Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 juin 2005
N° CERTA-2005-ACT-024

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité n° 2005-24

Gestion du document

Référence	CERTA-2005-ACT-024
Titre	Bulletin d'actualité n° 2005-24
Date de la première version	17 juin 2005
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

1.1 Ports observés

Le tableau 3 ainsi que la figure 2 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 02 et le 09 juin 2005.

1.2 Augmentation des rejets sur les ports 139/tcp et 80/tcp

Le CERTA constate, depuis le 01 juin 2005, une augmentation des rejets sur les ports 80/tcp et 139/tcp (voir figure 1). En effet, de nombreuses machines sous Windows semblent être à la recherche de ces deux ports.

Le CERTA n'est pas encore en mesure d'expliquer ce qui peut être à l'origine de cette activité.

1.3 Activité sur le port 143/tcp

Cette activité, bien que très faible, correspond à une recherche des serveurs IMAP. Nous rappelons que de nombreuses vulnérabilités récemment publiées affectent le serveur IMAP du produit `Ipswitch Imail` (avis CERTA-2005-AVI-185). Des outils exploitant automatiquement ces vulnérabilités sont disponibles sur l'Internet.

Recommandation :
Il est extrêmement important d'appliquer les correctifs indiqués dans l'avis du CERTA dans les plus brefs délais, et de vérifier l'intégrité des serveurs qui n'ont pas encore été mis à jour.

