PayPal™

2211 North First Street, San Jose, CA 95131

United States Department of Commerce
National Institute of Standards and Technology
1401 Constitution Avenue, NW., Room 4822,
Washington, DC 20230

Attn: Willie E. May, U.S. Department of Commerce
Lawrence E. Strickling, U.S. Department of Commerce
Rand Beers, U.S. Department of Homeland Security

[Docket No. : 110829543-1541-01]

Dear Misters May, Strickling and Beers:

PayPal, a leading global online payment company, is pleased to submit comments in response to the request put forth by the U.S. Department of Commerce and the U.S. Department of Homeland Security for comments on the creation of a voluntary code of conduct to address the detection notification and mitigation of botnets.

PayPal firmly believes that the Internet is an ever more critical resource to the global economy and people's lives, and that preserving an open, innovative, generative Internet is an important goal.
It is vital to not conflate principles which would make the Internet as safe as reasonably possible for consumers with proprietary or commercial interests.

In specifically addressing the request for comments, PayPal offers the following guiding principles:

- The success of the Internet ultimately rests upon consumers trusting the Internet and its safety. While this cannot be absolute, it is clear that the current trends are driving the Internet towards less, rather than more, trust.
- Network and telecom regulation should be fully supportive of ecosystem safety and security. Regulations should be narrowly tailored to disallow inappropriate behavior while still allowing network operators and service providers to provide protection against security threats.
- Cybersecurity solutions must require that those best able to provide for security be held responsible and accountable for doing so. In essence, we believe that many of the security and safety problems that the Internet suffers today are due to negative externalities. Using natural choke points to effectively manage negative externalities is one of the most important principles in making the Internet safer.

Internet Service Providers (ISPs) play a central role in the security and governance of the Internet. Because of their role as providers to consumers and businesses, their backbone transit of both regular Internet traffic and in many cases human-safety critical traffic, and their role in both detecting and responding to large-scale attacks, ISPs must be relied upon to take an active role in making the Internet and the overall communications ecosystem safer.

Before answering the questions posed specifically about botnets it is perhaps appropriate to make some general statements about the size, scope, and nature of the problem, general efforts to date to combat botnets both in the U.S. and elsewhere, and then turn to the specific questions asked.

First, we believe that botnets are a problem that impacts the user of an infected computer as well as the other members of the internet ecosystem. While some botnets are merely harmful to the individual user and impact the privacy and security of their data, many botnets are used to send SPAM and Phishing email, and participate in large-scale Distributed Denial of Services (DDoS) attacks. Any system we develop must take into account both of these types of harm - harm to the individual, and harm to the environment.

Long gone are the days of computer viruses that impact only the individual computer they infect. Today's botnets are more akin to pollution - a negative externality with impacts often far beyond the negative results to any single user. Any system to combat them must therefore rely on the right combination of voluntary and incented cooperation, partnered with enforcement and regulation to ensure that the costs of botnets aren't shifted only to the victims of the crimes they enable. In this sense we believe that the system of rules and regulations we design to combat botnets and malware should be thought of similarly to the rules and regulations that govern pollution. Just as organizations such as the Environmental Protection Agency (EPA) have a mandate to reduce the harms of pollution (commensurate with the costs) we believe that commerce must examine similar models to mitigate the harms of malware and botnets.

Second, we believe that law enforcement should be at least as active in countering botnets as they are other types of online abuse. The coalitions put together by U.S. law enforcement working in concert with foreign law enforcement to combat child pornography and other types of abuse online such as counterfeiting and intellectual property theft (piracy) can and must be brought to bear to fight botnet activity as well.

Law enforcement should be careful in these cases to eliminate false positives in their enforcement. As well intentioned as recent actions by DHS/ICE may have been, their mistaken takedowns of some substantial amounts non-infringing content are problematic both from a legal standpoint, but also from a public policy and public opinion standpoint. Takedown efforts should be narrow and targeted to ensure the highest amounts of cooperation from legitimate actors in the ecosystem: to maintain their trust, willingness to act aggressively on government and private requests, and to act against botnets hosted within their areas of control.

Law enforcement should continue to explore aggressive strategies against botnets and their operators. We are encouraged by the FBI's recent actions against the Coreflood botnet. However, we believe these same tools could have been used effectively much sooner and against other botnets, rather than relying on private operators to initiate their own actions against botnets. While coordinated action may be needed against both the operators of a botnet and the infrastructure and software which supports it, it's not necessarily clear that law enforcement organizations are the best type of organization to be operating botnet takedown operations.

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.

Roughly speaking there are two general network-based techniques that can be used to detect malware and botnet infected computers remotely without the use of software on the infected computer: 1) Network Traffic Analysis and 2) Packet Inspection, or "Deep Packet Inspection" (DPI).

