Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 mars 2007
N° CERTA-2007-ACT-009

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2007-09

Gestion du document

Référence	CERTA-2007-ACT-009
Titre	Bulletin d'actualité 2007-09
Date de la première version	02 mars 2007
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-2007-ACT-009.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-2007-ACT-009/

1 Activités en cours

1.1 L'hébergement mutualisé de sites

Le CERTA a traité cette semaine le cas du site d'une administration victime de défiguration (remplacement de la page d'accueil). Après analyse, il s'est avéré que le site vulnérable ayant permis cet acte malveillant n'était pas le site de l'administration, mais un autre site hébergé sur le même serveur.

Nous rappelons donc que la sécurité d'un site (et plus généralement d'un système d'information) dépend à la fois de sa conception, mais aussi de l'environnement dans lequel il est placé. Il convient donc de prendre en compte tous les paramètres pouvant influer sur le système, sans se focaliser uniquement sur sa qualité intrisèque.

Concernant la problématique de l'hébergement mutualisé, une note d'information du CERTA ("Bonne pratiques concernant l'hébergement mutualisé", CERTA-2005-inf-005) donne quelque conseils et recommandations quant à ce type particulier d'hébergement.

1.2 Bombe logique

L'analyse d'une machine compromise a été faite par le CERTA. Cette machine était compromise par un code malveillant destiné à réaliser un déni de service contre une adresse IP située en Estonie. Le nom de domaine visé

correspond à un domaine victime d'attaque par un *malware*. Ce *malware* a la particularité de ne pas se mettre à jour et de ne pas recevoir d'ordre d'attaques depuis un point central. S'il n'est pas détecté à temps, le seul moyen de savoir qu'on est contaminé est de constater l'attaque.

En particulier, des traces de traffic important inhabituel vers l'Estonie ces dernières semaines pourraient être le signe de machines contaminées.

Le CERTA invite ses correspondants à le prévenir dans le cas où des traces seraient visibles dans les journaux.

1.3 Joyeux anniversaire

Depuis quelques jours, un ver de messagerie se propage sous la forme d'un message électronique intitulé « Anniversaire » et contenant le texte *Peux tu reconnaître qui est a coté de moi?*. Le fichier `Anniversaire.asx` est joint à ce message. Les fichiers au format `ASX` sont relatifs à des films vidéo, il est donc possible que le système d'exploitation affiche l'icône d'un lecteur multimedia devant le fichier.

Le fait de double-cliquer sur ce fichier provoque l'apparition d'une demande de téléchargement d'un prétendu *codec* sous la forme d'un fichier intitulé `codecs.exe`. Ce dernier se révèle être un code malveillant qui provoque lui-même le téléchargement d'autres programmes malveillants (`downloader`).

Ce ver a la particularité d'être rédigé en français, et d'avoir en pièce jointe un lien vers un code malveillant. Cette technique pourrait permettre d'échapper au contrôle des anti-virus.

Ce ver exploite une attaque par ingénierie sociale dans la mesure où il incite l'utilisateur à cliquer sur un message pour récupérer de faux codecs. Encore une fois, la plus grande prudence, et la plus grande protection, consistent à se méfier de toute sollicitation particulière, spécialement quand celle-ci ne semble pas provenir d'une source de confiance.

Par ailleurs, il est préférable de bloquer par défaut toute extension de fichier au niveau de la passerelle de messagerie, puis de n'autoriser que celles qui sont légitimes dans le réseau.

Recommandations :

Le CERTA recommande aux administrateurs de vérifier dans d'éventuels journaux de *proxy* si des appels à des fichiers `codecs.exe` ont été effectués, et de prévenir le CERTA le cas échéant.

Parmi les cas rencontrés, la deuxième phase de connexion s'effectuait vers les deux sites suivants :

– http://updatecodecs.t35.com
– http://servercodecs.com

2 Danger de la configuration par défaut d'Adobe Reader

2.1 Introduction

`PDF`, ou `Portable Document Format` est un format créée par la société Adobe Systems. Il permet de préserver la mise en forme du document, comme la police d'écriture, ou les objets graphiques, indépendemment de l'application ou de la plateforme utilisées pour le lire.

