ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Indian Journal of Science and Technology, *Vol 9(4), DOI: 10.17485/ijst/2016/v9i4/84803, January 2016*

An Analysis of Modern Approaches to the Delivery of Unwanted Emails (Spam)

D. S. Silnov*

Department of Information Systems and Technologies, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia; ds@silnov.pro

Abstract

Background: A new way of spam sending was discovered. Old spam techniques not effective now, spammers find new ways. **Analysis:** The analysis shows that spammers find new ways to bypass very efficient tools to catch spam like DNSBL, SPF and some others. **Findings:** New discovered approach uses cheap domain names and cheap hosting services to imitate legal mail servers. **Conclusion:** New anti-spam tools needed to fight against new spam sending wave.

Keywords: Email Spam, Filters Bypass, Spam Filtering, Spam Hosting

1. Introduction

Spam servers deploy multiple technologies. Up until mail servers started receiving and analyzing email messages, the servers were analyzing remote mail servers on "trustworthiness". The server checks the IP address of a remote host and decides whether to accept or reject the incoming email message. At the moment, such technologies include DNSBL (checking to see if an IP address is blacklisted), checking the PTR records of IP addresses and mail domain, SPF and the recent DKIM and some others[1]. Spam problem related not only to e-mail services, but also to some social networks[2,3].

2. Analysis of Technologies used

The PTR record of an IP address is contained in the host DNS server. The mail server, which received a message, checks the sending server's domain contained in email headers with the PTR record of the IP address from which that message is sent. If the PTR record is different from this domain, the message is marked as spam. If there is no PTR record, the message is also marked as spam. Only the owner of the IP address block – mainly hosting companies – can change a PTR record.

With SPF technology, a special line is added in the DNS record of the domain[4]. The line indicates which servers are allowed to send mail messages. The recipient mail server checks the address of the sending server with the DNS record. If the sending server is not included in the list of trusted servers, the email message is marked as spam, and in some cases, simply rejected by the server.

For DKIM[5], a digital signature is added to the email message. With this signature, the recipient server certifies that the mail message was actually sent from the server contained in the email header.

DNSBL (DNS Ban list or DNS Blocklist) are lists of DNS host records that were previously noticed in spam sending[6]. When prompted to receive an email message, the mail server checks the IP address of the remote host with the list of undesired addresses previously noticed in spamming. If the IP address is in blacklists, the mail server regards the received message as spam and refuses to receive it[7]. The remote host is most often notified of refusal to accept a message.

**Author for correspondence*

To date, these technologies have helped in fighting spam efficiently. If spam is sent with substitution of the sender's address, the mail server will effectively detect this substitution and mark the email message as spam.

Technologies for installation of proxy/socks services on hacked computers were once popular among spammers. The services were (invisibly to the user) installed either on compromised servers that had constant Internet connection or on PCs of online users with the help of malware. These proxy/socks servers were used to send out spam from the hacked computers. Today, such spamming methods have become inefficient thanks to emergence of modern anti-spam tools (explained above). Most spam messages sent through socks/proxy services don't reach the end user[8,9].

Spammers continue to adapt and find new methods of bypassing spam filters[10]. Over the past two months, the number of spam messages that bypassed the spam filters described above and reached the end-user has increased significantly. After analyzing the contents of messages, one can, with total probability, argue that these emails are spam. Such messages were analyzed and innovations were identified in the issue of spamming.

3. Analyzing the Problem

Detailed analysis revealed a new technology used by spammers. In order to understand how they managed to bypass spam filters, we had to examine thoroughly the logs of the mail server and headers of spam messages.

First, we checked the reverse record of the sending server. To do this, we made a request for the reverse record by the IP address of the sending server. The reverse record received matches the server address from the field 'sender'. Consequently, the message passes this test.

Spammers use their own domains to send spam. Spam sending requires large number of domains. To reduce the cost of spamming, the cheapest domains are used. When buying with a discount from the registrar, the *co.ua domains go for a minimum price of US$3, thus securing minimal expenses. The *.ru domains are also cheap (the author of this article can register such domains for just US$1.5). The low price makes these domains suitable for spamming.

DNS records of the ******.co.ua domain confirm that a message was sent from the specified mail server. The rule prescribed says that if the IP address of the server is different from the specified in *A* and *MX* records of the domain, the message won't pass the server filter check.

Among the many domain names, we choose one: insteras.co.ua.

