StopBadware comments on DHS and DOC Botnets RFI (Docket No. 110829543–1541–01)

Thank you for soliciting comments on the establishment of a voluntary code of conduct to address botnets. StopBadware is a not for profit anti-malware organization based in Cambridge, Massachusetts, and with origins at the Berkman Center for Internet & Society at Harvard University. We focus on the prevention, mitigation, and remediation of badware websites. As these websites are a common means of distributing malware (bot-related and otherwise) to end users, our work is itself a form of botnet prevention. In addition, our efforts closely parallel the work being explored to combat botnets. As such, it is our hope that our experience in this area can provide valuable insights to inform the Departments and the industry.

Prior to addressing specific questions raised in the RFI, we offer one observation about the semantics of the request. The RFI repeatedly references “detection, notification, prevention, and mitigation” of botnets and their attendant malware. Missing from this list is “remediation,” which in this context refers to removing malware from end user devices and repairing any damage done by the malware. In contrast, “mitigation” refers to reducing the impact of malware presently infecting user devices.

Our remaining comments focus on three areas identified within the RFI: prevention of malware infections; the needs of users; and opportunities for shared, collaborative resources.

Prevention of malware infections

This section discusses several, but by no means all, effective approaches to reducing the risk of malware infection of individual end user devices, such as computers or smartphones. Because the methods of malware distribution and infection tend to be independent of the malware’s behavior on the infected device, we do not distinguish botnet-related malware from malware more broadly.

One important element of prevention at a systemic level is reducing the vectors by which users can encounter malware. Thousands of websites each day, for example, are established or compromised to distribute malware to unsuspecting site visitors. StopBadware has assisted hundreds of thousands of website owners in remediating their compromised sites and protecting them from future compromise. In so doing, the number of website visitors exposed to malware infection through these sites has been sharply curtailed. Still, additional work remains to be done in this area. With greater resources and broader collaboration, we can develop the notification mechanisms, the educational materials, the industry practices, and the shared knowledge needed to fundamentally disrupt the use of the Web as a malware distribution vector.

A second effective approach to protecting end user devices from malware is minimizing users’ exposure to the threat vectors that *do* exist. Much progress, for example, has been made in filtering spam email, which frequently attempts to distribute malware to users via links or attachments. We are also making progress in shielding users from malicious websites. All of the major Web browsers and the dominant U.S.-based search engines use blacklists of known malware URLs to warn users before they are exposed to threats. Some browsers, like Internet Explorer 9, also provide warnings about suspicious file downloads. StopBadware collaborates with Google and Mozilla to ensure that users encountering malware warnings through their products are not only protected, but also exposed to "just in time" educational messaging[1]. This helps raise awareness of the risks so that users are less likely to fall victim to malicious sites in the future.

One limiting factor in protecting devices from malicious content is that users do not always use current generations of products which are frequently more secure and offer additional protection against malware. Data from comScore, for example, shows that 36.8% of browsers used in the U.S. and Canada are "legacy" versions that lack the latest protection. This is true even though there exist free, newer versions capable of running on users' existing operating systems. This is why StopBadware is part of a coalition of companies and organizations supporting the Online Trust Alliance's "Why Your Browser Matters" initiative. This initiative employs popular consumer-facing websites in detecting the use of older Web browsers and alerting their users to the benefits of upgrading. Early evidence is that this project is showing success in prompting upgrades.

When users and devices *are* exposed to malware, it is important to limit the potential damage. Recent studies[2] have shown that today's malware typically exploits well known, and already fixed, vulnerabilities in commonly used applications like Oracle's Java, Adobe Reader, Adobe Flash Player, and Microsoft's Internet Explorer. It is therefore evident that one effective measure to reduce malware infection rates is to install updated versions of these applications. In practice, this will require user education, along with tools that make it easy for users to learn which software requires updates[3].

