

**Arbor Networks : Les attaques DDoS, des menaces informatiques évoluées**

**Sécurité**

Posté par : JPilo

Publiée le : 31/1/2013 11:00:00

**Arbor Networks Inc**, publie sa 8ème étude annuelle sur **la sécurité des infrastructures IP mondiales** (WISR, Worldwide Infrastructure Security Report), offrant aperçu unique des problèmes de sécurité les plus critiques auxquels sont confrontés les opérateurs réseau.

**Parmi les principaux résultats de l'enquête cette année** : les menaces persistantes avancées (APT) viennent en tête des préoccupations des opérateurs comme des entreprises ; les attaques par déni de service distribué (DDoS) voient leur ampleur se stabiliser mais gagnent en complexité ; les centres de données et les services Cloud sont des cibles particulièrement visées ; les opérateurs mobiles continuent de réagir a posteriori en termes de visibilité réseau. L'étude aborde également l'impact du BYOD ainsi que les questions d'infrastructure telles que la VoIP et IPv6.



S'appuyant sur les données fournies par des opérateurs réseau à travers le monde, cette étude annuelle est conçue pour éclairer les décisions stratégiques de ces derniers en matière de sécurité et d'intégrité des infrastructures IP critiques (Internet et autres). Elle est rendue possible chaque année par la précieuse collaboration de nos clients. En effet Arbor entretient des relations de longue date avec ses clients non seulement comme fournisseur mais aussi comme conseiller. Cliquez ici pour accéder à la 8ème étude annuelle d'Arbor Networks sur la sécurité des infrastructures IP mondiales.

« Depuis sa fondation, Arbor Networks collabore avec les opérateurs réseau les plus exigeants au monde. Cette étude annuelle est le fruit d'un authentique partenariat avec nos clients et la communauté de la sécurité informatique dans son ensemble », commente **Colin Doherty**, président d'**Arbor Networks**. « Cette année encore, elle fournit de précieuses indications pour les opérateurs de services Cloud, de réseaux mobiles et de réseaux d'entreprise. »

**Principaux résultats :**

Les menaces persistantes avancées (APT) viennent en tête des préoccupations des opérateurs comme des entreprises

- 61% classent les « botnets » ou autres systèmes hôtes infectés au premier rang de leurs inquiétudes

- 55% placent les menaces persistantes avancées (APT) en tête de leurs préoccupation

DDoS : stabilisation de l'ampleur des attaques ; recrudescence des attaques multivecteurs complexes

- L'attaque la plus massive relevée a atteint 60 Gbit/s en 2012 (comme en 2011, contre 100 Gbit/s en 2010).

- 46% des responsables interrogés signalent des attaques multivecteurs.

### Les centres de données et les services cloud sont de plus en plus victimes d'attaques

- 94% des opérateurs de centres de données font état d'attaques.

- 90% d'entre eux imputent des dépenses opérationnelles aux effets de ces attaques.

### Les opérateurs mobiles continuent de réagir a posteriori

- 60% n'ont aucune visibilité sur leur trafic de paquets mobiles/évolués.

### Le BYOD crée de nouvelles problématiques

- 63% des responsables interrogés autorisent désormais le BYOD (usage d'équipements personnels) sur leurs réseaux.

- Cependant, seuls 40% disposent d'un moyen de surveiller ces équipements.

### L'infrastructure DNS demeure vulnérable

- 27% de participants à l'enquête ont subi sur leur infrastructure DNS des attaques DDoS ayant eu un impact sur leurs clients, soit une nette augmentation par rapport à l'an passé (12%).

71% des responsables interrogés estiment avoir une bonne visibilité des couches réseau 3 et 4, mais seulement 27% en ce qui concerne la couche 7. Ce manque de visibilité, auquel s'ajoute l'absence de personnel de sécurité dédié, crée un environnement très propice aux attaques. Les agresseurs ont dorénavant à leur disposition de nombreuses cibles à partir desquelles lancer des attaques par réflexion.

### Les déploiements IPv6 gagnent du terrain

- 80% des participants ont déjà déployé IPv6 ou prévoient de le faire dans les 12 prochains mois.