scripted

Volume 7, Issue 2, August 2010

ZOMBIE BOTNETS

Alana Maurushat[*]

Abstract

Zombie botnets are the greatest Internet threat of the current generation. Botnets are said to be involved in most forms of cybercrime and civil wrongdoing ranging from sending spam, to denial of service attacks, to child pornography distribution to key-logging technology and traffic-sniffing which captures passwords and credit card numbers. This article traces the rhetoric of the term zombie in the world of computer security, describes the inner workings of a botnet, and argues that one method of botnet curtailment will be through Internet Service Provider bot remediation programs that slow down the propagation methods of botnets and act as a catalyst to clean up infected computers.

DOI: 10.2966/scrip.070210.370

[*] Lecturer, Deputy Director of the Cyberspace Law and Policy Centre, and PhD Candidate – all within the Faculty of Law, the University of New South Wales. The subject of the author's PhD is botnet policy.

"It is a truth universally acknowledged that a single man, in possession of a good fortune, must be in want of a wife."

Pride and Prejudice by Jane Austen

"It's a truth universally acknowledged that a zombie in possession of brains must be in want of more brains."

Pride and Prejudice and Zombies by Seth Grahame-Smith & Jane Austen

"It's a truth universally acknowledged that a botnet in possession of zombies must be in want of more zombies."

Zombie Botnets by Alana Maurushat

1. Zombie Botnets

The term 'zombie' has been appropriated by the computer security community as colloquial jargon for a compromised computer in a botnet. The reference of 'zombies' to botnets has been used humorously in writing on botnets:

> In *The Night of the Living Dead*, zombies sucked brain matter in a frenzied hunger. In the computer world, a Trojan can be used to turn your PC into its own computing matter – turning it into a zombie machine. Once under the control of such an illicit program, the Trojan can be accessed by attackers intent on any number of ominous deeds.[1]
>
> "Zombies are coming; not for your brains but for your computer."[2]

While the term 'zombie' is still used in association with botnets, the rhetoric among computer security experts has shifted from this fun and humorous term to one which better connotes the serious problem of botnets. The term "bot" or "compromised computer" is replacing "zombie" in much of the botnet research and writing, including my own research and writing. My own personal reluctance to use the term "zombie" stems in part (I must confess) from my personal disdain for horror films and the monster genre (as evidenced by my reference to classical literature and Jane Austen) but more importantly, from my experience in researching botnets and crime. I find it difficult to associate over-dramatised horror films and humour with a tool that is used to distribute child pornography, launch distributed denial of service attacks, steal personal information and perpetrate fraud, and to launch cyber warfare attacks,

[1] M Landesman, "Haunting Thought: Is Your PC a Zombie?", available at http://antivirus.about.com/od/whatisavirus/a/zombiepc.htm (accessed 4 May 2010).

[2] A Saenz, "Beware the Botnets-Zombie Cyber Attacks" (4 Mar 2010), available at

http://singularityhub.com/2010/03/04/beware-the-botnets-zombie-cyber-attacks/ (accessed 4 May 2010).

especially where cyber warfare is followed by an actual war.[3] While it's a truth universally acknowledged that a botnet in possession of zombies must be in want of more zombies, for the purpose of this article, I'm afraid the term "zombie" stops here and will be replaced with either "bot" or "compromised computer".

A botnet is a collection of remotely controlled and compromised computers known as bots controlled by a bot master / botherder that installs software (typically malicious) on the bots computer and performs acts, nearly always criminal, using the innocent bot computer.[4] All the while, owners sit complacently unaware of the demon seed residing underneath their keypads. In a metaphorical sense, a botnet parallels a mode of distribution. Botnets may involve anywhere from a few hundred bots to several thousand to one documented case involving 13 million bots.[5] Bots receive their instructions from the bot master in the form of a bot (malicious software). The bot must retrieve its instructions from what is known as the "command and control" (C & C) of the botnet. This often occurs in the Internet Relay Chat server or a set of designated domain names allowing a botmaster or a bot herder to control the bots remotely to perform activities which tend to be of a malicious nature. Other botnets leverage peer-to-peer networks and computer game consoles for their command and control locations.

