

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-06

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-2007-ACT-006>

Gestion du document

Référence	CERTA-2007-ACT-006
Titre	Bulletin d'actualité 2007-06
Date de la première version	09 février 2007
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-2007-ACT-006.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-2007-ACT-006/>

1 Activités en cours

1.1 Compromission par filoutage

Les bonnes pratiques en cas de compromission par filoutage de votre site Internet :

Cette semaine le CERTA a été informé de nombreux cas de filoutage (ou *phishing*). Une machine compromise héberge, à l'insu de son propriétaire, la copie des pages Web d'un site légitime. Des victimes potentielles sont ensuite incitées à se rediriger vers cette machine (par courrier électronique par exemple) pour leur dérober des informations personnelles.

Le CERTA peut être amené à contacter le propriétaire de la machine qui héberge les pages malveillantes, afin de l'informer du problème.

À de trop nombreuses reprises, la réponse trouvée est la suppression des fichiers douteux, soit directement, soit par le biais de l'hébergeur du site.

Le CERTA rappelle que, dans le cas d'une compromission, les fichiers présents sur le serveur Web sont des traces qui pourront être exigés par les autorités judiciaires dans le cas d'une plainte déposée par les responsables du site légitime qui a été copié.

Il est donc fortement recommandé de contacter son hébergeur afin de l'informer de la compromission du site Internet et de lui demander de prendre les mesures nécessaires à la préservation des données. La note d'information du CERTA (CERTA-2002-INF-002) sur les bons réflexes en cas d'intrusion peut vous aider dans vos démarches.

Documentation

<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002>

<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005>

1.2 Les changements de statuts, ou noms

Le CERTA a traité cette semaine la compromission d'un site Web. La cause en était la suivante : l'organisme détenteur a changé de nom et de statut. L'ancien site pointait donc vers le nouveau, hébergé sur une autre machine. Dans le même temps, la maintenance de la machine accueillant l'ancien site a été arrêtée. En d'autres termes, cette machine présente toutes les conditions favorables à une compromission, d'autant plus que celle-ci peut être abandonnée de la sorte pendant plusieurs mois, voire quelques années.

Dans ces conditions, il est important de prendre les précautions suivantes :

- fixer une période pendant laquelle l'ancienne machine doit rester active ;
- identifier une personne responsable de sa maintenance ;
- limiter les services sur la machine à de simples pages Web redirigeant vers le nouveau site. Dans le cas de l'incident traité, la machine continuait à héberger un forum inactif par exemple. Celui-ci n'est pas indispensable, mais accroît les risques de compromission ;
- modifier éventuellement le DNS pour faire pointer vers le nouveau site.

Très souvent, une simple page statique en HTML avec une redirection vers le nouveau site reste bien suffisante. Elle permet de limiter les installations et la maintenance de la machine (pas besoin d'installer PHP, la configuration du serveur Web peut être minimale, etc.).

Le CERTA invite les personnes ayant connaissance de tels sites à vérifier que ceux-ci répondent bien aux points mentionnés ci-dessus.

1.2.1 Recommandations concernant les sites orphelins

La situation précédente peut être vue comme un cas particulier de site orphelin.

De manière générale, comme il a été mentionné dans un précédent bulletin (CERTA-2006-ACT-052), les recommandations concernant les sites orphelins sont les suivantes :

- maintenir la liste des responsables des sites, techniques (exploitation, administration, développement) et éditoriaux ;
- assurer la redondance des personnes et les relais ;
- documenter et maintenir le développement et les configurations ;
- réviser périodiquement la configuration pour l'adapter aux utilisations et à la menace.

1.3 La gestion de l'affichage des messages d'erreur

Le CERTA a traité cette semaines deux cas d'incidents sur des serveurs Web. Ceux-ci présentaient aux personnes naviguant sur le site des messages d'erreurs, notamment PHP.