Network traffic analysis is generally effective in identifying computers that are part of well-known botnets who have either a well-known list of command-and-control (C&C) servers, or where some other easily identifiable behavior is observable, sometimes even from afar.

Some other types of malware and botnets can only be detected through a deeper analysis of the exact contents of the network traffic sent to and from and infected computer.

In general network traffic analysis is substantially easier to deploy on a network and requires substantially less network gear. It can often be deployed in front of common "choke points" on a network such as DNS servers, and because it does simple pattern matching is much less Central Processing Unit (CPU) and memory intensive, and consequently is much cheaper to deploy. There is more than one vendor with a relatively low-cost commercial offering in this space.

Deep packet inspection is substantially more difficult to deploy as it requires significant network equipment and is often expensive. Though the term DPI is a relatively new term to describe this technology and is occasionally marketed as a different product or niche, the equipment is fundamentally identical to intrusion detection systems which have been around for quite a number of years. Because this technique is capable of more extensive data analysis it has the potential for a reduction in false-positive rates. Some critics of DPI technologies deployed at the ISP point out that DPI technology can be abused to be privacy invading, and misused to negatively impact consumer security. However, it's worth noting that DPI originated as a security technology and is still overwhelmingly used for purposes that are entirely benign.

While there is not enough public information about which of these two techniques are most effective at fighting malware and botnets, we believe that technologies that rely on network traffic analysis are both easier and cheaper to deploy, and less capable of being abused and used for purposes other than detecting botnet activity. While we don't believe that regulations should specifically require one technology or the other at this time based on a lack of evidence of their effectiveness, we do believe that the department should seek input from those who have deployed this equipment in "carrier grade" deployments to share what information they can about the effectiveness of each approach.

Once potentially compromised hosts have been detected using the data generated by these network-based detection systems, several options are available to multiple players in the network: 1) Notification to the user, 2) Traffic Filtering, and 3) Network Quarantine, placing the user in a so-called "walled garden".

Several countries have experimented with each of these approaches. Perhaps the oldest is the system actively deployed by the Australian Communications and Media Authority (ACMA), a voluntary program known as the Australian Internet Security Initiative (AISI) which is a user-notification mechanism paired with a central entity that facilitates the collection and distribution of a list of suspected compromised IP addresses (home computers).

Most deployed user notification systems rely on each ISP to notify their customers that their machine may be compromised, by consulting their own, and community compiled, lists of potentially compromised computers. These notifications take the form of either content placed on webpages owned and controlled by the ISP itself, or via "redirects" or "content injection" when a user attempts to visit a regular website on the internet.

While both of these "redirects" or "injections" can be effective in notifying consumers that they may be infected, we remain uneasy about the security implications of legitimizing the modification of authentic content by an intermediary, even with the best of intentions. With the trend of many popular websites deploying HTTPS in greater numbers, we also believe that content modification is at best a short-term strategy. As more sites move to HTTPS, and other secure end-to-end signaling mechanisms, content-injection is both no longer possible, and no longer differentiable from the actions of an attacker.

As such we actually favor ISPs notifying their customers through their own websites, email, phone calls, postal mail, and working in concert with other parties in the ecosystem that are also positioned to notify users, and in a position of trust. Much like multiple websites have acted in concert to advise users to upgrade their web browser as part of the Online Trust Alliance's (OTA) "Why Your Browser Matters" Campaign[1], we believe that one way to make a security notification more effective is to deliver the notices via websites a user already trusts, has a relationship with, and from whom the message may be taken more seriously.

We expect that financial institutions, webmail providers, and even social networks are likely candidates to participate in this sort of notification effort, because they, after consumers, are some of the entities most negatively impacted by malware and botnets in the ecosystem.

We are also in favor of ISPs deploying traffic filtering solutions to eliminate certain types of botnet traffic. When feasible we believe ISPs should aggressively filter traffic to known botnet C&C servers from their networks.

[1] http://www.whyyourbrowsermatters.org

In addition to filtering C&C traffic we strongly believe that ISPs should be responsible for providing both ingress and egress filtering on their networks. Ingress filtering ensures that traffic entering the ISP's network from outside does not spoof traffic from hosts at the ISP itself, thus protecting the ISPs customers from certain types of attacks. Egress filtering at the ISP ensures that hosts within the ISP's network do not spoof or pretend to be hosts from another ISP. Many of the most devastating DDoS attacks on the internet have occurred due to spoofed network traffic. ISPs that implement network egress filtering can then at least ensure that they do not themselves contribute to this specific problem.

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.

Today there is a substantial difference of opinion between anti-malware researchers as to the cause of most infections. Some researchers in this area report that, judged by prevalence when scanning and examining internet sites that "drive-by downloads", or malware that exploits a technical security flaw without user interaction, as the most common source of infections[2]. Other researchers are reporting that roughly 50% of malware infections are due to "social engineering malware", or malware that tricks a user into installing it by purporting either to be a different type of software than it is, or by falsely claiming it is security software that will remediate an existing infection on a user's machine.[3]

Regardless of which group of researchers are correct we believe that any anti-malware strategy should focus on both types of problems.

