



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 décembre 2009
N° CERTA-2009-ACT-053

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2009-53

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-053>

Gestion du document

Référence	CERTA-2009-ACT-053
Titre	Bulletin d'actualité 2009-53
Date de la première version	31 décembre 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-053.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-053/>

1 Bonne année

L'année 2009 s'achève, c'est le moment des bilans et des bonnes résolutions.

Encore une fois, cette année a été riche en événements, avec comme point d'orgue la propagation de différentes versions de vers exploitant la vulnérabilité MS08-067 (Conficker, Kido, ...). Ces événements nous ont prouvé, s'il en était encore besoin, que les procédures les plus simples (contrôle du SI, mises à jour, etc.) restent la base de la sécurisation des systèmes. Sans cette brique essentielle, tout le reste ne sera que château de sable et s'écroulera au premier problème venu.

L'année 2009 aura également été marquée par une forte augmentation des alertes. Le CERTA rappelle que de nombreuses vulnérabilités sont toujours non corrigées comme dans Adobe Reader, Adobe Acrobat et Thunderbird 2. La plus grande prudence est donc recommandée lors de l'ouverture de certains courriels ou documents PDF, par exemple les cartes de vœux.

D'un côté plus organisationnel, 2009 a vu la naissance de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), dont le CERTA fait partie, preuve s'il en est que la sécurité informatique est au cœur des préoccupations de l'État.

Le bulletin d'actualité est pour le CERTA, le moyen de partager sa vision et son expérience en matière de traitement d'incident. Tout retour sur cette production est toujours bénéfique. N'hésitez donc pas à nous faire part de vos remarques.

Il ne nous reste désormais plus qu'à vous souhaiter une bonne fin d'année 2009 et à vous donner rendez-vous l'année prochaine pour continuer ensemble l'effort global de sécurisation de nos systèmes d'information.

Très bonne année à toutes et à tous !

2 Incidents de la semaine

Danger des scripts de gestion de fichiers

Certains webmasters ont recours à des scripts, généralement écrits en PHP, pour assurer la gestion des fichiers sur le serveur. Leur rôle consiste à permettre le dépôt de fichiers (*upload*) ou le téléchargement (*download*). Malheureusement, ils ne sont pas toujours bien écrits ou ne s'adaptent pas toujours à la politique de sécurité du système d'information.

En l'espace d'une semaine, le CERTA a traité plusieurs incidents relatifs à de tels scripts :

- une porte dérobée a été déposée dans un répertoire de stockage de fichiers temporaires puis utilisée pour la mise en place d'un site de *phishing*;
- un scénario similaire a mené à la défiguration d'un site Web ;
- plusieurs fichiers de téléchargement ont été utilisés par des attaquants pour récupérer des fichiers de configuration de serveur Web. L'un de ces fichiers contenait des identifiants de connexion à une base de données.

Le recours à de tels scripts doit avant tout s'inscrire dans la politique de sécurité. Il est nécessaire d'identifier au préalable les fichiers susceptibles d'être manipulés et de restreindre l'utilisation des scripts à ces fichiers. D'autre part, une attention toute particulière doit être apportée à l'écriture de ces programmes. Il est possible qu'ils fassent appel à des fonctions dangereuses qui peuvent être détournées pour réaliser diverses attaques. Enfin, le fait qu'il s'agisse souvent d'un développement « maison » ne préserve pas des attaques, puisqu'ils sont assez facilement trouvés à l'aide d'un moteur de recherche.

3 Un cadeau de Noël pour Microsoft IIS

La semaine dernière, de nombreux articles ont été publiés concernant une vulnérabilité non corrigée dans Microsoft IIS 6.

Microsoft, par l'intermédiaire de son centre de sécurité, a répondu qu'il ne s'agissait pas d'une vulnérabilité. Même si une faiblesse existe dans le traitement du caractère « ; » dans une *URL* par le serveur web de Microsoft, celle-ci ne peut être exploitée que sur un serveur mal configuré.

En effet, il est nécessaire pour une personne malveillante voulant profiter de cette faiblesse d'avoir les droits en écriture et en exécution sur le répertoire dans lequel un fichier malveillant aurait été déposé. Cette configuration, qui n'est pas celle par défaut, n'est pas en accord avec les bonnes pratiques de configuration d'un serveur Web.

