www.abuse.ro – un raport de activitate

După cum probabil ştiţi, în luna august am lansat www.abuse.ro, un portal de resurse împotriva spamului autohton. Site-ul se doreşte a fi un punct de colectare al mesajelor raportate ca fiind nesolicitate şi totodată sursa de informaţii brute pentru cele două liste tehnice antispam: **rbl.abuse.ro** şi respectiv **uribl.abuse.ro**.

Prima listă publică **adresele IP** ale expeditorilor de spam, fiind foarte simplu de instalat pe aproape orice server de email. Avantajul major al acestei liste este faptul că mesajele expediate de la adrese listate nu mai sunt procesate de serverul destinatar (economisindu-se bandă internet şi resurse de procesare). Dezavantajul este acela că pot fi filtrate şi mesaje legitime, în cazul în care expeditorii de spam şi cei legitimi împart aceeaşi adresă IP.

A doua listă publică **domeniile web** (doar domeniile, de forma *domain.tld*, nu şi subdomeniile) promovate prin spam sau care sunt folosite ca vector de transmitere. Mesajele ce conţin domenii *spamvertizate* nu sunt respinse direct, ci scorul lor de spam creşte cu nota setată la configurare. Această listă este mai precisă şi funcţionează foarte bine chiar dacă mesajele sunt expediate de pe ferme de adrese IP, însă necesită procesarea mesajelor de modulul SpamAssassin din serverul de mail.

Pe parcursul lunii septembrie (am considerat luna august ca fiind una de aşezare a datelor primare) am adunat câteva informaţii statistice care vă vor da o idee generală asupra situaţiei actuale.

Aşadar, iată datele:

Site-ul www.abuse.ro are în acest moment **58 de membri raportori** înregistraţi - voluntari ce trimit mesaje nesolicitate pentru agregarea datelor de spam. Dintre aceştia, cam 12 sunt activi, o parte înregistrându-se din motive necunscute încă (oricum nu au drepturi suplimentare).

Pe parcursul lunii septembrie 2012 au fost raportate un număr de **101 mesaje nesolicitate**, majoritatea provenind de la firme de "*email marketing*" (trebuie menţionat că o bună parte din mesajele nesolicitate sunt primite pe conturi de momeală). Ca şi fapt divers, în luna septembrie am primit **cinci** mesaje nesolicitate **româneşti** pe adresa contact@abuse.ro, în condiţiile în care adresa nu e folosită pentru corespondenţă;

Liderul absolut în campaniile de spam este Mailway Romania, care are nu mai puţin de **40 de adrese IP** (dintr-o clasă de 256) listate în rbl.abuse.ro. De altfel, Mailway Romania este şi subiectul unei anchete a ANDSPSC privind o posibilă încălcare a Legii privind protecţia datelor cu caracter personal. La mare distanţă, dar totuşi, foarte agresive, sunt site-urile de reduceri. Notabile sunt groupall.ro, crocodilo.info, therealdeal.ro sau publicitateprinemail.ro.

În medie, lista **rbl.abuse.ro** serveşte cam 307.000 cereri zilnic, cu o tendinţă uşor crescătoare pe parcursul lunii.

