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 avril 2008
N° CERTA-2008-ACT-014

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-14

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-014`

Gestion du document

Référence	CERTA-2008-ACT-014
Titre	Bulletin d'actualité 2008-14
Date de la première version	04 avril 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-014.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-014/

1 Incidents de la semaine

1.1 Abandon des sites en fin de vie

Cette semaine, le CERTA a informé plusieurs gestionnaires de sites web de la compromission de ces derniers. A plusieurs reprises, les responsables des sites, qui ont réagi promptement, ont répondu avoir supprimé les fichiers et dossiers frauduleux. Malgré les relances du CERTA leur indiquant que ces actions ne sont pas suffisantes, car elles ne corrigent en aucun cas les failles exploitées, certains gestionnaires en sont restés là ou ont répondu que « le site web était voué à disparaître prochainement ». Le CERTA insiste donc sur le fait que même inutilisé, un site en ligne doit être maintenu à jour ; si ce n'est pas le cas, alors il vaut mieux tout simplement le supprimer.

Le CERTA rappelle que tant que la vulnérabilité exploitée par les attaquants n'a pas été identifiée, le serveur reste vulnérable et utilisable à des fins malveillantes : envois de courriers non-sollicités (*SPAM*), filoutage (*phishing*), revendications diverses, détournement ou encore compromission des internautes, ... Bien souvent l'analyse des journaux de connexions suffit à mettre en évidence la faille exploitée. Si les journaux ne sont plus disponibles ou ont été compromis il faudra alors s'orienter vers une analyse plus poussée. Enfin, le CERTA rappelle qu'une analyse régulière des journaux peut permettre de déceler un comportement malveillant ou encore une compromission en cours.

Documentation

– Note d'information CERTA-2002-INF-002, « Les bons réflexes en cas d'intrusion sur un système d'information » :
http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/

2 Vulnérabilité dans MS Jet Database Engine - suite

Dans le bulletin de la semaine dernière, l'article « Vulnérabilité sur Microsoft Jet Database Engine » détaillait l'alerte CERTA-2008-ALE-005 portant sur une vulnérabilité de la bibliothèque `msjet40.dll` pour les versions inférieures à 4.0.9505.0. La particularité de cette faille est d'être exploitable via l'ouverture d'un fichier Word, alors que `msjet40.dll` est utilisé par *Access*. Pour rappel, les systèmes d'exploitation *Windows Vista*, *Windows Vista SP1* et *Windows Server 2003 SP2* ne sont pas vulnérables.

Le CERTA a présenté la semaine dernière un cas d'exploitation dans lequel la victime recevait un fichier au format `zip` contenant un fichier `doc` et un fichier `mdb`. Sur le bloc-notes de *McAfee*, un autre cas d'exploitation a été présenté. La victime reçoit cette fois-ci deux fichiers au format `doc`. Le premier fichier contient un lien vers le deuxième, qui est en fait un fichier `mdb` renommé. Via la faille MS Jet, celui-ci lance un *shellcode* qui ouvre le premier fichier pour y décoder un exécutable dissimulé par une simple opération XOR puis l'exécuter.

Cette semaine, Microsoft a annoncé les huit mises à jour prévues pour le 8 avril, et celles-ci n'incluent pas de correctif pour cette vulnérabilité. La liste prévisionnelle des mises à jour est disponible sur le site de Microsoft (cf. Documentation).

Le CERTA tient donc à rappeler qu'il existe un contournement provisoire pour cette faille qui rend inaccessible le fichier `msjet40.dll` et empêche donc l'exploitation de la vulnérabilité (cf. CERTA-2008-ALE-005). Il est également recommandé d'être très vigilant lors de la réception de fichiers au format Office et de n'ouvrir que des documents de confiance.

