Australian Government

Australian Institute of Criminology

Trends & issues in crime and criminal justice

ISSN 0817-8542

No. 526 December 2016

Spam and criminal activity

Mamoun Alazab and Roderic Broadhurst

Abstract | The rapid growth of the internet is transforming how we engage and communicate. It also creates new opportunities for fraud and data theft. One way cybercriminals exploit the vulnerabilities of new technologies and potential victims is the use of deceptive emails on a massive scale.

In a sample of more than 13 million emails identified as spam, more than 100,000 contained malicious attachments; nearly 1.4 million contained malicious web links. If opened, these attachments and links could infect the recipients' devices with software that allows cybercriminals to remotely access them.

This paper describes how crime groups increasingly adopt novel approaches to cybercrime. Increased law enforcement capacity, the cultivation of high-level coordination between industry, government and police, and the further development of machine learning techniques should be at the forefront of government initiatives in this area.

Criminology Research Grants

The internet's decentralised structure offers fast communication with a global reach, but also provides anonymity, a characteristic invaluable to the commission of illegal activities. Cybercrime has evolved rapidly in parallel with the spread of the internet and ecommerce. Unsolicited email, or spam, is the basis of many forms of cybercrime. One of the earliest online criminal partnerships formed was between malware authors and email spammers, who socially engineer emails to spread malware to computers and other digital devices; email remains one of the major vectors for the dissemination of malware. Unlike cybercrime that targets low-volume, high-value victims like banks and requires advanced hacking ability, spam allows malware to reach high-volume, low-value targets, which are less likely to have effective antivirus or other countermeasures in place. A typical example would be a malicious email containing content that entices the recipient to click on a URL link to a malicious website, or to download a malicious attachment.

Deceptive, socially engineered email is relatively well understood, but less is known about advanced methods like 'spear phishing', or whether different forms of social engineering are related to different types of malware and crime. Cloaking methods that disguise malicious executable files as harmless Microsoft Word files, PDF or text documents are now common. These methods include, among others, manipulating the encoding method, applying fake double extensions in compressed form and mimicking URL shortening services to spread malicious files and links through the web. Understanding spam activity and the threat malicious spam poses—especially the prevalence, frequency, duration and severity of these common forms of cybercrime—is the key to prevention. States lack the capability to suppress spam and must rely on mutual interest, and a host of non-state actors, to perform tasks usually the province of law enforcement agencies.

This research used real-world datasets from the Australian Communications Media Authority (ACMA) Spam Intelligence Database (SID) to describe the nature of, and trends in, spam-borne malware. A total of 13,450,555 spam emails were processed; of the 492,978 that had attachments, 21.4 percent were malicious, and 22.3 percent of the links in the 6,230,274 that contained a URL proved malicious. This paper argues that, because the IT security focus on perimeter protection is increasingly ineffective, crime prevention activities must refocus on the modus operandi of offenders and the vulnerabilities of victims.

Malicious spam emails

The number, type and sophistication of email threats to Australia are significant and evolving. Anyone with an email account is aware of the problem of spam. Spam takes many forms and has long been a focus of information security industry attention and international law enforcement concern (European Commission 2009; UNODC 2013). Legislation criminalising or limiting spam has been introduced in more than 30 countries (OECD 2006, 2004), but there is no internationally agreed definition of spam. The 2004 London Action Plan brings together 27 states and agencies (Australia, Belgium, Brazil, Canada, Chile, China, Denmark, Finland, 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-government agencies like Spamhaus Project and M3AAWG; telecommunications and information security companies like Verizon and McAfee; and corporate and consumer groups, to implement anti-spam activities (London Action Plan 2016) and further global cooperation and public/private partnerships to address spam-related problems. Despite this international effort, spam remains a significant cost and risk (UNODC 2013). The Plan acts as a clearinghouse, establishes a contact point for spam-related problems such as online fraud, phishing and virus dissemination, and engages university and private sector researchers in anti-spam activities.

Spam can carry advertising that is annoying but benign; however, it can also be an initial contact point for cybercriminals—like the operators of a fraudulent scheme who use emails to solicit money from prospective victims, as in advance fee frauds, or to commit identity theft by deceiving recipients into sharing their personal, banking and financial information. It can also be used to deliver malware like computer viruses, worms and ransomware, or to distribute child exploitation material.

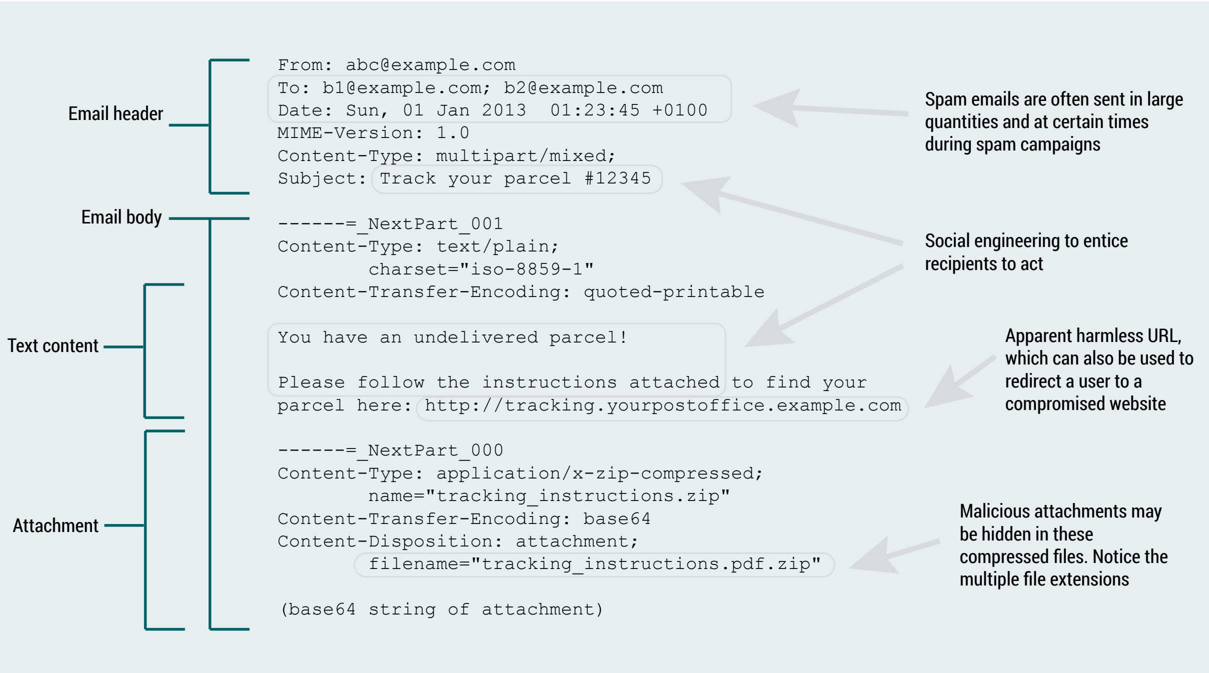
Put simply, spam is not just email. Spam is difficult to define precisely but, broadly, is any unsolicited electronic message—usually, but not necessarily, sent in bulk. The definition varies depending on whether the emphasis is on lack of consent (unsolicited) or the content of the email. The Australian Communication and Media Authority (ACMA), which is the regulator, defines spam as ‘unsolicited commercial electronic messages’, which may not capture spam’s versatility (see also the *Spam Act 2003*, s. 6). By this definition, a single electronic message could be considered spam if it were unsolicited. On the other hand, Spamhaus considers an email to be spam if it is both unsolicited and sent in bulk (Spamhaus 2015). This distinction is important because legislators may focus on the content of spam messages, rather than the delivery method and technique, which could be crucial in reducing the problems spam causes (Wang, Irani & Pu 2013).

