KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

November 14, 2011

The Honorable Lawrence E. Strickling
Assistant Secretary for Communications and Information
Department of Commerce
1401 Constitution Avenue, NW
Room 4822
Washington, DC 20230

RE: Request for Information Regarding Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware

Dear Assistant Secretary Strickling:

The Center for Democracy & Technology (CDT) promotes balanced laws and policies that protect both national security and individual rights. CDT submits these comments in response to the September 21, 2011 Request for Information (RFI) issued by the Department of Commerce (Commerce) National Institute of Standards and Technology (NIST), the National Telecommunications and Information Administration (NTIA), also at Commerce, and the Department of Homeland Security (DHS).[1] The RFI concerned the proposed creation of a voluntary industry code of conduct to address the detection, notification, and mitigation of botnets, as recommended by Commerce's "Green Paper" on Cybersecurity, Innovation and the Internet Economy.[2]

Botnets pose a serious and challenging threat to the nation's computing environment. A botnet is created when an intruder installs malicious software on a consumer's computer or other Internet communications device and then connects that device to a remotely controlled network. The intruder may use the bot to capture information from the consumer's device, facilitating fraud or identity theft. In addition, the intruder may exploit the consumer's computing power and Internet access to perform malicious activities pursuant to the directions of the intruder. These activities may include disseminating spam, launching denial of service attacks, or hosting illegal content.

An important and unique aspect of the botnet problem is that the intruders, once they have taken over a consumer's device, then use that device to infect other consumers. In order to prevent the spread of botnets, malicious software must be immediately removed or mitigated. However, the bot often runs without degrading the computing experience of the infected

[1] 76 Fed Reg. 58466-58469 (Sept. 21, 2011).

[2] http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf

consumer. The challenge posed by botnets is to either equip consumers to determine for themselves if their computers are infected or for Internet Service Providers (ISPs) to determine which computers are infected and then to notify in an effective manner those consumers and encourage them to take action.

We applaud Commerce and DHS (collectively, the “Departments”) for their leadership in this area and for seeking to facilitate a multi-stakeholder process to develop private sector standards and practices to address the botnet threat. We urge the Departments, as they facilitate this process, to ensure that steps recommended in any industry code to address the botnet threat also preserve Internet privacy and the free flow of information. Below, we identify a number of best practices we would like to see ISPs adopt, and we also identify certain practices that should be avoided.

The focus of the RFI is on what ISPs can do to address residential broadband vulnerabilities, but, of course, the botnet problem involves many players and cannot be solved by ISPs alone. Botnets gain access to a consumer’s device through software vulnerabilities, through poor user practices such as the failure to install patches or the use of weak passwords, through malicious Web sites, and through social engineering techniques. We commend the Departments for taking as a first step a narrow approach with a focus on the role of ISPs and residential broadband, but we encourage the Departments to consider how to promote improvements in other sectors, such as software.

I. Developing and promoting an effective, yet flexible, voluntary code of conduct

The Green Paper proposed the development of security best practices that can become the basis for a voluntary code of conduct. We agree with the Green Paper that the process of developing such a code should be transparent and multi-stakeholder, open to consumer advocates and full participants. As described in the RFI, this code would be directed at ISPs and would include best practices on detection, notification and mitigation of botnets. Currently, there is no such code, and ISPs function independently in addressing botnets, or they participate in informal arrangements through which they share information about botnets and botnet mitigation with other ISPs and/or security vendors. We see benefits to organizing a set of industry best practices in this area, but we must also point out the benefits of the latitude that ISPs currently have in monitoring their networks to protect against malware. ISPs have used that authority very cautiously and have appropriately resisted calls that they become gatekeepers in the service of various societal interests. We are very concerned that any code for ISP cybersecurity practices not become a model for the assumption or imposition of broader gatekeeping functions. The best way to do that, we believe, is to be explicit about the risks of ISP gatekeeping. To that end, the botnet code should not only recommend best practices but it should also discourage intrusive approaches or methods that would be harmful to privacy or the openness of the Internet. The code will be as important for what it recommends against as for what it recommends affirmatively.

One of the challenges in creating industry standards to address botnets is that the threat is constantly evolving, and what may at one time have been an effective practice to protect an ISP’s network may be obsolete by the time that practice is incorporated in a voluntary code. The voluntary code should not be so prescriptive that it diminishes incentives for ISPs to adopt new and innovative ways to combat botnets. In particular, the code should not directly or indirectly impose technology mandates. We suggest that the Departments plan to work with stakeholders to re-valuate the code on a regular basis, with public comment.

As a final note, we flag that significant open questions remain concerning how the voluntary code will interact with existing law, including Section 5 of the Federal Trade Commission Act, and with Federal Trade Commission enforcement and what legal impact the code might have on ISPs that agree to follow the best practices and those that do not.

II. Both government and ISPs play an important role in preventing botnet infections through consumer education

One of the essential components of any solution to the botnet problem is consumer education. Consumers should have a basic understanding of malware, what steps they should take to reduce the risk that their devices will be infected, how to tell if they have a bot, and where they can go for help to mitigate a botnet infection. DHS has sought to educate consumers through its Cybersecurity Awareness campaign. We would like to see botnet education included in that campaign.

ISPs, of course, play an important role in malware education through their own communications with their customers. A voluntary code should encourage ISPs to provide specific information to their customers. We agree with the recommendations of the Federal Communication Commission's Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 8 that ISPs should educate their customers in a number of important areas.[3] A code of best practices should specifically recommend that ISPs provide their customers with information about how to mitigate a botnet once they have been infected and about the services the ISP will provide to assist its customers with botnet mitigation.

As CSRIC concluded, educated consumers will also need certain tools to protect their computers. The voluntary code should recommend that ISPs provide their customers with anti-virus security software, firewalls, and reminders to regularly update and to use strong passwords.[4]

[3] In Best Practice Prevention 2, CSRIC Working Group 8 recommended educating consumers about the following: use of legitimate security software that protects against viruses and spywares; ensuring software downloads or purchases are from a legitimate source; use of firewalls; configuring computers to download critical updates to both the operating system and installing applications automatically; scanning computers regularly for spyware and other potentially unwanted software; keeping all applications, application plug-ins, and operating system software current and updated; exercising caution when opening e-mail attachments; using judgment when downloading programs, viewing Web pages, using instant messaging, and social networking sites; and good practices around using passwords and keeping them private. http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.

[4] CSRIC Working Group 8 Best Practice - Prevention Number 3.

III. ISPs must use detection methods that protect consumer privacy

A voluntary code should encourage ISPs to detect and identify botnets in their networks, but the code should also encourage ISPs to do so in a manner that maintains consumer privacy and their ability to access the Internet.[5]

First, the code should recommend that ISPs assess where the threats are coming from and narrowly tailor their detection methods to meet those threats. For example, bots generally do not communicate through email, instant message, or VoIP traffic, so it is not reasonable for ISPs to scan those communications unless their assessment indicates otherwise.

Second, the code should recommend against the broad application of intrusive monitoring techniques such as deep packet inspection (DPI). We agree with the recommendations in the CSRIC report, that ISPs should first "cast a wide net" using less intrusive techniques such as traffic analysis to identify possible spam or other traffic indicative of botnet infection and should apply DPI or signature techniques only to traffic flagged as a potential problem by those less intrusive means.[6] A code of best practices should specify that ISPs should use a privacy-invasive measure only after other measures have failed and only if the ISP reasonably believes it is necessary to protect the customer and the network. In addition, it should be a best practice to minimize the collection and use of application-related data.

Third, ISPs must be very judicious in collecting the content of customer communications or personally-identifiable information about customer communications. The best practices should specify that ISPs should not generally collect content or other information about the communications of specific customers, but should only do so if it is necessary to do so and only where it is reasonable to believe a particular customer is infected.

