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 août 2008
N° CERTA-2008-ACT-032

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-32

Gestion du document

Référence	CERTA-2008-ACT-032
Titre	Bulletin d'actualité 2008-32
Date de la première version	08 août 2008
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-2008-ACT-032.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-2008-ACT-032/

1 Incident de la semaine

1.1 Que faire des pourriels ?

1.1.1 Présentation

Cette semaine, le CERTA a informé le responsable d'un site internet de la compromission de ce dernier.

En effet, le site Web avait été visité par des personnes malveillantes qui y avaient déposé des pages frauduleuses d'une campagne de filoutage (*phishing*). Une rapide analyse du site a permis de mettre en évidence que la compromission a été facilitée par un défaut de mise à jour du gestionnaire de contenu utilisé (*CMS*). Au delà de cette compromission, une discussion s'est engagée, entre le CERTA et le responsable du site, sur la gestion des pourriels de filoutage.

Le CERTA rappelle qu'en France l'association `Signal Spam`, regroupant la plupart des organisations françaises concernées par la lutte contre le spam, tente de fédérer les efforts de tous pour lutter contre les pourriels. `Signal Spam` met à disposition sur son site des outils et des conseils permettant de leur rapporter facilement et rapidement des courriers indésirés. De tels signalements ne vont pas réduire, instantanément, le nombre de pourriels dans les boites mais vont assurément contribuer à lutter contre ce fléau.

1.1.2 Documentation

- Note d'information du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information : http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/
- Le site de Signal Spam : http://www.signal-spam.fr

2 Les journaux d'événements de Microsoft SQL

Les journaux d'événements, les « *traces* », sont par défaut dans le répertoire `LOG` contenu dans le repertoire racine de la base de données. La liste des traces configurées, avec les fichiers associés, s'obtient à l'aide de la commande *fn_trace_getinfo*. Les fichiers sont au format binaire et peuvent être lus en utilisant la fonction *fn_trace_gettable*. Les événements et les informations associées enregistrés (*EventClass, DatabaseID, TransactionID* ....) sont paramétrables à l'aide de procédures stockées. Il est nécessaire de désactiver une trace avant de la modifier. Par défaut, une trace système est activée et ne peut être arretée que par l'utilisation de la procédure *sp_configure*. Voyons dans l'exemple suivant la création d'une nouvelle trace pour laquelle on va activer l'enregistrement des événements *118 - Audit Object Derived Permission Event*. Pour ces enregistrements, on veut comme informations : *TextData*(1), les *BinaryData*(2) et le *startTime*(14).

```
DECLARE
@traceidnum INT,
@on BIT,
@file_path NVARCHAR(256),
@maxsize bigint;
SET @on = 1;
SET @maxsize =5;
SET @file_path = 'c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\trace';

/* creation de la trace
EXEC sp_trace_create  @traceid = @traceidnum OUTPUT, @options = 2, @tracefile = @file_pa

/*desactivation de la trace
EXEC sp_trace_setstatus @traceidnum, 0

/*parametrage
EXEC sp_trace_setevent @traceidnum, 118, 1, @on
EXEC sp_trace_setevent @traceidnum, 118, 2, @on
EXEC sp_trace_setevent @traceidnum, 118, 14, @on

/*activation de la trace
EXEC sp_trace_setstatus @traceidnum, 1
```

La fonction *fn_trace_getinfo* permet de vérifier que la trace a bien été créée :

```
select * from fn_trace_getinfo(default)
```

Pour lire les données enregistrées il faut utiliser la fonction *fn_trace_gettable* (L'argument *default* indique que tous les fichiers associés seront lus) :

```
SELECT *  FROM fn_trace_gettable('C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LO
```

Le CERTA rappelle l'importance de bien configurer les journaux d'événements et de les analyser régulièrement.

2.1 Documentation

- Introducing SQL Trace : http://msdn.microsoft.com/en-us/library/ms191006.aspx
- Option default trace enable : http://msdn.microsoft.com/fr-fr/library/ms175513.aspx
- Version gratuite du serveur *Microsoft SQL Server Express* : http://msdn.microsoft.com/fr-fr/express/aa718378.aspx?wt.srch=1

3 FLASH : Attention aux fausses mises à jour !

3.1 La menace

Cette semaine, l'éditeur *Adobe* a publié, sur le *blog* de son équipe de réponse aux incidents de sécurité, une mise en garde contre de fausses mises à jour de son lecteur *Flash*.

