Muke po ClamAVu

Nedavno smo vas obavijestili [1] da zbog određenih problema dolazi do skidanja djelomične, odnosno oštećene neslužbene baze potpisa antivirusnog programa ClamAV. Kao posljedica, bili su zaustavljani svi mailovi koji sadržavaju niz znakova "**www.**", što je, priznat ćete, mnogo poruka. Nisu svi bili zahvaćeni ovim problemom, jer nemaju svi iste inačice ClamAVa (postoji inačica iz standardnog i *volatile* repozitorija). Možemo pretpostaviti da neki nisu ni bili svjesni problema, jer im se korisnici nisu potužili.

Nažalost, problem još postoji, no sporadično. Moguće je da se radi o preopterećenju poslužitelja ili mreže. No, sada je problem manje izražen, jer skidanje potpisa "puca" na drugom mjestu i rezultat više nije tako katastrofalan. Pogledajmo:

```
 # wget 'http://www.malware.com.br/cgi/submit?action=list_clamav' -O mbl.wget
--2012-03-14 22:04:14--  http://www.malware.com.br/cgi/submit?action=list_clamav
...
Length: unspecified [text/plain]
Saving to: `mbl.wget'

    [  <=>                                  ] 36,696      80.8K/s   in 0.4s

2012-03-14 22:04:15 (80.8 KB/s) - `mbl.wget' saved [36696]
```

Možemo probati s nekim drugim latom, poput **curl-a**, ali rezultat će biti isti.

```
curl 'http://www.malware.com.br/cgi/submit?action=list_clamav' -o mbl.curl
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 36696    0 36696    0     0  23023      0 --:--:--  0:00:01 --:--:-- 25430
```

Obje datoteke su velike 36696 bajtova, a trebale bi biti velike 256654 bajtova (ove vrijednosti su trenutne, kod vas mogu biti drugačije):

```
# ls -l /var/lib/clamav/mbl.ndb
-rw-r--r-- 1 clamav clamav 256654 Mar 15 00:23 /var/lib/clamav/mbl.ndb
```

Zadnji redak unutar nepotpunih datoteka nakon dekodiranja izgleda ovako:

```
# tail -1 mbl.curl | sigtool --decode-sigs
VIRUS NAME: MBL_210910
DECODED SIGNATURE:
down.ezenjoy
```

Puni potpis glasi "**down.ezenjoy.com/2010_update_2/file/update**", ali "skraćen" ovaj put nema takve posljedice kao što je to imao nesretni "**www.".** Kako bi spriječili daljnje probleme s ovim repozitorijem, možete postupiti po uputama u prethodno navedenom članku, ili instalirati paket **clamav-unofficial-sigs.** Paket se ne nalazi u standardnom repozitoriju za lenny, nego u repozitoriju *backports*. Kako lenny više nije aktualan, nećemo ni pokazivati kako dodati ovaj paket.

Lakši način je prijeći na squeeze. Ovdje samom instalacijom paketa clamav-cn dobijete i paket clamav-unofficial-sigs. Od tog trenutka više ne morate brinuti, jer ćete u slučaju oštećene baze mailom dobiti sljedeću poruku:

```
Subject: Cron <clamav@server> [ -x /usr/sbin/clamav-unofficial-sigs ] &&
    /usr/sbin/clamav-unofficial-sigs

Clamscan reports Sanesecurity mbl.ndb database integrity tested BAD -
SKIPPING
```

Ostaje još samo da dečki sa www.malware.com.br poprave ovaj (sporadični) problem, kako bi svi mogli malo mirnije spavati.

Napomena: mbl.db je stariji oblik baze, a **mbl.ndb** je noviji, ali u suštini problem ostaje isti.

čet, 2012-03-15 01:04 - Željko Borš**Vijesti:** Linux [2]
Kuharice: Linux [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/961

Links
[1] https://sysportal.carnet.hr/node/944
[2] https://sysportal.carnet.hr/taxonomy/term/11
[3] https://sysportal.carnet.hr/taxonomy/term/17