

Machine Semi Hackée2 du 29/09/2004

Qu'est-ce que ça veut dire semi hackée ? Cela veut juste dire que la machine ne doit pas être réinstallée, car le hacker n'a pas pu se connecter en root sur la machine. On peut donc prendre le risque de penser qu'étant donné que le hacker n'a pas été connecté en root, il n'a pas pu modifier le système.

Pourquoi 'du 29/09/2004' ?

Simplement parce que ce jour, les machines hackées ont généré une attaque de 1Gb vers un destinataire qui ne doit pas être content.

### Comment voir ?

```
# ls -aul /proc/*/exe 2>/dev/null | grep deleted
lrwxrwxrwx 1 nobody nobody 0 sep 29 11:24 /proc/5910/exe -> /tmp/upxCKRKOKLAPA4 (deleted)
```

ou

```
# find /proc -name exe -ls 2>/dev/null | grep deleted
```

Nous voyons qu'il y a un processus qui est lancé en user nobody, group nobody, dont le binaire original a été effacé. Si cette commande ne sort aucun résultat, c'est que vous n'êtes pas actuellement hacké. Cependant, peut-être que nous avons déjà fait le ménage et donc que nous vous avons déjà contacté. Reportez vous au grep des logs apache pour vérifier.

```
# cat /proc/5910/cmdline
/usr/local/apache/bin/httpd
```

La ruse du hacker est qu'il a renommé son processus en '/usr/local/apache/bin/httpd' pour être discret.

L'attaque du jour a été menée par l'ip :

```
# host 210.169.91.66
66.91.169.210.in-addr.arpa is an alias for 66.64.91.169.210.in-addr.arpa.
66.64.91.169.210.in-addr.arpa domain name pointer january.medical9.gr.jp.
```

Pour trouver votre script qui est à l'origine de la faille de sécurité, faire un grep de cette ip dans vos logs d'apache (attention, certaines machines sont hackées de longue date (log en .gz)).

Note : si le ménage a déjà été fait, seul le parcours des logs vous permettra de trouver la trace du hack.

### Faille originelle

Ce hack s'appuie sur une erreur de programmation en php. Un 'include' prend en paramètre le fichier a

## OVH

inclure. 'include' va chercher le fichier et l'exécute sur le serveur. La faille est que php permet d'aller chercher ce fichier sur une url (note : faille ne veut pas dire bug). L'erreur de programmation est que ce fichier est en fait une variable. Et cette variable est remplie à partir d'une information passée lors de l'appel de la page. Le hacker a donc tout simplement rempli cette variable avec le lien vers son script de hack sur un site distant.

### **Menage**

Pour faire le ménage referez vous au guide MachineSemiHackee.