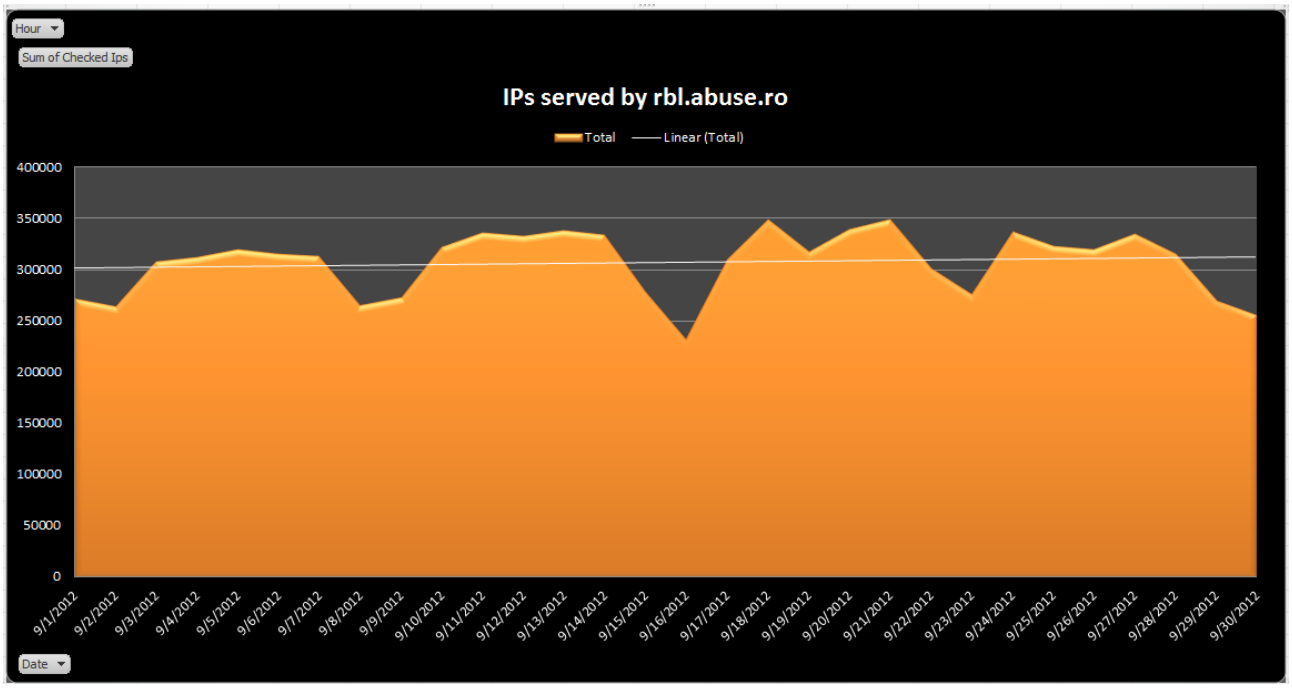

fig. 1: în septembrie, rbl.abuse.ro a servit în medie 307.508 adrese IP pe zi

Pe parcursul zilei, lista are un vârf de utilizare bine definit, între orele 10.00 şi 14.00 (e vorba de cereri de verificare servite în total, nu neapărat de spam).