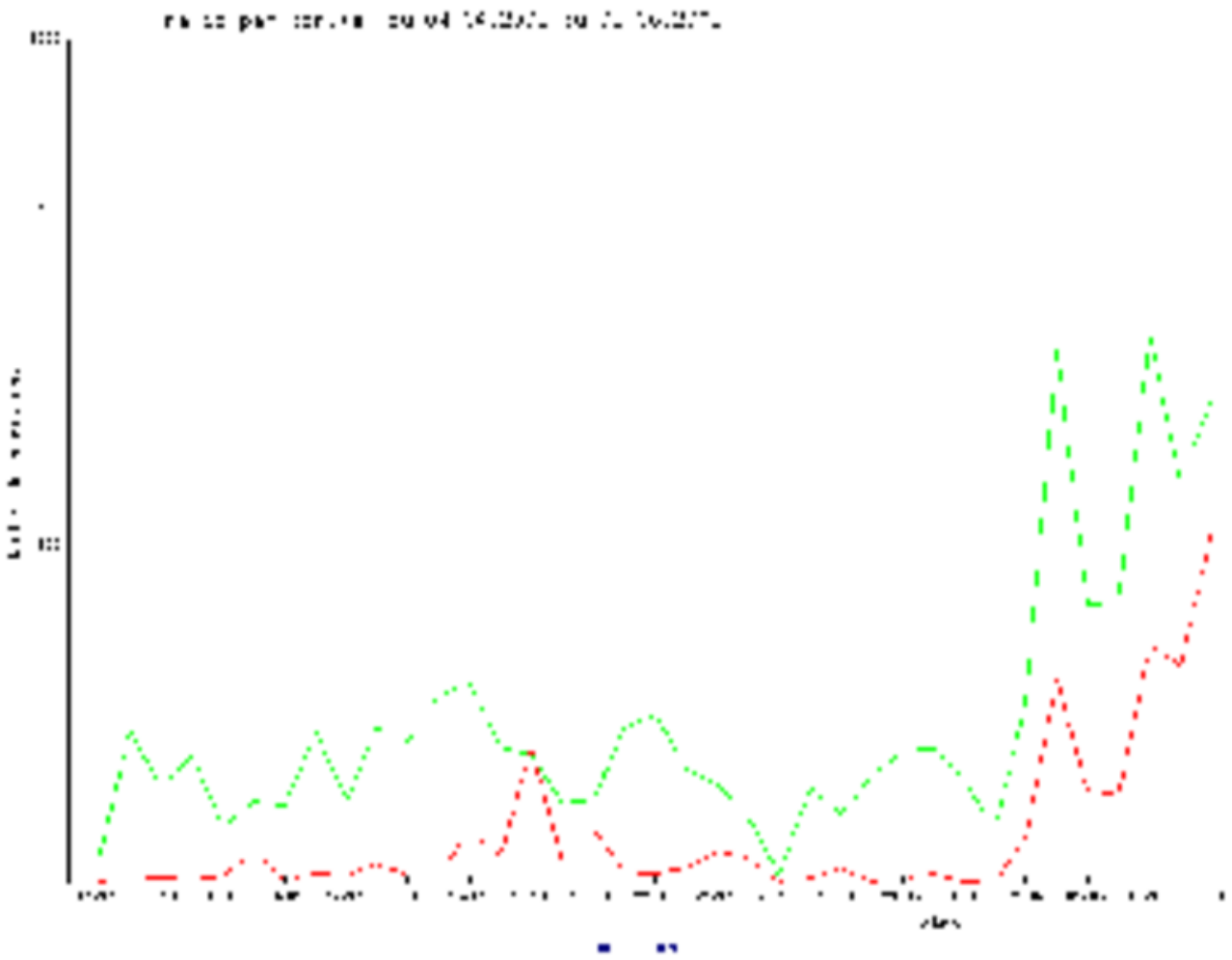

FIG. 1 – *Evolution des rejets sur les ports 80/tcp et 139/tcp*

2 Correctifs de Microsoft

Microsoft a publié cette semaine 10 correctifs de sécurité (avis CERTA-2005-AVI-210 à CERTA-2005-AVI-219). Certains de ces correctifs sont particulièrement critiques, puisqu'ils concernent des applications très répandues comme Internet Explorer et Outlook Express. A noter que selon la société `Eeye`, il existe encore au moins 3 vulnérabilités non corrigées dans ces produits permettant l'exécution de code arbitraire à distance.

Un des correctifs concerne le service SMB de Windows (qui utilise les ports 139/tcp et 445/tcp). Il est possible qu'un ver exploitant cette vulnérabilité soit prochainement publié, des tentatives de réaliser du `reverse engineering` de ce correctif ayant déjà eu lieu.

Recommandation :

Comme toujours, il est très fortement conseillé d'appliquer ces correctifs même sur des machines situées derrière un pare-feu.

3 Rappel des avis et mises à jour émis

Durant la période du 06 au 10 juin 2005, le CERTA a émis les avis suivants :

- CERTA-2005-AVI-192 : Vulnérabilité de Net-SNMP
- CERTA-2005-AVI-193 : Vulnérabilité du pare-feu Microsoft ISA Server 2000
- CERTA-2005-AVI-194 : Vulnérabilité de Solaris
- CERTA-2005-AVI-195 : Vulnérabilité de libtiff
- CERTA-2005-AVI-196 : Vulnérabilité de type injection SQL dans Mailutils
- CERTA-2005-AVI-197 : Vulnérabilité de Sun ONE Application Server
- CERTA-2005-AVI-198 : Vulnérabilité d'IBM Websphere Application Server
- CERTA-2005-AVI-199 : Vulnérabilités de rpc.mountd sous SGI IRIX
- CERTA-2005-AVI-200 : Multiples vulnérabilités sous Mac OS X
- CERTA-2005-AVI-201 : Multiples vulnérabilités sur BEA Weblogic

