Comments by National Cyber Security Alliance on:
Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware

Submitted by: Michael Kaiser, Executive Director, National Cyber Security Alliance
michael@stayfafeonine.org
202-570-7430

A. General Questions on Practices To Help Prevent and Mitigate Botnet Infections

(2) What preventative measures are most effective in stopping botnet infections before they happen?

Prevention falls into two categories: technology and behavior.

Technology: Today the best prevention measures from the consumer side is to ensure the use of basic primary protections. To be effective ideally, every computer connected to the Internet would have basic protections—current and modern operating systems and browsers as well as a suite of automatically updating security software—in place. While there will be a lag between everyone running the latest and greatest software for a myriad of reasons—speed of technological change, cost to individuals and businesses, the general cycle of adoption of new software—it is critical that that computer users are reminded to keep their computers defended. We have seen improvements over time such as widespread deployment of software that updates automatically with out have to turn the feature on. However, we can expect that at least in the short term there will be no silver bullet to prevent infections or a sudden decrease in the cybercriminals and others attempting to develop botnets.

Prevention can also be achieved by coordination of activities of service providers participating botnet reduction efforts. By organizing a partnership among service providers, greater information sharing could take place including information about bots (possibly including law enforcement), consumer responses to notification and remediation efforts and bets practices. By creating a partnership that includes government as well, it might be possible to speed up the adoption of new ideas and techniques to prevent botnets.

Behavior: In the STOP. THINK. CONNECT. campaign, one of the tips we was created was “keep a clean machine” to encourage users to be sure their system is ready to

connect to the Internet. The notion of a clean machine is the need to keep your system prepared to use the Internet more safely and securely.

Infections of machines can occur in a variety of ways and threats are likely to evolve so continued pubic education about safe surfing, the use of USB devices, phishing and spear phishing—need to be continuous. Specific threats may also exist. Foe example, currently, Small Businesses have been a target of opportunity or cybercriminals. While spear phishing is the

There should also be increased education around bots, botnets and malware in general. Computer users don't need to be technology experts. However, if notification and mitigation schemes are going to be successful, computer users have to have some basic understanding of the risks so they will be responsive when they are notified of a problem. NCSA research in the development of the STOP. THINK CONNECT. campaign indicated that computer users make the connection about what they do to protect their machines also protects others. Botnets are clearly an area where the health of an individual machine impacts others and education efforts should include those themes. Therefore, education efforts should not only focus on threats but include the need for computer users to rid systems of malware, the methods by which it can be removed from a system and how the positive outcomes for those beyond the individual user.

(3) Are there benefits to developing and standardizing these practices for companies and consumers through some kind of code of conduct or otherwise?

NCSA believes that standardizing practices is extremely important. This doesn't mean that everything that every company has to be done the same way. It means that companies should follow a similar set of steps in notification and remediation (assume that companies may use different ways of identifying). This important for a few reasons:

- Internet connections are not stagnant. While many people might have a primary Internet connection at a home of office, many users are mobile and may use a variety of ISP's. By having some standardization it will help consumers who may not be aware of which ISP they are actually using to connect to the Internet.
- By standardizing some practices, it will make it easier for consumers who do get infected to learn what to do to remediate the problem.
- Notifications methods should also be standardized to some extent. We need to be aware that notifications could become a way that cybercriminals social engineer people as they have with "scareware" and phishing. Coming up with

a verifiable way for consumers to know that notifications are legitimate is critical.

- Standardization would also create mechanisms making it easier for others to join the effort. Since botnets are a global issue and many of the companies that will engage in the fight against them are global by creating mechanisms that can be shared the global fight against botnets could be accelerated.

(4) Please identify existing practices that could be implemented more broadly to help prevent and mitigate botnet infections.

The continued investments of government and industry in the harmonized messaging effort of STOP. THINK. CONNECT. can be built upon. In developing STOP.THINK. CONNECT., Industry and government worked in collaboration to address cybersecurity education and awareness. Using STOP. THINK. CONNECT. and engaging stakeholders to conduct a special campaign around botnets and keeping a clean machine. STOP. THINK. CONNECT. could be come the harmonizing message for the botnet reduction effort. The message was created by 25 companies and 7 Federal agencies, many of the companies involved would also be critical to the botnet reduction effort and includes ISP's security software providers, financial services and ecommerce. STOP. THINK. CONNECT. was designated the national education and awareness message by President Obama in October of 2010.

The STOP. Think. CONNECT. effort is a true public private partnership. This issue has the similar characteristics that could lead to a public private partnership including: botnets are a shared problem, no one entity can resolve the situation by themselves, cleaning up infected machines benefits a broad spectrum of industry, government as well as the general public.

