Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 mai 2008
N° CERTA-2008-ACT-021

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2008-21

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-021`

Gestion du document

Référence	CERTA-2008-ACT-021
Titre	Bulletin d'actualité 2008-21
Date de la première version	23 mai 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-021.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-021/

1 Les incidents de la semaine

Cette semaine, un forum non modéré sur un site public a permis la diffusion de liens vers des sites pornographiques. Au-delà des problèmes de responsabilité liés au contenu, le CERTA attire l'attention sur la possibilité de détourner un tel forum pour mener des attaques informatiques.

Pour réaliser une infection d'ordinateurs à grande échelle, par exemple pour constituer un *botnet*, un « cyber-attaquant » peut compromettre un site très fréquenté et y déposer un lien vers un site malveillant. Ce dernier site réalise l'infection du poste de l'internaute. Ce schéma est bien connu. Il a mis en lumière le rôle de certains objets *HTML* comme les `<IFRAME>` et des ensembles de logiciels malveillants comme *Mpack*. Des milliers de sites italiens en ont été victimes en 2007. D'autres vagues ont eu lieu depuis. Ces insertions de liens malveillants ont nécessité de la part de l'attaquant la recherche de vulnérabilités sur les sites visés. Un forum non modéré sans le moindre filtrage permet à quiconque de publier de tel liens sans avoir à trouver de vulnérabilité sur un site web.

Le problème fondamental est le contrôle sur le contenu de sites publics. Les forums, les blogs et toutes les applications qui permettent à tout internaute d'ajouter du contenu qui sera automatiquement publié présentent cet inconvénient.

Le CERTA recommande le filtrage à la fois syntaxique et démantique des entrées des internautes. La recommandation n'est pas technique, mais organisationnelle. Son application se traduit par la désignation de modérateurs ou de responsables d'édition.

2 Vulnérabilité OpenSSL et OpenSSH - suite

Le CERTA détaillait dans le bulletin d'actualité de la semaine dernière CERTA-2008-ACT-020 qu'un problème d'aléa faible avait été mis en évidence dans les versions *Debian* d'`OpenSSL` et `OpenSSH`. Il existe désormais sur l'Internet des bases complètes de clefs vulnérables pré-calculées. Ceci facilite évidemment le travail d'un potentiel attaquant car il lui suffit d'utiliser ces fichiers pour essayer un ensemble de clefs sur un serveur vulnérable. Par ailleurs, la vulnérabilité affectant `OpenSSL` peut avoir un impact qui va bien au-delà des serveurs offrant une couche `SSL`. On pourra prendre comme exemple une infrastructure sans-fil s'appuyant sur la norme `WPA2` qui offre, entre autres, une authentification `TLS` via un serveur de type `RADIUS` (mode *WPA Enterprise*). Or les certificats et clefs associées utilisés par le serveur `RADIUS` pour réaliser cette authentification peuvent avoir été créés par une version d'`OpenSSL` vulnérable. Il devient alors possible à un attaquant de s'introduire sur un réseau sans-fil `WPA2` réputé pourtant pour son niveau de sécurité convenable.

Dans ce contexte, il reste impératif de s'assurer de la mise à jour des paquetages `OpenSSL` et `OpenSSH` sur les distributions `Debian` et dérivées. Mais il est toujours indispensable de s'assurer que toute clef ou certificat vulnérable a bien été remplacé par un nouveau engendré à partir d'un paquetage à jour.

3 Le jargon des antivirus

Qui n'a jamais été confronté au choix cornélien proposé par un antivirus ? Doit-on choisir *désinstaller* ? Mettre en quarantaine ? Qu'est-ce qui se cache derrière ces termes ? Essayons de lever le voile sur ces expressions connues de tous et pourtant toujours aussi obscures.

