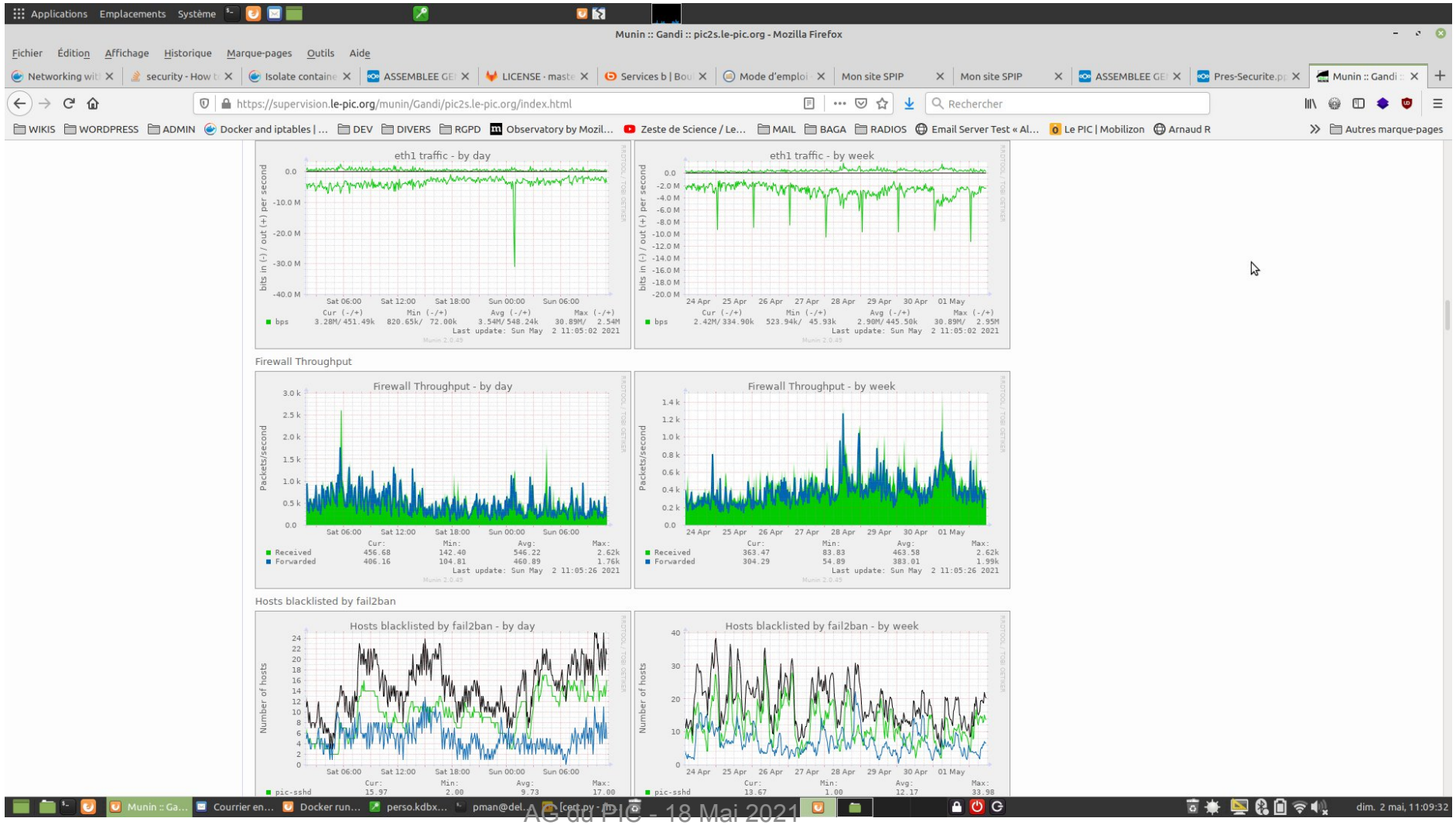
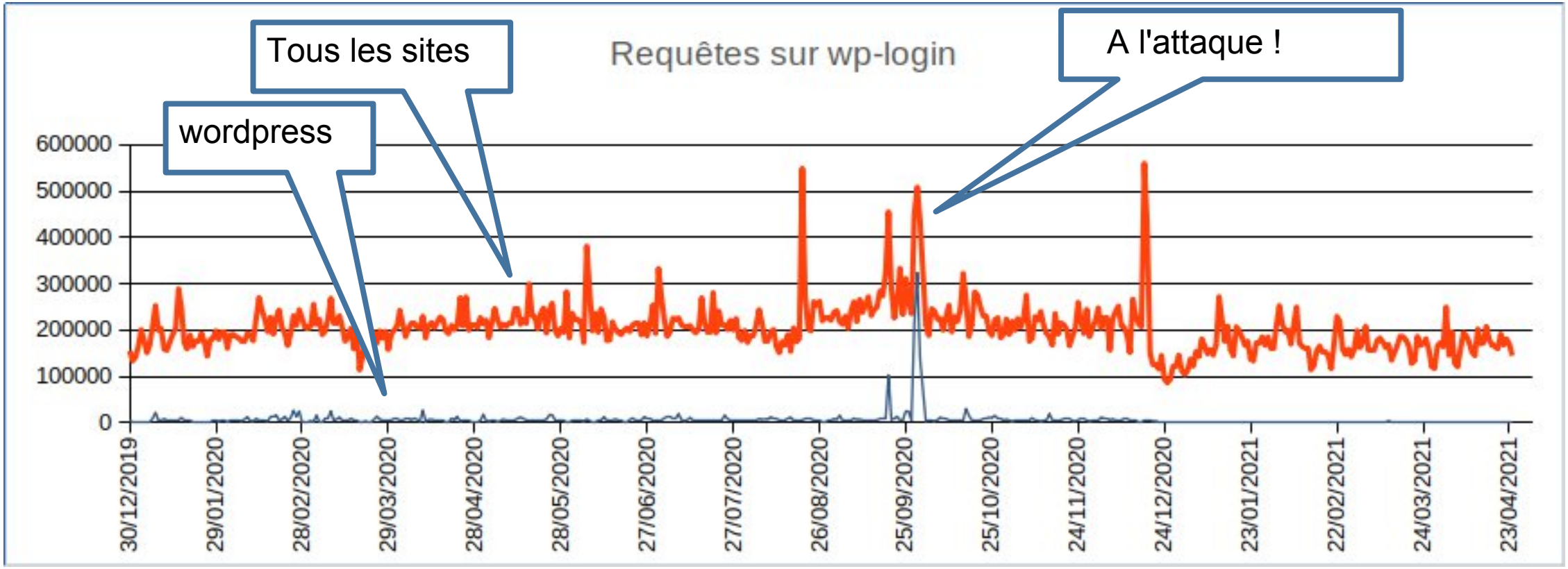
Améliorer la sécurité