Why do botnets matter? Botnets are said to be involved in *most forms* of cybercrime and civil wrong ranging from sending spam, to denial of service attacks, to child pornography distribution, to worm propagation, to click-fraud, to keylogging technology and traffic sniffing which captures passwords and credit card information, and to mass identity theft. [6] In the words of leading botnet researcher Jeremy Linden of Arbor Networks, "Almost every major crime problem on the Net can be traced to them."[7] Internet security guru Vincent Cerf[8] has equated botnets to a pandemic,

[3] The cyberwar attacks which affected much of Georgia's critical infrastructure preceded the invasion of Russian into Georgia in 2008. See the *Washington Post*'s recount of the event: K Hart, "Long-time Battle Lines Are Recast in Russian and Georgia Cyberwar" (9 Aug 2008), available at http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html (accessed 4 May 2010).

[4] According to Clarke, bots and botnets are explained as: "(Generally, a program that operates as an agent for a user or another program. More specifically:) software that is capable of being invoked remotely in order to perform a particular function. (Typical functions include emailing spam or repetitively sending messages to a target device in order to overload it and thereby deny service; but also despatch of meta-data for files held on the device. A device on which a bot is installed is called a zombie. A set of devices on which bots are installed is called a botnet. Generally intended for largely automated operation, but under the control of a person who may be called a botnet master or botnet herder)." See: R Clarke, "Malware Glossary", available at http://www.rogerclarke.com/II/MalCat-0909.html (accessed 8 Mar 2010).

[5] The Mariposa Botnet is said to have had 13 million zombies. See J Finkel (of *Wired Magazine*) "Spain Busts Hackers for Infecting 13 Million PCs" (2 Mar 2010), available at http://www.wired.com/threatlevel/2010/03/spain-busts-hackers-for-infecting-13-million-pcs/ (accessed 21 April 2010).

[6] T Rychlicki, "Legal Issues of Criminal Acts Committed Via Botnets." (2006) 12 *Computer and Telecommunications Law Review* 161-167.

[7] Quote taken from S Berinato, "Attack of the Bots" 14.11 *Wired Magazine* (November 2006).

[8] Vincent Cerf in many ways is "Father Internet". This is not surprising given that he was involved in the original ARPANET project, was Chair of ICANN, has worked at a number of internationally

warning that a quarter of all personal computers have already become bots.[9] Botnets are perceived by many experts as a pandemic yet most users are unaware of the term or the threat that botnets pose to the Internet.[10]

More compelling is the description of botnets, compromised computers and related crimes from someone within the inner workings of the commercial child pornography industry. The article, "My Life in Child Pornography" was posted to the wikileaks site and is considered by many security experts and cybercrime researchers to be accurate and authoritative.[11] The anonymously written document was translated from German to English. A relevant excerpt is copied below:

> But how, specifically, child pornography is sold? ... Today, the answer is SPAM.... In order to send spam Trojan-infected (zombie) computers are used. But zombie computers have yet another use: it will be used in a targeted fashion to steal identities. They even use the computer of the user whose identity is stolen to conduct credible transactions such as purchase of domains, etc. But that is not everything: the installed Trojans are sometimes used as a SOCKS proxy to upload CP. The Russians have even worked out a schema to use infected computer as a network combing these infected computers (each computer would be part of a huge, redundant cluster) as a kind of huge, distributed and remote servers can be (a kind of Freenet Project, however, by using infected computers as the nodes). I want to make one thing clear: if you have an email address, there is a possibility that there is child pornography on your computer because you have received CP advertising. And if your computer is not 100% safe against Trojans, viruses and rootkits, there is the possibility that your computer is part of the vast child pornography network.

For those readers having difficulty with the technology, allow me to put it into layman's terms. Once a computer is a bot, it can be used in every illegal function of the child pornography distribution chain. This includes SPAM botnets which may contain links to child pornography, links found within SPAM messages which trigger the downloading of malicious software (malware). The malware infects your computer and takes it over without your ever knowing that it has done so. Your banking details are stolen. Other items related to your identity are stolen (e.g. usernames and passwords, so your email address is highjacked). The stolen identity (email and credit card details) are then used to register and purchase domain names, to launder money, to store child pornography, and to distribute child pornography. All of this done typically in a manner so that the user has no idea that their computer is a

reputed universities, and has held key positions at IBM and Google. He is considered to be one of the most influential researchers in computer science and the internet.

[9] Presentation given at the World Economic Forum 2007. The statistics have been highlighted in a number of news reports and blog sites. See, for example, N Anderson, "Vint Cerf: one quarter of all computers part of a botnet" (25 Jan 2007; *Ars Technica*), available at http://www.arstechnica.com/news.ars/post/20070125-8707.html (accessed 4 May 2010).

