Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 janvier 2008
N° CERTA-2008-ACT-001

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-01

Gestion du document

Référence	CERTA-2008-ACT-001
Titre	Bulletin d'actualité 2008-01
Date de la première version	04 janvier 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-001.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-001/

1 Incidents de la semaine

1.1 Le PC compromis sert à attaquer le serveur

Cette semaine le CERTA a traité un incident relatif à la compromission d'un serveur web. Suite à la compromission, par un

enregistreur de frappes clavier, d'une des machines servant à mettre à jour le site web, les attaquants ont réussi à récupérer les informations de connexion au service FTP. Munis de ces informations, il a été facile aux attaquants de compromettre le site Internet légitime et d'y déposer des fichiers frauduleux afin de réaliser un filoutage contre une banque anglaise. Une fois informé, l'administrateur du serveur a rapidement identifié les causes de l'incident.

Le CERTA rappelle qu'il est dangereux de stocker des identifiants de connexion dans un fichier ou dans un appareil transportable susceptible d'être perdu ou volé (clé USB, téléphone, assistant personnel, etc.). De plus les mots de passe doivent être choisis de manière à être suffisamment complexes à deviner par un attaquant ou par une recherche exhaustive à base de dictionnaires. Le CERTA rappelle également que la politique de sécurité des mots de passe doit inclure une politique de changement régulière de ceux-ci.

Documentation

- Note d'information du CERTA sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/
- Note d'information du CERTA sur les bons réflexes en cas d'incident :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

1.2 Le site web oublié

Cette semaine le CERTA a informé une victime que son site Internet hébergeait des codes malveillants. Ces codes, de type `PHP Shell`, ont participé à des attaques informatiques contre d'autres serveurs web. La victime a indiqué que ce site web n'était plus utilisé et qu'elle pensait devoir le conserver pour ne pas perdre son nom de domaine. Le CERTA rappelle que le nom de domaine et les services Internet comme l'hébergement de site web, la messagerie, ... sont des informations distinctes. Il est tout à fait possible de conserver un nom de domaine sans pour autant avoir un site web. Dans le cas de cet incident, la victime contactera son hergeur pour désactiver son site et modifiera ses enregistrements DNS inutilisés.

2 Les attaques utilisant les référencements

Le début d'année est souvent propice aux bilans de l'année précédente. La fréquentation du site du CERTA a augmenté par rappor t à l'année précédente, ce qui indique certainement l'intérêt toujours croissant des internautes pour la sécurité informatique. Cette hausse de fréquentation est également en rapport avec un meilleur référencement du site dans les moteurs de recherches. Mais la hausse du nombre de visiteurs est sans commune mesure avec la hausse du nombre de tentatives d'attaque contre le site web. Cela s'explique car de plus en plus de programmes malveillants se basent sur les résultats des moteurs de recherches pour conduire leurs attaques.

Les journaux des connexions ne sont pas les seules sources d'informations contre une compromission. Toutefois ils peuvent permettre de mettre en évidence des vulnabilités et des tentatives d'attaque. La politique de sécurité doit inclure l'analyse et la gestion des journaux des connexions.

3 Fin du support de Netscape Navigator

`AOL` a annoncé, le 28 décembre 2007, la fin du support de son navigateur à compter du premier février 2008. Après cette date `AOL`, propriétaire de `Netscape Navigator` ne fournira plus de correctifs de sécurité à son application. Malgré la sortie de `Netscape Navigator 9` en juin dernier, celui-ci ne sera plus maintenu et il n'y aura plus d'évolution, tout comme pour les versions précédentes. Il restera cependant disponible en téléchargement. Le CERTA recommande l'utilisation d'un navigateur alternatif toujours maintenu par son éditeur afin de permettre sa mise à jour et de limiter ainsi les risques de vulnérabilité.