Avant cela, rétablissons une vérité. Un antivirus est un logiciel qui permet à l'origine de détecter (le mot a son importance) un code malveillant suivant certaines méthodes (base de signature, apprentissage automatique, etc.). Il s'agit d'un indicateur, basé sur des règles, mises à jour plus ou moins régulièrement et plus ou moins efficaces, mais en aucun cas d'un outil permettant de réparer un problème. Il doit donc être utilisé en ayant conscience de cet aspect structurel, et en gardant à l'esprit qu'un tel logiciel ne doit pas devenir la clef de voûte de la sécurité d'un système d'information, mais plutôt une aide supplémentaire utile une fois que tout le reste a été mis en place (mises à jour, cloisonnement, éducation des utilisateurs, etc.).

Une fois qu'un problème a été découvert, en règle générale, la plupart des antivirus vous proposent plusieurs choix : ne rien faire, supprimer le programme découvert, désinfecter le fichier, ou le mettre en quarantaine. Les deux premières propositions semblent parfaitement claires, les deux suivantes un peu moins :

- « désinfecter » : cette action permet d'essayer de retirer une partie *infectée* d'un fichier légitime. La zone en question est alors comblée le plus souvent par du *padding* (remplissage inerte).
- « mettre en quarantaine » : ceci a pour effet de renommer le fichier incriminé et parfois de limiter ses droits afin de restreindre les accès qui pourraient être fait.

Même si ces choix semblent, de prime abord, permettre une désinfection correcte d'un poste contaminé, quelques doutes subsistent. En effet, comment s'assurer dans le cadre d'une suppression que toutes les composantes du code malveillant ont été supprimées (clefs de registre, dll, fichiers temporaires, etc.) ? Comment s'assurer que la désinfection a supprimé toutes les parties malveillantes d'un programme légitime ? Et comment s'assurer que le fichier mis en quarantaine ne soit pas à nouveau exécuté, volontairement ou non, par une personne ou par un autre code ? Ce n'est *a priori* pas possible. Dès l'instant où une machine est compromise, le doute subsistera tant que celle-ci ne sera pas proprement réinstallée.

Il convient donc de comprendre les enjeux réels ainsi que les forces et les faiblesses d'un antivirus avant d'opter pour l'installation de cet outil. Cette bonne pratique reste valable, bien entendu, pour la plupart des outils de sécurité : comprendre avant d'utiliser.

4 Cartographie de réseaux

Certaines personnes cherchent à cartographier les réseaux, à la recherche de services spécifiques. Par exemple, les listes de serveurs mandataires (*proxies*) « ouverts » sont généralement établies à la suite de sondages réseau

(*network scan*) massifs sur des ports bien précis. Sans connaître les réelles motivations des auteurs de ces cartographies, nous pouvons néanmoins soulever les problèmes suivants :

- nous rappelons que ce qui est autorisé en France peut être interdit à l'étranger ;
- les « scans » des réseaux peuvent être non conformes à la charte d'utilisation des moyens informatiques ;
- les sondages réseau peuvent, par le volume de paquets envoyés et reçus, engendrer dans certains cas des dégradations de performances voire des dénis de service ;
- certains administrateurs réagissent à cette activité par une mise en liste noire (*blacklisting*) ce qui peut, par effet de bord, conduire à un déni de service ;
- les réseaux de CSIRTs (*Computer Security Incident Response Team*) sont généralement sollicités pour résoudre les incidents liés à cette activité, puisqu'elle peut avoir pour origine une machine compromise.

Le CERTA déconseille donc fortement d'avoir recours à ce genre d'activité, même si l'auteur de celle-ci le fait « de bonne foi » depuis une de ses machines. Quelle que soit la motivation ou le moyen employé, les cartographies de réseau peuvent avoir des effets néfastes.

5 Vulnérabilité dans Internet Explorer 7 et 8 bêta

Une nouvelle faille concernant Internet Explorer 7 et 8 bêta a été publiée la semaine dernière.

Les deux versions de ce navigateur proposent une fonctionnalité peu utilisée, qui est l'ajout d'une table de liens lors de l'impression d'une page. Cette fonctionnalité est vulnérable, car une personne malintentionnée peut, via un lien spécialement conçu, provoquer l'exécution de code arbitraire.