Il s'agit, malgré les apparences, d'un format très riche et très complexe. Pour s'en convaincre, il est possible de consulter un document de référence fourni par Adobe à l'adresse suivante :

http://www.adobe.com/devnet/pdf/pdf_reference.html

Le format autorise plusieurs options, comme par exemple le taux de compression des images et des textes, la qualité d'impression du document, et les droits qui lui sont accordés (interdiction de le modifier, de l'imprimer, etc.).

Il permet aussi d'être interactif en incorporant par exemple des menus déroulants, des champs de texte, afin d'obtenir des formulaires.

Le PDF a la particularité suivante : il peut contenir du code JavaScript. Ce dernier peut ensuite être interprété, ou pas, selon les applications de lecture utilisées. Par défaut, et à la date de rédaction de ce bulletin, `Adobe Acrobat Reader` et sa version Linux `acroread` l'interprètent. `Foxit Reader`, une alternative sous Windows, demande explicitement s'il faut installer le module JavaScript, tandis que `xpdf` ne l'interprète pas.

Dans la documentation fournie par Adobe, il est écrit que, bien qu'optionnelles, les actions suivantes sont possibles :

– une action JavaScript peut être déclenchée quand l'utilisateur frappe une combinaison de touches dans un champ de texte ;

– une action JavaScript peut être déclenchée avant que le champ soit formatté pour afficher sa valeur, ou quand celle-ci est modifiée ;
– une action JavaScript peut être déclenchée au moment d'enregistrer ou de fermer un document ;
– une action JavaScript peut être déclenchée avant ou après la phase d'impression du document ;
– etc.

En d'autres termes, des actions JavaScript peuvent être interprétées à tout moment si l'application de lecture le permet.

2.2 Le problème d'Acrobat Reader

Acrobat Reader comprend les liens réticulaires (URLs) de type `file://`. Ceux-ci sont un moyen pour regarder et naviguer dans le système de fichiers, ou les ouvrir. A valeur d'illustration, le fait de taper `file:///C:/` ouvre une fenêtre pour visiter la partition C: (si celle-ci existe).

Il est possible de combiner les deux propriétés citées ci-dessous, les interprétations de JavaScript et de l'URL `file://`, afin de permettre à des objets JavaScript d'accéder au système de fichiers et d'en voler, sous certaines conditions, le contenu.

Cette vulnérabilité existe dans les versions d'Adobe Acrobat Reader 6.0, 7.0 et 8.0 les plus récentes.

Du code d'exploitation est actuellement disponible sur l'Internet. Il est possible que des courriers électroniques, contenant des documents au format `.pdf` spécialement construits, apparaissent prochainement.

2.3 Recommandations du CERTA

Dans l'attente d'un correctif d'Adobe, il est fortement recommandé d'appliquer les mesures suivantes :
– désactiver l'interprétation de JavaScript par défaut : Edition => Préférences => JavaScript. Il faut décocher la case "Activer Acrobat JavaScript" ;
– désactiver les options Internet par défaut : Edition => Préférences => Internet. Il faut décocher les cases "Autoriser l'affichage rapide des pages Web", et "Autoriser le téléchargement spéculatif à l'arrière-plan".

Les recommandations plus classiques sont également applicables :
– vérifier que les applications et les anti-virus soient mis à jour ;
– n'ouvrir que des documents provenant de sources de confiance ;
– utiliser éventuellement une application alternative pour la lecture de documents PDF.

3 Telnet sous Sun Solaris

3.1 Rappel des faits

Le CERTA a mentionné dans le bulletin précédent l'existence d'une vulnérabilité concernant le service telnet sous Sun Solaris. Celle-ci a également fait l'objet de l'alerte CERTA-2007-ALE-005.

Pour rappel, cette vulnérabilité permet à un utilisateur de se connecter à distance sur le système vulnérable sans fournir un quelconque mot de passe.

