Change of the National Top-Level Domain and its Influence to Some Spam Detection Characteristics

Slobodan Mitrović[1], Slaviša Aćimović[2], Slađana Janković[3], Norbert Pavlović[4], Sanjin Milinković[5]

Abstract – **In this paper some experiences related to spam detection and change of national top-level domain in Republic of Serbia are presented. Email and spam detection statistics as well as efficiency of several spam detection tests before and after this change are considered. Presented statistics are based, as example, on the MTA log and spam-filter data of the Faculty of Transport and Traffic Engineering Computer center in Belgrade.**

Keywords – **email, spam detection, national top-level domain, statistics**

I. INTRODUCTION

One of the most important Internet services is electronic mail (email) service that uses Simple Mail Transfer Protocol (SMTP) for transfer of messages. This type of service has some security disadvantages which make it suitable for spam delivering. During last decade spam is identified as one of major threats for business or other kinds of activities, especially in systems with large number of employees, such as national corporations (i.e. Railways) or Internet corporations that host webmail services (i.e. Google, Yahoo, Microsoft (Live mail), etc.). This was the primary motive for many institutions to build email filtering mechanisms and monitoring service that collects data about email traffic.

Some major changes, such as change of national top-level domain (nTLD) have crucial influence to many features of the Internet traffic of the corresponding country. This reflects to email traffic structure, and also to efficiency of spam detection filters. In Section II the concept of used email filter and email monitoring is briefly presented, as well as collected statistics before and after nTLD change. Section III presents some of the most successful anti-spam filtering tests before this change and their efficiency afterwards. This will be followed by corresponding conclusions presented in Section IV.

[1]Slobodan Mitrović is with the Faculty of Transport and Traffic Engineering, University of Belgrade, Vojvode Stepe 305, 11000 Belgrade, Serbia, Email: s.jankovic@sf.bg.ac.rs.

[2]Slaviša Aćimović is with the Faculty of Transport and Traffic Engineering, University of Belgrade, Vojvode Stepe 305, 11000 Belgrade, Serbia, Email: slavisa@sf.bg.ac.rs.

[3]Slađana Janković is with the Faculty of Transport and Traffic Engineering, University of Belgrade, Vojvode Stepe 305, 11000 Belgrade, Serbia, Email: s.jankovic@sf.bg.ac.rs.

[4]Norbert Pavlović is with the Faculty of Transport and Traffic Engineering, University of Belgrade, Vojvode Stepe 305, 11000 Belgrade, Serbia, Email: n.pavlovic@sf.bg.ac.rs.

[5]Sanjin Milinković is with the Faculty of Transport and Traffic Engineering, University of Belgrade, Vojvode Stepe 305, 11000 Belgrade, Serbia, Email: s.milinkovic@sf.bg.ac.rs..

II. EMAIL STATISTICS BEFORE AND AFTER NTLD CHANGE

Republic od Serbia as successor of former Yugoslavia used national TLD "***.YU***" until 2009 when IANA assigned new TLD "***.RS***", with transition period that ended on March, 31st of 2010.

During last 15 years, many of users' email addresses were ended in spammers' databases because of various security issues, which leaded to increase of unwanted email traffic amount. This was primary reason for our Computer center to engage security measures, in order to make email service more usable and friendly for end users. The concept of security measures is based following structure: our email system consists of *Postfix* MTA [1] integrated with *SpamAssassin* anti-spam filter [2] and *Syslog-NG* logging engine [3] that collects log data for all activities related to email traffic. Further, collected log data is statistically processed by Mailgraph [4], which uses RRDtools [5]. This is internally called *PSRM integration* [6], which has many similarities with other standardized *Postfix* integrations.
This means that incoming messages are tested against *Postfix SMTP* rejection rules that consist of HELO, sender and recipient restrictions. The goal of this standard procedure is rejecting sessions from any system that fails to identify itself. Further, those messages that passed this primary filter are tested with anti-virus and anti-spam filters, respectively. Infected messages are passing through cleaning procedure. Message that is identified as spam, if not rejected by primary filter, ends in mailbox called *spamcontainer*. Content of the message is modified with brief description how the message has been qualified as spam. Original content is placed as attachment.

In this way, increase of local email traffic and also unnecessary increase of amount of local users' mailbox is avoided. In case of *false-positive* message, end user can look for it by searching the content of *spamcontainer* mailbox. Further, this mailbox is used for collecting information related to spam characteristics.

