Response to 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

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Mountain View, California, Symantec has operations in more than 40 countries. As a provider of protection tools against botnet infections, we have international experience in anti-botnet initiatives, and we welcome the opportunity to submit a response to the joint request for information of the Department of Commerce and the Department of Homeland Security on "Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware." As a key security provider who undoubtedly would play a role in such models, we focus our comments on issues within our own remit. For consistency, some questions are answered in groups rather than one-by-one.

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

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

The identification and mitigation of a bot infected machine is essentially a matter of detecting and deleting malicious code. The best practice is the use of dedicated security software. There are solutions specifically geared towards addressing bot infections, and others have the more general purpose of ridding machines from all kinds of malware. Both may be equally effective, but results depend on the individual user's willingness and ability to use these tools. Existing assistance practices include:

- Awareness raising to encourage users to check their systems for possible infections;
- Bot detection at the edge of a legitimate third party network (internet access provider, content provider, communications service provider, etc.) and warning communication by third party;
- Guidance and support to those who, though aware of an infection, cannot address it on their own;
- Provision of cleaning tools to disseminate the actual technology needed to fix an infection.

However, all these best practices find their counterparts in the "worst practices" developed by cyber criminals to further propagate cyber threats: awareness raising websites covertly conveying malware, fake infection warnings and guidance to lure users to compromised websites, provision of malicious software masquerading as legitimate security tools[1]. As such, using best practices requires great care to avoid their misuse for malicious purposes through various means as will be explained later on.

It should also be noted that operations like the notable takedown of the Rustock botnet [2] earlier in 2011 address the command and control centers of botnets, and not the infections on the individual machines. If a new command and control infrastructure is able to identify, connect to and resume the malicious exploitation of infected machines, the botnet once taken down could be back online again.

Bot infections may propagate through any channels used to distribute malware. Possible avenues include: spam, drive-by downloads, targeted attacks, denial-of-service attacks, web site scrapers, SMS messages, and injection through existing backdoors. Therefore, comprehensive security is needed to best protect individual devices from getting infected. Depending on the type and breadth of the infrastructure considered (from individual households to large organizations), this should involve, among others:

- rigorous discipline in patching systems as soon as security updates are made available;
- use of antivirus protection to identify and block malware seeking to infiltrate a machine whether from the network (mobile messaging, websites, remote servers) or from – even offline – devices (e.g. thumb-drives, cameras, cell phones);
- traffic monitoring solutions (e.g. parental control and similar) to block connections to websites known to harbor or suspected of harboring malicious or otherwise undesirable content, or having certain suspicious features (e.g. lack of encryption, invalid or missing certificate, etc.);
- firewall protection to block unauthorized up and down traffic;
- spam filtering to block unwanted mass messages (email, mobile, etc.);
- additional mail and web security to counter more individualized threats;
- strong authentication both of persons (administrators and users) and devices (e.g., laptops, smart phones, tablets) allowed to access systems or networks, to prevent unauthorized third parties from interfering, and authorized insiders from abusing processes or technologies;

[1] Additional detail is available on these matters in Symantec's report on rogue security software: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_WP_20016952.en-us.pdf

[2] http://www.computerworld.com/s/article/9214759/With_Rustock_a_new_twist_on_fighting_Internet_crime

- as well as backup and recovery solutions to remediate infections that may nevertheless happen.

Such solutions are available in various forms and should be deployed at various levels (e.g., endpoint, server, gateway, network, cloud) to provide an end-to-end security solution. Consumers, enterprises and network service providers should preserve the measures applicable to them in security policies that are regularly updated, checked for relevance and effectively enforced. Meanwhile, promoting these practices with the public at large is also essential. All possible means to raise awareness and foster responsible protection by consumers and organizations alike should be explored. However, any codification of practices can only address some aspects of the issue.

It can help to explain and recommend the processes that individuals and organizations need to implement to secure their infrastructures as comprehensively as possible. However, no particular technological solutions should be mandated. A longstanding feature of the cyber threat landscape has been the fast emergence of new techniques and methods of malware propagation that allow cybercriminals to keep their edge. A good example is the evolution from malware distribution through mass mailing (spam) to more sophisticated targeted attacks, often leveraging social engineering. These attacks could be emails with sender identities faked to look trustworthy, subject lines forged to appear relevant, and attachments or embedded hyperlinks customized to look legitimate and avoid malware detection. While possibly pursuing the same objective as spam (e.g. to distribute bot infections), these attacks are not only likely to reach their target more effectively, but also have a high level of uniqueness that makes them virtually undetectable by filters geared towards mass mailing only. Therefore it is very important that security practices care able to keep evolving as the threat landscape changes.

Moreover, security is about processes, technologies, and people. The human factor will remain essential and cannot be codified: many infections originate in an individual user's behavior, whether it is by omission (e.g., failure to comply with processes such as delay in patching, forgetfulness in using encryption or locking down machines when not in use) or by action (e.g., inadvertent or malicious use of technology, such as connecting a device, opening a file or clicking on a hyperlink). Looking at the human threats in the cyber landscape, three types can be identified that are relevant to this discussion:

- Well-meaning insiders, who make mistakes: they are best addressed through training and awareness raising about the proper use of technology and the observance of policies and processes, but there is no guarantee that errors will not still happen.

- Malicious insiders, who willfully abuse processes and misuse technology: segregation of duties, authentication and access control can help mitigate risks, but will not eradicate malicious intent.

- Cyber-criminals, whose purpose is to defeat security policies that are in place: these are professionals in finding weakest links and exploiting vulnerabilities; thus, any codification of practices should make sure that it neither creates single points of failure, nor hints at how the codified protection processes may be circumvented or exploited.

There are certainly benefits to streamlining protection processes and security measures to prevent bot infections, mostly in terms of raising awareness and providing guidance on do's and don'ts. Additionally, in a code of conduct model, the more organizations and individuals who adhere to such a code, the higher the level of protection may become. On the other hand, should the code be flawed by inherent vulnerabilities (e.g., too rigid to allow adaptation to emerging threats) or induce vulnerabilities (e.g., failure to address a particular threat vector), it could also end up increasing every signatory's exposure to those particular threats. Therefore, while the development of a code of conduct is welcome, it should neither be exclusive of other initiatives, nor mandatory. Moreover, it should never be suggested that security is achieved by adhering and complying to a code. While helpful as a baseline for protection, a code should neither be a compliance framework, nor create a false sense of security.

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

The cybersecurity community, comprised of security vendors such as Symantec, and also many other stakeholders such as CERTs, law enforcement agencies, standards organizations, national or regional anti-botnet initiatives, hardware manufacturers, software developers, technology users and research labs, routinely shares information on malicious trends, security incidents, malware outbreaks, new vulnerabilities discovered, etc. This has proven helpful in raising awareness and in speeding up the development and deployment of software updates to patch vulnerabilities, block new malware variants, address infections, and so on. There are currently many information exchange fora and collaboration platforms on malware in general and on botnets in particular. Given the international scale of the issue and the sheer number of stakeholders involved, this variety is not only understandable, but also highly desirable to maintain. Indeed, it allows better distributed and more versatile detection across the global infrastructure than a single mechanism could ever achieve.