3.2 Description du ver

Cette semaine, l'existence d'un ver exploitant cette vulnérabilité a été signalée. Le CERTA a mis l'alerte à jour pour en fournir les détails. Il utiliserait les comptes `adm` ou `lp` pour se propager. Sun fournit sur son bloc-notes quelques commandes pour vérifier que le ver n'a pas infecté la machine.

Par exemple, l'existence des fichiers `/var/adm/.profile` ou `/var/spool/lp/.profile`, ainsi que la modification de la table des tâches `crontab` seraient des indications d'une contamination par ce ver.

Bien que ce ver soit apparu, le CERTA n'a pas été informé d'activités de scan particulières vers le port telnet (TCP 23) cette semaine. Sa propagation ne semble actuellement pas virulente ou bruyante, bien que Sun mentionne dans son annonce un `active worm`.

Documentation

- Mise à jour de l'alerte CERTA-2007-ALE-005 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-005/
- Bloc-Note Sun :
  http://blogs.sun.com/security/entry/solaris_in_telnetd_worm_seen
- Bulletin d'alerte Sun #102802 mis à jour le 28 février 2007 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-102802-1

4 Certificats racines pour l'administration française

Le journal officiel de la république française du 17 février 2007 contient la publication des certificats de l'IGC/A.

L'éditeur de logiciel Microsoft a inclus les certificats dans la mise à jour facultative du 28 février 2007.

Des informations sont disponibles sur la page :
http://support.microsoft.com/kb/931125

Ceci ne concerne bien sûr que les systèmes Windows et les navigateurs Internet Explorer.

Pour prendre en compte ces certificats avec le navigateur Firefox, il convient de :

- se rendre sur le site de la DCSSI :
  http://www.ssi.gouv.fr/fr/sigelec/igca/installer.html
- de télécharger ces certificats au format `CRT`,
- d'ouvrir chacun des deux fichiers avec Firefox (ouvrir avec).

5 Vol d'informations de navigation sur Internet

Le CERTA a été informé de la possibilité de vol d'informations personnelles concernant les habitudes de navigation. Le principe général n'est pas récent , mais necessitait l'utilisation de code `JavaScript` que le CERTA recommande par ailleurs de désactiver par d éfaut dans le navigateur. Aujourd'hui, l'utilisation de `JavaScript` ne semble plus necessaire afin de connaitre les sites fréquentés par un internaute. Elle s'appuie sur la gestion des feuilles de styles concernant les pages visitées (format `CSS`).

Cette technique fonctionne avec la version 7.0 de `Microsoft Internet Explorer` et la version 2.0.0.2 de `Mozilla Firefox`.

Le CERTA, recommande de désactiver par défaut dans le navigateur, l'utilisation du `JavaScript` et, dans l'attente d'un correctif , de désactiver la fonction "historique" et nettoyer régulièrement le cache du navigateur Internet.

6 Vulnérabilité dans Google Desktop

Google desktop est une application permettant à un utilisateur d'effectuer des recherches de fichiers sur son système.

Récemment, une vulnérabilité dans Google Desktop a été publiée. Elle permet à une personne malintentionnée de prendre le contrôle de l'application à distance, et ainsi effectuer des recherches sur le système de fichiers de la victime, ou exécuter des applications présentes sur la machine.

Cette attaque nécessite tout d'abord une action de l'utilisateur, qui est l'exécution indirecte d'un script malveillant (une attaque de type cross-site scripting) sur le domaine www.google.com. Le script profite ensuite d'une vulnérabilité permettant l'exécution de code à chaque recherche de l'utilisateur sur Google Desktop.

Cette vulnérabilité a été corrigée dans une mise à jour de Google Desktop. Toutefois, d'une manière générale, il est recommandé de désactiver la fonctionnalité de recherche automatique sur la machine lors d'une requête sur internet.

Enfin, pour éviter les attaques d'exécution de code indirecte, le CERTA rappelle l'importance de vérifier les liens, de configurer sa messagerie pour lire les courriels en texte brut, et de taper manuellement les URL visitées.