2.1 Documentation

– Alerte CERTA-2008-ALE-005 du 25 mars 2008 :
http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-005/
– Mises à jour de Microsoft prévues pour le 8 avril 2008 :
http://www.microsoft.com/technet/security/bulletin/ms08-apr.mspx
– Analyse d'exploitations MS Jet sur le bloc-notes de McAfee :
http://www.avertlabs.com/research/blog/index.php/2008/03/26/more-analysis-on-the-ms-jet-exploits-camouflaging-as-microsoft-word-files/

3 La tempête du premier avril

Plusieurs bulletins d'actualité du CERTA en témoignent : le ver `Storm Worm` a profité de chaque événement ces derniers mois (Halloween, Saint Valentin), et il persiste... Une nouvelle variante s'est propagée sur la toile pour fêter le premier avril. Cette fois-ci, le mail disposait d'un titre faisant penser à un poisson d'avril (*All Fools' Day*, *Doh! April's Fool*, ...), et le corps du message ne contenait qu'un message sibyllin suivi d'une adresse réticulaire (URL). Si l'utilisateur clique sur le lien, il est dirigé vers une page affichant une caricature, et proposant le téléchargement de trois fichiers : `funny.exe`, `foolsday.exe` et `kickme.exe`.

Chacun de ces fichiers est une variante de `Storm Worm` sans grande originalité. En revanche, le soupçon ambiant de fausse rumeur due à la journée internationale de la blague et du calembour a peut-être desservi l'annonce de cette nouvelle variante. Certains sites d'*experts* en sécurité ont d'ailleurs accentué cela en remplaçant leur site Internet par une copie de la page infectée, les exécutables servis ne contenant qu'un code affichant : "It was a joke!".

Il est inévitable que chaque événement serve de point d'appui pour la propagation de code malveillant. Ceux-ci sont pour la plupart basés sur la méconnaissance des risques, et un support adéquat leur permet de leurrer plus facilement leurs victimes. Aussi, une bonne hygiène d'utilisation de l'outil informatique permet de se prémunir de ce genre d'attaque : afficher ses mails en texte brut, ne pas ouvrir les courriels dont la source ou l'objet ne semble pas légitime, ne pas cliquer directement sur les liens contenus dans les mails, ne pas exécuter sans précautions un fichier obtenu sur l'Internet, ...

4 L'utilisation détournée des certificats

4.1 Rappel sur les chaînes de certification

Une chaîne de certification peut être modélisée en simplifiant par une architecture à trois niveaux : une autorité racine, une autorité intermédiaire, et une entité finale.

L'autorité racine est la base de la chaîne de certification. C'est elle qui dispose de la confiance. Dans les faits, l'autorité racine, supposée de confiance, émet un certificat qui sera embarqué dans un logiciel ou installé directement par l'utilisateur. Ainsi, un certificat signé par une telle autorité de certification racine disposera d'un gage de confiance vérifiable par le plus grand nombre.

Parfois, on peut souhaiter disposer soi-même de la possibilité de signer des certificats (certification interne à une entreprise, à un projet spécifique, ...). Il faut alors créer une autorité de certification en interne, dont personne ne pourra nier la confiance, et qui permettra de signer des certificats. Le problème de ce procédé est que les certificats signés de cette manière n'auront aucune valeur sortis du contexte de l'entreprise ou du projet. Il est donc nécessaire, dans un souci d'interconnexion, de valider la confiance de l'autorité de certification par une autorité racine.

Ainsi la chaîne de certification sera la suivante :

`Autorité racine -> Autorité intermédiaire -> Certificat final`

Cette vision simpliste d'une chaîne de certification peut être rallongée à l'envie. L'objectif de cet article n'est pas de détailler le mécanisme, mais de mettre en avant le comportement de certaines applications dans la vérification de cette chaîne.

4.2 La problématique

Lorsqu'un certificat est utilisé (message électronique signé, connexion en *HTTPS*...) l'application doit remonter la chaîne de certification, et donc accéder au certificat intermédiaire. Dans le standard RFC concerné (RFC 3280), il est défini que ce dernier peut être référencé dans le certificat initial par une URL externe. Le problème vient du fait que tant que la chaîne de certification n'a pas été complétée, le certificat initial n'est pas considéré comme de confiance, et donc l'URL contenue non plus. Certains logiciels implémentant les fonctionnalités décrites tentent donc d'accéder automatiquement à cette URL.