[10] D Barroso (of the European Network and Information Security Agency), *Botnets – The Silent Threat* (2007), at 6 (available at http://www.enisa.europa.eu/act/res/other-areas/botnets/botnets-2013-the-silent-threat (accessed 29 Jan 2010)).

[11] B Schneier, "The Techniques for Distributing Child Porn", available at http://www.schneier.com/blog/archives/2009/03/the_techniques.html (accessed 4 May 2010).

bot, not to mention that child pornography and other nefarious materials are being stored and later distributed using your computer.[12]

Governments and organisations are beginning to recognise the importance of tackling botnets. The problem of botnets is described by the European Network and Information Security Agency as:[13]

> Botnets represent a steadily increasing problem threatening governments, industries, companies and individual users with devastating consequences that must be avoided. Urgent preventive measures must be given the highest priority if this criminal activity is to be defeated. Otherwise the effect on the basic worldwide network infrastructures could be disastrous.

Governments are focusing much attention on cyber security and cyber crime with botnets driving many initiatives. The United States, the United Kingdom and Australian governments have all announced major cyber security strategies in 2009 with botnets featured predominantly.[14]

2. Combating Botnets

The following diagram explains a botnet. In Step 1, the botnet herder needs to acquire bots to form part of his/her botnet. This may be done in a variety of ways but it is often done with malicious software that self-replicates known as a worm. The computer becomes infected and a bot subject to the commands of the botnet herder. In Step 2, the botnet herder then uses software to command the bot to perform certain actions. The software instructs the bots to retrieve updates from the Command and Control (C & C) of the botnet. The C & C may be located in websites, through keyword search engine, in the Internet Relay Channel, in peer-to-peer channels or more likely, a combination of all of the above. In a typical botnet, there will be several Command & Control locations to retrieve instructions. Many botnets will change the location of the C & C every week, others every day. Webpages of C & C are typically registered with domain name registrars that are known to be lax in their practices and uncooperative with security researchers and law enforcement in either blacklisting or domain name removal. Many of these reticent domain name registrars are located in countries with no cyber crime laws. Knowledge as to where the C & C is located does not produce information about the identity of a botnet master. Many

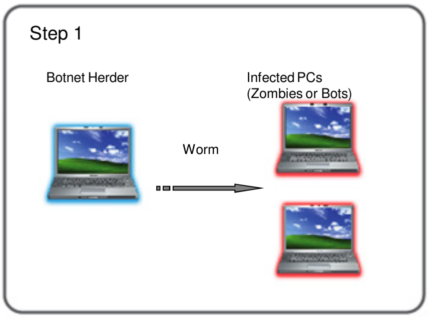
[12] Child pornography was found on the sub-directory of a Queensland dentist in Australia. It was revealed to the public when the Australia's Internet filter blacklist (a list of websites hosting child pornography that are blocked by the filter) was leaked to wikileaks. It is suspected that the material was placed there by a botnet.

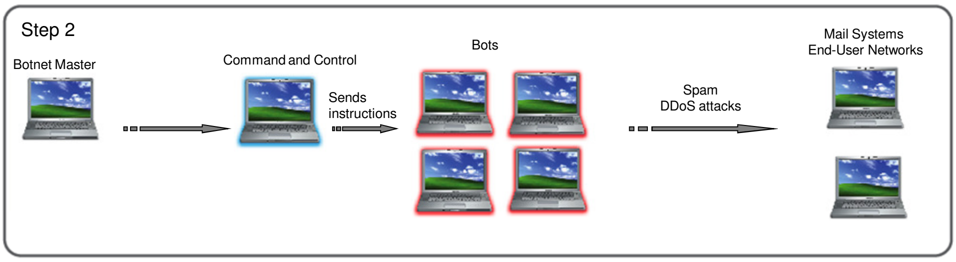
[13] Barroso (ENISA), see note 10 above.

[14] United States Government, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009), available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed 29 Jan 2010); United Kingdom Office of Cyber Security, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (2009), available at http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf (accessed 29 Jan 2010); Australian Government, *Cyber Security Strategy* (2009) available at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf (accessed 29 Jan 2010).

botnet masters use a dynamic system in which their IP address changes every 20 minutes. Additionally, many communications sent to the C & C are encrypted and thus not easily detectable. Tracing back to an individual botnet master is virtually impossible. Where a C & C is shut down, most botnets are programmed to automatically receive its instructions from a new C & C location, or from a set default. Many botnets contain hundreds of thousands if not millions of infected bots.