To combat "drive-by downloads" users should make sure that their operating system, web-browser, and "plugins" (Java, Flash, etc) are up to date. They should also make sure they have applied all of the recent patches to the software on their machine, and have configured that software where possible to "auto-update". Users should also take care to run without administrator privileges during the normal course of their computer usage, and rely on administrator rights only when necessary to install software or intentionally modify their operating system and its settings. Most current major consumer operating systems such as current versions of Apple's MacOS and Microsoft's Windows-7 product are configured in this manner by default, as are most common Linux distributions such as Ubuntu, to name but one.

In addition to software updates, users are advised to run a web browser that consults a "blacklist" of known malware and phishing sites, and warns that user they may be visiting a site likely to infect their computer or steal their usernames and passwords.

We also remain convinced that despite some warnings about the effectiveness rates of anti-virus software, that it remains a viable option for stopping a meaningful percentage of malware. Anti-virus packages in conjunction with other filtering technologies such as Microsoft's "Smartscreen" software can use "crowdsourcing" to defend against certain types of malicious software.

[2] http://googleonlinesecurity.blogspot.com/2011/08/four-years-of-web-malware.html
[3] http://www.microsoft.com/security/sir/default.aspx

User education remains an important component of preventing malware infections, but detailed instructions about how to detect malware are less likely to be successful than training users to keep their computers configured in a secure manner.

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?

Because malware and botnets are such an enormous problem in the ecosystem, concerted action by all responsible parties is required. We do believe that each ISP should have the flexibility to implement botnet mitigations using the solution most appropriate to their network. However, in order to both incent cooperation and determine whether all actors are fulfilling what we believe are their duties, a baseline code of conduct is required to set appropriate expectations.

A code of conduct should be an initial step, leading to reporting and metrics that can signal to other entities in the ecosystem whether each player is doing their part to mitigate botnets.

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

Several practices, which if deployed more broadly and by default by software vendors, operating systems makers, and systems vendors, could make a significant impact on the prevalence of malware and botnets.

1. All software should be configured by default to auto-update itself with security patches.
2. All computers sold to home users should come configured with antivirus software by default.
3. Each computer sold should have a quick setup guide with basic user-safety instructions advising users not to disable their auto-updates and antivirus software.
4. Computer vendors should ship new computers with third-party auto-updaters to keep all of the software on the computer up to date automatically. This is especially important as some software does not auto-update.
5. Home networking gear should come configured with unique administrator passwords. We note that some networking vendors already do this by using the serial number of the device or other unique value printed on a sticker on the device as the administrator password.

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

We believe that a program modeled after the AISI model described in our answer to question-1 is the best model. The AISI program is a voluntary public/private partnership, which appears to be the most workable model in the US as well. However, we believe that in the US the best approach may be a public/private partnership with many of the costs borne by the relevant government agency, but run by a designated private non-profit entity. Organizations such as the National CyberSecurity Alliance (NCSA) or StopBadware who already have a mandate to fight malware, educate users about cybersecurity, and work towards that public good might be options to host this function. The NCSA is at least partially funded by the DHS and is a good example of the principle described above. Obviously any entity selected to run or coordinate a production botnet information and compromised host clearinghouse function needs to have strong operational experience as the work is not insignificant and such an entity will also be the subject of attacks by malware authors and botnet owners.

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?

In the US we are not aware of any legal hurdles to the sharing of compromised host data and the IP addresses of suspected botnet member machines, though clarity that U.S. privacy laws including ECPA don't apply would be welcomed by many members of the community.

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?

For both this question and question 8, we do not yet have an opinion on the best direct ISP to consumer contact mechanism. We are hopeful that the several ISPs in the U.S. market that current provide botnet detection services can and will provide details to the department on what customer notification mechanisms they find most effective in getting customer attention, and remediation of the problem.

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?

As mentioned above when discussing the types of networking monitoring that can be performed, we are strong supporters of networking technologies that can detect some types of malware, but without the attendant risks posed by Deep-Packet-Inspection (DPI) tools.

Additional lessons can be learned from the Australian AISI model. Under the AISI model:

1. ISPs sign up for the Australian Internet Security Initiative (AISI) program
2. ACMA uses various intelligence sources to compile a list of Internet Protocol (IP) addresses which are apparently compromised by malware
3. ACMA communicates that list to the relevant signed up ISPs
4. 4. In turn the ISPs then communicate with the end-customer that there's a problem with one or more of their personal computers (PCs).