This paper describes the types of spam-driven email attacks that are potential sources of malware infection. It also describes the different kinds of spam threats that targeted Australian cyberspace during 2012, and suggests ways to better prevent spam-driven cybercrime.

Understanding spam formats

Email formats are well understood, and the email data used to construct the features for analysis for this research are shown in Figure 1, formatted using standard SMTP. Figure 1 illustrates the structure of the typical malicious spam email, stripped of irrelevant metadata. The example email is presented in raw text format, with annotations showing the parts of the email that were used to extract the variables used in this research. The email header contains delivery instructions for mail servers, and the email body may have many sections for text and attachments. The subject and text content of malicious spam can reveal social engineering methods of varying levels of sophistication that seek to manipulate recipients into first reading, and then acting on, the email. In this case, the premise is an undelivered (in fact, non-existent) parcel; the recipient is asked to download a compressed file (its contents disguised, but including multiple file extensions) to facilitate the parcel's delivery. Downloading the compressed file will transmit the malicious payload. The compressed file hides executable malware from the virus scanners applied by the mail server, the potential victim's internet service provider (ISP) or the local systems administrator. In this example, the URL acts as a secondary method of delivering malicious content. Like attachments, malicious URLs can disguise a malicious or compromised website (eg example.com) by adding subdomains that represent a known and safe website (eg tracking.yourpostoffice). This example also shows a typical spam template, where attachments or URLs may have different names but the same malicious purpose.

Figure 1: An example (fake) malicious spam e-mail



```
From: abc@example.com
To: b1@example.com; b2@example.com
Date: Sun, 01 Jan 2013  01:23:45 +0100
MIME-Version: 1.0
Content-Type: multipart/mixed;
Subject: Track your parcel #12345

------=_NextPart_001
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

You have an undelivered parcel!

Please follow the instructions attached to find your
parcel here: http://tracking.yourpostoffice.example.com

------=_NextPart_000
Content-Type: application/x-zip-compressed;
        name="tracking_instructions.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
        filename="tracking_instructions.pdf.zip"

(base64 string of attachment)
```

Email header
Email body
Text content
Attachment
Spam emails are often sent in large quantities and at certain times during spam campaigns
Social engineering to entice recipients to act
Apparent harmless URL, which can also be used to redirect a user to a compromised website
Malicious attachments may be hidden in these compressed files. Notice the multiple file extensions

Spam templates are often used in spam campaigns where many emails are sent in a short period of time, often with minor changes to the wording of their content (Stone-Gross et al. 2011). In the example, the tracking number, attachment name or URL could be different. Such variations are an attempt to overcome routine spam detection methods and mail server filters. Other cloaking methods include manipulating email headers to include legitimate email addresses, which also helps to avoid spam filters and thus allows more spam to be sent undetected. For further examples of exploit templates, see Mouton, Leenen and Venter 2016.

Why are spam emails prominent and persistent?

Responses such as the London Action Plan recognise that malicious email poses a global challenge because it is a major vector for the dissemination of malware that can have a significant social and economic impact (Anderson et al. 2013; Rao & Reiley 2012). Malware is commonly distributed through two types of spam: email with an attachment that contains a virus or Trojan, which installs itself on the victim's computer when the attachment is downloaded; and email containing a hyperlink to a compromised web page, from which the malware is downloaded onto the victim's computer (Tran, Alazab & Broadhurst 2013). The opportunities afforded by a low-risk, low-cost, profitable criminal activity like spamming—and in particular embedding malware in spam—attract criminal actors and networks (Thomas et al. 2015). As outlined below, this explains why spam is so prominent and persistent.

Low cost, mass scale

Spam is problematic not just because of its criminal potential but because of its sheer volume, which impedes the flow of legitimate internet traffic around the world. Although the volume of malicious spam may seem insignificant at an individual level it has been estimated that, in 2013, approximately 183 billion emails were sent and received every day, and the volume of malicious communication was substantial (Radicati & Levenstein 2013). In 2015, the Internet Governance Forum reported a lower estimate of 116 billion emails sent each day (Internet Governance Forum 2015). It has been estimated that 80 to 85 percent of this mass email traffic is spam (BarracudaCentral 2015; International Telecommunication Union 2015; Symantec 2014). Another study of spam and phishing identified a small number of high-risk ISPs that were 'internet bad neighbours'. The majority of 'bad' ISPs were concentrated in India, Brazil, West Africa and Vietnam. For example, 62 percent of all the addresses serviced by Spectranet, an ISP in Nigeria, were sending out spam and/or hosting botnets (networks of compromised computers; Moura 2013). The proliferation of botnets has allowed large volumes of coordinated spam to be sent rapidly, amplifying the risk of cybercrime (Stone-Gross et al. 2011); internet security company CYREN reported, for example, that 40 to 50 million emails could be distributed in less than five minutes (CYREN 2015). With minimal start-up costs and using a normal computer and basic configurations, a spammer can send tens of thousands of messages in seconds. Once the configurations are in place, greater volumes of spam can be sent at almost no cost—except to ISPs and the recipients.

Performance and profit

Unlike low-volume, high-value cybercrime that targets financial services and requires advanced hacking capability (Alazab & Venkatraman 2013), spam allows malware to reach high-volume, low-value targets that are less likely to have effective anti-virus or other countermeasures in place. Botnets are the backbone of spam delivery and account for between 80 and 90 percent of all spam sent globally (Stringhini et al. 2011). For example, a thousand computers sending a thousand spam emails each will deliver them more quickly than one computer sending 1,000,000 spam emails. Spamhaus (2015) estimates about 80 percent of the world's spam was sent by botnets operated by about a hundred active crime groups. Sophos (2014) demonstrated that just one infected computer could send spam to about 5.5 million email addresses in one week (ie 30 GB). This mass spam comprised 750,286 unique spam messages. Twenty-six percent of these included malware; 3,771 different URL-shortener links (see below) were used, and 74 percent of the content was linked to a pharmaceutical website.

Spam offers a high return with little investment. MessageLabs estimated that, for a spam advertisement to be profitable, one in 25,000 spam recipients needed to open the email and make a purchase in an underground market (Symantec 2008). In 2010, spam earned its senders US$2.7m in profit from fake sales of pharmaceuticals alone (Krebs 2012), while costing ISPs and users worldwide billions (Anderson et al. 2013). One study on the economics of spam (Rao & Reiley 2012) calculated that spammers collect gross global revenues in the order of US$200m per year, while some $US20b is spent fending off unwanted emails. Thomas et al. (2015: 7) list a variety of spam-vector malware revenues, but note the absence of estimation methodologies and lack of recognition of the complex value chains involved.

Social engineering

The chances of malware infection are increased by improved methods of deception, known as social engineering. According to Microsoft's Security Intelligence Report (Microsoft 2011), malware that requires user interaction, such as campaigns that entice users to download and execute a malicious file, account for almost half (44.8%) of the identified compromised emails, and are often preferred to other propagation tactics like autorun, file infector or brute-force methods. Although some reports note that spam is in decline (International Telecommunication Union [ITU] 2013; Cisco 2011), others suggest the use of malware in spam is on the rise (Symantec 2014). Cisco and Trend Micro argue that spammers have shifted their focus toward advanced persistent threat (APT) attacks like spear phishing, which combine 'big data' harvesting of personal data with related bespoke email content (Trend Micro 2012; Symantec 2014).