En effet, de nombreux sites malveillants, proposant par exemple de lire des vidéos en ligne, incitent le visiteur à télécharger une mise à jour du lecteur *Flash* afin de pouvoir lire correctement les vidéos mises à disposition. Ces mises à jour se révèlent être des chevaux de Troie et permettent à des personnes malveillantes de prendre le contrôle de la machine compromise ou d'enregistrer les frappes claviers. La diffusion de ce code malveillant repose sur une campagne de pourriels invitant à venir visiter des sites malveillants et sur de l'ingénierie sociale via des sites de réseaux sociaux.

3.2 Les recommandations

Le CERTA profite de cette actualité afin de rappeler certaines bonnes pratiques et recommandations afin de se protéger et de limiter l'impact de ce type de compromission :

- ne jamais suivre un lien provenant d'une source non fiable ;
- toujours se procurer les mises à jour sur le site officiel de l'éditeur ;
- maintenir l'ensemble des applications (système d'exploitation, navigateur, antivirus, . . .) à jour ;

L'éditeur *Adobe* donne également un moyen de vérifier si la mise à jour provient bien chez lui. Il est en effet possible de vérifier le certificat qui est validé par *Microsoft Windows* pour les utilisateurs de ce système d'exploitation. Pour effectuer cette vérification, il suffit de vérifier l'organisme de publication : il doit toujours être « *Adobe Systems, Incorporated* ». Cette vérification peut être faite au lancement de l'installation ou en faisant un clic-droit sur le fichier exécutable, puis « Propriétés ». Dans l'onglet « signature » figure l'information sur l'éditeur de la mise à jour ou de l'application.

Enfin, il existe une page web permettant de déterminer la version du client *Flash* installé sur le système et de déterminer la version courante pour ce dernier. L'adresse de cette page est disponible ci-dessous.

Documentation

- Mise en garde d'*Adobe* :
  http://blogs.adobe.com/psirt/2008/08/verifying_installers.html
- Site de téléchargement des mises à jour officielles :
  http://www.adobe.com/go/getflashplayer/
- Page de vérification de version du Flash Player :
  http://www.adobe.com/products/flash/about/

4 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur des dispositifs de filtrage, entre le 01 et le 07 août 2008.

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=1935
- 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 01 au 07 août 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-383 : Vulnérabilités de phpMyAdmin
- CERTA-2008-AVI-384 : Vulnérabilité dans SAP MaxDB
- CERTA-2008-AVI-385 : Vulnérabilité dans HP-UX
- CERTA-2008-AVI-386 : Vulnérabilité CA ARCserve Backup
- CERTA-2008-AVI-387 : Vulnérabilité de libxslt
- CERTA-2008-AVI-388 : Multiples vulnérabilités dans Mac OS X
- CERTA-2008-AVI-389 : Faiblesse du Microsoft Protected Storage
- CERTA-2008-AVI-390 : Multiples vulnérabilités dans Ingres
- CERTA-2008-AVI-391 : Vulnérabilités de Python
- CERTA-2008-AVI-392 : Multiples vulnérabilités dans Apache Tomcat
- CERTA-2008-AVI-393 : Vulnérabilité dans HP-UX libc

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 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 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 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.