4.3 L'objectif

Il est imaginable, par exemple, que ce fonctionnement soit utilisé par une personne malveillante pour déterminer si une adresse électronique est valide, ou quand le message est lu. Il lui suffit pour cela d'envoyer un courrier signé à l'aide d'un certificat pointant, à l'aide d'une URL unique, vers une autorité intermédiaire sur laquelle il a un regard. La problématique est alors la même que celle de mouchards Internet (`Web Bug`) ou d'accusés de réception automatiques.

4.4 Conclusion

La plupart des clients ayant ce comportement ne permettent pas, à la date de rédaction de ce bulletin, de désactiver ce comportement génant. Pour se prémunir, il est possible d'utiliser des solutions alternatives. *Microsoft Outlook* et *Windows Mail* (remplaçant de *Outlook Express*) semblent chercher à atteindre systématiquement l'URL, contrairement à *Mozilla Thunderbird*, *Lotus Notes 8*, *Apple Mail* et les clients reposant sur *OpenSSL*. *Microsoft Office 2007* offrant la possibilité de signer des documents souffre de la même faiblesse. Il est aussi possible de contrôler les connexions sortantes utilisant l'agent «*Microsoft-CryptoAPI/**».

4.5 Documentation

- RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" :
  http://www.ietf.org/rfc/rfc3280.txt
- Cynops, "HTTP over X.509" :
  http://www.cynops.de/techzone/http_over_x509.html

5 MacOS X et la commande « defaults »

Il existe sous `MacOS X` une sorte d'équivalent à la base de registre `Microsoft` ou au *Gconf* de l'environnement graphique `GNOME`. Cet équivalent est accessible et manipulable par le biais de la commande *defaults*. Cette dernière peut prendre les arguments *read* ou *write* pour respectivement lire ou écrire des informations ou des paramètres. Grâce à cette commande, il est possible par exemple de :

- récupérer son profil d'utilisateur : *defaults read "AddressBookMe"* ;
- connaître les documents ouverts via `Preview` : *defaults read "com.apple.Preview.bookmarks"* ;
- connaîte les documents récement ouverts : *defaults read "com.apple.recentitems" Documents* ;
- ....

Pour avoir l'intégralité des paramètres disponibles, il suffira de lancer la commande *defaults read*.

Il est également possible de fixer des valeurs dans cette configuration afin de modifier le comportement du système : par exemple,

```
default write com.apple.desktopservices "DSDontWriteNetworkStores"  "true"
```

permet de ne plus avoir de répertoire de vignettes créé dans les lecteurs amovibles lors de leur insertion. Ces directives permettent donc d'altérer des mécanismes ou comportements permettant éventuellement de conduire des attaques.

Elles peuvent également donner accès, de façon parfois très précise, à des informations sensibles comme le comportement de l'utilisateur de la machine.

Toutes ces informations ou paramètres modifiables peuvent ainsi devenir très problématiques sur des machines en libre service ne disposant pas de plusieurs profils utilisateur, puisqu'il sera alors possible de connaître le comportement de l'utilisateur précédent ou de « piéger » la prochaine session.

Recommandation :

Il conviendra lors de l'utilisation de telles machines de prendre garde aux actions entreprises sur celles-ci et, le cas échéant, une procédure de « nettoyage » devra être mise en place évitant ainsi de laisser trop de traces susceptibles de servir à un éventuel attaquant.

6 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 mars et le 03 avril 2008.

7 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/

8 Rappel des avis émis

Dans la période du 28 mars au 03 avril 2008, le CERTA a émis les avis suivants :

– CERTA-2008-AVI-165 : Vulnérabilité dans OpenSSH
– CERTA-2008-AVI-166 : Vulnérabilité dans Acrobat Reader
– CERTA-2008-AVI-167 : Vulnérabilité dans OpenVMS
– CERTA-2008-AVI-168 : Vulnérabilité de phpMyAdmin
– CERTA-2008-AVI-169 : Vulnérabilité du logiciel antivirus Avast!
– CERTA-2008-AVI-170 : Vulnérabilité dans des produits Computer Associates
– CERTA-2008-AVI-171 : Vulnérabilité dans OpenSSH
– CERTA-2008-AVI-172 : Vulnérabilité du logiciel GnuPG
– CERTA-2008-AVI-173 : Vulnérabilité dans Novell Netware server
– CERTA-2008-AVI-174 : Vulnérabilité dans Macrovision OCI
– CERTA-2008-AVI-175 : Vulnérabilité dans IBM DB2 Content Manager
– CERTA-2008-AVI-176 : Vulnérabilité dans Sympa
– CERTA-2008-AVI-177 : Vulnérabilité dans lighttpd
– CERTA-2008-AVI-178 : Vulnérabilité dans Apache-SSL
– CERTA-2008-AVI-179 : Multiples vulnérabilités du logiciel multimédia Quicktime d'Apple