What information to share?

Various players collect or generate different types of botnet-related information, some of which may be of commercial or otherwise confidential nature. There are infrastructures whose operators may not wish – or not be able to – share information even on the fact that a botnet infection or attack hit them, let alone any technical details. In such cases, remediation is done confidentially and involves very few stakeholders if any at all. While leveraging the intelligence gathered from such cases to subsequently enhance protection in the public domain would be desirable, even that may not always be possible.

For data that can be shared, several initiatives were developed to standardize malware-related taxonomy[3] and information[4] or incident reporting[5]. These tools are definitely helpful and deserve to be

[3] E.g. the Malware Attribute Enumeration and Characterization Language (MAEC): http://maec.mitre.org/

[4] E.g. the Malware Metadata Exchange Format (MMDEF): http://standards.ieee.org/develop/indconn/icsg/mmdef.html

promoted, but they are not universally used, and they do not by themselves ensure that all parties who should be involved actually share or receive information.

Why share information?

Every legitimate – but also every rogue – stakeholder in the ecosystem is keen on situational awareness, while none of them is eager to disclose their own vulnerabilities or failures. Both the evaluated cost of the average security breach[6] and the magnitude of the damage caused by cybercrime[7] are significant enough to act as true incentives for better cooperation in protecting the infrastructure, but they also make the attribution of responsibility for failures and vulnerabilities more problematic and more sensitive. In order to limit the situational awareness of cybercriminals, and to prevent any form of race between stakeholders to avoid liabilities, information sharing needs to happen in a secure environment and in a climate of confidence and trust.

Where and how to share information?

Given the scale of the problem and the number of players to involve, such a climate cannot emerge expeditiously. Nor can the required secure information exchange infrastructure be set up overnight. Existing and longstanding partnerships, whether sectoral, horizontal, national or international, public and/or private, should certainly be used. Such initiatives, whether botnet-oriented or related to other cyberthreats, have valuable infrastructures, partnerships, experience and best practices. In particular, extensive work has already been done by the Department of Homeland Security and the Sector Coordinating Councils, as identified under HSPD-7 for critical infrastructure protection[8]. Information Sharing and Analysis Centers (ISACs) established for telecommunications[9], information technology[10], or banking and finance[11] sectors are all relevant as operational structures that should be used and enhanced.

---

[5] E.g. IETF's Incident Object Description Exchange Format (IODEF) : http://tools.ietf.org/html/rfc5070

[6] See the Symantec Internet Security Threat Report, Volume XVI, April 2011: http://www.symantec.com/business/threatreport/

[7] See the Norton Cybercrime Report, September 2011: http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/

[8] Homeland Security Presidential Directive 7 on Critical Infrastructure Identification, Prioritization and Protection http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1

[9] Telecom ISAC: http://www.ncs.gov/services.html

[10] IT-ISAC: https://www.it-isac.org/

[11] FS-ISAC: http://www.fsisac.com/

(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?

Measuring botnet activity and associated risks for situational awareness is a complex matter. The European Network and Information Security Agency drew up a fairly comprehensive and detailed description of available techniques and methods[12]. Different players in the marketplace have different metrics of variable accuracy on several aspects, but a comprehensive risk-based picture of the botnet-related threat from the standpoint of the Nation's infrastructure is difficult to draw, especially as not all intelligence may be pooled. The metrics below are only some of the most often discussed ones. Here, they are explored with threat characterization in mind. Some of these metrics will be considered in the perspective of mitigation efficiency measurement later on, under question 13.

Number of bots in a botnet

Often quoted as an indicator of the threat posed by a botnet, the figure in itself is only indicative of the scale of the infection and hence of the effort required to clean the ecosystem, but not of the actual threat. Depending on the objective pursued, smaller botnets with superior capabilities may well cause more damage than larger ones with a lesser potential for disruption. Besides, there is no agreed methodology to generate meaningful botnet size data that could be comparable across regions or over time. The best place to find an accurate metric would be the control and command (C&C) center of the botnet itself, but that is often beyond the reach of investigators. Cybercriminals renting out botnets under their control might disclose data on the size of their net when pricing and advertising their services in the underground marketplace[13], and this information may of course be collected, but it is hard to verify.

Network defense players on the other hand only have a partial view, as perceived through the lens of their own customer base or corporate infrastructure. Botnets generally spread across the networks of several ISPs, and may include zombie machines of various types (e.g., desktops, phones), that run software from various vendors, and are used by individuals whose roles and behaviors in cyberspace differ greatly. Therefore each operator will see a different picture of the same botnet. The picture is even further nuanced by the fact that, legally speaking, a provider of access, hardware, software, service

[12] ENISA, *Botnets: Detection, Measurement, Disinfection & Defence*, http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence

[13] See Symantec's report on the underground economy: http://www.symantec.com/content/en/us/about/media/pdfs/Underground_Econ_Report.pdf
Monetizing botnets as well all manner of attack toolkits has remained a current and growing trend, as shown in the Symantec report on attack toolkits and malicious websites: http://www.symantec.com/content/en/us/enterprise/other_resources/b-symantec_report_on_attack_kits_and_malicious_websites_21169171_WP.en-us.pdf

or content will only be able to detect a bot-infected machine in so far as statutory rules or contractual terms allow it.

For example, users of an enterprise endpoint software may choose to deny any feedback from their machines to the software manufacturer, in which case the latter may not even know if said machines are hit by botnet attacks, or are themselves bot-infected. This is also why, even in the case of a botnet that operates by exploiting a particular vulnerability in one particular product, even the provider of that product is unlikely to have a complete view of the botnet. Some machines may not send any feedback at all and remain invisible to the provider, others may use counterfeit versions of the product and thereby deliberately fall outside any contractual feedback mechanisms.

From the particular perspective of a security vendor such as Symantec, a machine running our solutions should normally be protected from bot infections. Therefore, most of the bot activity we may be able to identify does not originate in our own customer base, but hits the sensors of our Global Intelligence Network[14] from the outside. In that sense, most bots we detect are unknown third parties to us.

Geographic spread of a botnet

While interesting for various types of analysis, this indicator may have little relevance from the standpoint of national infrastructure protection. The fact that a botnet is not entirely located within the national jurisdiction does not mean that it constitutes a lesser threat. Even botnets without a single zombie on the homeland territory can be used to launch attacks into the Nation's infrastructure. Having botnets based mainly or completely abroad only means that domestic players such as ISPs cannot address them, and nor can national law enforcement tackle them without international cooperation.

Second, the geographic location of infected machines depends on many factors. Among others, public networks worldwide have different levels and measures of security in place. Infections can follow the geographic spread of the particular products and vulnerabilities exploited by the botnet. Certain groups of people or organizations may be particularly negligent in patching systems or using security solutions. Certain communities sharing particular practices or technologies such as peer-to-peer networks or social platforms may suffer from outstanding exposure to certain threats.

