FROM THE EXECUTIVE PRESIDENT

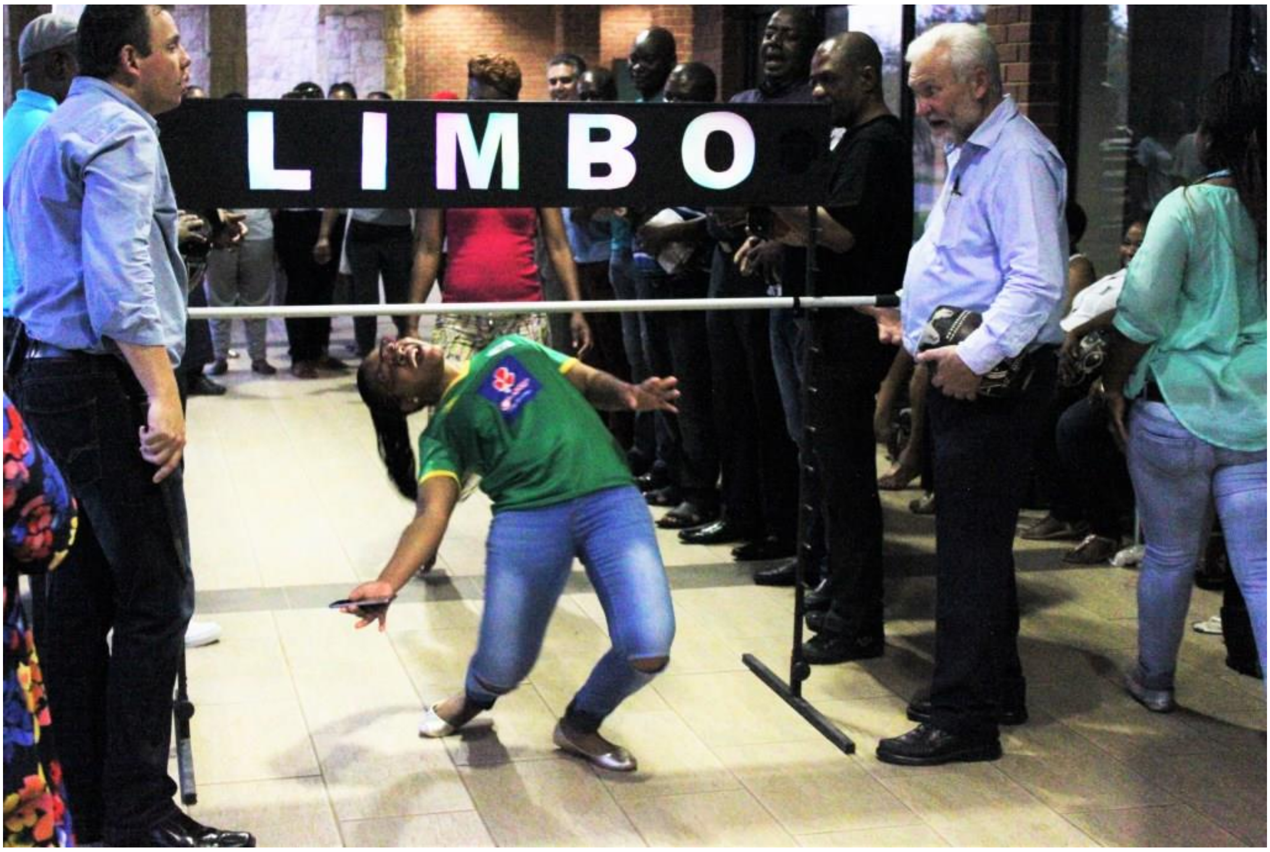
I saw a cartoon where an interviewer asked the interviewee “If the earth rotates 30 times faster, what will happen?” The person then answered convincingly “We will get our salary everyday”…..
It seems to me that time goes by quicker and quicker every year. Here we are already at the end of 2016. We all had prepared lists of what we wanted to do in 2016 and if your time has been like mine….. we didn’t get to do everything on our lists….
With SAIMAS the year also flew past and we hosted a few memorable events throughout the year.

SAIMAS hosted a workshop in September “A STRUCTURED WAY TO ASK THE RIGHT QUESTIONS TO ARRIVE AT THE RIGHT ANSWERS”

The workshop was well attended and the attendees asked Dr. Cisca du Plessis the right questions on the day and it was valued by all.

As always the annual SAIMAS conference did not disappoint at all.

“People, Process & Performance – Pathway to Success” was the theme for the 26th Annual Conference held from 26 to 28 October 2016 at the Euphoria Golf estate and Hydro in Limpopo. The conference content exceeded all expectations and after the limbo dancing competition some had stiff muscles where they never realized they had muscles before, see photo below.



SAIMAS would like to thank all of you for the continued support throughout the year. Without your support and attendance there would be no SAIMAS.

Thank you to all the Council members for your time and efforts spent to make the running of SAIMAS as an Institute as smooth as possible.

