



November 14, 2011

Sent via email to [consumer\\_notice\\_RFI@nist.gov](mailto:consumer_notice_RFI@nist.gov)

Mr. Lawrence E. Strickling  
Assistant Secretary for Communications & Information, Department of Commerce  
National Institute of Standards and Technology  
U.S. Department of Commerce  
1401 Constitution Avenue N.W.  
Room 4822  
Washington, D.C. 20230

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

Docket No. 110829543-1541-01

Dear Mr. Strickling,

The Online Trust Alliance, (OTA), is pleased to submit these comments in response to NIST's, NTIA's, and DHS's (collectively, "the Agencies") Notice of Inquiry dated September 21, 2011. As a member-based non-profit association, OTA includes over 85 organizations representing the Internet ecosystem. OTA's mission is to develop and advocate best practices and public policy to mitigate privacy, identity, and security threats to online services, brands, organizations and consumers, thereby enhancing online trust and confidence.

As echoed in your paper, OTA agrees that bots and related malicious software represent a significant threat not only to consumers but to the broad public and private sectors including service providers, businesses and government agencies. Bots can compromise users' and businesses' information and communications, exploiting their computing functionality and Internet access. Once a bot is deployed, criminals have the ability to access personal information, browsing history and email communications, compromising the user's identity, privacy and personal documents, as well as a business's confidential information. Botnets impact not only the user and their computer, but like contagious disease can impact the general population of internet users. It is important to recognize this is a transnational issue and one which requires global support to effectively counter these emerging threats.

We believe a “voluntary code of conduct” or recommended practices can provide a framework for all parties including ISPs, carriers and related service providers to identify best practices and accelerate efforts to detect, mitigate and remove bots from Internet-connected devices. Such a code and respective voluntary guidelines represent the shared responsibilities between the public and private sector and demonstrate a commitment to self-regulation. Providing a voluntary code is effective, OTA believes our economy is best suited with such self-regulatory efforts over added legislation and regulations, which risks encumbering legitimate businesses and stifles innovation.

This position is based on the assumption that such guidelines are meaningful, actionable and measurable. As an incentive to stakeholders who embrace such efforts and demonstrate they are taking measures to protect consumer from harm, they should be viewed favorably by existing State and Federal laws and regulations such as Section 5 of the FTC Act.

OTA has a long-history of supporting such efforts and codes of conduct including ISP best practices, publishing specific guidelines for countering malvertising, driving adoption of email authentication, enhancing security of email service providers and publishing data breach readiness guidelines.<sup>1, 2, 3, 4</sup>

To aid in the development of such voluntary practices, it is recommended the Department of Commerce work with the private sector and other government agencies to fund a workshop to share best practices and lessons learned with the goal of accelerating the development of solutions to address botnet threats. To be effective, such a program must include all stakeholders across the entire ecosystem. Ultimately this will lead to the development of a tool kit and framework for broad usage. A model to be considered is the recently released “Why Your Browser Matters” initiative. Recognizing the browser is the first line of defense; OTA formed a cross industry working group including browser developers, security vendors and leading consumer facing web properties. This effort led to the development of a comprehensive implementation guide released in September in cooperation with National Initiative of Standards and Technology’s (NIST) Cybersecurity Education workshop.<sup>5</sup>

---

<sup>1</sup> Anti-Malvertising Guidelines - <https://otalliance.org/resources/malvertising.html>

<sup>2</sup> Security by Design Email Marketing Guidelines - <https://otalliance.org/resources/securitybydesign.html>

<sup>3</sup> Data Incident Planning Guide - <https://otalliance.org/resources/Incident.html>

<sup>4</sup> Email Authentication <https://otalliance.org/resources/authentication/index.html>

<sup>5</sup> Why Your Browser Matters – Implementation Framework & Voluntary Guidelines <https://otalliance.org/browser>

The following is a summary of key questions which OTA has addressed:

1. What existing practices are most effective in helping to identify and mitigate botnet infections? Where have these practices been effective? While there are multiple security techniques to identify and mitigate botnet infections, one technique is to use signature-based intrusion detection technology that is embedded in the service provider's network. This detects botnet command and control (C&C) traffic coming from the subscribers' home networks, as well as the activity of other serious forms of malware. Signature-based intrusion detection provides evidence that the customer is infected, identifies the specific malware involved and has proven to be very effective in service provider deployments. Being able to identify the specific malware lends credibility to the notification messages and can help to select the best tools during the remediation process.

