Before the
Department of Commerce

Models To Advance Voluntary Corporate)
Notification to Consumers Regarding the) Docket No. 110829543–1541–01
Illicit Use of Computer Equipment by)
Botnets and Related Malware)

COMMENTS OF AT&T

Keith M. Krom
Theodore R. Kingsley
AT&T Services, Inc.
1133 21st Street, NW
Suite 900
Washington, D.C. 20005
(202) 463-4627

November 14, 2011

Before the
Department of Commerce

Models To Advance Voluntary Corporate	**)**	
Notification to Consumers Regarding the	**)**	**Docket No. 110829543–1541–01**
Illicit Use of Computer Equipment by	**)**	
Botnets and Related Malware	**)**	

TABLE OF CONTENTS

*　　*　　*

Before the
Department of Commerce

Models To Advance Voluntary Corporate)
Notification to Consumers Regarding the) Docket No. 110829543–1541–01
Illicit Use of Computer Equipment by)
Botnets and Related Malware)

COMMENTS OF AT&T

AT&T, on behalf of itself and its affiliates, hereby submits these comments in response to the Department of Commerce (Commerce) and the Department of Homeland Security (DHS) (collectively “the Departments”) in the above referenced proceeding.[1]

I. Executive Summary

Perhaps the most insidious type of cyber attack that exists today is the botnet – the remote control of a collection of compromised end-user machines, usually broadband connected personal computers.[2] AT&T, a global IP network and Internet connectivity services provider, provides a wide range of tools and resources which are intended to safeguard consumers from botnet attack. AT&T selectively notifies its subscribers today of suspected botnet or malware infections, based on the type of threat, and assists affected users in remediation. AT&T makes available security software to its broadband subscribers and offers a variety of customer care options to remediate threats including both "self-help" resources provided by AT&T and third

[1] Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware, 76 Fed. Reg. 58,467 (September 21, 2011) (*Notice*).

[2] Amoroso, Cyber Attacks: Protecting National Infrastructure (Butterworth-Heinemann, 2011) at 6.

parties as well as fee-based customer care and professional support services through AT&T's ConnecTech organization for consumers in need of additional assistance. AT&T is also developing a web portal designed to help consumers diagnose whether a device has malware infections and to provide remediation solutions.

Customer notification is simply one tool that can be employed to combat cyber threats. Cybersecurity itself is a complex, multi-dimensional challenge not subject to simple solutions. As effective as ISP notification may be in certain instances, programs mandating such notification raise a number of implementation challenges, among them: how to identify end user devices that are infected with botnets or malware; how to provide effective and practical notices that end users will recognize as authentic, given to the prevalence of bogus notifications by malware distributors; how to remediate problems, given the complexity of many botnets and the fact that many consumers are ill equipped to remove malware; and how to manage substantial customer care burdens attendant upon such notification.

In contrast, the combination of consumer education efforts and the use of contextual customer notification with other cybersecurity tools provide a more effective strategy for enabling consumers to respond to botnets in a manner that reduces collateral implementation challenges. For example, an ISP referral of a customer to a tool such as a web portal allows customers to "self identify" the problem and take immediate action to obtain information or access tools to remediate the problem.

Even with this flexibility, ISPs alone cannot wage a successful defensive effort against botnets. The starting point for a meaningful solution is a sustained effort to educate consumers about the threat of botnets and the steps that consumers should take in order to protect themselves. Next, comprehensive collective action involving (i) the software makers who develop the operating systems and applications; (ii) the computing platform vendors who build and configure the hardware; (iii) the security vendors who provide the firewalls, anti-virus and anti-malware detection capabilities; (iv) domain name registrars; (v) search engines and online services providers; and (vi) ISPs and hosting service providers, is necessary to address the threat holistically within the Internet ecosystem.[3] For example, there may be other effective ways to provide notice to consumers, perhaps through services such as search engines, web browsers, security services, web mail and other online services that establish relationships with end users.[4]

Moreover, the effectiveness of any customer notification program is directly dependent upon an end user's ability to remediate the threat for which notification is received.[5] Notification alone will not suffice; consumers must have concurrent access to tools that effectively equip consumers to deal with the specific threat that is the subject of the notification. For example some malware is well known in the industry and can be addressed using existing security software or other tools. In other cases malware may be more sophisticated or relatively unknown and could require actions as extreme as the user having to reimage their machine. The combination of appropriate notice and concurrently available, appropriately tailored, remediation tools is the best solution.

