Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 09 novembre 2012
N° CERTA-2012-ACT-045

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-045

Conditions d'utilisation de ce document :	`http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document :	`http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-045`

1 Attaques en déni de service impliquant des serveurs français

Les attaques en déni de service distribué, également appelées DDoS (acronyme provenant de l'anglais *Distributed Denial of Service*), sont fréquentes. Elles consistent généralement à inonder la victime de paquets (TCP, UDP ou ICMP), jusqu'à saturation de sa bande passante. Récemment, des banques américaines, britanniques et françaises ont été la cible de telles attaques.

En général, les attaques en déni de service distribué ont pour origine des *botnets*, c'est-à-dire des ensembles de machines compromises qui sont en communication avec un serveur de contrôle (appelé serveur de C&C pour *command and control*). Le profil-type des machines faisant partie des *botnets* est un poste client fonctionnant sous Microsoft Windows.

La particularité des dénis de service qui ont ciblé les banques américaines est le profil des machines attaquantes : il ne s'agit pas ici de postes client mais de serveurs Web. Ces derniers ne communiquent avec aucun serveur de C&C, ils reçoivent leurs instructions d'attaques via des requêtes classiques du protocole HTTP. Certains des serveurs compromis disposant d'une bande passante importante, les dénis de service ont été très efficaces.

Le CERTA a eu l'occasion d'analyser plusieurs de ces serveurs Web compromis. Il en ressort que le mode opératoire des attaquants est simple : ils utilisent des portes dérobées déposées par d'autres intrus lors d'attaques antérieures (par exemple des défigurations) pour installer quelques fichiers PHP sur le serveur. Ils accèdent ensuite à ces pages, en spécifiant des paramètres bien précis, dans le but de déclencher le déni de service.

Pour les cas étudiés par le CERTA, les attaques en déni de service ont également eu des conséquences sur les réseaux hébergeant les sites Web compromis. En effet, les volumes de données émis par les serveurs compromis étaient tels que les réseaux attaquants n'étaient plus accessibles depuis l'Internet. Le déni de service a donc affecté à la fois la cible et la source, les rendant tous deux indisponibles.

Pour se préparer aux attaques en déni de service, le CERTA préconise l'application des recommandations de la note d'information CERTA-2012-INF-001 intitulée « Dénis de service - Prévention et réaction ».

Par ailleurs, le CERTA recommande aux administrateurs de serveur Web de vérifier régulièrement qu'aucun fichier illégitime n'est présent dans l'arborescence de leurs sites Web. En outre, en cas d'incident sur un serveur Web, comme une défiguration par exemple, il est fortement recommandé de réinstaller le serveur compromis, après en avoir réalisé une analyse, afin de mettre en évidence les faille exploitées et pouvoir ainsi les corriger.

Documentation

– Note d'information CERTA-2012-INF-001 :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-INF-001/

2 Vulnérabilité dans Cisco ACS

Cisco a publié le 7 novembre 2012 un bulletin de sécurité (voir avis CERTA-2012-AVI-634) indiquant que son produit *Secure Access Control System* (ACS), largement employé pour gérer la politique d'accès aux équipements réseau, comporte une vulnérabilité critique.

Cette vulnérabilité permet à un attaquant de se connecter à un équipement réseau en contournant le mécanisme d'authentification. Elle est exploitable lorsque les conditions suivantes sont réunies :

- le protocole d'authentification utilisé est TACACS+ ;
- un annuaire LDAP est utilisé.

Dans ces conditions, si un attaquant a connaissance d'un nom d'utilisateur valide de l'annuaire LDAP, il peut exploiter la vulnérabilité en envoyant une séquence de caractères particulière comme mot de passe. Il héritera alors des droits de l'utilisateur dont il a usurpé le compte.

Le CERTA recommande vivement d'appliquer au plus tôt les correctifs fournis par Cisco pour résoudre ce problème.

Documentation

- Avis CERTA-2012-AVI-634 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-634/
- Avis Cisco du 7 novembre 2012 :
  http://www.cisco.com/en/US/products/csa/cisco-sa-20121107-acs.html

3 Antivirus - Risques et précautions

Dans la grande majorité des politiques de sécurité il est préconisé d'installer un système antivirus sur les différents éléments du système d'information. Cette pratique est certes importante pour assurer un niveau de sécurité homogène mais elle comporte également certains risques.