Low risk

Cybercrime is an attractive growth industry, and less risky than traditional crimes like armed bank robbery—or even other means of committing crime online, such as infected USB or storage keys. The internet makes it easy for cybercriminals to operate virtually from abroad, and technologies like The Onion Router (TOR), the Dynamic Domain Name System (DDNS), virtual private networks (VPN) and the deep web allow them to remain anonymous online and make them difficult to trace. Spam can come from multiple sources—for example, from a friend's computer or the workplace (spear phishing)—and most often an international source. Such methods ensure online anonymity and avoid network surveillance and traffic analysis that could allow the origin of the attack to be traced. In practice, spam—indeed any email—may be traced back to its source, but that source is often an innocent victim or compromised computer (known as a 'zombie').

Crime networks

The image of the lone hacker belies the collective nature of much cybercrime (Broadhurst et al. 2014). The factors outlined above account for the increasing involvement of networked crime groups and this, in turn, has influenced the scale and sophistication of cybercrime. McGuire (2012) estimated about 80 percent of cybercrime could be the result of some form of organised or distributed crime activity. This does not mean, however, these groups take the form of traditional, hierarchically organised crime groups or that they exclusively commit digital crime (Wall 2015). However, the dissemination of spam requires a collaborative network of actors because of the degree of specialisation required, something evident in other underground online economies (Thomas et al. 2015). The diverse skills required include malware coding, email address harvesting, social engineering of messages and distributing messages to the spammer, who engineers the emails to evade anti-spam filters and attaches malware to them, which in turn will manage the compromised computers.

Spam intelligence datasets

Table 1: Three feeds datasets—malware (%)

Dataset Statistics	Number of emails & malware (%)	With attachments		With URLs	
		Total	Malware (%)	Total	Malware (%)
HabuL	1,369 (7.1%)	55	19 (34.5%)	534	78 (14.6%)
Botnet	317,109 (2.4%)	6,015	3,008 (50.0%)	142,486	1,647 (1.6%)
OzSpam	13,132,057 (11.3%)	486,908	102,238 (21.0%)	6,087,757	1,385,962 (22.8%)

Source: ACMA SID 2012

This research used three real-world datasets of spam emails, collected in 2012 from the Australian Communication Media Authority (ACMA) Spam Intelligence Database (SID). Emails can be identified as spam in two ways: an email user could determine that an email is spam, or the email might be identified as originating from a known spamming network. Both scenarios are captured in the datasets used in this research.

The first dataset, the HabuL Data Set (HabuL DS), comes from the HabuL plugin for Thunderbird (an open-source, cross-platform email service and Usenet based on Mozilla code), which uses an adaptive filter to learn and test variations from emails a user has labelled 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 was labelled the Botnet Dataset (Botnet DS). The third dataset, labelled the OzSpam Dataset, or OzSpam DS, consists of suspect emails reported by Australian ISPs, sourced via the SID. Table 1 summarises the descriptive statistics of the three DS feeds. The HabuL DS is much smaller than the Botnet DS or OzSpam DS, but its advantage is that the emails collected in it have been viewed by a potential victim (the recipient) and identified by that person as spam. The Botnet DS and OzSpam DS, however, contain spam that has circulated around the world, but there is no certainty that the emails reached their intended targets.

The datasets were received in anonymised form, and no identifiable email or IP addresses were available for analysis; these data were excluded for privacy reasons. However, some metadata such as third-level domain names would have assisted in better understanding victim risks, and would be helpful in further research. This analysis only looked at spam that appeared to have been relayed through Australia—for example, the last hop IP address was in Australia. The spam datasets used were composed entirely of emails that had already breached existing filters, both at the provider and end-user level. SID cannot distinguish spam embedded with malware that was ultimately successful from other spam, although case evidence from ACMA and the Australian Cybercrime Online Reporting Network (ACORN) shows many of the common deceptions identified and described below are, indeed, successful.

The analysis was limited to spam containing at least one malicious attachment or URL. The attachments and URLs were extracted from each email, uploaded to VirusTotal, an online virus checker that supports researchers, and scanned for viruses and suspicious content. VirusTotal uses over 40 different virus scanners, and attachments or URLs were determined to be malicious if at least one virus scanner showed a positive result. Blacklists such as VirusTotal are more accurate than any scan that takes place when the spam is received, because the URLs were scanned long after they were potentially delivered.

Altogether, about 13.5 million spam emails were collected, including nearly half a million attachments and over six million URLs. The number of emails collected and the proportion identified as malware from these three sources is reported in Table 1. 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, 5.7 percent of hyperlinks and 1.4 percent of attachments of emails in the HabuL DS were identified as malware. Of emails in the OzSpam DS, 10.6 percent of hyperlinks and 0.8 percent of attachments were identified as malware. The Botnet DS had fewer malicious hyperlinks (0.5%), as expected given the method of dissemination, but a similar proportion of malicious attachments (0.9%).

The three datasets also showed some general similarities: 39 percent of HabuL DS, 45 percent of Botnet DS and 46 percent of OzSpam DS spams contained at least one URL. Interestingly, almost a quarter (22.8%) of URLs in emails from the OzSpam DS were identified as malicious, a much higher proportion than found in HabuL DS emails (14.6%) and emails from the Botnet DS (1.2%). By contrast, 35 percent of HabuL emails with an attachment were malicious, while the same was true of 50 percent of Botnet DS emails and 21 percent in the OzSpam DS.

There were distinct monthly variations in both the number of emails and the proportion of those containing malicious content in all three datasets, suggesting different types of mass propagation campaigns. The emails sent during these campaigns were usually similar in content, which also may indicate the risk of malicious content. Despite these variations in the prevalence of malware, embedded hyperlinks are now a crucial vector for compromising a computer and inserting malware.

Notably, there was no clear relationship between the number of emails sent during any specific period over a month or a week, and the proportion that contained malicious content. For example, the highest number of emails was sent in February, but emails sent in February had one of the lowest proportions of malicious content of any in the Botnet DS.

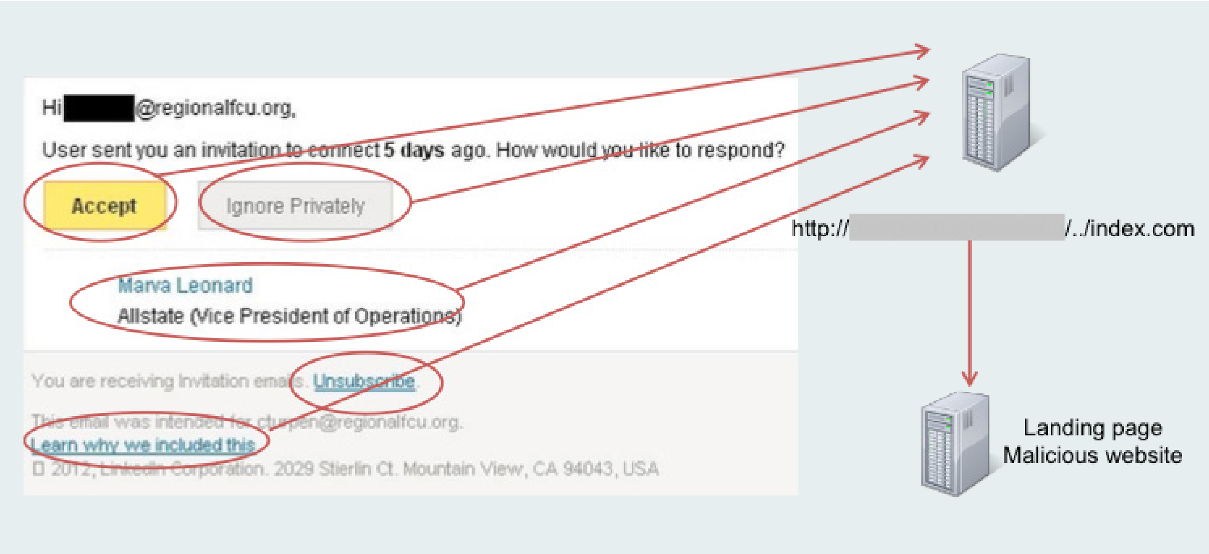
Sending spam emails via botnet

Botnet-based spam emerged well over a decade ago as advanced distribution networks, which are also often associated with Distributed Denial of Service (DDoS) attacks; botnets are responsible for most large-scale spam campaigns. Botnets are groups 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 DDoS attacks, install other malicious code (eg fake anti-virus software) and steal sensitive information, like harvested passwords and credit card and bank accounts, to be used or sold. Spammers manipulate global networks of infected computers and servers to deliver large volumes of spam. Spam botnets operate as bulk mailers or open relays, cloaking the spammer’s address (Stringhini et al. 2011); spammers prefer to use hacked accounts to spread spam (Mezzour & Carly 2014).

