c < c^*$. On the other hand, if $c \geq c^{++}$, ISP chooses to disconnect vulnerable users, and consumer surplus becomes the smallest. The results are summarized in the next proposition.

Proposition 2 Assume that $\beta \in (2, 1 + \sqrt{2})$, $\alpha \in [\underline{\alpha}, \alpha^+)$, and $c < c^*$. Then, $CS_2 < CS_0 < CS_1$ and

(i) $\pi_2 < \pi_1 \leq \pi_0$ if $c \in [c^+, c^{++})$.

(ii) $\pi_1 \leq \pi_2 < \pi_0$ if $c \in [c^{++}, c^*)$.

5.2.2 Does ISP clean up botnet malware when disconnecting vulnerable users is more profitable than taking no action?

Next, if the degree of precautions' cost difference is large ($\beta \geq 1 + \sqrt{2}$), ISP would disconnect vulnerable users even if there is not liability since $\pi_2 \geq \pi_0$. In this case, imposing liability on ISP dose not affect its action to secure the

network. However, the cleanup cost c can change ISP's action from disconnecting vulnerable users to cleaning up botnet malware, though depending on the parameter α.

When $\pi_2 \geq \pi_0$, $D_2(c)$ is a vertical shift down of $D_0(c)$ by the same argument as above, and thus $c^{++} \leq c^{+} < c^{*}$ (see figure 2). Since $n_1 = 1$ for $c = \underline{c}$,

$$\begin{aligned} D_2(\underline{c}) &= p_1 - \underline{c} - \pi_2 \\ &= \frac{\beta - 2}{2} - \frac{\alpha^2}{4(\beta - 1)} \\ &> 0 \iff \alpha < \sqrt{2(\beta-1)(\beta-2)} \equiv \alpha^{++}. \end{aligned}$$

Lemma 5 $\underline{\alpha} < \alpha^{++} \leq \alpha^{+}$ for $\beta \geq 1 + \sqrt{2}$

Proof. See Appendix.

By the lemma 5, if α is small enough, there exists $c \in [\underline{c}, c^{++})$ such that ISP chooses to clean up botnet malware rather than to disconnect vulnerable users when $\pi_2 \geq \pi_0$. In this case, however, an incentive for ISP to change its action to cleaning up botnet malware requires even lower users' benefit of taking precautions compared to the case that cleaning up botnet malware is the only option to secure the network.

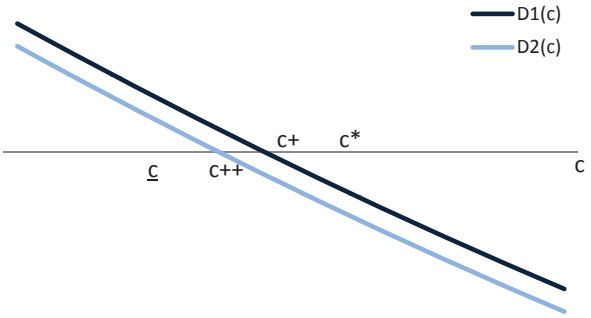

Figure 2: $D_2(c)$ and $D_1(c)$

6 Conclusion

Several researchers have argued that ISPs should take a more active role to clean up botnets from the Internet, and have suggested imposing indirect liability on

ISPs for damages caused by their customers' computers infected by botnet malfare, from which they are currently exempted. A concern of imposing liability on ISPs is that it may result in excluding a part of users of Internet access and reduce positive externalities. ISPs may raise access fee to compensate costly effort to clean up botnet malware, or they may disconnect connections of users who do not take precautions against malware to achieve the secured network without incurring cost.

The model analysis of this paper clarifies how the cost of malware clean-up affects a liable ISP's behavior and social welfare. If the cost is sufficiently low, ISP can have an incentive to voluntarily clean up botnet malware from its users' computers without disconnecting those users. If the cost is not low enough for ISP to have an incentive of voluntarily cleaning up botnet malware, imposing liability on ISP can have the following two effects on consumer surplus. The first effect is an increase in consumer surplus. Imposing liability on ISP removes negative externalities from the network and makes accessing the network more attractive, which results in an increase in on-line users and thus positive externalities. The second one is a decrease in consumer surplus. Imposing liability on ISP raises access fee or purges botnet-infected users, which result in a decrease in on-line users and thus positive externalities. If the clean-up cost is sufficiently high, the latter effect dominates the former one, and thus imposing liability on ISP decreases social welfare because both ISP's profits and consumer surplus decrease.