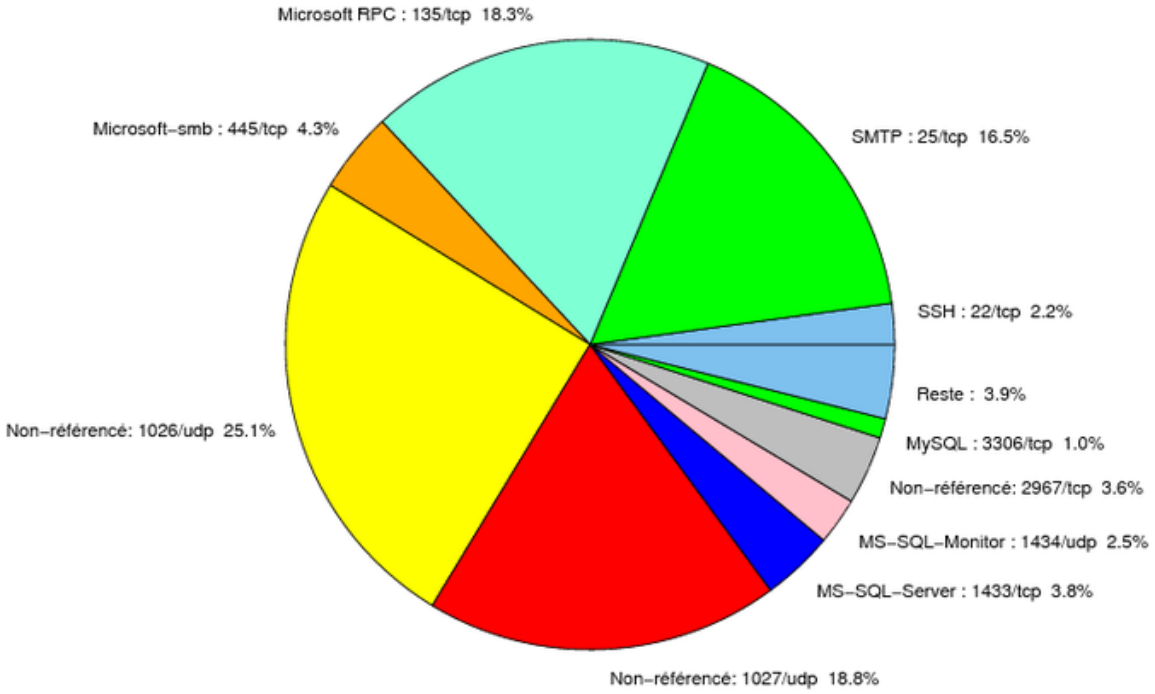

FIG. 1: Répartition relative des ports pour la semaine du 01.08.2008 au 07.08.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CERT
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CERT
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CERT
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CERT
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CERT
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CERT
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT http://www.certa.ssi.gouv.fr/site/CERT

				http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CER
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
427	TCP	Novell Client	–	http://www.certa.ssi.gouv.fr/site/CER
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
445	UDP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CER
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CER
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CER
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CER
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CER
2381	TCP	HP System Management	–	http://www.certa.ssi.gouv.fr/site/CER
2512	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2513	TCP	Citrix MetaFrame	–	http://www.certa.ssi.gouv.fr/site/CER
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CER
3104	TCP	CA Message Queuing	–	http://www.certa.ssi.gouv.fr/site/CER
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
3268	TCP	Microsoft Active Directory	–	http://www.certa.ssi.gouv.fr/site/CER
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
5151	UDP	IPSwitch WS_TP	–	http://www.certa.ssi.gouv.fr/site/CER
5151	TCP	ESRI ArcSDE	–	http://www.certa.ssi.gouv.fr/site/CER
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER

6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6106	TCP	Symantec Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
6502	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6503	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
6504	TCP	CA BrightStor ARCserve Backup	–	http://www.certa.ssi.gouv.fr/site/CER
8080	TCP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
10080	TCP	Amanda	MyDoom	–
10110	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CER
10916	TCP	Ingres	–	CERTA-2007-AVI-275-001
10925	TCP	Ingres	–	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	–	http://www.certa.ssi.gouv.fr/site/CER
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CER
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CER
54345	TCP	HP Mercury	–	http://www.certa.ssi.gouv.fr/site/CER
65535	UDP	LANDesk Management Suite	–	http://www.certa.ssi.gouv.fr/site/CER

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

port	pourcentage
1026/udp	25.08
1027/udp	18.76
135/tcp	18.29
25/tcp	16.5
445/tcp	4.33
1433/tcp	3.81
2967/tcp	3.63
1434/udp	2.49
22/tcp	2.16
3306/tcp	1.03
4899/tcp	0.94
139/tcp	0.89
23/tcp	0.66
137/udp	0.47
21/tcp	0.37
80/tcp	0.33
3389/tcp	0.14
143/tcp	0.09

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

08 août 2008 version initiale.