Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 août 2008
N° CERTA-2008-ACT-034

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-34

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-2008-ACT-034`

Gestion du document

Référence	CERTA-2008-ACT-034
Titre	Bulletin d'actualité 2008-34
Date de la première version	22 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-034.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-034/

1 Les incidents traités cette semaine

1.1 un scénario d'attaque de bout en bout

1.1.1 Présentation

Cette semaine, le CERTA a participé au traitement d'incident relatif à la compromission d'un serveur web. Le premier jour de traitement, cet incident ressemblait à un banal cas de filoutage : un site Web compromis et des pages frauduleuses déposées à distance. La compromission semblait venir du mot de passe du compte FTP utilisé pour mettre à jour le site Web. Or un jour plus tard, le CERTA apprend que la victime a reçu plus tôt cette semaine un courriel semblant venir de son hébergeur lui demandant de mettre à jour ses identifiants de connexion. Le problème est que ce courrier était malveillant et qu'il a redirigé la victime vers une page frauduleuse reprenant celle de l'hébergeur. Sans prêter suffisamment d'attention ni respecter les principes de sécurité élémentaires, la victime a cliqué sur le lien du courrier et renseigné ses identifiants de connexion. Dans cette campagne de filoutage, les identifiant volés ont été exploités rapidement. L'une des premières actions des individus malveillants a été de modifier le mot de passe de la victime afin d'empêcher cette dernière de mettre fin rapidement aux méfaits réalisés par la suite par les attaquants.

Comme souvent, le filoutage commence par un courrier électronique contenant un message prétendument important et un lien (une URL) frauduleux. Un des conseils très souvent rappelé par le CERTA est de ne jamais cliquer sur un lien présent dans un courriel. Il est préférable de se rendre soi-même sur le site désiré, en recopiant l'adresse réticulaire (URL) à la main.

Le CERTA rappelle une nouvelle fois que les campagnes de filoutage (ou *phishing*) ne concerne pas uniquement le milieu bancaire. Toute information personnelle peut intéresser et peut être exploitée par des personnes malveillantes, que ce soit pour usurper l'identité, réaliser de l'ingénierie sociale, du chantage ou encore voler des fonds.

1.1.2 Documentation

- Note 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/
- Note du CERTA sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/

1.2 Défiguration de masse en 1 clic

1.2.1 Présentation

Cette semaine le CERTA a analysé les journaux des connexions d'un serveur Web mutualisant plus d'une centaine de sites Web (140 en tout). Tous ces sites ont été défigurés par la même personne en l'espace de quelques secondes. Les journaux des connexions, bien qu'en partie effacés par l'attaquant, montrent qu'à la suite de l'exploitation d'une vulnérabilité PHP, présente sur l'un des sites, l'attaquant a déposé ce qu'il est commun d'appelé un *PHP Shell*. Ce petit fichier se présente sous la forme d'une page écrit en langage PHP et offre la possibilité d'exécuter des commandes système à distance via le navigateur Internet. Il devient donc trivial en une ou deux lignes de commande *Shell* de modifier toutes les pages des sites Web présents et d'effacer ses traces.

Le CERTA rappelle que les CMS et leur composants sont des applications qu'il convient de mettre à jour et de suivre en terme de sécurité. PHP est un langage puissant , mais les variables ne doivent jamais être utilisées avant d'être contrôlées. Enfin le CERTA rappelle que l'hébergement mutualisé comporte des risques qu'il faut prendre en compte au préalable.

1.2.2 Documentation

- Note du CERTA sur le bon usage de PHP :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/
- Note du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/

2 Exploitation d'une vulnérabilité dans Ovidentia

Cette semaine a été marquée par l'exploitation d'une vulnérabilité du gestionnaire de contenu *Ovidentia*. Cette faille permet de réaliser des injections `SQL` et a fait l'objet de l'avis CERTA-2008-AVI-423. Un outil permettant d'exploiter facilement la vulnérabilité a été publié sur l'Internet. Celui-ci laisse des traces aisément repérables dans les journaux. Celles-ci sont du type :

`GET /index.php?tg=contact&idx=modify&item=-99999` suivi de l'inclusion `SQL`

Les prochaines versions 6.7.0 d'*Ovidentia* devraient inclure le correctif à ce problème. En attendant, une version corrigée du fichier `contact.php` a été mise à disposition sur le site du produit (voir avis CERTA). Il s'agit d'appliquer un simple remplacement de ce fichier afin de se protéger de ces attaques. À noter que la convention de nommage du produit *Ovidentia* est un peu particulière puisque la version 6.6.97 en téléchargement est en fait la version 6.7.0 bêta. La dernière version stable en téléchargement est la version 6.6.5. Il est important de préciser que les versions proposées actuellement en téléchargement sont vulnérables, et qu'il faut donc appliquer le correctif après installation.

Le CERTA recommande aux administrateurs de serveur Web de rechercher dans leurs journaux d'éventuelles attaques à l'encontre du produit *Ovidentia*.