Fourth, if ISPs do collect information about customer communications related to botnet detection, the voluntary code should require that they safeguard that data in a way that protects privacy and appropriately discard it as soon as it is no longer being used. Specifically, the voluntary code should recommend that any data collected for bot detection purposes be protected with the same security safeguards that the company applies to other data it collects about the functioning of its network. The code should also include as a best practice that ISPs de-identify data where possible and delete or aggregate data they no longer need.

Fifth, ISPs should disclose in their privacy policies the circumstances under which they examine the communications of individual customers, under what circumstances they record information about the communications of particular individuals, and what they do with any communications information they record. ISPs can provide sufficient transparency to customers without providing a level of technical detail that could be a roadmap for intruders.

Finally, if the Departments adopt the proposal to facilitate a private or public resource center for botnet information and consumer education, then the voluntary code should include specific

[5] As described in CSRIC's report, ISPs use a range of methods to detect botnet infection, including external feedback, observation of network conditions and traffic such as bandwidth or traffic pattern analysis, signatures, behavior techniques, and forensic monitoring of consumers on a more detailed level. CSRIC Working Group 8 Best Practice - Detection Number 2, p. 21.

[6] CSRIC Working Group 8 Best Practice - Detection Number 3, p. 22.

provisions detailing under what circumstances it is appropriate for ISPs to share consumer information with such a center. If a resource center is not created, the voluntary code should address information sharing and make it clear that if ISPs share personally identifiable information with any third party (i.e., with a private clearinghouse or with other ISPs) then the third party must be under a contractual obligation to secure the information and not use it for any purpose other than botnet detection or mitigation.

IV. Effective consumer notification is essential for botnet remediation

Timely and effective notification to consumers that their devices are infected with a bot, and information and support on how to mitigate, are essential to address the botnet threat. If consumers are unaware that their devices are infected, they will not take steps to mitigate and the bot will continue to attack and exploit the consumer's device as well as others. However, how ISPs can effectively notify their customers is a real challenge.

The voluntary code should encourage ISPs to employ a number of methods to notify their customers of a problem. These methods include email to the account holder, notice through the browser, phone calls, text messages, and postal mail. No method of notification is perfect, and it is important that any voluntary code give carriers the flexibility to choose the best method of notification tailored for both the needs of their company and the individual customer. Notification needs to be especially robust if the consequence of failing to respond to notice could include a restriction on a customer's Internet access. In any such case, the ISP should include processes to affirmatively confirm that notice has actually reached the responsible customer (as opposed to, for example, the household teenager). Whichever method of notification is used, the content of the notification must clearly and simply inform the customer of the infection, explain what to do in order to mitigate the bot, and urge the customer to take action quickly. The message should not solicit the customer for additional business or be confused with a commercial solicitation.

ISPs should be encouraged to evaluate a number of considerations in selecting a notification method:

- An account may have multiple users, some of whom are children.
- To be effective, notice must be reliable and the ISP must avoid sending notices that a customer will mistake as spam or a virus.
- The email address that an ISP associates with an account may be wrong or infrequently used by its customer, and there is no guarantee that a consumer will read an email in a reasonable time frame.

V. ISPs should assist consumers in mitigating botnet infections

The most important step an ISP can take to mitigate botnet infections is to help its customers clean up their own devices. We strongly urge the Departments not to affirmatively encourage ISPs to restrict the Internet access of consumers in response to this threat. Overall, we believe other steps that can be included in the voluntary code will go a long way in addressing the botnet problem, so we recommend that for the time being that walled gardens not be endorsed as a best practice.[7] However, the best practices should include due process standards for ISPs to follow to ensure that they do not excessively restrict consumers from accessing the Internet. In addition, the best practices should include measures to ensure that ISPs do not engage in blocking or filtering practices that carry risk of interfering with lawful content and websites.

