Communiqué de presse
Le 3 février 2009

SOGETI, LA "LUTTE INFORMATIQUE OFFENSIVE[1] " OU SENSIBILISER POUR MIEUX NEUTRALISER LES ATTAQUES INFORMATIQUES

Sogeti, filiale du Groupe Capgemini, a organisé le 3 février 2009 un séminaire sur la lutte contre les offensives informatiques. L'objectif était de sensibiliser les directions informatiques aux attaques massives (cybercriminalité et botnets) et aux attaques ciblées (contournement des défenses et intrusion). Cette démarche s'inscrit dans le prolongement du livre blanc de la Défense nationale.

Face à l'évolution des menaces informatiques (espionnage étatique ou industriel, cyber-guerre, …), l'État français a décidé de se doter des moyens adaptés à l'évolution du contexte international : « *Il convient donc de disposer d'une capacité de neutralisation à l'intérieur même des centres d'opérations adverses : c'est l'objet de la Lutte Informatique Offensive.* » (Livre blanc sur la Défense nationale et la sécurité nationale - juin 2008).

Sogeti a présenté les résultats de ses travaux axés sur les thèmes suivants :

La cybercriminalité

Monsieur David BIZEUL, Responsable du CERT[2] de La Société Générale a expliqué la problématique concrète d'une banque. Son intervention a permis de mettre en exergue les menaces et les types d'incidents liés à la cybercriminalité vécue en interne par ses équipes dédiées.

Les hébergeurs deviennent des proies sensibles

Les hébergeurs bulletproof offrent des services d'hébergement classique, tout en garantissant à leurs clients un anonymat total et une qualité de service maximale. Les services, dotés d'une très grande permissivité sur le contenu hébergé, sont particulièrement destinés à des activités criminelles : stockage de code malicieux, serveurs d'upload de données volées, serveurs de commande (C&C) de botnets, campagnes de spam, etc.

Cas pratiques : analyse du botnet Sality

Dans le cadre de la cybercriminalité, l'équipe R&D de Sogeti a expliqué les agissements d'un groupe de malfaiteurs à partir d'un virus récupéré lors d'une intervention d'urgence chez un client. En effet, le développement de virus n'est plus seulement l'apanage d'adolescents, mais s'intègre à une cybercriminalité organisée générant des profits illégaux importants. Certains virus sont

[1] lutter contre les offensives informatiques
[2] Computer Emergency Response Team

CONTACTS PRESSE
Eric DELEAGE - Directeur du Marketing et de la Communication SOGETI - Tél : +33 (0) 1 41 12 51 02
Anne BAYLAC – relations presse SOGETI - Tél : +33 (0) 1 41 12 46 06
SOGETI : 6 rue Duret - 75784 Paris cedex 16 - Tél. : +33 (0) 1 58 44 55 66

développés avec des techniques industrielles et s'organisent en réseaux de machines infectées : les botnets. Ces derniers sont contrôlables à distance par des cyber criminels pour réaliser du spam, du déni de service ou d'autres activités génératrices de revenus illégaux.

Les produits de sécurité sont-ils tous fiables ?
Sensibiliser aux différentes façons de contourner les produits de sécurité pour mieux appréhender les risques**.** Le marché des produits de sécurité demeure très vaste et dense avec une offre de protection dite optimale, accrue ou encore de détection et de protection de nouvelles menaces. Pourtant, il n'est pas rare de voir des erreurs d'implémentation ou de conception réduire drastiquement, voire à néant, le niveau de sécurité d'un produit. Lors de cette présentation nos experts ont détaillé l'analyse réalisée sur des produits de sécurité tels que firewalls, IDS et anti-virus.

La norme PDF, un vecteur d'infection ?
Un fichier PDF peut se révéler être un vecteur d'infection rêvé pour un attaquant. La norme PDF, devenue incontournable, est désormais une norme internationale ISO-32000-1. Aux yeux de nombreux utilisateurs, un fichier PDF n'est autre qu'une simple feuille prête à imprimer. Pourtant, ce type de fichier peut posséder un contenu actif directement exécuté par le lecteur PDF de manière tout à fait standard.

Les navigateurs web, nouvelle faille
Les navigateurs Web embarquent un nombre croissant de fonctionnalités (rootkits pour navigateurs). Présents sur la très grande majorité des machines connectées au réseau, manipulent du contenu sensible (logins/passwords, mails confidentiels, informations personnelles ou professionnelles), ils sont très souvent autorisés à se connecter à Internet. Ils deviennent une cible de choix pour quiconque voudrait subtiliser de l'information de haute valeur à l'insu de l'utilisateur et du SI. Le laboratoire sécurité de Sogeti, à titre expérimental, a développé des rootkits navigateurs pour illustrer ces attaques qui peuvent être menées sur les navigateurs Web tels que le vol de mots de passe, de fichiers du poste utilisateur ou encore la prise de contrôle à distance de la machine.

A propos de Sogeti
Sogeti est l'un des leaders des services informatiques et d'ingénierie de proximité, spécialisé dans la gestion des applicatifs et des infrastructures (*application and infrastructure management*), le conseil en technologies (*high-tech engineering*) et le *testing*. Sogeti aide ses clients à optimiser les performances de leurs systèmes d'information grâce à l'innovation technologique. Présente dans 14 pays avec plus de 200 implantations en Europe, aux Etats-Unis et en Inde, la société réunit plus de 20 000 professionnels. Sogeti est une filiale à 100% de Cap Gemini S.A., coté à la Bourse de Paris. Plus d'informations sur : www.sogeti.com.

CONTACTS PRESSE
Eric DELEAGE - Directeur du Marketing et de la Communication SOGETI - Tél : +33 (0) 1 41 12 51 02
Anne BAYLAC – relations presse SOGETI - Tél : +33 (0) 1 41 12 46 06
SOGETI : 6 rue Duret - 75784 Paris cedex 16 - Tél. : +33 (0) 1 58 44 55 66