User education can also be helpful in preventing users from becoming victims of social engineering attacks. There is no "one size fits all" solution to educating users, but there are a few elements that can improve the efficacy of educational initiatives:

- Each initiative should start with an understanding of its target users' existing mental models of security. Researcher Rick Wash mapped several common mental models and their implications on users' security practices in his 2009 paper "Folk Models of Home Computer Security[4]."
- Consistent messaging, like that espoused by the Stop. Think. Connect. campaign[5], helps to reinforce a small number of broadly applicable, easily understood principles.
- Just in time messaging, like that embodied by StopBadware's aforementioned collaboration with Google and Mozilla, or the Anti Phishing Working Group's Education Landing Page Program[6], often has a greater impact than broad, out of context information campaigns.
- Similarly, mitigation and remediation efforts can lead directly to opportunities to educate users about prevention from future infection.

[1] See, for example, http://www.stopbadware.org/firefox.

[2] See, for example, http://www.csis.dk/en/csis/news/3321 and http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf

[3] Examples of such software include Qualys's Browser Check and Secunia's Personal Software Inspector.

[4] http://www.rickwash.com/2009/folk-models-of-home-computer-security/

[5] http://www.stopthinkconnect.org

[6] http://education.apwg.org/r/about.html

A final critical element of prevention is the use of current, automatically updated security software. While it is true that no software offers perfect protection, claims that security software is largely ineffective are frequently based on outdated testing methodologies. Recent anti-virus products and security suites incorporate a number of layers of protection that substantially reduce the risk of device infection. That said, security software should be treated as the final layer of defense, much like an alarm system in a home or office, rather than being depended upon for complete protection.

Together, the bulk of today's malware should be preventable on end user devices through a layered approach that reduces the number of threat vectors, mitigates exposure to the remaining threats, limits vulnerabilities on devices, supports informed decision making, and offers detection of those threats that have still slipped through.

The needs of users

As the Departments consider what industry can do to address the threat of botnets, it is critical to also recognize the important role played by individual consumers and small businesses that own or use infected devices. In particular, if users are to be expected to remove malware after being notified that their devices are infected, we must have a clear understanding of what users need to do so effectively.

StopBadware is particularly well suited to comment on this issue. Our longest running project is a collaboration with Google and two other blacklist operators[7] to assist website owners—mostly consumers and small business owners—that have recently been informed that their sites were blacklisted due to detection of malware. This can be a surprising and stressful experience for individuals that frequently have little or no experience with malware remediation. We have learned, and continue to learn, how to effectively guide users from notification to a successful resolution (i.e., a website that is no longer a threat to visitors, is cleared from the blacklist, and is protected against future compromise).

Based on our experience, when site owners first learn that their site is blacklisted, they ask a series of questions that typically looks something like this:

1. What does this mean?
2. Why do you think my site has malware on it?
3. How is it possible my website could be infected without my knowledge?
4. What am I supposed to do about this?
5. What will happen if I do (or don't) remove the malware?
6. How do I find and remove the malware?
7. I need help. Who can I trust to help me find and remove the malware?
8. How can I remove my website from the blacklist?
9. How do I make sure this doesn't happen to me again?

A well crafted notification can go a long way toward answering, or pointing users toward the answers to, many of these questions. See, for example, the email notification sent by Google to the owners of

[7] GFI and NSFOCUS

blacklisted websites[8]. In the cases of #6 through #9, users demand a broad range of support that includes both free self help resources and paid products and services. Genuinely valuable free resources allay user concerns that the notifications are intended to sell products and help to distinguish legitimate notifications from copycat scams that seek to trick users into purchasing fake products. Free resources are also essential to ensuring that users—especially those of limited means—voluntarily take the steps necessary to address the malware. On the other hand, just as many car owners choose to pay someone else to change their oil, many malware victims prefer the convenience, expertise, and other benefits that come with paid products and services.

Fortunately, in the case of malware, there exists a robust market of products and services at a variety of price points. ISPs engaged in notifying customers of malware may choose to enter this market themselves, partner with existing vendors to offer services to their customers, and/or leverage the broader market. Whatever the approach, it is important that consumers are aware of their options and that ISPs do not abuse their role as notifier by artificially constraining the market through misleading communications or overly restrictive walled gardens.

As for free resources, these might be offered directly by the ISP or through referral to a third party resource. An ideal set of offerings might include the following:

- A website with educational content, in written and/or video form, walking users through each of the required steps.
- Basic tools to assist users with prevention, identification, and remediation of malware and vulnerabilities.
- A volunteer-driven online community where users can seek and receive assistance from other users and/or industry experts[9].
- A directory of vetted products and services for users that are unable or unwilling to address their concerns themselves and/or that offer enhanced security beyond the free resources provided. One model for offering a broad directory of such services would be to create a marketplace with feedback mechanisms that allow users to rate and share reviews of products and services they have used.