A very special word of thanks goes out to Ms. Gerda Morrison, our Office Administrator, for all your hard work and support and the work behind the scenes.

I trust that you all will have a Blessed Festive season and safe journeys wherever you travel for a break.

SAIMAS greetings

Ben Gouws

The ‘Dark Side of the Net’

Article series: Part One

By : Dr Marcus Leaning
Senior Fellow
School of Media and Film
University of Winchester, Winchester, United Kingdom
eMail: marcus.leaning@winchester.ac.uk

and

Udo Richard Averweg
IT Project Manager
Information Management Unit
eThekwini Municipality, Durban, South Africa
eMail: udo.averweg@durban.gov.za

Introduction

This article is the first in a series that considers what we may term the ‘dark side of the net’. This series will look at a number of practices and activities on the internet that either verge on the illegal or are illegal. Such practices and activities can have serious consequences for how organisations function and we discuss these in the hope that readers may have their awareness and understanding of these issues reinforced.

We commence the series with a discussion of the activity of spam as this often serves as a gateway to and facilitator of many other forms of illicit behavior (Krebs, 2014). We understand spam to refer to the mass sending of unsolicited messages - most typically emails. We do recognise that the term spam is also used to refer to other types of unsolicited communication, such as personal messaging, texting and communication on virtual forums. Spam accounts for a significant proportion of all email traffic and though the prosecution of key spam senders often has an impact upon the total volume, such actions tend to be short lived and new spammers soon take their place. Spam email currently amounts to 86% of all email traffic (Robertson, 2016) though much spam is caught in the various filters on servers and email clients in organisations. Indeed only approximately 30% of spam sent gets through the various filters (Stone-Gross, Holz et al., 2011).

Spam is sent so as to make some form of financial gain for the sender. As will be discussed below, the various ways in which the financial benefit is achieved is varied but the main purpose is to induce some action on the part of the recipient that will facilitate the sender of the spam email obtaining benefit.

Though much spam is sent from legitimate organisations as part of their marketing campaigns, a significant proportion of unsolicited email traffic is sent by or criminal or semi-legal activity and it is this aspect that we focus upon in this article. Indeed Brian Krebs, an internet security expert, sees a strong link between criminally orientated, spam email and organised crime. We commence with a discussion of the mechanics of how spam are distributed and then move onto to examine the different types of spam emails currently circulating. We also offer some advice for mitigating against the damage spam can have on an organisation.

The spam eco system

Spammers make use of a number of different campaign techniques to increase the success rate of spam emails. Spam email campaigns tend to be differentiated by the level of particularity of the email. At one end of the spectrum is the 'spear phishing' technique in which emails are crafted for particular people (information about the target is gained through web searching and 'social engineering' – contacting the organisation and using charm and simple lies obtaining information about the people and organisation). The information is then used to craft emails that are likely to get through spam filters and be opened and actioned by the intended targets. At the other end of the spectrum is the mass emails sent out to millions of people simultaneously. Such emails require the assistance and collaborative activity of computer system penetration experts and other types of hackers.

Central to the sending of mass spam emails are email lists - these are the large lists of email addresses of potential recipients. Email lists can be composed in a number of ways including the manual and automated gathering of emails from various sites and services. Email lists can also be purchased or rented (when buying a list, the actual email addresses are sold; when renting a list, the organisation who owns the list will send out the emails) through various legitimate services which collate email addresses that have been entered on legitimate sites such as surveys or acceptances of service for free wi-fi. Such lists can be specific and relate to key demographics and psychographics. Email lists are also sold by hackers who purposefully break into an organisation's central records (such as billing systems or customer databases) to steal email addresses (Spammer-X, 2004). In some cases such lists are highly valuable as the proportion of genuine, active email addresses to inactive or false ones tends to be very high. The sale of such lists and the contracting for the commission of thefts of specific lists of email addresses is conducted through various ‘dark markets’ – venues for the trading of illegal merchandise on the internet or through personal contacts.

Botnets

The sending of spam emails for illicit purposes cannot be done through usual email practices which would reveal the spammers identity and make them liable to prosecution and other forms of sanction. Accordingly spammers often make use of what is termed botnets (robot network) or zombie armies: networks of private computers that have been infected with viruses (which were typically delivered by a spam email). The viruses on such computers operate often undetected and while allowing the legitimate user of the computer to carry on working causing the computer to carry out other tasks simultaneously (hence the label zombie). For spammers the most common task is to transform the computers in the botnet into a device that can send and relay emails in a complex network (Stone-Gross, Holz et al., 2011). Such compromised computers are used to send and pass on spam emails and to replace details of the originating sender with a fake name. The growth, use and maintenance of botnet armies is a practice often conducted by acolyte hackers as it can be achieved through the use of ‘off-the-shelf’ hacking software packages. Such packages involve the hacker infecting private computers with a virus and then using a control application to launch email campaigns (or other activities such as a deliberate denial of service attacks on particular web sites or services) from the infected machines.