One of the key reasons that signature-based, network intrusion detection techniques is effective is that while the packaging of the malware may change frequently and make it difficult for client-based security signatures to keep up, the command and control traffic tends not to change. For example, only one network signature is needed to detect the C&C traffic for the Zeus Banking Trojan whereas hundreds of client-based signatures would be needed to detect the different varieties of Zeus installed on the computer.

2. What preventative measures are most effective in stopping botnet infections before they happen? Where have these practices been effective? One of the key preventative measures that consumers need to take to stop botnet infections is to ensure their security software, operating systems and other applications and plug-ins are up-to-date on all devices including computers, smartphones, tablets, gaming consoles, etc. Consumers should turn on automatic updates and install the updates when prompted but most consumers are not diligent. OTA strongly recommends all users (consumers and businesses), upgrade to modern browsers which include the most up to date security and privacy features.

Today upwards of 40% of users have outdated browsers. As the first line of defense, having an up-to-date browser is a simple step to protect users and their devices from abuse. In September 2011, OTA launched "Why Your Browser Matters", an industry wide initiative. This initiative calls on service providers and web sites to provide teachable moments to notify users of outdated browsers the importance to their security, privacy and online experience to upgrade to a more current browser. Several companies including PayPal, Ticketmaster and Publishers Clearing House, (PCH) are implementing such programs, effectively enhancing users' security and privacy protection. With the message coming from a site the user trusts and frequents, and provided at time of data collection results can be extremely effective. PCH, reports upwards of 60% of users have upgraded their browser when presented with a contextual notification.<sup>6</sup> (See question 4 for additional recommended preventative measures).

---

<sup>6</sup> Why Your Browser Matters – Implementation Framework <https://otalliance.org/browser>

3. Are there benefits to developing and standardizing these practices for companies and consumers through some kind of code of conduct or otherwise? Service providers who adopt the code of conduct have the potential to realize a wide range of benefits including increased consumer loyalty, enhanced brand reputation and service differentiation. Additionally, having a customer base with better protected PCs and devices can reduce support costs and lower bandwidth requirements due to reduced malicious traffic/spam. In addition, by taking this proactive course of action, they demonstrate a commitment to self-regulation, reducing the call for legislation and regulation.

For consumers, the benefits include reducing the risk of consumer's data and personal information from being compromised along with enhanced online performance and connectivity. For small businesses and those who work from home (typically entities without any IT and technical support infrastructure), such detection and remediation can help protect their infrastructure, data and resulting loss of productivity and income as a result of a bot related incident.

In addition, such efforts could aid in preventing a data breach or data loss incident, which can significantly impact any business.<sup>7</sup> Combined these benefits represent the potential for businesses to realize costs savings as well as increased consumer confidence in the use of their services and enhanced brand integrity which collectively are the foundation of online commerce and internet based services.

4. Identify existing practices that could be implemented more broadly to help prevent and mitigate botnet infections. Prevention measures are a shared responsibility of service providers including ISPs, web site owners, government agencies as well as the end user. OTA advocates for the following best practices:
- a. Commerce, banking and government online services, develop “teachable moments” to upgrade drive users to upgrade their browsers to current versions offering enhancing security and data privacy features and controls.
  - b. All software, applications and operating systems be configured to auto-update as the default setting.
  - c. Providers of wireless routers / modems configure devices to require a password and unique user name.
  - d. eCommerce, banking and related sites migrate to “always on SSL”.
  - e. All business and government agencies authenticate their outbound and inbound email, to help counter the distribution of malicious and malware infected email which is the one of the leading sources of botnet code distribution.
  - f. Promote education and security awareness, through the use of teachable moments.

---

<sup>7</sup> See Data Breach & Incident Readiness Planning Guide <https://otalliance.org/resources/Incident.html>

5. Upon discovering that a consumer's computer or device is likely infected by a botnet, should an ISP or other private entity be encouraged to contact the consumer to offer online support services for the prevention and mitigation of botnets? Such notification is a critical step toward protecting the future of the Internet ecosystems. Internet service providers have a unique “line of sight” into the Internet traffic coming from a user’s machine and as a result have an opportunity to notify a user of such activities.

