



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 01 septembre 2006  
N° CERTA-2006-ACT-035

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2006-35**

---

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-2006-ACT-035>

---

### Gestion du document

Référence	CERTA-2006-ACT-035
Titre	Bulletin d'actualité 2006-35
Date de la première version	01 septembre 2006
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.

## 1 Activité en cours

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-2006-ACT-035.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-2006-ACT-035/>

### 1.1 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 24 et le 31 août 2006.

## 2 Incidents traités

### 2.1 Défigurations

Le CERTA a traité cette semaine deux cas de défiguration de site web. Dans les deux cas, les auteurs des faits ont profité de droits en écriture laissés accidentellement par l'administrateur. Pour l'une de ces défigurations, l'analyse des journaux a permis de montrer que de nombreuses attaques avaient eu lieu sur plusieurs jours en exploitant toujours la même vulnérabilité. Des fichiers ont été déposés sur le site vulnérable.

Des droits en écriture sont parfois laissés afin de faciliter les mises à jour des contenus des sites web. Il est important dans ce cas de restreindre les adresses IPs accédant à cette fonctionnalité, ou déployer des procédures d'authentification.

## 2.2 Ver ciblant MS06-040

Le CERTA a été informé de la compromission de nombreuses machines en France. Au total, 26000 adresses IPs distinctes ont été identifiées (en tenant compte de l'adressage dynamique, ce chiffre représente probablement moins de machines physiques infectées).

Le ver à l'origine de ces compromissions avait été signalé dans le bulletin d'actualité CERTA-2006-ACT-033. Il porte différents noms : Graweg, MocBot, W32.Wargbot, W32/SDbot, W32/Vanebot, W32.Randex. Deux enregistrements dans la base CME (*Common Malware Enumeration* : <http://cme.mitre.org>) lui sont dédiés : CME-762 et CME-482.

Plusieurs variantes de celui-ci sont identifiées, dont le comportement consiste à établir des connexions vers des serveurs à l'étranger sur le port 18067/TCP ou 4915/TCP.

## Recommandations

Le CERTA recommande d'appliquer les correctifs de sécurité mis à disposition par Microsoft dans le bulletin MS06-040 (CERTA-2006-AVI-338). D'autre part, le CERTA suggère de surveiller dans les journaux des pare-feux d'éventuelles connexions vers les ports 18067/TCP et 4915/TCP.

## 3 Liens utiles

- Mémento sur les virus :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information sur l'acquisition de correctifs :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html>
- Note d'information sur les systèmes obsolètes :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html>
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html>
- Note d'information sur les mots de passe :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html>
- Note d'information sur la terminologie d'usage au CERTA :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :  
<http://www.auscert.org.au/render.html?it=1935>

## 4 Rappel des avis et mises à jour émis

Durant la période du 25 au 31 août 2006, le CERTA a émis l'alerte suivante :

- CERTA-2006-ALE-011 : Multiples vulnérabilités de produits Microsoft

Pendant la même période, le CERTA a publié les avis suivants :

- CERTA-2006-AVI-372 : Vulnérabilité dans Xsan Filesystem
- CERTA-2006-AVI-373 : Multiples vulnérabilités dans Wireshark (Ethereal)
- CERTA-2006-AVI-374 : Vulnérabilités dans VAIIO Media Server
- CERTA-2006-AVI-375 : Multiples vulnérabilités dans Joomla!
- CERTA-2006-AVI-376 : Vulnérabilité dans isakmpd sous OpenBSD
- CERTA-2006-AVI-377 : Vulnérabilité dans XOrg X11 et des bibliothèques associées
- CERTA-2006-AVI-378 : Vulnérabilité dans Sendmail
- CERTA-2006-AVI-379 : Vulnérabilité dans solaris
- CERTA-2006-AVI-380 : Multiples vulnérabilités des Imprimantes Dell
- CERTA-2006-AVI-381 : Multiples vulnérabilités dans le noyau Linux

Pendant cette même période, les mises à jour suivantes ont été publiées :

- CERTA-2006-AVI-340-001 : Multiples vulnérabilités dans Internet Explorer (modification liée à la seconde version du correctif)