From a takedown perspective, what is most interesting is to identify the location of the command and control servers operating a botnet. Such servers may be swiftly moved from country to country and are often duplicated in several jurisdictions to achieve resilience by redundancy. Moreover, as explained earlier, taking down the C&C servers does not fix the individual infected machines. And as a matter of fact, the resilience of a botnet's C&C server is often more relevant to the botnet's threat characterization than the geographic distribution of its zombies.

Malware and botnet functionalities

[14] http://us.norton.com/symantec-beyond-box/article

The picture of how a botnet propagates and what real threat it constitutes is further complicated by another set of factors. First, bot infections are not a standalone type of malware. They propagate through various channels including non-internet protocols (e.g., mobile messaging), exploit diverse vulnerabilities in various layers of the logical and physical infrastructure, and often come in combination with many other functionalities embedded in a single piece of malware. A worm or virus that carries a bot infection may also include: a Trojan component and open backdoors to allow remote access, comprise a keystroke logger to intercept user data, conceal other data theft functionalities to steal information, use rootkit and obfuscation techniques to remain undetected, create virtual private networks to encrypt malicious communications, and connect to remote proxy servers to disguise actual locations. Conversely, the same bot infection can also propagate using various pieces of malware. In other words, "bot" itself can be considered as one functionality among many others that can be built into any custom piece of malware.

Second, the bot component itself may have various functionalities, that may change over time. A botnet can be used to distribute spam. Or to launch denial of service attacks. Or to spy on the users of the infected machines and steal their information. Or to transfer data, e.g., other malware infections through or onto the host machines. Or to host malicious sites. Bots can also remain dormant for long periods. Some bots have all these functionalities and many more. New functionalities may be added when the C&C server distributes malware updates to its zombies. In such cases, the threat posed by that particular botnet may be multiplied instantly.

Third, one physical machine can belong to several botnets all at once and have certain functionalities here, other functionalities there. It has been observed in the competition between botnet herders that certain bot infections specifically seek to remove competing infections from the machines they hit[15], but that is not always the case. Moreover, with the development of virtualization, single physical machines can host several virtual machines, each of which may suffer from one or many infections. As a result, threat assessment becomes very complex:

- Determining the capabilities of a particular botnet requires in-depth analysis of the actual malware, using honeypots and sinkholes to capture it, isolated testbeds to observe its behavior, and reverse engineering to uncover all of its features. Experts such as security vendors are able to do that, but it is time and resource intensive.

- Mitigating the infection can be facilitated by identifying the exploits used by the botnet and by patching the corresponding vulnerabilities. Vendors of the products concerned have an interest in doing that, but deploying the patches requires the cooperation of the individual users.

[15] About the "Kill ZeuS" function of the SpyEye malware toolkit, see page 18 of the previously quoted Symantec Report on Attack Kits and Malicious Websites.

Evidence suggests that long since patched vulnerabilities are still exploited years later[16], meaning that patch deployment is not effective.

- Assessing the intensity of botnet activity requires overall traffic monitoring at the level of the network, as well as at the level of individual bots' up and down traffic. It is complicated by the fact that many botnets run simultaneously, some with C&C centers distributed across many servers. This makes it difficult to attribute precise individual shares to particular botnets, whether at network or at machine level. In fact, unless the actual C&C center of a botnet is monitored, its activity can be at best estimated, not measured. Symantec's evidence[17] suggests that the Rustock takedown had a very measureable immediate – albeit temporary – impact on global volumes of spam (a sharp drop of 24.7%), but that kind of *post mortem* information also emphasizes how little we may know in real time about the magnitude of certain threats.

Reputation-based information

With malware attacks becoming more targeted and better customized, security practices need to evolve. Malware distributed massively is noticed hundreds of thousands of times around the globe. Identifying them by their signature (inherent specificities) is an effective method to block them. Our latest findings however indicate that malware polymorphism and variance (the malware's ability to mutate when propagating) have become so widespread that signature-based detection is often defeated.

For example, 166 million unique samples of malicious code were observed in just three months[18], which equates to more than 20 new ones every second. It is simply unrealistic to feed this many signature updates to the antivirus solutions protecting the ecosystem. Moreover, on average, a piece of polymorphic malware will infect 16 or so machines before mutating. So even if signatures could be issued at such a pace, each of them would protect a handful of not yet infected machines at best. Clearly an ineffective model.

How to address this? By reversing the paradigm and using the fact that legitimate code (e.g., software installers, legitimate content files) will occur identically several times without causing any trouble. Such pieces of code will have a high reputation of trustworthiness. This is particularly effective in addressing

[16] A vulnerability discovered in August 2003 and patched in July 2004 was still the second most exploited vulnerability in web based attacks observed in 2009. For more on this, see the Symantec Internet Security Threat Report Volume XV of April 2010: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

[17] http://www.symantec.com/connect/blogs/rustock-takedown-s-effect-global-spam-volume

[18] See Symantec Intelligence Quarterly, April-June 2011: http://www.symantec.com/content/en/us/enterprise/white_papers/b-symc_intelligence_qtrly_apr_to_jun_WP.en-us.pdf

highly customized, tailored attacks where the malware used is rare or unique, and therefore has a low or no reputation. Of course, this fact alone is not enough to justify blocking, as many a legitimate file will also have unique characteristics. Nevertheless, from the standpoint of situational awareness, closer inspection of certain unique files hitting particular points in the network could reveal polymorphic malware outbreaks, or targeted attacks going on against specific infrastructures or organizations.

Aside from files, reputation techniques may also be applied relevantly to other types of information, e.g., network addresses such as IP addresses. For instance, an IP address that is repeatedly and consistently confirmed as the source of spam is likely to be a bot. Or widespread traffic patterns all originating from one point could be indicative of a botnet C&C center distributing instructions.

Whereas reputation techniques are very useful for security providers to block malicious traffic on the basis of its origin, they may also be helpful in locating individual infected machines in the network, for instance to notify their users. From the perspective of the security provider though, the identity of that user cannot be known, as the security provider does not allocate the IP address.

This is a main reason why, while IP reputation information may be generated and used quite effectively for the purpose of bot detection and notification, only the ISP who allocated that IP address has the legal and the technical ability to locate the user to notify. Therefore, any initiative in this area should account for the exchange and the processing of such information in a way that advances network security and situational awareness without compromising the privacy of personally identifiable information (see further down).

(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?
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?

Who should notify?

As stated above, while malicious traffic may be traced back to a given point in the network, only the ISP is able and entitled to correlate the address of that point in the network at that moment with the user who should be notified. This does not mean that other players in the ecosystem may not be able to notify a user that their machine is infected. For instance a software provider may detect a malware infection trying to infect – or already residing on – a machine, and flag this to the user of that machine, this however is not a case of bot notification as referenced in this RFI:

- The provider notifies its customer based on their license agreement, regardless of where that customer is in the network, not knowing anything either about which ISP allocated its momentary IP address to that machine, nor about whether the licensee of the software is the same person as the internet subscriber to whom the IP address was allocated.