Les messages d'erreurs affichés sont dangereux, car ils fournissent beaucoup d'informations à une personne malveillante qui chercherait à s'introduire par le biais du site. Cela peut inclure les versions des applications ou bibliothèques, les fonctions mises en œuvre dans le code, la structure de la base de données contactée par le site, etc.

Il est donc fortement recommandé de vérifier que la configuration du site ne permet pas de tels affichages. Cela ne doit évidemment pas remplacer une surveillance fréquente des journaux.

A valeur d'illustration, il est possible dans le fichier de configuration `php.ini` (pour les versions supérieures à 4.0.3) de spécifier la variable suivante : `display_errors` (affichage des erreurs). Celle-ci est par défaut à "1", mais doit être positionnée à "0" quand le site devient opérationnel.

1.4 Cas d'un déni de service

Le CERTA a récemment traité un cas de déni de service qui a consommé toutes les ressources mémoire d'un routeur, suite à l'envoi massif de paquets TCP à destination d'une machine d'un réseau local.

On peut distinguer deux catégories de machines ciblées par les dénis de service :

- les machines offrant un service sur l'Internet, par exemple les serveurs web ;
- les machines déjà compromises utilisées à des fins malveillantes, par exemple des postes client sur lesquels tourne un bot irc et pouvant subir une contre-mesure dangereuse.

Lorsqu'un tel déni de service est constaté, il est suggéré d'isoler la machine ciblée et de procéder à son analyse pour vérifier si celle-ci est compromise. Le filtrage en sortie et l'examen du trafic réseau précédant l'attaque aident grandement pour vérifier la compromission de la cible du déni de service.

Dans le cas traité par le CERTA, aucun filtrage en sortie n'était mis en place et la machine ciblée a été réinstallée avant d'être examinée, ce qui ne permet pas d'analyser correctement l'incident.

1.4.1 Recommandations

- filtrer correctement le trafic sortant suivant une politique restrictive par défaut. Il est vivement déconseillé de laisser par défaut tous les paquets provenant de machines internes sortir vers l'Internet ;
- journaliser le trafic sortant, afin de constater les tentatives internes anormales de connexion vers l'extérieur : celles-ci peuvent indiquer la compromission de l'une des machines du réseau ;
- débrancher la machine suspecte du réseau, pour bloquer ses agressions avec l'extérieur et préserver les traces ;
- contacter son responsable de sécurité ou le CERTA.

2 La Saint-Valentin approche

La Saint-Valentin approche. Gare aux amoureux des... courriers électroniques malveillants ! Les courriels qui contiennent des fichiers malveillants, ou qui redirigent vers des sites malveillants (filoutage) doivent motiver les personnes à ouvrir la pièce jointe, ou cliquer sur un lien. Ils profitent donc généralement des thèmes de l'actualité, et de la sensibilité des personnes.

La fête de la Saint-Valentin se prête donc parfaitement à ce genre d'activité. Le CERTA recommande la plus grande prudence vis-à-vis des courriers électroniques reçus sur le sujet.

Ils peuvent être un vecteur de propagation de virus, chevaux de Troie, ou autres contenus malveillants. Il est donc nécessaire de maintenir la vigilance et de sensibiliser les utilisateurs. La note CERTA-2000-REC-002 rappelle quelques précautions à prendre lors de la réception de tels messages.

3 Bluetooth et le mode "découverte"

De plus en plus d'équipements, tels que les téléphones portables, les assistants personnels numériques et les ordinateurs (clavier, souris, haut-parleurs), sont équipés d'une interface *Bluetooth* afin d'interconnecter facilement et sans fil des appareils hétérogènes. La majorité des équipements dotés d'une connexion *Bluetooth* offrent une option appelée mode "découverte" qui permet de dissimuler ou non sa présence aux autres dispositifs *Bluetooth* à portée. Le fait de désactiver le mode découverte permet de se prémunir d'attaques opportunistes ou non ciblées, cependant cette action ne permet pas de se protéger contre un attaquant plus motivé. En voici les raisons :