Analysis shows 40 percent of the datasets consisted of emails that had been distributed more than 50 times and sometimes more than a thousand times (with either the same or different attachments). This suggests different botnets are used to send this multiple or mass spam, which may reflect the involvement of different spam operators or crime groups (see Spamhaus 2015).

Fully automated spam created by crimeware toolkits like Blackhole often contain a malicious attachment or a link to a legitimate website that has been compromised. These toolkits are easy to use. They leverage existing vulnerabilities by, for example, concealing intrusions through an intermediary website or ‘waterhole’. A waterhole is a site the victim visits and considers trustworthy, but which is also undetected by spam filters. The waterhole redirects the visitor to a landing page where the malicious code is hidden (see Figure 2). Such attacks can be automated using a template for spam content that includes a URL to a compromised website, which is distributed through, often, thousands of infected computers by a botmaster, or botnet operator, who charges fees to do so.

Figure 2: An example of a redirect link ‘Waterhole’ attack



Hi [redacted]@regionalfcu.org,

User sent you an invitation to connect 5 days ago. How would you like to respond?

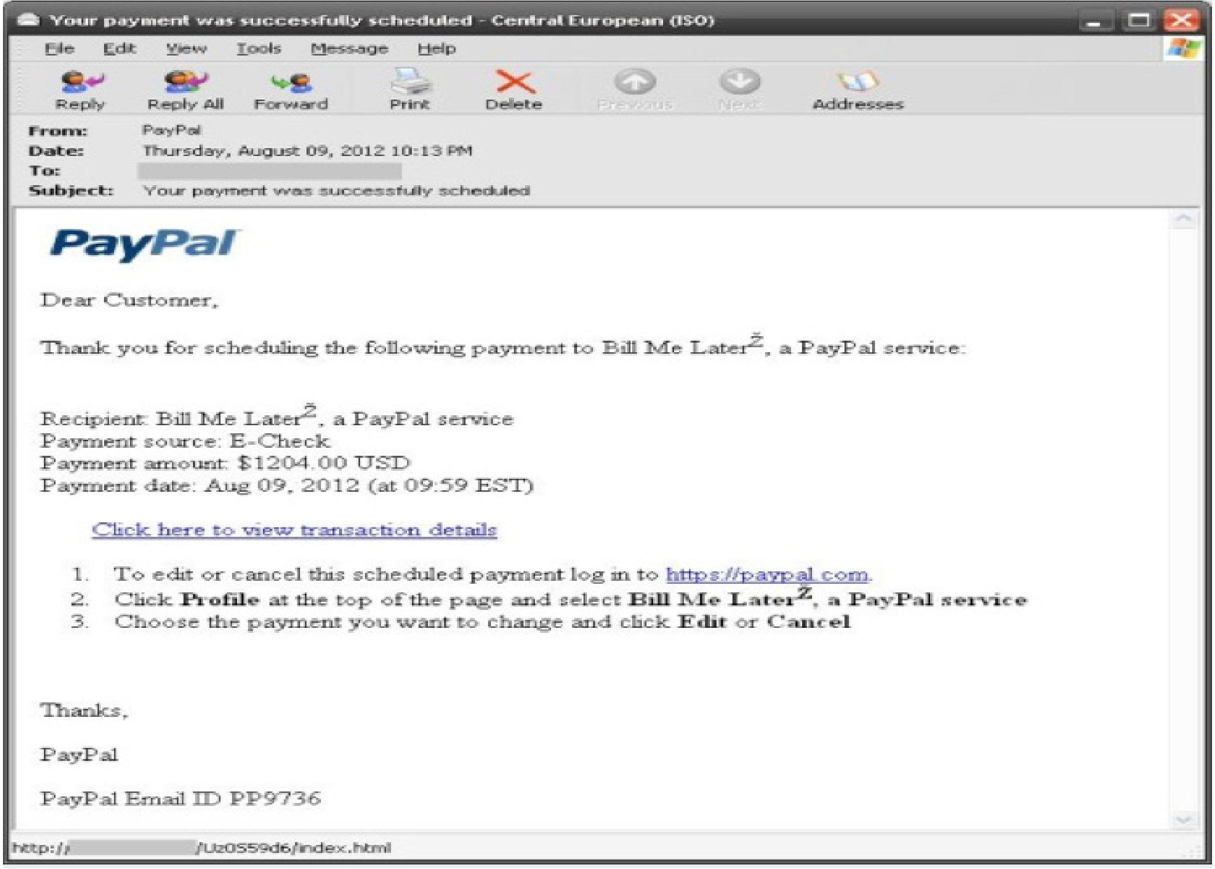
Marva Leonard
Allstate (Vice President of Operations)

You are receiving Invitation emails. Unsubscribe.

This email was intended for cturpen@regionalfcu.org.
Learn why we included this.
□ 2012, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA

Figure 3 is a screenshot of a fake PayPal email containing a Blackhole exploit kit and a Remote Access Trojan (RAT) used to create a botnet and delivered via a spam campaign. This is a typical example of basic social engineering. Although the email appears legitimate it contains a malicious URL which, when clicked upon, redirects the victim’s computer through a number of websites unseen to the victim to the website containing the Blackhole exploit kit.

Figure 3: A spam email including a Blackhole exploit


Your payment was successfully scheduled - Central European (ISO)
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses
PayPal

From: PayPal
Date: Thursday, August 09, 2012 10:13 PM
To: [redacted]
Subject: Your payment was successfully scheduled

Dear Customer,

Thank you for scheduling the following payment to Bill Me Later$^{\check{Z}}$, a PayPal service:

Recipient: Bill Me Later$^{\check{Z}}$, a PayPal service
Payment source: E-Check
Payment amount: $1204.00 USD
Payment date: Aug 09, 2012 (at 09:59 EST)

Click here to view transaction details

1. To edit or cancel this scheduled payment log in to https://paypal.com.
2. Click **Profile** at the top of the page and select **Bill Me Later$^{\check{Z}}$, a PayPal service**
3. Choose the payment you want to change and click **Edit** or **Cancel**

Thanks,

PayPal

PayPal Email ID PP9736

http://[redacted]/Uz0559d6/index.html

Spam services (crimeware-as-a-service)

Cybercrime as a service lowers the barriers for new actors. Software toolkits are now also readily available, allowing even a novice to successfully launch spam attacks. These tools have contributed to other criminal activity such as pay per install (PPI) services and botnet rental, which in turn stimulates the illicit market. These tools are sold on underground trading forums and instant messaging (IM) sites. The prices of tools and services can vary depending on their features and effectiveness. Online crime groups have long provided illicit services like the creation or rental of botnets, complete with databases of email addresses and various malware (add-on) services (see Thomas et al. 2015).