The model analysis also indicates that ISP can have an incentive to disconnect users vulnerable to botnet malware even without liability if users' preferences for precautions against malware is sufficiently different. In this case, securing the network by disconnecting vulnerable users makes it possible to charge other users the access fee high enough to increase ISP's profits. However, if the clean-up cost is sufficiently low, cleaning up malware from infected computers without disconnecting any users can be more profitable to ISP because letting vulnerable users be on-line makes positive externalities larger than disconnecting them.

There is an empirical case that can be a support for the results of this paper's model analysis. van Eeten et.al (2010) gathered data on the location of botnet

infected computers in the period 2005-2009 for the empirical analysis of global botnet infection. A part of their findings indicates that ISPs in Japan and Finland are, on average, among the least infected networks in the wider OECD area. These two countries are known for the collaboration between governments and ISPs for cybersecurity. For example, in Japan, ISPs collaborates with the government at the Cyber Clean Center (CCC). CCC detects infected users and passes the information to ISPs. Then, ISPs notify the affected users of infection and direct them to CCC's website, which offer free malware removal software developed by CCC. Thus, the Japanese government bears a large part of the cost for cleaning up botnet malware.

An implication of this paper's results is that making the cost of cleaning up botnet malware low is the most important to remove botnets from the Internet. Clayton (2010) illustrates how costly it is to detect end-user computers infected with malware and to effectively clean up those computers. Then, Clayton (2010) recommends subsidies to ISPs for cleaning up malware rather than imposing liability on ISPs as proposed by Lichtman and Posner (2006). This paper's results give theoretical justification for subsidies to ISPs by showing that imposing liability on ISP can worsen social welfare if the clean-up cost is not sufficiently low.

Appendix

Proof of Lemma 1

(i) $c^* < \overline{c}$

For $\beta \in (2, 3)$,

$$\begin{aligned} \overline{c} - c^* &= \frac{\alpha(4-\beta)}{2\beta} - \frac{\alpha}{\beta(\beta-1)} \\ &= \frac{\alpha}{2\beta(\beta-1)}(3-\beta)(\beta-2) > 0. \end{aligned}$$

(ii) $\underline{c} \leq c^*$

$$\begin{aligned} c^* - \underline{c} &= \frac{\alpha}{\beta(\beta-1)} - \frac{\alpha - 2\beta + 4}{2} \\ &= (\beta-2)\left\{1 - \alpha\frac{\beta+1}{2\beta(\beta-1)}\right\} \geq 0. \end{aligned}$$

since $\beta > 2$ and

$$\alpha \leq \overline{\alpha} = \frac{2\beta(\beta-1)}{\beta+1} \iff \alpha\frac{\beta+1}{2\beta(\beta-1)} \leq 1.$$

Proof of Lemma 2

Since $n_1 = n_0$ when $c = c^*$,

$$\begin{aligned} D_1(c^*) &= n_1(p_1 - c^* - p_0) \\ &= n_1\left\{\frac{\alpha+2c^*}{4} - c^* - \frac{\alpha(\beta+1)}{4\beta}\right\} \\ &= n_1\left(-\frac{\alpha}{4\beta} - \frac{c^*}{2}\right) < 0. \end{aligned}$$

Therefore, if $D_1(\underline{c}) > 0$, there exist $c^+ \in (\underline{c}, c^*)$ such that $D_1(c^+) = 0$ because $D_1(c)$ is decreasing for $c < \overline{c}$. Since $n_1 = 1$ for $\underline{c} = \alpha/2 - \beta + 2$,

$$\begin{aligned} D_1(\underline{c}) &= p_1 - \underline{c} - n_0 p_0 \\ &= \frac{\alpha+2\underline{c}}{4} - \underline{c} - \frac{\alpha^2(\beta+1)^2}{8\beta^2(\beta-1)} \\ &= \frac{\beta-2}{2} - \frac{\alpha^2(\beta+1)^2}{8\beta^2(\beta-1)}. \end{aligned}$$