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

- CERTA-2005-AVI-186-001 : Multiples vulnérabilités dans Mailutils
  (ajout référence au bulletin de sécurité Debian)
- CERTA-2005-AVI-038-006 : Multiples vulnérabilités dans SquirrelMail
  (ajout de la référence au bulletin de sécurité SUSE)
- CERTA-2005-AVI-170-002 : Vulnérabilité dans FreeRADIUS
  (ajout du bulletin SUSE SUSE-SR:2005:014. Ajout référence CVE)
- CERTA-2005-AVI-178-001 : Multiples vulnérabilités d'Ethereal
  (ajout référence au bulletin de sécurité SUSE)
- CERTA-2005-AVI-180-001 : Vulnérabilités dans Qpopper
  (ajout référence au bulletin de sécurité SUSE)
- CERTA-2004-AVI-308-001 : Vulnérabilité dans OpenSSH
  (ajout références aux bulletins RHSA-2005-106 et RHSA-2005-165 de Red Hat)
- CERTA-2005-AVI-104-009 : Vulnérabilité de libXpm
  (ajout référence au bulletin de sécurité Red Hat (RHSA-2005:198) relatif à xorg-x11)
- CERTA-2004-AVI-189-002 : Vulnérabilité de Mailman
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-033-002 : Vulnérabilité des serveurs DNS BIND
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-038-007 : Multiples vulnérabilités dans SquirrelMail
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-042-005 : Multiples vulnérabilités dans Squid
  (ajout d'un bulletin de sécurité FreeBSD et modification des références FreeBSD)
- CERTA-2005-AVI-048-002 : Vulnérabilité dans UW-Imapd
  (ajout de la référence au bulletin de sécurité FreeBSD)

- CERTA-2005-AVI-078-002 : Vulnérabilité de l'application sympa
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-084-006 : Vulnérabilité dans Squid
  (ajout de la référence au bulletin de sécurité FreeBSD)
- CERTA-2005-AVI-097-002 : Vulnérabilité dans UW-imapd
  (ajout des références aux bulletins de sécurité Gentoo, Mandrake, Red Hat, FreeBSD)
- CERTA-2005-AVI-114-003 : Multiples vulnérabilités de xli
  (ajout des références aux bulletins de sécurité FreeBSD)
- CERTA-2005-AVI-164-001 : Multiples vulnérabilités dans tcpdump
  (ajout référence au bulletin de sécurité FreeBSD)

4 Actions suggérées

4.1 Respecter la politique de sécurité

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.

4.2 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.

4.3 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.

4.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiat. 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.

4.5 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.

4.6 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 inexpliqués 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 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.