Le CERTA recommande donc aux utilisateurs de Microsoft IIS de prendre connaissance et d'appliquer les bonnes préconisations de Microsoft disponibles ci-après.

Documentation

- La réponse de Microsoft :
<http://blogs.technet.com/msrc/archive/2009/12/29/result-of-investigation-into-holiday-iis-claim.aspx>
- Les bonnes pratiques de sécurité pour Microsoft IIS 6 :
[http://technet.microsoft.com/fr-fr/library/cc782762\(W.S.10\).aspx](http://technet.microsoft.com/fr-fr/library/cc782762(W.S.10).aspx)

4 D'où vient mon plug-in ?

D'une manière générale, le CERTA recommande de ne pas installer de greffons supplémentaires, et ceci pour plusieurs raisons : confiance dans l'éditeur, manque de lisibilité, ajout de vulnérabilités supplémentaires, etc. Cependant, force est de constater que dans certains cas, l'ajout de greffons supplémentaires à un navigateur apporte un plus tant en termes de fonctionnalité qu'en termes de sécurité.

Lorsque l'on installe un de ces greffons ou une mise à jour de ces greffons, plusieurs choix s'offrent à nous :

- le bon choix : se rendre sur la page de l'éditeur et rechercher directement le greffon souhaité ;

- le mauvais choix : installer le greffon directement depuis un site tiers (avec tous les risques que cela comporte) ;
- le choix médian : cliquer sur le lien d'un site tiers nous proposant de télécharger et d'installer le greffon depuis le site de l'éditeur.

A priori, ce dernier choix semble sûr : une fois rendu sur le site de l'éditeur, l'utilisateur peut vérifier qu'il est bien sur un site légitime, éventuellement en HTTPS avec un certificat valide. Malheureusement, ce n'est pas si simple. En effet, il est aisé pour un site malveillant de construire un lien qui aura deux actions conjointes : afficher la page valide de l'éditeur et proposer le téléchargement d'un greffon provenant d'un site tiers malveillant (cf. Capture d'écran). Même si dans le cas de Firefox (dans cet exemple), le nom du site malveillant s'affiche, rien n'empêche l'attaquant de construire un nom de domaine approchant ou trompeur. Il est alors très difficile pour l'utilisateur de se rendre compte qu'il est en train de télécharger et d'installer un greffon malveillant. À noter que ceci est vrai pour tous les navigateurs permettant l'ajout d'extensions.



FIG. 1: Exemple de téléchargement d'un greffon malveillant

Le seul bon choix reste donc le premier. Le CERTA vous encourage donc, dans le cas où vous auriez besoin d'installer un greffon supplémentaire, à faire la recherche de ce greffon sur un site de confiance (l'éditeur dans la plupart des cas).

5 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=1937>
- 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/>

6 Rappel des avis émis

Dans la période du 25 au 31 décembre 2009, le CERTA a émis les avis suivants :

- CERTA-2009-AVI-562 : Vulnérabilité dans Sendmail
- CERTA-2009-AVI-561 : Multiples vulnérabilités dans Directory Server Enterprise Edition

Pendant la même période, les avis suivants ont été mis à jour :

- CERTA-2009-AVI-549-001 : Multiples vulnérabilités dans Drupal (ajout des références CVE)
- CERTA-2009-AVI-552-001 : Vulnérabilité dans des produits Horde (ajout des références CVE)
- CERTA-2009-AVI-554-001 : Multiples vulnérabilités dans Wireshark (ajout des références CVE et de la référence au bulletin de sécurité Fedora)
- CERTA-2009-AVI-556-001 : Multiples vulnérabilités dans IBM AIX (ajout des références CVE)
- CERTA-2009-AVI-557-001 : Vulnérabilités dans OSSIM (ajout des références CVE)

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique63.html

8 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.

