Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

ISSN 1836-2206 (Online) | ISBN 978 1 925304 65 7 (Online)

No. 603 September 2020

Abstract | A 10 percent sample of a 2016 dataset of 25.76 million spam emails provided by the Australian Communications and Media Authority's Spam Intelligence Database was scanned for malware using the VirusTotal Malware database. Nearly one in 10 (9.9% or 255,222) emails were identified as malware compromised and, similarly, 9.9 percent were identified as inactive. Of the compromised URL sites, nearly one-third (31.8% or 81,176) could be further classified as phishing (58.4%) or trojan-compromised URLs (40.6%) or dedicated malicious websites (1%). All 115,025 unique file attachments found in the entire sample (0.5% of all spam) were also scanned and 31.4 percent (36,405) were compromised with various forms of malware. The majority of compromised attachments were found in images (55.6%), followed by PDFs (15.0%) and binary files (10.0%). Various trojans and ransomware were the most common malware, and these and others identified in the sample are described.

Malware in spam email: Risks and trends in the Australian Spam Intelligence Database

Roderic Broadhurst and Harshit Trivedi

Introduction

Unsolicited emails, or spam, remain a major vector for the dissemination of malware, and emails are among the most common means of online communication. Spam may only carry benign advertising; however, it can also be a vector for fraudulent schemes or scams that use emails to contact and solicit money from prospective victims (such as through advance fee frauds) or to commit identity theft by deceiving recipients into revealing personal information (such as bank account details and personal data). The menace of manipulative and deceptive emails and associated malware goes beyond commercial losses or identity theft and includes interference with confidential databases and political or electoral processes.

CRG CRIMINOLOGY RESEARCH GRANT

By June 2019, the internet had reached over half of the world's 7.716 billion people (4.536 billion or 58.8%) and continues to grow rapidly in the developing world (Internet World Stats 2019). Disparity remains, however, because internet adoption rates are about 47 percent in developing countries and 19 percent for the least developed countries, compared with 87 percent for the developed countries (International Telecommunication Union 2019). About 88 percent of Australians are actively connected to the internet and 60 percent to Facebook (Internet World Stats 2019). This digital divide also has another dimension—the gap between those digital devices that are secure and those that are insecure. The disparity in security reflects the significant presence of older, insecure (and sometimes pirated) software and hardware, as well as the costs of newer technologies. The digital security divide creates criminal opportunities via the low cost of widely available cybercrime tools that 'attack' older 'legacy' computer software and hardware.

Spam is usually described as unsolicited bulk email with identical content but can include attempts to deceive users into downloading malware. Spamhaus (2018) defines spam as follows:

> An electronic message is 'spam' if (A) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (B) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent…Spam is an issue about consent, not content.

The content can be diverse; 'an advert, a scam, porn, a begging letter or an offer of a free lunch, but that is irrelevant—if the message was sent unsolicited and in bulk then the message is spam' (Spamhaus 2018). The Australian Communications and Media Authority (ACMA) enforces the *Spam Act 2003* (Cth), which also prohibits the harvesting or aggregation of email addresses for the purposes of spam. ACMA emphasises the commercial nature of spam and either a single mail or bulk dissemination of an email classified as spam evokes regulatory intervention.

Spam email also has the potential to compromise computers through malware. Malware is software that secretly accesses a device or network without the user's knowledge. It is used to compromise computer or network functionality, bypass access control, steal or alter data, or otherwise cause harm to the host. Malware can be inserted into a computer via email, hacked websites, online games, compromised toolbars, browser add-ons, music files or indeed anything else that the user downloads from the internet onto a device that is not protected with anti-malware software. Anti-malware software will only protect against malware that has previously been identified. Malware such as a trojan (or 'backdoor' access to a computer) installs code to control a 'compromised' computer and is frequently delivered via a deceptive phishing (spam) email that invites a click to a fake website or attachment.

As well as these dangers, the massive volumes of spam now present can congest the flow of legitimate internet traffic. Spam was estimated to account for about 85 percent of all email traffic by 2018 (Cisco Talos 2018; Symantec 2018a). Statista (2020) estimated that in 2017 average worldwide email volumes were about 269 billion per day and that spam accounted for 48.2 percent of this traffic—mostly related to healthcare or dating. Estimates vary depending on the data sources, which are often cybersecurity service client lists. Kasperksy, a large cybersecurity vendor, reported that 66.5 percent of all emails sent in the first quarter of 2013 were spam and on average 3.3 percent of these contained malicious attachments (Gudkova 2014). However, by 2015 the proportion of spam among emails had fallen to about 55 percent (Vergelis et al. 2015), similar to the proportions (53–55%) identified by cybersecurity providers Symantec (2018a) and Kaspersky for 2015–2017 (Gudkova et al. 2018). Gudkova et al. (2018) note that variants of Trojan-Downloader were the type of malware most often found in spam traffic and that email content used current topics (natural disasters, sporting events, air-ticket giveaways, or cryptocurrency mining promotions) as leads or hooks. Australians, along with internet users in Brazil, China, Qatar and Bolivia, were among those most often targeted.

Criminals use sophisticated tools and methods to distribute a wide range of malware and to steal personal credentials via email, texts, phone calls and social media. These tools often employ deceptive 'social engineering' and individually designed approaches that entice victims to open email attachments or direct them via URL hyperlinks to especially crafted websites, or compromised websites. Essentially, phishing scams are attempts to trick individuals into giving out personal information such as bank account numbers, passwords and credit card numbers (Australian Cyber Security Centre (ACSC) 2018). 'Phishing' emails include generic (eg 'your inbox is full'), individually targeted (or 'spear' phishing) or tailored emails (eg 'whaling'—targeting a specific organisation) that appear to come from a trustworthy source (Australian Competition and Consumer Commission (ACCC) nd). ACCC's Scamwatch, the Australian clearing house for fraud alerts, received 24,292 phishing scam reports in 2018 and 29 percent of these were through email, 41 percent were via phone, 25 percent by text message and 2.5 percent via mobile and other internet applications, a trend that has continued in 2019 (ACCC nd).

Once an attachment to an email is opened or a compromised URL acted upon, control over the computer passes to criminal actors who may exploit the processing power of the computer, harvest sensitive data and alter or misuse data. Although malware differs in its characteristics and mode of replication, all types of malware exhibit similar symptoms on the infected machine, such as an unusually slow computer. Other indicators may include frequent pop-up ads and crashes; strange or odd start-up of the computer; increased CPU usage; freezing or crashing of the host machine; modified or deleted files, or the appearance of strange files and programs; emails being sent automatically without the user's knowledge or consent; and programs running, turning off or reconfiguring automatically.

Malware and spam

Spam, with its mass reach via botnets (networks of computers used to automate mass emails), has been a mainstay for the delivery of malware and a potent means of credential theft, although texting and other forms of messaging now play an increasing role, along with the 'classic' phone call. The increased number of attacks and rising professionalisation among cybercriminals have been at the root of malware's proliferation. According to AV-TEST, an independent IT security institute based in Germany, the presence of malicious programs on the internet has increased almost exponentially in the past 10 years, increasing from 29 million malware programs in 2009 to a massive 780 million in 2018 (AV-TEST 2018).

The estimated annual cost of global cybercrime, including the cost of disruption, was estimated by the Internet Society's Online Trust Alliance (2019) to be US$45b in 2018, including US$8b for ransomware: a newer form of invasive malware used to target a user's confidential data or assets and render them inaccessible until a fee or ransom is paid.

Demand for cybersecurity products and services is expected to increase from US$75b in 2015 to US$175b in 2020 and the cybersecurity insurance industry is projected to grow from US$2.5b to US$7.5b in 2020 (Morgan 2016). The value of cybersecurity services is expected to exceed US$300b by 2024, more than doubling the US$120b estimated for 2017–18 (Bhutani & Wadhwani 2019).

Unsolicited bulk email is banned worldwide by all internet service providers (ISPs); however, 'the countries with the highest number of spammers operating within their networks are usually those with poor or non-existent spam laws' (Spamhaus 2018). Spamhaus (2018) reported that as of August 2018 the United States and China, with 2,941 and 2,697 active spam operations respectively, are the leading sources of spam. Australia ranked 16th because at least one of the major global spam operations may be based in Australia. Numerous incidents of socially engineered emails used to target cyber intrusions have been detected by the Australian Signals Directorate, and frequent advisories and mitigation strategies have been issued to internet users in Australia (ACSC 2017).

The market for malware is growing rapidly, and while there is no discernible trend in the forms of malware or in any specific group of threats, the wide range of methods and tools significantly lowers the technological threshold for potential cybercriminals. As online services become increasingly popular, malware developers are shifting their focus from carrying out malicious breaches to offering their services to others who want to perform these operations. Malware as a Service (MaaS), Crimeware as a Service (CaaS) and Fraud as a Service (FaaS) are now widely available along with the stolen credentials of vulnerable targets on the darknet or illicit cryptomarkets, greatly amplifying the market for malware (Broadhurst et al. 2018: 27–29).

Cybercriminals have used, over many years, the same handful of effective techniques to get malware onto victim devices. Four common vectors or methods used to deploy malware are also identified in our study: phishing, often employing individually designed social engineering approaches (spear phishing); trojanised software; 'watering holes' (eg a fake or compromised website commonly accessed by a particular targeted group); and 'malvertising'. We observed spyware, trojans, adware, ransomware and various viruses among the malware found in the Spam Intelligence Database (SID).

Aims

The Australian National University (ANU) Cybercrime Observatory collaborated with ACMA to access data from SID. This database was developed by ACMA in conjunction with industry partners, including Telstra and Optus, as part of the Australian Internet Security Initiative. Use of SID is subject to a non-disclosure agreement regarding identification of end users. SID does not report whether the spam captured has been identified as spam or acted on by the end user. The data cannot distinguish spam embedded with malware that was ultimately successful from other spam. Nevertheless, it is a useful tool for identifying malware potentially present in Australia. For example, an earlier analysis of 2012 SID found that over a fifth of attachments and URLs embedded in spam emails linked to malware (Alazab & Broadhurst 2016). Spam-borne malware may reflect the presence of new forms or variants of malware and whether targeting or campaigns focus on particular sectors or areas of vulnerability. Thus, examining spam for malware helps in understanding the dynamic nature of cybercrime and the assessment of its risks and harm.

This study describes the malware found in SID between January and September 2016, and the most common file formats used to deliver spam. It examines the relative risk of malware-compromised spam, and the differences between spam that includes malware and spam without malware.

Data and method

The dataset for this study consists of all spam emails for the first nine months of 2016 acquired from Australian internet service providers who participated in the Australian Internet Security Initiative. The data comprised 25,768,090 emails including duplicates or identical emails that were repeatedly sent to Australian email addresses in the first three quarters of 2016. These data were transferred to the ANU Cybercrime Observatory by ACMA over Secure Shell late in 2017. Due to a hardware failure at the ANU Cybercrime Observatory the data for October, November and December 2016 were lost and could not be recovered. The original SID 1.0 data had been archived by ACMA as SID 2.0 became operational in 2018, thus preventing the data from being re-acquired.

