International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Pre-Emptively Block Dynamic IP Ranges and Impose Stringent Requirements on other Servers Wishing to Deliver Mail

J. Praveen Kumar[1], P. Ravali[2], K. Manideep Goud[2], M. Srikanth Reddy[2]
[1]Assistant Professor, Department of Information Technology in Teegala Krisha Reddy Engineering College,Telangana, India
[2]UG Scholar, Department of Information Technology in Teegala Krisha Reddy Engineering college, Telangana, India

ABSTRACT

Spam is legally permissible according to certain criteria. If the spam fails to comply with any of these requirements it is illegal. To combat the problems posed by botnets, open relays, and proxy servers, many email server administrators pre-emptively block dynamic IP ranges and impose stringent requirements on other servers wishing to deliver mail. Forward-confirmed reverse DNS must be correctly set for the outgoing mail server and large swaths of IP addresses are blocked, sometimes pre-emptively, to prevent spam. These measures can pose problems for those wanting to run a small email server off an inexpensive domestic connection.In this paper we give an Blacklisting of IP ranges due to spam emanating from servers and IP range.

Keywords : *IP Range, DNS..*

I. INTRODUCTION

Email spam, also known as junk email, is a type of electronic spam where unsolicited messages are sent by email.Many email spam messages are commercial in nature but may also contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments (trojans). Spam is named after Spam luncheon meat by way of a Monty Python sketch in which Spam in the sketch is ubiquitous, unavoidable and repetitive.

Spammers collect email addresses from chatrooms, websites, customer lists, newsgroups, and viruses that harvest users' address books. These collected email addresses are sometimes also sold to other spammers.

Definition:

Unsolicited bulk email (UBE)—unsolicited email, sent in large quantities.

Unsolicited commercial email (UCE)—this more restrictive definition is used by regulators whose mandate is to regulate commerce

Replica	5.40%
Enhancers	2.30%
Phishing	2.30%
Degrees	1.30%
Casino	1%
Weight Loss	0.40%
Other	6.30%

Table 1: Spam general topics

Sending spam violates the acceptable use policy (AUP) of almost all Internet service providers.

Providers vary in their willingness or ability to enforce their AUPs. Some actively enforce their terms and terminate spammers' accounts without warning. Some ISPs lack adequate personnel or technical skills for enforcement, while others may be reluctant to enforce restrictive terms against profitable customers.

As the recipient directly bears the cost of delivery, storage, and processing, one could regard spam as the electronic equivalent of "postage-due" junk mail.[2][19] Due to the low cost of sending unsolicited email and the potential profit entailed, some believe that only strict legal enforcement can stop junk email. The Coalition Against Unsolicited Commercial Email (CAUCE) argues "Today, much of the spam volume is sent by career criminals and malicious hackers who won't stop until they're all rounded up and put in jail.

II. PROPOSAL OVER VIEW

Accessing privately owned computer resources without the owner's permission is illegal under computer crime statutes in most nations. Deliberate spreading of computer viruses is also illegal in the United States and elsewhere. Thus, some common behaviors of spammers are criminal regardless of the legality of spamming *per se*. Even before the advent of laws specifically banning or regulating spamming, spammers were successfully prosecuted under computer fraud and abuse laws for wrongfully using others' computers.

The use of botnets can be perceived as theft. The spammer consumes a zombie owner's bandwidth and resources without any cost. In addition, spam is perceived as theft of services. The receiving SMTP servers consume significant amounts of system resources dealing with this unwanted traffic. As a result, service providers have to spend large amounts of money to make their systems capable of handling these amounts of email. Such costs are inevitably passed on to the service providers' customers.

Spammers may engage in deliberate fraud to send out their messages. Spammers often use false names, addresses, phone numbers, and other contact information to set up "disposable" accounts at various Internet service providers. They also often use falsified or stolen credit card numbers to pay for these accounts. This allows them to move quickly from one account to the next as the host ISPs discover and shut down each one.

Spammers frequently seek out and make use of vulnerable third-party systems such as open mail relays and open proxy servers. SMTP forwards mail from one server to another—mail servers that ISPs run commonly require some form of authentication to ensure that the user is a customer of that ISP. Open relays, however, do not properly check who is using the mail server and pass all mail to the destination address, making it harder to track down spammers.

The first known spam email, advertising a DEC product presentation, was sent in 1978 by Gary Thuerk to 600 addresses, which was all the users of ARPANET at the time, though software limitations meant only slightly more than half of the intended recipients actually received it.[36] As of August 2010, the number of spam messages sent per day was estimated to be around 200 billion.[37] More than 97% of all emails sent over the Internet are unwanted, according to a Microsoft security report.[38] MAAWG estimates that 85% of incoming mail is "abusive email", as of the second half of 2007. The sample size for the MAAWG's study was over 100 million mailboxes.

