30

Spam and crime

Roderic Broadhurst and Mamoun Alazab[1]

1. Introduction

Unsolicited bulk, mass emails, or 'spam', pose a global challenge because they form a major vector for the dissemination of malware. Spam takes many forms and has many varieties. Spam can merely carry annoying but benign advertising; however, it can also be the initial contact for cybercriminals, such as the operators of a fraudulent scheme who use emails to solicit prospective victims for money or to commit identity theft by deceiving recipients into sharing personal and financial account information.

Legislation criminalising or limiting spam has been introduced in more than 30 countries (OECD 2004) but there is no mutual agreement on its definition. Spam is difficult to define precisely, but broadly includes any unsolicited electronic message, usually sent as a bulk transmission. Definitions vary depending on whether the emphasis is on lack of consent (unsolicited) or the content of the email. The Australian Communications and Media Authority (ACMA 2004, 2014) defined

1 We acknowledge the assistance of the Criminology Research Council (Grant CRG 13/12-13) and the Australian Research Council. We also thank the Australian Communications and Media Authority (ACMA) and the Computer Emergency Response Team Australia for their assistance in the provision of data and support. We thank our colleagues Peter Grabosky, Khoi-Nguyen Tran, Ki-hong 'Steve' Chon and Brigitte Bouhours for their contributions to the data collection and analysis.

spam as 'unsolicited commercial electronic messages', which may not capture the versatility of spam. Under this definition, a single electronic message can be considered spam if it is unsolicited. On the other hand, Spamhaus (2014) considers an email is spam if it is both unsolicited and sent in bulk.

Despite international efforts initiated under the 2004 London Action Plan On International Spam Enforcement Cooperation[2] to further global cooperation and public–private partnerships to address spam-related problems, spam remains a significant cost and risk (UNODC 2013). The action plan brings together 27 states and agencies (Australia, Belgium, Brazil, Canada, Chile, China, Denmark, Finland, Hong Kong, Hungary, Ireland, Japan, Latvia, Lithuania, Malaysia, Mexico, Netherlands, New Zealand, Nigeria, Norway, Portugal, South Korea, Spain, Switzerland, Sweden, the United Kingdom and the United States), non-governmental agencies (for example, Spamhaus Project, M3AAWG), telecom and information security companies (for example, Verizon, McAfee) and corporate and consumer groups to implement anti-spam activities. The London Action Plan invites and encourages informal cooperation among states. It acts as a clearing house, establishes for each participant a designated contact point for spam-related problems and engages the private sector in anti-spam activities. The plan encourages crime prevention as well as improvements in the investigation of spam-related crimes such as online fraud, phishing and virus dissemination.

Thus, the plan is an example of how informal and pluralistic attempts at regulation of a costly and harmful global activity arise when much of the behaviour occurs beyond domestic borders—outside the sovereignty of the state. When states alone lack the capability to suppress spam, they must rely on mutual interest among states and a host of non-state actors to perform tasks that are usually the province of law enforcement agencies. So, via partnerships, states seek to steer private actors and multinational corporations (especially in information technology and related domains) that often have the means to monitor and interdict to play a regulatory role (see Grabosky, Chapter 9; and Tusikov, Chapter 20, this volume).

2 See: londonactionplan.org/.

Although levels of malicious spam may seem insignificant at the individual level, it is estimated that in 2013, approximately 183 billion emails were sent and received every day, so the number of malicious communications can be substantial. Symantec (2013) estimated that about 30 million spam emails are sent each day, and, as we show, significant proportions include malware. It is not surprising that a huge amount of spam emails are necessary because it has been estimated that, for a spam advertisement to be profitable, one in 25,000 recipients need to open the email and make a purchase in an underground market (Symantec 2008). Spam sent in 2010 earned its operators US$2.7 million (AU$3.5 million) in profit from fake sales in pharmaceuticals alone (Krebs 2012), while the cost of spam to internet services providers (ISPs) and users worldwide reaches into the billions of dollars (Anderson et al. 2013). A recent study on the economics of spam (Rao and Reiley 2012) calculated that spammers may collect gross global revenues of the order of US$200 million (AU$262 million) per year, while some US$20 billion (AU$26 billion) is spent fending off unwanted emails.