[3] While ISPs have an essential role to play in combating botnets, ISPs are not the root cause of the botnet threat. Additional incentives and best practices are necessary in the area of software development, so that security aimed at reducing the botnet threat is designed and built into new applications and services from the outset.

[4] Third party lists are available that provide relevant information, such as end user IP addresses that are suspected to be infected with certain botnets. For example shadowserver.org maintains a list of suspected Conficker infected machines. These lists could be used by a variety of parties to provide notice to their end users and may help alleviate privacy concerns arising out of ISP information sharing.

[5] There are no metrics on either the practical or the cost effectiveness of any of these measures. While the Department states that many security researchers support notification as a means to reduce the prevalence of malware, and some countries have implemented programs such as what is contemplated, there is no evidence to support that these programs have had a measurable impact on the prevalence of malware.

ISPs such as AT&T are actively working with a wide variety of security organizations to share information about security practices. Service providers have market incentives to offer a variety of robust security solutions, including various forms of notifications. In the absence of any demonstrable, empirical evidence that notification efforts have materially reduced botnet threat, the Department should resist calls for standardized, sector-wide notification regimes. Rather, even as stakeholders study the effectiveness of these notification programs, the Department should encourage experimentation and innovation in order to avoid the potential of prematurely standardizing any solution that may ultimately prove sub-optimal in addressing the changing cyber threat.

Government engagement can effectively support private sector efforts to combat botnets in the following areas: (1) continuing to support efforts to promote cyber security awareness and education, including broad education on the need for good cyber security; (2) sponsoring research on the effectiveness of notification programs; (3) aiding industry collaboration and identification of how collective action can be applied to reduce the threat of botnets; and (4) engaging industry in a dialog on ways to couple education and awareness with building market demand for consumer security services that may incent ISPs and others to develop more innovative tools for consumers to help themselves.

II. AT&T Offers Consumers a Range of Tools and Services to Combat Botnets

As the largest provider of communications and network services in the world, AT&T has a long history of engaging in a range of cybersecurity activities necessary to protect its network and its customers and we invest significant resources to innovate and keep pace with emerging technology that may be either the source or the target of cyber-threats. The size and scope of

AT&T's global network, coupled with its industry-leading cybersecurity capabilities, gives AT&T a unique perspective on malicious, world-wide cyber-activity.

For example, our intelligent network enables us to analyze traffic flows to identify very early indicators of attacks and address them at the network layer before they have the opportunity to become major events. We are constantly improving our cyber-capabilities, including the ability to detect and mitigate the most sophisticated and pernicious forms of cyber attack, including Advanced Persistent Threats. We also develop and offer a wide variety of industry-leading managed security services to individual consumers, small and medium business, public sector entities, and private sector enterprise customers.

AT&T provides a wide range of tools, resources and capabilities for consumers to choose from in order to stay safe online - including tools that notify consumers of the presence of malware, tools that enable consumers to detect the potential presence of malware and botnets on their internet access service or in some cases computing devices, and tools that do both. AT&T offers a web portal that provides "self-help" resources to consumers to remediate problems and offers paid customer care and professional support through its AT&T ConnecTech organization in situations where consumers need additional assistance. AT&T also supports a variety of education and awareness efforts in order to point consumers to resources that will help them stay safe online.

AT&T provides a number of consumer remediation and notification tools related to botnet and other threats, including the following:

- *AT&T Internet Security Suite.* AT&T currently offers an Internet security suite that is powered by McAfee and includes anti-virus, anti-malware, anti-spam and other capabilities. The service is free of charge to certain AT&T High Speed Internet (i.e., DSL) and AT&T's U-verse Broadband High Speed Internet Access service subscribers. For those customers that are not eligible to receive AT&T's Internet security suite for free, AT&T offers the option to purchase AT&T's Internet Security Suite for a monthly charge or obtain information on how to access other free Internet security suite offerings, such as Microsoft Security Essentials, which offers similar capabilities to the McAfee suite of tools provided by AT&T.