The potential exists to leverage resources across the public and private sectors toward this messaging effort. In both Germany and Japan the government invested in public education campaigns in conjunction with botnet remediation efforts. Those centralized investments were critical to their success.

(7) 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?

Yes, proactive notification of botnet infection should, over time, become routine for all computer users. Because the malware that infects machine may not always be apparent to the computer user, if a trusted third party becomes aware of an

infection there should be a process in place to notify consumers, provide information about remediation and as appropriate remediation services.

Hopefully, through continuous education and successful remediation, consumers will come to understand that infections are possible and that notification, from a variety of sources is likely, is a helpful tool to enhancing their safety and security and the safety and security or others and that responsible computer use includes timely remediation of the issue. Ideally, it would become institutionalized and computer users would expect to be notified by an ISP or other trusted service providers if their computer is infected and be prepared o act quickly to protect themselves and others.

If so, how could support services be made available?

Notification should always come with pathways to remediation. Just telling computer users that their system is infected is not adequate. Any notification of infection should come with information (or links to information) on support services. There should be some flexibility in how services are made available. Companies invest significant resources in developing relationships with customers that they should be able to use to make services available in a way that their customers would expect. That said, consumers should be offered more than one-way to get help. There should always be the availability of a no cost option that consumers can pursue to clean up their own system. Just like cars, there will be some people that fix their own cars, some that always use a mechanic and some that know how to fix them and sometimes do it on their own and sometimes use a mechanic. We can expect that same to be true of consumers notified the have infected machine. Empowering consumers with choices is in general a good practice.

In addition, there may be companies participating in notifications such as smaller ISP's or ecommerce sites that don't have the customer service staff or capabilities of providing in-house assistance to computer users. Any system developed that anticipates the participation of these entities should provide options for having some of the functions provided by third parties. Some flexibility should also be provided to allow for partnerships between companies. Many ISP's, for example, already have established relationships with AV and security providers and may choose to engage them or other partners in helping with all aspects of the program from notification through remediation. This should be allowed as along as there is agreed upon standards for courses of actions and the goals of the effort can be met.

One of the key questions is whether or not there should be one entity where very consumer with an infected machine gets referred. This is an idea worthy of additional

discussion. This appears to be an effective model in Japan and Germany. Such a model may be appropriate for the United States. However, that decision should be made in consultation with industry and nonprofits. If a decision to go that route is made, it would probably be a collaborative effort between industry, nonprofits and government with industry and government providing the resources to execute the effort. There would have to be agreement about the scope of the entity ad whether or not it would engage in direct remediation for customers. In Germany, they found that only a small number of people actually called for direct assistance and most people were able to resolve the situation through information on the website and the cleaning tool they offered. It is hard to know with some testing if that would be true in the United States. Since the United States is roughly 4 times the size of Germany, this would need to be a well-funded resource.

(9) Describe scalable measures parties have taken against botnets. Which scalable measures have the most impact in combating botnets? What evidence is available or necessary to measure the impact against botnets? What are the challenges of undertaking such measures?

Germany, Japan and Australia have all engaged in scalable efforts to address the botnet issue. They have all used the basic strategies of identification, notification and remediation. Their models have some similarities, such as both Japan and Germany use notification by traditional mail which has been effective for their citizens, although would need testing in the United States. . All have a major focus as ISP's as the primary identifier of infection. Japan and Germany have invested public/government funds in education efforts and provide websites with remediation tools. Australia has a voluntary model that provides a framework and options for ISPs to participate.

The issue of measuring the impact will require coordination among participants in the effort. It is expected that initially, measurement will come in the form of raw numbers about the numbers of machines identified, notifications made and machines cleaned or remediated. As time goes on the effort becomes more routinized and botnet creators modify their ways (perhaps going from mass infections to targeted infections of more malicious software variants), new measures of success will have to be developed. Measuring consumer awareness should also be considered. If prevention is one of the key goals then measuring computer user efforts to prevent infections should also be included. NCSA, for example, has conducted home user and Small business studies for many years that look at security behaviors and certain kinds of risks that could lead to infections. Many companies also undertake surveys of users. In response to the botnet issue it might be a good idea to coordinate, If possible, at least some of these efforts to develop some standard measures.

B. Effective Practices for Identifying Botnets

(12) 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 (such as operating system vendors, search engines, security software vendors, *etc.*) can participate in anti-botnet related efforts. Should voluntary efforts focus only on ISPs?

Voluntary efforts should not focus solely on ISP's for several reasons. First and foremost, protecting the Internet is a shared responsibility and does not and should not fall solely on one player in the ecosystem. By building on the rusted relationships computer users have with a variety of players online, it increases the likelihood that consumers will respond to notices and expand options for remediation.