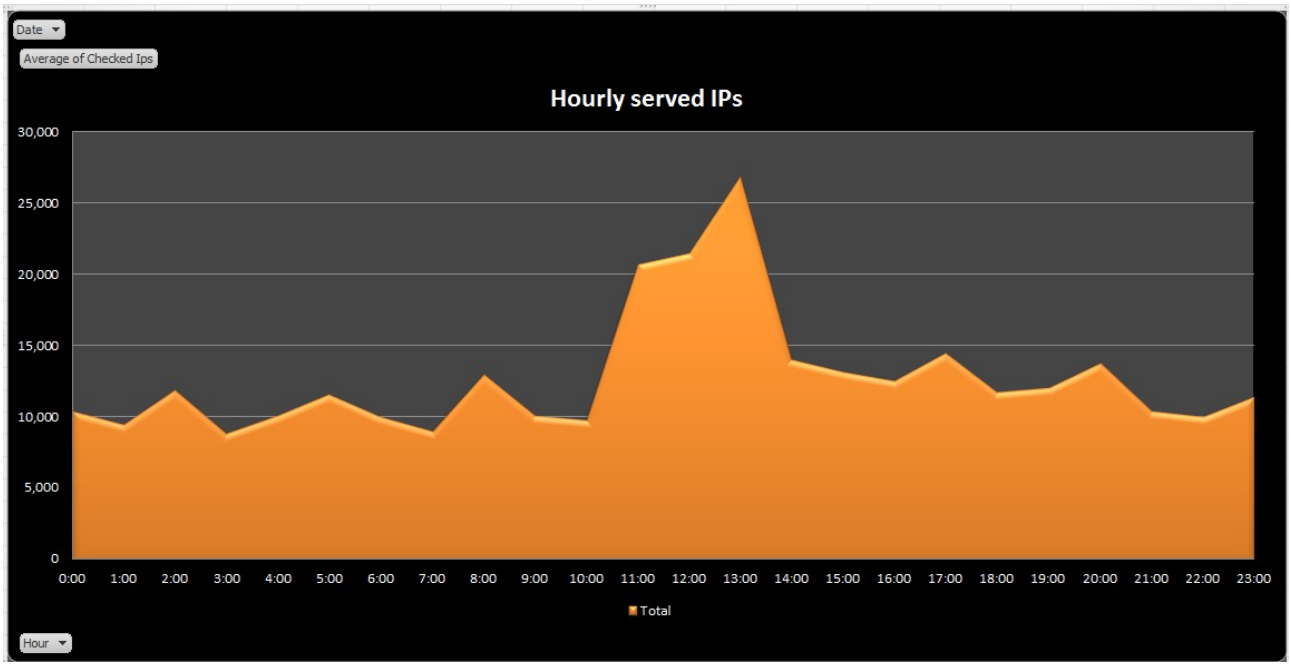

fig. 2: lista rbl.abuse.ro este utilizată cel mai mult la orele prânzului

De cealaltă parte, lista **uribl.abuse.ro** serveşte zilnic cam 7.500 de cereri, cu o tendinţă de creştere a utilizării mult mai pregnantă decât lista de adrese IP, rbl.abuse.ro.