9 Actions suggérées

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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

10 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.

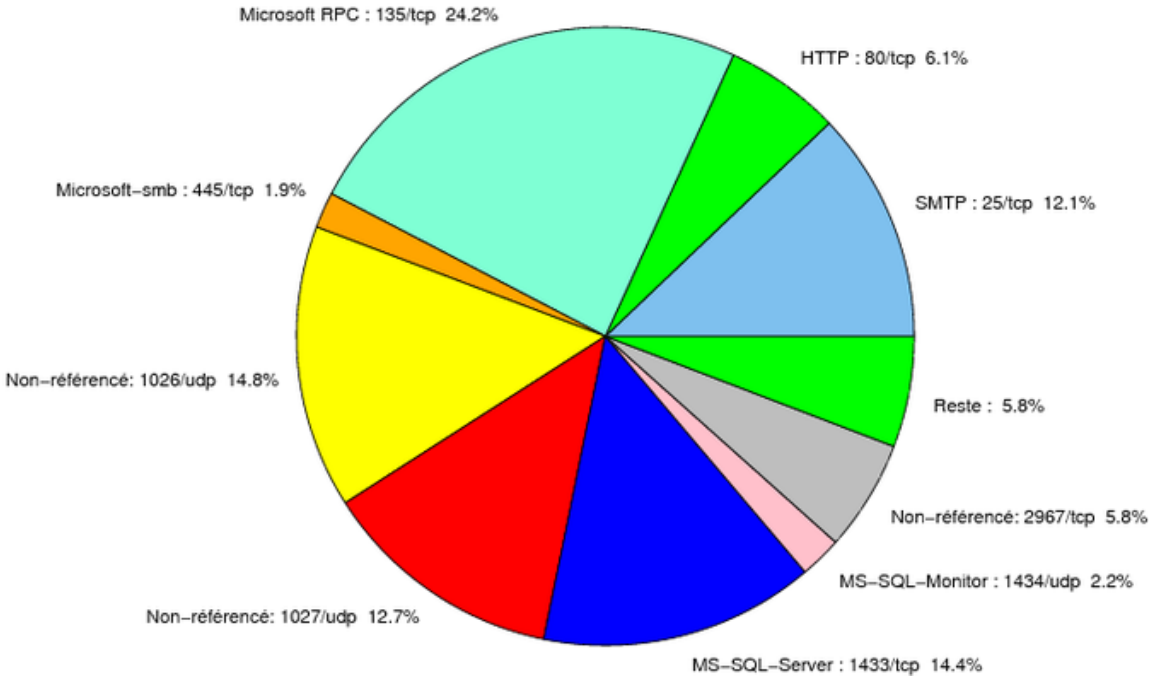

FIG. 1: Répartition relative des ports pour la semaine du 27.03.2008 au 03.04.2008

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/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/CERT
6014	TCP	IBM Tivoli Monitoring	–	http://www.certa.ssi.gouv.fr/site/CERT

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

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

port	pourcentage
135/tcp	24.2
1026/udp	14.81
1433/tcp	14.51
1027/udp	12.73
25/tcp	12.1
80/tcp	7.16
2967/tcp	5.8
1434/udp	2.2
445/tcp	1.87
22/tcp	0.99
139/tcp	0.91
3306/tcp	0.8
4899/tcp	0.76
137/udp	0.7
23/tcp	0.67
21/tcp	0.57
143/tcp	0.15
1080/tcp	0.13
3128/tcp	0.07

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

04 avril 2008 version initiale.