- If the licensee does not fix the issue, the provider cannot take remedial measures, unlike the ISP who may have the contractual grounds to act for reasons of network security.

What support should be provided?

Various best practices have emerged from experiences in other regions, ranging from providing educational content, through recommending commercially available security products, all the way to offering purpose-built, bot-specific cleaning tools. Help lines and similar consumer support facilities may also be afforded. All these solutions have merits and their inclusion into an overarching anti-botnet initiative deserves consideration.

How should support be provided?

Any available communication channels may be used, with a likely focus on internet-based ones, as the issue at hand is internet-related and affects internet users first and foremost. Ongoing technological evolution towards new generation mobile networks further strengthens this, as these networks use the Internet Protocol to carry all communications, whether voice, messaging or data.

In any case, there are two key aspects to consider: effectiveness particularly on the user's side (see question 14) and authenticity of supporting and supported parties alike. The support resources, starting with the notification itself, need to be and look legitimate, so they don't end up misused or ignored.

Regardless of the communication channels considered and of the actual contents involved, the core functions to foresee should be the following:

- delivering notifications;
- providing general information and guidance materials;
- making available technical tools; and
- affording individual assistance upon request.

All of these functions are decisive in the process, but at the same time, each of them has the potential to be misused for malicious purposes, which could aggravate the problem instead of mitigating it.

The Symantec Rogue Security Software Report shows that cybercriminals are proactive in finding and using the best routes to distribute malware. Pretending to offer security is a particularly efficient lure. In many respects, given its scope, purpose, objective, legitimacy, credibility and *modus operandi*, an anti-botnet initiative makes an ideal resource for them to compromise. Spoofing emails or websites, intercepting, diverting and engineering live-chats in a "man-in-the-middle" fashion, and faking phone calls are all well-established criminal methods, and may all be used for purposes such as spreading malware, breaching data, and stealing identities. Moreover, just as cybercriminals may seek to impersonate an anti-botnet support agent in order to harm the user, they may just as well masquerade as users seeking support in order, for instance, to infiltrate and compromise the support resource, or

even simply to gather intelligence by mapping processes, capturing interface designs, etc., all of which may then be re-used for malicious purposes.

Therefore, any interaction between the support facilities and the users should involve more than the simple exchange of information. On the one hand, it should involve mutual authentication of the parties so that both the user and support facility can ascertain the identity of their interlocutor and certify that the exchange is legitimate. On the other hand, confidentiality of the exchanges is essential, therefore any communication should take place in a protected environment. Among others, this means end-to-end encryption of exchanged and stored data, certified websites, protected communications channels, and, to the extent feasible, authenticated devices. The requirement for such a high level of security should be built comprehensively into the anti-botnet scheme from the very start, and it may even be desirable to foresee iterative processes using alternative communication paths.

Experience with the current paradigm utilized in two-factor authentication schemes is relevant in this respect. If the infected device considered is a laptop, then utilizing a second contact route like an SMS to the device owner's smartphone is a way to ensure that the information gets to the user correctly and securely, notwithstanding any malicious interference with the web communications to or from the infected laptop. If it is then determined that the smartphone is in fact also infected, then a secondary confirmation could be made to the user through a voice message, and so on. Ultimately, the key is that the process ensuring the authenticity of the parties relies on more than just one channel, one token or one technology. Details will have to be worked out in regard of the concrete scheme(s) to be developed.

(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?

When considering scalable measures, it is important to gauge the magnitude of the issue. The previously quoted Symantec Internet Security Threat Report featured the following finding:

"*The U.S. is the main source of bot-infected computers for Rustock, one of the largest and most dominant botnets in 2010, and for the botnet associated with the Tidserv Trojan. At the end of 2010,* ***Rustock was estimated to have 1.1 million to 1.7 million bots and accounted for 48 percent of all botnet spam*** *sent out during the year. The Tidserv Trojan uses an advanced rootkit to hide itself on a computer, and* ***over half of all infected computers*** *that were part of this botnet* ***were located in the U.S.*** *in 2010.*"

This magnitude, measured in 2010, is likely to multiply as the number of web-connected devices increases[19], information explosion continues, bandwidth grows, cloud computing and virtualization technologies develop, mobility leveraging the capabilities of smart devices becomes even more

[19] According to IDC's Device Base Model 2009, there are an estimated 10-billion non-PC devices connected to the internet today, and the figure is foreseen to reach 20-billion by 2014: http://www.idc.com

commonplace, and the "consumerization of IT" progresses[20]. Anti-botnet measures both in terms of monitoring and mitigation will need to scale up, and technology can be helpful in a number of ways. Trusted distributed data and analytics will be essential in deploying a solution that will scale to the required capacity and performance.

Automation: Several solutions exist to automatically spot suspicious behaviors in the network and to generate equally automated remedial action as consequences. What such actions could be in the context of an anti-botnet initiative is certainly subject to further discussion and depends on a wide range of legal and operational factors, but technical capabilities exist to, *inter alia*, limit or interrupt traffic to or from specific points in the network, isolate those points, inspect data in transit to block and/or capture malware, bounce back information to points where malicious behavior is originating from, etc. Such technologies are used for example in corporate environments to prevent data loss and malware incursions, to enforce security policies, to measure and report regulatory compliance, etc. Applying them to public ISP networks for the purpose of botnet detection and mitigation is a possibility, subject to the availability of the necessary resources, and to the observance of all privacy and security safeguards.

The cloud: By concentrating computing power where it can be leveraged the most efficiently, cloud computing does afford superior security capabilities. For example patch deployment and email security are more efficiently done at one point in the cloud than at millions of endpoints. Therefore the cloud is certainly a relevant level for overall traffic monitoring and reporting, malware detection and blocking, and IP reputation assessment.

Distributed, on-demand service provision: Strongly related to the development of cloud computing is the massive emergence of services offered on demand, i.e. the possibility for users to pull from the cloud the services they require as and when they need them. This can actually range from simply providing information or tools (e.g., software) all the way to offering online services (e.g., live streamed personal assistance, remote intervention). Several models exist from public clouds (available to everyone) to hybrid clouds (leveraging public components but delivering services to a restricted circle of users only), to private clouds (self-contained, segregated systems providing services to their users only). Depending on the configuration of an anti-botnet initiative, any or several of these models may be used in combination, for instance by providing general awareness raising information in a public cloud model, delivering notifications from a hybrid cloud exclusively to subscribers served by the ISPs involved in the initiative, and offering tailored support services by the individual ISPs though a private cloud only accessible to their own consumers[21].

[20] Alan Drummer, *The "Consumerization" of IT*, in Symantec CIO Digest, April 2009: http://eval.symantec.com/mktginfo/enterprise/articles/b-ciodigest_april09_solutions.en-us.pdf

[21] This is only a theoretical illustration of possibilities, but not an actual architecture recommendation.

Technically, generating the intelligence needed to trigger any remedial measures involves, among others, the collection and processing of data such as IP addresses. In turn, the provision of any services to the end-user requires communications with that user, involving security measures such as authentication and encryption. The legal requirements are critical to define:

- how data, particularly PII, may or may not be collected, processed and transferred;
- when, where and by whom;
- what communications may or should take place between whom, in what circumstances and under what conditions.