The botnet herder may issue commands or he/she may hire out the botnet to third parties for nefarious purpose such as to send illegal spam, click fraud, install Trojans to steal usernames and passwords later used for fraud and identity theft, or to launch a distributed denial of service attack.





There are approximately four methods of tackling botnets which I will refer to as:

1) ISP and/or domain name service (DNS) registrar disconnection of C & C when located on webpages,

2) Infiltration and disruption of the C & C in IRC or P2P channels (typically by security organisations),

3) Prosecution of the botnet herder(s), and

4) Bot remediation (typically by the ISP).

Each of these methods requires some elaboration as to the architectural structure of the botnet and the role of the parties in dismantling the botnet.

3. ISP and/or DNS Registrar Disconnection of C & C locations

The first method involves contacting the DNS registrar or ISP to inform them that they have clients who use their services to run botnets. Where a botnet is programmed to receive its instructions (C & C) from a website, a request may be made for disconnection of service or the ISP may blacklist the range of unique Internet Protocol Addresses the botnet is using to run its C & C. The DNS registrar may also be contacted with a request to remove the domain name from its register. This can be an effective route but requires the person to know the webpage the botnet is connecting to to receive its instructions (C & C), the DNS/IP address of the IRC server, port and nickname of the bot, and most importantly, it requires desire on the ISP or DNS registrar to take action.

There is no legal obligation for ISPs and DNS registrars to take any action to disconnect the webpage or remove the domain name. That said, many DNS providers and ISPs do not tolerate abuse of their service and will take measures to stop the botnet by blacklisting the IP addresses where the C & C receives its instruction or termination of their connection contracts. This approach, however, is not always possible for a number of reasons. The service provider may have legal obligations that restrict its ability to disconnect or blacklist to situations where the terms of use are violated. This is not always easy to prove with botnets. The diversification of IP addresses and webpages across multiple ISPs and DNS registrars and even jurisdictions may make this approach unfeasible. For example, where a botnet has multiple channels for receiving its instructions, several hundred ISPs may need to be contacted across different jurisdictions. Any action taken would require disconnection by ISPs at the same time. Otherwise the botnet merely selects another channel to receive its C & C. Botnet could be set to receive instructions through multiple channels: webpages, search engine keywords, IRC, and P2P. Where the C & C is located in a P2P channel, ISPs do not play a role. The instructions could be embedded in an innocent party's webpage such as CNN. The ISP will not disconnect an innocent party though they may be in a good position to contact and inform the innocent third party that they are being used as part of a botnet.

4. Infiltration and Disruption of the C & C in IRC or P2P Channels (Typically by Security Organisations)

The second method has security researchers[15] running interference with the C & C of the botnet. This might include infiltrating the C & C and initiating commands of their own, thereby disrupting the botnet. In some instances, the individuals may elect to launch a Distributed Denial-of-Service (DDoS) attack on webpages where the C & C receives its instructions. Again, this disrupts the botnet. This type of approach, however, requires perpetual observation and constant attention by the individual or organisation disrupting the botnet. It does not permanently shut down the botnet. It is neither desirable nor practical and, in the case of a DDoS attack, it is outright illegal as it would constitute a computer offence of /illegal access, interception or interference to a computer or data held in a computer.[16] Self-defence would likewise not apply in this situation as botnet activists are often not defending their own property but, rather, the property of third parties. Moreover, where C & C is embedded into innocent third party websites, the extent of tolerated interference significantly diminishes.

[15] The term 'security researchers' is used broadly here. This may include security organisations, security experts, individual researchers, security companies or simply hacker activists.

[16] The *Council of Europe Convention on Cybercrime* uses the language in Articles 4-6 of illegal access and interference whereas in Australia, for example, the terminology is one of unauthorised access, modification or impairment as found in the *Criminal Code 1995 (Cth)*, s 476.