Cette faille est due au fait que le système, lors de l'impression de la table de liens d'une page, ne vérifie pas les liens et qu'il est donc possible d'y injecter des scripts. Ceux-ci sont alors exécutés en zone locale, qui n'est pas soumise aux mêmes règles de sécurité que la zone Internet (confirmation par exemple de l'exécution de scripts par l'utilisateur, etc.).

L'ajout d'une table de liens dans l'impression d'une page étant une fonctionnalité très peu utilisée, le CERTA n'a pas émis d'alerte concernant cette vulnérabilité. Son utilisation est évidemment fortement déconseillée jusqu'à la publication d'un correctif par Microsoft.

6 Adobe AIR

Adobe AIR est le nouveau kit de développement de l'éditeur créateur du format *PDF*. L'acronyme de *AIR* signifie *Adobe Integrated Runtime*. Cet outil est issu du rachat de la société *Macromedia* par *Adobe* et vise à créer des applications uniques permettant la visualisation des formats *PDF* et *swf*. *Adobe AIR* se base sur un environnement d'exécution, il permet la programmation avec les langages Flash/Flex/ActionScript ou HTML/Javascript/CSS/AJAX avec le kit dédié aux applications Internet.

Les applications développées avec cet environnement de développement permettent de nombreuses actions :

- lancement de tâches de fond ;
- service Internet *web service* ;
- ressources réseaux *sockets* ;
- manipulation de fichiers ;
- stockage en local et paramétrage d'*API*.

Les applications utilisant cette technologie sont de plus en plus fréquentes. On peut notamment citer ReadAir, un agrégateur de flux d'informations de type *RSS*, le site eBay, AOL,...

Le CERTA tient donc à attirer l'attention sur ces applications qui permettent de nombreuses actions. Il est important de vérifier le fonctionnement de ces applications avant de les déployer. Sous la perspective d'applications Internet riches et interactives peut se cacher des intentions intrusives ou malveillantes. De manière plus générale, le CERTA est toujours très prudent sur l'utilisation d'applications reposant sur des technologies capables d'exploiter une multitude de fonctionnalités sans en maîtriser l'implémentation.

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 15 et le 22 mai 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 16 au 22 mai 2008, le CERTA a émis les avis suivants :

- CERTA-2008-AVI-247 : Multiples vulnérabilités dans Symantec Altiris Deployment Solution
- CERTA-2008-AVI-248 : Vulnérabilité dans Red Hat Directory Server
- CERTA-2008-AVI-249 : Multiples vulnérabilités dans Net-snmp
- CERTA-2008-AVI-250 : Multiples vulnérabilités dans libvorbis
- CERTA-2008-AVI-251 : Vulnérabilités dans Citrix Presentation Server
- CERTA-2008-AVI-252 : Multiples vulnérabilités du noyau Linux
- CERTA-2008-AVI-253 : Vulnérabilité dans les produits Cisco CSM
- CERTA-2008-AVI-254 : Vulnérabilité de Cisco Unified Presence
- CERTA-2008-AVI-255 : Multiples vulnérabilités dans Cisco Unified Communications Manager
- CERTA-2008-AVI-256 : Vulnérabilité de Cisco Building Broadband Service Manager
- CERTA-2008-AVI-257 : Multiples vulnérabilités dans IBM Lotus Domino Web Server
- CERTA-2008-AVI-258 : Vulnérabilités dans CA ARCserve Backup
- CERTA-2008-AVI-259 : Vulnérabilité d'Emacs
- CERTA-2008-AVI-260 : Vulnérabilité dans Alcatel OmniPCX Office
- CERTA-2008-AVI-261 : Vulnérabilité d'un préprocesseur de Snort
- CERTA-2008-AVI-262 : Multiples vulnérabilités dans GnuTLS
- CERTA-2008-AVI-263 : Vulnérabilité dans HP-UX
- CERTA-2008-AVI-264 : Vulnérabilité dans IBM Lotus Sametime
- CERTA-2008-AVI-265 : Vulnérabilité de Nagios
- CERTA-2008-AVI-266 : Vulnérabilités dans Trillian
- CERTA-2008-AVI-267 : Multiples vulnérabilités d'AIX
- CERTA-2008-AVI-268 : Multiples vulnérabilités du serveur SSH des équipements Cisco
- CERTA-2008-AVI-269 : Multiples Vulnérabilités dans Cisco Service Control Engine

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'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.

