Clamav: problem s neslužbenim antivirusnim definicijama (MBL_207346.UNOFFICIAL)

Dana 22. veljače u prijepodnevnim satima mnogi su sistemci dobili dojavu svojih korisnika da im mailovi ne stižu na odredište, ali i obrnuto, njima poslani mailovi nisu stizali u njihove sandučiće e-pošte. Nakon što su pogledali u logove, vidjeli su da poštu zaustavlja Amavis i stavlja u karantenu kao virus. Stavljanje u karantenu nije nešto neuobičajeno, ali broj zaustavljenih mailova svakako jest, kod nekih je iznosio 50%, pa i više. Je li riječ o nekoj greški u sustavu, ili se pojavio opasan virus koji je odjednom zarazio mnoga računala? Pogledajmo logove:

```
Feb 22 11:36:18 server amavis[12430]: (12430-17) Blocked
INFECTED (MBL_207346.UNOFFICIAL), LOCAL [127.0.0.1]
[161.53.XXX.YYY] <korisnik@domena.hr> -> <korisnik2@domena2.hr>,
quarantine: r/virus-r6BsjEx0FIl3, Message-ID:
<dd6035aad2dd00b46969f945c569a4e8.squirrel@mail.domena.hr>,
mail_id: r6BsjEx0FIl3, Hits: -, size: 17210839, 2401 ms
```

Korisnik je preko webmaila slao veliku datoteku, za koju je provjerom antivirusnim alatima utvrđeno da nije zaražena, što dodatno ukazuje na nekakvu grešku u mail sustavu. Kako se na CARNetovim poslužiteljima rabi isključivo besplatni antivirusni softver ClamAV (osim ako vaša institucija nije kupila neki drugi), vjerojatno je riječ o nekoj greški unutar ClamAV-a.

Pregledom web stranica ClamAV-a mogli smo naći informaciju da se ne radi o službenoj bazi (zbog ekstenzije UNOFFICIAL), nego o dodatnim antivirusnim definicijama koje se mogu naći u bazi MalwarePatrola. Naravno riječ je o definiciji MBL_207346, koja se nalazi u datoteci /var/lib/clamav/mbl.db:

```
...
MBL_207048=63616674616e2e6e61726f642e72752f70726f6772616d73
MBL_207301=77616b6162612d746f6f6c732e676f6f676c65636f64652e636f6d2f66696c6573
MBL_207346=7777772e
```

Ova zadnja definicija, odnosno potpis (signature) je očigledno kraći, je li moguće da se datoteka nije skinula do kraja i da je puklo na ovom potpisu? Datoteke koje nisu unutar osnovnog ClamAV-a se osvježavaju svaki sat preko cron skripte /etc/cron.hourly/clamav-sanesecurity s adrese http://www.malware.com.br/cgi/submit\?action=list_clamav (iz Brazila!). Provjerom smo pronašli da je zaista riječ o datoteci koja nije kompletna, jer bi trebala završiti s ovim potpisom:

```
MBL_99905=666f746f736c696e6b733433393835362e636f6d2e7361706f2e7074
```

Dakle, mnogo ključeva nedostaje, a barem jedan je oštećen. No, zašto onda zaustavlja većinu mailova i označava ih kao virus? Ovdje nam može pomoći vlastiti ClamAV-ov alat "sigtool" (hvala Valentinu!):

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

```
# sigtool --find-sigs MBL_207346 | sigtool --decode-sigs
VIRUS NAME: MBL_207346
DECODED SIGNATURE:
www.
```

Za usporedbu, ovako izgleda taj potpis na neoštećenom sustavu:

```
VIRUS NAME: MBL_207346
DECODED SIGNATURE:
www.thinkertec.com/trial
```

Znači, ako se u mailu pojavljuje "www.thinkertec.com/trial" mail će biti blokiran. A u gornjem slučaju? **Bit će blokiran svaki mail koji sadržava niz znakova "www."!**

Ne moramo napominjati da ovo za neke znači gotovo potpuni prekid rada mail sustava, da ne spominjemo stotine i tisuće mailova u karanteni koje treba pronaći i "osloboditi".

No, nije sve tako strašno, jer su mailovi i dalje u karanteni, nisu obrisani i mogu se ponovo poslati. Neka vam pomogne ovaj *one-liner*:

```
grep 207346 /var/log/mail/mail.log | grep virus- | sed -e 's/^.*quarantine: //g' -e '
s/,.*$//g'
    | xargs -I{} amavisd-release {}
```

(cijeli ovaj niz naredbi mora biti u jednom redu)

Ovaj će niz naredbi u logovima provjeriti jesu li zaustavljeni mailovi po potpisu MBL_207346, pripremiti popis oznaka u karanteni te ih proslijediti naredbi amavisd-release. Ukoliko samo želite provjeriti postoje li zaustavljene poruke, izostavite dio s naredbom xargs.

Napomene: ukoliko je vaš mail.log na drugoj lokaciji, poput /var/log/mail.log, navedite tako u naredbi. Također, ukoliko su se logovi već zarotirali (a svakako hoće prko noći), provjerite i datoteku mail.log.0.

Čini se da naposlužiteljima sa starom inačicom ClamAV-a ovaj problem nije izražen u većoj mjeri. Prepoznat ćete stari ClamAV po poruci "Your ClamAV installation is OUTDATED", iako to ne znači da ClamAV ne radi, samo da je izašla barem jedna novija inačica.

Situacija se navečer normalizirala, pa više ne postoje parcijalni zapisi. Ukoliko unatoč tome ne želite riskirati, onemogućite cijelu MalwarePatrol bazu, tako da preimenujete datoteku mbl.db i onemogućite daljnje osvježavanje:

```
cd /var/lib/clamav
mv mbl.db mbl.disabled
/etc/init.d/clamav-daemon restart
```

Još samo trebate na samom početku datoteke /etc/cron.hourly/clamav-sanesecurity dodati "exit 0". Time onemogućujete pokretanje skripte. Ponovit ćemo, ove dvije operacije nisu nužan korak, jer trenutno sve radi kako treba i nema potrebe blokirati ovu korisnu dodatnu zaštitu od virusa, malvera i spama.

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Nadamo se da smo pomogli i da će vaši korisnici biti tolerantni prema ovom problemu.

- Logirajte [1] se za dodavanje komentara

sri, 2012-02-22 23:13 - Željko Borš**Vijesti:** Linux [2]
Kuharice: Linux [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (3 votes)

Source URL: https://sysportal.carnet.hr/node/944

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

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr