FRnOG 33

Logs, CGNat et cybercriminalité

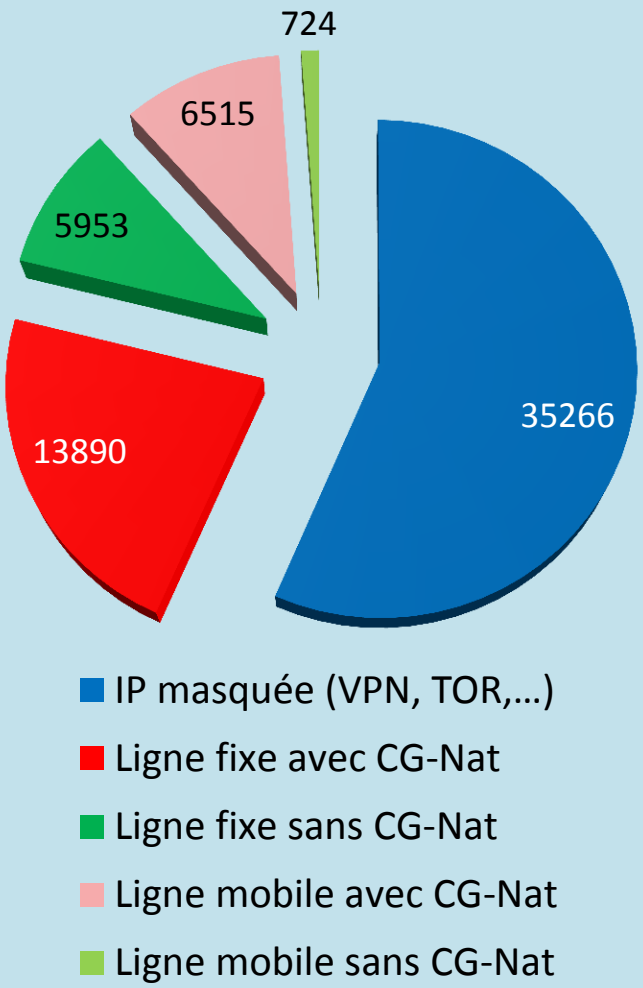
Vivien Guéant

Twitter: @lafibreinfo

13 septembre 2019

Exemple Europol 2018: Pédopornographie

Répartition des 62 348 membres



Forum pédopornographique de 62 348 membres.
Géré par des suspects en Asie, mais les serveurs sont en Europe.
10 enfants victimes, exploités pour alimenter le forum en matériel.

Le système loguait les adresses IP de connexion.

Facile? Pas vraiment…

Seuls 10% des membres du forum pouvaient être identifiés directement.

Solutions ?

- **Court terme :** Réduire le nombre d'utilisateurs derrière une même adresse IP publique (ex: code de bonne conduite en Belgique => max 16 clients / IPv4)
- **Moyen terme :** Obligation de stocker le port source pour les services d'hébergement, média sociaux, etc... Mettre en place la RFC 6302 qui date de 2011
- **Long terme :** Transition quasi-totale à l'**IPv6**, avec extinction progressive d'IPv4

BCP 162 / RFC 6302: Recommandations pour les logs serveurs

IETF BCP 162 / RFC 6302 (Juin 2011)=> port source + horodatage + IP
Problème : les applications ne gardent pas le port source par défaut.

Les 3 formats de log proposés par Apache2: (extrait /etc/apache/apache2.conf)

```
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
```

Définition :

```
%h          : IP
%l          : Le nom de connexion distant
%u          : L'utilisateur distant
%t          : Date
%{remote}p  : port source
%{local}p   : port destination
```

Trois solutions :

- Rajouter le port source (`%{remote}p`) juste après l'IP. Risque de casser les outils d'analyse de logs
- Rajouter le port source à la fin de la ligne de log
- Utiliser des champs inutilisés : juste après l'IP (%l et %u) sont rarement utiles.
  ➔ Les utiliser pour avoir un log avec IP, port source, port destination, date, etc.

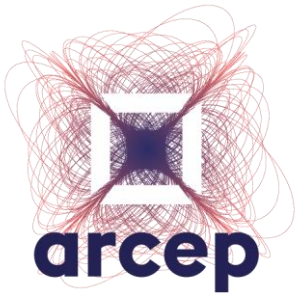
Conclusion :

1. Tentez de convaincre les développeurs de vos applications de rajouter le port source aux log sur l'adresse IP, sans oublier l'horodatage si ce n'est pas fait
2. Proposez tous vos services en **IPv6** et vérifiez que votre application remonte bien les IPv6 (des surprises sont possibles)

Merci
de votre
attention

Vivien Guéant

Twitter: @lafibreinfo



Annexe : Mise en place avec APACHE HTTP SERVER PROJECT sous Ubuntu / Debian

Modifier directement le fichier /etc/apache/apache2.conf va compliquer la mise à jour vers une version ultérieure d'Apache2. Il est donc préférable de ne pas le modifier.

Solution propre : créer un fichier spécifique
/etc/apache2/conf-available/apache2-log-personnalise.conf

```
# Log du type combined, avec port source et port destination
LogFormat "%h %{remote}p %{local}p %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combiport
```

Activation du fichier apache2-log-personnalise.conf **:**

```
sudo a2enconf log-personnalise
sudo service apache2 reload
```

Mise en place dans le « Virtual Host » :
Il faut éditer chaque fichier de serveur virtuel,
pour remplacer « combined » par « combiport ».

Exemple :

```
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combiport
```

Durée de conservation des logs :
Pensez à modifier le fichier /etc/logrotate.d/apache2 , afin de garder 1 an de logs :

```
sudo sed -i -e "s/rotate 14/rotate 365/g" /etc/logrotate.d/apache2
```