La solution Pravail APS v.2.5 d'Arbor Networks assure la disponibilité des services sur Internet

Protection des services critiques SSL et prise en charge des réseaux de type CDN en particulier contre les attaques DDoS

Paris, 9 mars 2011 – Arbor Networks, Inc., société leader dans la fourniture de solutions de sécurité et de gestion de réseaux d'opérateurs convergents et de centres de données de nouvelle génération, annonce la nouvelle version de sa solution Pravail APS (*Availability Protection System*), qui protège les réseaux d'entreprise contre les menaces pour leur disponibilité, en particulier au niveau de la couche application, contre les attaques par déni de service distribuées (DDoS). Outre une visibilité, un contrôle et un reporting renforcés, Pravail APS v.2.5 apporte des fonctions optimisées pour la protection de services critiques basés sur les technologies SSL et CDN (*Content Delivery Network*).

Une récente étude d'Infonetics Research, consacrée aux perspectives du marché des appliances de prévention des attaques DDoS (*DDoS Prevention Appliance Market Outlook*), cite Arbor Networks comme « *le leader dominant en matière de prévention DDoS* » sur l'ensemble du marché ainsi que dans les segments Opérateurs de transport et Haut débit fixe, Centres de données d'entreprise et Mobiles.

Grâce à son système de surveillance d'Internet ATLAS, Arbor Networks constate que les réseaux d'entreprise sont exposés à des attaques DDoS de plus en plus variées, allant d'attaques de flooding à des attaques applicatives de moindre envergure, plus difficiles à détecter, visant la messagerie, les services Web, le e-commerce et la téléphonie sur IP (VoIP). Les attaques gagnent en complexité mais sont néanmoins plus faciles à perpétrer. De ce fait, les réseaux d'entreprise à travers le monde sont plus fréquemment victimes de pannes dues à attaques DDoS, avec des conséquences d'une gravité sans précédent pour les entreprises concernées.

« *Avec le produit Pravail APS, nous avons intégré notre technologie d'identification et de neutralisation DDoS de classe opérateur à une solution conçue sur mesure pour les centres de données d'entreprise. Face au paysage des menaces aujourd'hui complexes, les attaques applicatives doivent être traitées à la périphérie du réseau, avant qu'elles ne submergent les équipements de sécurité existants tels que les pare-feu (firewalls) et les systèmes de prévention d'intrusion (IPS) et, en tout cas, avant qu'elles ne touchent les services critiques comme SSL* », explique Colin Doherty, président d'Arbor Networks.

Informations mondiales sur les menaces, avec mises à jour automatiques

Les données de trafic anonymisées issues de plus d'une centaine de réseaux clients, combinées à un réseau mondial de sondes de type « honeypot », constituent le cœur du système de surveillance d'Internet ATLAS d'Arbor Networks qui alimente toutes les solutions de la marque, y compris l'appliance Pravail APS. Les données ATLAS permettent à l'équipe ASERT (*Arbor Security Engineering & Response Team*) d'élaborer une vision globale du trafic malveillant traversant les réseaux qui forment l'épine dorsale d'Internet. En cas de détection d'un nouveau botnet ou d'une nouvelle attaque applicative, une signature est créée, diffusée via le flux AIF (*ATLAS Intelligence Feed*) et installée sur le produit Pravail APS d'Arbor.

AIF permet aux équipes informatiques des entreprises d'exploiter les informations mondiales sur les menaces provenant du réseau ATLAS, associées à l'analyse quotidienne de ces mêmes menaces par les chercheurs d'Arbor, leur faisant ainsi gagner un temps précieux en leur évitant d'avoir à mettre à jour manuellement les signatures en fonction des dernières attaques détectées. Enfin et surtout, grâce à ce dispositif intégré et automatisé de lutte contre les menaces, les entreprises peuvent rapidement bloquer les attaques DDoS avant qu'elles n'aient un impact sur leurs services critiques.