7 Ports observés

Le tableau 3 et la figure 1 montrent les rejets pour les ports sous surveillance que nous avons constatés sur deux dispositifs de filtrage, entre le 22 février et le 01 mars 2007.

8 Liens utiles

- Mémento sur les virus :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/
- Note d'information sur l'acquisition de correctifs :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/index.html
- Note d'information sur les systèmes obsolètes :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html
- Note d'information sur les bonnes pratiques concernant l'hébergement mutualisé :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/index.html
- Note d'information sur les mots de passe :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/index.html
- Note d'information sur la terminologie d'usage au CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/index.html
- Note d'information sur les enjeux de sécurité liés à une migration vers IPv6 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
  http://www.auscert.org.au/render.html?it=1935
- Note d'information du CERTA CERTA-2006-INF-006, Risques associés aux clés USB :
  http://www.certa.ssi.gouv.f r/site/CERTA-2000-INF-006/
- Note d'information du CERTA CERTA-2006-INF-008 sur les outils d'indexation et de recherche :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/

9 Rappel des avis émis

Durant la période du 23 février au 01 mars 2007, le CERTA a émis les avis suivants :

- CERTA-2007-AVI-099 : Vulnérabilité de TYPO3
- CERTA-2007-AVI-100 : Vulnérabilité dans IBM DB2
- CERTA-2007-AVI-101 : Vulnérabilité dans Novell ZENworks
- CERTA-2007-AVI-102 : Multiples vulnérabilités de produits Mozilla
- CERTA-2007-AVI-103 : Vulnérabilité de eTrust
- CERTA-2007-AVI-104 : Vulnérabilités dans les Cisco Catalyst
- CERTA-2007-AVI-105 : Vulnérabilité dans McAfee Virex
- CERTA-2007-AVI-106 : Vulnérabilité dans Citrix Presentation Server

Pendant cette période, des avis ainsi qu'une alerte ont également été mis à jour :

- CERTA-2007-ALE-005-001 : Vulnérabilité de Sun Solaris
  (ajout d'informations concernant la propagation d'un ver)
- CERTA-2007-AVI-069-001 : Multiples vulnérabilités sous PostgreSQL
  (ajout de la référence au bulletin de sécurité Sun Solaris)
- CERTA-2007-AVI-090-001 : Multiples vulnérabilités de produits Cisco
  (correction des liens)

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.