Du boulot pour tout le monde !

Supervision des serveurs



Requêtes sur la page de connexion de wordpress



Bloquer les attaquants

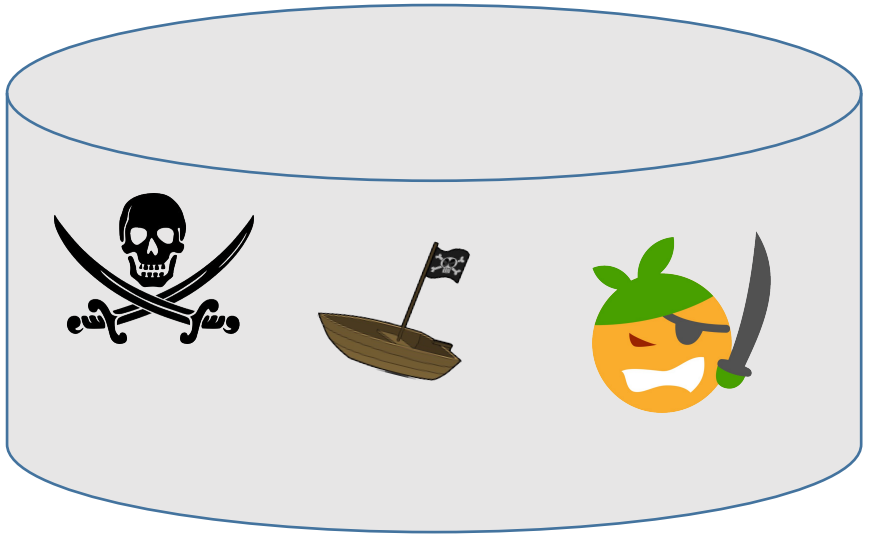
- **Surveiller** les requêtes sur wordpress (page de connexion):
  - Plus de 5 requêtes de la même adresse durant 30 s = **blocage** !
  - *ça peut vous arriver ! (désolé !)*
- **Bloquer totalement les requêtes sur xmlrpc**
  (un vieux machin dangereux)
  - Pourrait être gênant ? (désolé il vous faudra trouver autre chose)
  - *(En fait probablement pas)*
- **Surveiller et bloquer les accès sftp**
  - **fail2ban:** raté-viré ! *(bientôt)*