The voluntary code should encourage ISPs to provide to their customers a "security portal" that offers resources for mitigation, including the steps customers must take to clean their devices and kept them free of infection. This portal should also point customers to third parties that specialize in mitigation and can provide extra assistance, even for a fee. Finally, ISPs should be encouraged to provide a phone number for assistance and information for customers who are not able to, or comfortable with, accessing the information online.

We believe that these are resources most ISPs are best suited to provide directly to their customers. We have doubts about whether a centralized consumer center, as described in the RFI, will be helpful or necessary in this role. We do see value in promoting information sharing among ISPs on detected botnets, compromised hosts, bad domains, or new techniques to mitigate bot infections and new threat vectors, but any such clearinghouse should be non-governmental. In information sharing, consumer privacy must be protected, and where possible information should be de-identified prior to being shared. The private sector may already have established adequate information sharing systems; the impediments to more effective information sharing may center on perceptions about what current law permits or prohibits. Other than clearing up legal uncertainties in a narrow and privacy-protective fashion, we see little need for government action in this regard.

The voluntary code should clearly lay out what ISPs should not do to mitigate botnets. In particular, we are concerned that ISPs might block or re-direct traffic or interfere with the Internet activity of consumers on the basis of erroneous determinations. As a threshold matter, therefore, the multi-stakeholder process should assess the degree to which ISP botnet determinations are reliable, and this assessment should drive the decision about what anti-botnet measures are appropriate. If the stakeholders decide that ISPs are capable of appropriately blocking infected IP addresses without impacting lawful communications, then ISPs should also be required to document their reason for blocking a particular IP address. ISP should disclose the number of websites they block and their false positive rates, *i.e.*, the number of blocked IP addresses that were later assessed not to be involved in illegal activity. This information should be evaluated during future reviews of the voluntary code, and, if the false positive rate is too high, then additional due process steps should be included in the voluntary code as a means for IP addresses to contact ISPs if they believe they are wrongly labeled as a bot or as a "command and control" center for a botnet.

CDT also has concerns with ISPs disrupting their customers Internet connections in order to force the consumers to mitigate a botnet infection. Blocking consumers from the Internet or otherwise interfering with their access is sometimes called the "walled garden" approach, and it raises many complicated issues. We understand that for particularly dangerous and invasive

[7] By "walled garden" we mean the practice of cutting off or otherwise interfering with a customer's Internet connection until the customer cleans his computer or other infected device of the bot. We do not think it would be inappropriate, when other notification methods have proven unsuccessful, to require a customer to click on a botnet notification pop-up box before proceeding with their session. The box would advise the customer that his device is infected with a bot and point the customer toward the ISP and third party services available to deal with the problem.

bots, or for consumers who have been repeatedly notified but refuse to – or are unable to – clean their devices, walled gardens might seem a potential option for ISPs that otherwise would have no recourse. However, we do not believe that the voluntary code should recommend to ISPs that they include walled gardens as one of their mitigation methods. At most, this decision should be left up to the ISPs. However, the code should recommend that ISPs adhere to certain procedural safeguards if they do decide on their own to place their customers in walled gardens. For example, ISPs should use walled gardens only for serious infections and solely as a last-ditch notification effort directed at a customer who has failed after repeated notifications to mitigate his or her device. The IPS should ensure, however, that the customer is still able to communicate in an emergency (for example VoIP), and the ISP should provide an accessible and effective process for the customer to demonstrate that his or her device is in fact not infected.

VI. Conclusion

We thank the Departments of Commerce and Homeland Security for the opportunity to issue these comments. CDT is heartened by the steps the Departments and the industry have taken to address botnet infections. It is critical that all stakeholders work together to improve the overall security of the Internet. Please do not hesitate to contact us if we can be of any assistance.

Greg Nojeim

Greg Nojeim
Director, Project on Freedom, Security & Technology

Kendall C. Burman
Senior National Security Fellow