Spam thrives on the acquisition of active email addresses, and these addresses are harvested in three different ways.

- Addresses can be found by searching on websites and message boards. In 2012, Trend Micro reported that more than half of the total number of addresses collected for spam attacks were obtained from websites (Trend Micro 2012).
- Addresses can be generated manually by performing a 'dictionary attack.' This combines randomly generated usernames with known domain names to guess correct addresses.

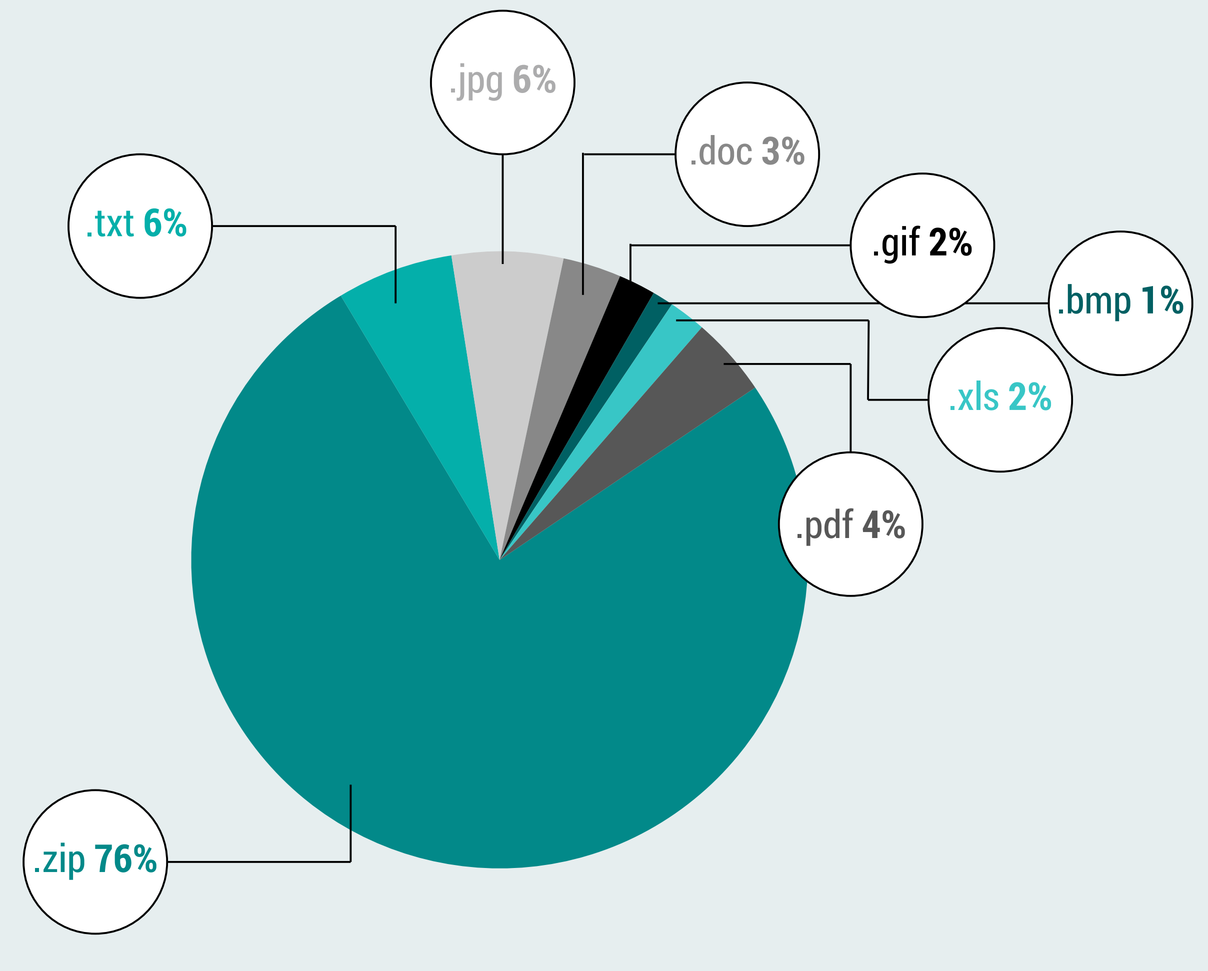
- More commonly, spammers purchase email address lists (McAfee 2013), usually from individuals or organisations in underground or darknet markets (Takahashi, Sakai & Sakurai 2010).

Once they have harvested email addresses, spammers distribute spam via botnets controlled by a botmaster, who often rents the botnet to spammers and others who use them to deliver malware. Examples of botnets include Storm Worm, Grum, PushDo, Bobax, Cutwail, Maazben and Rustock.

Social engineering and spear phishing

As noted above, some reports claim that spam volumes are declining because spammers have shifted their focus toward Advanced Persistent Threats (APT) like spear phishing. Social engineering techniques are commonly used to trick recipients into believing a spam email is legitimate and convince them to act on the email (Broadhurst & Chang 2013). Cybercriminals favour social engineering tactics to persuade their victims to click on a malicious URL or download malware, because this is easier than trying to insert malware remotely, for example through Trojans (Hong 2012; Abraham & Chengular-Smith 2010).

Figure 4: Top 10 malicious file extensions



Source: ACMA SID 2012

Social engineering attempts to manipulate behaviour by building rapport with a victim, then exploiting that emerging relationship to obtain information from or access to their computer (Chantler & Broadhurst 2006). For example, spam often uses alarming language (eg 'Your bank account has been suspended') to convince users to click on a malicious URL and rectify the problem (FireEye 2013). The text used in malicious attachments provides some insights. File names are often related to recognisable trusted brands, like FedEx or PayPal, that act as lures. The file names of the malicious attachments in the three datasets showed a clear trend to use trusted business brands rather than other brands or general names. Labels or brands related to shipping are among the most common—for example FedEx, UPS, USPS or DHL.

Spear phishing is a spamming method that targets selected users or groups via a compromised computer, known as a slave or zombie computer, that imports malware such as keyloggers and crypters to steal banking passwords and other confidential data. Spear-phishing emails are personalised, and often try to imitate a trusted source to avoid anti-spam detection at the system level. The analysis showed spammers use common business terms in their file names as enticements—for example, as noted, the names of common logistics brands. The type of shared file most likely to be falsely branded were zip files (file extension .zip); these made up 76 percent of all attachments of spear-phishing emails during the monitoring period (see Figure 4). Zip files have long been a popular way to deliver malware, and remain effective when combined with targeted deception. The remaining 24 percent of malware was attached in other common file formats like .pdf, .xls, .doc, .jpg, .txt, .bmp, and .gif; JPEG and text files accounted for most of these. Spear phishing continues to be an effective cyberattack technique and a common way to initiate advanced malware campaigns. The data show the majority of email attacks were targeted at one victim (69%), and 88 percent of emails had only one file attachment, rather than multiple or bundled files. This suggests spammers have learnt to focus on sending a single malicious attachment and crafting the vehicle necessary to get the payload to the end user. It is likely that attachment names and subject lines will further vary (eg 'World Cup', 'Missing Malaysian aircraft') as spammers search for new ways to deliver malicious attachments.