Statistics that are presented in this paper are collected in the last 12 months before change of national TLD and also in the first 12 months after this change. Those statistics that are related to amount of detected spam and infected messages are given in Table 1.

TABLE I
EMAIL STATISTICS BEFORE AND AFTER THE CHANGE OF NATIONAL TLD

Message type / period	March 2009 - March 2010	April 2010 - March 2011
Total	2.692.324	291.899
Rejected by primary filter	2.032.849	159.680
Messages with virus content	6.624	482
Identified spam	471.515	8.695
Regular messages	181.336	123.042

Statistics presented in Table 1. show significant decrease of amount of incoming messages after change of national TLD, which is graphically presented in Fig 1. It could be also noticed that more than 93% of all incoming messages have been treated as unwanted before the change of national TLD. This ratio decreases to almost 58% in the first year after the change of national TLD.

Some additional issues related to presented statistics must be taken into consideration:

- Various end user surveys show presence about 4% of *false negatives* and 0.5% of *false positives* in corresponding mailboxes, in period before this change.
- There have been increased amount of rejected regular emails in first two weeks after the change of national TLD, because recipients' email addresses have not been updated by many uninformed senders that use domestic Internet Service providers (ISP). This is important issue, because many domestic ISPs didn't remove all DNS records related to old TLD. This is also shown in Fig. 1.

Furthermore, it have been noticed increased ratio of *false positives* after change national TLD, because *SpamAssassin* filter trigger have been tuned with *combined score* that is not appropriate to be used in new situation. In order to improve results, some additional assessments had to be done.

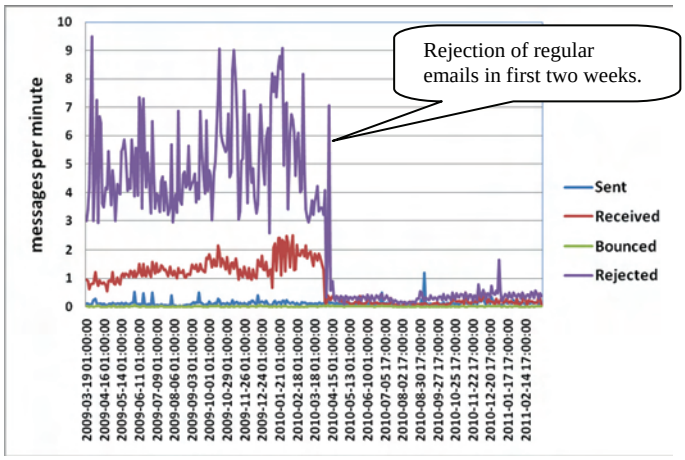

Fig. 1. Email statistcs before and after change of national top-level domain

III. SPAMASSASSIN FILTERING BEFORE AND AFTER NTLD CHANGE

SpamAssassin is used in our *PSRM integration* as secondary mail filter, for the purpose of spam determination. This flexible and powerful set of Perl programs, unlike older spam filtering approaches, uses the *combined score* from multiple types of checks to determine if a given message is spam [2]. Its primary features are [2]:

- Header tests
- Body phrase tests
- Bayesian filtering
- Automatic address whitelist/blacklist (AutoWhitelist)
- Manual address whitelist/blacklist (ManualWhitelist)
- Collaborative spam identification databases (DCC, Pyzor, Razor2)
- DNS Blocklists, also known as "RBLs" or "*Realtime Blackhole Lists*"
- Character sets and locales.

The scores are assigned using a neural network trained with error back propagation (*Perceptron*). Both systems attempt to optimize the efficiency of the rules that are run in terms of minimizing the number of *false positives* and *false negatives* [2].

During years before change of national TLD *SpamAssassin* engine that belongs to our *PSRM integration* used *combined score* trigger value of **6.5**, which was determined as optimal for our email service in terms of minimizing the number of *false positives* and *false negatives.* Significant increase of *false positives* in first several weeks after change of nTLD indicated a need for determination of new optimal *combined score* triggers value. Hence, it has been lowered to value of 4, but after only one week it has been additionally lowered to value of 3. Lowering of this value has been done on empiric basis because of emerging need for decreasing *false positives* rate.