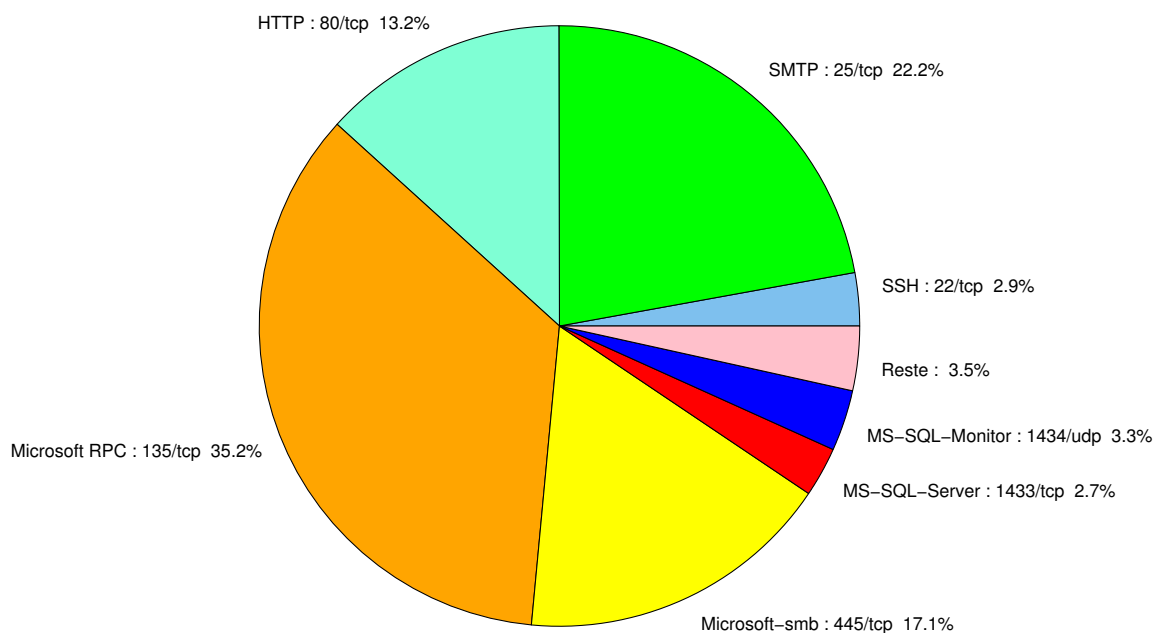


FIG. 2: Répartition relative des ports pour la semaine du 25 au 31 décembre 2009

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	–	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	–	– CERTA-2007-AVI-008
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368 CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213

				CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321
143	TCP	IMAP	-	CERTA-2005-AVI-185
389	TCP	LDAP	-	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 CERTA-2007-AVI-294
427	TCP	Novell Client	-	CERTA-2006-AVI-538
443	TCP	HTTPS	-	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
445	TCP	Microsoft-smb	-	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	-	CERTA-2007-ALE-010
1023	TCP	-	Serveur ftp de Sasser.E	-
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	-	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	-	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	-	CERTA-2005-ALE-002
2381	TCP	HP System Management	-	CERTA-2006-AVI-248
2512	TCP	Citrix MetaFrame	-	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	-	CERTA-2006-AVI-491
2745	TCP	-	Bagle	-
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	-	CERTA-2007-AVI-331
3127	TCP	-	MyDoom	-
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	-	CERTA-2007-AVI-294
3306	TCP	MySQL	-	-
4899	TCP	Radmin	-	-
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	-	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	-	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	-
5900	TCP	VNC	-	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	-	CERTA-2007-AVI-183
6070	TCP	BrightStor ARCserve/Enterprise Backup	-	CERTA-2005-AVI-293

6101	TCP	Veritas Backup Exec	-	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	-	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	-	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	-	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	-	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	-	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	-	CERTA-2007-AVI-153
8866	TCP	-	Porte dérobée Bagle.B	-
9898	TCP	-	Porte dérobée Dabber	-
10000	TCP	Webmin, Veritas Backup Exec	-	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	-
10110	TCP	IBM Tivoli Monitoring	-	CERTA-2007-AVI-183
10916	TCP	Ingres	-	CERTA-2007-AVI-275-001
10925	TCP	Ingres	-	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	-	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	-	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	-	CERTA-2005-AVI-310
54345	TCP	HP Mercury	-	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	-	CERTA-2007-AVI-176

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
135/tcp	35.23
80/tcp	34.02
25/tcp	22.17
445/tcp	17.07
22/tcp	4.43
1434/udp	3.28
1433/tcp	2.67
23/tcp	0.72
2967/tcp	0.6
1080/tcp	0.54
4899/tcp	0.48
3128/tcp	0.42
3389/tcp	0.3
3306/tcp	0.06

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

31 décembre 2009 version initiale.