Par définition un antivirus traite des fichiers potentiellement malveillants, qui sont généralement formatés avec des bugs ou des incohérences. Ces documents sont donc analysés avant leur ouverture par un utilisateur, ce qui place les antivirus en première ligne des protections du système d'information. Le CERTA rencontre parfois des documents exploitant des vulnérabilités dans les applications antivirales qui permettent à un attaquant d'obtenir un accès à la machine ciblée sans action de l'utilisateur.

Récemment, un chercheur a découvert des vulnérabilités dans l'antivirus « Sophos », ce qui remet ce sujet sur le devant de la scène. Les failles dans les systèmes antivirus ne sont pas nouvelles, tous les grands acteurs du marché se sont retrouvés confrontés à des problématiques de sécurité similaires.

Le risque est d'autant plus grand que les antivirus sont souvent associés à un niveau de privilèges élevés sur le système (lié à la nature de leurs analyses). Le système de protection devient alors un moyen potentiel d'intrusion.

Le CERTA a rencontré plusieurs fois des virus ciblés qui infectaient le réseau des victimes au moyen des logiciels antivirus, ce qui a considérablement accéléré la reproduction des codes malveillants.

Si l'utilisation d'un système antiviral reste évidemment primordiale pour protéger un parc des logiciels malveillants génériques, ces systèmes doivent cependant être soumis à des limitations (restriction de droits, des communications réseau, etc) pour les zones les plus sensibles. Par ailleurs, une surveillance minutieuse de ces plates-formes et leurs mises à jour régulières doivent impérativement être effectuées.

4 Site Internet et contact sécurité

Le CERTA est fréquemment amené à traiter des incidents concernant des sites Internet compromis. Ces compromissions peuvent être une défiguration, des fuites d'information, la mise en place d'une campagne de *phishing* ou encore le déploiement, sur le site de la victime, de kits d'exploitation.

Dans le cadre du traitement de ces incidents, le CERTA doit pouvoir rapidement prendre contact avec la personne responsable du site. Il n'est cependant pas toujours évident de trouver ce type de contact sur les sites Internet.

Le CERTA recommande donc la mise en place d'informations de contacts techniques facilement identifiables sur les sites Internet, ainsi que la mise à jour régulière des informations d'*abuse* (adresse email de contact visibles lorsqu'on liste les informations d'enregistrement relatives à un nom de domaine) des sites administrés.

5 Rappel des avis émis

Dans la période du 02 au 08 novembre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-614 : Vulnérabilité dans Cisco Prime Data Center Network Manager
- CERTA-2012-AVI-615 : Multiples vulnérabilités dans Cisco Unified MeetingPlace Web Conferencing
- CERTA-2012-AVI-616 : Vulnérabilité dans Avaya Aura Session Manager
- CERTA-2012-AVI-617 : Multiples vulnérabilités dans Hitachi JP1
- CERTA-2012-AVI-618 : Multiples vulnérabilités dans Apple iOS
- CERTA-2012-AVI-619 : Multiples vulnérabilités dans Apple Safari
- CERTA-2012-AVI-620 : Multiples vulnérabilités dans HP Performance Insight
- CERTA-2012-AVI-621 : Vulnérabilité dans libtiff
- CERTA-2012-AVI-622 : Vulnérabilité dans IBM Rational
- CERTA-2012-AVI-623 : Vulnérabilité dans IBM WebSphere DataPower
- CERTA-2012-AVI-624 : Multiples vulnérabilités dans IBM Tivoli Federated Identity Manager
- CERTA-2012-AVI-625 : Vulnérabilité dans Webmin
- CERTA-2012-AVI-626 : Vulnérabilité dans vBulletin
- CERTA-2012-AVI-627 : Multiples vulnérabilités dans Sophos
- CERTA-2012-AVI-629 : Multiples vulnérabilités dans Apache Tomcat
- CERTA-2012-AVI-630 : Multiples vulnérabilités dans Opera
- CERTA-2012-AVI-631 : Multiples vulnérabilités dans Google Chrome
- CERTA-2012-AVI-632 : Vulnérabilité dans le système SCADA Siemens SiPass Server
- CERTA-2012-AVI-633 : Vulnérabilité dans KVM
- CERTA-2012-AVI-634 : Vulnérabilité dans Cisco Secure Access Control System

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2012-AVI-628-001 : Multiples vulnérabilités dans Adobe Flash Player (ajout de la mise à jour Microsoft)

Gestion détaillée du document

09 novembre 2012 version initiale.