Flash Presse
Paris, le 03 juillet 2009

Deny All publie un patch contre Slowloris, une attaque visant les serveurs Web

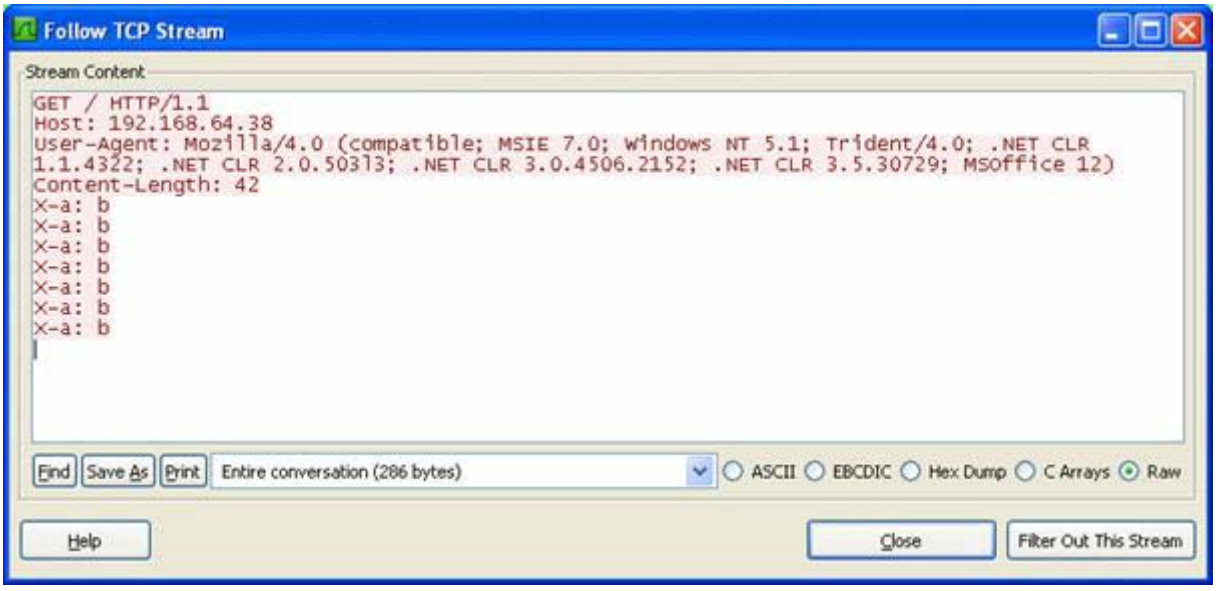
Slowloris, qui met en oeuvre une attaque par dénis de service contre les serveurs Web, a été publié le 17 juin.

Le DARC (DenyAll Research Center), division interne de Deny All dédiée à l'analyse des menaces et aux techniques de protection, a effectué une analyse de l'outil et du concept de l'attaque. Après 10 ans d'activité, les recherches effectuées dans ce département ont mené à la conception des meilleurs moteurs de protection des applications Web actuellement disponibles sur le marché.

Description de l'attaque

Slowloris est un script perl qui peut être exécuté sur n'importe quel système Unix.

L'attaque consiste à initier des requêtes HTTP sans les terminer, la connexion étant maintenue active par l'envoi répétitif d'en-têtes. La figure ci-dessous montre une trace de ces requêtes, et identifie clairement l'en-tête « X-a : b » utilisé par l'outil.



Le serveur Web Apache ne transmet les requêtes aux modules de traitement qu'une fois ces dernières complétées. Par conséquent, le serveur est vulnérable dans la mesure où il ne libère pas les connexions actives établies par l'outil. Pour la même raison les modules de sécurité ne peuvent être appliqués.

Une fois l'attaque lancée le serveur cible maintient des connexions ouvertes dans l'état ESTABLISHED.

Après un temps relativement court le serveur n'est plus accessible. Cet état est maintenu pendant toute la durée de l'attaque.

Protection

Le samedi 20 juin 2009, le DARC a fourni à ses clients une solution de contournement. Celle-ci, basée sur des règles de filtrage et des mécanismes de limitation de connexion, permet de protéger les sites Web contre cette attaque.

Le 26 juin 2009, un patch a été publié pour l'ensemble des produits et ce dernier est publiquement distribué aujourd'hui à l'issue d'une semaine de tests.

Par conséquent, **l'ensemble des clients Deny All bénéficient dès à présent d'une protection contre cette attaque ainsi que l'ensemble de ses variantes.**

Il s'agit de la première publication d'un patch pour un produit basé sur Apache contre cette attaque.

A ce jour, aucune protection native à Apache n'est disponible dans la mesure où elle nécessite une modification de son mode de fonctionnement interne.

Grâce à l'étude menée par son centre de recherche, Deny All est le premier éditeur à avoir fournit un correctif pour l'ensemble de ses plates-formes en production.

A Propos de Deny All

Pionnier du WAF (Web Application Firewall), Deny All est aujourd'hui le leader européen de la protection et de l'accélération des applications Web, XML et FTP. Deny All fournit des solutions éprouvées aux Grands Comptes au niveau mondial, sur tous secteurs d'activités. Ses produits, disponibles sous forme logicielle ou appliance, assurent la protection, l'authentification et l'accélération des transactions Internet, extranet et intranet. Les solutions de Deny All sont faciles à installer et garantissent le plus haut niveau de protection contre les attaques connues et inconnues grâce à un filtrage applicatif des flux HTTP(S), SOAP/XML et FTP(S). Aujourd'hui, les solutions de Deny All protègent plus de 10 000 applications web à travers le monde.
Deny All est membre du CLUSIF, de l'OWASP, de l'OSSIR, de la SAP Global Security Alliance et de Liberty Alliance.

Ayant son siège social à Paris, Deny All est présent dans la plupart des pays européens via des équipes locales en Allemagne, Benelux, Espagne, et Pays Nordiques et via son réseau de partenaires.