Spamhaus, a non-profit spam monitor operating since 1998, maintains the Register of Known Spam Operations (ROKSO) and estimates that about 100 spam operations or spam 'gangs' are active and may be responsible for as much as 80 per cent of the spam present in cyberspace at any one time. These simple and often virtual crime operations may comprise small groups of up to five people who first

> acquire a list of victim email addresses from a specialised harvester, rent a botnet[3] … join a spam affiliate programme and include a link to an illegal market site on his spam emails. (Stringhini 2015: 36)

Once this process is in place, the spammer receives a cut of the affiliate market earnings generated by his/her victims.

Spamhaus can make traces via aliases, addresses, redirections, locations of servers, domains and Domain Name System (DNS) setups to a relatively small hardcore group, who:

3 A botnet is a group of computers that have been infected by some form of malware. They respond to instructions from a remote computer through command-and-control servers, to send bulk spam, make denial of service attacks, install other malicious code (such as fake antivirus software) and steal sensitive information, such as harvested passwords and credit card and bank account numbers, to be used or sold.

> pretend to operate 'offshore' and hide behind anonymity. Some pretend to be small 'ISPs' themselves, claiming to their providers that the spam is being sent not by them but by non-existent 'customers'. When caught, almost all use the age old tactic of lying to each ISP long enough to buy a few days or weeks more of spamming and when terminated simply move on to the next ISP already set up and waiting. (Spamhaus 2015)

Spam emails with hidden malware or uniform resource locators (URLs) that direct users to malware are common methods used by cybercriminals to find new victims. For example, spammers may want to expand their botnets or cybercriminals may use them to propagate their computer intrusion software (that is, software developed as 'crimeware') to harvest passwords, credit card accounts, bank accounts and other sensitive personal information. The need to develop preventive methods to help reduce the propagation of malware via the frequently used medium of spam emails is the focus here. Before presenting our results, we briefly describe our data and how criminals disseminate spam emails.

Unlike 'low volume–high value' cybercrime that targets financial services and requires advanced hacking capability, spam enables malware to reach 'high volume–low value' targets that are less likely to have effective antivirus measures in place. Such malware is distributed through two types of spam: those with an attachment that contains a virus or trojan horse that installs itself in the victim's computer when opened; and those with a hyperlink to a web page where the malware is downloaded on to the compromised computer.

Spam thrives on the acquisition of active email addresses and these addresses are harvested in three different ways: first, by searching for email addresses listed on websites and message boards; second, by performing a 'dictionary attack', which is a combination of randomly generated usernames with known domain names to guess correct addresses; and finally, by purchasing address lists from other individuals or organisations such as in underground markets (Takahashi et al. 2010). Once email addresses are harvested, spammers distribute spam by using botnets, and this technique is used by large spam botnets such as Storm Worm, Grum and Bobax (Stringhini et al. 2012). Spam often contains a malicious attachment or a link to legitimate websites that have been compromised by a web attack toolkit (for example, Blackhole).

Botnet-based spam emerged around 2004 as a novel distribution network and is responsible for almost all large-scale spam campaigns. Beside its potential for crime, spam is problematic because of its sheer volume, which impedes the flow of legitimate internet traffic. Spam volumes are estimated to be about 30 million spam emails each day (Symantec 2013).

A recent innovation involves attacking computers indirectly by concealing intrusions in an intermediary website or 'waterhole'—that is, sites the target is likely to visit and which also host malicious code on the landing page (see Figure 30.1). Cybercriminals also create links in spam messages that point to exploit portals hosting malware—an alternative approach that avoids the need to hack legitimate websites before planting malicious code.

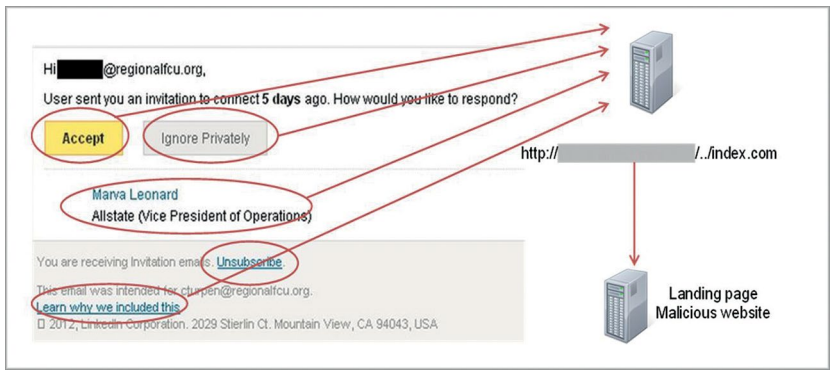

Figure 30.1 Example of a redirection link 'waterhole' attack
Source: Authors' work.

