Forum: Aide - Recherche de logiciels

Topic: PoP Peeper utilisation

Subject: Re: PoP Peeper utilisation

Publié par: RGSOFT

Contribution le : 05/02/2014 07:24:30

bonjour à tous,

Poppeeper par rapport Poptrayu

moins d'options que poptrayu avec un design un peu vieillot mais agréable et plus facile à manipuler

il ne dispose pas de moyen de filtrage des spams mais d'un autre coté c'est pas sa vocation.c'est simplement un "notificateur" et pas un anti-spam au sens propre du terme.

Un assistant de creation automatique de compte que Poptrayu n'a pas.

Pour une utilisation optimale en terme de sécurité,
configurer "Options" => "View Messages" => "Default Message Viewing Preference" et choisir le texte brut, seule forme d'affichage insensible aux virus .

Aucun problème de confidentialité à craindre Les emails restant sur le serveur vous pouvez toujours les consulter . Heureusement !
Mais alors, pourquoi une option de sauvegarde sur votre disque dur ?

Pour une question de sécurité, on peut aussi lancer Pop Peeper sous Sandboxie

****

Ci-dessous, j'ai trouvé sur le web : sécuriser PoP Peeper

Comment sécuriser POP Peeper ?
Les points forts:
Pour Gmail, il suffit d'activer l'accès "pop" sur le serveur de Gmail, puis de suivre les instructions de configuration indiquées (qui sont d'ailleurs valables pour tous les logiciels compatibles pop)

MAIS il faut télécharger le PLUG IN "SSL" dans pop peeper et l'activer.

Des efforts importants ont été contribué à la sécurité de POP Peeper.
Voici une liste des fonctionnalités liées à la sécurité:
Les mots de passe et autres informations sensitve sont cryptées en utilisant des algorithmes de cryptage bien établis
Deux méthodes de protection par mot de passe vous permettent de protéger les comptes individuels et ou de l'accès à l'interface principale
Le support de SSL, TLS et APOP Crypter les données lors de l'utilisation des protocoles traditionnels

Méthodes pour détecter la falsification des mots de passe et autres données sensibles sont utilisés pour aider à protéger les données
Toutes les données peuvent être stockées sur un appareil portable donc pas de données seront laissés derrière lorsque vous quittez l'ordinateur
De nombreuses options sont fournies pour la lecture de votre e-mail, y compris la conversion en texte brut, la suppression des images et des données stockées sur un autre serveur, et plus

Comment puis-je m'assurer POP Peeper est aussi sécurisé que possible ?

Ci-dessous quelques suggestions pour ajouter une sécurité supplémentaire lors de l'utilisation POP Peeper.
Ces suggestions sont facultatifs et pas tous peuvent avoir besoin d'être mises en œuvre en fonction de votre environnement.

Utiliser SSL ou des connexions TLS pour POP3 et IMAP (SSL / TLS de soutien pour Imap a été introduit dans la version 3.1). Cette option crypte toutes les communications de données entre votre ordinateur et le serveur, y compris votre identifiant et votre mot de passe. Les services de messagerie utilisent intrinsèquement chiffrement lorsque vous connecter
Pour activer SSL ou TLS support, suivez ces instructions:
1. Téléchargez et installez le plugin SSL
2. Modifiez chaque POP3 et Imap compte et à droite de la "Type de serveur", sélectionnez "TLS" ou «SSL» (choisir un qui fonctionne, la différence est
négligeable; supporte pas tous les serveurs TLS et ou SSL)
Une alternative à SSL / TLS est APOP (pour POP3) et ne nécessite pas le plugin SSL. Cette méthode ne crypte le login et le mot de passe. Très peu de serveurs POP3 en charge cette méthode.

Activer la protection par mot de passe pour empêcher d'autres personnes d'accéder à l'interface POP Peeper:
1. Options Access / Set Admin Password
2. Entrez le mot de passe et la confirmation et cochez la case «activer la protection par mot de passe"
3. Appuyez sur OK
Alternativement, vous pouvez activer la protection par mot de passe pour les comptes individuels en modifiant le compte et permettant "Mot de passe protégé"
Afficher les messages à l'aide de texte brut ou enrichi par défaut. Affichage des messages en HTML vous rend plus vulnérable aux scripts malveillants, des virus et des agents de suivi.
1. Outils d'accès / Options
2. Sélectionnez la page "Afficher le message"
3. Réglez le "Message par défaut Affichage Préférence" à "texte riche" (ou "texte")
4. Cliquez sur OK
Si vous constatez qu'un message est sûr à vue (ie. il est d'une source fiable), vous pouvez afficher les messages individuels avec HTML. Vous pouvez ajouter le bouton "HTML" de la barre d'outils du message en utilisant les étapes suivantes:
5. Afficher un message
6. Accès Vue Personnaliser la barre /
7. Recherchez et sélectionnez le bouton "HTML" dans la fenêtre de gauche
8. Dans la fenêtre de droite, cliquez sur le bouton que vous souhaitez que le bouton HTML à comparaître devant
9. Cliquez sur le bouton "Ajouter"

10. Appuyez sur Fermer
Chaque fois que vous souhaitez afficher le message en cours avec le langage HTML, appuyez sur le bouton de la barre d'outils HTML

je pense que ma recherche ci-dessus, intéressera quelques uns.

RGSOFT