

Jean-Marc LAMBERT
www.specialistes.be
navis.lambert@gmail.com
00 32 496 10 65 90

VoIPBullGuard Présentation du service

A quoi sert VoIPBullGuard ?

Chaque fois qu'un nouveau serveur VoIP entre en production, les hackers VoIP commencent à s'introduire après moins de 24 heures à l'aide de programmes automatiques, en procédant en plusieurs étapes.

VoIPBullGuard sert à protéger les serveurs VoIP contre les attaques sur **le port ssh, le port 5060** (VoIP) et **le port 80** (serveur Apache)

VoIPBullGuard utilise **fail2ban** et **iptables**, deux sous-programmes de **Linux CentOS**.

Pour assurer une bonne protection, il est important que le serveur VoIP ne soit plus joignable sur le port 22, et qu'il soit nécessaire de d'abord s'identifier par un compte secondaire avant de passer au compte root.

Il est possible de bloquer des ip entrantes avec iptables, cependant cette opération nécessite des interventions journalières d'un informaticien spécialisé.

VoIPBullGuard permet d'automatiser la défense du serveur, parfois avant même que celui-ci soit attaqué.

Remarque : Les attaques sur le port 80 consiste à accéder à votre billing ou à phpmyadmin, elles consistent à chercher le dossier qui contient ces sections sensibles, et génèrent de multiples messages d'erreur qui épuisent le processeur et bourre le fichier log du serveur Apache.

Ce que ne peut pas faire VoIPBullGuard ?

VoIPBullGuard ne peut pas vous protéger contre le vol des login & mots de passe de billing par un cheval de troie introduit dans un ordinateur.

Cet incident peut se produire quand vous utilisez un antivirus périmé, ou que vous n'utilisez pas un **anti-malware**, tel que **Emsisoft**. (complément incontournable d'un antivirus)

Il en est de même si vous consultez vos billing dans un cybercafé, ou que vous utilisez un ordinateur domestique connecté **via le wifi**, avec un mot de passe trop faible.

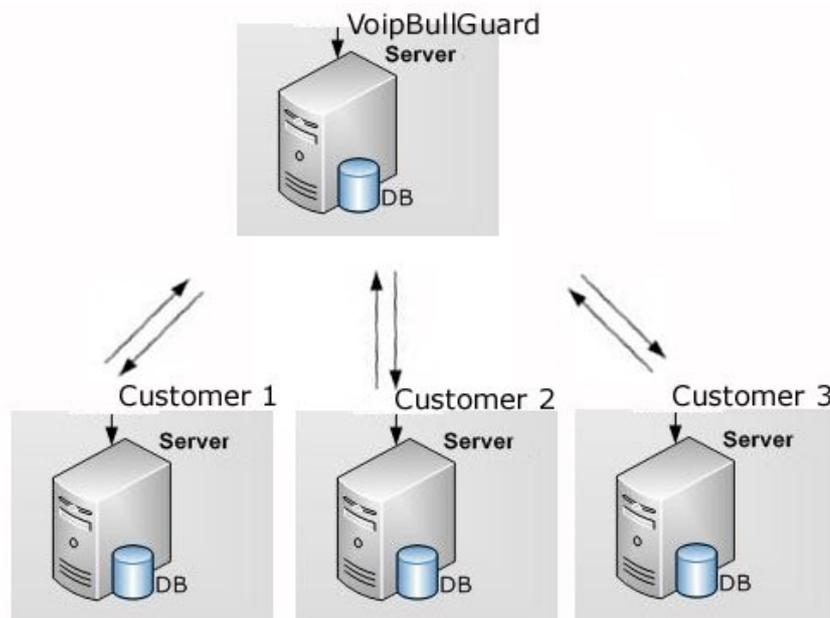
Jean-Marc LAMBERT
www.specialistes.be
navis.lambert@gmail.com
00 32 496 10 65 90

Fonctionnement de VoIPBullGuard

Le programme fail2ban des serveurs VoIP « clients » envoient par email les ip suspectes relatives à des tentatives d'intrusion

Le serveur « Maître » contient une base de données de hackers, que son webmaster alimente après avoir vérifié la provenance de l'attaque.

Le serveur « Maître » envoie une liste de 5 ip à bloquer par jour à tous les serveurs « clients », qui ajoutent une fois par jour les ip à bloquer dans le fichier d'iptables.



Comment activer ce service ?

→ Soit nous le faisons nous-mêmes, après avoir reçu un accès via à Putty à votre serveur. Cette opération prend une dizaine de minutes, ensuite vous pouvez votre mot de passe root.

→ Soit nous vous envoyons la procédure à suivre pour activer notre service sur votre serveur. En pareil cas, nous n'avons pas besoin d'accéder à votre serveur.

Les avantages

→ Nous sommes prévenus des attaques par plus de 60 serveurs VoIP

→ Plus besoin de demander à un informaticien d'intervenir sur iptables

Tarifs

- **60,00 euros par mois TTC,**
- **181,00 euros TTC à la première intervention si nous devons au préalable sécuriser nous-mêmes votre serveur (changement de port ssh, compte secondaire, fail2ban)**