Our analysis shows that 40 per cent of our dataset consists of emails that have been distributed more than 50 times and sometimes more than 1,000 times, suggesting that these spam emails have been sent by different groups, using botnets to distribute them (Alazab and Broadhurst 2016).

2. Dataset and results

We use three real-world datasets (DS) of spam emails collected in 2012. Emails are identified as spam in two ways: first, an email user may determine that an email is spam; second, emails may be collected and identified as originating from known spamming networks. Both scenarios are captured in our real-world DS. For each email, we

extracted attachments and URLs, uploaded them to VirusTotal and scanned for viruses and suspicious content. We considered an attachment or URL to be malicious if at least one scanner showed a positive result.

The first dataset, the HABUL DS from the HABUL Plugin for 'Thunderbird', uses an adaptive filter to learn (machine learn variants of spam text) from a user's labelling of emails as spam or normal email. The second dataset is an automated collection from a global system of honeypots and spam-traps designed to monitor information about spam and other malicious activities, which we labelled the 'Botnet DS'. The third dataset is formed from spam emails reported by Australians and sourced from the spam intelligence DS (provided by the Australian Communications and Media Authority), which we labelled the 'OzSpam DS'. While the spam in the HABUL DS has been viewed by a potential victim, the Botnet DS and OzSpam DS contain spam that circulated all over the world, but without the certainty that the emails have reached their intended targets.

Altogether, about 13.5 million spam emails were collected, which included nearly half a million attachments and over six million URLs. The proportion of spam that carried malicious code in attachments or through hyperlinks in the body text of the email varied across the different sources. For example, 1.38 per cent of HABUL attachments and 13 per cent of HABUL hyperlinks were identified as malware and this was similar to the OzSpam DS, which identified 10.5 per cent of hyperlinks and 0.77 per cent of attachments as malware. The Botnet DS, however, had fewer suspect hyperlinks (0.52 per cent), which was as expected given the method applied, but approximately similar proportions of malware in the attachments (0.95 per cent) forwarded with the spam mail.

For each dataset, there were peak periods of spam that contained malicious content or did not contain it, and which suggested different types of spam (mass propagation) campaigns. These campaigns usually shared similarities in the content of their emails, and this alone may indicate the risk of malicious content.

Four main methods of attack were noted: social engineering and spear phishing, compressed files, right-to-left override email attacks and URL shortening. These are discussed in further detail below.

Social engineering and spear phishing

Cybercriminals favour social engineering tactics to persuade their victims to click on a malicious URL or download malware because it is easier than trying to insert malware remotely (such as via trojan horses) so that key-loggers can obtain banking passwords or other sensitive information. In examining the malicious attachment file names in our data, we found a trend towards referencing trusted business labels (for example, labels or brands related to shipping) rather than other labels or general names.

Spear phishing is a spamming method that targets selected users or groups via a compromised computer that can then be used as a 'zombie' computer capable of importing malware (key-loggers, crypters, and so on) to steal banking passwords and other confidential data. Spear phishing emails are personalised, and often try to impersonate a trusted source to avoid anti-spam detection at the system level. The most commonly found shared file types using purloined brands had the file extension '.zip', and were responsible for 76 per cent of the total number of spear phishing email attachments during our monitoring period. File extensions bearing other common formats—such as '.pdf', '.xls', '.doc', '.jpg', '.txt' and '.gif'—accounted for the remaining 24 per cent of malware, and, of these, .jpg and .txt extensions accounted for most. Spammers have also learnt to focus only on sending a single malicious attachment and to craft the payload necessary to get that attachment to the end user.

Compressed files

Spam emails can carry different types of files as attachments; however, it appears that files disguised under the extension .zip are the most common malware file type. The majority of spam filters block email attachments with the '.exe' file extension, but do not reliably scan archived and zipped documents, therefore encouraging spammers to compress executable files (.exe) into an archived form such as .zip. Our analysis showed that .zip files represent the majority (90 per cent) of malicious files.

There are malware formats that also try to get a recipient to download them using the double extensions method (for example, as 'per.doc.exe'). Other detection avoidance measures use double extensions ('.jpg.exe') to try to trick users or filters. Recipients will see .jpg or .pdf and may feel

comfortable to open up what seems to be an image or a standard pdf file. Our analysis of the three DS confirms that these simple avoidance methods are still commonplace.