The SID data were confidentialised in order to mask the receiver and sender details and protect the identity of the ISP's customers (eg bob@optus.com was changed to id342@a2.com). Additionally, in order to preserve user privacy, only the MD5 (Message-Digest algorithm 5) hash or encrypted values of the attachment files were uploaded to the VirusTotal application programming interface (API). The URLs did not contain any personal information and could be scanned as found.

The email data are composed in MIME format, and this was first extracted, cleaned and then converted to a database (a MySQL database parsed using Python) containing all the available characteristics and features of SMTP emails (date, subject, payload, content type, attachments, email content etc) and the attachment files (file name, content type, MD5 payload, B64 payload etc) and any URLs detected (URL, valid/invalid etc).

The database was also used to store the scan results and associated metadata of the scanned URLs and attachment files. The data were then scanned against the VirusTotal API to check whether the URLs and attachments contained in the emails were malicious.

VirusTotal inspects the submitted items (URLs, files or MD5/SHA1/SHA256 hashes) with over 70 antivirus scanners and blacklisting services (VirusTotal 2018). In this study, we used the HTTP-based public API to query VirusTotal's antivirus network, as this offers bulk uploads of items and downloads of scan reports. Due to the scale of the scanning required and limitations of time and cost, we were only able to scan a random sample of about 10 percent of SID emails for malware. A 10 percent sample of 2,576,709 SID emails were randomly selected for analysis. The sample excluded all 115,025 emails with attachments, which were analysed separately. VirusTotal was generous in assisting this research, and 20,000, and later 50,000, emails per day were scanned without a fee. However, even limited to a 10 percent sample of SID, scanning 50,000 emails per day would require over 500 days to complete the process. Consequently, VirusTotal relaxed the quota for a short period, enabling as many as 200,000 emails per day to be scanned.

Our analysis describes the monthly patterns and trends in spam-borne malware from the features of the URLs embedded in SID emails. The results of this analysis are described in the next section.

Results

Once duplicates in the dataset had been removed, 21,131,389 unique emails were identified. A small fraction of these (0.54%, 115,025) included attachments and about 31 percent of these were identified as compromised by malware. Over half (53%) of all the attachments identified were duplicates (varying from 35% in January to 57% of emails in May), indicating repeated use of some attachments likely linked to a spam campaign. About 10 percent of the sample of spam emails embedded with URLs (255,222) linked to a compromised website. The ratio of duplicate URLs to all URLs was consistently between 12 and 15 percent each month, suggesting that for the most part the absence of concerted or long-term spam campaigns where particular URLs and malware are repeatedly used.

Malware prevalence in URLs

The prevalence, form and monthly trends of malware associated with URLs embedded in spam or file attachments are described in Table 1. The number of attachments and URLs and the proportion malware compromised, invalid or inactive is reported. Table 1 shows nearly one in 10 (9.9% or 255,222) of the URLs were identified as malware-compromised and a further 9.9 percent were identified as invalid or inactive at the time of scanning. Adjusting for inactive URLs, overall 10.8 percent of the URLs were linked to a malware payload. Of the compromised URLs, about 32 percent (*n*=81,176) were further classified by VirusTotal as phishing (58.4%, *n*=47,420), other malware (40.6%, *n*=32,970) or malicious or suspicious websites (0.97%, *n*=786) (see Figure 1).

The data were categorised by month in order to assess trends over the nine months of data available from SID. The monthly distribution of spam emails was not uniform, with surges during February, May and July 2016. These surges suggest the presence of spam campaigns bearing particular malware sometimes targeting Australian email addresses. Variations in the effectiveness of countermeasures also amplify volatility in the mass dissemination of spam.

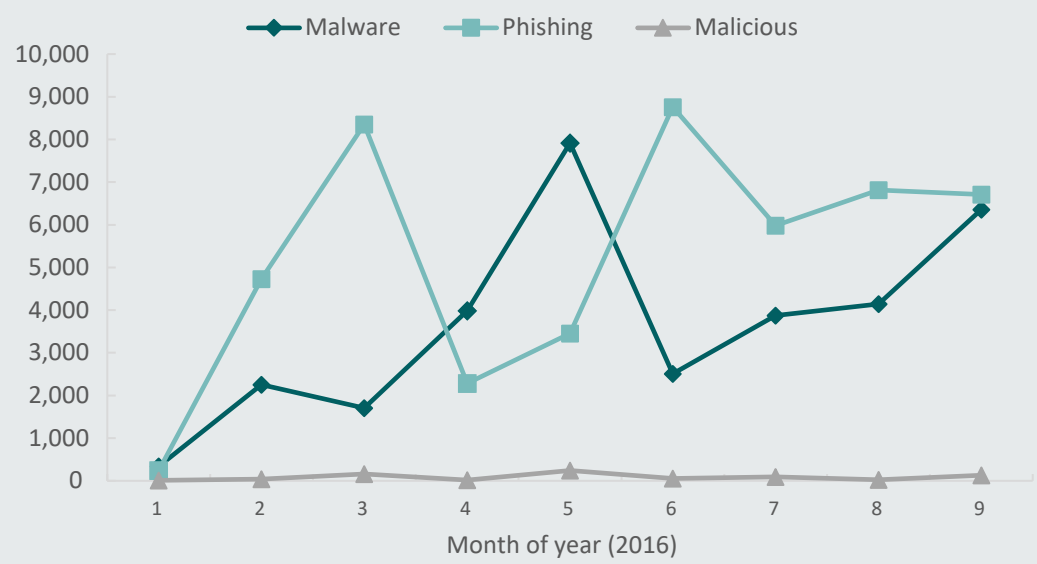
Table 1: Malware found in URLs and attachments in SID

