# Attaques Cryptographiques Sur Les Serveurs Linux : Mineurs Malveillants et Vulnérabilités SSH

Une vague de cyberattaques cible spécifiquement les serveurs Linux en les intégrant de force dans des réseaux de minage de cryptomonnaies et en propageant simultanément des attaques par déni de service distribué. Selon le rapport récent du AhnLab Security Emergency Response Center (ASEC), des cybercriminels exploitent des failles de sécurité en devinant les identifiants SSH à travers des attaques par force brute, communément appelées attaques par dictionnaire. Ces intrusions permettent l'installation de scanners de ports et de logiciels malveillants variés, dont DDOSbot et CoinMiner.

Après installation, ces programmes malveillants scrutent le réseau à la recherche de nouveaux serveurs à compromettre, amplifiant ainsi la portée de l'attaque. Parallèlement, les informations d'accès obtenues (IP et identifiants) sont souvent vendues sur le dark web, augmentant le risque de violations futures.

L'ASEC souligne que l'outil d'attaque semble provenir d'un collectif nommé PRG old Team, bien que modifié pour ces opérations spécifiques. Ces attaques ciblent principalement des systèmes exposant le port 22, le port par défaut pour les connexions SSH, exploitant ainsi les faiblesses des politiques de mots de passe et de sécurité.

En réponse, il est vivement recommandé aux administrateurs et utilisateurs de renforcer les mots de passe, d'assurer une mise à jour constante des systèmes, et si possible, de déplacer le service SSH vers un port moins conventionnel que le port 22. Ces mesures préventives sont d'autant plus cruciales à la suite des récentes attaques de Terrapin (CVE-2023-48795), visant spécifiquement le protocole SSH à travers une technique de troncature de préfixe.

Face à la menace persistante des attaques de Terrapin, une mobilisation des chercheurs a mené à contacter près de 30 fournisseurs de services SSH. Ils signalent que le processus de mise à jour et de correction des vulnérabilités peut être long, mettant en lumière la nécessité d'une vigilance et d'une adaptation continues face aux évolutions des menaces cybernétiques.

*Source :*
*https://www.linux-magazine.com/Online/News/Linux-Machines-with-Poorly-Secured-SSH-Servers-are-Under-Attack*

## Configurer une alerte par mail

Pour configurer un serveur afin qu'il envoie un email chaque fois qu'une connexion SSH se produit sur un compte particulier, vous pouvez utiliser les scripts de shell et la fonctionnalité de notification par e-mail du système. Voici une méthode générale que vous pourriez suivre, en supposant que vous avez déjà une configuration de serveur de messagerie ou un service SMTP que vous pouvez utiliser pour envoyer des e-mails:

1. **Configurer le Serveur de Messagerie**:

Assurez-vous que votre système est capable d'envoyer des emails. Cela peut être fait via `sendmail`, `postfix`, ou un client SMTP comme `ssmtp` ou `msmtp` relié à un service à un fournisseur SMTP.

2. **Créer un Script de Notification**:

Créez un script shell (`notify.sh` par exemple) qui envoie un email lorsque quelqu'un se connecte via SSH. Voici un exemple de ce à quoi le script pourrait ressembler:

```
#!/bin/bash

# Mettez l'adresse e-mail du destinataire ici
RECIPIENT="your-email@example.com"

# Message de notification
SUBJECT="Alerte de Connexion SSH"
MESSAGE="Une connexion SSH a été établie sur $(hostname) par $(whoami) à $(date)."

# Commande pour envoyer l'email
echo "$MESSAGE" | mail -s "$SUBJECT" $RECIPIENT
```

3. **Modifier le Fichier de Configuration SSH**:

Éditez le fichier de configuration SSH `sshd_config` situé normalement dans `/etc/ssh/sshd_config`.

Ajoutez ou modifiez la ligne `ForceCommand` pour l'utilisateur spécifique ou globalement pour exécuter le script à chaque connexion. Par exemple:

```
Match User nomutilisateur
ForceCommand /chemin/vers/notify.sh
```

4. **Rendre le Script Exécutable et Redémarrer le SSHD**:

Assurez-vous que le script est exécutable : `chmod +x /chemin/vers/notify.sh`.

Redémarrez le service SSH pour appliquer les modifications : `sudo systemctl restart sshd` ou `sudo service sshd restart` selon votre système.

5. **Testez la Configuration**:

Testez en vous connectant via SSH pour voir si vous recevez un email.

## Notes importantes

- Assurez-vous que le script et la configuration ne nuisent pas à la capacité de se connecter en SSH. Testez cela soigneusement.
- Soyez conscient de la sécurité et des implications de la confidentialité de l'envoi d'informations par e-mail.

- Cette méthode envoie une notification pour chaque connexion SSH, pas seulement pour les connexions réussies. Vous pouvez affiner le script pour répondre à des besoins plus spécifiques.

C'est une approche de base.