Common deceptions: Compressed files, double extensions and right-to-left override

The majority of spam filters block executable email attachments (ie attachments with an .exe file extension), but do not reliably scan archived and zipped documents (Krebs 2011), thereby encouraging spammers to compress executable files into an archived form like zip, RAR or tar. The analysis showed the vast majority of malicious files are zip files (90%). Zip attachments can contain many different file types and, because users are often unaware of the risks associated with these file extensions, they remain effective for disseminating malware. Information security services often block or reject emails that contain executable attachments, prompting criminals to use two methods of circumvention. One common technique is to disguise the executable file using a double file extension. In this example, *tracking_instructions.pdf.zip*, the first extension is that of a benign attachment—in this example it is .pdf, but it might be .jpg or another common file extension. The second extension, however, shows what the file really is: a zip file containing executable files. For example, the Kraken botnet attempted to avoid .exe blocking filters by sending executable files in a compressed form like zip, or tried to confuse users and filters with a double-extension format (eg .jpg.exe). The recipient sees the .jpg or .pdf file extension and opens a file that appears to be an image or a standard PDF file. Analysis of the three datasets confirms these simple avoidance methods are still commonplace. Another technique is to simply insert a gap between the two extensions; this can prevent some spam filters from determining that the attachment is an executable file.

The right-to-left override (RLO) refers to a special Unicode character (U+202e). Unicode is an encoding system that enables computers to exchange information regardless of the language used. It supports languages that are written right to left, like Arabic and Hebrew. RLO can be used to disguise a malicious file (Krebs 2011). Box 1 provides an example of how RLO can be used. When executable files are decompressed, their appearance usually provokes suspicion. Spammers conceal executable files with fake icons to make them appear to be harmless files like PDFs, Word documents, Excel or JPEGs, and employ Unicode's right-to-left override (RLO) to reverse the character ordering from right to left. Users then download and execute the hidden malicious file. The technique is often combined with very long file names that help to disguise the .exe file extension. Although this deception has been known for some time (Davis & Suignard 2013), it can be hard to detect. To make detection even harder, the malicious files whose names are manipulated in this way are often delivered in zip files or archives.

Box 1: Example of a 'Right-to-Left Override' email attack

Actual attachment name is:

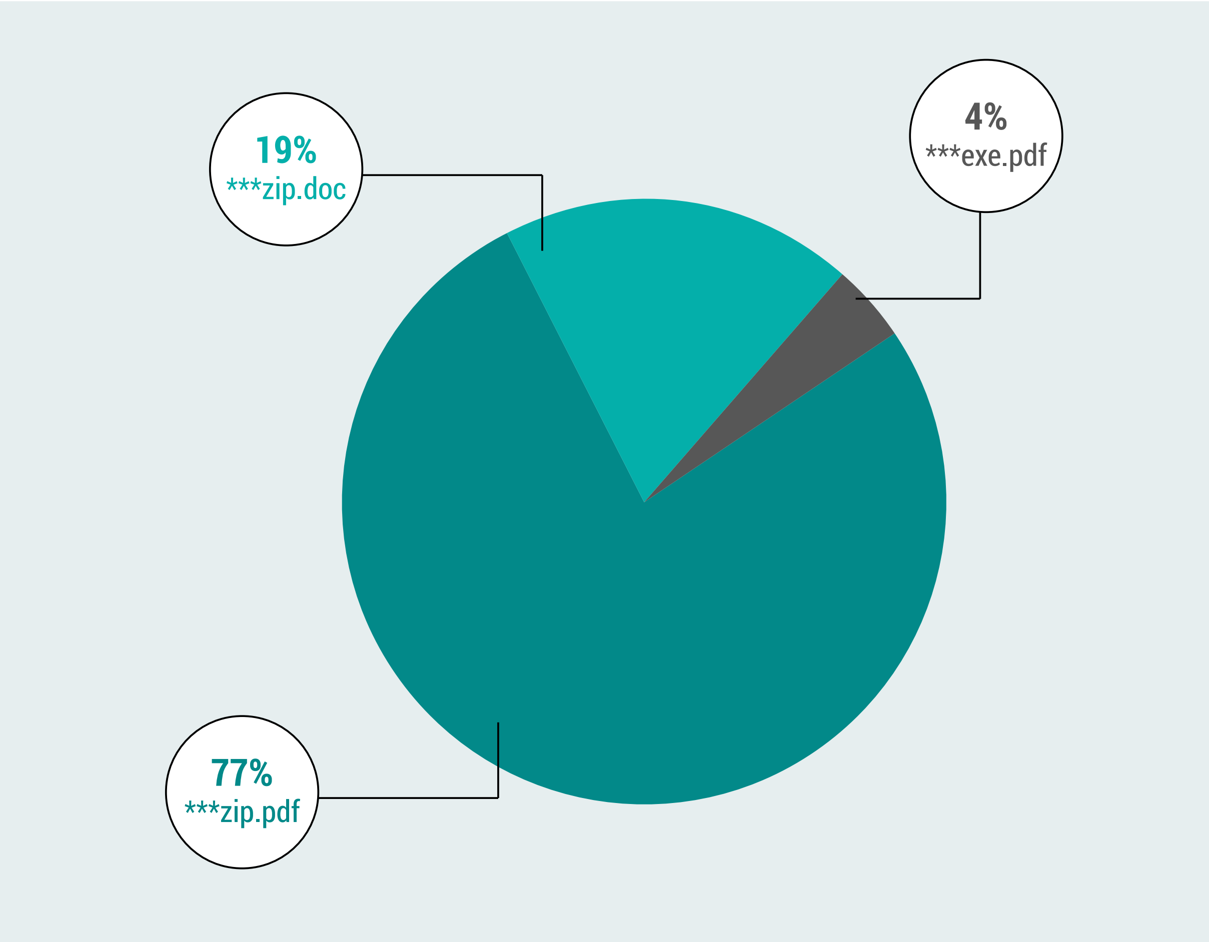
*Your_personal_details_15.6.2012_E.hey***doc.***exe*

But the disguised file name is:

*Your_personal_details_15.6.2012_E.heyexe.***doc**

Figure 5 illustrates the various RLO techniques found in the datasets. Malicious content was most often masked as a PDF or Word file (.doc). The .pdf and .doc extensions allow spammers to disguise attacks because users trust them and are unaware that malware can be disguised as these file types.

Figure 5: Spam using RLO email attacks (%)



Source: ACMA SID 2012

URL shortening

URL shortening services have become popular, especially among social network users. These services also enable the disguise or obfuscation of spam and malware. URL shortening transforms long URLs into much shorter URLs, thus making use of the link more likely. Spammers also use URL-shortening services, even establishing their own shortening services (Symantec 2012). Inadvertently this shortening allows spammers to deceive recipients and hide the true destination or location of the link to avoid detection. Some URL shortening services provide feedback through a dashboard that shows the number of clicks made and the locations and internet browsers that potential victims visit. This allows spammers to determine which URL links engage users and thus tailor links to improve the effectiveness of their campaigns. Spammers usually redirect a link through many different shortened links, rather than straight to the spammer's destination website. Initially, the links point to a shortened URL on the spammer's fake URL shortening website, before redirecting to the final website and its malicious content. URL shortening services have become more common because of their simplicity, automated capability and anonymity (Wang, Irani & Pu 2013; Wang et al. 2013).

There are many URL shortening services spammers can use or they can create their own. Many popular URL shortening websites, like Google URL Shortener, the Twitter URL shortener and Bitly, provide an easy interface that allows users to convert long URLs into short URLs. These services use a hash function to map the long URL to a short string of alphanumeric characters, which is then added to the domain name of the shortener and returned as the short URL. URL shortening services can also be exploited when a criminal group gains control of a legitimate URL shortening service or creates such a service, which appears to be legitimate but is adapted for malicious use. These are often hosted in Russia or Ukraine, or have Russian domain names (Symantec 2012). Spammers use Twitter's large audience and reach to entice users to use Twitter's URL shortener; the results mimic tweets. This analysis confirmed these findings; Table 2 shows how legitimate URL shortening services were used in spam emails from all three datasets.