4 Bogue dans Windows Home Server

`Microsoft` a publié cette semaine le bulletin *KB946676* relatif à un problème dans `Windows Home Server`. Ce dysfonctionnement apparaît lorsque des fichiers présents sur le machine équipée de `Windows Home Server` sont édités par certaines applications comme :

- Windows Vista Photo Gallery ;
- Windows Live Photo Gallery ;
- Microsoft Office OneNote 2007 ;
- Microsoft Office OneNote 2003 ;
- Microsoft Office Outlook 2007 ;
- Microsoft Money 2007 ;
- SyncToy 2.0 Beta ;

Les fichiers édités par l'intermédiaire des partages réseau sont corrompus au moment de l'enregistrement et les rendent inutilisables. Ce problème intervient alors que le système est en pleine charge lors de l'édition des fichiers. Le dysfonctionnement ne concerne que `Windows home Server` et serait dû au système de partage de répertoire qui a été simplifié afin de le rendre plus convivial. `Microsoft` travaille à la création d'un correctif. Le CERTA recommande de faire une sauvegarde des données présentes sur les machines équipées de ce système d'exploitation et de ne pas éditer de fichiers via le réseau avec les applications précédemment citées.

Documentation :

- Bulletin Microsoft KB946676 du 29 décembre 2007 :
  http://support.microsoft.com/kb/946676

5 Les "métadonnées" surprennent encore

5.1 Introduction

Une métadonnée (du grec *meta* (après) et du latin *data* (informations)) est une donnée servant à décrire une autre donnée. Si le terme est devenu relativement courant, nombreux sont ceux qui les utilisent sans s'en rendre compte. L'exemple le plus courant, et qui a fait partie de notre actualité de la semaine, concerne simplement les photos numériques, mais les métadonnées concernent quasiment tous les fichiers électroniques.

Les appareils photos numériques utilisent en standard le format de fichier `JPEG` et exploitent les métadonnées associées. Ces informations sont renseignées par l'appareil au moment de la prise et contiennent des détails tel que la vitesse d'obturation, les dimensions, la date, la marque, voire le numéro de série de l'appareil et des coordonnées GPS. Elles contiennent aussi une vignette de taille réduite servant d'aperçu. Il existe plusieurs formats de métadonnée, et la norme `JPEG` prévoyant un champ d'informations de taille variable, il est possible d'en utiliser plusieurs à la fois sur la même photo. Historiquement, les fichiers `JPEG` contiennent des métadonnées au format `Exif` qui n'est plus maintenu et il est conseillé d'utiliser des alternatives tel que `XMP` (*Extensible Metadata Plateform*) ou `IPTC` (*International Press Telecommunications Council*).

Lors de manipulations graphiques ces informations ne sont pas toujours modifiées, par exemple, lors d'un redimensionnement ou de modification des contrastes, la marque de l'appareil ou la date de la prise de la photo ne sont pas modifiées. Si les logiciels d'imagerie courants n'exploitent pas ces champs, il existe des logiciels dédiés tel que `exiv2` ou `hachoir` qui permettent d'éditer ces informations.

5.2 La preuve par l'exemple

La photo utilisée dans l'exemple suivant a été prise par un photographe professionnel. Elle montre bien la cohabitation des métadonnées. En effet, le champ résolution fait partie du format `Exif`, alors que le *copyright* vient du format `IPTC`.

```
#exiv2 imageOriginale.jpg
File name       : imageOriginale.jpg
File size       : 280937 Bytes
Camera make     : NIKON CORPORATION
Camera model    : NIKON D200
Image timestamp : 2007:08:31 13:37:25
Exposure time   : 1/320 s
Aperture        : F9.5
...
Exif Resolution : 964 x 646
Thumbnail       : JPEG, 5764 Bytes
Copyright       : photos :  © xxxxxxxxxxxxxxxxxxxxxxxxe.com, © tous droits reservés © all rights reserved
```

En utilisant l'option `-pt` d'`exiv2` on peut obtenir davantage d'informations. Ainsi on voit que la photo originale a été modifiée sous Photoshop le 09/09/2007. En s'amusant à la redimensionner et modifier sous `Gimp`, on remarque aussi que le *thumbnail* n'a plus la même taille et a donc certainement été regénéré. Cela est facilement verifiable grâce à la commande `exiv2 -et file1.jpg file2.jpg` qui va extraire les aperçus dans *file1-thumb.jpg* et dans *file2-thumb.jpg*. On voit aussi, que la description `Exif` de la taille ne change pas, ce qui prouve qu'il n'est vraiment pas aisé de maîtriser l'évolution de ces informations discrètes.

```
#exiv2 -pt imageOriginale.jpg
...
Exif.Image.Software                           Ascii      30  Adobe Photoshop CS3 Macintosh
Exif.Image.DateTime                           Ascii      20  2007:09:09 22:22:12
Exif.Photo.PixelXDimension                    Long        1  964
Exif.Photo.PixelYDimension                    Long        1  646
Exif.Thumbnail.JPEGInterchangeFormatLength    Long        1  5764
...
```