- *PC Health Check.* AT&T "PC Health Check" is a free web based tool offered by AT&T's ConnecTech organization that performs a detailed scan and diagnosis of a customer's PC performance, health and security risks, including malware detection. PC Health Check is linked to AT&T's ConnecTech customer care services which, as described in more detail below, are designed to help consumers remediate problems.
- *AT&T Identity Project.* AT&T Identity Project is a paid identity protection service that tracks consumer's information in order to determine if they are at risk for identity theft.
- *Bot or Not.* AT&T is developing a "Bot or Not" service that will help consumers determine if their PCs are potentially infected with a botnet. It will also include a self-help web portal as well as a range of paid customer care options. Our planned "Bot or Not" portal, which is scheduled to be launched next year, will permit consumers to determine whether their PCs may be infected based upon two methods: (1) an online questionnaire that will help users self-assess whether their machine is potentially infected with malware; and (2) a free web-based tool for AT&T's broadband subscribers that will identify whether the subscriber's account has been communicating with known malicious hosts based upon subscriber traffic flow

information.[6] As part of the planned "Bot or Not" portal AT&T will provide links to "self-help" remediation tools and information about paid customer care options offered by AT&T's ConnecTech organization in the event the end user needs additional assistance. This service will be optional and will be self-initiated by AT&T's subscribers.

- *AT&T Mobility Security Applications*. As smartphone adoption increases, technologists and researchers expect criminals to step-up their efforts with new delivery mechanisms for attacks, ushering in a new phase of mobile security risks. While only in their infancy today, the volume, severity and sophistication of those threats should earn them a prominent place on the security agenda. Thus AT&T is also investing in a new mobile security platform that is designed to manage and protect smartphones and customer information at the network and device layers by providing government, businesses, and consumers with the ability to protect services and applications seamlessly between wired and wireless environments. The application is intended to provide customers anti-virus, anti-malware, personal firewall, anti-spam, and application monitoring and control.
- *Customer Notifications*. AT&T notifies end users of botnet infections and helps with remediation on a case-by-case basis in response to large scale threats.[7] This is typically done in response to botnets such as the Rostock or Zeus botnets and for those end users impacted by fast flux. However it is not limited to those threats and

[6] AT&T currently "tags" AT&T issued IP addresses that have communicated with known botnet host controllers based upon a variety of sources. When a subscriber elects to use the planned "Bot or Not" portal AT&T will attempt to determine whether the IP address assigned to that end user account has been tagged as communicating with malicious hosts, indicating a high likelihood of infection.

[7] In September 2011 AT&T issued several thousand such notices to its subscribers.

includes recent botnets and other emerging security threats. Notification is accomplished by AT&T's Internet Investigation Security Services Center ("IISSC"). [8] When an end user account has been identified AT&T will send a notification to all e-mail addresses, primary and secondary, associated with the subscribers account. Subscribers are then directed to do-it-yourself support options linking to information about security tools available on the Internet as well as information about AT&T's customer care options, including "AT&TConnecTech."

- *AT&T ConnecTech.* AT&T ConnecTech customer care services are available for a fee and include a series of home computer configuration and support services delivered on premises or through an authorized remote connection. Subscribers can use AT&T ConnecTech services on a one-time basis, a per incident basis, or on a subscription basis through AT&T's "Support Plus" service which offers unlimited help with software, hardware, peripherals, network issues and anti-virus/malware solutions currently for $14.99/month. In addition to removing viruses or adware/spyware, AT&T ConnecTech focuses on: resolving connectivity issues; installing and configuring software; dealing with operating system or browser problems; improving computer performance; and setting up a wireless network or connect additional peripheral devices. More information is available at https://buyconnectech.att.com/ctcomm/home/index.jsp.
- *Consumer Awareness.* Finally, AT&T provides a variety of resources and partners with third parties to raise consumer awareness of security issues. AT&T Smart Controls is a web portal that provides information and tools across AT&T's mobile

[8] The IISSC was established to implement Internet Engineering Task Force ("IETF") standard RFC2142 that was established in 1997 that called for ISPs to maintain an address for reporting abuse. For example if an AT&T IP address was distributing spam or involved in fast flux it could be reported to the abuse center by a third party.

and wireline platforms to help consumers. The portal includes AT&T Smart Limits for wireless (providing end users with the ability to block calls, text messages and otherwise limit phone use), Internet parental controls (providing end users the ability to manage web content, spam and time spent online), U-verse parental controls, and articles, resources, tips and advice on topics ranging from fighting malware to social networking safety.