Table 2: URL-shortening services identified

Name	Service provider	% of all services
Twitter	t.co	56.3%
Google	goo.gl	29.9%
HootSuite	ow.ly	3.5%
ViralURL	vur.me	3.4%
Bitly	j.mp	3.0%
TinyURL	tinyurl.com	0.7%
ViralURL	vurl.bz	0.6%
is.gd	is.gd	0.6%
scrnchlet	scrnch.me	0.5%
Bitly	bitly.com	0.5%

Conclusion: Challenges and recommendations

Existing detection and defence mechanisms for dealing with malicious spam are mostly reactive, and therefore ineffective against the constantly evolving formats used to conceal malware payloads. New malware-embedded spam attacks must be identified as rapidly as possible, without waiting for updates from spam scanners or blacklists. Spam scanners attempt to filter suspect emails but often cannot be updated as quickly as the novel variants of malware and/or social engineering appear, and necessarily rely on many different resources to identify malicious content. Spam filtering, from a computer science perspective, is a mature research field; rule, information retrieval and graph-based filtering techniques are available, as are machine learning and hybrid techniques. However, identifying emails with malicious content remains a problem worthy of further investigation (Tran et al. 2013; Alazab et al. 2013). One popular malicious spam countermeasure is the development of machine learning techniques (a form of self-excited intelligence analysis) that routinely check the content of emails, attachments and suspect URLs, and can match suspect websites or URLs, attachments and socially engineered email content with known blacklists of such activities. This can reveal the scope and nature of the malicious content (Tran et al. 2013).

Public–private partnerships—like the London Action Plan and SignalSpam, a French anti-spam initiative founded in 2005 that established a national spam reporting centre (https://www.signal-spam.fr/)—encourage cross-cultural and cross-jurisdictional cooperation. These partnerships train more skilled cybercrime investigators and information security specialists (ITU 2014; Internet Governance Forum 2014). Enabling harmonisation by reducing cross-border legal barriers that hinder rapid data seizure and preservation by law enforcement should be a priority. The Council of Europe's Cybercrime Convention is a good example of what can be achieved at the regional level and beyond.

However, the absence of universal laws to suppress cybercrime, combined with inadequate law enforcement in many countries, often renders cross-jurisdictional investigations ineffective (Broadhurst 2006). Coordinated cross-jurisdictional operations by law enforcement agencies and the private sector have been crucial in taking down several complex botnets (eg McColo, Gameover ZeuS, Grum and Coreflood; Krebs 2014). For example, a coordinated operation by Microsoft, FireEye, US federal law enforcement agents and the University of Washington reduced spam volumes from 89 billion spam emails in July 2010 to 25b in June 2011. This was the result of taking down two major botnets: Cutwail, which was shut down in August 2010, and Rustock, which was shut down in March 2011 (Microsoft 2011). The demise of Rustock alone led to a drop of about 30 percent in global spam volumes (ITU 2013).

Cybercriminals increasingly use sophisticated tools and methods to distribute a wide range of malicious content, often combining deceptive social engineering with the hosting of phishing sites and identity theft (Smith & Hutchings 2014). Deceptions in spam emails, including disguising malicious executable files as documents and the misuse of URL shortening services, are now commonplace. While some basic elements of earlier spam attacks are still apparent, methods continue to be adapted and modified. Spam is likely to persist in the form of advanced persistent threats, as crime follows opportunity—for example, it may continue in combination with crypto-lockers (ransomware) or via spam that creates botnets and deploys exploits aimed at automated financial activities.

The three biggest trends in spam are:

- sophistication (larger spam botnets that are easier to use and, increasingly, automated, like Gameover ZeuS);
- commercialisation (crimeware-as-a-service, like spam botnets for rent and markets for active email addresses); and
- changes to criminal organisation structures, as when diverse offender groups communicate and collaborate with each other (Grabosky 2013; Thomas et al. 2015).

Spam's role as a vector for the propagation of malware is underestimated. User complacency is another problem, and many victims may overestimate their capacity to detect spam, and especially malware embedded in spam designed specifically to appeal to them. The social engineering used in spam has also become more sophisticated, personalised and compelling, thus improving spam's capacity to deceive users into infecting their systems with malware. Spear phishing is a good example of offender innovation. The use of personal information obtained through deception, or inserting a remote access tool via email or social media with apparently relevant content from a trusted sender, can circumvent countermeasures. The rapid emergence of bespoke email content, tailored to entice a specific victim or type of victim, also poses dangers that call for both targeted education and crime prevention efforts. Platforms like SCAMwatch (www.scamwatch.gov.au) and the Office of the Children's eSafety Commissioner's eSafety site (www.eSafety.gov.au), together with the development of crime prevention practices that focus on current methods of deception, are crucial.

Spam cannot be fought by technical measures alone, and law enforcement agencies must have the capacity to effectively investigate and prosecute cyber criminals. A combination of technology and relevant, up-to-date laws and policies, and the constant reformulation of crime-prevention practices that keep pace with the evolution of spam and malware, are necessary to fight spam. There must be effective partnerships between the state, private actors and multilateral groupings of states, corporations and consumer groups to tackle the cross-jurisdictional essence of spam and malware propagation. Effective partnerships must be formed between law enforcement agencies, academic and private-sector researchers, and stakeholders like ISPs. Support from the information security industry is vital. Constant attention must be paid to any shifts to new vectors for malware attacks. Spam-like methods based on astute and tailored social engineering also require constant attention. The shift to Twitter and other new media is a good example of how URL shortening methods may prosper. While effective civil measures (including anti address-harvesting laws) are in place to mitigate the commercial misuse of spam in Australian cyberspace, the challenge lies in integrating the countermeasures that could further suppress the use of malicious spam.

Maintaining the high level of coordination between industry, government and law enforcement agencies necessary to disrupt malware-driven spam campaigns and other cybercrime must be at the forefront of any government-led initiative. The co-regulatory burdens on industry must be reassessed. 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 to secure continued partnership with government in the fight against cybercrime.

Acknowledgements

The authors thank Dr. Khoi-Nguyen Tran and Professor Peter Grabosky for their contributions to data collection and analysis. The authors acknowledge the assistance of the Criminology Research Advisory Council and the Australian Research Council.

References

URLs correct at June 2016

Alazab M & Venkatraman S 2013. Detecting malicious behaviour using supervised learning algorithms of the function calls. International *Journal of Electronic Security and Digital Forensics* 5(2): 90–109

Anderson R et al. 2013. Measuring the Cost of Cybercrime. In Böhme r (ed.), *The Economics of Information Security and Privacy* IV:. 265–300

BarracudaCentral 2015. *Spam Data.* http://www.barracudacentral.org/data/spam

Broadhurst R 2006. Developments in the global law enforcement of cyber-crime. *Policing: an International Journal of Police Strategies and Management* 29(3): 408–433

Broadhurst R & Chang L 2013. Cybercrime in Asia: trends and challenges. In Liu j, Hebenton b & Jou S (eds), *Handbook of Asian Criminology* New York: Springer:49–63

Broadhurst R, Grabosky P, Alazab M & 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): 1–2.