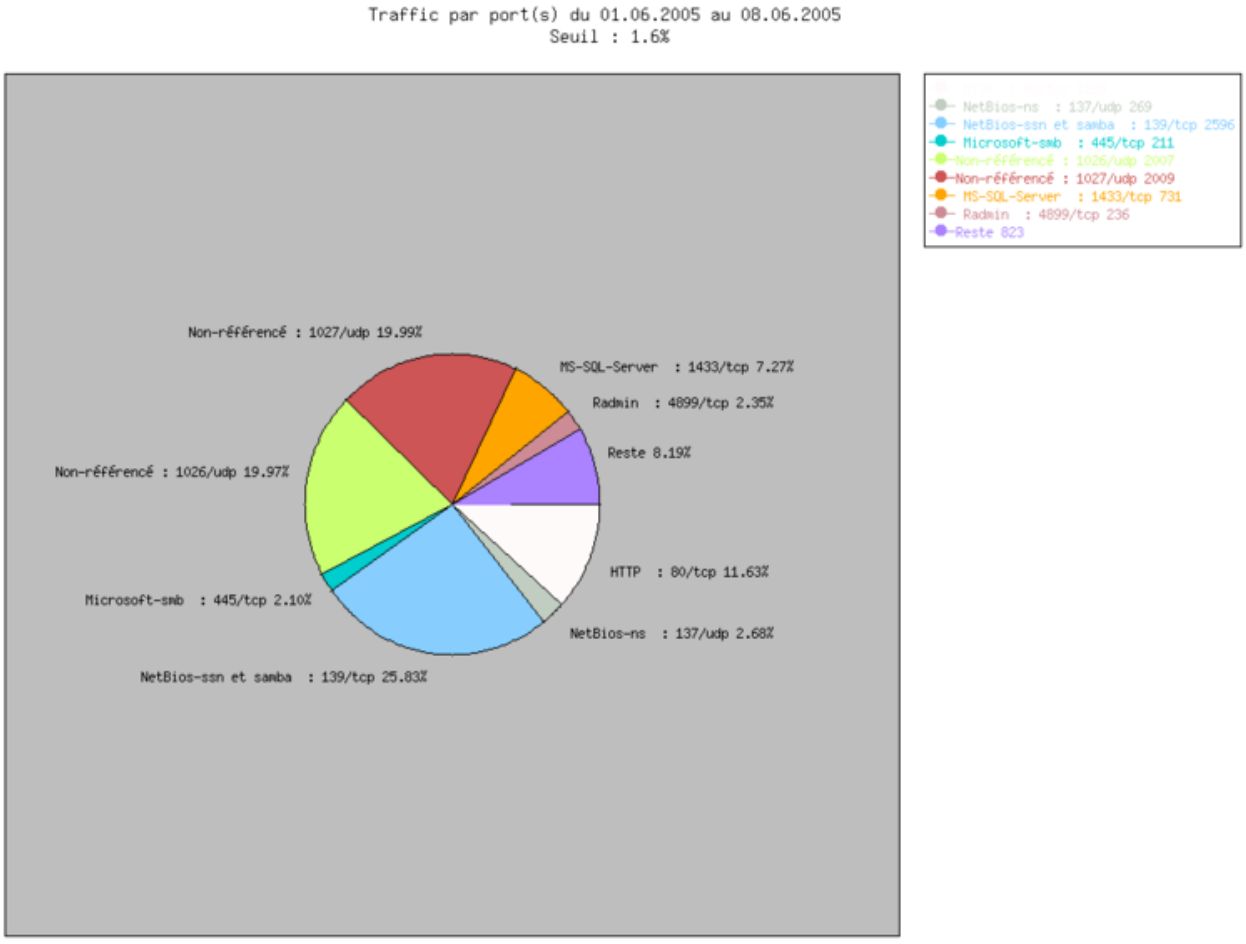

FIG. 2 – *Repartition relative des ports*

Liste des tableaux

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-20 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-13
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-13
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-38
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-19 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-23
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-05
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-ALE-00 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-11 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-03
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-36 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-16 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-21
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-18
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-04 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-00 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-15 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-24 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-05 http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-10 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-12 http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-05
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	–
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-00
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-15
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-ALE-00
2745	TCP	–	Bagle	–
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-06 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-18 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-31 http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-34
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-AVI-21
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-16
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-02
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CERTA-2002-ALE-00
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-21
8866	TCP	–	Porte dérobée Bagle.B	CERTA-2004-COM-001
9898	TCP	–	Porte dérobée Dabber	–
10080	TCP	Amanda	MyDoom	–
11768	TCP	–	Netdepix	–
15118	TCP	–	Netdepix	–

TAB. 2 – *Correctifs correspondant aux ports destination des paquets rejetés*

port	pourcentage
1026/udp	25,58
139/tcp	24,56
1027/udp	18,62
80/tcp	10,85
1433/tcp	7,21
137/udp	3,43
4899/tcp	2,32
445/tcp	1,83
1434/udp	1,33
15118/tcp	0,77
9898/tcp	0,40
2745/tcp	0,40
5554/tcp	0,31
1080/tcp	0,30
22/tcp	0,29
25/tcp	0,24
3306/tcp	0,18
3127/tcp	0,17
21/tcp	0,17
6101/tcp	0,16
6129/tcp	0,12
23/tcp	0,11
2100/tcp	0,11
42/tcp	0,10
11768/tcp	0,09
5000/tcp	0,08
111/tcp	0,07
143/tcp	0,06
1023/tcp	0,05
443/tcp	0,05
3389/tcp	0,03
135/tcp	0,02

TAB. 3 – *Paquets rejetés*

Gestion détaillée du document

17 juin 2005 version initiale.