Origin of spam

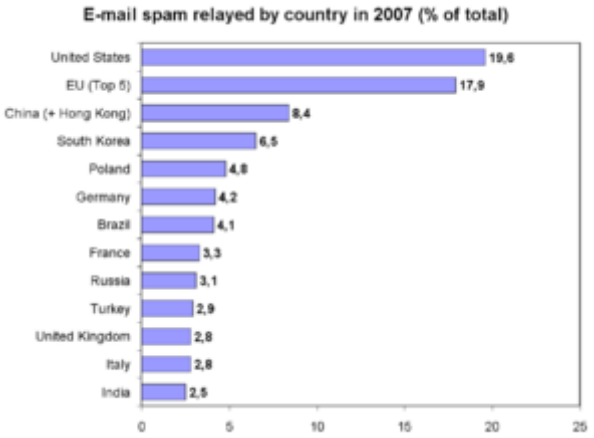

Figure 1: Email spam relayed by country in Q2/2007.

III. PRACTICAL VIEW

Origin or source of spam refers to the geographical location of the computer from which the spam is sent; it is not the country where the spammer resides, nor the country that hosts the spamvertised site. Because of the international nature of spam, the spammer, the hijacked spam-sending computer, the spam vertised server, and the user target of the spam are all often located in different countries.

Some popular methods for filtering and refusing spam include email filtering based on the content of the email, DNS-based blackhole lists (DNSBL), greylisting, spamtraps, enforcing technical requirements of email (SMTP), checksumming systems to detect bulk email, and by putting some sort of cost on the sender via a proof-of-work system or a micropayment. Each method has strengths and weaknesses and each is controversial because of its weaknesses. For example, one company's offer to "[remove] some spamtrap and honeypot addresses" from email lists defeats the ability for those methods to identify spammers.

Outbound spam protection combines many of the techniques to scan messages exiting out of a service provider's network, identify spam, and taking action such as blocking the message or shutting off the source of the message.

In order to send spam, spammers need to obtain the email addresses of the intended recipients. To this end, both spammers themselves and *list merchants* gather huge lists of potential email addresses. Since spam is, by definition, unsolicited, this *address harvesting* is done without the consent (and sometimes against the expressed will) of the address owners. As a consequence, spammers' address lists are inaccurate. A single spam run may target tens of millions of possible addresses – many of which are invalid, malformed, or undeliverable.

Sometimes, if the sent spam is "bounced" or sent back to the sender by various programs that eliminate spam, or if the recipient clicks on an unsubscribe link, that may cause that email address to be marked as "valid", which is interpreted by the spammer as "send me more". This is illegal under most anti-spam legislation. However, a recipient should not automatically assume that an unsubscribe link is an invitation to be sent more messages: if the originating company is legitimate and the content of the message is legitimate, then individuals should unsubscribe to messages or threads or mailing lists they no longer wish to receive.

IP-range filtering is a packet filtering to try to prevent source address spam of mail traffic, and thus indirectly combat various types of botnet abuse by making Internet traffic traceable to its source.After tracing the IP-range the network ingree filtering are defined by RFCs 2827,3704 and BCP 84 respectively.

BCP 84 recommends that upstream providers of IP connectivity filter packets entering their networks from downstream customers, and discard any packets which have a source address in the IP-range framed as illegal which is not allocated to that customer.

There are many possible ways of implementing this policy; one common mechanism is to enable reverse path forwarding on links to customers, which will indirectly apply this policy based on the provider's route filtering of their customers' route announcements.

IV. CONCLUSIONS

The Area of Internet marketers, unsolicited commercial email (also known as spam) has become a major problem on the Internet. To detect the IP addresses of repeatedly coming spam mails is proposed. The proposed framework exploits both IP-range and mail streaming in advance and further processing of low-level features. This work promises to enhance the spam-filtering domain in future.

V. REFERENCES

[1]. Kim W, RanJeong O, Kim C, So J. The dark side of the Internet: Attacks, costs and responses. Information Systems. 2011; 36(3):675–705.

[2]. Sawwashere S, Srivastava S, Lanjewar A, Bhilare DS. Optimizing DDOS attacks using LCIA. International Journal of Application or Innovation in Engineering and Management (IJAIEM). 2013; 2(12):11–17.

[3]. Preetha G, Kiruthika Devi BS, Shalinie SM. Autonomous agent for DDoS attack detection

and defence in an experi¬mental testbed. International Journal of Fuzzy Systems. 2014; 16(4):520–8.

[4]. Beitollahi H, Deconinck G. Analyzing well-known countermeasures against distributed denial of service attacks. Computer Communications. 2012;