Spamassasin zabušava a spamovi stižu

Odjednom su nas zapljusnuli SPAMovi. Gljivice iskaču sa svih strana. Spamovi su napisani na hrvatskom jeziku i to bez očitog google translate-a. Prva pretpostavka je: Spamassin ih ne prepoznaje jer nisu na engleskom, jer su ciljani upravo na naše tržište. Pod tom pretpostavkom krećemo vatrogasnu akciju, pišemo vlastita pravila za spamassasin, blokiramo pošljatelja, itd. No jesmo li provjerili radi li uopće naš spamassasin ili možda zabušava na poslu.

Prvu naznaku da nešto nije kako treba biti našao sam u syslogu

```
Jan 25 03:32:23 XXXXXX  amavis[23923]: (23923-09) Passed CLEAN {RelayedInbound},
[212.129.18.13]:48794 [212.129.18.13] <r0hcb71@example.com> -> <xx.xx@xx.hr>, Queue-
ID: 79A32600787, Message-ID:
<606405.cbppixpvifpfcxtomjzbiwpzgdp@wmjfzjg.example.com>, mail_id: jqQeoXU2g53M,
Hits: 0, size: 2499, queued_as: 9D411600786, 98 ms
```

Kako je moguće da sve poruke imaju isti spam-score od 0? Amavis i spamassasin rade, očito, ali ne rade ništa korisno.

Da spamassasin nije pokupio nova pravila za prepoznavanje spama saznao sam u logovima spamassain update-a.

```
~# tail /var/log/sa-update.log
25-01-2018 06:25:24: Fetching new SA rules...
gpg: process '/usr/bin/gpg' finished: exit 2
error: GPG validation failed!
The update downloaded successfully, but the GPG signature verification failed.
channel: GPG validation failed, channel failed
25-01-2018 06:25:26: No new rules. Exiting now.
25-01-2018 06:25:26: Will restart services due to updated rules...
```

Pokrenuo sam spamassin update u debug modu i saznao:

```
~# sa-update -D
....cut...
Jan 25 12:36:36.587 [7597] dbg: gpg: calling gpg
Jan 25 12:36:36.596 [7597] dbg: gpg: gpg: Signature made Thu 25 Sij 2018 09:31:33 CET
using RSA key ID 24F434CE
Jan 25 12:36:36.596 [7597] dbg: gpg: gpg: WARNING: signing subkey 24F434CE is not
cross-certified
Jan 25 12:36:36.596 [7597] dbg: gpg: gpg: please see https://gnupg.org/faq/subkey-
cross-certify.html for more information
Jan 25 12:36:36.596 [7597] dbg: gpg: [GNUPG:] ERRSIG 6C55397824F434CE 1 2 00
1516869093 1
Sij 25 12:36:36.596 [7597] dbg: gpg: gpg: Can't check signature: general error
gpg: process '/usr/bin/gpg' finished: exit 2
error: GPG validation failed!
The update downloaded successfully, but the GPG signature verification failed.
channel: GPG validation failed, channel failed
....cut...
```

O čemu se ovdje radi?

Spamassin je to ovako objasnio: (vidi https://wiki.apache.org/spamassassin/SaUpdateKeyNotCrossCertified [1] iz 2009. godine)
"As bug 5775 [2] describes, the GnuPG developers decided to create a new error condition for a potentially-dangerous signature style, which unfortunately was one we use for the SpamAssassin [3] update-signing key."

Kako bi ažuriranja proradila moramo uraditi sljedeće:

```
~# wget http://spamassassin.apache.org/updates/GPG.KEY
~# sa-update --import GPG.KEY
~# sa-update -v
~# service amavis restart
```

Et Voila, amavis i spamassasin više ne zabušavaju.

```
Jan 25 13:08:26 XXXXX amavis[9978]: (09978-01) Passed CLEAN {RelayedInbound},
[108.174.3.174]:52818 [108.174.3.174] <yy@yy.yy> -> <xx@xx.xx>, Queue-ID:
0A8B55C0319, Message-ID: <wwwwww>, mail_id: utJBsRvK0jvd, Hits: -3.101, size: 108973,
queued_as: 7B0F15C02FC, 3382 ms

Jan 25 13:08:37 XXXXX amavis[9980]: (09980-01) Blocked SPAM
{BouncedInbound,Quarantined}, [188.130.45.145]:53946 [103.94.80.21] <yy@example.com>
-> <xx.xx@xx.xx>, quarantine: F/spam-FW-ft4yLAm_S.gz, Queue-ID: 3A7025C02FC, Message-
ID: <20D252E4-039D-45A2-BB1D-4AC6D35F8384@example.com>, mail_id: FW-ft4yLAm_S, Hits:
7.596, size: 1859, 2633 ms
```

Ovo sam uočio na nedavno reinstaliranom serveru. Dakle problem je u samom paketu!

čet, 2018-01-25 23:09 - Velimir Skroza**Kategorije:** Spam [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

story_tag: spamassasin [5]
amavis [6]

Source URL: https://sysportal.carnet.hr./node/1793

Links
[1] https://wiki.apache.org/spamassassin/SaUpdateKeyNotCrossCertified
[2] http://issues.apache.org/SpamAssassin/show_bug.cgi?id=5775
[3] https://wiki.apache.org/spamassassin/SpamAssassin
[4] https://sysportal.carnet.hr./taxonomy/term/34
[5] https://sysportal.carnet.hr./taxonomy/term/216
[6] https://sysportal.carnet.hr./taxonomy/term/217