AT&T is also an active participant in and supporter of a variety of third party cybersecurity and online safety education campaigns. AT&T is a founding member of the national cybersecurity awareness campaign "STOP. THINK. CONNECT.," and also is active in and with variety of relevant non-profit organizations including the Family Online Safety Institute (FOSI), iKeepSafe and other third party partners.

III. Suggested Roles for Government

The U.S government, working in partnership with technology providers in the private sector, should continue to support educational efforts which promote cyber security awareness and increase innovation while at the same time improving the underlying technology foundation to address cyber threats such as botnets. Integral to this effort is widespread consumer education on the need for good cyber security, which should have the collateral effect

of igniting market demand for diverse cybersecurity solutions that will, in turn, spur technological innovation. Because there are a variety of tools and resources already available to help consumers protect themselves online, but that are not being used to make a significant dent in the botnet problem, the Departments should align with other government agencies and the private sector to expand efforts to both educate consumers on the nature of the botnet threat and on the availability of existing tools to help them stay safe online.

As an example, the Commerce Department should consider expanding its efforts with the National Cybersecurity Alliance ("NCSA") in connection with the ongoing "STOP. THINK. CONNECT." cybersecurity awareness campaign. In an expanded role, the Department in partnership with NCSA could develop a web portal under the auspices of the awareness campaign to provide consumers a "menu" of resources provided by ISPs and other entities to help steer them to better use of the tools already available today. Government can also sponsor research on the effectiveness of notification programs.[9] The Department can also play a convening role to ensure industry collaboration and determine how collective action from all parties in the ecosystem can be leveraged to address botnets. A good place to start would be a catalog of current private and public sector practices in this space. There are multiple efforts already underway in the private sector along these lines that could be beneficial for this purpose. Issues such as notification and remediation techniques and resources should be part of this effort.

IV. Responses to Issues Raised by the Department

Code of Conduct

The private sector, and in particular ISPs, already have strong market incentives to adopt rigorous cybersecurity practices appropriate to their unique platforms and commercial offerings including the offering of a variety of cybersecurity services to our customers. ISPs are already actively engaged in a variety of efforts to share cybersecurity practices such as the Messaging Anti-Abuse Working Group or MAAWG and a variety of other security organizations. Thus there exists a general understanding of the various practices that are being employed in the industry. Several other entities who are participants in the internet ecosystem are active in these

[9] While the Commerce RFI notes that many security experts agree that notification is one tool that has proven effective in reducing the rate of botnet infection they offer no evidence to support that claim. Also the foreign governments and private sector companies that have introduced similar programs have not offered any data to prove that these programs are effective.

efforts as well. Thus it is unclear as to whether or not a code of conduct will materially improve cybersecurity in as much as much of this information is already being shared and a variety of techniques are being experimented with.

Neverthless, it would be appropriate for the Department to play a convening role in encouraging an ecosystem wide conversation to catalog and identify some of these practices, while at the same time resisting calls for adoption of a more rigid and restrictive code that in the end does not improve, and indeed, harms, cybersecurity.[10] The nature of the cyber threat is constantly changing and ISPs and others in the ecosystem should be encourage to experiment with different approaches to determine what is most effective. Adopting a rigid code could encourage a "check-the-box"mentality that discourages innovation through trial and error.. Moreover, publishing a rigid and static code to follow will discourage investment and innovation and could potentially provide cyber criminals with a baseline, if not a roadmap, to exploit end users.. Therefore, with respect to "Codes of Conduct," The government should therefore avoid a rigid approach with respect to an ISP Code of Conduct and instead encourage a framework that allows for ISPs and others to experiment with different and innovative techniques to deal with the botnet threat.

Education and Awareness

There is a critical need for more resources to truly ensure that current cybersecurity awareness campaigns effectively reach end users. As part of an invigorated information campaign, tips on how to address botnets and information on what tools are available to consumers should be included.

[10] AT&T is unaware of any empirical evidence that notification on any scale has materially reduced the botnet threat.