Blocages préventifs avec AbuseIPDB

Une

base de données (**DB**)

pour les adresses **IP**



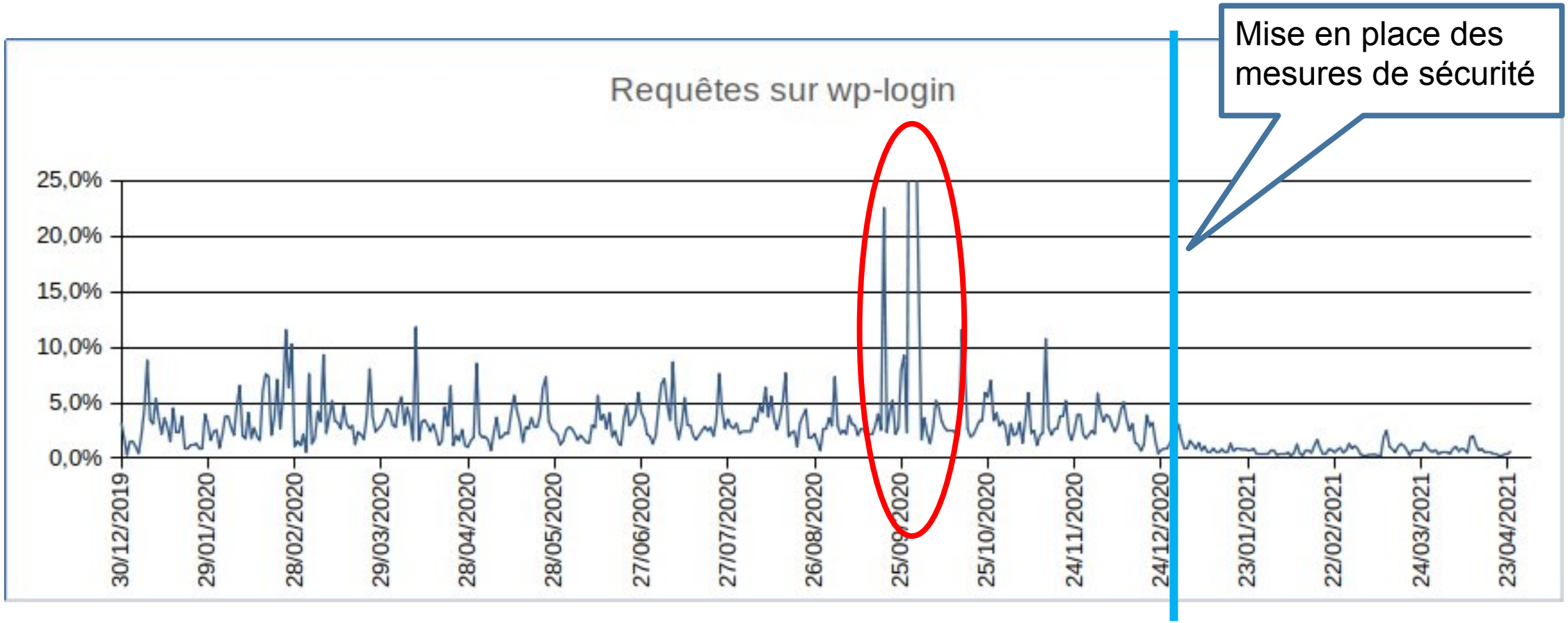
qui maltraitent (**abuse**)

nos serveurs

AbuseIPDB

- Un projet collaboratif (d'origine E.U.)
  - Chacun signale les IP qui l'embêtent
  - Chacun télécharge des listes d'IP signalées par beaucoup de gens (10000/j)

Requêtes sur la page de connexion de wordpress (%)



Une brève histoire de piratage

- **J+0 Un mail de Gandi...**

> **Cher Client, Chère Cliente,**
>
> **Il nous semble que vous soyez victime d'un piratage de votre site internet à des fins frauduleuses,**
>
> **------ Incident Information ------**
>
> **URL: https://frimousses.le-pic. org/wp-content/uploads/b/?email=abuse@ionos.com**
>
> **IP addresses: 95.142.162.68, 2001:4b98:dc0:47:216:3eff:fec8:b67f**

  - **quand on va sur le site de l'association**
    firefox nous prévient que "ce site est dangereux !"