Chaque interface *Bluetooth* dispose d'une adresse physique, ces adresses sont distribuées par plages aux industriels qui eux-même affectent des sous plages d'adresses à leurs différents équipements. Ainsi, un utilisateur malintentionné peut réaliser une attaque de type force brute et découvrir un appareil Bluetooth avec le mode découverte désactivé. Ce dernier répondra malgré tout à une requête lui étant explicitement adressée. Par conséquent, le fait de désactiver physiquement l'interface *Bluetooth* permet de se protéger des attaques déjà existantes et ciblant ces dispositifs.

De manière générale, l'interface de ces appareils communicants ne doit être sollicitée que ponctuellement, et elle doit rester par défaut éteinte.

4 Problèmes liés aux protections contre le filoutage et contre les fenêtres intempestives

4.1 Protection contre le filoutage

Un problème concernant la protection contre le filoutage a été identifié sur toutes les versions de Firefox le supportant, y compris la version actuelle (2.0.0.1), ainsi que sur Opera 9.10. En effet, ces navigateurs ne reconnaissent pas des adresses répertoriées comme étant des sites de filoutage si des caractères « / » supplémentaires sont insérés comme séparateurs de répertoire.

Ainsi, si l'adresse http://www.site_filoutage.com/filoutage est répertoriée comme site de filoutage, l'adresse http://www.site_filoutage.com///filoutage n'avertira pas l'utilisateur qu'il est en train de naviguer sur un site apparemment malveillant (selon la liste noire maintenue).

Des mises à jour ne sont pas encore disponibles pour corriger cette vulnérabilité.

4.2 Protection contre les fenêtres intempestives, ou *pop-ups*

Une vulnérabilité a été identifiée concernant le système de blocage des fenêtres intempestives de Firefox 1.5.0.9.

En temps normal, Firefox empêche un site Internet d'accéder à l'espace de nommage `file://`, qui correspond aux fichiers de l'ordinateur du client qui se connecte. Cependant, lorsqu'un utilisateur choisit consciemment d'ouvrir une fenêtre intempestive qui a été bloquée, le code source de cette fenêtre peut appartenir à cet espace de nommage. La *pop-up* a ensuite accès à l'espace `file://` puisqu'elle est dans la même « zone ».

Ainsi, si un attaquant peut prédire le nom d'un fichier téléchargé pour l'appeler par la suite dans une *pop-up*, cela lui permettrait, via ce fichier qui a des droits sur la machine locale, d'accéder en lecture aux autres fichiers de l'ordinateur du client.

Cette vulnérabilité concernerait la branche 2.0 de Firefox.

5 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 01 et le 08 février 2007.

6 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>
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/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>
- Note d'information du CERTA CERTA-2006-INF-006, Risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA CERTA-2006-INF-008 sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-008/>

7 Rappel des avis émis

Durant la période du 02 au 09 février 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-065 : Multiples vulnérabilités dans Sun Solaris
- CERTA-2007-AVI-066 : Vulnérabilité de Sun Solaris
- CERTA-2007-AVI-067 : Multiples vulnérabilités de Wireshark (Ethereal)
- CERTA-2007-AVI-068 : Multiples vulnérabilités de Samba
- CERTA-2007-AVI-069 : Multiples vulnérabilités sous PostgreSQL
- CERTA-2007-AVI-070 : Vulnérabilité dans Mambo
- CERTA-2007-AVI-071 : Vulnérabilité de BlueCoat WinProxy
- CERTA-2007-AVI-072 : Vulnérabilité dans WinRAR et RAR
- CERTA-2007-AVI-073 : Vulnérabilités des produits Trend Micro
- CERTA-2007-AVI-074 : Vulnérabilité dans Avast Server

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

- CERTA-2007-AVI-020-002 : Multiples vulnérabilités dans Fetchmail
(ajout de la référence au bulletin de sécurité RedHat)
- CERTA-2007-AVI-055-003 : Vulnérabilité de GTK2
(ajout de la référence au bulletin de sécurité Ubuntu)

8 Actions suggérées

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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>

9 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.

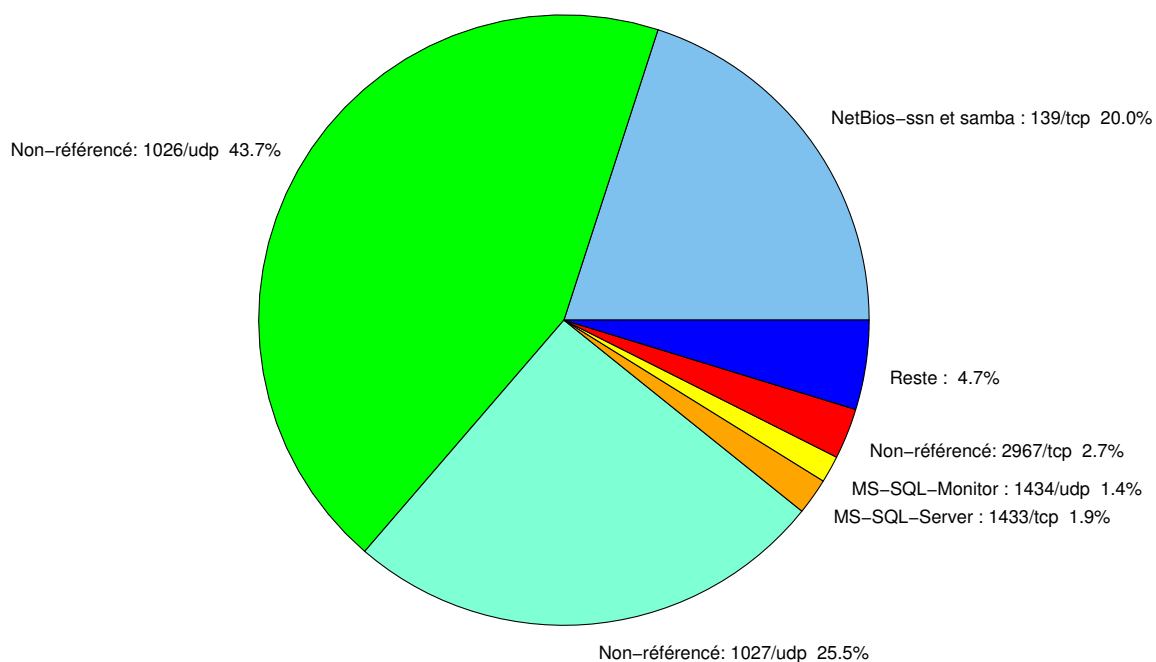


FIG. 1: Répartition relative des ports pour la semaine du 01.02.2007 au 08.02.2007

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
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
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	–	–
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
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
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343
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
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
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	CERTA-2002-AVI-213
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	–	CERTA-2005-AVI-024
6112	TCP	Dtspcd	–	CERTA-2002-ALE-001
6129	TCP	Dameware Miniremote	–	CERTA-2003-AVI-214 CERTA-2005-AVI-326
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	–
13701	TCP	Veritas NetBackup	–	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	–	CERTA-2005-AVI-310

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

port	pourcentage
1026/udp	43.67
1027/udp	25.54
139/tcp	20.01
2967/tcp	2.67
1433/tcp	1.92
1434/udp	1.42
4899/tcp	0.95
137/udp	0.92
22/tcp	0.55
80/tcp	0.5
1080/tcp	0.4
443/tcp	0.32
3128/tcp	0.27
3306/tcp	0.15
15118/tcp	0.1
3127/tcp	0.07
11768/tcp	0.05
2100/tcp	0.02

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

09 février 2007 version initiale.