In particular, privacy and security safeguards need to be defined so as not to obstruct effective monitoring for network security, whether the purpose is malware detection and mitigation, or more general analysis and reporting. As for measuring the impact of actions undertaken, see question 13.

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?

Recalling earlier explanations about roles and responsibilities in the ecosystem on the one hand, and about the various types of intelligence available on the other, a workable model would be the following:

ISPs could track connection patterns throughout their network, using anonymization techniques and segregation of duties, so that those patterns cannot be linked to any particular PII when intelligence is gathered. For instance, similar or identical behaviors may be observed simultaneously at several endpoints, suggesting effective botnet activity, without relating any of these to particular users. Yet, these anonymous data could then be correlated with equally anonymous IP reputation feeds such as those used by security providers in support of their services. Meanwhile, endpoints that communicate with sites known as dangerous could also be spotted and examined. If, based on that kind of anonymous investigations, sufficient reasons emerge to suspect a particular endpoint of being bot infected, then that specific record could be de-anonymized. The due process in this respect should ensure that the confidentiality of the information is preserved and that the already mentioned segregation of duties[22] is observed. Ultimately, the end user could be located and contacted so that remediation can ensue.

Another option, in parallel, is to make available detection tools that consumers can use to scan their systems when they see fit. This approach used in Germany and Australia minimizes the need to process

[22] Whether they belong to a same organization or not, the agents processing the bulk anonymous intelligence and those able to identify particular subscribers should only exchange information on a need to know basis.

PII[23], but fully depends on users' willingness to cooperate. In that sense, it is something useful to have on top of a notification scheme, but it is not equivalent in meeting the network defense objective.

(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)?

Security providers leverage heuristics and contextual information such as reputation. Typically, whereas infections may come in highly singularized forms as explained earlier, botnet related activity remains observed in wide-spread patterns[24]. Potentially suspicious behavior witnessed at one or few isolated points in the network is unlikely to be botnet activity, unless it is a new bot infection in early stages of distribution. Such cases should be investigated further before a positive detection is made.

That said, for an organization suspecting that it has been infected, the nature of this infection (bot or other) is secondary. If a suspicious or illegitimate behavior or action is observed and generates a positive detection, then it should in any case be investigated and remediated. A true positive will mean an infection that needs fixing, whereas a false positive will indicate flaws in the security policies, control processes and/or technological tools used, which then also need to be addressed.

In practice, the rate of false positives will depend on a large number of factors ranging from the granularity of security policies (e.g., segregation of duties, definition of roles), to the accuracy with which control processes are defined and enforced (authentication and access control, checks against authorized and forbidden actions, etc.), all the way to the performance and quality of the technological solutions implemented (poorly designed, maintained or operated technologies will have higher false positive rates). Even high levels of control automation allow for very low levels of false positives: it is a matter of using the most appropriate tools in the best suitable ways at the most relevant levels, iteratively fine-tuning settings and mechanisms on the basis of experience and empirical evidence. Generally speaking, the best way for organizations to avoid false positives is to define policies rigorously, enforce controls effectively, leverage technologies of proven efficiency, and, if a false positive nevertheless occurs, then take all measures needed to identify and address its causes.

[23] The processing of PII should be minimized but not excluded entirely: earlier explanations made it clear why any interactions should be protected. Making such tools publicly available is helpful, but as far as possible, those tools should not get into the wrong hands. Depending on what technologies are used (certification, authentication, electronic signature, encryption), some level of automated PII processing may be required, which should always be in compliance with relevant privacy safeguards, such as FTC FIPPs: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

[24] However, this is absolutely not say that all wide-spread patterns are malicious: identical simultaneous data flows from one source to millions of endpoints may well result from a perfectly normal and legitimate activity, e.g. distribution of security software updates to all customers, web streaming broadcasts, etc.

(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?

ISPs are not the only operators in the market who can play a role. However, they remain essential, with a unique position and function in managing their networks. This is particularly the case when it comes to notifying the individual users whom only they are able and entitled to identify behind the network address of an infected machine. It is all the more so if a machine needs to be cut off from the network. That aside though, many other stakeholders have a role to play in sharing intelligence, expertise and technology, to advance detection, improve protection and facilitate mitigation of bot infections. Foreign experience such as the German example noted under question 13 has been conclusive in showing that cross-sector initiatives with the strong and committed involvement of ISPs along with other stakeholders like security vendors and national network and information security agencies can be very effective.

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?

Assessing the spread of botnets was already discussed earlier. As for their negative impact, tools that enable cybercriminals to put millions of machines to tasks as varied as distributing spam and malware, stealing information, launching denial of service attacks, hosting malicious websites or committing clickfraud[25] do have a substantial negative impact. In terms of scale, the previously quoted Symantec reports provide a vast array of metrics on the financial, reputational and security impacts of malicious activities, many of which are botnet-related. For instance in 2010, an average data breach exposed 260,000 identities and had an average remediation toll of 7.2 million dollars. The damage inflicted by cybercrime is at an estimated 114 billion dollars yearly, counting neither lost gain nor remediation costs (another 274 billion). Web-based (often bot-related) attacks have grown by 93% from 2009 to 2010.

When it comes to measuring the impact of anti-botnet actions, other metrics can also be used. What may not be relevant for threat characterization (question 6) may well be relevant to assess the performance of a national anti-botnet initiative. The number or rate of infected machines[26] and the

[25] Fraudulently force clicks on advertisements to boost revenue.

[26] See the chart of the latest Symantec ISTR: http://www.symantec.com/business/threatreport/topic.jsp?id=threat_activity_trends&aid=bot_infected_computers

geographical spread[27] of bot infections are cases in point. The 2010 Intelligence Report from Symantec's MessageLabs[28] ranks countries according to their estimated bot infection rate, calculated as a function of that country's share in the global traffic of bot-generated spam, compared to that country's share in the global online population. Combined with the earlier quote from the Symantec ISTR (question 9), this metric suggests that while the U.S. may have the highest absolute number of zombies in certain botnets, the rate of bot-infected machines in proportion of the online population is much higher in other regions. Nevertheless, as the U.S. alone accounts for 12% of the world's online population, it is also the first by absolute volume of bot-related malicious traffic (14% of the global volume), and second by the volume of bot-generated spam (7% of the global volume). In comparison, countries with anti-botnet initiatives, actively involved CERTs and diligent ISPs such as Germany and Japan perform better in spite of internet penetration comparable to that of the U.S. Others like Austria, Finland and Australia, who also have anti-botnet initiatives in place, but also much smaller populations, don't even make it on the radar of top-10 countries by bot-related malware or spam origin.