Spamcontainer mailbox content was analyzed in order to identify those *Spamassassin* tests that have crucial weight in scoring process of spam determination, before and after nTLD change. In this purpose, *spamcontainer* messages are divided in two groups, called *Before* and *After*. Mailbox group *Before* was analyzed first. This group contains 417515 spam messages that have been identified in last 12 months before nTLD change. In first turn, there have been extracted four groups of spam messages:

- Messages that contain keyword *Viagra*. These messages were automatically redirected to *spamcontainer*, upon header checks.
- Messages that contain keyword *Rolex*. These messages were also automatically redirected to *spamcontainer*, upon header checks.
- Messages that were identified by *SpamAssassin* as type *Nigerian 419*.

- Messsages cought by blacklist which was created within *SpamAssassin* with score value of 100.

In second turn, there have been extracted another nine groups of spam messages, regarding frequency of test with score that was crucial for message to be qualified as spam:

- HELO_DYNAMIC_IPADDR - *Relay HELO'd using suspicious hostname* (score 4.4). An untrusted relay used an IP address as a HELO argument during a SMTP transaction.
- FORGED_MUA_OUTLOOK - (score 4.2). Spammer's client is trying to pretend to be an MS Outlook
- FH_DATE_PAST_20XX - *The date is grossly in the future* (score 3.6)
- BAYES_99 (score 3.5)
- BAYES_95 (score 3.0)
- HTML_IMAGE_ONLY (score 2.6)
- HELO_DYNAMIC_DHCP-*Relay HELO'd using suspicious hostname* (score 2.6). An untrusted relay used a hostname (FQDN) as a HELO argument during a SMTP transaction that appears to suggest a dynamically allocated hostname. [2].
- BAYES_80 (score 2.6)

Spam statistics related to these tests are presented in Fig. 2.

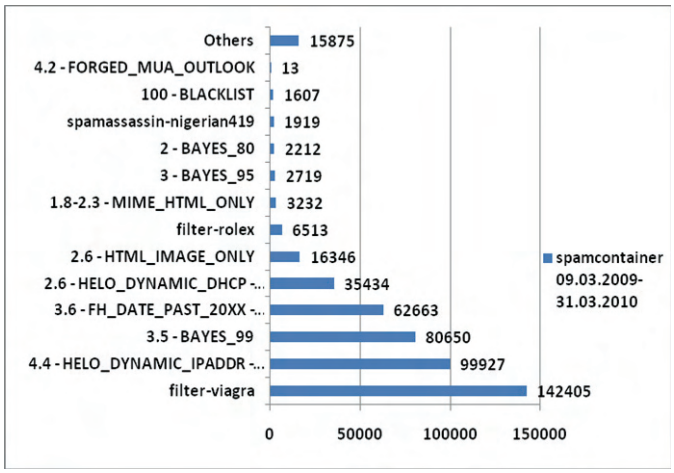

Fig. 2. Spam detection statistics before change of national top-level domain

These nine tests with score that was crucial for message to be qualified as spam, as well as four specific tests were used to analyze mailbox group *After*. This mailbox group contains 8695 spam messages that have been identified in first 12 months after change of national TLD. Statistics related to tests applied on this mailbox group are shown in Fig. 3.

In order to determine types of spam that has not been affected by change of national TLD, presence of determined tests in mailbox groups *Before* and *After* has been compared, as it shown in Fig. 4.

It could be noticed that only one test has almost identical level of presence on both mailboxes. It is test called HELO_DYNAMIC_IPADDR with score value of 4.4. Other

