27 September 2011
Promia Incorporated
CCR registered DUNS 835050907 CAGE 1KTA6

Promia Comments to Federal Register Notice Citation 76 FR 58466, Docket No. 110829543-1541-01

Summary - The U.S. Department of Commerce and U.S. Department of Homeland Security are requesting information on the requirements of, and possible approaches to creating, a voluntary industry code of conduct to address the detection, notification and mitigation of botnets. Over the past several years, botnets have increasingly put computer owners at risk. A botnet infection can lead to the monitoring of a consumer's personal information and communication, and exploitation of that consumer's computing power and Internet access. Networks of these compromised computers are often used to disseminate spam, to store and transfer illegal content, and to attack the servers of government and private entities with massive, distributed denial of service attacks. The Departments seek public comment from all Internet stakeholders, including the commercial, academic, and civil society sectors, on potential models for detection, notification, prevention, and mitigation of botnets' illicit use of computer equipment.

Questions:

(1) What existing practices are most effective in helping to identify and mitigate botnet infections? Where have these practices been effective? Please provide specific details as to why or why not.

For detection of botnets using standard protocols, signatures are able to be seen globally by SRI Bothunter, Promia Raven and many other IDS signature detection tools. In the case of the Promia Raven product used globally in every Navy Fleet Network Operation Center, the addresses of the devices identified can be added to the common repository. The common repository of block list addresses (with ports) can include government, commercial and malware-specific (such as Zeu$) infected device lists.

For detection of botnets using unknown communications protocols, analytic work using tools like Promia Analytic Tools Units and Promia Analytic Storage Units, also developed for use in global Navy networks, can be used.

To mitigate and protect home consumers from keylogging botnets workstation blocking tools such as "Norton 2010" from Symantec or "Promia Workstation Blocker" periodically access secure servers then download new IP/port combinations for blocking access/egress to and from consumer's workstations.

To mitigate and protect corporate or government agency networks a number of IPS tools from many vendors provide blocking capabilities. Promia has the Raven family of interconnected devices for asset monitoring and management, security event management and active blocking at IP, port, URL, proxy and signature levels. These tools are used in banks, energy companies and government / military installations.

Tools such as these can be integrated to use common lists from the ISP-based DHS systems to coordinate a grid of network, server and consumer protection into a fabric of anti-botnet devices. Every protected machine, even if it already infected, is blocked from joining an adversary botnet.

The new Cyber Security Evaluation Tool from NIST promises to be an effective tool to provide awareness and help consumers with best security practices. We have just downloaded it and are now evaluating it.

(2) What preventative measures are most effective in stopping botnet infections before they happen? Where have these practices been effective? Please provide specific details as to why or why not.

Configuration management policy and enforcement such as BMC Blade Logic Server Automation tools provide assurance that all devices are kept to a proper baseline as approved by the organization IT and NetOps groups. BMC network operations products are used in DISA as well as many US intelligence agency facilities.

If proactive blocking is in place at the ISP, corporate, employee and consumer workstations, and personnel are trained and vigilant, and if proactive baseline scanning is in place the incidence of infection is greatly reduced.

We suggest more emphasis be placed on proactive hidden protocol identification through regular periodic analysis of large sample sets of live data searching to indications and warnings. When this has been applied in Navy networks over the past ten years there has always been an increase of the situational awareness of the exploits in the network traffic, and whether associated attacks were successful.

The new Cyber Security Evaluation Tool from NIST promises to be an effective tool to provide awareness and help consumers with best security practices. We have just downloaded it and are now evaluating it.

(3) Are there benefits to developing and standardizing these practices for companies and consumers through some kind of code of conduct or otherwise? If so, why and how? If not, why not?

There are many obvious benefits, and these can be reduced into hard dollar savings. In reality companies and consumers are very hesitant to define and enforce policies necessary for these practices, and they are also very hesitant to spend the money to implement, operate and maintain them.

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

Extend Einstein to coordinate and share common blocking lists to corporate system, third party vendor tools and consumer blocking tools. Provide a mechanism to give feedback from the blocking devices back to the list manager when unauthorized network connections are attempted and blocked. Provide a mechanism to allow address owners the capability of correcting wrong block list entries, or entries that have subsequently been cleaned up. Provide a penalty (disconnection?) for consumers who allow their home machines to operate in an unblocked infected state.

The new Cyber Security Evaluation Tool from NIST promises to be an effective tool to provide awareness and help consumers with best security practices. We have just downloaded it and are now evaluating it.

(5) What existing mechanisms could be effective in sharing information about botnets that would help prevent, detect, and mitigate botnet infections?

There is much information updated daily on the Internet with respect to each specific type of known botnet, IP addresses of infected servers for net sysadmins or consumers to use either in routers or IPS systems or other blocking tools. There are many commercial and government tools available for this work. There are hundreds of entries on the Internet for each of these main categories. What is needed here is organization, policy, development and execution of an operational plan to coordinate this information.

(6) What new and existing data can ISPs and other network defense players share to improve botnet mitigation and situational awareness? What are the roadblocks to sharing this data?

SRI International and Promia, together with the members of Cyber-Threat Assessment (www.cyber-ta.org) project team, produced a solution called the "anonymizer" whose sole purpose was to allow shielding of cyber reported information from different stakeholders on a field-by-field basis. Consideration was included to enable the reporters to keep their own identify private while reporting, and selectively disallow certain fields in cyber data to keep customer and employee data safe. The project was completed a few years ago.