Right-to-left override email attacks

Usually when executable files are decompressed their appearance provokes suspicion. So spammers conceal executable files with fake icons to make them appear as harmless file extensions, such as .pdf, .doc, .xls or .jpg, and employ the Unicode's right-to-left override (RLO) technique, which reverses the character ordering from right to left and so changes the order of characters.

Spammers thus use the RLO technique to deceive users into downloading and executing the malicious file hidden in an attachment under the cover of a fake file name extension, and the technique is often combined with very long file names that disguise the .exe file name extension. To make the process even harder, the malicious file names manipulated in this method are also delivered within .zip files or archives.

URL shortening

A service called 'URL shortening' has become popular and also enables methods to disguise or obfuscate spam/malware. This service allows long URLs to be transformed into much shorter URLs and thus enhances the likely use of the link. Spammers use URL-shortening services, even establishing their own.

Spammers redirect a link through many different shortened links: rather than leading straight to the spammer's final destination website, the links point to a shortened URL on the spammer's fake URL-shortening website, before redirecting to the spammer's final website and its hidden malicious content. This service has become more common because of its simplicity, automated capability and anonymity. Popular URL-shortener websites such as Google URL Shortener and Bit.ly provide an easy interface that allows users to convert long URLs into short ones. Information security companies have warned that attacks using URL-shortening services are on the rise, and our data showed that URLs shortened via Twitter accounted for 56 per cent of these events.

3. Responses: Joint investigations and legal interventions

Technological or legal responses alone are not as effective as those that combine technical methods with sound law enforcement practices and process. Coordinated operations were needed to take down several complex botnets (for example, McColo, GameOver ZeuS, Grum, Coreflood, Rustock). The advantage of using legal processes is that it mandates the removal of all the top-level domain names associated with spam. The examples noted also showed the benefits of international police cooperation, even though the investigations were unable to disarm the techniques used or arrest the offenders involved.

In June 2014, the US Justice Department and the Federal Bureau of Investigation (FBI) announced a national and international effort to disrupt the GameOver ZeuS botnet (US Justice Department 2014). It was a joint effort by investigators at the FBI, Europol and the United Kingdom's National Crime Agency as well as security firms CrowdStrike, Dell SecureWorks, Symantec, Trend Micro and McAfee and academic researchers at Vrije University in Amsterdam and Saarland University in Germany. The GameOver ZeuS botnet spread mainly through spam email and was thought to be involved in the theft of banking and other credentials from individuals and businesses all around the world. These combined technical and law enforcement responses to complex cybercrime activities also depend on the role of private information security businesses to achieve the most effective solution (OECD 2006; Krebs 2014).

A recent study of spam and phishing identified the location of high-risk ISPs that acted as 'internet bad neighbours', and found that spam originates from a small number of ISPs. The majority of 'bad' ISPs were concentrated in India, Brazil, West Africa and Vietnam. Typically, cybercrime is executed in a jurisdiction that is not party to multilateral enforcement agreements such as the Council of Europe's Cybercrime Convention, which enables mutual legal assistance across borders to facilitate the investigation of a cybercrime event, while the victim is located in another jurisdiction (Broadhurst 2006). For example, 62 per cent of all the addresses serviced by Spectranet, an ISP in Nigeria, were sending out spam (Moura 2013). In 2009, the US Federal Trade Commission, for example, closed the ISP 3FN service, as it was found to be hosting spam-spewing botnets, phishing

websites, child pornography and malicious web content (Federal Trade Commission 2009). However, Trend Micro (2010) reported that the service was back in business a few days later—reinvented and established outside US jurisdiction.

Laws, regulations and policies can, however, sometimes hinder the effectiveness of public or private actions. Policies such as 'network (net) neutrality' or common carrier policies (EC 2009) can hinder ISPs and other network providers from acting to eliminate criminal traffic from their networks because of the risk of breaching network neutrality regimes. Even in states where laws do not specifically preclude action, the conventional approach is to minimise possible interventions by ISPs and other actors that could counter or eliminate undesirable behaviour (such as hate mail, spamming). A potential policy change would be to reframe network neutrality laws or practices to allow for the alteration of internet traffic flows that indicate a high risk of being malicious. Under some interpretations of privacy laws, such as the US *Electronic Communications Privacy Act* (*ECPA*), companies that detect illegal activity on their networks are unable to voluntarily share information with other parties (for example, other ISPs or information security firms) about such activities to prevent further illegal activity. For instance, corporations are concerned about sharing non-redacted spam and phishing mail feeds, for fear of unintentionally violating their customers' privacy rights under the *ECPA* (Barrett et al. 2011). Similar concerns prevail in Australia and have the effect of fragmenting collective countermeasures and creating barriers to applied research on such problems.

