Before the
Department of Commerce
Washington, D.C. 20230

In the Matter of	**)**	
	)	
Models to Advance Voluntary Corporate	**)**	
Notification to Consumers Regarding	**)**	**Docket No: 110829543-1541-01**
the Illicit Use of Computer Equipment	**)**	
by Botnets and Related Malware	**)**	

COMMENTS OF KINDSIGHT

Basil Alwan
Chairman of the Board and CEO
Kindsight
755 Ravendale Drive
Mountain View, CA 94043

November 14, 2011

Table of Contents

Before the
Department of Commerce
Department of Homeland Security
Washington, D.C.

In the Matter of	**)**	
	)	
Models to Advance Voluntary Corporate	**)**	
Notification to Consumers Regarding	**)**	**Docket No: 110829543-1541-01**
the Illicit Use of Computer Equipment	**)**	
by Botnets and Related Malware	**)**	

COMMENTS OF KINDSIGHT

I. INTRODUCTION

Kindsight applauds the National Institute of Standards and Technology, the National Telecommunications and Information Administration, and the National Protection and Programs Directorate of the Department of Homeland Security (collectively, the "Agencies") for this effort to identify how public and private actors can work together to counter botnet infections. The Agencies are right to identify botnets and malware as serious threats. Kindsight supports the development of a voluntary code of conduct that encourages Internet service providers ("ISPs") and individuals to use effective and affordable tools to enhance online security. To achieve the potential of these tools, it is critically important that a code of conduct preserves the ability of industry players to choose which technologies to deploy, how to package offerings for consumers, and how best to recoup investment in Internet security.

Kindsight provides an additional layer of protection against botnets and other malware by partnering with ISPs to deploy a network-based security service that ISPs can offer to subscribers using different business models. We encourage the Agencies to develop an industry code of conduct that supports botnet detection and eradication methods that work in real-world settings. Based on our experience:

- *ISPs are ideally positioned* to detect botnets and many other serious forms of malware, notify subscribers, and assist subscribers in removing botnets from infected devices.

- *Signature-based intrusion detection technology embedded in an ISP's network is one of the best methods for detecting botnets.* Signature-based intrusion detection technology provides indisputable evidence that the customer is infected, identifies the specific malware involved, and has proven to be very effective in service provider deployments. Unlike security software hosted on end-user devices that may not be kept up-to-date with rapidly-changing malware signatures and can be disabled by hackers, network-based

technology is maintained by the ISP so it's always-on, always up-to-date and cannot be disabled like client-based software. It detects malware based on its communications with command and control servers, which results in increased protection since that communication changes infrequently.[1]

- *To boost ISP and consumer participation, a code of conduct must encourage a variety of funding solutions.* Embedding signature-based intrusion technology in a network can be expensive, due to growing numbers of subscribers and climbing traffic loads. Detection sensors must be placed throughout an entire network. At the same time, studies show that rates of subscribership to a security service are higher if the service is offered on both a no cost (funded by advertising) and a paid basis, versus rates of subscribership to a paid offering alone.[2] In order to drive the offering and adoption of enhanced Internet security, industry players must be free to develop innovative business plans, such as Kindsight's offering of intrusion detection service at no-cost to Internet subscribers who explicitly opt-in to receive targeted ads.

Finally, Kindsight urges the Agencies to promote greater clarity and harmonization of federal and state law potentially applicable to network-based security technologies. For maximum effectiveness, ISPs must be able to examine the entire contents of suspicious information packets traveling within their networks to determine if they are malicious. At the same time, no detection services can guarantee 100% effectiveness, and removing malware from a computer may not be possible without causing additional harm. Further, while the potential for targeted advertising to help fund wide-spread adoption of enhanced Internet security is great, privacy laws and expectations are often unclear – even with respect to offerings like Kindsight that require an individual's prior, informed, opt-in consent. Such uncertainty discourages ISPs and other industry players from investing in existing, proven detection technologies. The Agencies should help establish the right incentives by supporting legal "safe harbors."