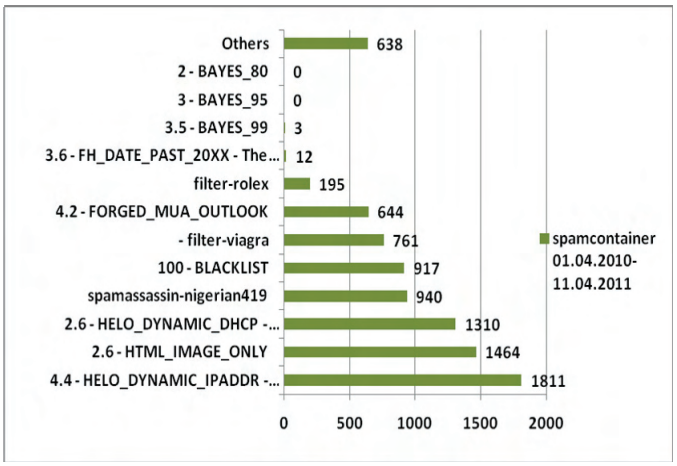

Fig. 3. Spam detection statistics after change of national top-level domain

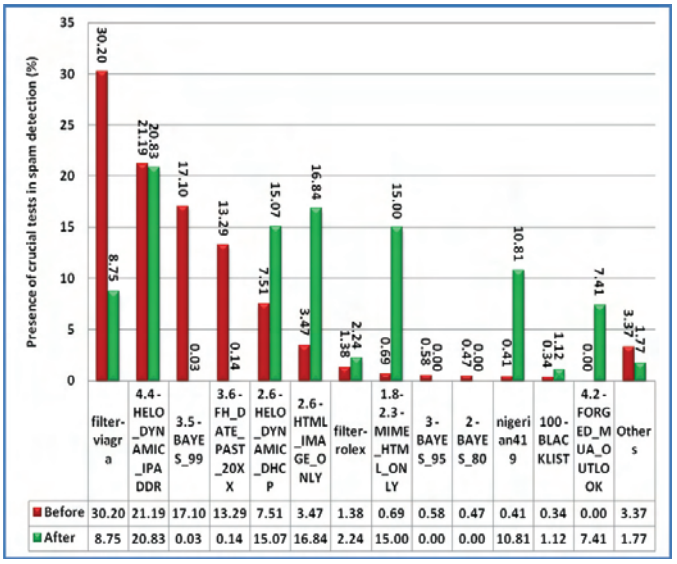

Fig. 4. Presence of determined tests in mailbox groups *Before* and *After*

tests have almost opposite levels of presence, with exception of *Nigerian 419* spam messages which level of presence is seems to be independent of other tests' occurring frequencies. This can be logically explained in terms of nature of this spam type [7].

It could be also noticed that tests related to *Bayes* analysis lost crucial role in spam detection in *After* mailbox group, comparing to their efficiency before change of national TLD. In that period BAYES_99 test has been the most successful test, while BAYES_95 and BAYES_80 just "helped" other tests in reaching of *combined score* trigger value for targeted spam.

Each other *SpamAssassin* test has insignificant level of presence in *Before* mailbox group comparing to levels of those nine tests. Similar situation could be found in mailbox group *After*, with exception of BAYES_95 and BAYES_80 tests which are included in comparative purposes.

IV. Conclusion

In this paper the change of national top-level domain and its influence to email delivery and spam filtering is considered. In the first several weeks after this change, significant amount of regular emails that have been originated from domestic senders has been rejected, because of inconsistent DNS records.

SpamAssassin filter maximized its efficiency in spam determination, using neural network trained with error back propagation as well as optimal *combined score* trigger value regarding amount of spam attacks during last several years before change of national TLD. This efficiency has been disrupted after nTLD change, which is confirmed by several important issues, such as increased number of *false positives*, that involved the need for modification of *combined score* trigger value. Improving efficiency of Bayesian filter in presence of decreased number of spam attacks would be subject of some future analysis.

Change of national TLD involved significant decrease of spam attacks, because spammers email address listings obviously became out-of-date. This is new chance for network administrators to increase security measures in order to protect end users from email addresses harvesting.

Acknowledgement

This work is partially supported by the Ministry of the Science and technological development of the Republic of Serbia under No. 036012.

References

[1] www.postfix.org, (03.04.2011)
[2] http://wiki.apache.org/spamassassin/ (05.04.2011)
[3] http://balabit.com/network-security/syslog-ng, (03.04.2011)
[4] http://mailgraph.schweikert.ch, (03.04.2011)
[5] http://oss.oetiker.ch/rrdtool/doc/rrdtool.en.html, (03.04.2011)
[6] S.Mitrović, V.Radojičić, “A new approach in tracking efficiency of anti-spam filter”, XLV International Scientific Conference on Information, Communication and Energy Systems and Technologies, Proceedings of Papers: ICEST 2010, Ohrid, Makedonija, str. 345-348
[7] Cukier W.,Nesselroth E.,Cody S.,Genre, "Narrative and the "Nigerian Letter" in Electronic Mail", 40th Annual Hawaii International Conference on System Sciences, Proceedings of Papers: HICSS-40, 2007, Waikoloa, HI, pp. 70-70.
[8] Dagon, D.; Lee, W. “Global Internet Monitoring Using Passive DNS”, Cybersecurity Applications & Technology Conference for Homeland Security, Proceedings of Papers: CATCH '09, 2009. pp. 163 – 168