Having said that, as most existing anti-bot initiatives are still fairly recent, there is so far quite little statistical evidence to accurately measure their impact in the longer run. Whether the deployment of comparable initiatives elsewhere can succeed in curbing the bot-related malicious activities is yet to be seen. For the time being, Japan's Cyber Clean Center Anti-Botnet Project, started in 2006, is the longest standing benchmark to consider. The metrics used in their latest comprehensive activity report[29], compiling findings from their detailed monthly reports[30], include among others the number of first and second user notifications, the number of visits to the information website, the number of downloads of the disinfection tool, the number of disinfection completion reports received, as well as detected infection rates in proportion of broadband penetration. Measured since 2007, all these metrics have shown a decreasing trend, with one exception: the number of users warned after a bot-generated attack was traced back to their machine has remained steady. This means that while the overall infection rate has decreased, infected machines are launching proportionally more attacks. Over time, as other anti-botnet schemes - such as the German Botfrei[31] initiative or the Australian icode[32] initiative - kicked off in 2010, and mature and start reporting their results, metrics should be refined and further developed.

---

[27] An example of per-country breakdown in the Europe, Middle-East, Africa region: http://www.symantec.com/business/threatreport/topic.jsp?id=emea&aid=emea_bot_infected_computers_by_country

[28] http://www.messagelabs.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf

[29] https://www.ccc.go.jp/en_report/Report_on_the_activities_of_the_Cyber_Clean_Center.pdf

[30] https://www.ccc.go.jp/en_index.html

[31] https://www.botfrei.de/en/ueber.html

[32] http://icode.net.au/

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

As mentioned earlier, a key challenge is to combine user-friendly convenience with authenticity (question 8). Provided that the authenticity aspect is addressed, the means of notification should take into account a number of factors.

The user who has to be notified is an internet user, whatever the device; the issue that needs fixing is internet-related; and the internet also provides a convenient way for the user to access remediation tools or request support. Therefore internet-based notifications (e.g. email) could legitimately be favored in priority to alternatives, provided that sufficient security can be ensured around the exchange, In particular the notified party needs to be assured that the notification is legitimate, while the notifying party needs to verify that the it was well received. The advantages of email notification include the ability to embed hyperlinks towards support resources such as remediation tools and guidance materials, enabling the user to click directly through to the relevant sites. That said, such emails should:

- be protected (encryption) and verified as authentic (certification, e-signature);
- be delivered to addresses actually used by the notified parties, bearing in mind for example that internet subscribers may choose not to use a default email address allocated to them by their ISP, and use other email services instead – various techniques exist to validate active email addresses, and are used for example in the field of online retail;
- withstand email security processes such as spam filtering or security scanning of content and attachments, including hyperlinks (important to minimize the risks of misuse).

Emails however may not always work for a number of reasons: there may be no valid email address for the user in question, disconnection of that user from the internet between the detection and the notification may occur, there may be presence on the infected device of malware specifically designed to intercept such notifications[33]. For such cases, and more generally as a matter of precaution, back-up solutions should also be foreseen, such as phone communications (using voice, text messaging, network messaging), as well as regular mail. For all these communication channels, a prerequisite is, again, for the notifying party to have accurate and up-to-date contact details to the notified party, which makes the prior collection of these data necessary, as well as the ability to check their ongoing accuracy and validity and make corrections whenever needed. This should be foreseen in the framework of the contractual relations established between the parties (e.g. when the user subscribes with the ISP), and to the extent that PII are concerned, the FTC FIPPs should apply.

[33] Such malware may even fraudulently return a successful delivery and read report to the notifying party, so that both parties are fooled while the infection goes unaddressed.

(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?

Recalling the explanations provided on streamlining or codifying practices (question 3), standardizing notification processes may be an option, as long as it remains at the level of the process, ensures the mutual authentication of the notifying and notified parties, and preserves the security and confidentiality of exchanges. But no specific technology should be mandated, as a technology specific standard could actually end up designating the points of failure for cybercriminals to breach in order to exploit the standard technology and turn it into a vector for cyber attacks.

(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?

IT security services such as botnet mitigation solutions are provided in many different business models. Some are fee-based or free of charge, some are deployed at endpoint or the local gateway level, and others are cloud services. They come under various contractual arrangements, licensing terms, service level agreements, terms of use. Whether a service is free or not is irrelevant to the effectiveness of the given product, which depends intrinsically on the quality of the engineering and intelligence behind the technology. Experiences such as the Japanese and German anti-botnet initiatives indicate that the provision of a cleaning tool free of charge is perceived by consumers as efficient and convenient, but when it comes to preventing re-infections, all initiatives point consumers to commercially available comprehensive security solutions, which may then be, indiscriminately, free or against payment.

As far as the attractiveness of products is considered, products with a higher performance and reliability track record are generally more attractive, irrespective of the pricing strategy in their marketing. Customers – especially those who have compliance requirements to satisfy and are particularly exposed to financial, reputational and IT risks (e.g. public agencies, large enterprises) – will seek solutions which are known to be effective, and have demonstrably reputable engineering, security intelligence and response capabilities. Other users, such as small businesses and consumers, may have different price sensitivities, but at the same time, convenience and ease of use of products are also particularly attractive for them. As technology penetration and public awareness of cyber risks progress, this segment also grows conscious of the benefits of investing in high quality security solutions, rather than finding themselves repeatedly exposed to malware infections and often expensive remedial measures.

(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?

Experience abroad shows that a consumer resource center is very helpful in raising awareness, and as such, it strengthens the IT security market. Such centers don't compete with value-added services but earn them higher visibility. Even those that provide cleaning tools free of charge for a one-shot initial disinfection (e.g., Symantec's Norton Power Eraser offered in the German Botfrei initiative) will bring

consumers to consider value-added services to meet their needs for ongoing comprehensive security. Therefore, providers of such services support these anti-bot schemes as part of their own marketing strategies, expecting such partnerships to deliver mutual benefits.

Whether offers for value-added services may or may not be included in a notification scheme will depend on the nature and legal framework of the scheme: competition and technology neutrality requirements will be different in a private partnership between a closed circle of ISPs and security providers, a public-private partnership open to all participants, or a public initiative operated by public agencies with industry support. Examples in other regions have shown that even the public nature of a notification scheme is not incompatible with, for instance, the inclusion of links to value-added offerings on the initiative's information website. Exact details of what may or may not be involved in a notification will need to be defined depending on the structure considered, on the understanding that the ability to reach more consumers is a key incentive for private operators to join such partnerships.

Finally, about the prevention of abuses and fraudulent offers, this issue was already discussed in the earlier explanations on rogue security software and measures against them.

(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 bot-infected computer constitutes a threat to the network, and if the owner of that machine fails to remediate the threat in spite of one or several notifications, then the only technological recourse without intrusion into the perimeter of the said system is to isolate it from the network. The network access being provided by the ISP, the ISP is also the operator in a position to isolate that connection.

Whether this is possible and should be considered as an ultimate step if a user fails to follow up on a notification depends on the contractual arrangements – and possibly on the regulatory requirements and legal possibilities – applicable to the bilateral relation between the ISP and the user. The exact process, including roles and responsibilities, should be subject to further discussions between all participants. Unless possible options for network security measures, such as putting infected machines in a walled garden or disconnecting those which launch attacks, are provided for under law, it is essential that contractual terms between ISPs and users entitle the ISP to take any remedial actions foreseen. To that end, as a matter of legal certainty, the user needs to be informed and should give prior consent. In the context of a partnership or code of conduct such as described in the RFI, it is proposed that ISPs subscribing to the code ensure that their ongoing and future contractual terms are drafted or amended accordingly, and users are informed and their consent is sought.