4. Discussion

Spam as a prime means for social engineering continues to be a popular way to spread and inject malware on digital devices. Household users and small enterprises are most vulnerable to cyberattack due to factors such as the cost of maintaining up-to-date security. Thus, the oft-repeated cliché that our security is only as good as our weakest link applies.

Existing detection and defence mechanisms to deal with email spam containing malicious code are mostly reactive and ineffective against constantly evolving spam email formats that hide ever improving malware payloads and capabilities. There is an urgent need to identify new malware-embedded spam attacks (especially in the increasingly

common URL approach) without the need to wait for updates from spam scanners or blacklists (Tran et al. 2013). Machine-learning methods of identifying spam and other spam-filtering methods aim to be highly responsive to changes in spamming techniques, but have not been sufficiently flexible to handle variations in the content or delivery methods found in spam emails (Blanzieri and Bryl 2008; Alazab 2015).

The widespread use of botnets shows how spammers manipulate the networks of infected computers and servers around the world to ensure high volumes of spam are delivered. The increased role for networked crime groups has also impacted on the scale and sophistication of cybercrime. The emergence of bespoke email content tailored to entice a specific victim or victim type via spear phishing also poses dangers that require equally targeted education and crime prevention efforts. The use of spam emails remains an important and underestimated vector for the propagation of malware.

In short, fighting spam requires a combination of technology and relevant, up-to-date laws and policies as well as the constant reformulation of crime prevention practices to keep abreast of the evolution of spam–malware techniques. This, as we noted in the introduction, requires effective partnerships between the state, private actors and multilateral groupings of states, corporations and consumer groups that can tackle the cross-jurisdictional nature of spam and malware propagation. Shifts in malware attacks to new vectors using spam-like methods often based on astute and tailored social engineering also need constant attention. A good example is the shift to Twitter and other new media, where, for example, URL-shortening methods may prosper. While effective civil measures (including anti-address-harvesting laws) are in place to mitigate commercial misuse of spam in Australian cyberspace, the challenge lies in the integration of countermeasures that can further suppress the spam–malware vector. In addition, maintaining the high-level industry–government–law enforcement agency coordination required for successful disruption of malware-driven spam campaigns and other cybercrime must be at the forefront of government-led initiatives. To maximise such cooperation, a reassessment of the co-regulatory burdens on industry may be required and proposals to deregulate the current e-marketing and spam industry codes of practice, for example, may be welcome if they encourage more self-help and help secure continued partnership with government in the fight against cybercrime.

In spam emails, 'crimeware as a service' is more evident than ever and it involves selling exploits and tools for computer trespass. Once attack tools are in place, buyers can rent them to deliver attacks. Individuals and businesses need to increase their awareness of the dangers of spam emails, especially targeted attacks (for example, spear phishing) and create effective policies and practices to prevent their distribution. Botnets generally account for the global dissemination of spam. The widespread uses of botnets show how spammers manipulate the networks of infected computers and servers around the world to ensure high volumes of spam are delivered. The increased role of networked crime groups has also impacted on the scale and sophistication of cybercrime (Broadhurst et al. 2014). Trends in spam designed to create botnets also show increasing malware complexity that exploits new opportunities arising from automated financial activities (for example, GameOver ZeuS and CryptoLocker). The internet has also become the preferred platform on which to deploy spam attacks to intentionally disrupt or subvert these automated services and also to launch denial of service (DDoS) attacks (for profit or ideological motives). These tools have far-reaching implications for the evolution of cybercrime, which need to be explored and investigated. Spear phishing is a good example of offender innovation. By using personal information already gathered through deception or by inserting a remote access tool via an email with apparently *relevant* content from a trusted sender, this method can circumvent countermeasures.