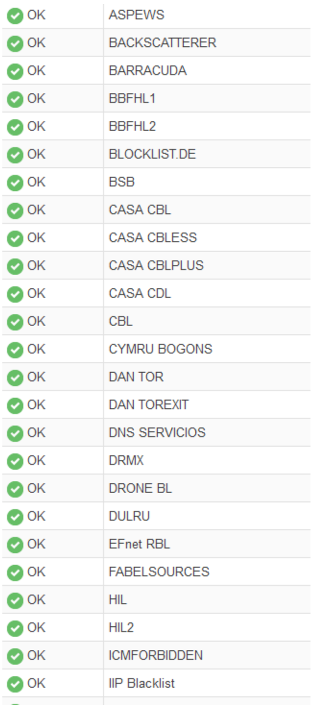
116.13.25.85.in-addr.arpa. 5078 IN PTR mail.isteras.co.ua.

2015-11-30 11:13:23 Delay 0 for mail.isteras.co.ua [85.25.13.116] with HELO=isteras.co.ua. Mail from avpoyyj@isteras.co.ua

isteras.co.ua. 960 IN TXT "v=spf1 a mx -all"

Another way of fighting spam is to compare the sender's IP address and server domain with public lists. These lists contain IP addresses that send spam messages.

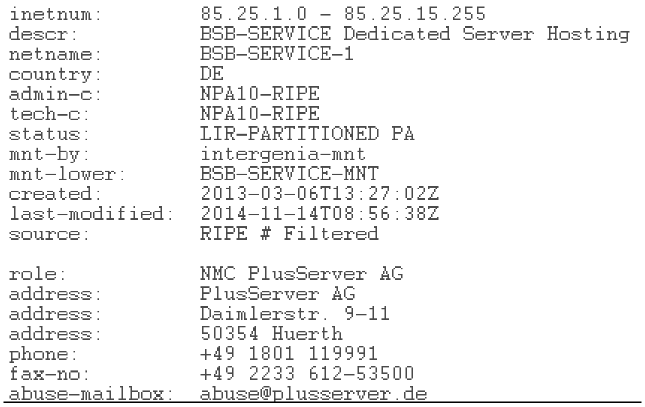
The domain of the sender's server and its IP address were checked on the Spamhaus site. It was shown that the lists contain no records with IP range to which this server belongs. This means that these messages will pass the blacklist check. Among many other databases, this IP address is also not listed in the blacklist (Figure 1)



✓ OK	ASPEWS
✓ OK	BACKSCATTERER
✓ OK	BARRACUDA
✓ OK	BBFHL1
✓ OK	BBFHL2
✓ OK	BLOCKLIST.DE
✓ OK	BSB
✓ OK	CASA CBL
✓ OK	CASA CBLESS
✓ OK	CASA CBLPLUS
✓ OK	CASA CDL
✓ OK	CBL
✓ OK	CYMRU BOGONS
✓ OK	DAN TOR
✓ OK	DAN TOREXIT
✓ OK	DNS SERVICIOS
✓ OK	DRMX
✓ OK	DRONE BL
✓ OK	DULRU
✓ OK	EFnet RBL
✓ OK	FABELSOURCES
✓ OK	HIL
✓ OK	HIL2
✓ OK	ICMFORBIDDEN
✓ OK	IIP Blacklist

Figure 1. Result of IP checking in DNSBL.

85.25.13.116 is the IP address of the server from which spam is sent and to which the domain is linked. Analysis of WHOIS information of the service makes it clear that this address is part of a block of IP addresses belonging to an organization called Plus server and registered in Germany (Figure 2). The cheapest price for a virtual server at one of the sites belonging to Plus server is €13. Plus server operates under a reselling program, where it acts as a data center that services incoming requests, while intermediaries that are not explicitly listed on the site are the ones directly involved in the sale of virtual servers.



```
inetnum:        85.25.1.0 - 85.25.15.255
descr:          BSB-SERVICE Dedicated Server Hosting
netname:        BSB-SERVICE-1
country:        DE
admin-c:        NPA10-RIPE
tech-c:         NPA10-RIPE
status:         LIR-PARTITIONED PA
mnt-by:         intergenia-mnt
mnt-lower:      BSB-SERVICE-MNT
created:        2013-03-06T13:27:02Z
last-modified:  2014-11-14T08:56:38Z
source:         RIPE # Filtered

role:           NMC PlusServer AG
address:        PlusServer AG
address:        Daimlerstr. 9-11
address:        50354 Huerth
phone:          +49 1801 119991
fax-no:         +49 2233 612-53500
abuse-mailbox:  abuse@plusserver.de
```

Figure 2. Whois information about given spam.