There are similarities to how utility companies act today to protect the greater good of the community and their infrastructure. For example a water utility may require the installation of backflow valves and annual testing. Upon discovery of a defective valve, they may terminate or restrict water supply until the problem has been rectified. In this example it is important to note the utility company is not a plumber and does not have the responsibility for repairs within a home.

In order to help remove the botnet and prevent it from spreading or causing damage, the service provider or other private entity should contact the user with one of several mechanisms: email, SMS or interstitials (i.e. warnings appended to the next web page(s) visited by the subscribers after detection). The long-term use of interstitials is cautioned including the risk of spoofing and use by the cybercriminal. Online support services should be made available 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. In deciding to adopt these and other notifications, providers need to consider the cost impact and ability to scale for a large number of users with a range of expertise and operating environments.

In some cases, it may also be appropriate to temporarily suspend the subscriber’s service, or quarantine them with limited access such as educational resources, self-service tools and instructions on how to remove the infection.

In addition, it is recommended that a directory of service providers including both remote support and walk-in service centers be provided that can help with such remediation including system scan/clean/wipes and recovery. It is anticipated service providers may negotiate special offers and discounts for their customers.

6. What should customer support in this context look like (e.g., web information, web chat, telephone support, remote access assistance, sending a technician, etc.) and why? Due to the potentially high cost of providing customer support, the initial effort should be in the form of a self-service website that offers instructions, diagnostic tools and FAQs that will help the user remove the botnet from their system. Second tier telephone support, remote access or onsite support can be offered as a fee based or value-added service to help off-set the operational costs of providing such services.
7. When identifying botnets, how can those engaged in voluntary efforts use methods, processes and tools that maintain the privacy of consumers' personally identifiable information? Anti-bot practices, technologies and services need to address privacy concerns and by default include safeguards to prevent the use of user data for any other purposes. It is

understood that, when evidence of a botnet is detected, there is a minimum set of information that needs to be stored in order to notify the consumer and help them remove the threat. This information may include the type of malware that was detected, the source and destination IP addresses, and the time the malware was detected. It may also be beneficial to capture samples of the malware for further analysis in order to develop better techniques to detect and mitigate it in the future. All of this information must be managed in a secure and sensitive manner in order to maintain the privacy of consumers.<sup>8</sup> As an incentive for adoption of voluntary best practices, it is suggested a safe harbor for data usage be created to help alleviate these concerns for service providers with verifiable privacy protections.

It is also anticipated there may be legitimate scenarios where a user may allow the service provider to collect personal information or monitor online activities. This is reasonable providing the user is provided notice specifically stating what data elements collected, the purposes it is used for and who it may be shared with along with the ability to opt-out of any such collection without penalty.<sup>9</sup>

8. How can organizations best avoid “false positives” in the detection of botnets? False positives are an inherent reality of virtually all online abuse detection systems. For example they can result in legitimate email being classified as spam or web sites being classified as a potential phishing or malicious site. Today service providers and browser vendors provide recommendations for users, email marketers and web sites to adopt best practices to help avoid such false positives. It is anticipated that similar advice can be provided to users to minimize the risk with botnets and to provide them the ability to self-assert they have completed a system analysis or provide their service provider remote access to verify the removal of the threat.

Improved and increased sharing of data among service providers will aid in the timely detection of zero-day exploits, reduce the risk of false positives and ultimately increase the confidence of such notices. Today many service providers and security vendors provide such services on a real-time basis for ISPs, business and government uses and data sharing among trusted service providers is encouraged.

9. To date, many efforts have focused on the role of ISPs in detecting and notifying consumers about botnets. It has been suggested that other entities beyond ISPs can participate in anti-botnet related efforts. Should voluntary efforts focus only on ISPs? If not, why not? OTA believes there is shared responsibility across a range of service providers, web sites and industry to provide services to help defeat botnets. For example, today many anti-virus providers provide tools resident on the client machine to detect abnormal system behavioral and comprehensive system scanning and signature analysis. Others entities may include frequently visited and trusted web properties including social networking, banking and

---

<sup>8</sup> See OTA ISP best practices [https://otalliance.org/docs/OTA\\_FCC\\_CyberSecurity\\_10-15.pdf](https://otalliance.org/docs/OTA_FCC_CyberSecurity_10-15.pdf)

<sup>9</sup> See FTC Privacy Statement Guidelines <http://www.ftc.gov/opa/2010/12/privacyreport.shtm>

commerce sites; companies which provide online analytic tools and browser vendors that are increasingly adding security functionality within the browser.

