

## PROTECTION CONTRE LES ATTAQUES DE TYPE RANSOMWARE

**Q :** *Comment se protéger des attaques par ransomware ?*

**GPT-4 :** La protection contre les ransomwares nécessite une approche multicouches. Voici quelques étapes essentielles à suivre pour renforcer votre défense contre ce type de menace :

**Mises à jour régulières :** Assurez-vous que tous vos systèmes d'exploitation, applications et logiciels sont régulièrement mis à jour. Les cybercriminels exploitent souvent des vulnérabilités connues dans les logiciels obsolètes.

**Sauvegardes régulières :** Effectuez des sauvegardes régulières de vos données importantes et assurez-vous qu'elles sont stockées hors ligne ou dans un emplacement sécurisé, tel qu'un service de stockage en cloud sécurisé. Testez également la restauration de ces sauvegardes pour vous assurer qu'elles fonctionnent correctement.

**Évitez les pièces jointes suspectes :** Soyez très prudent lorsque vous ouvrez des pièces jointes ou cliquez sur des liens dans des e-mails, surtout si vous ne connaissez pas l'expéditeur.

**Formation et sensibilisation :** Formez-vous et, si vous gérez une organisation, formez vos employés à reconnaître les tentatives de phishing et d'autres techniques de compromission.

**Utilisez un logiciel antivirus/antimalware :** Installez et mettez régulièrement à jour un logiciel de sécurité réputé qui offre une protection en temps réel contre les menaces.

**Firewall :** Utilisez un pare-feu pour filtrer le trafic entrant et sortant. Cela peut aider à bloquer les communications malveillantes.

**Réduisez les privilèges :** N'utilisez pas de comptes avec des privilèges élevés pour les tâches quotidiennes. Utilisez un compte avec des droits limités et n'activez les privilèges d'administrateur que lorsque cela est absolument nécessaire.

**Mise en place d'une politique de liste blanche :** Autorisez uniquement les applications et les services spécifiquement approuvés à s'exécuter sur les systèmes de votre réseau.

**Segmentez votre réseau** : Divisez votre réseau en segments distincts pour limiter la propagation des ransomwares en cas d'infection.

**Filtres de messagerie** : Utilisez des outils avancés de filtrage des e-mails pour détecter et bloquer les e-mails malveillants avant qu'ils n'atteignent les utilisateurs.

**Désactivez les macros** : Beaucoup de ransomwares se propagent via des macros malveillantes dans les documents. Configurez vos logiciels de bureau pour désactiver les macros par défaut et n'autorisez leur exécution que si vous êtes absolument certain de leur provenance.

**Plan de réponse aux incidents** : Préparez un plan sur la manière de réagir en cas d'infection par un ransomware. Cela peut inclure la déconnexion des appareils infectés du réseau, la notification des autorités compétentes, et les étapes à suivre pour la récupération des données.

Enfin, soyez toujours vigilant et informé. Les tactiques et les techniques des cybercriminels évoluent constamment, il est donc crucial de rester à jour sur les dernières menaces et les meilleures pratiques de sécurité.

*Q : Ces conseils valent pour les particuliers et les entreprises possédant au moins un ordinateur portable ou de bureau connecté à Internet. Mais dans le cas particulier d'un forum, comment peut-il se protéger de ce genre d'attaque ?*

**GPT-4** : Les forums, comme d'autres sites web, peuvent également être ciblés par des ransomwares et d'autres types de cyberattaques. Les principes fondamentaux de la sécurité restent les mêmes, mais il y a des mesures spécifiques que les propriétaires et administrateurs de forums peuvent prendre pour protéger leur plateforme :

**Mise à jour du logiciel du forum** : Assurez-vous que la plateforme logicielle du forum est toujours à jour. Les éditeurs de logiciels corrigent régulièrement des vulnérabilités, il est donc essentiel d'appliquer ces mises à jour dès qu'elles sont disponibles.

**Sauvegardes régulières** : Tout comme pour les données personnelles, effectuez des sauvegardes régulières de la base de données du forum et de tout autre contenu essentiel. Stockez ces sauvegardes dans un emplacement sécurisé, idéalement hors site ou dans le cloud, et testez régulièrement la restauration.

**Contrôle d'accès strict** : Limitez les privilèges d'administrateur à un petit groupe de personnes de confiance. Utilisez des mots de passe forts et distincts pour chaque

compte administratif. Envisagez d'implémenter une authentification à deux facteurs pour l'administration.

**Protection contre les injections SQL** : Étant donné que de nombreux forums sont basés sur des bases de données, ils peuvent être vulnérables aux injections SQL. Assurez-vous d'utiliser des requêtes préparées ou des ORM (Object-Relational Mapping) qui traitent correctement les entrées pour éviter les injections.