To bypass spam filters, the DNS PTR record is registered for each IP address involved in spam sending. For the insteras.co.ua domain, the reverse zone looks like this:

116.13.25.85.in-addr.arpa. 30461 IN PTR mail.isteras.co.ua.

The owner of the IP address block registers the PTR record in the DNS. As a rule, when renting a virtual server, such service is not standard, and by default, a PTR record matches with the name of the host server. Hence the conclusion that spammers don't use standard virtual server service. They somehow manage to register the PTR record for IP addresses belonging to plus server. Therefore, it is concluded that Plus server pays insufficient attention to issues of spamming from its servers.

4. Conclusions

It is obvious that spammers link their domains to rented servers, add necessary DNS records, set up a PTR record, install and configure mail servers. This makes it impossible to add the mail server into the 'spamming' category by standard methods.

Statistics on the amount of spam messages from *co.ua domains under the technology described is presented in the graph in Figure 3. Data were taken from the logs of the mail server. The graph shows that in two months, there was increased activity of spam emails. It also shows that the activity is uneven in a week. The highest amount of spam is recorded on weekdays. The volume of spam decreases on weekends. On Sundays, there are almost no spam messages sent.

Prosecuting spammers legally is also not possible as they use very cheap domains in the co.ua zone. The only way to combat this type of spam in the present circumstances is to block domains from which the spam messages are sent or even to block the entire *co.ua domain zone in the case of mass deployment of similar technologies.

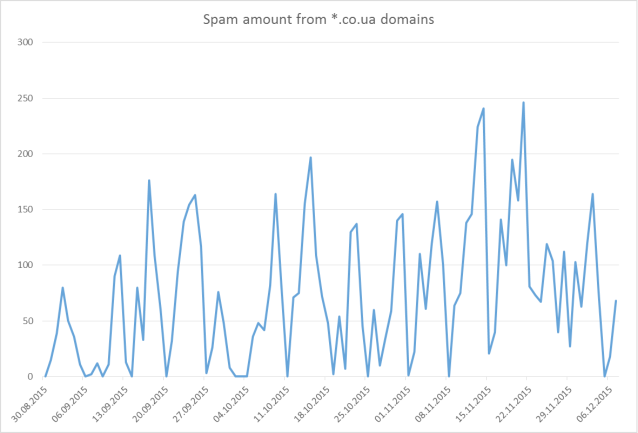


Figure 3. Spam amount from *.co.ua domains per day.

5. References

1. Almomani A, Obeidat A, Alsaedi K, Al-Hazaimeh Obaida M, Al-Betar M. Spam E-mail Filtering using ECOS Algorithms. Indian Journal of Science and Technology. 2015 May. 8(S9). Doi:10.17485/ijst/2015/v8iS9/55320.
2. Anbazhagu UV, Praveen JS, Soundarapandian R, Manoharan N. Efficacious Spam Filtering and Detection in Social Networks. Indian Journal of Science and Technology. 2014 Nov; 7(S7). Doi: 10.17485/ijst/2014/v7iS7/61956.
3. Adamkani J, Nirmala K. A Content Filtering Scheme in Social Sites. Indian Journal of Science and Technology. 2015 Dec; 8(33). Doi:10.17485/ijst/2015/v8i1/80128.
4. Sipahi D, Dalkilig G, Ozcanhan MH. Detecting spam through their Sender Policy Framework records. Security and Communication Networks. 2015 Dec; 8(18):3555–63.
5. Kataria S, Bansal D, Sethi P. Domain Keys Identified Mail. Networking and Communication Engineering. 2015; 7(6):260–64.
6. Lewis C, Sergeant M. Overview of best email DNS-based list (DNSBL) operational practices. 2012 Jan; 1–21.

7. Ramachandran A, Feamster N, Dagon D. Detecting botnet membership with dnsbl counterintelligence. In Botnet Detection. Springer: US. 2008; 131–42.
8. Hameed S, Kloht T, Fu X. Identity based email sender authentication for spam mitigation. In Eighth International Conference on Digital Information Management (ICDIM), Islamabad. 2013 Sep 10-12. p. 14–19.
9. Ferreira N, Carvalho G, Pereira PR. A Scalable Spam Filtering Architecture. In Technological Innovation for the Internet of Things. Springer Berlin: Heidelberg. 2013; 107–14.
10. Leiba B, Ossher J, Rajan VT, Segal R, Wegman MN. Method for recognizing spam email, U.S. Patent No. 7,475,118. Washington, DC: U.S. Patent and Trademark Office. 2009; 1–8