The forms of social engineering used in spam emails have also become more sophisticated, personalised and compelling, thus improving their ability to deceive many users into malware self-infection. Given the limitations in what may be learned by technical investigations to identify new attacks and trends, turning to what victims experience and what we can learn from them will be increasingly important. Victim studies will be most useful if experimental and observational studies that compensate for the absence of technical knowledge about the modus operandi of the cyberattack can be employed. Constant education and the development of crime prevention practices that focus on methods of deception are crucial and need to be as current as the novel and advanced forms of malware that present on the internet.[4] Informal regulatory practices such as those sponsored by global efforts like the London Action Plan

4 For example, SCAMwatch (scamwatch.gov.au/); and ACMA's Cybersmart (cybersmart.gov.au/).

serve as examples of how groups of actors ('coalitions of the willing') can influence the behaviour of cybercriminals (who continue to enjoy the safe havens provided by rogue states and bulletproof ISPs), despite the limits of sovereignty and the failure to create an international regulatory regime to combat cybercrime.

Further reading

Grabosky, P 2013. 'Organised crime and the internet', *The Royal United Services Institue (RUSI) Journal* 158(5): 18–25.

Krebs, B 2014. *Spam Nation: The Inside Story of Organized Cybercrime—From Global Epidemic to Your Front Door*. Naperville, Ill.: Sourcebooks, Inc.

Maimon, D, Wilson, T, Ren, W and Berenblom, T 2015. 'On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents', *British Journal of Criminology* 53(3): 615–34. doi.org/10.1093/bjc/azu104.

References

Alazab, M 2015. 'Profiling and classifying the behavior of malicious codes', *Journal of Systems and Software* 100: 91–102. doi.org/10.1016/j.jss.2014.10.031.

Alazab, M and Broadhurst, R 2016. *Spam and criminal activity*, Trends and Issues in Crime and Criminal Justice, No. 526, Australian Institute of Criminology, Canberra.

Anderson, R, Barton, C, Böhme, R, Clayton, R, Eeten, M, Levi, M, Moore, T and Savage, S 2013. 'Measuring the cost of cybercrime', in R Böhme (ed.), *The Economics of Information Security and Privacy*. Heidelberg: Springer, pp. 265–300. doi.org/10.1007/978-3-642-39498-0_12.

Australian Communications and Media Authority (ACMA) 2004. *Spam Act 2003: An Overview for Business*. Melbourne: ACMA. Available at: acma.gov.au/webwr/consumer_info/spam/spam_overview_for%20_business.pdf.

Australian Communications and Media Authority (ACMA) 2014. Website. Melbourne: ACMA. Available at: acma.gov.au/.

Barrett, M, Steingruebl, A and Smith, B 2011. *Combating Cybercrime: Principles, Policies, and Programs*. San Jose, CA: PayPal. Available at: paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf.

Blanzieri, E and Bryl, A 2008. 'A survey of learning-based techniques of email spam filtering', *Artificial Intelligence Review* 29(1): 63–92. doi.org/10.1007/s10462-009-9109-6.

Broadhurst, R 2006. 'Developments in the global law enforcement of cyber-crime', *Policing: An International Journal of Police Strategies and Management* 29(3): 408–33. doi.org/10.1108/13639510610684674.

Broadhurst, R, Grabosky, P, Alazab, M and Chon, S 2014. 'Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime', *International Journal of Cyber Criminology* 8(1): 1–20.

European Commission (EC) 2009. *EU study on the legal analysis of a Single Market for the Information Society: New rules for a new age? 10. Spam. 11. Cybercrime*, European Commission's Information Society and Media Directorate-General, Brussels. Available at: ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=838.

Federal Trade Commission 2009. 'FTC shuts down notorious rogue internet service provider, 3FN Service specializes in hosting spam-spewing botnets, phishing web sites, child pornography, and other illegal, malicious web content', Press release, 4 June, Federal Trade Commission, Washington, DC. Available at: ftc.gov/news-events/press-releases/2009/06/ftc-shuts-down-notorious-rogue-internet-service-provider-3fn.

Krebs, B 2012. 'Who's behind the world's largest spam botnet?', [Blog], *Krebsonsecurity*, 1 February. Available at: krebsonsecurity.com/2012/02/whos-behind-the-worlds-largest-spam-botnet/.

Krebs, B 2014. '"Operation Tovar" targets "Gameover" ZeuS Botnet, CryptoLocker scourge', 2 June, *Krebsonsecurity*. Available at: krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/.