In the next section, we identify an opportunity to establish a national or international resource center to provide these services for users whose ISPs choose not to offer such a resource themselves.

Opportunities for shared, collaborative resources

We see three areas in which shared, collaborative resources can do more to advance the public interest of fighting botnets than a voluntary code of conduct alone.

First is a clearinghouse for information about detected bots. Several non-profit and for-profit security organizations, such as ShadowServer and Arbor Networks, detect bot activity in the course of their work.

[8] Reproduced at https://badwarebusters.org/main/itemview/3972
[9] See, for example, our online community for website owners at https://badwarebusters.org.

Third party DNS services, including Google DNS and OpenDNS, also can detect certain malware-related behavior exhibited by their users' devices. In July of this year, Google even demonstrated that it could detect computers infected with a particular variety of malware as they visited Google's websites[10].

While ISPs should also leverage their unique ability to detect bot traffic on their own networks, a clearinghouse would provide ISPs a more comprehensive view into the infected devices within their zones of control. The Australian Internet Security Initiative[11] exemplifies a model in which an independent entity serves as a clearinghouse for efficiently gathering intelligence about detected bots from a variety of sources and sharing it with the appropriate ISPs, which can then proceed with notification.

A second opportunity for shared effort is providing a national—or perhaps international—resource center for users that encompasses some or all of the free offerings described in the previous section. As an organization that currently serves as a free resource for website owners, StopBadware provides some of the services we have described and is continually working to add more. As a result, a wide variety of companies from behemoths like Google to small Web hosting providers direct customers to our sites for assistance. This, in turn, allows us and our volunteer community to continue learning and improving our resources to help more people in the future. There are economies of scale in building such a resource centrally, rather than each ISP developing its own equivalent. For smaller ISPs and those that don't desire to be in the malware remediation business, directing customers to such a resource is likely to be an appealing option. This could be made even more appealing through cobranding arrangements that create a seamless user experience for customers. If users can be made broadly aware that such a resource exists, it would also help ensure that every user, regardless of provider, has access to a baseline set of information s/he needs to facilitate remediation and prevention.

The third area of need that can be addressed collaboratively is the sharing of information and knowledge about botnets: the extent of the problem, strategies for addressing it, effectiveness of existing efforts, and new threats. Two of the biggest challenges that now face the ecosystem in addressing botnets and other malware is a lack of good data and limited knowledge sharing across organizations. By aggregating data from ISPs and other sources, and by engaging industry players in ongoing conversations, the entire industry would be better able to prioritize and improve its efforts to fight botnets.

These three opportunities need not each be done separately. Indeed, in the Web context, StopBadware serves several of the functions described. Our working groups and partnership channel facilitate ongoing discussion among experts from multiple industry and public service organizations. We publicly release aggregated data and report on trends in website-related malware. We offer educational content and a volunteer-driven online community to assist website owners with remediation and prevention, as well as an independent review process to facilitate removal of websites from blacklists. And we are in the early stages of developing a system for aggregating reports of malicious URLs and reporting them to the relevant site owners and Web hosting providers. Each of these functions supports the others; for

[10] See http://googleblog.blogspot.com/2011/07/using-data-to-protect-people-from.html

[11] http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317

example, what we learn while educating webmasters can be passed along in our conversations with industry experts to help them better serve their customers.

Whether together or separate, we believe independent non-profit organizations are best suited to building these collaborative solutions. Public charities offer consumers the assurance that services are in the consumers' own interests. Multi-stakeholder organizations offer industry players influence and benefits without concern of government regulation or competing interests. And non-profit organizations can fund their work through a combination of government support, corporate contributions, philanthropy, and fee-based services.

StopBadware is pleased to see momentum towards addressing botnet notification, mitigation, and remediation on a cooperative, systematic basis. Combined with other efforts, including our own and those of several other multi-stakeholder groups, we believe this country and the Internet community more broadly are on a path to substantively reducing the threat of bots and other malware.