Then,

$$\begin{aligned} D_1(\underline{c}) > 0 &\iff \beta - 2 > \frac{\alpha^2(\beta+1)^2}{4\beta^2(\beta-1)} \\ &\iff \alpha^2 < \frac{\beta-2}{\beta-1}\left\{\frac{2\beta(\beta-1)}{\beta+1}\right\}^2 = \frac{\beta-2}{\beta-1}\overline{\alpha}^2 \\ &\iff \alpha < \sqrt{\frac{\beta-2}{\beta-1}}\overline{\alpha} \equiv \alpha^+. \end{aligned}$$

$\alpha^+ < \overline{\alpha}$ is apparent. For $\alpha^+ > \underline{\alpha}$,

$$\begin{aligned} \frac{\alpha^+}{\underline{\alpha}} &= \sqrt{\frac{\beta-2}{\beta-1}}\frac{\beta(\beta-1)}{(\beta+1)(\beta-2)} \\ &= \sqrt{\frac{\beta^3-\beta^2}{\beta^3-3\beta-2}} > 1 \end{aligned}$$

since $\beta^3 - \beta^2 - (\beta^3 - 3\beta - 2) = \beta(3-\beta) + 2 > 0$ for $\beta \in (2, 3)$. Therefore, for $\alpha \in [\underline{\alpha}, \alpha^+)$, there exists $c^+ \in (\underline{c}, c^*)$ such that $D_1(c^+) = 0$, which implies that $D_1(c) > 0$ for $c < c^+$.

Proof of Lemma 3

(i) $n_1 > n_0 \iff n_{s1} > n_{s0}$, $n_{v1} > n_{v0}$

The utility of a secure user $x = x_{si}$ and a vulnerable user $x = x_{vi}$ are

$$u_{si}(x_{si}) = n_i - (1 - \delta_i)n_{vi} + \alpha - \beta n_{si} - p_i = 0, \tag{a1}$$

$$u_{vi}(x_{vi}) = n_i - (1 - \delta_i)n_{vi} - \beta n_{vi} - p_i = 0. \tag{a2}$$

From equations (a1) and (a2), it follows that $\alpha - \beta n_{si} + \beta n_{vi} = 0$. Thus,

$$n_i = n_{si} + n_{vi} = 2n_{si} - \alpha/\beta = 2n_{vi} + \alpha/\beta.$$

Thus, $n_1 > n_0$ is equivalent to $n_{s1} > n_{s0}$ and $n_{v1} > n_{v0}$.

(ii) $n_{s1} > n_{s0} \iff u_{s1}(1) > u_{s0}(1)$, $n_{v1} > n_{v0} \iff u_{v1}(0) > u_{v0}(0)$

The utility of a secure user $x = 1$ and a vulnerable user $x = 0$ are

$$u_{si}(1) = n_i - (1 - \delta_i)n_{vi} + \alpha - p_i, \tag{a3}$$

$$u_{vi}(0) = n_i - (1 - \delta_i)n_{vi} - p_i. \tag{a4}$$

Substituting (a3) and (a4) into (a1) and (a2) respectively, we have

$$u_{si}(1) - \beta n_{si} = 0,$$

$$u_{vi}(0) - \beta n_{vi} = 0.$$

Thus, $n_{s1} > n_{s0}$ is equivalent to $u_{s1}(1) > u_{s0}(1)$ and $n_{v1} > n_{v0}$ is equivalent to $u_{v1}(0) > u_{v0}(0)$.

(iii) $n_1 > n_0 \iff CS_1 > CS_0$

Since $CS_i = \frac{1}{2}n_{vi}u_{vi}(0) + \frac{1}{2}n_{si}u_{si}(1)$, by the above (i) and (ii), $n_1 > n_0$ is equivalent to $CS_1 > CS_0$.