- Avis du CERTA CERTA-2008-AVI-423 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-423/

3 Fichiers de session avec Adobe

3.1 Présentation

Certains sites présentent, directement ou non, des animations Flash. Celles-ci peuvent déposer des fichiers sur le disque. Les fichiers de sessions Flash portent le nom de `LSO` (*Local Shared Objects*) ou *Flash cookies*. Ils sont pris en compte depuis la version 6 d'Adobe Flash et peuvent contenir tous types d'information comme des dates, des mots de passe, des pseudonymes, etc.

Ils permettent par exemple de conserver :

- le niveau sonore et l'activation du son lors de la précédente visite ;
- l'animation d'introduction si ce n'est pas la première visite ;
- la dernière page visitée d'un site développé en Flash ;
- garder le résultat du score le plus élevé d'un joueur ;
- etc.

Le fichier LSO a une extension `.sol`. Ce format est assez simple. Un fichier se compose d'un en-tête de 16 octets et du bloc de données constitué de déclarations de variables :

- la longueur du nom de la variable ;
- le nom de la variable ;
- le type de variable ;
- les données dont la taille dépend du type précédent ;

Les types de données peuvent être des nombres, des valeurs booléennes, des chaînes de caractères, une table, un pointeur, une date,.... Le type `XML` est une chaîne de caractères particulière ayant une longueur beaucoup plus importante (pas de limite particulière).

3.2 Différences avec des fichiers de session usuels

3.2.1 Rappel sur les fichiers de session HTTP

Les fichiers de session ou *cookies* sont des informations échangées dans les en-têtes du protocole HTTP. Elles sont positionnées par le serveur via l'en-tête `set-cookie` ou fournies par le navigateur via l'en-tête `cookie` et doivent respecter certaines conditions :

- leur taille ne doit pas excéder 4ko ;
- un client ne peut en stocker plus de 300 ;
- un serveur ne peut postitionner que 20 fichiers de session maximum.

Leur principe général est de gérer des sessions à un niveau applicatif et de suivre les habitudes de navigation de l'utilisateur. Le principe semble donc identique avec les applications Flash souhaitant stocker des informations sur le poste de l'utilisateur avec les LSO.

3.2.2 Les différences

Par défaut, l'utilisateur n'est pas prévenu du stockage des informations LSO.

Par ailleurs, ces fichiers Flash ne sont pas temporaires. Il n'y a pas de date d'expiration. Un ordinateur peut en stocker plusieurs dizaines sans soucis. La taille des données stockées peut atteindre 100ko par site, en comparaison aux 4ko des fichiers de session HTTP traditionnels. Cette taille peut même être dépassée avec un signalement par une boîte de dialogue.

L'usage des informations stockées par les LSO est normalement restreint aux domaines à l'origine de leur création. Cependant, des sociétés publicitaires ont montré dès 2005 qu'elles pouvaient également lire ces informations. L'intérêt est ici de récupérer des informations sur l'utilisateur même si ce dernier nettoie régulièrement ses fichiers de session HTTP. Il s'agit du principe des « LSO tiers » qui donnent accès à l'objet pour plusieurs sites/domaines (cf. section Documentation).

3.3 Recommandations

Les navigateurs les plus courants (Internet Explorer, Opera, Mozilla Firefox) ne prennent pas en compte ces informations. Une configuration rigoureuse de ces derniers n'empêche pas le stockage de ces informations.

Un site peut déposer un fichier de session classique et un LSO. Il est important de garder la même cohérence de nettoyage pour les deux.

La gestion des LSO se fait par le biais du site Web d'Abobe via une interface dédiée. L'adresse est indiquée dans la section « documentation » de cet article.

http://www.adobe.com/go/settingsmanager

Les fichiers de session Flash (LSO) se trouvent selon les systèmes d'exploitation dans différents répertoires :

```
Sous Windows :
        C:\Documents and Settings\XXXX\Application Data\Macromedia\Flash Player
Sous Mac OS X :
        ~/Library/Preferences/Macromedia/Flash Player
Sous Linux :
        ~/.macromedia
```

Il est toujours possible de modifier les droits de ces répertoires (en particulier sous Linux) pour ne pas donner de droits d'écriture et de lecture dessus.

Une extension du navigateur Mozilla Firefox permet de visualiser les LSO. Cependant l'usage de ces applications tierces doit être fait avec parcimonie et précautions.

Il est également possible d'utiliser différents navigateurs ou différents profils d'utilisation.

L'usage des modules Flash dans les navigateurs impliquent des soucis de confidentialité et de protection de la vie privée. Les risques sont plus importants que ceux des fichiers de session HTTP mais sont paradoxalement moins bien considérés par les utilisateurs et les applications Web. Ces risques doivent être connus et pris en compte dans la politique de sécurité.

Une solution radicale consiste simplement à ne pas utiliser de module Flash associé au navigateur.

