EJLT European Journal of Law and Technology

Battling Botnets with Digital Rights in Mind

Aaron Martin [1], Norberto Nuno Gomes de Andrade [2]

Cite as: Martin, A. K, Andrade, N. N. G.de, ‘Battling Botnets with Digital Rights in Mind’, European Journal for Law and Technology, Vol. 3, No. 2, 2012

Botnets pose an increasingly sinister threat to the security and trustworthiness of the digital environment. Bots are computers that have been hijacked by malicious software without their owner's awareness. Through that malware, a person – or even another machine – gains remote control over a computer. When the hijacker connects the bots, the resultant network, or botnet, co-opts thousands upon thousands of machines, forming a powerful supercomputer that can be unleashed to send spam or execute distributed denial-of-service (DDOS) attacks, or to commit identity theft and commercial fraud. Ultimately, botnets allow controllers to mount large-scale attacks without purchasing the vast computing power needed to do so. More poignantly still, botnets operate by turning the virtues of openness and connectivity into vulnerabilities.

Botnets compromise the privacy and confidentiality of those who use and communicate through a hijacked computer, but they provide a nearly impenetrable shield of anonymity for the hijackers themselves. Even skilled victims may find it difficult to identify the origins of the infection vector and it is seldom possible to follow the trail all the way back to the original malefactor. These anonymity benefits are so profound that botnets have become a preferred tool for cyber criminals. They provide low-cost, high-profit opportunities with only a miniscule risk of identification, sanction, punishment or arrest. [3] This boon has fuelled a thriving marketplace, where the technology and expertise required to co-opt thousands – even hundreds of thousands – of personal computers, can be bought, sold, rented and leased.

There is an inverse correlation between the advantages botnets offer to criminals and the dangers they pose to the digital economy. The use of e-commerce, e-government, and other Internet-based services, which depend on trust and confidentiality, decreases when users doubt their security, integrity and functionality. And as more and more facets of everyday life move online, the continued presence of malware and botnets will have an even larger impact on our activities. In the past the defence against botnets was reactive and disorganised. An investigation would be launched and networks would be recalibrated to defend against the particular attack that had been used. Nevertheless, botnets could easily continue to pursue their nefarious goals with a sense of impunity, as only a slight modification of the malware would be needed to evade existing defences, thus revitalising the whole cycle of attack and remediation. Today, counter-botnet operations tend to be better structured and organised, deploying collaborative efforts that stress proactive and co-ordinated strategies. These strategies often depend on the co-operation of private, for-profit Internet Service Providers (ISPs), which may not view the eradication of botnets as their responsibility.

Yet ISPs have the potential to play a decisive role in the defence against malevolent botnets. First and foremost, these service providers act as a conduit for most of the online traffic that botnets exploit. In fact, a recent analysis discovered that about half of all botnet-affected machines in the world access the Internet through just 50 ISPs. [4] In addition, since ISPs provide consumers with access to the Internet, they have the contacts and capacity to raise public awareness. This allows ISPs to disseminate information about attacks and to help consumers adopt better personal online security practices. Enlisting ISPs as a lead actor in the battle against botnets is not an entirely straightforward proposition. Strictly speaking, ISPs are responsible for providing access to the Internet, and not necessarily for mediating, regulating or safeguarding customers who purchase that access. The cost of policing connections may dissuade ISPs from participating. Moreover, the attribution of the role of botnet cop – and the burden to develop the capacity to do so – could turn some ISPs into improvised censors of online activity. This is a fact that raises important legal and regulatory questions, particularly from a privacy and data protection point of view.

Though the risks to ISPs are formidable, ISPs could also reap considerable gains from joining the crusade against botnets. The retreat of botnets would allow ISPs to enhance network performance by first managing and then reducing the number of compromised connections on their networks. This would not only provide for a higher quality of customer service, but would also buttress ISP brand equity in vulnerable areas like security, privacy and confidentiality. Heightened user confidence should lead to higher usage, which is always good business for ISPs. Fewer botnets would also mean fewer technical support requests from affected clients, and this in turn translates into lower customer service costs, and therefore higher profits.

Governments are starting to realise that ISPs have much to gain from the broader public benefit of botnet reduction. Several countries, including Australia, Germany, Ireland, Japan, Korea, the Netherlands, the United Kingdom and the United States, are therefore forging partnerships with ISPs to harden the Internet against botnet attacks. Sometimes, the result is an ISP-led initiative and sometimes it is a public-private partnership covering a range of potential activities, including efforts to identify compromised machines through data-sharing between ISPs, or between an ISP and a national Computer Emergency Response Team. Other tactics involve the use of honeypots, DNS sinkholes, spam traps, packet sniffing and malware analysis, to name just a few techniques. Owners of infected computers are notified by text message or e-mail that their connection has been compromised. Some ISPs prefer an arbitrary password reset to force the customer to call the helpdesk so an agent can explain the situation and advise the customer how to disinfect their machine.