Month (2016)	Unique spam emails (*n*)	URLs (*n*)	Malware present in URLs *n* (%)	Invalid or inactive URLs *n* (%)	Unique file attachments present (*n*)	Malware infected attachments *n* (%)
Jan[a]	208,043	21,930	898 (5.5)	5,506 (25.1)	360	91 (25.3)
Feb	2,814,178	285,621	15,286 (5.6)	12,415 (4.4)	14,104	5,307 (37.6)
Mar	1,079,592	186,208	13,030 (7.1)	3,645 (2.0)	6,938	3,383 (48.7)
Apr	2,900,775	372,297	43,328 (12.8)	35,205 (9.4)	18,649	7,698 (41.3)
May	3,761,801	360,747	45,856 (12.9)	6,663 (1.9)	20,503	7,493 (36.5)
Jun	2,091,183	247,163	20,386 (9.2)	24,447 (9.9)	8,444	2,451 (29.0)
Jul	4,190,704	429,809	42,384 (11.1)	49,595 (11.5)	15,316	3,252 (21.2)
Aug	3,970,088	399,087	45,405 (13.2)	55,591 (13.9)	16,190	4,489 (27.7)
Sep	2,856,089	273,847	28,649 (11.7)	30,036 (11.0)	14,521	2,241 (15.4)
Total	21,016,364	2,576,709	255,222 (9.9)[b]	223,103 (9.9)[b]	115,025	36,405 (31.4)

a: The low number for January 2016 likely reflects undercounting as a result of interruptions to the delivery of spam by ISPs to SIDs through the Australian Internet Security Initiative

b: Denotes the overall proportion

Figure 1: Number of malicious URLs and type of malware by month



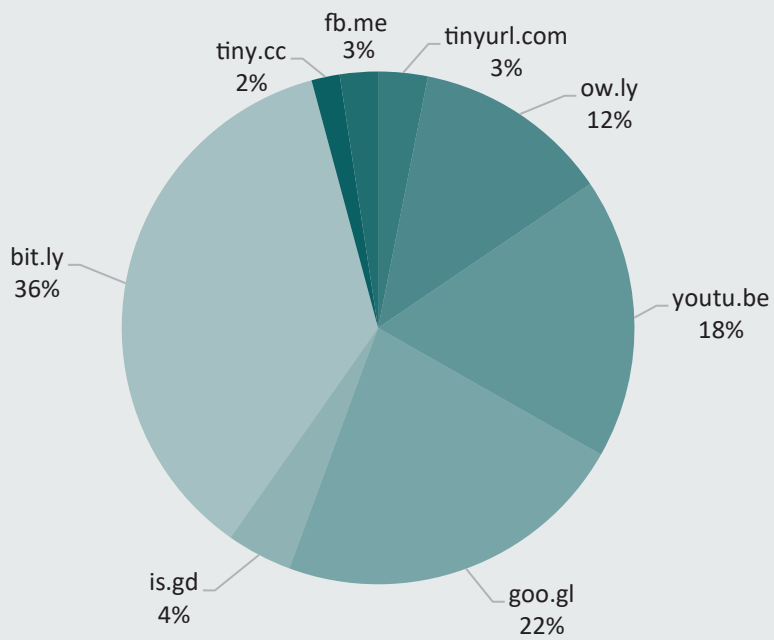
Depending on the month, between 5.5 percent and 13.2 percent of URLs present in spam were malicious, and between 2.0 percent and 25.1 percent of URLs were invalid or inactive and could not be scanned by VirusTotal's antivirus API. VirusTotal results showed almost an equal share between phishing and malware sites (sites that distribute malware). A small number of URLs were classified as 'malicious sites' containing hacking tools (eg targeting victims' banking credentials) or other malware (see Figure 2).

Website URL links were often obscured by various URL shortening services and we next examine the use of these services. This is followed by further analysis of file extensions or attachments, brand or label misuse, and a brief description of the major forms or types of malware detected in SID.

URL shortening

URL shortening services are frequently used when embedding links in emails. These services are also employed by cybercriminals to disguise URLs leading to phishing websites. These services disguise the original domain name and can also deceive antivirus programs into passing them as benign links. Due to this, many URL shortening services have been banned or their use is strongly discouraged. For example, Wikipedia does not accept links that use any URL shortening services (Wikimedia 2018). The Reddit community also strongly discourages their use, and in some subreddits shortened URLs are banned because they lead to storage redundancy and duplication. Our findings suggest that Bit.ly dominated the spam market during 2016, along with other trusted shortening services such as Google (goo.gl) and YouTube (youtu.be), as shown in Figure 2. Note that TinyURL once accounted for 75 percent of the market but by 2016 its share had been reduced to three percent of identified services (Lloyd 2018; TechCrunch 2009). In March 2018, Google shut down support for its link-shortening service and completely shut down the goo.gl service in March 2019 (Montti 2018).

Figure 2: Share of various URL shortening services in the email dataset

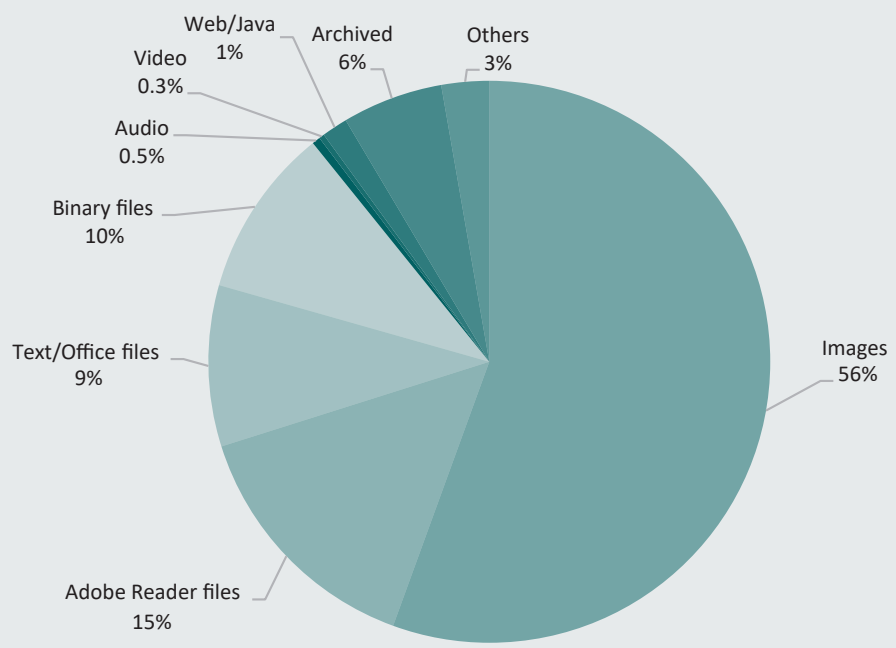


File attachments

Table 1 shows that nearly one-third (31.4%) of the 115,025 unique file attachments identified were compromised. The different formats of attachments were relatively consistently distributed across each month, but many of the attachments and associated malware were re-used more frequently than was found with URLs. Overall, trojans and ransomware (the usual payloads of compromised URLs) were the most commonly found malware in attachments. The attachments in SID came in a variety of different file formats, ranging from various image formats and video and audio files to commonly used zipped archives, PDFs and text documents (see Figure 3). The spread of malware through infected file attachments has long been used as means of compromising computers, although it is now becoming less common due to improved countermeasures. Earlier, executable files (.exe) were used as a vector for malware. However, most email services now block these files from being sent as attachments. Macro-enabled Word and Excel file formats (.docx, .xlsm, .docm) are also commonly used, because malware-embedded macros help avoid antivirus software.

HTML web applications may also be suspect file formats (.htm, .html, .hta, .js, .jar) for ransomware variants, including cryptoviruses such as the Locky and Cerber ransomware tools. Adobe Reader files (.pdf) are less often used for hiding malware due to their tendency to crash when loaded with malicious scripts. However, a workaround exists using 'document inception', where another text document loaded with a malicious macro is included in a PDF document (Biasini et al. 2017).

Figure 3: Distribution of file formats in email attachments



In the 2016 SID dataset 56 percent of all attachments were image files with extensions such as .jpg, .png, .gif, .bmp and .tiff. Of the 64,414 image files, about a fifth (20.6%, 13,261) were related to suspect labels or brands (eg IMG, DCIM, photo, foto). Adobe Reader files (.pdf) accounted for 15 percent of the total, and text/Office document files (.doc, .ppt, .xls, .rtf, .txt) and binary files were among the top four most used file types found in SID (see Figure 3). Attachments carried a variety of payloads, mostly trojans and ransomware (described below), and their presence in attachments by month (including repeated malware attachments) is reported in Table 2.

Table 2: Main malware types found in all attachments by month

Month	Locky ransomware	Nemucod trojan/ransomware	Cerber ransomware	Razy trojan
Jan[a]	3	57	0	313
Feb	5,190	14,757	0	138
Mar	7,903	15,836	4	130
Apr	6,111	24,825	1,055	1,287
May	4,515	12,154	42	425
Jun	256	868	20	144
Jul	342	1,005	4	215
Aug	1,567	6,763	21	64
Sep	2,818	9,187	4	57
Total	28,705	85,452	1,150	2,773

a: The low number for January 2016 likely reflects undercounting as a result of interruptions to the delivery of spam by ISPs to SIDs through the Australian Internet Security Initiative

Note: Duplicate attachments included

The VirusTotal scan of attachments revealed a risky vector, with just under one-third of the attachments returning a positive result, with March (49%) and April (41%) yielding above average numbers of compromised attachments (see Table 1). Table 2 shows the monthly presence of the four most common malware types found embedded in attachments but these were also common payloads on URL-compromised sites.

Misuse of business labels or brands

During our analysis of the file attachment names, we gathered further details on the purpose and, where possible, the content of some of the attachments, based on their names and the brands or labels attached to them. For example, a PDF attachment with the file name DHL-Tracking_Number-xxx-xxx.pdf was crafted to appear to contain the shipment details of a parcel sent through the DHL Express international postal service. However, these labels or brands are covers for malicious attachments with crafted, personalised file names that trick the user into downloading and opening them. File attachments with such fake brands or labels made up about 13.6 percent of the attachments, a substantial number given the risk of credential or identity theft associated with such files (see Table 3).

Table 3: Different business labels/brands in email attachment files

Category	Keywords	Examples	Number of matches
Parcel shipments	FedEx DHL Parcel USPS UPS Post	DHL-Tracking_Number.pdf DHL_Shipping_Details003.pdf Your FedEx Package.docx DHL Postal Receipt.htm	4,599
Tickets and invoices	Tickets Receipt Invoice	TenantInvoice.pdf TransactionReceiptxxxxxxxx.pdf PO Invoice.zip Electronic ticket receipt for xxxx.pdf performa invoice.zip	5,551
Account verification or restoration	Account Verify Restore	Account Verification.html Account Notice.pdf Profile & Account—Verification.pdf SunCorp Car Renewal Account xxxx-xxxx.pdf	1,701
Payments & deposits	Payment Transfer Payslip Deposit	Bank Payment Slip.jar EMAIL! APPROVED PRIZE PAYMENT 2016.pdf Official Payment Letter by Google.pdf PAYMENT OF PRIZE AND CLAIM.docx ANZ_EFT_PAYMENT.lzh WESTERN-UNION PROOF OF TRANSFER.pdf	3,854
Images	Img Picture Photo Foto DCIM	IMG_20151130_153244.jpphoto shoot 131.png PIC-871.jpg photo.jpg	13,261

Common malware types

Analysis of the malware detected by the VirusTotal scan enabled us to identify the main types of payload delivered by the attachment or by the action on the URL hyperlinks. Several common malware types found in SID, usually ransomware or trojan variants, are described next.

The 'JS.Locky.AY1 / Locky Ransomware' encrypts files using Advanced Encryption Standard (AES) 128-bit or the Rivest–Shamir–Adleman (RSA) 2048-bit encryption algorithms stored on the victim's machine. Once the files are encrypted, a text file containing the ransom demand is saved on the system. In some variants, the desktop background is also changed to display the demand (FireEye 2016; TechHive 2018). The ransom file provides instructions on how to pay, usually in bitcoin. In previous iterations of Locky, JavaScript was utilised to download the Locky script but with Trojan-Downloader:JS/Locky the attached JavaScript file also evolved into ransomware. Victims are usually exposed to Locky ransomware via a spam message with a compressed (.zip) file attachment that often contains a JavaScript (.js) file (FireEye 2016). In SID, Locky was identified in 28,705, or nearly a quarter (24.3%), of the compromised attachments.

Variants of the 'Trojan.Downloader.JS.NEMUCOD' (ie JS_NEMUCOD.SMKx) are associated with distributing ransomware (typically Locky), Zeus malware variants and various info-stealers (F-Secure 2018b; McAfee 2018b). These were common in SID (85,452 were identified or 72.4% of compromised URLs). Threats in JS_NEMUCOD are malicious, obfuscated JavaScript files most commonly zipped and attached to spam (Microsoft 2018). These Javascript files connect to a website and download a malicious payload to the computer (Symantec 2018c). The emails used to deliver Nemucod are typically spam, sent out to recipients in mass mailings by the malware's distributors. Nemucod campaigns were prolific in the fourth quarter of 2016 (ThreatMiner 2018) and were particularly prominent in SID in 2016 (especially in March, April, August and September). This trojan is attached to files with '.doc.js' and '.pdf.js' extensions; when executed, it connects to a compromised site that then downloads dynamic library links (DLLs) and other executable files that in turn compromise the operating system in Windows computers (Symantec 2015).

Cerber ransomware is usually sent as an email attachment that locks system functionality, demanding that the victim pay to be able to use their device again. Additionally, it may open 'security back doors', overriding security on the device, and making it more vulnerable to future attacks. Cerber ransomware also browses system files to determine the location of the device. If the device is located in Russia, or surrounding Eastern European countries, it will not activate, and will remain dormant. This ransomware, once activated on a user's device, will remain active even if disconnected from the internet (Kortepeter 2017). As of December 2017, Cerber was active, accounting for 25 percent of all ransomware incidents (Symantec 2018a) but was found in SID in less than one percent (0.97%) of compromised attachments, mostly in one surge in April 2016, when 1,055 of the 1,150 Cerber ransomware found in SID were identified.

The 'W.97M.Downloader' comprises a malicious macro that comes embedded in a Microsoft Word document. The W97M.Downloader (variations '.DAF' and '.AJN') is a Microsoft Word macro financial trojan that is designed to download malware and is propagated through the use of spam or phishing emails (Symantec 2016a). The malicious code is stored in the Visual Basic for Applications (VBA) macro-code in Excel. The macro is placed within the body of the infected documents as well as the macro itself (McAfee 2018a). The file is a simple Word document (a '.doc' or '.docx' file). Common aliases for this trojan include X97M/DownldExe.A (Command), X97M.DownLoader.3 (Dr. Web), VBA/TrojanDownloader.Agent.DZ (ESET), W97M/Agent.KXRS!tr.dldr and TROJ_XLSDROP.WJ (Microsoft 2014). This trojan had a significant impact in 2016 (Gardiner 2016). It was found to be frequently occurring during three of the nine months of available data in 2016 (February, June and July). Other generic script versions of the trojan were also present in SID. For example, the 'HUER: Trojan-Downloader.Script.Generic' is embedded in a script file that opens back doors and grants remote users access to the system, such as specific network ports or by granting firewall exceptions. Additionally, it may also download more malware to the infected device, allowing for further compromises to system security and functionality. Usually, this file will be appended to emails or instant messages as a file attachment (Lynmich 2017).

'Razy Trojan' is a generic Windows trojan that typically spreads bundled with freeware software downloaded from untrusted sites as well as adware toolbars. Other means of infection include email spam campaigns using social engineering to deceive the victims into downloading Razy, and this was observed in SID during April. Crypto-ransomware versions emerged in 2016 and recently a focus on bitcoin mining has been observed. When the intrusion is complete, the virus starts to encrypt the target user's files and adds the '.razy' extension to the affected data. This is a high-impact threat that also works with locally mounted drives, as well as network shares using the Advanced Encryption Standard cipher.

Discussion

The manipulation of trust and the deceptive use of spam is a significant and 'tried and true' vector for computer intrusion. Measures to deal with malware-bearing spam remain largely reactive and thus less effective against constantly novel spam email formats that effectively disguise malware payloads. Therefore, the ability to identify new spam attacks that include malware payloads (either via URL web links or attachments) without waiting for updates from spam scanners or blacklists would help reduce the risk of victimisation. Scanners attempt to filter suspect emails but often miss novel variants of malware and/or deceptive content and necessarily draw on a variety of sources, often dated, to identify malicious content (Alazab & Broadhurst 2016; Tran et al. 2013).

Compared to the 13.45 million spam emails captured throughout 2012 by SID and scanned for the presence of malware by Alazab and Broadhurst (2016), attachments remain a high risk. Of the 492,978 spam emails with attachments in SID 2012, 21.4 percent were malicious, compared to 31.4 percent in the present study. The prevalence of attachments, however, declined from 3.7 percent of all spam in 2012 to 0.54 percent of spam in 2016. Of the 6.23 million emails in SID 2012 that contained a URL, 22.3 percent of the web links were malicious but only 10.8 percent were found to be malicious in SID 2016.

One potentially useful measure against malicious spam has been to develop machine learning techniques that routinely check on the content of emails, attachments and suspect URLs, and can match suspect websites or URLs, attachments and socially engineered email content with known blacklists provided by services such as VirusTotal. Machine learning methods for identifying spam and improving filtering methods must be responsive to changes in spamming techniques, but have not yet been sufficiently adaptable to variations in either content or delivery methods and often fail to recognise carefully crafted phishing attacks.

For some time, the mantra 'technical solutions cannot tackle spam alone' has been widely acknowledged because it recognises that human error, insider threats and poorly implemented countermeasures contribute to the opportunities for cybercrime. The importance of a focus on the unsolicited nature of spam is more fruitful because 'legislators spend inordinate amounts of time attempting to regulate the content of spam messages, and in doing so come up against free speech issues, without realizing that the spam issue is solely about the delivery method' (Spamhaus 2018).

Observational studies of the effectiveness of phishing show that tailored and individualised malware-bearing spam can have high rates of success (Broadhurst et al. 2019). Cybercrime awareness education may be the long-term solution, but constant tinkering and criminal innovation require such prevention strategies to be dynamic and flexible.

Fighting spam requires a combination of technology and crime prevention strategies. While effective civil measures help mitigate commercial misuse of spam in Australian cyberspace, a significant problem is how to suppress the spam–malware vector and the malware–exploit markets that are the engines of innovation and distribution. The communication-centric nature of the internet also provides the means for the mitigation of such tactics via rapid responses and consumer alerts (US Department of Homeland Security 2016: 9).

The creation of effective partnerships between law enforcement agencies and stakeholders such as ISPs and the private sector is vital. Supporting the development of both individual and industry-level cybercrime prevention and self-help strategies has led to industry–government coordination focusing on the disruption of malware-driven spam campaigns as well as education about phishing, ransomware and other intrusions.

Conclusion

The SID emails examined here suggested that, although attachments were much less common than in SID 2012 emails, where attachments are present they are more likely to include malware. Compromised URLs are also less common than in the 2012 SID emails but malware-embedded web links continue to use shortening services, to spoof trusted services and to carry potent payloads such as trojan downloaders and ransomware.

SID contains useful features for further analysis, such as the content of spam emails, which could be valuable in distinguishing malware-bearing spam from other spam. Further analysis and research are warranted given that spam may also help identify new malware variants and social engineering scripts. If active rather than retrospective versions of SID were available to researchers, this would provide 'live' data to develop and test a dynamic detection system for spam-borne malware.

The mass dissemination of spam-borne malware affects us all, but what can be done to reduce the prevalence of malware as a criminal service, and the relative ease and low cost of acquisition? Continued monitoring and exploration of the main facilitators of cybercrime, such as darknet digital product markets, specialist malware forums, and spam and social media vulnerabilities, is warranted. Research is also needed on the most effective means of suppressing cybercrime via better digital trace technologies and enhanced prevention strategies including 'target hardening' and 'crime proof' design standards and practices. Partnerships between governments, industry and academia will also be crucial in responding to the opportunities for cybercrime in a period of uncertainty and disruption driven by rapid social and economic change.

Acknowledgements

We thank Bruce Mathews and Daniel McNamara of ACMA, and Svetla Yankova and Karl Hiramoto of VirusTotal. We also thank Nguyen Tran, Nick Sifniotis, David Lord, Christopher Bugler, Corey Johnston, Donald Maxim and the anonymous reviewers for their assistance.

References

URLs correct as at May 2020

Alazab M & Broadhurst R 2016. *Spam and criminal activity. Trends & issues in crime and criminal justice* no. 526. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi526

Australian Competition and Consumer Commission (ACCC) nd. Whaling & spear phishing. https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing/whaling-spear-phishing

Australian Cyber Security Centre 2018. Phishing. https://www.cyber.gov.au/threats/phishing

Australian Cyber Security Centre 2017. Malicious email mitigation strategies guide. https://acsc.gov.au/publications/protect/malicious_email_mitigation.htm

AV-TEST 2018. Malware statistics & trends report. https://www.av-test.org/en/statistics/malware/

Bhutani A & Wadhwani P 2019. Global cyber security market size worth $300bn by 2024. *Global Markets Insights*. https://www.gminsights.com/pressrelease/cyber-security-market

Biasini N, Brumaghin E, Mercer W & Grady C 2017. Jaff ransomware: Player 2 has entered the game. Talos, 12 May. https://blog.talosintelligence.com/2017/05/jaff-ransomware.html

Broadhurst R et al. 2018. *Malware trends on 'darknet' crypto-markets: Research review*. Report for the Korean Institute of Criminology. https://ssrn.com/abstract=3226758

Broadhurst R, Skinner K, Sifniotis N, Matamoros-Macias B & Ipsen YG 2019. Phishing and cybercrime risks in a university student community. *International Journal of Cybersecurity Intelligence & Cybercrime* 2(1): 4–23

Cisco Talos Intelligence Group 2018. Email and spam data. https://talosintelligence.com/reputation_center/email_rep

FireEye 2016. Threat research: Locky ransomware. https://www.fireeye.com/blog/threat-research/2016/08/locky_ransomwaredis.html

Fortinet. 2017. Threat Reports: Threat Landscape Report. Retrieved July 11, 2018, from: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report.pdf

F-Secure 2018a. Trojan-Downloader: JS/Locky. https://www.f-secure.com/v-descs/trojan-downloader_js_locky.shtml

F-Secure 2018b. Trojan Downloader.JS.Nemucod. https://www.f-secure.com/v-descs/trojan-downloader_js_nemucod.shtml

Gardiner B 2016. Financial institutions at growing risk of trojan attacks: Report. https://www.cio.com/article/3497548/financial-institutions-at-growing-risk-of-trojan-attacks-report.html

Gudkova D 2014. *Kaspersky security bulletin: Spam evolution 2013*. https://securelist.com/kaspersky-security-bulletin-spam-evolution-2013/58274/

Gudkova D, Vergelis M, Shcherbakova T, Demidova N 2018. Spam and phishing in 2017. https://securelist.com/spam-and-phishing-in-2017/83833/

International Telecommunication Union 2019. *Measuring digital development: Facts and figures 2019*. Geneva: ITU Publications. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

Internet Society's Online Trust Alliance 2019. *2018 Cyber incident & breach trends report*. https://www.internetsociety.org/breach2019/

Internet World Stats 2019. Usage and population statistics. http://www.internetworldstats.com/stats.htm

Kortepeter D 2017. Cerber ransomware: How it works and how to handle it. http://techgenix.com/cerber-ransomware/

Lloyd S 2018. The entire history of URL shorteners: From TinyURL to Twitter's t.co. https://blog.rebrandly.com/the-history-of-url-shorteners/

Lynmich S 2017. HEUR.Trojan.Script.Generic Virus manual removal guide. Yoo Care. https://blog.yoocare.com/heur-trojan-script-generic-virus -manual-removal-guide/

McAfee 2018a. McAfee Labs threat advisory: W97M/Downloader: X97M/Downloader. https://kc.mcafee.com/corporate/index?page=content&id=KB91920&locale=en_US

McAfee 2018b. Virus profile: Nemucod. https://home.mcafee.com/virusinfo/virusprofile.aspx?key=9609531#none

Microsoft 2018. Malware encyclopedia: Nemucod. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=JS/Nemucod

Microsoft 2014. TrojanDownloader: W97M/Adnel. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanDownloader:W97M/Adnel

Montti R 2018. Goo.gl shutting down: These are your options. https://www.searchenginejournal.com/goo-gl/246569/

Morgan S 2016. Cyber crime costs projected to reach $2 trillion by 2019. https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6f43cdd63a91

Scamwatch 2019. Scam statistics. https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=29&date=2019

Spamhaus 2018. The definition of spam. The Spamhaus Project. https://www.spamhaus.org/consumer/definition/

Statista 2020. Global spam volume as percentage of total e-mail traffic from January 2014 to December 2019, by month. https://www.statista.com/statistics/420391/spam-email-traffic-share/

Symantec 2018a. *Internet security threat report, volume 23.* https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Symantec 2018b. Malicious code classifications and threat types. https://support.symantec.com/en_US/article.HOWTO101622.html

Symantec 2018c. Writeup: Nemucod. https://www.symantec.com/security-center/writeup/2015-120112-4419-99

Symantec 2017. *White paper: ISTR ransomware 2017*. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf

Symantec 2016a. W97M.Downloader | Symantec. https://www.symantec.com/security-center/writeup/2014-110100-2117-99

Symantec 2016b. Ransom.Cerber. Symantec. https://www.symantec.com/security_response/earthlink_writeup.jsp?docid=2016-030408-0817-99

Symantec 2015. JS.Nemucod. https://www.symantec.com/security-center/writeup/2015-120112-4419-99

TechCrunch 2009. URL shortening wars: Twitter ditches TinyURL for bit.ly. https://techcrunch.com/2009/05/06/url-shortening-wars-twitter- ditches-tinyurl-for-bitly/

TechHive 2018. Locky ransomware. https://images.techhive.com/images/article/2016/02/locky-ransomware-100645181-large.jpg

ThreatMiner 2018. *AV: JS.Nemucod.E.* https://www.threatminer.org/av.php?q=JS.Nemucod.E

Tran KN, Alazab M & Broadhurst R 2013. Towards a feature rich model for predicting spam emails containing malicious attachments and URLs. 11th *Australasian Data Mining Conference* (AusDM 2013), Canberra, Australia, in Zhao YC, Kok-Leong Ong KL, & Liu L (eds), *Conferences in Research and Practice in Information Technology* (CRPIT), vol. 146

US Department of Homeland Security 2016. *Malware trends*. Industrial Control Systems Emergency Response Team (ICS-CERT) and Advanced Analytical Laboratory (AAL). https://www.us-cert.gov/sites/default/files/documents/NCCIC_ICS-CERT_AAL_Malware_Trends_Paper_S508C.pdf

Vergelis M, Shcherbakova T, Demidova N & Loseva D 2015. *Kaspersky security bulletin: Spam and phishing in 2015*. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07194944/KSB_SpamPhishing_2015.pdf

VirusTotal 2018. Reports: VirusTotal. https://support.virustotal.com/hc/en-us/articles/115002719069-Reports

Wikimedia 2018. Spam blacklist: Meta. https://meta.wikimedia.org/wiki/Spam_blacklist

Roderic Broadhurst is a Professor of Criminology at the Australian National University.

Harshit Trivedi is a Research Assistant at the Australian National University's 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 1836-2206 (Online)

ISBN 978 1 925304 65 7 (Online)

GPO Box 1936
Canberra ACT 2601, Australia

Tel: 02 6268 7166

aic.gov.au