For some stakeholders competitive opportunities including the desire for product differentiation and the long-term impact alone will justify the development of such services. We have already observed some ISPs such as CenturyLink and Comcast providing self-service tools, resources and base-line support at no-charge. It is anticipated others may charge, offer annual subscriptions or provide advanced support on a fee-basis.

10. What means of notification would be most effective from an end-user perspective? Email remains one of the most effective notification systems, yet its use can be limited. Primary limiting factors include the fact the email address on record with the ISP may no longer be used or infrequently checked. As reported in OTA research, email spoofing, fraudulent email security warnings and use of malvertising and pop-up warnings are increasingly diluting the impact of legitimate notices.<sup>10</sup> To help address the possibility of users not receiving email alerts, or ignoring them, service providers should explore methods to proactively reach out to customers to update the email address for such critical notifications. Multiple notification methods should be considered including SMS and mobile apps. In addition, notices such as inclusion in billing statements and mailings should be considered.
11. For those companies that currently offer mitigation services, how do different pricing strategies affect consumer response? Are free services generally effective in both cleaning computers and preventing re-infection? Are fee-based services more attractive to certain customer segments? A free or no-charge service most likely will drive higher consumer adoption as it removes any financial barrier or potential or perceived conflict of interest of a service provider of putting monetization above consumer's best interests. While this is clearly best for the long-term health and vitality of the internet, such support can be costly and could lead to overall increased costs for all users. It is anticipated the market and desire for competitive differentiation will drive such business decisions including the potential emergence of advertising supported services to off-set such costs. While OTA is not advocating for such practices, if offered the consumer must be presented with and agree to clear terms about how the service is offered and how such advertising or tracking of their online behavior is conducted. In such service offerings, the subscriber needs to understand what information they are providing in exchange for any cost savings and how they may opt-out without any penalty. If such practices are developed, service providers must have verifiable processes to remove PII and covered information, limit retention and have a data loss incidence plan in place.
12. Once a botnet infection has been identified and the end-user does not respond to notification or follow up on mitigating measures, what other steps should the private sector consider? What type of consent should the provider obtain from the end-user? Who should be responsible for considering and determining further steps? In some cases, it may be

---

<sup>10</sup> <https://otalliance.org/news/releases/EmailAuthTPoint.html>

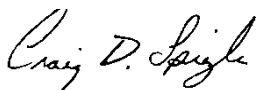
appropriate for a service provider to suspend the subscriber's service, or quarantine them preventing access to the Internet until the infection has been removed. In such cases where a user does not respond to notification, the infected machine is not just a threat to the owner/user, but a persistent threat to all those within the ecosystem. Quarantining can help prevent further damage to other users while limiting internet access and can serve as an incentive for the user to take corrective action. It is important to note service providers who bundle VOIP and connectivity need to take steps to assure phone and 911 services remain uninterrupted.

Such practices are not totally unique to internet users. For example users of outbound email accounts can be suspended, blocked or throttled in the event of detected abuse (spam) or malicious activities. In other case websites with known malicious code or downloads may be blocked by browsers and ISPs until the site owner is able to remove the threat. Such actions are taken to minimize abuse and impact to other users as well as the impact to the overall infrastructure.

In summary, developing voluntary guidelines embraced by multiple stakeholders will represent a significant step toward protecting users and businesses while enhancing online trust and confidence. To be effective we need to not only look at the U.S., but work with our international partners to curb the creation and distribution of these threats and share threat intelligence.

These comments reflect the general consensus of our membership and technical committees. OTA looks forward to making continued contributions towards these efforts including working with the Commerce Department in creating a workshop to accelerate the sharing of best practices and drafting of an implementation framework. Working together, the public and private sectors have a shared responsibility to enhancing online trust and confidence while protecting online security and privacy of all users.

Sincerely,



Craig D. Spiegle  
Executive Director and President  
Online Trust Alliance