Moura, G 2013. *Internet Bad Neighbourhoods*. Enschede, The Netherlands: Ipskamp Drukkers BV. Available at: doc.utwente.nl/84507/1/thesis_G_Moura.pdf.

Organisation for Economic Co-operation and Development (OECD) 2004. *Background paper for the OECD workshop on spam*, OECD Digital Economy Papers No. 78, OECD Publishing, Paris. Available at: dx.doi.org/10.1787/232784860063.

Organisation for Economic Co-operation and Development (OECD) 2006. *Report of the OECD task force on spam: Anti-spam toolkit of recommended policies and measures*, OECD Digital Economy Papers No. 114, OECD Publishing, Paris. Available at: dx.doi.org/10.1787/231503010627 or oecd.org/internet/consumer/36494147.pdf.

Rao, J and Reiley, D 2012. 'The economics of spam', *Journal of Economic Perspectives* 26(3): 87–110. doi.org/10.1257/jep.26.3.87.

Smith, R and Hutchings, A 2014. *Identity crime and misuse in Australia: Results of the 2013 online survey*, Research and Public Policy Series No. 128, Australian Institute of Criminology, Canberra. Available at: aic.gov.au/media_library/publications/rpp/128/rpp128.pdf.

Spamhaus 2014. *Spamhaus Project*. London & Geneva: Spamhaus. Available at: spamhaus.org/.

Spamhaus 2015. *The Register of Known Spam Operations (ROKSO)*. London & Geneva: Spamhaus. Available at: spamhaus.org/rokso/.

Stringhini, G, Egele, M, Kruegel, C and Vigna, G 2012. 'Breaking the loop: Leveraging botnet feedback for spam mitigation', in *Proceedings of the Seventh Annual Graduate Student Workshop on Computing*. Santa Barbara, CA: University of California, pp. 25–6. Available at: ofutureschola r.com/paperpage?docid=1139739.

Stringhini, G 2015. 'Thinking like they do: An inside look at cybercriminal operations', in *Proceedings of the International Crime and Intelligence Analysis Conference. Manchester, UK. 26–27 February 2015*, London: University College London, pp. 36–7. Available at: ucl.ac.uk/jdi/events/int-CIA-conf/Downloads-ICIAC/ICIAC15_eBrochure.

Symantec 2008. *MessageLabs Intelligence: 2008 Annual Security Report*. Mountain View, CA: Symantec. Available at: ifap.ru/pr/2008/n081208a.pdf.

Symantec 2013. *Internet Security Threat Report 2013. Volume 18*. Mountain View, CA: Symantec. Available at: scm.symantec.com/resources/istr18_en.pdf.

Takahashi, K, Sakai, A and Sakurai, K 2010. 'Spam mail blocking in mailing lists', in K Nishi (ed.), *Multimedia.* Rijeka, Croatia: InTech, pp. 439–52. Available at: intechopen.com/books/multimedia/spam-mail-blocking-in-mailing-lists. doi.org/10.5772/7628.

Tran, KN, Alazab, M and Broadhurst, R 2013. 'Towards a feature rich model for predicting spam emails containing malicious attachments and URLs', in P Christen, P Kennedy, L Liu, KL Ong, A Stranieri and Y Zhao (eds), *Eleventh Australasian Data Mining Conference (AusDM)*. Conferences in Research and Practice in Information Technology Vol. 146. Canberra: Australian Computer Society, pp. 161–71. Available at: crpit.com/Vol146.html.

Trend Micro 2010. *The Botnet Chronicles: A Journey to Infamy. A Trend Micro White Paper*. Tokyo: Trend Micro. Available at: countermeasures.trendmicro.eu/wp-content/uploads/2012/02/the_botnet_chronicles_-_a_journey_to_infamy__nov_2010_.pdf.

Trend Micro 2012. *Spear-Phishing Email: Most Favored APT Attack Bait*. Tokyo: Trend Micro. Available at: trendmicro.com.au/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf.

United Nations Office on Drugs and Crime (UNODC) 2013. *Comprehensive Study on Cybercrime*. Vienna: UNODC. Available at: unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

United States Justice Department 2014. *A complaint USA v Evgeniy Bogachev*. Washington, DC: Department of Justice. Available at: justice.gov/opa/documents/dgzc/complaint.pdf.

This text is taken from *Regulatory Theory: Foundations and applications*, edited by Peter Drahos, published 2017 by ANU Press, The Australian National University, Canberra, Australia.