Botnets, by and large, are dismantled through the efforts of security organisations. In some instances, this may involve formal participation by computer companies such as Microsoft and Panda Labs or it may be done by security activists such as those members of Zert or it may be through security researchers at universities, and is often the case, it is a collaboration of many types of organisations.[17]

5. Prosecution of Botnet Herder

This method looks at prosecution of a botnet herder. In order to prosecute a botnet herder, you must first make an identification of the botnet herder. This is an extremely difficult task. Several factors must be present in order to identify a botnet herder:

- The IP address of the IRC server must be known along with the port, and nicknames of the bot
- The IP address may be traced to the ISP or DNS registrar
- The ISP or DNS registrar would have to provide subscriber information (either voluntarily or through a production order to disclose subscriber information and data traffic logs)
- The subscriber information would have to be truthful and accurate in order to correctly ascertain the identity of the botnet herder
- Evidence would need to be collected before proceeding to press charges

An order to produce subscriber information would, in most instances, be imperative to a successful prosecution of a botnet herder. The reality, however, is that many criminals do not use their real identities to subscribe to Internet services, or they register the services under an empty holding company.[18] To add to this, stolen credit cards are often used as payment for many Internet services. The reality is that traceback of a botnet herder, depending on the sophistication of the botnet and the efforts of the botnet herder to remain anonymous, is in many instances very difficult. Where botnet herders use obfuscation tools such as proxies, fast-flux, P2P and dynamic DNS, traceback is almost impossible. The sophisticated botnet herders are believed to be connected to organised crime. The less sophisticated groups tend to leave evidence by lingering in chatrooms using their hacking names, discuss botnet techniques, and leave C & C channels open for long periods of time.[19] Traceback of this type of botnet herder is more probable. Without successful traceback, a botnet

[17] Pandalabs was heavily involved in the takedown of the Mariposa botnet. Microsoft was heavily involved in the takedown of the Waledec botnet. Law enforcement, and a number of international computer security organisations and university researchers aided Microsoft and Pandalabs in the takedown of these botnets. See: "Waledec Questions Answered", available at http://www.lavasoft.com/mylavasoft/company/blog/waledec-questions-answered (accessed 4 May 2010); L Corrons, "Mariposa Botnet" (3 Mar 2010), available at http://pandalabs.pandasecurity.com/mariposa-botnet/ (accessed 4 May 2010).

[18] I-defense, for example, documents several holding companies in Hong Kong as being used to register many Internet webpages, IP addresses etc. for organised crime. See E Jellenc and K Zenz, *Global Threat Research Report: Russia* (2007), available at http://versign.com/static.042139.pdf (accessed 20 Apr 2010).

[19] N Provos and T Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection* (Harlow: Addison Wesley, 2007).

herder cannot be identified and there can be no prosecution. Where prosecution is an option, you are often dealing with either a lower level amateur botnet herder or a botnet master located in a cybercrime safe haven. This type of botnet master typically takes fewer precautions to shield their identities as well as the operation of their botnets. Botnets linked with organised crime often operate in stealth mode where they are difficult to detect by both technologies and law enforcement.

6. ISP Bot Remediation

The last approach involves remedying the compromised computers that the botnet has control of - known as 'bot remediation'. In Seth Grahame-Smith's mash-up, *Pride and Prejudice and Zombies*, the author uses the passages of Jane Austen's famous book and interjects the narrative with a separate zombie plot. As the book's scenario states:[20]

> As our story opens, a mysterious plague has fallen upon the quiet English village of Meryton – and the dead are returning to life! Feisty heroine Elizabeth Bennet is determined to wipe out the zombie menace, but she's soon distracted by the arrival of the haughty and arrogant Mr. Darcy. What ensues is a delightful comedy of manners with plenty of civilized sparring between the two young lovers – and even more violent sparring on the blood-soaked battlefield as Elizabeth wages war against hordes of flesh-eating undead.

In much the same way as Elizabeth Bennet and her cohorts must deviate from their intended romance plot to one of tackling flesh-eating zombies, ISPs are increasingly being asked to address computer security issues, including botnets, in addition to their core of providing telecommunication infrastructure and as conduits of communications.

As long as a botnet herder has bots waiting to receive instructions and carry out commands, a botnet is still susceptible to receiving new instructions to perform malicious activity while most botnets are self-replicating. The question then becomes how we are to successfully reduce the number of bots. Some alternatives look at requiring users to have a computer license before they are allowed to connect to the Internet.[21] Another option would require every computer sold to have pre-installed anti-virus software before it can be connected to the Internet.[22] However, anti-virus software only blocks a certain percentage of malicious traffic, and is reliant on the end-user patching their systems (browser, router, hardware) on a frequent basis.[23] Once a user's machine is infected and part of a botnet, he or she is likely to be unaware that the computer has been compromised. If a user is aware of the infection, it is extremely unlikely that that awareness will extend to whether the machine is

[20] S Grahame-Smith and J Austen, *Pride and Prejudice and Zombies* (Philadephia: Quirk Productions, 2009).