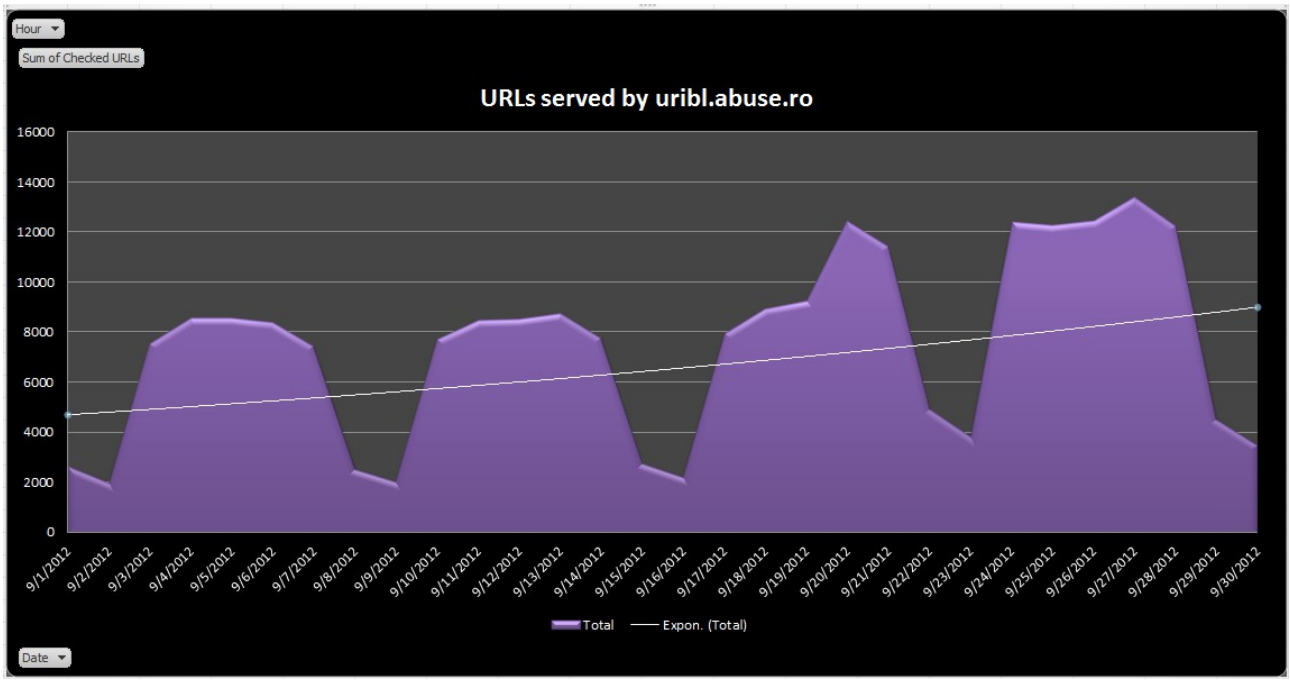

fig. 3: lista uribl.abuse.ro procesează în medie 7500 de cereri zilnic

Lista este utilizată cel mai mult pe perioada zilei (între orele 9.00 şi 20.00).

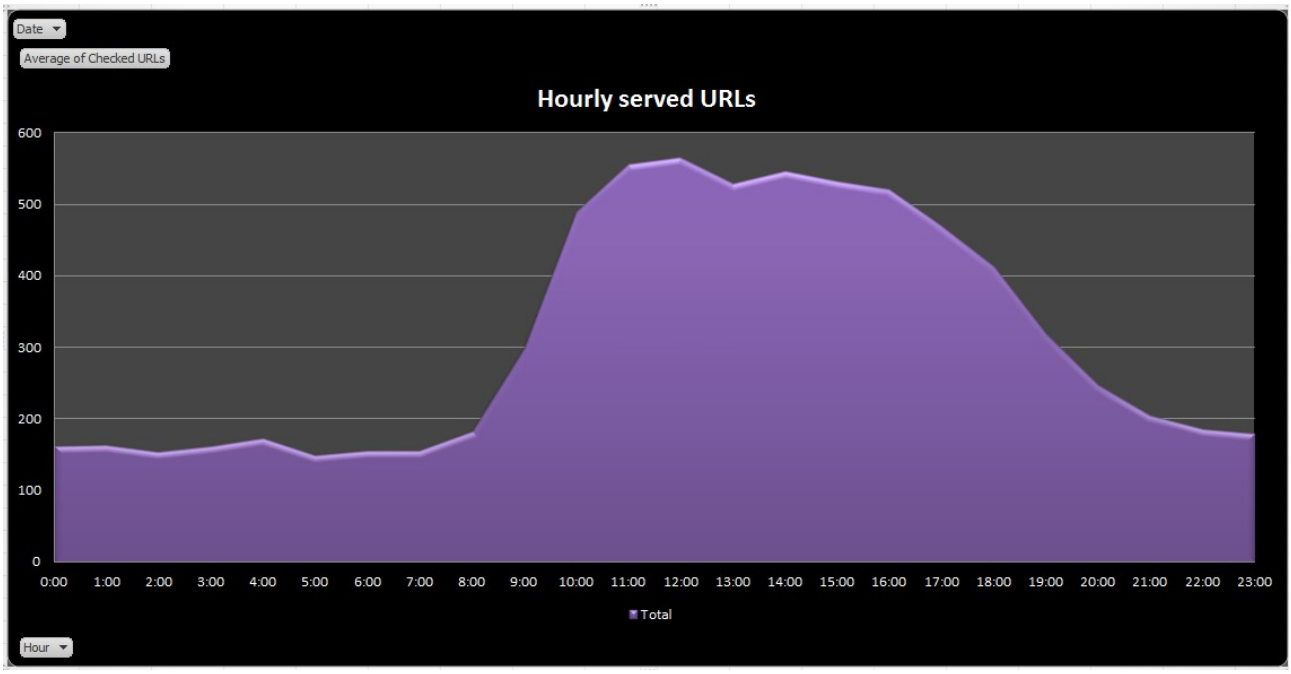

fig. 4: distribuţia utilizării orare a listei uribl.abuse.ro

Pe parcursul lunii septembrie observăm o creştere moderată al rezultatelor pozitive returnate de rbl.abuse.ro şi o creştere pregnantă a rezultatelor pozitive returnate de uribl.abuse.ro.