Chantler A & Broadhurst R 2006. *Social Engineering and Crime Prevention in Cyberspace*. Brisbane: Queensland University of Technology. http://eprints.qut.edu.au/7526/1/7526.pdf

Cisco 2011. *Cisco 2011 Annual Security Report*. http://www.cisco.com/c/en/us/products/security/annual_security_report.html

Cisco 2014. *Spam Hits Three Year High-Water Mark*. http://blogs.cisco.com/security/spam-hits-three-year-high-water-mark/

CYREN 2015. 2015 Cyber Threats Yearbook. http://pages.cyren.com/SecurityYearbook_2015.html

Davis M & Suignard M 2013. *Unicode Technical Report #36: Unicode Security Considerations*. http://unicode.org/reports/tr36/#Bidirectional_Text_Spoofing

European Commission 2009. *EU study on the legal analysis of a Single Market for the Information Society: New rules for a new age?* http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=7022&

FireEye 2013. *FireEye Advanced Threat Report – 2H 2012*. http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2h2012.pdf

Grabosky P 2013. *Organised Crime and the Internet*. *The Royal United Services Institute (RUSI) Journal* 158(5): 18–25. doi: 10.1080/03071847.2013.847707

Hong J 2012. The State of Phishing Attacks. *Communications of the ACM* 55(1): 74–81

Internet Governance Forum 2014. *Best Practice Forum on Regulation and Mitigation of Unsolicited Communications (e.g. "spam").* https://www.intgovforum.org/cms/documents/best-practice-forums/regulation-and-mitigation-of-unwanted-communications/411-bpf-2014-outcome-document-regulation-and-mitigation-of-unsolicited-communications-spam/file

Internet Governance Forum 2015. *Regulation and mitigation of unsolicited communications.* http://review.intgovforum.org/igf-2015/best-practice-forums/regulation-and-mitigation-of-unsolicited-communications/

International Telecommunication Union (ITU) 2013. *Practices to Reduce Spam, Question 22-1/1: Securing information and communication networks: best practices for developing a culture of cybersecurity.* http://www.itu.int/net/wsis/implementation/2014/forum/agenda/session_docs/164/WSIS_10_Spam_WS_Presentations.pdf

ITU 2014. *ITU and Internet Society collaborate to combat spam*. http://www.itu.int/net/pressoffice/press_releases/2014/61.aspx#.VpRYVRV96Uk

Krebs 2011. *'Right-to-Left Override' Aids Email Attacks.* http://krebsonsecurity.com/2011/09/right-to-left-override-aids-email-attacks/

Krebs 2012. *Who's Behind the World's Largest Spam Botnet?* http://krebsonsecurity.com/2012/02/whos-behind-the-worlds-largest-spam-botnet/

Krebs 2014. *'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge.* http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/

London Action Plan 2016. *The London Action Plan*. http://londonactionplan.org/

McAfee. (2013). *Cybercrime Exposed: Cybercrime-as-a-Service*. http://www.mcafee.com/au/resources/white-papers/wp-cybercrime-exposed.pdf

McGuire M 2012. *Organized Crime in the Digital Age*. London: John Grieve Centre for Policing and Community Safety

Mezzour G & Carley K 2014. Spam diffusion in a social network initiated by hacked e-mail accounts. *International Journal of Security and Networks* 9(3): 144–153

Microsoft 2011. *Microsoft Security Intelligence Report, Volume 11, An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software in the first half of 2011*. https://www.microsoft.com/en-us/download/details.aspx?id=27605

Moura G 2013. *Internet Bad Neighbourhoods*. Doctoral thesis, University of Twente, Enschede, Netherlands. http://dx.doi.org/10.3990/1.9789036534604

Mouton F, Leenen L & Venter HS 2016. Social engineering attack examples, templates and scenarios. *Computers & Security* 59: 186–209

OECD 2004. *Background paper for the OECD workshop on spam*. OECD Digital Economy Papers no. 78. http://www.oecd-ilibrary.org/docserver/download/5kz9lkpwj433.pdf?expires=1404874751&id=id&accname=guest&checksum=7EEF887CA79A0C9334103E9784E19103

OECD 2006. *Report of the OECD Task Force on Spam: Anti-Spam Toolkit of Recommended Policies and Measures, No. 114*. Paris: OECD Digital Economy Papers Retrieved from http://www.oecd-ilibrary.org/science-and-technology/report-of-the-oecd-task-force-on-spam_231503010627.

Radicati S & Levenstein J 2013. *Email Statistics Report 2013–2017*. http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf

Rao J & Reiley D 2012. The Economics of Spam. *Journal of Economic Perspectives* 26(3): 87–110.

Smith R & Hutchings A 2014. Identity crime and misuse in Australia: Results of the 2013 online survey. Research and Public Policy series no. 128. Canberra: AIC. http://www.aic.gov.au/publications/current%20series/rpp/121-140/rpp128.html

Sophos 2014. *How to send 5 million spam emails without even noticing*. https://nakedsecurity.sophos.com/2014/08/05/how-to-send-5-million-spam-emails/

Spamhaus 2015. *The World's Worst Spammers*. https://www.spamhaus.org/statistics/spammers

Stone-Gross B, Holz T, Stringhini G, & Vigna G 2011. The underground economy of spam: A Botmasters perspective of coordinating large-scale spam campaigns. *Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats*. Berkely, California: USENIX Association: 4

Stringhini G, Holz T, Stone-Gross B, Kruegel C & Vigna G 2011. BOTMAGNIFIER: Locating Spambots on the Internet. *Proceedings of the 20th USENIX conference on Security.* San Francisco, California: USENIX Association: 1– 16

Symantec 2008. *MessageLabs Intelligence: 2008 Annual Security Report*. http://www.ifap.ru/pr/2008/n081208a.pdf

Symantec 2012. *Symantec Internet Security Threat Report: Trends for 2011, Volume 17*. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

Symantec 2013. *Internet Security Threat Report 2013: Volume 18*. https://scm.symantec.com/resources/istr18_en.pdf

Symantec 2014. *Internet Security Threat Report 19*. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2014.pdf

Takahashi K, Sakai A & Sakurai K 2010. Spam Mail Blocking in Mailing Lists. In K. Nishi (ed.), *Multimedi.* Vukojar, Croatia: InTech

Thomas K et al. 2015. Framing Dependencies Introduced by Underground Commoditization. Paper presented to the 14th Annual Workshop on the Economics of Information Security (WEIS), Delft University of Technology, Netherlands, 22–23 June 2014. http://www.econinfosec.org/archive/weis2015/

Tran K-N, Alazab M & Broadhurst R 2013. Towards a Feature Rich Model for Predicting Spam Emails containing Malicious Attachments and URLs. Paper presented to the Eleventh Australasian Data Mining Conference: AusDM 2013, Canberra, 13–15 November 2013. http://www.iapa.org.au/Event/TheEleventhAustralasianDataMiningConferenceAusDM20

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

UNODC 2013. *Comprehensive Study on Cybercrime*. Vienna: UNODC. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Wall D 2015. Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime. *The European Review of Organised Crime* 2(2): 71–90

Wang D, Irani D & Pu C 2013. Is Email Business Dying? A Study on Evolution of Email Spam Over Fifteen Years. *ICST Transactions on Collaborative Computing, European Alliance for Innovation* 1(1): 1–14

Wang D et al. 2013. Click traffic analysis of short URL spam on Twitter. Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom) 2013. Austin, Texas: IEEE: 250–259

Mamoun Alazab is a lecturer at the Department of Security Studies and Criminology, Macquarie University and a lead investigator at the ANU Cybersecurity Observatory. Roderic Broadhurst is Professor of Criminology Research School of Social Sciences at the Australian National University and at the ANU Cybercrime Observatory.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology. Note: *Trends & issues in crime and criminal justice* papers are peer reviewed. For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: aic.gov.au

ISSN 0817-8542

GPO Box 1936
Canberra ACT 2601, Australia

Tel: 02 6268 7166

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government