II. KINDSIGHT

Kindsight, headquartered in Mountain View, California, partners with ISPs to offer security and analytics platforms that can provide consumers with an additional layer of protection against online threats that might lead to identity theft, misuse of consumers' devices as part of a botnet attack, and other crimes.[3]

---

[1] Kindsight agrees with the security experts identified by the Agencies in the Request for Information that a successful approach to "stemming the tide of botnets has been for private sector entities to voluntarily and timely detect and notify end-users that their machines have been infected," noting that such private sector entities are generally ISPs. *See* Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware, Request for Information, 76 Fed. Reg. 58466, 58467 (Sept. 21, 2011).

[2] For example, in a 2010 survey of 1200 web users commissioned by Kindsight, 46% of users would purchase a Kindsight-type service for a fee, whereas 71% would sign-up if paid and no-cost options were available.

[3] Kindsight was started as a concept within Alcatel-Lucent and transitioned into an independent corporation in 2007.

One can think of the Kindsight service as an online burglar alarm. Homeowners typically protect their residences with strong locks, and for an added level of security, they frequently use an alarm service. By adding security equipment to an ISP's network, Kindsight enables ISPs to make available to their subscribers the online equivalent of a burglar alarm. If the Kindsight service detects the presence of an online threat, it will send an alert to prompt the subscriber to remove any malware infection, protect personal information or take other appropriate steps to protect the subscriber's home network. Kindsight gives subscribers step-by-step instructions how to fix the problem and where to go for additional assistance.

ISPs can offer the Kindsight Security Service to their subscribers free of charge in exchange for the opportunity for ISPs to serve them advertisements based on their online behavior, using a traditional ad network model. As a result, consumers can substantially harden their Internet security without a cash outlay, and ISPs can offset security expenditures through advertising revenue. The Kindsight Security Service is also available for an affordable monthly fee to subscribers who do not wish their online activities to be scored for advertising purposes. Moreover, a consumer is never assumed to have opted-in to the Kindsight service. Consumers must first express their interest in the security service and then make a choice either to pay the monthly service fee or receive the service at no cost by accepting targeted advertising.

Kindsight accordingly provides two-fold value to consumers. First, it is an additional layer of protection that does not require the consumer to install anything and is always kept up-to-date against the latest threats, and unlike software on a consumer's computer, network installations like Kindsight cannot be disabled by hackers. Kindsight partners with some of the security industry's most respected brands and actively participates in several security industry organizations, including the Messaging Anti-Abuse Working Group, the Anti-Phishing Working Group, and the Online Trust Alliance. Second, it overcomes consumers' general resistance to spending on Internet security and ISPs' resulting hesitance to make certain network investments, resulting in substantial, real-world security enhancements.

The Kindsight service uses advanced threat detection technologies to analyze consumer Internet traffic for attacks and other malicious activity that could place the subscriber's personal information or computer at risk. This is the case for all subscribers to the Kindsight service, whether they choose the fee-based or the advertising-supported subscription option.

For subscribers that opt-in to the advertising-supported option, the subscriber's ISP, while analyzing the subscriber's Internet traffic for threats, will continually score the online activity related to a household Internet protocol ("IP") address. Scoring is the process of analyzing, but not storing, web sites visited and searches conducted to assign a numeric value to various interest categories.

The Kindsight service does not read or analyze the content of emails or instant messages for advertising purposes. It also does not examine for advertising purposes any traffic related to sites that Kindsight classifies as sensitive, including sites related to pornography, sexuality, health, politics, hate, violence, drugs or criminal behavior. Sites we identified as directed to children are not scored or used for targeting.

When a subscriber visits websites or performs other online activities, the Kindsight service is designed not to interrupt, affect, or inject anything in the communication between the consumer's computer and any Internet content. This means that no traffic management is performed.

Kindsight understands privacy sensitivities regarding behavioral advertising. Our approach, which offers ISP subscribers a reliable, effective, and needed network security service funded through relevant advertising, recognizes that transparency and consumer privacy are paramount to a fair exchange for consumers. Accordingly, Kindsight contractually obliges its ISP customers to use clear, transparent notice and to obtain subscribers' affirmative express consent. Kindsight also requires ISPs to include in monthly bills and monthly emails to subscribers a reminder of the service and to provide links to additional information, including how to change subscription types and discontinue the service.

