Securiteinfo uveo plaćanje svojih usluga

SecuriteInfo, francuska tvrtka koja se bavi IT sigurnošću, počela je naplaćivati svoje usluge. Ukoliko vam to ime zvuči poznato, njihove usluge rabimo preko paketa ClamAV, odnosno dodatnih i neslužbenih digitalnih potpisa za malver. Ovi potpisi se ne skidaju preko standardnih kanala i programa *freshclam*, nego ih skidamo pomoću skripte *clamav-unofficial-sigs* iz crona. No, u SecuriteInfo su ostavili mogućnost da se i dalje besplatno koriste njihove usluge, ali je za to potrebna registracija.

Novosti, formu za registraciju, kao i tarife dostupni su na ovoj adresi [1]. U međuvremenu, u logovima ili u mailu možete vidjeti poruke poput ovih:

```
Clamscan reports Sanesecurity honeynet.hdb database integrity tested BAD - SKIPPING
rsync: link_stat "/var/cache/clamav-unofficial-sigs/si-
dbs/honeynet.hdb" failed: No such file or directory (2)
rsync error: some files/attrs were not transferred (see previous errors) (code 23) at
 main.c(1070) [sender=3.0.9]
Failed to successfully update SecuriteInfo production database file: honeynet.hdb - S
KIPPING
Clamscan reports Sanesecurity securiteinfobat.hdb database integrity tested BAD - SKI
PPING
rsync: link_stat "/var/cache/clamav-unofficial-sigs/si-
dbs/securiteinfobat.hdb" failed: No such file or directory (2)
rsync error: some files/attrs were not transferred (see previous errors) (code 23) at
 main.c(1070) [sender=3.0.9]
Failed to successfully update SecuriteInfo production database file: securiteinfobat.
hdb - SKIPPING
Clamscan reports Sanesecurity securiteinfodos.hdb database integrity tested BAD - SKI
PPING
rsync: link_stat "/var/cache/clamav-unofficial-sigs/si-
dbs/securiteinfodos.hdb" failed: No such file or directory (2)
rsync error: some files/attrs were not transferred (see previous errors) (code 23) at
 main.c(1070) [sender=3.0.9]
Failed to successfully update SecuriteInfo production database file: securiteinfodos.
hdb - SKIPPING
Clamscan reports Sanesecurity securiteinfoelf.hdb database integrity tested BAD - SKI
PPING
```

Rješenje je jednostavno, treba isključiti skidanje tih digitalnih potpisa, jer to više ne radi i baze su obrisane. Za to uporabite direktivu "unset":

```
unset si_dbs
```

Ovu direktivu možete upisati direktno u **/etc/clamav-unofficial-sigs.conf**, ali prilikom nadogradnji ove promjene mogu biti "zgažene". Preporuka je postaviti lokalnu datoteku unutar drugog

direktorija: **/usr/share/clamav-unofficial-sigs/conf.d**. Ovo je klasični "conf.d" direktorij i primjenjuje se standardna pravila: zadnja datoteka poništava direktive u prethodnim. Zato smo kreirali datoteku **/usr/share/clamav-unofficial-sigs/conf.d/99-local.conf** i u nju upisali "unset si_dbs".

Sljedeće što treba napraviti je obrisati baze digitalnih potpisa. Poslužili smo se naredbom **su**, iako u istu svrhu možemo upotrijebiti i sudo:

```
# su -s /bin/bash clamav
clamav@server$ /usr/sbin/clamav-unofficial-sigs

File removed: /var/cache/clamav-unofficial-sigs/si-dbs/honeynet.hdb
File removed: /var/cache/clamav-unofficial-sigs/si-dbs/securiteinfobat.hdb
File removed: /var/cache/clamav-unofficial-sigs/si-dbs/securiteinfodos.hdb
File removed: /var/cache/clamav-unofficial-sigs/si-dbs/securiteinfoelf.hdb
File removed: /var/cache/clamav-unofficial-sigs/si-dbs/securiteinfo.hdb
File removed: /var/cache/clamav-unofficial-sigs/si-dbs/securiteinfohtml.hdb
File removed: /var/cache/clamav-unofficial-sigs/si-dbs/securiteinfooffice.hdb
File removed: /var/cache/clamav-unofficial-sigs/si-dbs/securiteinfopdf.hdb
File removed: /var/cache/clamav-unofficial-sigs/si-dbs/securiteinfosh.hdb
File removed: /var/lib/clamav/honeynet.hdb
File removed: /var/lib/clamav/securiteinfobat.hdb
File removed: /var/lib/clamav/securiteinfodos.hdb
File removed: /var/lib/clamav/securiteinfoelf.hdb
File removed: /var/lib/clamav/securiteinfo.hdb
File removed: /var/lib/clamav/securiteinfohtml.hdb
File removed: /var/lib/clamav/securiteinfooffice.hdb
File removed: /var/lib/clamav/securiteinfopdf.hdb
File removed: /var/lib/clamav/securiteinfosh.hdb
...
```

Ovime smo se riješili starih i nepotrebnih baza.

Međutim ako želimo i dalje rabiti SecuriteInfo, možemo (po njihovim uputama) staviti na kraj datoteke /etc/clamav/freshclam.conf:

```
DatabaseCustomURL http://www.securiteinfo.com/get/signatures/5...271ab2698f3c/securit
einfo.hdb
DatabaseCustomURL http://www.securiteinfo.com/get/signatures/5...271ab2698f3c/securit
einfo.ign2
DatabaseCustomURL http://www.securiteinfo.com/get/signatures/5...271ab2698f3c/javascr
ipt.ndb
DatabaseCustomURL http://www.securiteinfo.com/get/signatures/5...271ab2698f3c/spam_ma
rketing.ndb
DatabaseCustomURL http://www.securiteinfo.com/get/signatures/5...271ab2698f3c/securit
einfohtml.hdb
DatabaseCustomURL http://www.securiteinfo.com/get/signatures/5...271ab2698f3c/securit
einfoascii.hdb
```

Ove adrese ćete dobiti nakon besplatne registracije, i vrijede samo za jednu IP adresu, te 24 osvježavanja na dan. Ukoliko imate više poslužitelja koje želite zaštititi, možete jednostavno dati drugu IP adresu.

I to je uglavnom to, i dalje imamo dodatne potpise, samo ćemo ih pribavljati na drugčiji način.

uto, 2015-04-28 15:02 - Podrška za CARNetove sistem-inženjere**Kategorije:** sys.kuharica [2]

Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: https://sysportal.carnet.hr./node/1545

Links
[1] https://www.securiteinfo.com/services/improve-detection-rate-of-zero-day-malwares-for-clamav.shtml
[2] https://sysportal.carnet.hr./taxonomy/term/69