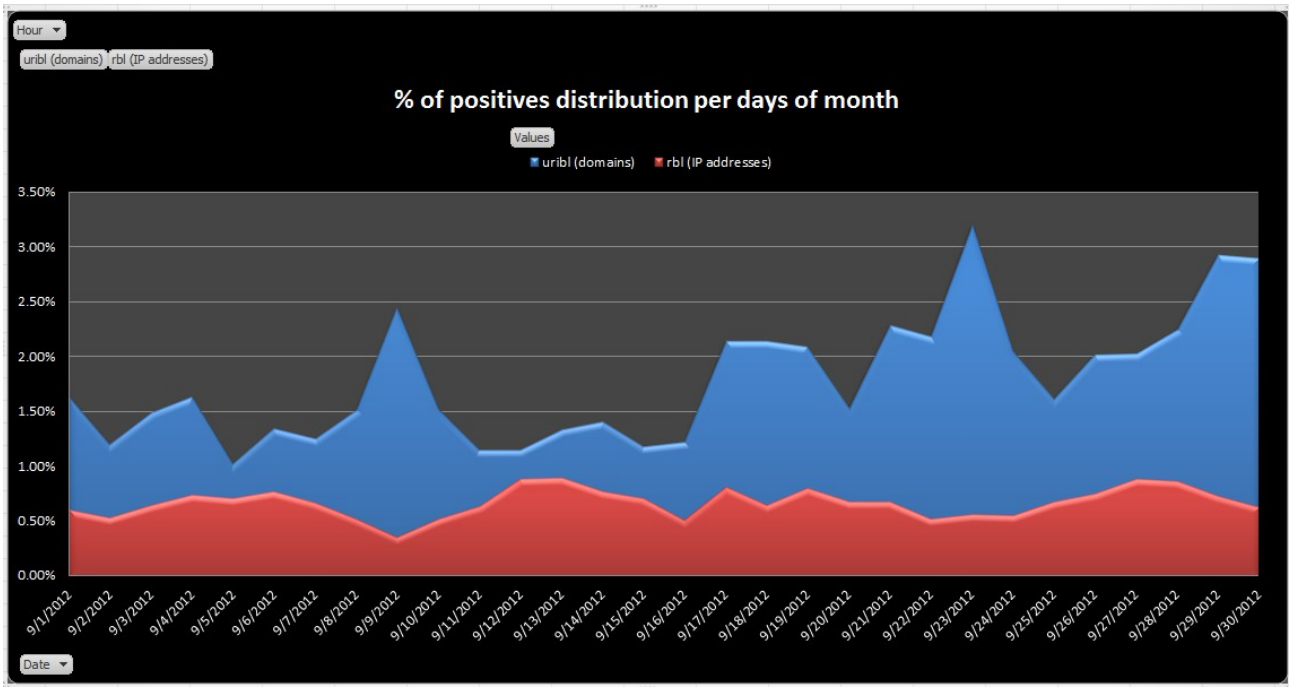

fig. 5: distribuţia zilnică a rezultatelor pozitive returnate de cele două liste

În medie, pe parcursul unei zile observăm o distribuţie clar nocturnă a mesajelor respinse datorită listei uribl.abuse.ro, distribuţia rezultatelor pozitive de la rbl.abuse.ro fiind relativ constantă.