(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? If so, how could support services be made available? If not, why not?

Any consumer computing device should be disallowed general access until it can be shown to be clean of infectious malware. They could be allowed hardened access to a site that assists consumers in the job of clearing the problem, whether online, offline or in person. Any machine that has a workstation blocker, whether infected or not, is disallowed access to any known malware server or adversary botnet server.

(8) 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?

All of the above services could and should be available in order to keep the system from infecting others or participating in large scale unauthorized network behavior.

(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?

The Promia Raven global grid of hierarchically connected ISP appliances was designed to protect all DoD networks against botnet attacks. For larger networks the Global Environment for Network Innovations (GENI) is a unique virtual laboratory for at-scale networking experimentation funded by the National Science Foundation with participations by BBN networks and many Universities.

B. Effective Practices for Identifying Botnets

(10) When identifying botnets, how can those engaged in voluntary efforts use methods, processes and tools that maintain the privacy of consumers' personally identifiable information?

Unless people trust each other to a large degree, some money will need to be spent to build a facility that contains the tools (such as SRI anonymizer) to enable privacy with information sharing.

(11) How can organizations best avoid "false positives" in the detection of botnets (i.e., detection of behavior that seems to be a botnet or malware-related, but is not)?

This cannot be answered simply in the context of this discussion. Many companies have spent many years building systems that perform this and other similar functions. These tools are constantly being updated to be more efficient.

(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? If not, why not? If so, why and who else should participate in this role?

The system has to include protection at the ISP, consumer workstation, telecommunications (landline, wireless 802.11, LTE, GSM, CDMA, and Broadband) and corporate server groups. ISPs cannot do the job completely. Local intranets networks, wireless and other large scale nets can pass viruses with no ISP intervention.

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?

A feedback loop from blocking devices, together with regional and local listening devices, can work together to provide effectiveness metrics.

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

A block to their access (temporary or permanent depending on first or second offense etc.), together with a message on their screen and/or an email notification would be effective. Proof of scan of the computer could be used as consumer argument they have a clean system. For repeat offenders either long term blocking or monetary penalty could be effective.

(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

If the ISP is blocking access to all networks then the ISP notification (non-standard) should be enough.

(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

These are being offered today over the internet and from large vendors from many companies. Consumers prefer solutions that work well, work easily and cost less than $39 per year.

(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

Certainly they could and should. Notification from ISPs such as Comcast and ATT provide this already.

(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

A block to their access (temporary or permanent depending on first or second offense etc.), together with a message on their screen and/or an email notification would be effective. Permission to do this should be in the initial end user agreement. Proof of scan of the computer could be used as consumer argument they have a clean system. For repeat offenders either long term blocking or monetary penalty could be effective.

(19) Are private entities declining to act to prevent or mitigate botnets because of concerns that, for example, they may be liable to customers who are not notified? If so, how can those concerns be addressed

We have not seen this in the field.

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

From our review the Australian model has worked well for all stakeholders overall.

(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

We do not know of any best or proposed practices for measuring this effectiveness.

D. Incentives To Promote Voluntary Action To Notify Consumers

(22) Should companies have liability protections for notifying consumers that their devices have been infected by botnets? If so, why and what protections would be most effective in incentivizing notification? If not, why not? Are there other liability issues that should be examined

Yes companies should have liability protection for notifying consumers their devices have been infected. The ability to notify them and the permission to block traffic from infected machines should be explained in their initial terms of use agreement. This protects the entire community. There are laws protecting drivers from other drivers who drive unsafe vehicles.

(23) What is the state-of-practice with respect to helping end-users clean up their devices after a botnet infection? Are the approaches effective, or do end-users quickly get re-infected

Depending on the infection, the state of practice is to scan it with virus or malware scanning tools. This may require taking the system off line for the scan and remediation. Based upon the finding the removal may be simple (fixed by Microsoft Malicious Code Removal Tool, or Norton Antivirus, etc) or more complex (registry editing, or even require reinstall of all systems back from checkpoint or fresh bare metal OS and systems reinstallation. If the consumer or customer does not provide industry-standard levels of protection it is likely they will be re-infected again soon. New systems under design use memory in a way that portions of the system software are constantly refreshed from persistent storage thereby minimizing vulnerability to many types of attacks.

(24) What agreements with end-users may need modification to support a voluntary code of conduct

Unknown

(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

Consumers want solutions that work easily, provide protection, work well and cost little, generally under $39 per year.

(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

Based upon the past we believe the best entity for doing this would be a public-private partnership and this would have to be funded from modest consumer and commercial fees.

(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

DHS should participate as the policy management partner. Representatives from ISPs, telecommunications groups, Internet vendors and standards groups (e.g. BITS from banking, etc) should form a steering committee.

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

DHS should participate as the policy management partner.

The new Cyber Security Evaluation Tool from NIST promises to be an effective tool to provide awareness and help consumers with best security practices. We have just downloaded it and are now evaluating it.

(29) Are there other approaches aside from the three scenarios suggested above that could be used to create a consumer resource and to incentivize detection, notification, and mitigation of botnets

The public/private partnership would join consumer, commercial and government involvement.

(30) Are there other positive incentives that do not involve creation of an organized consumer resource that could encourage voluntary market-based action in detection, notification, and mitigation of botnets?

Continue with the current model and provide financial grant and tax incentives for further involvement.