Furthermore, many parties might be in a position to identify infected machines and have the trusted relationship with consumers to encourage and help them clean up their machines. NCSA's understanding is that at least some of the data about infected machines and some of the techniques for identifying infected machines, is available from third parties beyond ISP's. That being the case, it opens up the door to more widespread participation in the effort.

While ISP's are clearly well situated to identify infected machines because the provide a gateway to the Internet, others such as search providers, financial institutions, ecommerce sites, AV and security providers, OS providers and others may also be in a good position to identify, notify and remediate as well. This will be especially true if consumers get infected while using an ISP other than their primary connection. For example, if a computer user got infected while traveling and was notified by an ISP they didn't recognize, they might not act or think it was a scam (although some kind of standardized notifications might help in these cases). However, if during the trip they also tried to conduct a bank transaction and were notified as well they may be more likely to act.

Additionally, consumers may see other entities as primarily responsible for helping with these kinds of issues other than then their ISP. NCSA research continuously shows consumers turn first to AV and Security software as a primary source of information Certainly AV and security software providers are well positioned to alert computer users about risks and problems. It is critical that that there be a network of potential industry participants that are trusted by computer users. This will allow computer users who may be suspicious of a specific notification to verify the condition of their machines with providers of their choice and have multiple choices

to remediate if they so choose. In addition and equally important, in our more mobile world computer users may not always be tied down to one ISP. For example, someone who travels frequently and uses local Internet connections could be connecting to multiple ISP's over a period time probably without knowledge of what ISP they are actually using.

One other option would be to consider a separate body—some form of partnership between industry and government—that actually identifies infected computers and then shares that information with participating parties that then go on and notify computer users.

C. Reviewing Effectiveness of Consumer Notification

(13) What baselines are available to understand the spread and negative impact of botnets and related malware? How can it be determined if practices to curb botnet infections are making a difference?

Measuring results will be critical including numbers of infected machines, numbers that are remediated and reinfection rates. Baselines should be collected prior to the inception of the program and should include the best possible estimate of infected machines and a clear understanding of the trajectory of success in other countries. In addition, consumer surveys about knowledge of botnets and their attitudes toward various components of the effort should be collected and tracked over time. This will be essential if the effort includes a significant public education component.

Other areas where data could be helpful for planning and review purposes include: the length of time between notification and remediation, how many notifications are required until remediation takes place, re-infection rates, the aggregate numbers of notifications and remediation and the number of botnets operating worldwide.

(14) What means of notification would be most effective from an end-user perspective?

End user notifications will have to take various forms depending on the entity that notifies the user. Multiple notifications from varied service providers will give consumers a valuable second opinion from another trusted source that computer is infected. Wherever possible, notification should be within a system already and known and trusted by the user whether that's a notice from an ISP, an alert from an AV or security firm or notice directly from an online service provider (search, commerce, etc.). The provisions and methods of providing notice are an excellent

opportunity for Industry and government to work together. Notice is one area that could be exploited by bad actors to get computer users to click on links to other infected sites, purchase bogus AV products, harvest personnel information or steal credentials.

Notice should be done in a way that computer users can easily verify the legitimacy of the notice before taking action. That will require coordination between all entities participating in botnet reduction efforts. More than likely there will be need to multiple ways to notify computer users. For example, not all ISPs will have email addresses of all their customers. Other kinds of notifications, such as browser warning or dialogue boxes might also be appropriate in some circumstances, although it is well documents that computer users click through security warnings. Therefore, there may not be one type of notification that is useable by every company or organization participating in the effort.

The importance of notifications cannot be over estimated. Proper notifications that instigate action by computer users is critical for success. A well-developed effort would tests several different notice schemes and track computer users responses. Over time, it maybe possible to tailor notification to specific circumstances so computer users are more likely to take action.

(15) Should notices, and/or the process by which they are delivered, be standardized? If so, by whom? Will this assist in ensuring end-user trust of the notification? Will it prevent fraudulent notifications?

Whether notices are standardized are not is not as important as providing computer users to ways to verify the legitimacy of the notice. It can be expected that bad actors will use whatever form of notice used to try and lure users into revealing private information or as a way of distributing malware. Therefore, all companies and organizations that participate in efforts to eliminate infected machines should work together to come up with some form(s) of verifiable notice and educate computer users about how to distinguish legitimate notices. Some service providers may have existing ways that they communicate with customers that could be used for this effort, such as messaging systems built into their platforms or providing specific account information. These efforts should be evaluated to see if they would be appropriate for this effort. Various websites, or a specially designated website should be available so consumers can check the form of notification used by various providers.

(16) 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?