III. EMBEDDED SIGNATURE-BASED INTRUSION DETECTION TECHNOLOGY IS ONE OF THE MOST EFFECTIVE METHODS FOR MALWARE DETECTION.

While there are multiple security techniques capable of identifying botnets, one of the most effective techniques is signature-based intrusion detection technology embedded in a service provider's network. This technology successfully detects botnet command and control traffic coming from subscribers' home networks, as well as the activity of other serious forms of malware.

While malware's frequently changing packaging makes it difficult for client-based applications to keep up, the command and control traffic on which network-based technology relies tends not to change. For example, only one network signature is needed to detect the command and control traffic for the Zeus Banking Trojan, whereas hundreds of client-based signatures are needed to detect the different varieties of Zeus that may be installed on a specific computer. Thus, signature-based intrusion detection technology is able to detect malware even where the similar client-based technology fails.

To accurately detect an infection, Kindsight looks for unequivocal evidence of infection coming from the user's computer. For example, command and control protocols show when the computer is infected and currently being exploited by an attacker. Detection technologies like Kindsight should not look for attempts to infect a user's computer in the first place, because these attacks are not always successful and reporting them will result in a large number of "false positives." By limiting false positives, Kindsight increases the likelihood that an end user will perceive the infection notification as a serious threat and take the remedial steps necessary to remove the malware. In sum, because signature-based network detection systems can accurately detect specific malware and avoid false positives, they provide a high level of notification accuracy and a high likelihood that end-users will actually respond.

Finally, embedded signature-based intrusion detection technology is valuable to the remediation process. Because Kindsight can identify specific types of malware with confidence, it can suggest the best eradication tools to consumers. Further, the technology can track re-

infections, let the user know that prior malware evictions were not successful, and suggest different approaches or contacting support experts for additional help.

Thus, because embedded signature-based intrusion detection technology is adept at identifying rapidly changing malware, can determine specific types of malware, and enables notifications that give users additional information to aid in the remediation process, Kindsight believes that this technology is the most effective technique for countering botnet threats stemming from consumer Internet use.

IV. ISPs ARE IDEALLY POSITIONED TO NOTIFY CONSUMERS AND AID IN REMEDIATION OF BOTNET INFECTIONS.

A voluntary code of conduct should provide guidance to ISPs on how they can help their subscribers deal with botnet threats, but any guidelines must preserve industry players' broad flexibility in achieving this goal. ISPs are ideally positioned to detect botnets (as well as many other serious forms of malware), notify subscribers, and assist subscribers in removing botnet infections from end-user devices. As addressed above, embedding the signature-based detection technology in a network is one of the most effective ways to detect malware communications. ISP involvement is also critical to effective notification processes. As consumers have an ongoing relationship with their ISP, they are also more likely to view alerts from the ISP as credible threats and take the recommended action to remove the infecting malware.

While email is an effective notification option, ISPs can use multiple notification methods, including SMS, desktop toolbars, mobile apps, and interstitials to alert their customers to infections.[4] In some cases, it may be appropriate for the ISP to send the consumer web-surfing directly to sites that provide self-service eradication tools and instructions to remove the infection. It is important that a code of conduct allow different types of notice, as using multiple notification methods is important, in addition to the fact that consumers will better recognize fraudulent notifications if they control how and when they receive notifications.

Service providers should have the flexibility to offer to their subscribers, for a fee, value-added services for additional technical support and remediation. After a consumer is notified of an infection, ISPs could provide online support services in the form of a self-service website that offers instructions, tools, and FAQs that will help the user remove the botnet from their system. Currently, many botnet infections can be removed using scan and clean tools that are available from security vendors, including those with whom Kindsight partners.

V. TO ENCOURAGE MAXIMUM PARTICIPATION WITH A VOLUNTARY CODE OF CONDUCT, THE GOVERNMENT MUST ALLOW PARTICIPANTS FLEXIBILITY IN MONETIZING THEIR PRODUCT AND LIMIT PARTICIPANTS' POTENTIAL LIABILITY.