(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?

Symantec has no particular experience to substantiate that concern. The liabilities of service providers towards their customers depend on the contractual terms, service level agreements and other mutual commitments between the parties, and will vary greatly whether the customer is a consumer, a small business, a large enterprise or a government, as well as whether the service in question is about network access, security, online content, etc. Moreover, the circumstances of the service provision may be very different even if the same service (e.g. security) is provided according to the same contractual terms to two similar customers (e.g. two individual consumers). For example, one consumer may be diligent in installing security updates while the other may be negligent, in which case the same malware may infect one machine and not the other, or the infection may be detected here but not there.

Service providers should know from their own contractual terms to what extent they are liable to each individual customer, e.g. for notifying an infection, in due consideration of the individual circumstances of each case. In the context of the proposed anti-botnet initiative, it should be foreseen that those participants who will take on the responsibility of notifying users make it clear in their contractual terms that the detection and notification of bot infections, as well as their mitigation, are subject to best efforts on both the provider's and the user's part, and liabilities should be defined – the case being exempted – accordingly. This, as well as the notification process discussed under the previous question – should be subject to further discussions, and will require specific legal expertise.

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?

As already mentioned, these initiatives have indeed been effective, although, apart from the Japanese case, statistical evidence on their impact is still scarce. The key lessons learnt are the following:

- There is definite willingness on the part of public authorities, ISPs, security providers and other stakeholders to cooperate, provided that the scheme provides benefits to all participants.
- The endorsement by public authorities may be helpful in strengthening the awareness raising aspect of such initiatives, whereas the technological input is best provided by the private sector.
- National initiatives can have a local impact, but in the longer run, international cooperation will be necessary to address an issue which, in fact, is global.
- The provision of publicly available detection and cleaning tools, the case being free of charge, so far has been an effective way of reaching out to individual consumers, who appreciate receiving information, support and resources when faced with malware they can't address on their own.

- That said, such initiatives don't compete with commercial offerings, but are complementary, and can even help build consumers' confidence in the efficiency and effectiveness of cleaning and ongoing security solutions, which in turn acts as a market incentive for industry.

(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?

Various stakeholders regularly analyze public perception and awareness of cyber security concerns and issues, whether among consumers or other market segments. Symantec regularly issues threat intelligence reports and studies as well as consumer behavior surveys (e.g. the Norton Online Family report[34]). While these may not have a particular focus on botnets, they give regular and fairly representative snapshots of the cyber threats and cybercrimes that individual consumers are faced with, and information from such studies, particularly the evolution of certain metrics over time, can certainly be helpful in assessing the impact of awareness raising initiatives.

That said, to date, in the specific context of anti-botnet campaigns, the Japanese Cyber Clean Center provides an example of metrics which, measured over several years already, have shown a definitely positive impact in terms of the number of notifications made, the usage of the cleaning tool, the number of completed disinfections, the number of visits registered to the information platform, as well as, more generally, the decreasing infection rates in a context of increasing broadband penetration, exponential growth of data and, accordingly, more and more sophisticated, varied, complex and dense cyber threats.

Similar or additional metrics should be developed in consultation with all stakeholders, and to the extent feasible in coordination with foreign initiatives, so as to make results comparable internationally.

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?

In the recommended scenario whereby notification of users would be the responsibility of the ISPs who serve their internet access, the most probable cases where the user may pursue the ISP's liability in relation to this notification duty (but notwithstanding any other aspects) would be the following.

Failure to notify: As explained earlier, the ISP's ability to detect a bot infection on a user's machine is subject to many factors and circumstances under the unilateral control of the user, who may or may not enforce patch levels, use virtual private networks or proxy servers, implement other technical measures on their machines that obstruct the effective remote detection of an infection, or refuse certain forms of processing of their PIIs so that their identification and/or their notification is impeded. In such cases, the liability of the ISP for not notifying should be excluded.

[34] http://us.norton.com/content/en/us/home_homeoffice/media/pdf/nofr/Norton_Family-Report-USA_June9.pdf

Notification by mistake: Whereas an erroneous notification is the result of a false positive detection and is as such a regrettable event, liability should not be incurred on the part of the ISP unless it causes effective and demonstrated damage to the user. In so far as the notification merely indicates a suspicion of infection and invites the user to take certain measures to check, and the case being disinfect their machine, running the test and finding no infection to remove should not in itself be considered as a damage. If the detection and cleaning tool is made available against payment of a fee, contractual arrangements between the parties should clarify in advance who is to bear the cost of it, the case being depending on whether the suspected infection is eventually confirmed or denied. Regardless of what the actual outcome of the process is, in any case an authenticated certificate should be returned from the user to the notifying ISP to establish in a verifiable way that the suspicion was ultimately either denied (in which case the burden of a potential fee may be put on the ISP), or confirmed (in which case the user should be liable for cleaning their machine).

To the extent that the scheme involves the possibility of such a measure, an additional aspect to consider relates to the case of a **user isolation** (walled garden, disconnection) following the user's refusal to address a bot infection in spite of having been notified – the case being iteratively. In such a case, should the measure be perceived as an arbitrary and unilateral breach of the service contract by the ISP, the user may of course pursue the ISP's liability. To avoid abusive litigation on this point, contract terms should foresee a duty for the user to check and clean their machine in case of a notified infection, and as a sanction, the possibility for the ISP to take protective measures without incurring liability, as a matter of ensuring the network's security. In the case described earlier where malware on the user's machine intercepts the notification and returns a fake receipt to the ISP, both parties are fooled and disinfection will not take place. This may ultimately lead to measures taken against the user who never actually received any notification. That however is attributable to malware present on the user's machine, and the ISP's liability should therefore also be excluded.

All these aspects will require further careful consideration and drafting by legal experts, depending on the parameters and characteristics of the scheme eventually adopted. That said, a common trait between these cases, as was already mentioned, is the need for both parties to be able to demonstrate in an unquestionable manner (e.g. using secure and authenticated electronic communications) that they fulfilled their contractual duties in any given situation, and are therefore exempted from further liability.

(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?

All anti-bot initiatives developed abroad combine the use of detection and cleaning tools to get rid of a first infection, the broadcasting of public awareness raising materials on the importance of ensuring permanent protection of systems, networks and data, and the link to commercially available services designed to provide such ongoing protection. It is critical to ensure that users who have suffered an infection, got notified, and managed to disinfect their systems take the necessary steps to prevent further re-infection, i.e. deploy ongoing protection solutions. Short of that, given that new unique malware variants emerge at a rate of more than 20 every second, a disinfection at one single point in

time can by no means prevent further re-infections, much to the contrary: a consumer who would be brought to believe that a one-off disinfection provides enough security, and who would consequently fail to take ongoing security measures, would most likely end up infected again very soon. In that sense, providing detection and cleaning tools, raising awareness and pushing to the use of permanent security solutions must go hand in hand at all times.