Protection contre les attaques sur le protocole SSL
Aujourd'hui, le protocole SSL (*Secure Sockets Layer*) offre aux entreprises et à leurs clients les fonctions de sécurité et de cryptage nécessaires pour sécuriser leurs transactions et communications sensibles sur Internet. Alors que les entreprises s'en remettent de plus en plus à SSL pour leurs échanges critiques, celui-ci devient une cible privilégiée pour les attaques DDoS. Afin d'assurer la disponibilité des services reposant sur SSL, la solution Pravail APS d'Arbor bloque désormais les attaques DDoS visant ce protocole, quelle que soit l'application concernée (HTTPS, POP3S, SMTPS, etc.) grâce à des protections conçues par ASERT pour contrer le trafic malformé, les tentatives de renégociation continuelle des connexions et d'autres attaques évoluées destinées à perturber la disponibilité des services.

Prise en charge des CDN et des proxies
Jusqu'ici, les entreprises employant des réseaux de type CDN et des proxies n'avaient guère de solutions pour en protéger la disponibilité, du fait que de nombreuses techniques de neutralisation DDoS se fondent outre mesure sur des listes noires d'adresses IP. Etant donné que les CDN et les proxies masquent les adresses IP des postes clients, les solutions trop simplistes bloquent toutes les connexions provenant d'un CDN ou d'un proxy – sans faire la distinction entre le trafic légitime et les attaques – dès lors qu'une attaque DDoS a été identifiée. Cette méthode de neutralisation ne fait alors qu'amplifier les attaques.

La solution Pravail APS prend dorénavant en charge les CDN et les proxies, ce qui lui permet d'opérer dans tous les environnements d'entreprise sans exiger une reconfiguration du réseau pour en protéger la disponibilité. Arbor Networks s'appuie à la fois sur une visibilité globale et sur des recherches avancées en matière de sécurité pour actualiser en permanence ses signatures. Les protections anti-DDoS évoluées conçues par ASERT permettent à la solution Pravail APS d'assurer une protection efficace de la disponibilité, avec ou sans listes noires. Les entreprises qui utilisent des CDN et des proxies n'ont donc plus à sacrifier leurs besoins métier sur l'autel de la sécurité.

Renforcement de la visibilité, du contrôle et du reporting
La confiance dans la protection contre les attaques DDoS est établie par la visualisation des attaques bloquées et finalement la disponibilité des services protégés. Nos clients peuvent avoir pleinement confiance en notre solution Pravail APS v.2.5 qui produit des rapports détaillés sur les systèmes hôtes bloqués et les raisons pour lesquelles ils l'ont été. L'interface utilisateur et les rapports générés confirment que le trafic légitime n'est pas filtré, et permet facilement de mettre sur liste blanche les hôtes à ne pas bloquer.

A propos d'Arbor Networks
Arbor Networks est une société leader dans la fourniture de solutions de gestion de la sécurité pour les centres de données de nouvelle génération et les réseaux d'opérateurs. Sa clientèle couvre la grande majorité des fournisseurs mondiaux d'accès Internet ainsi qu'un grand nombre des réseaux d'entreprises les plus importants aujourd'hui utilisés dans le monde. Les solutions éprouvées de gestion de la sécurité proposées par Arbor facilitent la croissance et la protection des réseaux, entreprises et marques de ses clients. Les relations privilégiées qu'entretient Arbor avec les opérateurs réseau du monde entier offrent une visibilité et une perspective hors pair sur la sécurité d'Internet et les tendances du trafic via ATLAS® (*Active Threat Level Analysis System*), un effort de collaboration unique en son genre, sachant qu'il allie plus de 100 fournisseurs de services à travers le monde, qui partagent ainsi en temps réel les informations de sécurité, de trafic et de routage.

Pour un aperçu technique concernant les dernières menaces à la sécurité et tendances du trafic Internet, veuillez consulter le site http://www.arbornetworks.com ou le blog http://ddos.arbor.net.

Contact presse :
Agence bpr France
Judith Martin-Tardivat, judith@bprfrance.com, Tel: +33 1 83 62 88 12
Sophie Decaudin, sophie@bprfrance.com, Tel: +33 1 83 62 88 11