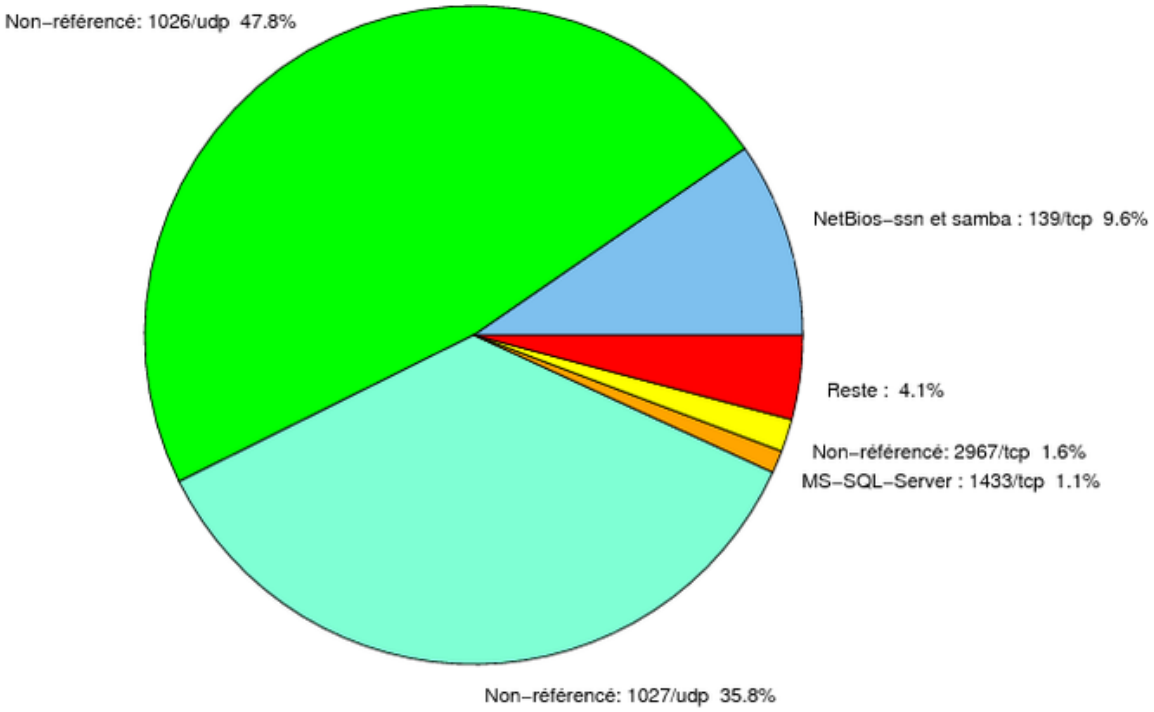

FIG. 1: Répartition relative des ports pour la semaine du 23.02.2007 au 02.03.2007

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
22	TCP	SSH	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
23	TCP	Telnet	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
25	TCP	SMTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
42	TCP	WINS	–	http://www.certa.ssi.gouv.fr/site/CE
80	TCP	HTTP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
106	TCP	MailSite Email Server	–	–
111	TCP	Sunrpc-portmapper	–	http://www.certa.ssi.gouv.fr/site/CE
119	TCP	NNTP	–	http://www.certa.ssi.gouv.fr/site/CE
135	TCP	Microsoft RPC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
137	UDP	NetBios-ns	–	http://www.certa.ssi.gouv.fr/site/CE
139	TCP	NetBios-ssn et samba	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
143	TCP	IMAP	–	http://www.certa.ssi.gouv.fr/site/CE
389	TCP	LDAP	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
443	TCP	HTTPS	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
445	TCP	Microsoft-smb	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	http://www.certa.ssi.gouv.fr/site/CE
1433	TCP	MS-SQL-Server	–	http://www.certa.ssi.gouv.fr/site/CE
1434	UDP	MS-SQL-Monitor	–	http://www.certa.ssi.gouv.fr/site/CE
2100	TCP	Oracle XDB FTP	–	http://www.certa.ssi.gouv.fr/site/CE

2381	TCP	–	HP System Management	http://www.certa.ssi.gouv.fr/site/CE
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	http://www.certa.ssi.gouv.fr/site/CE
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
3306	TCP	MySQL	–	–
3389	TCP	Microsoft RDP	–	http://www.certa.ssi.gouv.fr/site/CE
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–
5900	TCP	VNC	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
6070	TCP	BrightStor ARCserve/Enterprise Backup	–	http://www.certa.ssi.gouv.fr/site/CE
6101	TCP	Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE
6112	TCP	Dtspcd	–	http://www.certa.ssi.gouv.fr/site/CE
6129	TCP	Dameware Miniremote	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
8866	TCP	–	Porte dérobée Bagle.B	–
9898	TCP	–	Porte dérobée Dabber	–
10000	TCP	Webmin, Veritas Backup Exec	–	http://www.certa.ssi.gouv.fr/site/CE http://www.certa.ssi.gouv.fr/site/CE
10080	TCP	Amanda	MyDoom	–
13701	TCP	Veritas NetBackup	–	http://www.certa.ssi.gouv.fr/site/CE
18264	TCP	CheckPoint interface	–	http://www.certa.ssi.gouv.fr/site/CE

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

port	pourcentage
1026/udp	47.75
1027/udp	35.81
139/tcp	9.58
2967/tcp	1.6
1433/tcp	1.1
1434/udp	0.94
1080/tcp	0.78
4899/tcp	0.7
137/udp	0.49
22/tcp	0.32
25/tcp	0.29
3128/tcp	0.13
21/tcp	0.12
143/tcp	0.06
15118/tcp	0.05
3127/tcp	0.04
3306/tcp	0.02
9898/tcp	0.01

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

02 mars 2007 version initiale.