Une brève histoire de piratage

- **J+0 Premières mesures**
  - Le site est désactivé, archivé et supprimé
  - Nous contactons Gandi pour leur dire que nous prenons le problème en compte
  - Les premières analyses montrent que le problème a commencé le matin même... *Gandi et Firefox ont été très rapides !*
  - Des programmes "louches" ont été déposés...
  - L'association est prévenue du problème

Une brève histoire de piratage

- **J+0 Étude des journaux de connexion**
  - Une personne s'est connecté entre 7h00 et 8h00
  - On a l'adresse IP d'origine
  - Cette adresse est connue chez AbuseIpDb (37% indice de confiance)
    - On fait un signalement, histoire d'en rajouter
  - A part ça, R.A.S.

Les WC étaient fermés de l'intérieur

et

Le pirate avait le mot de passe !

Une brève histoire de piratage

- **J+1 Étude de la base de données**
  - On compare la B.D. à celle sauvegardée la veille de l'incident
  - Pas trop de changements...
  - ...mais on a **les informations de connexion !**

Grâce à ses empreintes ADN
on
connaît l'utilisateur !

Une brève histoire de piratage

- **J+1 Travail avec l'association**
  - Jean-Paul contacte l'utilisateur en lui conseillant de passer son PC Windows à l'antivirus et à l'antimalware
  - Logiciel conseillé = https://fr.malwarebytes.com/

Une brève histoire de piratage

- **J+2 Réinstallation du site**
  - On réinstalle le site à partir des fichiers sauvegardés **avant** l'attaque
  - On réinitialise tous les mots de passe du CMS
    (on n'est jamais trop prudent...)
  - On met à jour les plugins
    (par prudence, ni wp ni les plugins ne semblent en cause)
  - Le site est *toujours désactivé* tant que nous n'avons pas de nouvelles du PC (probablement) piraté !

Une brève histoire de piratage

- **J+3 Des nouvelles de l'asso**
  - L'utilisateur nous signale qu'il a découvert un malware sur son PC, l'anti-malware l'a éradiqué...
  - Le site est remis en production
  - Gandi est prévenu que tout est rentré dans l'ordre

The (happy) end

Une brève morale de la brève histoire

Attention à vos virus !

Faites-vous vacciner

Mettez à jour votre antivirus
(si votre machine est sous windows)

Une brève morale de la brève histoire

Attention à vos mots de passe

`azerty123`	**NON**
`Vivent les Geeks`	**NON**
`v!ventLeSGeEks`	**BOF**
`=3u]s`8q46H#gNJZ/t]^.!LF;3z#'.`	**OUI !**

Utilisez un coffre-fort de mots de passe
keypass.info

Une brève morale de la brève histoire

Pas de mots de passe par mail

- On utilise souvent le mail pour "stoker" ses données (mots de passe...)
- Or les comptes mails sont parfois "visités"

  - On envoie le nom d'utilisateur par mail
  - et le mot de passe par sms

Deux endroits différents

- Bientôt... page web "mot de passe oublié"

Utilisez un coffre-fort de mots de passe
keepass.info
keepassxc.org

Mises à jour de spip et de ses plugins

- Si vous nous avez demandé de nous en occuper, nous pouvons vous accompagner
  - Dans ce cas votre site est **dans la mutualisation spip**
- Sinon vous êtes censé le faire **vous-même**

- Mises à jour mineures (3.2.9 vers 3.2.11)
  - Si vous ne le faites pas **nous le ferons pour vous !**
  - ça ne casse rien et ça améliore la sécurité
  - La version 3.2.11 permet d'utiliser **php 7.4**

Mises à jour de Wordpress et de ses plugins

- Si vous nous avez demandé de nous en occuper, nous pouvons vous accompagner
- Sinon vous êtes censé le faire **vous-même**

- Mises à jour mineures (5.7 vers 5.7.1)
  - Si vous ne le faites pas **nous le ferons pour vous !**
  - ça ne casse rien et ça améliore la sécurité

Les artistes

- **Supervision**: Patrick et Jean-Paul
- **Wordpress**: Jean-Paul et Emmanuel
- **Spip**: Momo, Jean-Louis et Jean-Pierre
- **Galette et Dolibarr**: Hélène
- **Serveurs**: Emmanuel
- ***... et tous les adhérents du PIC !***