[21] L Edwards, "Dawn of the Death of Distributed Denial of Service: How to Kill Zombies" (2007) 24 *Cardozo Arts and Entertainment Journal* 23-29.

[22] *Ibid.*

[23] R Clarke and A Maurushat, ""Passing the Buck: Who Will Bear the Financial Transaction Losses from Consumer Device Insecurity?" (2008) 1 *Journal of Law, Information Technology and Science* 8-57.

being used to commit crimes. User education, therefore, is a must in any effort to better secure the Internet. There is a growing recognition that ISPs are in the best position to assist in bot removal. In Australia for example, it has been suggested that ISPs must be active not only in the removal and remedying of their customer's compromised machines but must also play a role in educating users on safer online habits.

Internet Service Providers have taken an increasingly active role in combating botnets and malicious activity. ISPs have typically placed a strong emphasis on filtering spam botnets. This has predominantly taken shape through sophisticated spam filters known as ingress and egress filtering. Ingress filtering refers to filtering packets as they enter into a system whereas egress filtering refers to filtering packets as they exit a network system.[24] The result is that much spam content does not arrive in one's "INBOX" but finds its way to the "BULK" or "SPAM" folders on a user's computer. This preventative measure merely quarantines the undesired content to a place where users may still access the files. This technique, while mitigating against some malicious activity, does not address the larger problem of what needs to be done once a machine is infected and part of a botnet. Many ISPs and organisations also block port 25. Much spam and malicious traffic is routed through port 25, therefore, it is thought that blocking this port reduces the problem of unwanted content distributed through botnets. As articulated in the ITU Botnet Mitigation Toolkit document, "attempting to combat botnets simply by blocking port 25 has been compared, colourfully (and validly) by one expert to "treating lung cancer with cough syrup"." Only a portion of malware travels through port 25 while malware actors may simply re-channel traffic through another port. Not all ISPs do any ingress and egress filtering for malicious content, nor do they all block port 25.

ISPs are generally not responsible for the security of their customer's computers or for monitoring the content that their customers place and distribute online. ISPs are generally seen as 'mere conduits' of information where they have not traditionally examined the content flowing through their networks.[25] The role of ISPs, however, is changing. ISPs often filter spam botnets, block problematic ports, and they will be filtering RC classified content under the Government's proposed Internet filtering scheme. The next proposed change is the role of the ISP to tackle botnets more generally as ISPs are seen as critical players in any successful initiative in the area.

There are proposals for ISP Bot Remediation programs. The American ISP, Comcast, has a bot remediation program. Comcast is one of the largest ISP providers in the United States capturing over 14% of the United States market.[26] Comcast is an innovator in the remediation of bots over its network. Based on its experience with methods used to remediate bots, the company has written an informal document for

[24] D Barroso, see note 10 above, at 6.

[25] Report written for Google: C Lumby, J Hartley and L Green, "Untangling the Net: Mandatory Internet Filtering" (Dec 2009), available at http://www.cci.edu.au/sites/default/files/alawrence/untanglingthenet_report.pdf (accessed 21 Apr 2010).

[26] *ISP-Planet* puts Comcast in at 14.7% in quarter 3 of 2008 while *Stat-Owl* puts Comcast in at 14.26 in July 09. See: http://www.isp-planet.com/index.html (accessed 29 Jan 2010) and http://www.statowl.com/network_isp_market_share.php (accessed 29 Jan 2010), respectively.

consideration as an informational-Request for Comment (RFC).[27] The document is an Internet-draft and has not at this point been placed on the Internet Engineering Task Force (IETF) standards track.[28] An Internet standard refers to "a specification produced by the IETF that has progressed through its standards development process to the final stage."[29] Standards do not have the effect of a legal rule, but are generally complied with because they are of a "high-quality, are timely, widely supported, and represent a high level of technical consensus amongst a broad group of experts and users."[30] The document is being considered as an informational-RFC. An informational-RFC is a working draft that is intended to become an RFC, then a proposed standard and possibly a standard. The Comcast document is merely a working RFC at present but will potentially become an Internet standard. The Comcast draft, therefore, is document that is highly relevant to the discussion of bot remediation.