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

Depending on how the initiative is designed, terms may need adaptation that relate to the processing of personally identifiable information (so that users are informed in advance and their consent is acquired), to the measures that may be taken by ISPs (ranging from detection through notification all the way to isolation or disconnection if necessary), and to the respective liabilities of the parties in various scenarios. These issues should be explored further and careful drafting should be conducted by legal experts, particularly competent in the ISP sector, in IT law, in consumer protection and in privacy.

(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?

The most effective in terms of incentives for market operators would be an initiative that is led by the private sector (model A or possibly model B). Whether the support of the public sector should be sought (model B), and if so, what level of involvement the public sector should have, remain to be discussed.

Experience from Germany's Botfrei initiative has revealed that a key incentive for the private sector to engage in such partnerships is the efficiency of operations, and the agility and flexibility with which they can adapt to swiftly evolving circumstances such as the overall cyber threat landscape. The German case has shown that this requires the private sector stakeholders to stay in control of the decision making processes and operational aspects of the partnership. In fact, in that particular case, the public authorities initially involved in decision making processes themselves chose to withdraw from that part of the partnership's daily operations, and went on to focus on areas where they can more efficiently contribute: awareness raising, visibility and credibility building, policy shaping, support to the standardization of processes, high level governance, international outreach. In other initiatives however, such as in Japan and Finland, public agencies or CERTs have taken an active, or even a leading role, while the private sector has been providing technological support, and these models have also borne fruit.

Therefore, it is recommended to take stock of these diverse experiences to fine-tune the proposed model B (public-private partnership) in a way that gives as much control as feasible to private operators to incentivize participation, while all the benefits of being supported by public agencies should also be leveraged. An additional argument in that direction is that whereas the private operators have contractual grounds to take certain actions and measures vis-à-vis their customers (such as monitoring, detection, identification, notification and follow-up), the place and role of public agencies in such schemes may be questioned, as, short of any legal or contractual grounds (a code of conduct not

providing any by itself), their direct involvement in matters that may require the processing of PIIs may be misunderstood, and therefore unhelpful or even counterproductive. On the other hand though, government agencies' endorsement of and support to these initiatives certainly has a lever effect by adding visibility and credibility to the partnership.

(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?
(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?

As just discussed, our recommendation would be a hybrid model combining the private sector and public-private approaches. Regardless of their structure and processes, public-private partnerships work best when they are purpose-specific, have clear goals, missions, and rules defined accordingly, and foster the development of a sense of mutual trust and confidence in information exchange. The partners who should be involved in an anti-botnet consumer resource initiative have very diverse backgrounds and complementary, but not identical interests. It is therefore unlikely that any already existing sectoral organization is able to broker sufficient trust from partners outside the given sector. On the other hand, existing cross-sector organizations may lack the purpose-specificity that the partnership requires to be effective. Therefore, in consultation with all categories of stakeholders to involve, both on the public and private sides, a dedicated structure should certainly be built. Whether this should be entirely new or could come within the framework of one or more already existing organizations, and which ones those could be, should be discussed further between all partners.

As far as incentives are concerned, points already made earlier should be recalled: Effective control of the resource by the private sector and the ability for partners to leverage the resource as a business driver (private sector) and/or a policy tool (public sector) are certainly good enough incentives. Likewise, the possibility for stakeholders to earn certainty on their responsibilities and liabilities both in the particular context of the botnet notification scheme, and more generally in the framework of national critical information infrastructure protection, should be well appreciated. Regarding the question of control and leadership, it should be ensured that the governance structure takes account of the fact that the business incentives may be different from one stakeholder to another (e.g. cost savings for ISPs, revenue opportunities for security providers), while the respective responsibilities are also different (monitoring and notification for ones, technological expertise or intelligence for others). All partners will want to have an influential role proportionate to the responsibilities they hold and the benefits they drive from the partnership, and that should be ensured.

Finally, looking at the participation by and contributions from government agencies, given the nature of the task undertaken and the objectives pursued, all agencies are legitimate to participate which have to do with cyber security, critical information infrastructure protection, computer emergency response,

telecommunications and related standardization, law enforcement in the area of cybercrime, international cooperation, as well as commercial data privacy and consumer protection. More concretely, the following should be invited to share their views on possible participation: US CERT, DHS, DOC, DOD and affiliated bodies (particularly DISA), FBI, FCC, FTC, NIST, NSA, NTIA, as well as possibly the Commission on Civil Rights, the Consumer Financial Protection Bureau, the Small Business Administration, and at least for information the White House Cyber Security Coordinator, the Chief Information Officers Council, as well as relevant resources in the Departments of State and Justice. Their contributions can range from sharing information to supporting visibility, credibility and awareness raising, to policy shaping, regulation and standardization if and where necessary, all the way to international outreach, cooperation and coordination.

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

A purely government-run approach may fail to generate sufficient incentives for market operators to contribute the indispensable technological expertise, intelligence and operational capabilities required for effectiveness. That said, when discussing the level of involvement of various agencies in a public-private approach, US CERT, FCC, FTC, NIST and NTIA are obviously top tier partners to take on board.

(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?

Various market operators may, on their own or through *ad hoc* business partnerships, set up comparable resources for the benefit of their own customer base, and/or provide similar services on a commercial basis. These however are merely restricted versions of the private sector model proposed in the RFI, and are typically not meant to achieve the nation-wide impact expected from an open-ended and all-inclusive anti-botnet public-private partnership such as envisioned here. That is not to say that such private initiatives are unhelpful or should be avoided, on the contrary. However, synergies should certainly be sought to the extent feasible with the national scale initiative that is to be developed.

(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?

Any scheme, whether public and/or private, that effectively raises consumers awareness of the importance of protecting devices from malware infections is a positive incentive in that it creates interest on the demand side and encourages a response from the industry on the offer side of the market. Nevertheless, botnet detection, notification and mitigation remains a highly sensitive issue, essentially due to the fact that it involves traffic monitoring and user identification, and may therefore be perceived as intrusive both on the data privacy and on the communication privacy fronts. As a consequence, any lack of clarity or void in the legal (contractual and regulatory) framework applicable to this activity is a major disincentive, in particular where liabilities may be sought. Therefore, it is desirable that even if an organized consumer resource center with clear rules for everyone is not set up, some form of general framework is built to clarify what the various operators should, may, or shall not do,

where liabilities may be excluded or engaged, how this activity fits into the national efforts at protecting critical information infrastructure, etc. In that sense, regardless of whether a consumer resource is created, the public-private partnership should be undertaken and developed at least to federate the players to involve and streamline the practices to follow, for example through a code of conduct.

Symantec looks forward to working further with the DoC and DHS on this matter and remains available for any additional queries at the contact details below:

Cheri F. McGuire
Vice President
Global Government Affairs and Cybersecurity Policy
Symantec Corporation
cheri_mcguire@symantec.com