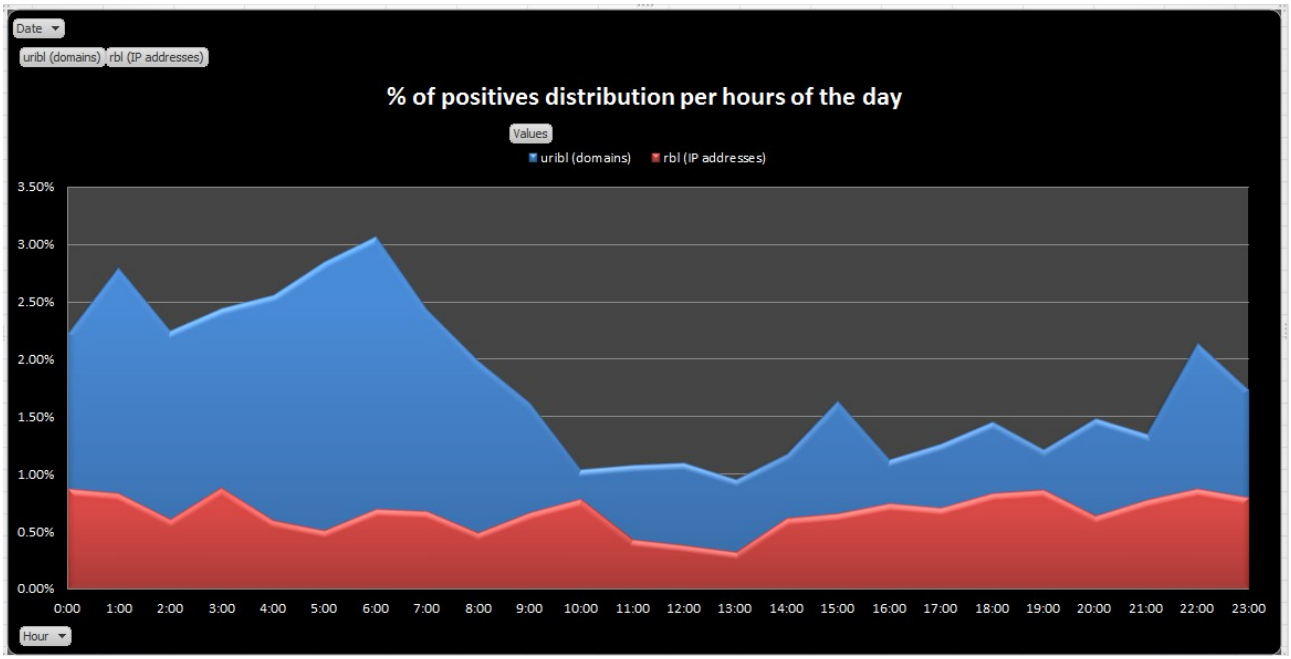

fig. 6: distribuţia orară a rezultatelor pozitive returnate de cele două liste

În septembrie a fost primită **o singură** cerere validă de delistare a unei adrese IP din rbl.abuse.ro. Au mai fost primite câteva solicitări nefondate, probabil din cauza implementării unor copii mai vechi ale listelor. E foarte probabil ca odată cu adoptarea mai largă a celor două liste, numărul cererilor de delistare să crească.

La final trebuie să menționăm următoarele observații:

- majoritatea serverelor de găzduire web (vorbim de servere Linux + cPanel) au implementat un sistem de respingere a mesajelor spam de la adrese IP ce anterior au fost regăsite pe astfel de liste; asta înseamnă că o singură interogare pozitivă la **rbl.abuse.ro** poate duce la blocarea a mult mai multor mesaje de la același IP;
- tot în serverele Linux + cPanel, există o limită implicită de 200kB a mesajelor scanate; cu alte cuvinte, mesajele mai mari de 200kB nu sunt scanate de filtrele SpamAssassin. Spamerii români par a fi învățat asta, mesajele trimise având în medie 700kB. Dacă furnizorii de servicii internet vor modifica această limită, concomitent cu utilizarea uribl,abuse.ro, eficacitatea filtrelor va crește dramatic.
- spamerii români preferă să lucreze noaptea :)