Après modification sous GIMP (redimensionnement et gribouillage)

```
#exiv2 -pt imageRetouchée.jpg
```

```
...
Exif.Image.Software                           Ascii      15  GIMP 2.4.0-rc3
Exif.Image.DateTime                           Ascii      20  2008:01:04 09:19:13
Exif.Photo.PixelXDimension                    Long        1  964
Exif.Photo.PixelYDimension                    Long        1  646
Exif.Thumbnail.JPEGInterchangeFormatLength    Long        1  6440
...
```

5.3 Les métadonnées dans notre actualité

Dans le cas de cette semaine, un webmestre indélicat utilisait des photos sans en citer l'auteur, pensant qu'un simple renommage et redimensionnement suffirait à en faire disparaitre la provenance. C'est là que les *tags* `Exif` l'on desservit, il serait très étonnant qu'il eut été en possession d'exactement le même appareil, qu'il lui aurait permis de prendre une photo en simultané au même endroit et avec les même paramètres....

Pourtant ces informations « cachées » ont déjà défrayé la chronique. En 2003, une personnalité de la télévision américaine, Catherine Schwartz, avait mis en ligne une photo de ses yeux, résultat de la découpe d'une de ses photos personnelles. Malheureusement, la manipulation n'avait pas modifiée la vignette d'aperçues qui la montrait à moitié nue.

5.4 conclusion

Si la présence de ces informations peut parfois aider à résoudre des problèmes de propriété intellectuelle, le manque de visibilité les concernant peut gêner aussi les développeurs qui finalement ne gèrent pas correctement ces champs. Ainsi plusieurs vulnérabilités touchant différents logiciels sont exploitables à l'aide d'images aux champs `Exif` spécifiquement construits (CVE-2007-6351, CVE-2007-6352, ...).

Le CERTA rappelle que les métadonnées concernent de très nombreux fichiers (DOC, PDF, ...) et qu'il est important de maîtriser complètement les formats utilisés pour éviter toute fuite d'informations.

6 Mise à jour et support de PHP

Comme décrit dans l'avis CERTA-2008-AVI-002, une mise à jour pour la branche 4 du langage `PHP` vient d'être publiée. Outre le fait que cette version apporte des correctifs de sécurité, il est à noter que, comme indiqué sur le site `http://www.php.net`, la branche 4 de `PHP` ne connaîtra plus de nouvelles versions. En effet, depuis le 31 décembre 2007, le développement de cette dernière est arrêté. la nouvelle version 4.4.8 ne fera donc plus l'objet que de correctifs de sécurité en cas de faille majeure. Elle sera definitivement abandonnée le 8 août 2008.

Documentation :

Il est donc recommandé de migrer vers la dernière version de la branche 5 : la 5.2.5 au moment de la rédaction de la présente publication

7 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 27 décembre 2007 et le 03 janvier 2008.

8 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/

9 Rappel des avis émis

Dans la période du 28 décembre 2007 au 03 janvier 2008, le CERTA a émis les avis suivants :

– CERTA-2007-AVI-552-001 : Vulnérabilité dans ClamAV
– CERTA-2007-AVI-566 : Multiples vulnérabilités dans Mambo
– CERTA-2007-AVI-567 : Vulnérabilité dans Novell Identity Manager
– CERTA-2007-AVI-568 : Multiples vulnérabilités dans VLC Media Player
– CERTA-2007-AVI-569 : Vulnérabilité de Tomcat
– CERTA-2007-AVI-570 : Vulnérabilité dans IBM DB2 Content Manager
– CERTA-2007-AVI-571 : Vulnérabilité de Mantis
– CERTA-2007-AVI-572 : Vulnérabilité dans Syslog-ng
– CERTA-2007-AVI-573 : Vulnérabilité dans Dovecot
– CERTA-2008-AVI-001 : Vulnérabilité dans Qt

Les mises à jour suivantes ont été publiées :

– CERTA-2007-AVI-555-001 : Multiples vulnérabilités dans Opera (ajout des références CVE associées)
– CERTA-2007-AVI-559-001 : Multiples vulnérabilités dans Wireshark (ajout de références CVE)

10 Actions suggérées

10.1 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.