But these proactive approaches are accompanied by several privacy and access-related challenges, especially as ISPs are attributed the role of monitoring Internet traffic by intercepting and analysing network packets. Depending on the ISP's home country, these 'deep packet inspection' techniques may not be unequivocally legal. [5] For example, the Netherlands recently passed 'net neutrality' legislation that strictly regulates how and when ISPs may employ such techniques. [6] In some countries, IP addresses are considered personal information and, as such, are protected under data protection law. This is the case in Germany, where customers' IP addresses are deliberately obscured whenever they are processed at the country's Anti-Botnet Advisory Centre. But in cases where multiple users share a single IP address, more differentiated information like a Media Access Control address may be needed in order to identify a bot. This would greatly increase the privacy risks of the botnet eradication process.

In order to effectively battle botnets without compromising or violating the privacy of the user, ISPs must also learn to distinguish benign anonymity protocols (like Tor) from botnets, even though they may produce similar traffic patterns. [7] [8] ISPs must also be closely supervised to ensure that they apply this distinction where it may be more expedient not to. Finally, legislation and regulation must clarify the power of ISPs to disconnect and quarantine affected machines and to provide for the transparent disclosure of logs and transcripts to prevent ISPs from imposing arbitrary and selective barriers to access for commercial, political or other non-security reasons.[9] These challenges notwithstanding, it stands to reason that if ISP-led anti-botnet programmes are designed with privacy and access concerns in mind, and if they are properly supervised, ISPs, legislators and civil society can mobilise an effective common front to protect against the evident danger of these malicious networks.

Enabling policy frameworks allow ISPs to realise the full potential of their position in the fight against malicious botnets. These frameworks must balance many competing needs: the public's need for secure connectivity must be balanced against the regulatory, oversight and disciplinary needs of the state, which in turn must satisfy the commercial needs of ISPs without transgressing on the privacy and data protection rights that civil society organisations defend in cases where public opinion does not understand the full risk of digitally-mediated crime and subversion. An enduring collaboration amongst the diverse actors in this coalition is possible, but it will not emerge without concerted effort and proactive co-operation. Ultimately, the entire effort depends on the willingness of ISPs to utilise the tools inherent to their business to provide an important public good in such a way that serves their interests and those of the public in equal measure.

[1] Dr Aaron Martin is a Scientific Officer at the Information Society Unit of the Institute for Prospective Technological Studies (IPTS) of the European Commission's Joint Research Centre. He researches technology policy, focusing on the issues of privacy, surveillance and identity. In 2011 he completed a PhD at the London School of Economics and Political Science. He was the main author of the original OECD report that forms the basis of this policy brief: http://dx.doi.org/10.1787/5k98tq42t18w-en

[2] Dr Norberto Nuno Gomes de Andrade (PhD in Law, European University Institute, Florence – Italy) is a Scientific Officer at the Information Society Unit of the Institute for Prospective Technological Studies (IPTS) of the European Commission's Joint Research Centre. His research interests are focused on law and technology, with a special focus on electronic identity, identity management, data protection, privacy, cloud computing, Internet governance and regulation, qualitative policy analysis, foresight and future-oriented technology analysis.

[3] ENISA (2011), 'Botnets: Measurement, Detection, Disinfection and Defence', http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/botnets/botnets-measurement-detection-disinfection-and-defence

[4] Van Eeten, M. et al. (2010), 'The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data', OECD Science, Technology and Industry Working Papers, 2010/05, OECD Publishing. http://dx.doi.org/10.1787/5km4k7m9n3vj-en

[5] Hustinx, P. (2011), 'Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data', European Data Protection Supervisor, Brussels,http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_EN.pdf

[6] Bits of Freedom (2012), 'Netherlands first country in Europe with net neutrality' https://www.bof.nl/2012/05/08/netherlands-first-country-in-europe-with-net-neutrality/

[7] Tor is a free software and open network that helps people defend against forms of network surveillance that threaten personal freedom and privacy, confidential business activities and relationships, and state security. Tor protects users by routing their communications around a distributed network of relays run by volunteers all around the world. See: https://www.torproject.org/.

[8] EFF (2011), 'Comments of Electronic Frontier Foundation In the Matter of Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware, National Institute of Standards and Technology', http://www.nist.gov/itl/upload/EFF-Comments-to-BotNet-RFI_11-4-11.pdf

[9] This concern is especially relevant in light of the recent statements from bodies such as United Nations that link Internet access to fundamental human rights. See La Rue, F. (2011), 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', United Nations Human Rights Council, New York, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf