Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 décembre 2006
N° CERTA-2006-ACT-049

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2006-49

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-049

Gestion du document

Référence	CERTA-2006-ACT-049
Titre	Bulletin d'actualité 2006-49
Date de la première version	08 décembre 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.

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-049.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-049/

1 Activité en cours

1.1 Code malveillant déposé sur un site défiguré

Un de nos correspondants a été infecté par un code malveillant suite à une visite sur un site défiguré. Le code malveillant, téléchargé sous la forme d'une bibliothèque `dll`, n'était pas reconnu par les antivirus. La visite sur le site défiguré a également provoqué l'arrêt inopiné du navigateur (*Mozilla Firefox*).

D'une manière générale, il est important de prendre conscience que les incidents de ce type peuvent survenir lorsque l'on navigue sur un site qui a subi une attaque. Il convient de prendre un maximum de précautions avant de vérifier la présence d'une page défigurée. Il est important de ne pas naviguer avec un compte ayant des privilèges d'administration, et des solutions basées sur des environnements virtuels (comme *VMWare* par exemple) peuvent être envisagées.

1.2 Alerte concernant Microsoft Word

Une nouvelle vulnérabilité, commune à de nombreuses versions du logiciel Word et fonctionnant sur les systèmes d'exploitation Windows et MacOS, est apparue. Elle n'est pas encore corrigée et le CERTA a publié une alerte le mercredi 6 décembre 2006 (CERTA-2006-ALE-014). Cette vulnérabilité est déjà exploitée.

Il est recommandé aux utilisateurs de ne pas ouvrir de documents Word dont la provenance est incertaine. Cette vulnérabilité est un vecteur idéal pour conduire des attaques ciblées, par exemple via une pièce jointe à un courriel. Par ailleurs, les fêtes de fin d'année seront propices à l'envoi de multiples messages électroniques contenant des pièces jointes de toutes sortes. Une grande vigilance est donc à nouveau recommandée dans l'ouverte des fichiers insérés en pièces jointes. Tout incident ou doute lors de l'ouverture d'un tel fichier devrait être immédiatement signalé.

Quelques liens utiles :

- Alerte CERTA-2006-ALE-014 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-ALE-014/index.html
- Les canulars par messagerie :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-005/index.html
- Les mesures de prévention pour la messagerie :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html
- Mise en garde au sujet des messages de voeux :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-REC-002/index.html

2 Nouvelle technique de contournement des antivirus

Une nouvelle technique de contournement des antivirus a été rendue publique cette semaine. Certains antivirus n'auraient pas le comportement attendu lors du traitement de fichiers encodés en `base64`. En particulier, lorsqu'un attachement contient un caractère ne faisant pas partie de « l'alphabet base64 », certains antivirus ne prennent pas correctement en compte le fichier attaché, alors que le client de messagerie l'affiche normalement.

Cette technique peut donc être utilisée pour échapper au contrôle de certains antivirus.

On peut donc s'attendre à la publication de correctifs par des éditeurs d'antivirus dans les jours à venir.

Pour plus d'informations, vous pouvez consulter le document à l'adresse suivante :
http://www.quantenblog.net/security/virus-scanner-bypass

3 Les clics dans les courriels

3.1 Introduction

Les courriers éléctroniques, tout comme les lettres postales, sont un moyen de communication aisé pour transmettre de l'information. Cependant, le processus standard pour les transmettre n'offre pas, sans service complémentaire, certaines garanties. Pour les lettres postales, l'expéditeur n'est pas vérifié, et l'entête du courrier (adresses, téléphone, dates) peut être falsifié. Il en va de même pour la messagerie électronique.

Ces problèmes sont à la source des attaques de filoutage (ou *phishing*), ou servent à conduire les utilisateurs vers des pages Web spécifiques.

3.2 Une origine incertaine

Parmi les protocoles de messagerie, SMTP (pour *Simple Mail Transfer Protocol*) est le plus fréquent, et est utilisé au transfert de courriers vers les serveurs de messagerie. Son fonctionnement est assez simple : après avoir indiqué l'expéditeur et le destinataire du message, le corps du message est transféré. C'est celui-ci qui s'affiche ensuite dans le client de messagerie. Il est possible de modifier l'expéditeur à tout moment. En général, ce dernier n'est pas vérifié, ni même la cohérence entre celui indiqué dans l'entête du message, et celui utilisé par l'envoi SMTP.

3.3 Un contenu pas nécessairement fiable

Le contenu que vous visualisez n'est pas nécessairement complet et exact. Par exemple, dans un message rédigé en HTML, un lien sera codé de la façon suivante :

```
<_a_ href="\emph{adresse-malveillante}">\emph{adresse-apparente}</_a_>
```

Le client de messagerie, s'il est configuré pour interpréter les messages en HTML, ne vous affichera que *adresse-apparente*, mais vous serez redirigé vers *adresse-malveillante*. Il y a également des questions d'encodage, qui peuvent perturber la visualisation correcte d'un courrier.

Recommandations du CERTA :

Comment pourriez-vous réagir étant donné les problèmes mentionnés dans les deux paragraphes précédents ?

Comme vous avez pu le constater, il n'est pas aisé de déterminer si un courriel a été envoyé à des fins malveillantes.

Quelques bons réflexes vous permettront, malgré la difficulté d'estimer le risque, de limiter les impacts d'une telle attaque :

- soyez circonspect quand l'expéditeur ou le destinataire affiché vous est inconnu, ou quand le style ou la syntaxe sont approximatifs ;
- soyez vigilant lorsqu'un courriel vous demande des actions urgentes, vous propose de l'argent facile ou des produits peu chers ;
- si vous avez cliqué trop vite, ne fournissez pas d'information sur le site Internet qui s'affiche en remplissant par exemple un formulaire ou en renseignant un mot de passe ;
- faites appel à votre correspondant informatique ou de sécurité si vous avez le moindre doute sur la nature d'un courriel reçu ou sur une page Internet visitée suite au clic depuis un courriel.

Quelques mesures plus techniques :
Pour aller plus loin, vous pouvez considérer des initiatives plus techniques :

- tapez directement dans le navigateur Internet l'adresse indiquée par le courrier électronique, sans cliquer dessus, et après l'avoir vérifiée. En effet le lien qui s'affiche à l'écran n'est pas nécessairement la véritable adresse Internet cible ;
- configurez votre client de messagerie pour lire tous vos courriers électroniques au format texte ;
- configurez votre navigateur Internet pour qu'il n'interprète pas les ActiveX, Java et le Javascript par défaut ;
- consultez le code source du courrier électronique pour vérifier les adresses incluses dans les liens HTML.

4 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 30 novembre et le 07 décembre 2006.

5 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.f r/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/

6 Rappel des avis émis

Durant la période du 01 au 07 décembre 2006, le CERTA a émis les avis suivants :

- CERTA-2006-AVI-518 : Vulérabilité dans KOffice
- CERTA-2006-AVI-519 : Vulnérabilité de Kronolith
- CERTA-2006-AVI-520 : Vulnérabilité Novell
- CERTA-2006-AVI-521 : Vulnérabilité dans F-Secure Antivirus et F-Secure Internet Gatekeeper
- CERTA-2006-AVI-522 : Multiples vulnérabilités de Xerox WorkCenter
- CERTA-2006-AVI-523 : Vulnérabilité du logiciel GnuPG
- CERTA-2006-AVI-524 : Multiples vulnérabilités de ProFTPD
- CERTA-2006-AVI-525 : Vulnérabilité dans Novell ZENworks Asset Management
- CERTA-2006-AVI-526 : Vulnérabilités dans SquirrelMail
- CERTA-2006-AVI-527 : Vulnérabilités dans F-Prot Antivirus pour UNIX
- CERTA-2006-AVI-528 : Vulnérabilité dans Sun Java System
- CERTA-2006-AVI-529 : Vulnérabilités dans IBM Tivoli
- CERTA-2006-AVI-530 : Vulnérabilité dans Ruby
- CERTA-2006-AVI-531 : Vulnérabilité dans Novell ZENworks Patch Management
- CERTA-2006-AVI-532 : Vulnérabilité de Citrix
- CERTA-2006-AVI-533 : Multiples vulnérabilité du produit Trend Micro Office Scan
- CERTA-2006-AVI-534 : Vulnérabilités dans SAP Internet Graphics Service
- CERTA-2006-AVI-535 : Vulnérabilité de Adobe Download Manager
- CERTA-2006-AVI-536 : Vulnérabilité dans Barracuda Spam Firewall
- CERTA-2006-AVI-537 : Vulnérabilité dans les pilotes de cartes réseau Intel
- CERTA-2006-AVI-538 : Vulnérabilité dans Novell Client

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'inf ormation de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'orga nisme 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 règlementaire, 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 œuvre (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 COSSI/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 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.

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, la DCSSI dispose d'un centre de formation :

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

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.

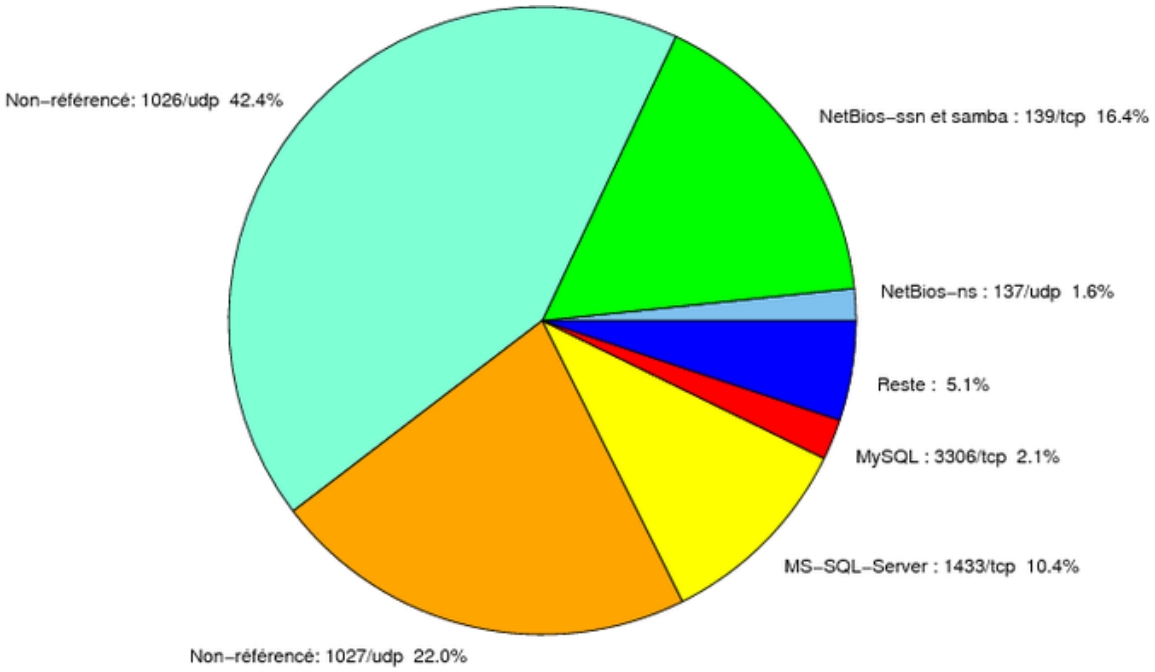

FIG. 1: Répartition relative des ports pour la semaine du 30.11.2006 au 07.12.2006

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CE
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CE
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CE
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CE
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE

				http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE
2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	–	Symantec Antivirus	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070 6101	TCP TCP	BrightStor ARCserve/Enterprise Backup Veritas Backup Exec	– –	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

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

port	pourcentage
1026/udp	42.38
1027/udp	21.99
139/tcp	16.35
1433/tcp	10.38
3306/tcp	2.09
137/udp	1.64
1080/tcp	0.92
80/tcp	0.84
1434/udp	0.71
4899/tcp	0.57
22/tcp	0.53
25/tcp	0.29
3128/tcp	0.19
443/tcp	0.15
15118/tcp	0.09
3389/tcp	0.08
143/tcp	0.05
5554/tcp	0.04
31511/tcp	0.02

TAB. 3: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Correctifs correspondant aux ports destination des paquets rejetés 7
3 Paquets rejetés 8

Gestion détaillée du document

08 décembre 2006 version initiale.