The Comcast document is best described by the contents of its abstract:

> This document contains recommendations on how Internet Service Providers can manage the effects of computers used by their subscribers, which have been infected with malicious bots, via various remediation techniques. Internet users with infected computers are exposed to risks such as loss of personal data, as well as increased susceptibility to online fraud and/or phishing. Such computers can also become an inadvertent participant in or component of an online crime network, spam network, and/or phishing network, as well as be used as a part of a distributed denial of service attack. Mitigating the effects of and remediating the installations of malicious bots will make it more difficult for botnets to operate and could reduce the level of online crime on the Internet in general and/or a particular Internet Service Provider's network.

In Australia, the Internet Industry of Australia has put forth a draft code on bot remediation.[31] The IIA E-Security Code provides guidance to ISPs in order to perform four functions. They are:

- Detect malicious activity on a customer's compromised computer;
- Take steps to respond to the AISI reports or any other source of information that may relate to malicious activity;
- Inform a customer as to what actions they can take to protect their computers from malicious activity; and

[27] *Comcast's Recommendation for the Remediation of Bots in ISP Networks*, available at

http://tools.ietf.org/html/draft-oreirdan-mody-bot-remediation-03 (accessed 4 May 2010).

[28] According to Jeremy Malcom, "the IETF, as the body responsible for the development of a large majority of such standards, it is unquestionably the Internet's pre-eminent standards development body." J Malcom, *Multi-Stakeholder Governance and the Internet Governance Forum* (Perth: Terminum Press, 2008), at 51.

[29] J Malcom, *Multi-Stakeholder Public Policy Governance and its Application to Internet Governance Forum* (2008), available at http://www.malcolm.id.au/thesis/ (accessed 4 May 2010).

[30] *Ibid*, at 51.

[31] Internet Industry Association, *Internet Service Providers Coluntary Code of Practice for Industry Self-Regulation in the Area of e-Security* (September 2009) [IIA E-Security Code].

- Notify Australian authorities of a malicious activity without prejudice.

No agreement has yet been made amongst stakeholders as to what modifications, if any, will be made to the Internet Industry Code of Practice in order to achieve the objectives. The following commentary is merely an example of how a bot remediation program might operate. An ISP would use live forensics to detect and monitor malicious activity over its network or the ISP would receive reports from third party organisations that perform security monitoring. Such detection and monitoring would identify computers connected to an ISP's network that are bots, and those computers that are likely to become bots in the near future. Computers without updated anti-virus and anti-spyware technologies, for example, are ripe targets for takeover. After identifying such computers, the ISP virtually quarantines the compromised computer or computer at risk. By this, the ISP could suspend a user's connectivity until otherwise notified by the customer that they had remedied their computer. A method in a similar vein that is gaining more popularity is the placing of customers in a "walled garden".

> A walled garden refers to an environment that controls the information and services that a subscriber is allowed to utilize and what network access permissions are granted. This is an effective technique because it could be able to block all communication between the bot and the command and control channel, which may impair the ability of a bot to disrupt or block attempts to notify the user.[32]

A walled-garden is the equivalent of being pulled over while driving for having a vehicle that, unbeknownst to you, is unfit and dangerous. The car is then placed in a tow lot or is towed to a mechanics garage for repair. The car is not allowed on the road while it is not safe. Once the car has been fixed by a mechanic and deemed fit for use, the owner is once again able to drive the car. The inability to use the dysfunctional car is, of course, an inconvenience to the owner but these measures are taken because motorway safety is thought to trump other considerations. Walled-gardens are similar. When a computer is compromised, the ISP restricts its use. This is like being placed in a virtual tow lot. The user is still able to perform certain functions with the computer, just as a driver would be able to sit in the car, listen to the stereo, turn it on to run air conditioning, and so forth. Only the hazardous services are restricted until a computer is remedied.

Once the user of the compromised machine has taken measures to ensure that the machine is no longer compromised and, therefore, no longer a bot connected to a botnet, he is able to use the Internet again. This may involve the ISP directing the user to trusted computer security websites that provide user education and information about how to de-bot the machine.