## **5 Actions suggérées**

### **5.1 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.

### **5.2 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 œuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

### **5.3 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.

### **5.4 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.

### **5.5 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 COSSI/CERTA peut vous aider dans ce travail d'analyse.

### **5.6 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.

## 5.7 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.formation.ssi.gouv.fr>

## 6 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.

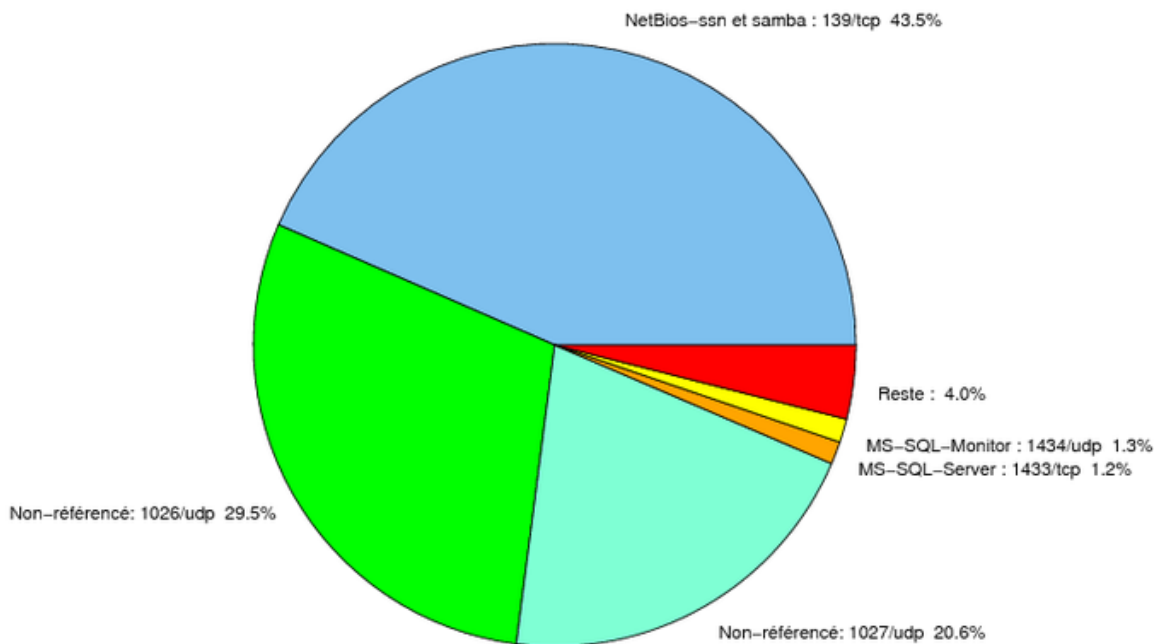


FIG. 1: Répartition relative des ports pour la semaine du 24.08.2006 au 31.08.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
22	TCP	SSH	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
23	TCP	Telnet	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
25	TCP	SMTP	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
42	TCP	WINS	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
80	TCP	HTTP	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
119	TCP	NNTP	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
135	TCP	Microsoft RPC	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
137	UDP	NetBios-ns	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
139	TCP	NetBios-ssn et samba	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
143	TCP	IMAP	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
389	TCP	LDAP	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
443	TCP	HTTPS	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
445	TCP	Microsoft-smb	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
1433	TCP	MS-SQL-Server	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
1434	UDP	MS-SQL-Monitor	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
2100	TCP	Oracle XDB FTP	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>

2381	TCP	–	HP System Management	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
2745	TCP	–	Bagle	–
2967	TCP	–	Symantec Antivirus	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
6101	TCP	Veritas Backup Exec	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
6112	TCP	Dtspcd	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
6129	TCP	Dameware Miniremote	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a> <a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>
18264	TCP	CheckPoint interface	–	<a href="http://www.certa.ssi.gouv.fr/site/CE">http://www.certa.ssi.gouv.fr/site/CE</a>

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

port	pourcentage
139/tcp	43.46
1026/udp	29.49
1027/udp	20.59
1434/udp	1.26
1433/tcp	1.21
137/udp	0.9
4899/tcp	0.86
1080/tcp	0.78
22/tcp	0.38
3128/tcp	0.3
80/tcp	0.17
25/tcp	0.15
443/tcp	0.05
143/tcp	0.03
15118/tcp	0.01

TAB. 3: Paquets rejetés

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	6
3	Paquets rejetés . . . . .	7

## Gestion détaillée du document

01 septembre 2006 version initiale.