10.2 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.

10.3 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.

10.4 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.

10.5 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.

10.6 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.

10.7 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

11 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.

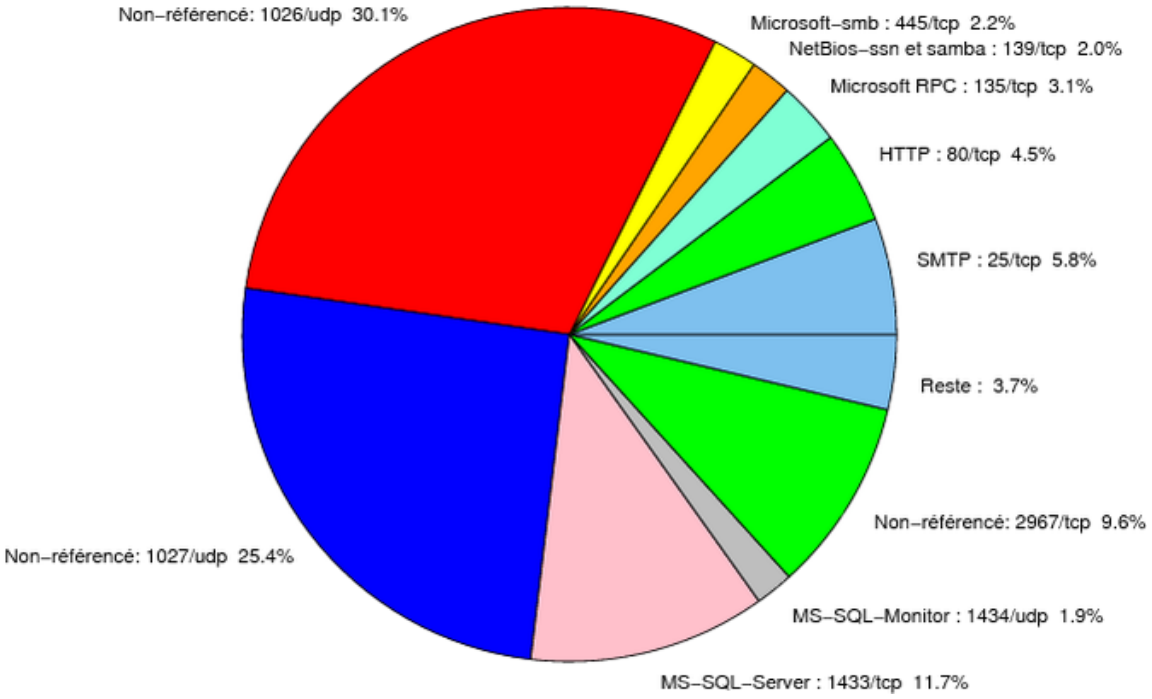

FIG. 1: Répartition relative des ports pour la semaine du au 27.12.2007 au 03.01.2008

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	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
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER CERTA-2007-ALE-005-001
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CER
69	UDP	IBM Tivoli Provisioning Manager	–	http://www.certa.ssi.gouv.fr/site/CER
80	TCP	HTTP	–	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
106	TCP	MailSite Email Server	–	– http://www.certa.ssi.gouv.fr/site/CER
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CER
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CER
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER http://www.certa.ssi.gouv.fr/site/CER
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CER
139	TCP	NetBios-ssn et samba	–	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 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	30.07
1027/udp	25.38
1433/tcp	11.72
2967/tcp	9.57
25/tcp	5.75
80/tcp	4.53
135/tcp	3.12
445/tcp	2.19
139/tcp	2.03
1434/udp	1.88
22/tcp	0.96
4899/tcp	0.85
3306/tcp	0.55
137/udp	0.33
1080/tcp	0.22
23/tcp	0.18
2100/tcp	0.06
3128/tcp	0.04
143/tcp	0.03

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

04 janvier 2008 version initiale.