Methods of Notice

To the extent that notice is provided ISPs should be afforded flexibility in how they help consumers address botnets. There are diverse approaches in the marketplace today - including e-mail notices, web portals, and walled gardens. No approach is superior for all purposes. One example is the "Bot or Not" portal approach that AT&T is developing. In this case the *user* would elect to use the tool and AT&T would not correlate information about an IP address identified as having communicated with a malicious host with a subscriber account until that user has initiated a request and consented to the identification. In addition, other entities such as operating system providers, web browsers, search engines, security software vendors, and others may also be in a position to improve botnet mitigation and situational awareness through communications with end users. At the same time, multiple notices to consumers from multiple entities may only add to consumer confusion and frustration. Cybersecurity is an industry-wide problem, and, given that there is little to no information on the effectiveness of notification programs to date, it is imperative that a broad discussion should take place concerning the best ways to reach consumers including how notice could be provided by other participants in the ecosystem.

Finally there are a number of ways in which the industry cooperates and shares information in regards to botnets and malware. For example, there are third party lists of infected machines that could be used by a variety of stakeholders to provide notice. Any mechanism put in place to share information has to safeguard the privacy and security of individual internet users. And there are anti-trust and other legal issues that the government could address that would provide a better environment for sharing information to address cyber threats.

Remediation

The Department also inquires about how a government help desk could play a role in this process. AT&T, upon discovering that a consumer's computer or device is likely to be infected by a botnet, contacts the consumer to offer both self-help and other support services. Other service providers respond in similar fashion. The private sector is more likely to offer timely and relevant remediation options to consumers than a government help-desk; however, as discussed above, government awareness and education efforts can enhance private sector remediation efforts.

Liability and Incentives

The Department asks whether or not companies should be granted protection from liability for acting to notify consumers that their services or devices are infected and, if so, what protections would be most effective in incentivizing notification.

Ideally, companies should operate within a clear legal framework. Most of the statutory regimes that could be applicable to cyber-threat detection, response and reporting were created before the Internet and before cybersecurity became vital to preserving integrity and trust in that system. These outmoded statutory frameworks impose significant liability risks for individuals and entities acting in good faith, particularly where those entities operate within multi-jurisdictional and complex regulatory structures. Liability protection, therefore, is essential.

A clear legal framework with appropriate liability protection should spur the more rapid development of cybersecurity solutions. The framework should be written in technical or functional terms, not legalistic, so that the technical experts can understand what they can and should do without having to engage in substantial legal analysis from their attorneys. Companies can spend significant sums of money and incur significant delays in responding to potential and actual cyber-threats while waiting for an analysis of whether the detection and proposed response could be construed as “wiretapping” or some other prohibited conduct under existing law. The potential threat of civil or even criminal sanctions for an unwitting violation of outmoded existing laws discourages creativity in formulating responses to anticipated and detected cyber-threats.

A legal framework that enables lawful legitimate cybersecurity activities, as opposed to narrowly construed “cybersecurity” exceptions written into existing civil and criminal statutes that were enacted before the current state of cyber threats, would be more helpful. Clarity, transparency, and the reduction of risk, will go a long way to free up private investment in cybersecurity solutions and increase voluntary participation by private sector entities in botnet mitigation.

Measuring Effectiveness

In addition to building market based incentives, there must necessarily be some understanding that the tools themselves are actually working to mitigate botnets. While there have been various attempts to study this problem, there doesn’t appear to be any empirical data that points to the effectiveness of these programs, whether being done domestically by other service providers or internationally in Australia, Japan or Germany. The Department should sponsor and encourage sound empirical research in this area.

V. CONCLUSION

The ultimate key to improving national cybersecurity is technology innovation driven by market demand from informed users and purchasers of all kinds. By creating market demand for cybersecurity through heightened consumer awareness, the Department can spur fundamental security innovation at all levels of the Internet eco-system, and create the conditions that will allow the United States to continue as a leader in Internet development.

Respectfully submitted,

By: _________*/s/* ____________

Keith M. Krom
Theodore R. Kingsley
AT&T Services, Inc.
1133 21st Street, NW
Suite 900
Washington, D.C. 20005
(202) 463-4627

November 14, 2011