

Kouba le 13 octobre 2008

**Objet** : Rapport de coupure du service d'hébergement du 09/10/2008.

Cher client,  
Voici la chronologie d'évènements liés à la coupure du 09/10.

### ***Mercredi***

**15h30** : Une lenteur inhabituelle du serveur a été signalée par certains clients. Lenteur affectant uniquement les sites web, la messagerie, à ce moment là, n'était pas encore concernée.

**16h00** : Reboot du serveur pour revenir à un fonctionnement normal. Le serveur a, effectivement, retrouvé son fonctionnement normal mais cela n'a duré qu'une heure de temps.

**17h00** : Le serveur ne répondait plus, les techniciens du Data Center en France ont intervenu spontanément pour remettre le serveur en marche, ils ont alors décelé un problème avec le firewall qui bloquait la machine, ils ont relancé le serveur en mode netboot (démarrage sur réseau) afin de nous permettre de procéder aux réparations nécessaires. La configuration d'un firewall peut s'avérer parfois délicate, nous avons donc décidé de le désinstaller momentanément pour permettre à la machine de démarrer. Nous avons ensuite redémarré le serveur qui semblait de nouveau fonctionner correctement.

**18h00** : Nouvelle coupure, cette fois c'est Apache (le serveur web) qui ne répondait plus. Nous avons procédé à sa réinstallation immédiate, mais il a de nouveau cessé de fonctionner après une dizaine de minutes. Nous avons donc compris à ce moment là que nous faisons peut-être l'objet d'attaques DDOS qui ont saturé Apache.

**19h45** : Confirmation des attaques, celles-ci provenaient d'Italie et de Russie. Nous avons procédé à la réinstallation et la reconfiguration immédiate du firewall.

**20h30** : Le serveur fonctionnait de nouveau normalement mais des courtes coupures étaient régulièrement enregistrées.

### ***Jeudi***

**7h35** : Nouvelle coupure, le firewall a été de nouveau reprogrammé, les attaques ont été bloquées vers 11h15. Le serveur est revenu à son état normal.

**18h30** : Nouvelle vague d'attaques, cette fois en provenance essentiellement d'Iran, le nombre était trop élevé (50 requêtes simultanées par IP). Nous avons demandé à notre fournisseur de mettre en place un appareil Cisco pour bloquer les attaques, mais comme cette opération ne pouvait se faire immédiatement, il fallait donc trouver la solution dans notre firewall

**18h45** : Notre partenaire DZSecurity chargé de la sécurité du serveur a intervenu pour trouver une solution définitive et radicale aux attaques DDOS. Il a procédé à ce qui suit :

- Recompilation du Kernel (noyau) ;
- Reconfiguration du firewall pour pouvoir bloquer tout type de ping ;
- Activation du Shell Fork Bomb Protection afin de stopper toutes les opérations de surcharge de serveur ;
- Ajout de nouvelles règles et caractéristiques dans les modules de protection et services afin de bloquer ce genre d'attaques à l'avenir.

Suite à cela, les attaques ont été définitivement bloquées et le serveur mis à l'abri contre d'éventuelles attaques futures.

Nous vous adressons nos sincères excuses pour la gêne occasionnée et nous pouvons, d'ores et déjà, vous garantir que les attaques DDOS ne toucheront plus nos serveurs.

Nous restons à votre entière disposition pour de plus amples information.

L'équipe Novihost