Unfortunately, bot removal may be beyond the ability of many users. It may be the case that bot removal requires specialised knowledge and skills. The reality is that attempts to remove bots may prove unsuccessful or only partially successful. Comcast states that "the only way a user can be sure they have removed some of today's increasingly sophisticated malware is by 'nuking-and-paving' the system: reformatting the drive, reinstalling the operating system and applications (including

[32] Comcast, see note 27 above.

all patches) from scratch, and then restoring user files from a clean backup".[33] ISPs who have used bot remediation programs, such as Comcast in the United States, Rogers in Canada and Australian ISPs have not published any statistics on the effectiveness of bot remediation programs.

Comcast notes that bot remediation programs "may leave a user's system in an unstable and unsatisfactory state or even in a state where it is still infected [and] ... attempts at bot removal can also result in side effects ranging from a loss of data or other files, all the way through partial or complete loss of system usability." [34] Again, the effectiveness of such bot remediation programs should be analysed against any damages and side-effects of a program. Currently the IIA Code does not provide for review of the program in order to ensure its effectiveness.

Recidivism refers to the recurrence of infection in a remedied machine. Compromised machines are cleaned and basically re-infected. According to the ITU, the Internet Architecture Board considered the issue at a workshop on "Unwanted Internet Traffic".[35] The IETF noted that notifications by ISPs would likely have a limited impact on user's remedying their machines. Users might ignore the notification, or clean their machine only to become re-infected within a short period of time. Notification where coupled with a mechanism designed to illicit expedient customer action such as speed throttling, walled gardens, and suspension of services and ultimately, termination of services where machines are unremedied, will prove more effective than mere notification with a link to how to clean up a machine. It is possible that machines will become re-infected once cleaned up. By installing anti-virus software and software to update routers and operating systems, the likelihood of re-infection is reduced significantly. One must remember that ISP involvement will be infinitely more effective with an overall cyber strategy where multiple-enablers, along with law enforcement agencies are involved. Changes, for example, to domain name resolving, along with changes to law enforcement**,** and additional regulatory changes to financial enablers will form an overall cyber strategy that will hamper botnet proliferation and the commercial malware industry in general. These areas, however, fall outside of the scope of this article.

7. The Botnet That Never Dies

The last method differs from the first three in one significant manner. It potentially remedies compromised machines. This is critical for long term takedown of a botnet.

The first two methods (ISP and/or domain name service (DNS) registrar disconnection of C & C when located on webpage, and Infiltration and disruption of the C & C in IRC or P2P channels), only puts off the botnet herder for a period of time. The botnet herder can still set up new C & C channels, and write new bots (malicious software programs) to communicate with the zombie computers. The takedown of the botnet is, therefore, only temporary as most botnets are self-

[33] Comcast, see note 26 above.

[34] *Ibid*, at 7.

[35] *ITU Botnet Mitigation Toolkit: Background Information* (January 2008), at 32. The Article refers to IETF's Internet Architecture Board workshop on "Unwanted Internet Traffic". The workshop proceedings are summarized in RFC 4984 and are available at http://www.isi.edu/in-notes/rfc4948.txt (accessed 29 Jan 2010).

replicating worms. This means that stopping the C & C of the botnet does not necessarily prevent the botnet from continuing to spread and thus acquiring new zombie computers. It also does not prevent a botnet from spreading new bots once a new C & C is established. Prosecuting the botnet herder is also not an absolute solution as the botnet is highly susceptible of being taken over by another botnet herder. Moreover, the zombie machines sit dormant awaiting new instructions. Only the last method, zombie/bot remediation, potentially removes the zombie computers from the equation. To use an analogy to war, one can disrupt an army by interfering with its communications systems, and one can kill the General but there will always be more Generals willing to step up, and ways of re-establishing communications. But if there are no soldiers, the General has no one to carry out the orders in his command.

8. Concluding Remarks

"An accomplished woman is one who has a thorough knowledge of music, singing, drawing, dancing and the modern languages; she must be well trained in the fighting styles of the Kyoto masters and the modern tactics and weaponry of Europe."[36]

In much the same vein, an accomplished botnet dismantler is one who has a thorough knowledge in malware, command and control in IRC and P2P, dynamic DNS, fast-flux, and contacts with ISPs; she must be well trained in the fighting styles of the botnet masters and the modern tactics and weaponry of the cyber underworld.

[36] S Grahame-Smith and J Austen, see note 20 above.