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 oeuvre (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 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.

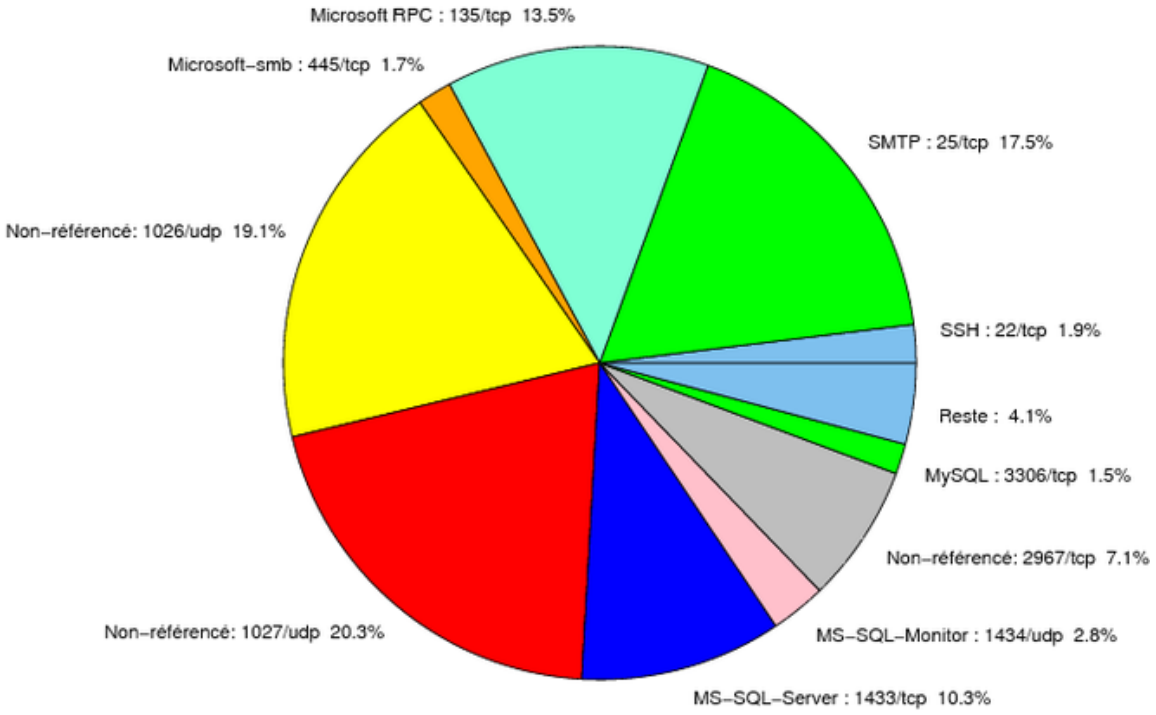

FIG. 1: Répartition relative des ports pour la semaine du 15.05.2008 au 22.05.2008

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
1027/udp	20.32
1026/udp	19.13
25/tcp	17.48
135/tcp	13.45
1433/tcp	10.31
2967/tcp	7.07
1434/udp	2.84
22/tcp	1.94
445/tcp	1.74
3306/tcp	1.54
80/tcp	1.49
139/tcp	0.79
137/udp	0.74
4899/tcp	0.44
143/tcp	0.39
1080/tcp	0.04

TAB. 3: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

23 mai 2008 version initiale.