Proof of Lemma 4

First, $n_2 < n_0$ and thus $CS_2 < CS_0$ since

$$n_2 = \frac{\alpha}{2(\beta - 1)} < n_0 = \frac{\alpha}{2(\beta - 1)}\frac{\beta + 1}{\beta}.$$

Second, $n_2 < n_0$ and thus $CS_2 < CS_0$ is confirmed as follows:

$$n_1 - n_2 = \frac{\alpha - 2c}{2(\beta-2)} - \frac{\alpha}{2(\beta-1)} = \frac{\alpha - 2(\beta-1)c}{2(\beta-2)(\beta-1)} > 0 \quad \text{for} \quad c < \overline{c}$$

since $\alpha - 2(\beta-1)\overline{c} = \alpha(\beta-2)^2/\beta > 0$. As is examined in section 4, $n_0 \lesseqgtr n_1$ is determined by the clean-up cost c. Thus, $CS_2 < \min(CS_0, CS_1)$.

Proof of Lemma 5

(i) $\underline{\alpha} < \alpha^{++}$

$$\frac{\alpha^{++}}{\underline{\alpha}} = \frac{\sqrt{2(\beta-1)(\beta-2)}}{2(\beta-2)} = \sqrt{\frac{\beta-1}{2(\beta-2)}} > 1 \quad \text{for} \quad \beta < 3.$$

(ii) $\alpha^{++} \leq \alpha^{+}$

$$\begin{aligned} \alpha^{+} &= \overline{\alpha}\sqrt{\frac{\beta-2}{\beta-1}} = \frac{2\beta(\beta-1)}{\beta+1}\sqrt{\frac{\beta-2}{\beta-1}} \\ &= \frac{\sqrt{2}\beta}{\beta+1}\sqrt{2(\beta-1)(\beta-2)} = \frac{\sqrt{2}\beta}{\beta+1}\alpha^{++} \end{aligned}$$

Since it is assumed that $\beta \geq 1 + \sqrt{2} = 1/(\sqrt{2}-1)$ and thus $\sqrt{2}\beta \geq \beta + 1$, it follows $\alpha^{++} \leq \alpha^{+}$.

References

[1] Choi, J.P., and B. Kim (2010) "Net neutrality and investment incentives," *Rand Journal of Economics*, 41, 446-471.

[2] Clayton, R. (2010) "Might Government Clean-up Malware?" 10th Annual Workshop on Economics and Information Security (WEIS10), available at http://weis2010.econinfosec.org/papers/session4/weis2010_clayton.pdf (last accessed on 2012/4/27).

[3] Economides, E. (2008) "Net Neutrality, Non-Discrimination and Digital Distribution of Content Through the Internet," *A Journal of Law and Policy for the Information Society*, Vol.4, pp. 209-233.

[4] Lichtman, D. and E. P. Posner (2006), "Holding Internet service providers accountable," in *The Law and Economics of Cybersecurity*, edited by M. F. Grady and F. Parisi, Cambridge University Press.

[5] Moore, T. (2010) "Introducing the Economics of Cybersecurity: Principles and Policy Options," Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, available at http://www.nap.edu/catalog/12997.html (last accessed on 2012/4/27).

[6] StopBadware Inc. (2011) "The State of Badware," available at http://www.stopbadware.org/pdfs/stateofbadwarejune2011.pdf (last accessed on 2012/4/27).

[7] Touré (2011) "Cyberspace and the Threat of Cyberwar," in *The Quest for Cyber Peace*, International Telecommunication Union and World Federation of Scientists, available at http://www.itu.int/pub/SGENWFS.0112011 (last accessed on 2012/4/27).

[8] van Eaten, M., J. M. Bauer, H. Asghari, S. Tabatabaie (2010) "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data," OECE Science, Technology and Industry Working Papers, available at http://www.oecd-ilibrary.org/scienceandtechnology/theroleofinternetserviceprovidersin-botnetmitigation_5km4k7m9n3vjen (last accessed on 2012/4/27).