3.4 Documentation associée

- Présentation Adobe, « Que sont des LSO (Local Shared Objects) ? » :
  http://www.adobe.com/fr/products/flashplayer/articles/lso/
- Project "Objection" d'extension de Mozilla Firefox :
  http://objection.mozdev.org/
- EPIC, Local Shared Objects – "Flash Cookies" :
  http://epic.org/privacy/cookies/flash.html
- Documentation Adobe du "Settings Manager" :
  http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html
- Site Adobe, "Flash Player - Settings Manager - Website Storage Settings panel" :
  http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html
- Adobe, "How to manage and disable LSO" :
  http://kb.adobe.com/selfservice/viewContent.do?externalId=52697ee8&sliceId=2
- Parseur possible :
  http://icube.freezope.org/temp/util/s2x
- Documentation "SOL File Format", 2005 :
  http://sourceforge.net/docman/display_doc.php?docid=27026&group_id=131628
- Adobe, « Que sont des LSO (Local Shared Objects) tiers ? » :
  http://www.adobe.com/fr/products/flashplayer/articles/thirdpartylso/

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 13 et le 21 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 15 au 21 août 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-419 : Vulnérabilité dans Symantec Storage Foundation for Windows
- CERTA-2008-AVI-420 : Vulnérabilités de Postfix
- CERTA-2008-AVI-421 : Vulnérabilité de VMware VirtualCenter
- CERTA-2008-AVI-422 : Multiples vulnérabilités dans xine
- CERTA-2008-AVI-423 : Vulnérabilité dans Ovidentia
- CERTA-2008-AVI-424 : Vulnérabilité dans GnuTLS
- CERTA-2008-AVI-425 : Vulnérabilité dans IBM WebSphere
- CERTA-2008-AVI-426 : Multiples vulnérabilités dans Opera

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.

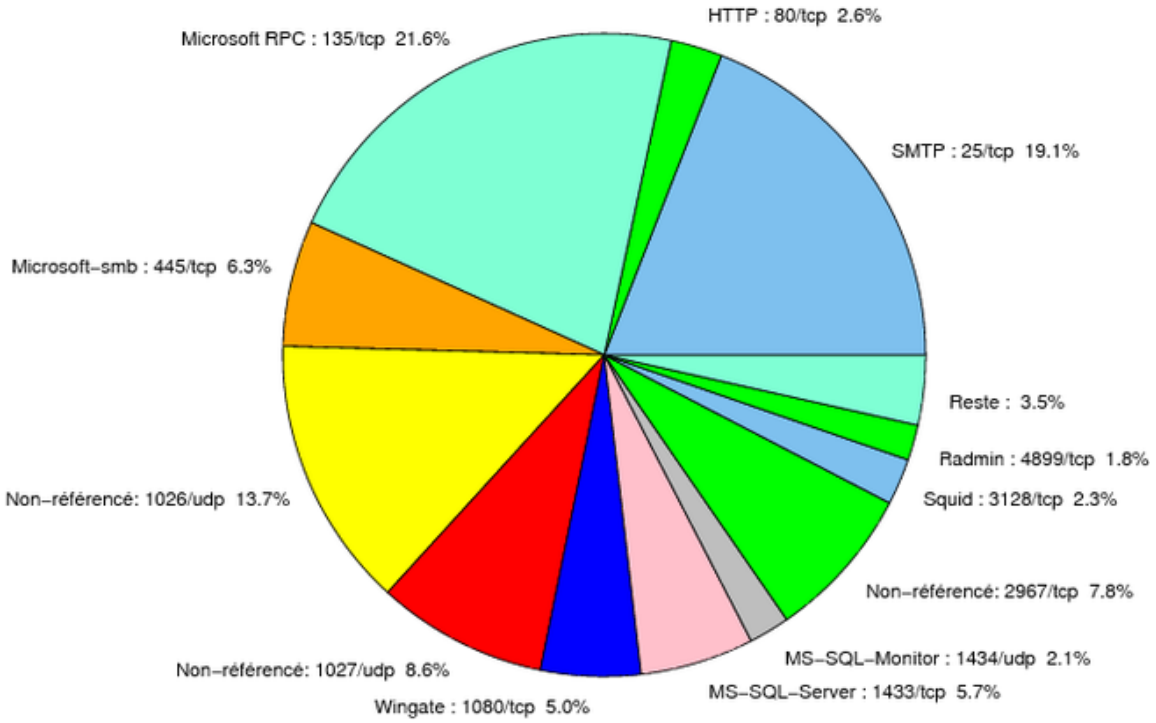

FIG. 1: Répartition relative des ports pour la semaine du 13.08.2008 au 21.08.2008

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

				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
135/tcp	21.59
25/tcp	19.06
1026/udp	13.66
1027/udp	8.58
2967/tcp	7.77
445/tcp	6.37
1433/tcp	5.72
1080/tcp	5.02
80/tcp	2.64
3128/tcp	2.32
1434/udp	2.05
4899/tcp	1.78
22/tcp	0.97
139/tcp	0.86
23/tcp	0.7
21/tcp	0.43
137/udp	0.32
3389/tcp	0.16
42/tcp	0.05

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

22 août 2008 version initiale.