**WAF (Web Application Firewall)** : Installez et configurez un pare-feu d'application web pour surveiller et filtrer le trafic web entrant. Cela peut aider à bloquer les tentatives d'attaque avant qu'elles n'atteignent votre site.

**Sécurisation des serveurs** : Assurez-vous que le serveur sur lequel le forum est hébergé est bien configuré, mis à jour et protégé. Désactivez tous les services et ports inutiles.

**Surveillance et détection** : Mettez en place des outils de surveillance pour détecter toute activité suspecte. Cela inclut la surveillance des journaux d'accès, des journaux d'erreur, et des tentatives de connexion.

**Filtrage des contenus** : Mettez en place un filtrage des publications et des téléchargements pour éviter l'upload de contenus malveillants ou de liens conduisant à des sites malveillants.

**Sensibilisation de la communauté** : Informez les membres du forum des meilleures pratiques en matière de sécurité, comme l'utilisation de mots de passe forts et le fait d'être vigilant face aux liens et téléchargements suspects.

**Plan de réponse aux incidents** : Comme pour les particuliers, les forums doivent avoir un plan en place pour savoir comment réagir en cas de violation ou d'attaque.

**Utilisez HTTPS** : Assurez-vous que votre forum utilise HTTPS pour crypter les données entre le serveur et les utilisateurs, protégeant ainsi les informations sensibles des utilisateurs.

**Sécurisation de la base de données** : Utilisez des mots de passe forts pour les bases de données, limitez l'accès à la base de données aux seuls IP nécessaires et envisagez d'utiliser un chiffrement pour les données sensibles.

La clé est d'adopter une approche multicouche pour la sécurité. Plus vous avez de barrières et de défenses en place, plus il est difficile pour un attaquant d'atteindre sa cible.

**Q :** *A propos de la sécurité d'un forum fonctionnant avec php, quelle différence y a-t-il entre `mysql_query` et `mysqli_query` ?*

**GPT-4 :** `mysql_query` et `mysqli_query` sont deux fonctions PHP qui permettent d'interagir avec des bases de données MySQL. Cependant, elles proviennent de deux extensions différentes et présentent des différences significatives en matière de fonctionnalités et de sécurité. Voici quelques points clés à connaître [ *j'ai supprimé les points qui ne présentaient pas d'intérêt essentiel* ] :

#### **Extension et Obsolescence :**

`mysql_query` fait partie de l'extension MySQL de PHP, qui est obsolète depuis PHP 5.5.0 et supprimée dans PHP 7.0.0. Elle ne doit pas être utilisée dans les nouveaux projets.

`mysqli_query` fait partie de l'extension MySQLi (MySQL improved) qui est plus moderne et offre une meilleure prise en charge des fonctionnalités de MySQL, une meilleure performance et une sécurité accrue.

#### **Sécurité et Prévention des Injections SQL :**

`mysql_query` ne fournit pas de moyen natif pour préparer des requêtes ou pour lier des paramètres, ce qui rend les requêtes vulnérables aux injections SQL si elles ne sont pas correctement traitées.

`mysqli_query` propose des "prepared statements" (requêtes préparées) qui permettent de lier des paramètres de manière sécurisée, ce qui contribue grandement à prévenir les injections SQL.

En résumé, si vous travaillez sur un projet PHP qui interagit avec une base de données MySQL, il est fortement recommandé d'utiliser l'extension MySQLi ou PDO (PHP Data Objects) plutôt que l'ancienne extension MySQL. Non seulement vous bénéficierez de meilleures performances et de fonctionnalités améliorées, mais vous serez également en mesure d'écrire un code plus sécurisé.

**Q :** *A partir de quelle date a-t-il été conseillé de remplacer `mysql_query` par `mysqli_query` ?*

**GPT-4 :** L'extension `mysql_` a été dépréciée en PHP 5.5.0, qui a été publiée le 20 juin 2013. À partir de cette version, il était officiellement recommandé de ne plus utiliser

les fonctions `mysql_` et de se tourner vers d'autres solutions, comme l'extension `mysqli_` (MySQL Improved) ou PDO (PHP Data Objects) pour une plus grande flexibilité avec différentes bases de données.

L'extension `mysql_` a ensuite été complètement supprimée dans PHP 7.0.0, ce qui signifie qu'elle n'était plus disponible du tout dans cette version et les suivantes. PHP 7.0.0 a été publié le 3 décembre 2015.

**Il est donc crucial pour tous les développeurs utilisant encore l'ancienne extension `mysql_` de migrer vers `mysqli_`, PDO, ou une autre solution de base de données moderne pour assurer la compatibilité et la sécurité de leurs applications.**