Types of criminal spam

We broadly identify four main types of criminally orientated, mass spam emails:

- The first type are emails that serve a marketing purpose for a product. In these emails the product is often ‘real’ – that is there is a definite product or service for sale though its effectiveness, fidelity or genuineness may vary. Examples of such emails include sales emails for various personal or sexual issues such as the ‘enlargement’ of various organs, adverts for pornography sites, adverts for illegal articles such narcotics, software or pirated media texts or adverts for cheap replica medicines and drugs (such emails are primarily targeted at citizens of countries with expensive private medical systems in which medicines would be out of the reach of most people. The emails do often offer medicines that are similar to those available in pharmacies but are produced outside of the legitimate supply chain and thus may not be as effective as the genuine drugs);

- A second common form of spam email are those emails termed advanced fee fraud and classified under the Nigerian Penal code as 419 violations. Such emails are varied and function by alerting the recipient to a possible large financial reward for their willingness to engage in a smaller transaction such as sending an ‘advance fee’. Of course the larger financial reward will never materialise and the recipient may need to send more money. A variant of this approach is to send a spear fishing attack claiming to be from a friend of the recipient and that they have been robbed or lost a bag while abroad and need emergency cash sent to them;
- A third approach involves attacking the recipient’s computer. This form of spam will often contain a link or a file which will install a virus upon the recipient’s computer. The viruses can serve a number of functions. The least serious involves using the computer as part of a botnet army to send out further emails to others. A similar use is for the recipient’s computer to be used in a distributed denial of service attack against a web host or other computer. Both such activities will involve slowing the host computer down but not damaging it so much that the recipient will want to have the decline in function investigated and remedied as to do so would involve the virus being removed (this mirrors the action of certain viruses in the natural world where ‘killing he host’ results in the virus not spreading so viruses evolve only to incapacitate their host to ensure their propagation). More severe are viruses that disable the host’s computer and demand a ransom fee payable to the sender in exchange for a code that will unlock the computer. Failure to provide the fee within a short period of time will result in an increase in the fee and eventually encrypting of all the information on the computer. Virus are also used to secure personal details from host computers that can be used in identity theft; and
- A fourth approach involves the recipient being sent what appears to be an email from their bank or other service (such as PayPal) requesting they log in to their account using the link provided – in some instances the email will seek to cause alarm in the recipient so as to encourage rapid action. The linked bank login page is a fake and the user will provide their login details to the fraudster. The details can then be used to steal money and other identity fraud activities.

Many organisations have software filters and rigorous user guidelines to prevent spam emails and hacking incursions. However, skilled spammers and hackers can circumvent such systems with original and cunning tricks. One of the authors of this article recently fell victim to an attack; this involved the use of a spam email that contained the header ‘printer malfunction’ and was spoofed so as to appear to come from the ‘ITHelpDesk’. Unfortunately the spam email arrived moments after a document had been sent to print. The author concluded that something had gone wrong with the printing (the printer was in a room on another floor and so could not be checked) and it was an automated response from the networked printer. The email contained a link which was said to lead to the printer queue – however, upon clicking the link it installed a virus. Remedying the situation involved having the computer reformatted and the user account frozen (and passwords on all internal accounts changed) until it could be determined that no further damage could occur. This resulted in significant inconvenience to the user and a delay of nearly two days. This then had an impact on other parts of the organisation for which time dependent tasks were pending. Even though the user was mindful of the many ways spammers and hackers work, the serendipitous timing plus a brief lack of thoroughness resulted in significant time wastage, inconvenience and a cost to the organisation.

Concluding remarks

While spam emails are relatively inexpensive to the sender, they can prove to be costly to an organisation. Spam emails invariably ‘rob’ organisations of valuable lost productive time when employees attempt to determine the legitimacy (and resultant deletion) of such emails. Furthermore there is also the cost of extra storage space which has been purchased for spam emails that have been quarantined until they are automatically purged. Accordingly, for organisations, we advocate a continuous promotion of anti-spam awareness raising activities (such as an organisation’s intranet) alongside rigorous technical means of spam defence. Such technical defence mechanisms for mitigating the resultant damage of spam in an organisation, should include plans and implementation schedules drawn up by reputable anti-spam consultants.

In the internet’s dark economy, spam email is often both annoying to an employee and can be harmful to an organisation. When an email address appears to be sending spam email, the most likely cause is that the email account has been compromised (or spoofed) via hacking. In our second article in this series on the ‘dark side of the net’, we discuss the activity of hacking.

Further reading

Krebs, B., (2014). Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door. Sourcebooks.

Robertson, J., (2016). E-Mail Spam Goes Artisanal. Bloomberg Technology 2016.

Spammer-X, (2004). Inside the SPAM Cartel: By Spammer-X. Syngress Publishing, Inc.

Stone-Gross, B., Holz, T., Stringhini, G. and Vigna, G., (2011). The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. LEET 11: 4-4.