A voluntary code of conduct's success depends on participation in the program. Botnet detection and eradication solutions are costly and complex; thus, for providers to participate,

[4] Interstitials are warnings appended to the next web page(s) visited by the subscribers after detection.

they must be have flexibility either to charge for the service, sell additional services or use novel funding approaches where the service is offered at no or low cost. Additionally, because of the potential legal uncertainty, it is essential that the government create a "safe harbor" for industry players.

A. A Code of Conduct Should Not Constrain Participants' Ability to Fund their Services.

From a consumer participation standpoint, a free detection and notification service clearly drives higher adoption as it removes the financial barrier and risks associated with an online monetary outlay. Kindsight's market research indicates that over two-thirds of subscribers would sign-up for a detection and notification service if there was a no-cost option.

At the same time, for such a service to provide maximum detection capability, the signature-based intrusion detection system's sensors must be deployed throughout the entire network. With the number of subscribers and bandwidth usage exponentially increasing, sensor deployment is an expense that keeps growing. For providers to offer botnet notification and detection services, there must be a business case that makes sense.

It is critical that any code of conduct developed by the Agencies preserve the ability to sell additional value-added services or obtain consumers' consent to targeted advertising. These are attractive methods to help subsidize the capital and support costs providers face in offering a botnet detection and notification service. As discussed above, Kindsight uses an alternative economic model in which ISPs offer the Kindsight Security Service to their subscribers for a small fee or free of charge in exchange for the opportunity for ISPs to serve them advertisements based on their online behavior. It is essential to note that, with Kindsight, a consumer is never assumed to have opted-in to the Kindsight service. Consumers must first express their interest in the service and then make a choice either to pay for the service or to receive the service at no cost through relevant advertising. Thus, this business plan both allows an ISP to offset its deployment and operational costs and overcomes obstacles to consumers obtaining enhanced security.

B. To Encourage Participation, the Government Should Provide Clarity and "Safe Harbors" to Participating Companies.

Unfortunately, no solution for botnet detection, notification and remediation can be 100% foolproof. In such an uncertain environment, ISPs may decline to provide these and like services for fear of potential liability. Thus, to encourage ISPs to provide detection and notification services, the government must provide some form of a "safe harbor" for ISPs and other industry players that try to implement and participate in this initiative.

Further, there continues to be privacy-related concerns around targeted advertising. Kindsight addresses these concerns by requiring informed, meaningful consent from consumers before scoring their traffic for advertising purposes. Kindsight obligates its ISP customers to use clear, transparent notice and obtain subscribers' affirmative express consent to the advertising-supported option, where it is elected. Subscribers also receive monthly reminders about their

service and are free to switch at will from the advertising-supported security service to the fee-based model, and also to decline the service.

Notwithstanding these comprehensive privacy and consumer choice procedures, uncertainty in applicable privacy laws and the resulting liability risks inhibit companies' ability to adopt effective offerings like Kindsight. To reverse this trend, it is imperative that the Agencies work to clarify legal obligations and provide "safe harbor" protections for industry players working in this space.

VI. CONCLUSION

Kindsight thanks the Agencies for this opportunity to share its perspective. We believe that ISPs are best situated to detect botnets and notify end-users. Yet, ISPs and consumers face two primary challenges in deploying such technology: expense and uncertain liability. For ISPs to make necessary, expensive investments in network security, they must find a way to offset deployment and operation costs. While charging consumers directly is a valid option, wide-spread adoption of enhanced security monitoring will require reducing the costs to consumers through approaches like turning to advertising revenue. ISPs and their partners must be allowed flexibility in finding creative ways to offset their expenditures, and a voluntary code of conduct should encourage such innovation. Additionally, to alleviate ISP fears about potential liability, clarification is needed about legal obligations and legal "safe harbors" should be created.

Respectfully Submitted,

KINDSIGHT

By: ___/s/ Basil Alwan

Basil Alwan
Chairman of the Board and CEO
KINDSIGHT
755 Ravendale Drive
Mountain View, CA 94043

November 14, 2011