Avis d'expert,
Paris, le 28 janvier 2011

Les récentes usurpations d'identités sur Facebook auraient pu être facilement évitées grâce à un Firewall Applicatif Web

Les réseaux sociaux continuent de faire parler d'eux mais sous un angle peu rassurant... Dernière actualité en date : le piratage du propre compte Facebook de Marc Zuckerberg, le fondateur du célèbre réseau social ! Comment un outil touchant plus de 500 millions de personnes à travers le monde peut-il être aussi vulnérable ? Deny All, à travers la voie de son Directeur technique, Renaud Bidou, apporte des éléments de réponses.

Mode opératoire du hacker :
Il suffit au pirate de se procurer un logiciel d'attaque par « force brute », disponible très facilement sur le Web. Depuis la page d'accueil de Facebook, le hacker rentre le login de l'utilisateur ciblé et lance le logiciel. Ce dernier travaille alors tout seul en utilisant la technique dite de « l'attaque par dictionnaire » : il essaie tous les mots existants dans le dictionnaire ainsi que leurs dérivés (ajouts de chiffres, de pluriels…), et finit par trouver le bon ! Le pirate devient ainsi l'utilisateur du compte et peut intervenir comme bon lui semble : changement de statuts, ajouts de commentaires, ou encore injection de « bouts » de codes malveillants qui infectent toute personne visitant le profil.

Pourquoi cette attaque a pu se produire ? Deux raisons possibles :
- Aucune protection sous prétexte qu'elle pourrait « ralentir » le chargement des pages ;
- ou bien, un WAF non performant.

Une solution simple pour se prémunir d'une telle attaque : un Firewall Applicatif Web (WAF) :
Une application Web, telle qu'une page Facebook, peut être protégée par un moteur statistique (aussi appelé moteur d'analyse comportementale) conçu pour détecter et bloquer ces attaques. Ce type de moteur décèle les tentatives d'authentification répétées, mode opératoire des logiciels d'attaque par force brute, et est mis en œuvre par certains Firewalls applicatifs Web (WAF).

Pour tout éclairage et expertise à ce sujet, n'hésitez pas à contacter OXYGEN pour être mis en relation avec Renaud Bidou, Directeur Technique de Deny All.

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 20 000 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 dans de nombreux pays du monde via son réseau de partenaires.