Under the AISI model the organization building the list of potentially infected machines does not have records on the identity of each user. ISPs voluntarily subscribe to the list but they don't necessarily compile it themselves. Though there are fears that IP addresses can be correlated to real individual identities, the data collected is not about the websites a user visits or the contents of their communications.

We believe that those who do examine network traffic for malicious activity must only keep records of the potentially malicious traffic itself. If an ISP watches client DNS traffic to detect compromised computers attempting to contact a C&C server by looking up the name in DNS, it would be entirely inappropriate for the ISP to keep records of any other unrelated DNS queries except in aggregate. Indeed, where the ISP has no legitimate security purpose for collecting the DNS query data (or other network data) except when it does match a malware C&C node, their software should be configured specifically to never log the traffic. Where such logging is technically unavoidable, extremely restrictive data retention rules with very short lifetimes should be required.

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)?

With the increase in the number of networked devices in the home all sharing the same public IP address space only ISPs with their visibility of the home network can effectively determine *which* home device is likely to be the actually infected computer. Without access to home network data, an outsider can only tell an ISP customer that *some* machine is likely infected. These false positives are problematic for experienced customers, and may prove an insurmountable barrier to non-expert users in remediating their problems.

As such, some combination of network-based botnet detection paired with end-user computer-based anti-virus software is a much better candidate for finding infected machines and reducing false-positives than network-based detection alone.

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?

Many current remediation efforts focus on post-infection action with little attention being given to prevention. While these efforts are important and should be continued, we believe efforts to address the problem closer to the source could yield significant results.

We believe that a concerted effort amongst OS vendors, system makers, software security vendors (anti-virus companies) and prominent websites is necessary to effectively combat malware. Campaigns to directly detect malware itself and to educate consumers about prevention must come through multiple venues. As an example, PayPal is running a safer-browser campaign[4] that educates users about the value of upgrading their web browser to a current version. In addition to the education campaign

[4] https://www.paypal.com/saferbrowser

PayPal also alerts customers if their browser is outdated when they log into the PayPal website. The Online Trust Alliance (of which PayPal is a board member) has also launched the "Why Your Browser Matters" campaign to get a broad coalition of browser makers and websites to collaborate on delivering a consistent consumer oriented message about the need to keep your browser up to date.

We believe that more efforts in this space are necessary to deliver consumer safety and security messages, and make the broadest impact on consumers and consumer behavior.

Another example is for Domain Name registries to perform periodic malware scans of web sites within their Domain and to take measured action, from notification up to and including suspension. Registries have a vested interest in protecting their brands in this way and should consider taking these actions on a voluntary basis, as recently proposed by Verisign to ICANN.

Going further back in the infection chain, we note that domain name registrants are poorly vetted and as a consequence, it is a simple matter for criminals to register and then use names for illegal activity, including distribution of malware used in botnets. Requiring Registrars to vet, and therefore better know their customers would make it more difficult to obtain one of the critical resources necessary to distribute malware. While this is perhaps outside the direct scope of the botnet question, we believe that stronger domain vetting is extremely important generally to ecosystem security and would help make the operation of certain classes of botnets more difficult.

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?

In the case of an end-user device participating in a destructive botnet, and where the ISP cannot mitigate the effects through traffic filtering, the user must be placed in a quarantined state so they cannot cause harm to others. Care must be taken when quarantining a user as certain life-safety critical systems could require internet access, including but not limited to VoIP services provided by someone other than the ISP. The best approach to defining if and when quarantines can be imposed is to call together an expert working group of ISPs, public-safety officials, and other government agencies such as the Federal Communications Commission (FCC) to study which approaches will be both safest for the ecosystem and the end-user whose network connection may be limited. It is worth remembering that this is fundamentally a balancing test between the harm to the end-user of the infected computer, and the harm they may be causing to others.

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 are unaware of any published statistics directly on this point, but several related efforts leads us to believe that users take online notices about security seriously when presented with a consistent message and are properly motivated.

Several organizations (including PayPal) have started notifying users when their web browser is out of date. At least one of the organizations relates that they have had a more than 50 percent success rate with users upgrading their web browser in order that they should still be able to reach the website of said organization.

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?

We aren't aware of any cases where an ISP or other service provider has been found to have liability in cases where they have failed to notify a customer about a security issue.

In closing, we are strong supporters of efforts to combat malware and botnets through concerted, coordinated, and shared actions by all players in the internet ecosystem. All actors have a role to play, and we welcome Commerce's role in engaging with a variety of stakeholders to improve the safety and security of the Internet. It's clear that today, government has been acting only sporadically in attempting to protect consumers and businesses from the operations of botnets. This is unfortunate, as coordinated action of the kind only possible by government is almost certainly key to substantially reducing their impact. The Department of Commerce is to be commended for its role in promulgating the safe operation of the Internet.

Sincerely,

Michael Barrett
Vice President - Information Risk Management
Chief Information Security Officer