There will have to be cost and no cost and no cost options for remediating infections. Some people will be ready, wiling and able with clear instructions to clean their machines. Others will choose to pay or feel that they don't have the capability to fix the situation on their own. In terms of pricing, NCSA would hope that the market would be dynamic enough and offer consumers choice and keep prices to a minimum. Germany has found that their service, a free cleaning tool, has been effective. It could well work in the United States as well. Testing of the response rate, re-infection rates and speed of consumer response for all methods should be tracked to see which ones work best.

Computer users cannot be viewed as single group. They are diverse in their technical abilities, financial wherewithal, and time availability to address computer issues. If we expect them to respond to notices and follow through, we have to have options that meet there needs. Recently, the FCC and major ISPs and technology companies have been making low cost high speed broadband available to low-income families. Botnet remediation services should include a low cost/no cost option for those participating in these programs.

(17) What impact would a consumer resource center, such as one of those described above, have on value-added security services? Could offers for value-added services be included in a notification? If not, why not? If so, why and how? Also, how can fraudulent offers be prevented in this context?

It is hard for NCSA to gauge exactly the impact on value added services that might be offered by other if there was a more public option. One assumption is that many computer users would want to use companies, if they so chose to pay for remediation, that they already have a relationship with. Established relationships of trust are certainly part of consumer decision making in choosing a vendor for a service. Since we don't at this time know if there would be a great price differential between a centrally provided service or a vendor provided service, it hard to predict if price would be a determining factor.

(18) 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?

While we wouldn't recommend a mandatory quarantining or walled gardening at the early stages of this effort, providing companies and organizations involved in identifying and notifying users of infections the option of denying service until the infection is resolved should be made available. These options should have extremely clear rules and guidelines and users should receive clear notices of the possibility of having services denied in each of many notices.

Interestingly, if services other than ISPs participate in the program they may be able to deny access to their specific site rather than participate in any quarantining activities. Even in these cases, service providers need have a policy of escalation. Over time as efforts to eliminate botnets become better understood and more of a part of everyday computer use, it may be more commonplace to quarantine or deny service to infected machines. Ideally, a public private partnership of government, industry and nonprofits would work together to help steer these efforts.

Best Practices for Consumer Notification

(20) Countries such as Japan, Germany, and Australia have developed various best practices, codes of conduct, and mitigation techniques to help consumers. Have these efforts been effective? What lessons can be learned from these and related efforts?

(21) Are there best practices in place, or proposed practices, to measure the effectiveness of notice and educational messages to consumers on botnet infection and remediation?

D. Incentives To Promote Voluntary Action To Notify Consumers

(25) Of the consumer resource scenarios described above, which would be most effective at providing incentives for entities to participate? Are there other reasons to consider one of these approaches over the others?

NCSA believes that a public private partnership is the best approach in this case. Robust participation of industry, governments and nonprofits is the best way to ensure that all infected computers are identified, users are notified and remediation takes place. That doesn't mean that there would not or could not be role differentials within the partnership. For example, it might be most appropriate for a nonprofit or government (or a partnership between the two) to lead the public

education efforts. ISPs and other service providers might be best to lead more operational efforts. However, they could all work together under a partnership that had information sharing and joint decision making.

(26) If a private sector approach were taken, would a new entity be necessary to run this project? Who should take leadership roles? Are the positive incentives involved (cost savings, revenue opportunity, *etc.*) great enough to persuade organizations to opt into this model?

A new entity would not necessarily be required if there was an entity that exists that all potential participants trust.

(27) If a public/private partnership approach were taken, what would be an appropriate governance model? What stakeholders should be active participants in such a voluntary program? What government agencies should participate? How could government agencies best contribute resources in such a partnership?

In a true public private partnership governance initially be by all members. For STOP. THINK. CONNECT. during the first year all decisions were made by consensus. This was critical because organizations of different sizes and resources shared the table. As time went on, participants self-selected into sub-groups that took on various aspects of the work. These groups brought decisions back to the committee of the whole. We would recommend that the group operate in this fashion until such time as all fundamental decisions are made and basic operations are in place.

Stakeholders should include any company actively interested in joining the effort to eliminate botnets. Initially, that would most likely include ISPs, AV companies, ecommerce providers and financial institutions and service providers and key nonprofits in the space. It could grow to include others and key to helping implement the effort. The partnership should be open to any government agency interested in addressing the issue. However, Department of Commerce and DHS would be critical. We could envision other citizen facing agencies participating as well.

NCSA would be willing to consider participation in the formation of such a public private partnership.

(28) If a government-run approach were taken, what government agencies should play leading roles?

While government could be a participant in the effort including notifying users if the attempt to access government networks with infected machines, it is not recommended that it solely be a government program. If it were to be a government led effort the best agency would likely be one that citizens perceive as neutral such as the Department of Commerce or the FTC.

There will always be a segment of the population that does not trust government. Since reaching all infected machines is important, a solely government programs is probably impractical. That does not mean government could not lead in aspects of the effort.